Computability of Rational Points on Curves over Function Fields in Characteristic $p$

1 Introduction

Let $k$ be a perfect field of characteristic $p$ and $K$ a function field over $k$. That is, $K = k(V)$ for some integral variety $V$ over $k$. Let $X$ be a geometrically integral, regular, projective curve over $K$ with arithmetic genus $g := g(X) = \dim_K H^1(X, \mathcal{O}_X)$. There are two important cases when $X(K)$ is known to be finite, namely

(i) $X$ is smooth, $g \geq 2$, and $X$ is not isotrivial [8], and

(ii) $X$ is not smooth.

Case (ii) occurs only in characteristic $p$ and is equivalent to $g > g(\widetilde{X}_K)$, where $\widetilde{X}_K$ is the normalization of $X_K$. The number $\widetilde{g} := g(\widetilde{X}_K)$ is known as the absolute genus of $X$. The fact that $X(K)$ is finite for such curves was proved by Samuel in the case where $\widetilde{g} \geq 2$ ([8], Théorème 6) and by Voloch and Jeong in the cases where $\widetilde{g} = 0$ or $\widetilde{g} = 1$ [15][4].

This paper is concerned with the question of computing the set $X(K)$. For case (i), this was solved by Szpiro [13] in the form of an explicit bound for the heights of rational points on $X$ (see Theorems 6.6, 6.8, and 6.10 below). Here, we answer the question for case (ii).

**Theorem 1.1.** Let $K$ be a field of characteristic $p$ finitely generated over a perfect field $k$. Let $X$ be a geometrically integral, regular, projective curve over $K$ that is not smooth. Then, $X(K)$ is finite and computable.

This theorem, together with Theorem 6.10 below, gives the following interesting corollary, to be proved in Section 6.

**Corollary 1.2.** Let $K$ be as in Theorem 1.1, and let $X$ be a geometrically integral, regular, projective curve over $K$. If $X(L)$ is finite for every finite separable extension $L$ of $K$, then $X(K)$ is computable.

The rest of this paper is devoted to the proof of Theorem 1.1. In Section 2, we elaborate on what it means for $X(K)$ to be computable. In Section 3, we give some background lemmas concerning curves $X$ that are regular but not smooth and prove facts that hold in any absolute genus. In particular, in proving Theorem 1.1, we show that it suffices to assume $K$ is a function field in one variable over $k$ and that there exists an inseparable degree $p$ morphism $\pi: X \to Y$, where $Y$ is a smooth curve over $K$ with $g(Y) = \widetilde{g}$. This latter assumption was a crucial step in [15] and is important for Proposition 3.8, which is used in every subsequent section. In Section 4, we handle the case where $\widetilde{g} = 0$. The approach here is an effective version of the proof of finiteness of $X(K)$ given in [4]. In Sections 5 and 6, we handle the cases where $\widetilde{g} = 1$ and $\widetilde{g} \geq 2$ respectively. In both sections, we give separate proofs in the cases where $Y$ is isotrivial and $Y$ is not isotrivial.
2 Computability

To make sense of the statement of Theorem 1.1, all elements of $K$ need to be described with a finite amount of information. Therefore, we assume $k$ has finite transcendence degree over $\mathbb{F}_p$. If $k$ is not algebraically closed, then $X(K)$ can be computed by first computing $X(kK)$ and checking which points are $K$-points. For this reason, we assume $k$ is algebraically closed. The curve $X$ will be definable over some field $K_0$ whose field of constants $k_0$ is finitely generated over $\mathbb{F}_p$. There will then exist a finite field extension $k_1$ of $k_0$ such that $X(K) = X(k_1K_0)$.

To explicitly specify a field $F$, we give a finite set of generators for $F$ over $\mathbb{F}_p$ (or another field already specified) together with any algebraic relations the generators satisfy. To specify a projective variety $V$ over a field $F$, we give generators of its homogeneous ideal for an embedding of $V$ in some projective space over $F$.

Given all of the above, in proving Theorem 1.1, we show that there exists an algorithm that takes the following as input.

**Input 2.1.**

(i) a prime number $p$,

(ii) a field $k_0$ finitely generated over $\mathbb{F}_p$,

(iii) a nonnegative number $m \in \mathbb{Z}_{\geq 0}$,

(iv) a finite separable extension $K_0$ of $k_0(t_1, \ldots, t_m)$ such that the largest algebraic extension of $k_0$ in $K_0$ is $k_0$, with $K := k_0K_0$, and

(v) a geometrically integral, nonsmooth, projective curve $X$ over $K_0$ such that $X_K$ is regular.

The algorithm will then give as output a finite extension $k_1/k_0$ with $K_1 := k_1K_0$ such that $X(K) = X(K_1)$ as well as the set $X(K_1)$. In Section 3, we show that we can make simplifying assumptions on $X$ and $K$. Therefore, to prove Theorem 1.1, Input 2.1 will be replaced by Input 3.14.

3 Regular nonsmooth curves

**Lemma 3.1.** Let $k$ be a field of characteristic $p$, and let $K$ be a field with separating transcendence basis $\{t_i\}_{i \in I} \subseteq K$ over $k$. Then $K$ is a purely inseparable extension of $kK^p$ generated by $\{t_i\}$. If $I$ is a finite set of size $n$, then $[K : kK^p] = p^n$.

**Proof.** $K$ is separable over $k(\{t_i\})$, and $K$ is purely inseparable over $kK^p$. This means $K$ is both separable and purely inseparable over $kK^p(\{t_i\})$, i.e., $K = kK^p(\{t_i\})$. If $I$ is a finite set of size $n$, then by a similar argument, $k(\{t_i\}) \cap kK^p = k(\{t_i^p\})$. Thus,

$$[K : kK^p] = [k(t_1, \ldots, t_n) : k(t_1^p, \ldots, t_n^p)] = p^n.$$

**Remark 3.2.** We will use Lemma 3.1 frequently in the following two cases.
(i) Let $K$ be a field of characteristic $p$ that is finitely generated over a perfect field $k$. If $t_1, \ldots, t_m$ is a transcendence basis of $K$ over $k$, then $K$ is a degree $p^m$ purely inseparable extension of $K^p$ generated by $t_1, \ldots, t_m$.

(ii) Let $K$ be a field of characteristic $p$, and let $X$ be an integral curve over $K$. Assume further that $X$ is geometrically reduced over $K$ so that there exists $z \in K(X)$ such that $K(X)$ is a finite separable extension of $K(z)$. Then, $K(X)$ is a degree $p$ purely inseparable extension of $K \cdot K(X)^p$ generated by $z$.

**Proposition 3.3.** Let $K$ be a field of characteristic $p$, and let $X$ be a geometrically integral projective curve over $K$ that is regular but not smooth. Let $X_i$ be a regular projective curve over $K$ with function field $K \cdot K(X)^p$. Let $g_i := g(X_i)$ and $\tilde{g} := g(\overline{X_{\overline{R}}})$, where $\overline{X_{\overline{R}}}$ is the normalization of $X_{\overline{R}}$. Then,

$$g_0 \geq g_1 \geq g_2 \geq \cdots$$

and $g_i = \tilde{g}$ for sufficiently large $i$. For such $i$, the curve $X_i$ is smooth.

**Proof.** First, notice that for $i \geq 0$,

$$K^{1/p_i}(\overline{X_{K^{1/p_i}}}) = K^{1/p_i} \cdot K(X) \cong K \cdot K(X)^p = K(X_i),$$

so $g_i = g(\overline{X_{K^{1/p_i}}})$. Then,

$$g_i = g(\overline{X_{K^{1/p_i}}}) = g\left((\overline{X_{K^{1/p_i}}})^{K^{1/p^{i+1}}_p}\right) \geq g\left((\overline{X_{K^{1/p^{i+1}}_p}})^{K^{1/p^{i+1}}_p}\right) = g(\overline{X_{K^{1/p^{i+1}}_p}}) = g_{i+1}$$

(e.g., [3], exercise IV.1.8). Now, $\overline{X_{\overline{R}}}$ is smooth and definable over some finite extension $L$ of $K$, so $\overline{X_L}$ is smooth. Let $M$ be the maximal subextension of $L$ that is separable over $K$. Then, $L^{p^e} \subset M$ for some $e$, so $\overline{X_{M^{p^{-e}}}}$ is smooth. Regular curves remain regular after base changing to a finite separable field extension (see [1], XV.5, Theorem 22), and $M^{p^{-e}}$ is separable over $K^{p^{-e}}$, so $\overline{X_{K^{p^{-e}}}}$ is smooth. Thus, $g_i = \tilde{g}$ and $X_i$ is smooth for all $i \geq e$. \qed

**Proposition 3.4.** Suppose there exists an algorithm that takes in Input 2.1 as well as the extra input

-(vi) a geometrically integral, smooth, projective curve $Y$ over $K_0$ with $g(Y) = g(\overline{X_{K}})$ together with a degree $p$ inseparable morphism $\pi : X \to Y$ over $K_0$.

and computes $X(K)$. Then there exists an algorithm to compute $X(K)$ without assuming (vi). Furthermore, assuming (vi), choose any $z \in K_0(X) \setminus K_0(Y)$ and $r := z^p \in K_0(Y)$. If there exists an algorithm to compute the set

$$\{P \in Y(K) \mid r \text{ is regular at } P \text{ and } r(P) \in K^p\},$$

then there exists an algorithm to compute $X(K)$.
Proof. Let $X_i$ be the normalization of $X^{(p^r)}$. Then $K_0(X_i) = K_0 \cdot K_0(X_i)^{p^r}$. Compute the curves $X_i$ for $i = 1, 2, 3, \ldots, n$, where $n$ is the smallest positive integer such that $X_n$ is smooth, which exists by Proposition 3.3. The relative Frobenius morphisms lift to a sequence of morphisms

$$X = X_0 \to X_1 \to X_2 \to \cdots \to X_{n-1} \to X_n.$$ 

The curve $X_{n-1}$ is nonsmooth and the morphism $X_{n-1} \to X_n$ satisfies the condition in (vi). Thus, use the presumed algorithm to compute $X_{n-1}(K)$. Then, compute $X(K)$ by computing preimages in the above sequence of morphisms.

Now, assume (vi) and choose any $z$ as in the statement of the proposition. Let $V \subset Y$ be the maximal affine open subset on which $r$ is regular, let $U := \pi^{-1}(V) \subset X$, and let

$$W := \{(w, P) \in \mathbb{A}^1_{K_0} \times V \mid w^p = r(P)\}.$$ 

Considering $r$ as a morphism $Y \to \mathbb{P}^1_{K_0}$, compute the poles of $r \circ \pi$ that are $K$-points of $X$. These are the $K$-points in $X \setminus U$, so all that remains is to compute $U(K)$. The morphism $W \to V \to Y$ induces a bijection

$$W(K) \to \{P \in Y(K) \mid r \text{ is regular at } P \text{ and } r(P) \in K^p\}.$$ 

Therefore, compute $W(K)$ using the presumed algorithm. Lastly, compute $U(K)$ by computing preimages in the (normalization) $K_0$-morphism morphism $U \to W$ defined by $Q \mapsto (z(Q), \pi(Q))$. 

Remark 3.5. Let $X$ be as in Proposition 3.4(i) and $L_0$ be a finite separable extension of $K_0$ with $L := kL_0$. To compute $X(K)$, it suffices to compute $X(L)$ and then determine which points are $K$-points. In this case, $X_{L_0}$ is again regular but not smooth [1], and $\pi_{L_0} : X_{L_0} \to Y_{L_0}$ is purely inseparable of degree $p$.

Lemma 3.6. Let $K$ be a field of characteristic $p$ that is separably generated over a field $k$, and let $D$ be the set of $k$-derivations of $K$. If $\alpha \in K$, then $\alpha \in kK^p$ if and only if $\delta \alpha = 0$ for all $\delta \in D$. Furthermore, if $V$ is a variety over $kK^p$, then each $\delta \in D$ can be extended to a $k$-derivation of $\mathcal{O}_{V_K}$ such that

$$\bigcap_{\delta \in D} \ker(\delta : \mathcal{O}_{V_K} \to \mathcal{O}_{V_K}) = \mathcal{O}_V$$ 

(here, $V_K \to V$ is a homeomorphism, so we consider $\mathcal{O}_{V_K}$ and $\mathcal{O}_V$ to be sheaves on the same topological space). If $\delta \in D$ and $U \subset V_K$, then the extension of $\delta$ to $\mathcal{O}_{V_K}(U)$ will be denoted $v \mapsto v^\delta$.

Proof. If $\alpha = \beta^p$, then $\delta \alpha = p^\beta \delta \beta = 0$. Conversely, suppose $\delta \alpha = 0$ for all $\delta$. By assumption, there exists a transcendence basis $\{t_i\}_{i \in I}$ of $K$ over $k$ such that $K$ is a separable algebraic extension of $k(\{t_i\}_{i \in I})$. By Lemma 3.1, $K$ is a purely inseparable algebraic extension of $kK^p$ with $K = kK^p(\{t_i\}_{i \in I})$. Write $\alpha = \sum c_j t^i$, where $j \in \{0, 1, \ldots, p-1\}^I$, $t^i = \prod_{i \in I} t_i^{l_i}$, and $c_j \in kK^p$. If $\delta_i$ is the derivation of $K$ such that $\delta_i t_i = 1$ and $\delta_i t_{i'} = 0$ for all $i' \neq i$, then $0 = \delta_i \alpha = \sum_j j_i c_j t_j^{i-1}$, where $l_i$ is the index with 1 in the $i$th entry and 0
in every other entry. Thus, \( c_j = 0 \) for all \( j \) such that \( j_i \neq 0 \) for some \( i \neq 0 \). In other words, \( \alpha \in kK^p \).

Now note that \( \mathcal{O}_V = \mathcal{O}_V \otimes \mathcal{O}_K \otimes kK^p \) \( K^p \). If \( U \subset V \) is an open subset, then extend \( \delta \) to \( \mathcal{O}_V(U) \) by \( v \otimes u \mapsto v \otimes \delta u \) for \( v \in \mathcal{O}_V(U) \) and \( u \in K \). Thus

\[
\bigcap_{\delta \in D} \ker (\delta : \mathcal{O}_V \to \mathcal{O}_K) = \mathcal{O}_V \otimes \mathcal{O}_K \bigcap_{\delta \in D} \ker (\delta : K \to K) = \mathcal{O}_V \otimes \mathcal{O}_K \otimes kK^p = \mathcal{O}_V.
\]

\( \square \)

**Remark 3.7.** If \( K \) is finitely generated over a perfect field \( k \) of characteristic \( p \), then \( K \) is separably generated over \( k \) (e.g., [5], Corollary 4.4). Furthermore, from the proof of Lemma 3.6, we see that to check \( \delta \alpha = 0 \) for all \( \delta \), it suffices to check \( \delta_i \alpha = 0 \) for all \( i \). Similarly, \( \nu^\delta = 0 \) for all \( \delta \) if and only if \( \nu^\delta_i = 0 \) for all \( i \).

**Proposition 3.8.** There exists an algorithm that takes in Input 2.1, (vi) and the morphism \( r \) from Proposition 3.4, a smooth projective curve \( Z \) over \( K_0 \), and an inseparable \( K_0 \)-morphism \( f : Z \to Y \) and computes the set

\[
\{ P \in Y(K) \mid r \text{ is regular at } P, r(P) \in K^p, \text{ and } P = f(Q) \text{ for some } Q \in Z(K) \}.
\]

**Proof.** View \( r \) as a morphism \( Y \to \mathbb{P}^1_{K_0} \). The composition \( r \circ f \) is inseparable, so it factors as \( r \circ f = s \circ F \), where \( F : Z \to Z^{(p)} \) is the relative Frobenius morphism and \( s \) is some morphism \( s : Z^{(p)} \to \mathbb{P}^1_{K_0} \). Explicitly, \( Z^{(p)} \) is defined by the same polynomials as \( Z \) but with their coefficients raised to the \( p \)th power. Compute the morphism \( s \). Let \( V \) be the curve defined over \( K_0^p \) given by the same polynomials as \( Z^{(p)} \), so that \( Z^{(p)} \simeq V_{K_0} \). Let \( \delta_1, \ldots, \delta_m \) be the derivations of \( K_0 \) corresponding to \( t_1, \ldots, t_m \). Because \( Z \) is smooth, \( V \) is smooth and therefore geometrically reduced. So, extend \( \delta_1, \ldots, \delta_m \) to derivations of \( K_0(V) = K_0(Z^{(p)}) \) as in Lemma 3.6. Let \( U \) be the maximal affine open subset of \( Z \) on which \( r \circ f \) is regular, and compute an embedding \( U \to \mathbb{A}^n_{K_0} \).

If \( (\alpha_1, \ldots, \alpha_n) \in U(K) \). Then,

\[
\delta_i(r(f(\alpha_1, \ldots, \alpha_n))) = \delta_i(s(\alpha_1^p, \ldots, \alpha_n^p))
\]

\[
= \sum_{i=1}^n \frac{\partial s}{\partial x_i}(\alpha_1^p, \ldots, \alpha_n^p)\delta_i \alpha_i^p + s^{\delta_i}(\alpha_1, \ldots, \alpha_n).
\]

Now, we claim that \( s^{\delta_i} \neq 0 \) for some \( i \). Suppose the contrary. Then, Remark 3.7 says \( s \in K_0^p(V) \), so \( s \circ F \in K_0(Z)^p \). Let \( (s \circ F)^{1/p} \in K_0(Z) \) be its \( p \)th root. Then, there exists a nonconstant morphism \( Z \to X \) defined on \( U \) by

\[
P \mapsto ((s \circ F)^{1/p}(P), f(P)).
\]

But, \( Z \) is smooth, which would imply \( X \) is smooth ([11], Lemma 0CCW). This is false by assumption, so \( s^{\delta_i} \neq 0 \) for some \( i \). Thus, let \( S \) be the zero set of all the \( s^{\delta_i} \circ F \) on \( Z \) so that

\[
S(K) = \{ P \in Z(K) \mid r \circ f \text{ is regular at } P \text{ and } r(f(P)) \in K^p \}.
\]

\( S \) is a 0-dimensional \( K_0 \)-variety, so compute \( S(K) \). Lastly, apply \( f \) to the elements of \( S(K) \) to get the set stated in the proposition.  \( \square \)
Lemma 3.9. Let $K$ be a field of characteristic $p$, let $X$ be a geometrically integral regular curve over $K$, and let $x$ be a closed point of $X$. Let $L$ and $K'$ be finite extensions of $K$ that are linearly disjoint over $K$. Let $L' := LK'$. Let $x_{L'} \in (\widetilde{X}_{K'})_{L'}$ be in the preimage of $x$ and $x_L$ its image in $X_L$. If $x_L$ is not a regular point of $X_L$, then $x_{L'}$ is also not a regular point of $(\widetilde{X}_{K'})_{L'}$. Therefore, if $x_L$ is nonregular, then $(\widetilde{X}_{K'})_{L'}$ is nonregular.

Proof. We first prove this in the case where $L/K$ is a finite purely inseparable extension of degree $p$ generated by an element $t$. In this case, the morphism $X_L \rightarrow X$ is a homeomorphism on the level of topological spaces. Therefore,

$$O_{X_L,x_L} = \lim_{U \ni x_L} O_{X_L}(U) = \lim_{V \ni x} O_{X_L}(V) = (\lim_{V \ni x} O_X(V) \otimes_K L) = (\lim_{V \ni x} O_X(V)) \otimes_K L = O_{X,x} \otimes_K L.$$ (3.1)

By assumption, $O_{X_L,x_L}$ is not a regular local ring, so there exists some element $g \in O_{X_L,x_L}$ (the normalization of $O_{X_L,x_L}$) that is not in $O_{X_L,x_L}$. Write

$$g = g_0 + g_1 t + \cdots + g_{p-1} t^{p-1},$$

where $g_i \in K(X)$. Let $x_{K'} \in \widetilde{X}_{K'}$ be the image of $x_{L'}$. For any $i$, if $g_i \in O_{\widetilde{X}_{K'},x_{K'}}$, then $g_i \in O_{X,x}$ because $O_{\widetilde{X}_{K'},x_{K'}}$ is integral over $O_{X,x}$ and $O_{X,x}$ is a regular local ring. Therefore, because $g \notin O_{X_L,x_L}$, there must be some $i$ for which $g_i \notin O_{\widetilde{X}_{K'},x_{K'}}$. But, because $L$ and $K'$ are linearly disjoint over $K$, we also have $[L':K'] = p$, $L' = K'(t)$, and $O_{(\widetilde{X}_{K'})_{L'},x_{L'}} = O_{\widetilde{X}_{K'},x_{K'}} \otimes_K L'$. This proves that $g \notin O_{(\widetilde{X}_{K'})_{L'},x_{L'}}$. But, $g$ is integral over $O_{(\widetilde{X}_{K'})_{L'},x_{L'}}$, so $O_{(\widetilde{X}_{K'})_{L'},x_{L'}}$ is not a regular local ring, i.e., $x_{L'}$ is not a regular point.

Now, consider the case of general $L$. Let $M_0/K$ be the maximal separable subextension of $L$. Consider a tower of fields

$$M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = L$$

such that $[M_i : M_{i-1}] = p$ for all $1 \leq i \leq n$. For each $i$, let $x_{M_i}$ be the image of $x_L$ in $X_{M_i}$. We know $x_{M_0}$ is a regular point because $M_0$ is separable over $K$. Thus, there exists some $1 \leq j \leq n$ such that $x_{M_{j-1}}$ is a regular point and $x_{M_j}$ is not a regular point. Let $y_{L'} \in (\widetilde{X}_{M_{j-1}K'})_{L'}$ be a preimage of $x_{L'}$ and $x_{M_jK'} \in (\widetilde{X}_{M_{j-1}K'})_{M_jK'}$ its image. By the previous paragraph, $x_{M_jK'}$ is a nonregular point, making $y_{L'}$ a nonregular point as well. The morphism $(\widetilde{X}_{M_{j-1}K'})_{L'} \rightarrow (\widetilde{X}_{K'})_{L'}$ is a birational morphism of curves. Therefore, $x_{L'}$ cannot be a regular point. \hfill $\Box$

Corollary 3.10. Let $K$ be a field of characteristic $p$, let $X$ be a geometrically integral regular curve over $K$, and let $x$ be a closed point of $X$. Let $L/K$ be an algebraic extension linearly disjoint with the residue field of $x$. Then every point in the preimage of $x$ in $X_L$ is a regular point.

Proof. Let $x_L \in X_L$ be in the preimage of $x$. Let $K'$ be the residue field of $x$, and let $L' := LK'$. Let $x_{L'} \in (\widetilde{X}_{K'})_{L'}$ be in the preimage of $x_L$ and $x_{K'} \in \widetilde{X}_{K'}$ the image of $x_{L'}$. Because $x_{K'}$ is a regular degree 1 point, it must be a smooth point (the proof is the same
as the proof that regular implies smooth over an algebraically closed field, e.g., [3], Theorem I.5.1). Therefore, \( x_{L'} \) is regular.

If \( L/K \) is a finite extension and \( x_L \) were nonregular, then \( x_{L'} \) would be nonregular by Lemma 3.9. Thus, \( x_L \) is regular.

\[ \square \]

Remark 3.11. Fix an algebraic closure \( \overline{K} \) with inclusions \( L, K' \subset \overline{K} \). The hypothesis that \( L \) and \( K' \) are linearly disjoint can be replaced by the hypothesis that \( L \cap K' \) is a separable extension of \( K \). This is because \( X_{L\cap K'} \) is regular and \( L \) and \( K' \) are linearly disjoint over \( L \cap K' \), so we can just apply Corollary 3.10 with \( K \) replaced by \( L \cap K' \).

**Proposition 3.12.** There exists an algorithm that takes in Input 2.1 and computes a finite subset \( S \) of \( \overline{K}_0 \), with \( k'_0 := k_0(S) \) and \( K'_0 := k'_0 \overline{K}_0 \), and a smooth, connected curve \( C \) over \( k'_0 \) such that

(i) the largest algebraic extension of \( k'_0 \) in \( K'_0 \) is \( k'_0 \),

(ii) \( K'_0 = k'_0(C) \), and

(iii) \( (\overline{X_{K'_0}})_{\overline{K}_0}\overline{K}_0 \) is regular but not smooth.

**Proof.** First, find nonnegative integers \( e_1, \ldots, e_m \) and \( 1 \leq j \leq m \) with \( F := k_0(t_1^{p^{-e_1}}, \ldots, t_m^{p^{-e_m}}) \) and \( L := k_0(t_1^{p^{-e_1}}, \ldots, t_j^{p^{-e_j}}, \ldots, t_m^{p^{-e_m}}) \) such that \( X_F \) is regular but \( X_L \) is not. This is possible because \( X \) is regular and \( X_{K_{p^{-e}}} \) is nonregular for some \( e \) by Proposition 3.3. After renaming \( t_1, \ldots, t_m \), we may assume \( j = 1 \).

Determine a primitive element \( u \) for \( K_0 \) over \( k_0(t_1, \ldots, t_m) \) and its minimal polynomial \( g \in k_0(t_1, \ldots, t_m)[x] \). Compute an irreducible factor \( g_1 \) of \( g \) in \( k_0(t_2, \ldots, t_m)(t_1)[x] \), and write

\[
g_1 = \frac{\sum w_i t_1^i x_j}{\sum w_i t_1^i}
\]

with \( v_{ij}, w_i \in k_0(t_2, \ldots, t_m) \). Let \( S \) be the set of all \( v_{ij} \) and \( w_i \) together with \( t_2^{p^{-e_2}}, \ldots, t_m^{p^{-e_m}} \). Let \( k'_0 \) and \( K'_0 \) be as in the statement of the proposition. This \( g' \) defines a geometrically integral curve \( U \) over \( k'_0 \) embedded as a locally closed subvariety of \( \mathbb{A}^2_{k'_0} \). Compute the normalization \( C \) of the projective closure of \( U \). Now, \( C \) may not be smooth. To fix this, repeatedly replace \( S \) by the set of all \( p \)th roots of elements of \( S \) and replace \( C \) by its normalization in the enlarged field \( k'_0 \) until \( C \) is smooth, which again works by Proposition 3.3. Now, \( (\overline{X_{K'_0}})_{\overline{K}_0}\overline{K}_0 \) may not be regular. To fix this, first compute the residue fields \( \ell_1, \ldots, \ell_s \) of the nonsmooth points of \( \overline{X_{K'_0}} \). Then, determine the maximum integer \( N \) such that for some \( 1 \leq i \leq s \) and \( 2 \leq j \leq m \), the field \( \ell_i \) contains \( t_j^{p^{-N}} \). Replace \( S \) by the set of \( p^N \)th roots of elements of \( S \). Now, for all \( i \), the field \( \ell_i \cap \overline{K}_0 \) inside any fixed algebraic closure \( \overline{K}_0 \) must be separable over \( k'_0 \). Therefore, by Remark 3.11, \( (\overline{X_{k'_0}})_{\overline{K}_0}\overline{K}_0 \) is regular.

Note that \( L \) and \( k'_0 F \) are linearly disjoint over \( F \) because \( k'_0 F \) does not contain a \( p \)th root of \( t_1^{p^{-e_1}} \). Therefore, by Lemma 3.9, the curve \( (\overline{X_{k'_0}})_{\overline{K}_0} \) is nonregular, so \( \overline{X_{k'_0}} F \) is not smooth. But, \( K'_0 \subset k'_0 F \), so \( \overline{X_{K'_0}} \) is not smooth. \( \square \)
Remark 3.13. Assume the notation in Input 2.1. Proposition 3.12 says that if we replace \( k_0 \) by \( k'_0 \) and \( K_0 \) by \( K'_0 \), we may reduce the problem of computing \( X(K) \) to the case where the transcendence degree of \( K \) over \( k \) is 1.

In light of Proposition 3.4 and Proposition 3.12, we define the following input to be used instead of Input 2.1.

**Input 3.14.**

(i) a prime number \( p \),

(ii) a field \( k_0 \) finitely generated over \( \mathbb{F}_p \), with \( k := \overline{k}_0 \),

(iii) a smooth, geometrically connected curve \( C \) over \( k_0 \), with \( K_0 := k_0(C) \) and \( K := kK_0 \),

(iv) a geometrically integral, nonsmooth, projective curve \( X \) over \( K_0 \) such that \( X_K \) is regular, and

(v) a geometrically integral, smooth, projective curve \( Y \) over \( K_0 \) with \( g(Y) = g(\overline{X_K}) \) together with a degree \( p \) inseparable morphism \( \pi : X \to Y \) over \( K_0 \).

The proof of Theorem 1.1 will handle the cases where \( Y_K \) is isotrivial and \( Y_K \) is non-isotrivial separately. Here, a curve \( Z \) over \( K \) is called isotrivial if there exists a curve \( Z_0 \) over \( k \) and a finite extension \( L/K \) such that \( Z_L \cong (Z_0)_L \).

**Proposition 3.15.** There exists an algorithm that takes in (i)-(iii) of Input 3.14 and a smooth connected projective curve \( Y \) over \( K_0 \) and determines whether \( Y_K \) is isotrivial. Furthermore, if \( Y_K \) is isotrivial, the algorithm computes a finite extension \( \ell_0/k_0 \), a finite separable extension \( L_0/K_0 \) such that the algebraic closure of \( k_0 \) in \( L_0 \) is \( \ell_0 \), a curve \( Y_0 \) over \( \ell_0 \), and an isomorphism \( \phi : Y_{L_0} \to (Y_0)_{L_0} \).

**Proof.** Compute the genus \( g := g(Y) \). If \( g = 0 \), then \( Y \) is isotrivial. In this case, choose any point \( P \in Y(L_0) \), where \( L_0/K_0 \) is a finite separable extension. Then, compute a basis \( \{1, \phi\} \) for \( H^0(Y_{L_0}, \mathcal{O}_{Y_{L_0}}(P)) \). The nonconstant function \( \phi \) can then be thought of as an isomorphism \( Y_{L_0} \to \mathbb{P}^1_{L_0} \). Compute the algebraic closure \( \ell_0 \) of \( k_0 \) in \( L_0 \) and set \( Y_0 := \mathbb{P}^1_{\ell_0} \).

If \( g = 1 \), then first choose any \( P \in Y(L'_0) \), where \( L'_0/K_0 \) is a finite separable extension and compute the algebraic closure \( \ell'_0 \) of \( k_0 \) in \( L'_0 \). Then, compute a basis \( \{1, x, y\} \) for \( H^0(Y_{L'_0}, \mathcal{O}_{Y_{L'_0}}(3P)) \) to put \( Y_{L'_0} \) into Weierstrass form

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

Then \( Y_K \) is isotrivial if and only if its \( j \)-invariant \( j(Y_{L'_0}) \) is in \( \ell'_0 \). Suppose this is the case. Construct an elliptic curve \( Y'_0 \) over \( \ell'_0 \) such that \( j(Y_0) = j(Y_{L'_0}) \) as in [10], Proposition III.1.4c. Compute a finite extension \( L_0/L'_0 \) and an isomorphism \( \phi : Y_{L_0} \to (Y_0)_{L_0} \) as in [10], Proposition III.1.4b or Proposition A.1.2b. Note that in this construction \( L_0 \) will be separable over \( L'_0 \). Compute the algebraic closure \( \ell_0 \) of \( \ell'_0 \) in \( L_0 \) and set \( Y_0 := (Y_0)_{\ell_0} \).

If \( g \geq 2 \), then suppose \( Y \subset \mathbb{P}^3_K \). Compute the Jacobian matrix \( J \) for the defining equations for \( Y \). Determine an open subset \( U \subset C \) on which the entries of \( J \) are regular.
functions and that J has rank \( n - 1 \). The equations for \( Y \) give rise to a smooth family \( \pi: Y \to U \) whose generic fiber is \( Y \). Choose any point \( P \in U(U_0) \) for some separable extension \( U'_0 \) of \( k_0 \). Let \( Y'_0 := \pi^{-1}(P) \). Now, let \( L'_0 := \ell'_0 K_0 \) and embed \( Y'_0 \) and \( (Y_0)_{L_0} \) in \( \mathbb{P}^N_{L_0} \) via the tricanonical embedding. Compute the equations an element \( \phi \in \text{PGL}_{N+1}(K) \) must satisfy to map \( Y_{\mathbb{P}} \) to \((Y_0)_{\mathbb{P}} \) to get an \( L'_0 \)-scheme \( Z \subset (\text{PGL}_{N+1})_{L'_0} \) isomorphic to \( \text{Isom}(Y'_0, (Y_0)_{L'_0}) \), which is 0-dimensional by de Franchis’s Theorem. Now, \( Y_k \) is isotrivial if and only if \( Z \) is nonempty. Suppose this is the case. \( Z \) is an \( \text{Aut}(Y'_0) \)-torsor over \( L'_0 \), and \( \text{Aut}(Y'_0) \) is étale over \( L'_0 \) because \( H^0(Y'_0, T_{Y'_0}) = 0 \) (see [11], Lemma 0DSW and Lemma 0E6G). This means there must be some \( \phi \in \mathbb{P}(L'_0) \), where \( L_0/L'_0 \) is a finite separable extension. Compute the algebraic closure \( \ell_0 \) of \( \ell'_0 \) in \( L_0 \) and set \( Y_0 := (Y'_0)_{L_0} \).

The following is a partial converse to the second part of Lemma 3.6 that will be needed in the absolute genus at least two case.

**Proposition 3.16.** Let \( k \) be a field of characteristic \( p \) and \( C \) be a smooth curve over \( k \) with \( K := k(C) \). Let \( \delta \) be a nonzero \( k \)-derivation of \( K \). Let \( Y \) be a geometrically integral curve over \( K \) with generic point \( \eta \). Suppose \( \delta \) extends to a \( k \)-derivation \( \tilde{\delta} \) of \( O_Y \) with kernel \( O' \) such that \( kK(Y)^p \subsetneq O'_\eta \). Then the ringed space \( Y' := (\text{sp}(Y), O') \) is a \( kK'^p \)-variety such that \( Y \cong Y'_{\tilde{K}} \) (here \( \text{sp}(Y) \) denotes to the topological space of \( Y \)).

If \( Y \) is a smooth curve of genus at least two, then there is at most one extension of \( \delta \) to a \( k \)-derivation \( \tilde{\delta} \) of \( O_Y \). Furthermore, in the case that \( \tilde{\delta} \) exists, it is automatically true that \( kK(Y)^p \subsetneq O'_\eta \).

**Proof.** Choose an element \( t \in K \setminus kK^p \). The statement remains unchanged if we replace \( \delta \) by \( \frac{1}{\delta t} \), so we may assume \( \delta t = 1 \). Define the homomorphism \( \phi: O' \otimes_{kkK^p} K \to O_Y \) of sheaves of \( K \)-algebras given by \( r \otimes u \mapsto ur \) for \( r \in O'(U) \) and \( u \in K \). We will show that \( \phi \) is an isomorphism. Let \( r \in (O' \otimes_{kkK^p} K)(U) \) be in the kernel of \( \phi \). We may write \( r = \sum_{i=0}^{p-1} r_i \otimes t^i \), where \( r_i \in O'(U) \). Then \( 0 = \phi(r)^\delta = \sum_{j=0}^{p-1} j r_i t^{i-1} \), which forces \( r = r_0 \otimes 1 \). This then implies \( r = 0 \), so \( \phi \) is injective. Now choose any \( s \in O_Y(U) \). We have

\[
K \cdot K(Y)^p = kK(Y)^p \otimes_{kkK^p} K \subsetneq O'_\eta \otimes_{kkK^p} K \subset K(Y).
\]

But \( [K(Y) : K \cdot K(Y)^p] = p \), so \( O'_\eta \otimes_{kkK^p} K = K(Y) \). Therefore we can write \( s = \sum_{i=0}^{p-1} s_i t^i \) for \( s_i \in O'_\eta \). Suppose \( s_j \notin O_Y(U) \) for some \( j \), and assume \( j \) is maximal. Then

\[
\sum_{i=0}^{j-1} s_i t^i = s - \sum_{i=j+1}^{p-1} s_i t^i \in O_Y(U),
\]

so

\[
s_j = \frac{1}{j!} \left( \sum_{i=0}^{j} s_i t^i \right)^{\delta_j} \in O_Y(U).
\]

This is a contradiction, so \( s_i \in O_Y(U) \) and therefore \( s_i \in O'(U) \) for all \( i \). This proves that \( \phi \) is surjective.

Let \( U \subset Y \) be an affine open subset and \( s \in O_Y(U) \) be nonzero. If \( r \in O'(D(s)) \), then there exists some \( r' \in O_Y(-U) \) and an integer \( i \geq 0 \) such that \( r = r'/s^p \). Then
0 = r^δ = (r')^δ/s^p, so (r')^δ = 0. This shows that \( \mathcal{O}'(D(s)) = \mathcal{O}'(U)_p \), so we have an isomorphism of ringed spaces \((U, \mathcal{O}'|_U) \cong \text{Spec} \mathcal{O}'(U)\). Therefore, the topological space of \( Y \) together with \( \mathcal{O}' \) defines a \( kK^p \)-variety \( Y' \) such that \( Y \cong Y'_K \).

Now suppose \( Y \) is smooth and has genus at least two. Suppose \( \tilde{\delta} \) and \( \tilde{\delta}' \) are two extensions of \( \delta \) to \( \mathcal{O}_Y \). Then \( \tilde{\delta} - \tilde{\delta}' \) is a \( K \)-derivation of \( \mathcal{O}_Y \). But \( \text{Der}_K(\mathcal{O}_Y, \mathcal{O}_Y) = H^0(Y, \mathcal{T}_Y) = 0 \), so \( \tilde{\delta} = \tilde{\delta}' \). The product rule for derivations generalizes to
\[
\tilde{\delta}^n(r s) = \sum_{i=0}^{n} \binom{n}{i} \tilde{\delta}^i(r) \tilde{\delta}^{n-i}(s).
\]
Taking \( n = p \) we see that \( \tilde{\delta}^p \) is also \( k \)-derivation. Furthermore \( \delta^p(t^i) = 0 \) for all \( i \), so \( \tilde{\delta}^p \) is actually a \( K \)-derivation. Thus, as before, \( \tilde{\delta}^p = 0 \). Let \( \tilde{\delta}_\eta \) denote the \( k \)-derivation on \( K(Y) \).

Let \( \{\alpha_1, \alpha_2, \ldots, \alpha_M\} \) be a subset of elements of \( K(S, p) \) that map bijectively to the image of \( K(S, p) \to (\mathbb{Z}/p)^S, \quad \alpha \mapsto (p \text{ord}_\xi \alpha \text{ (mod } p))_{\xi \in S} \), and let \( \{\alpha_1, \ldots, \alpha_M\} \) be lifts in \( K^\times \). If \( \text{Pic}_C[p] = \{D_1, \ldots, D_N\} \), then choose \( \beta_j \in K^\times \) such that \( \text{div} \beta_j = pD_j \). Then \( \tilde{\delta}_\eta \) has rank \( p^2 - 1 \) as a \( kK(Y)^p \)-linear map. This implies that \( \delta^p_\eta \) has rank at least \( p^2 - p \), a contradiction. \( \square \)

4 Curves of absolute genus zero

Lemma 4.1. Let \( k \) be a perfect field, and let \( K = k(C) \) for a smooth curve \( C \) over \( k \). Let \( S \) be a finite set of places of \( K \) and
\[
K(S, p) = \{v \in K^\times/K^{\times p} \mid p \text{ord}_\xi v \text{ for } \xi \notin S\}.
\]
Let \( \{\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_M\} \) be a subset of elements of \( K(S, p) \) that map bijectively to the image of \( K(S, p) \to (\mathbb{Z}/p)^S, \quad \overline{\alpha} \mapsto (p \text{ord}_\xi \alpha \text{ (mod } p))_{\xi \in S} \), and let \( \{\alpha_1, \ldots, \alpha_M\} \) be lifts in \( K^\times \). If \( \text{Pic}_C[p] = \{D_1, \ldots, D_N\} \), then choose \( \beta_j \in K^\times \) such that \( \text{div} \beta_j = pD_j \). Then, any element \( v \in K^\times \) with \( p \text{ord}_\xi v \) for all \( \xi \notin S \) is of the form \( v = \alpha_i \beta_j u^p \) for some \( u \in K \).

Proof. From the exact sequence
\[
0 \longrightarrow K^\times_{K^{\times p}} \longrightarrow \text{Div} C \longrightarrow \text{Pic} C \longrightarrow 0
\]
we have
\[
0 \longrightarrow \text{Pic} C[p] \longrightarrow K^\times_{K^{\times p}} \longrightarrow \frac{\text{Div} C}{p \text{Div} C} \longrightarrow \frac{\text{Pic} C}{p \text{Pic} C} \longrightarrow 0 \quad (4.1)
\]

Let \( \text{Div}_S C \) be the free abelian group generated by places not in \( S \), and let \( \text{Pic}_S C \) be the quotient of \( \text{Div}_S C \) by the image of \( K^\times \). From the diagram
\[
\begin{array}{ccc}
0 & \longrightarrow & 0 \\
\downarrow & & \downarrow \\
K^\times_{K^{\times p}} & \longrightarrow & K^\times_{K^{\times p}} \\
\downarrow & & \downarrow \\
\text{Div} C & \longrightarrow & \text{Div}_S C \\
\downarrow & & \downarrow \\
(\mathbb{Z}/p)^S & \longrightarrow & \frac{\text{Div} C}{p \text{Div} C} \\
\end{array}
\]

\[
0 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0
\]
and (1), the snake lemma gives

\[
0 \longrightarrow \text{Pic} C[p] \xrightarrow{} K(S, p) \xrightarrow{} (\mathbb{Z}/p)^S \xrightarrow{} \text{Pic} C \xrightarrow{p} \text{Pic} C \longrightarrow 0
\] (4.2)

This says that \( K(S, p) \) is the set of residue classes of all \( \alpha_i\beta_j \) in \( K^\times/K^\times_p \). From this, the lemma follows.

**Remark 4.2.** If \( k \) is algebraically closed, the degree map \( \text{deg} : \text{Pic} C/p\text{Pic} C \rightarrow \mathbb{Z}/p \) is an isomorphism of groups. Therefore, from (4.2) above, we see that the image of \( K(S, p) \rightarrow (\mathbb{Z}/p)^S \) is the set \( \{(a_s)_{s \in S} \mid \sum_{s \in S} a_s = 0\} \). Therefore, computing all elements of this set and finding preimages in \( K(S, p) \) allows us to compute \( \alpha_1, \ldots, \alpha_M \).

**Proof of Theorem 1.1, assuming \( \tilde{g} = 0 \).** Assume Input 3.14. First, as in Proposition 3.15, determine a finite separable extension \( L_0 \) of \( K_0 \) such that \( Y_{L_0} \cong \mathbb{P}^{1}_{L_0} \), and let \( x \in L_0(Y) \) be such that \( L_0(Y) \cong L_0(x) \). Set \( V = \mathbb{A}^1_{L_0} \subseteq Y \) and \( U = \pi^{-1}(V) \subseteq X \). As in Proposition 3.4, take \( z \in \mathcal{O}_X(U) \) with \( z \notin L_0(Y) \) and \( r = z^p \in \mathcal{O}_Y(V) = L_0[x] \). Next, determine a finite separable extension \( L_1 \) of \( L_0 \) such that

\[
r = \gamma(x - \alpha_1)^{e_1}(x - \alpha_2)^{e_2} \cdots (x - \alpha_{m_1})^{e_{m_1}}(x^{p^{f_1}} - \beta_1)^{f_1}(x^{p^{f_2}} - \beta_2)^{f_2} \cdots (x^{p^{f_{m_2}}} - \beta_{m_2})^{f_{m_2}},
\] (4.3)

where \( \gamma, \alpha_i, \beta_j \in L_1, \gamma \neq 0, \) and \( \ell_i \geq 1 \). For simplicity, we invoke Remark 3.5 and replace \( K_0 \) by \( L_1 \) for the remainder of the proof.

First, consider the case where \( p|e_i \) for all \( i \). Then, for some \( \ell \in K_0[x] \), we have \( r(x) = s(x^p) = s(F(x)) \). Using Proposition 3.8 with \( Z := \mathbb{P}^1_{K_0} \) and \( f := F \) together with 3.4 to compute \( X(K) \). Next consider the case where \( e_i \neq 0 \) (mod \( p \)) for some \( i \). Then, because

\[
eq e_1 + e_2 + \cdots + e_{m_1} + p^{f_1}f_1 + p^{f_2}f_2 + \cdots + p^{f_{m_2}}f_{m_2} + \text{ord}_\infty r = 0,
\]
either \( \text{ord}_\infty r \neq 0 \) (mod \( p \)) or \( e_j \neq 0 \) (mod \( p \)) for some \( j \neq i \). In either case, replace \( x \) by a linear fractional transformation to assume that \( \text{ord}_0 r \neq 0 \) (mod \( p \)) and \( \text{ord}_\infty r \neq 0 \) (mod \( p \)). Then, write \( r = r_1/r_2 \) for some polynomials \( r_1 \) and \( r_2 \). Replace \( r \) with \( r_2^p \) and \( z \) with \( r_2^p \) to assume \( r \) is again a polynomial in \( x \). Now, forget the notation in (4.3) and write

\[
r = \alpha_{m_1}x^{m_1} + \alpha_{m_1+1}x^{m_1+1} + \cdots + \alpha_{m_2}x^{m_2},
\] (4.4)

where \( \alpha_{m_1}, \alpha_{m_2} \neq 0 \) and \( m_1m_2 \neq 0 \) (mod \( p \)). Compute the finite set \( S \) of places \( \xi \) of \( K \) such that \( \text{ord}_\xi \alpha_i \neq 0 \) for some \( i \). If \( \xi \) is a place of \( K \) not in \( S \) and \( w \in K \), then the only possible slopes in the Newton polygon for \( r - w^p \) are 0, \( -p(\text{ord}_\xi w)/m_1 \), or \( -p(\text{ord}_\xi w)/m_2 \). This shows that for \( \xi \notin S \), if \( v \in K \) and \( r(v) \in K^p \), then \( p|\text{ord}_\xi v \). We know \( r(0) = 0 \in K^p_0 \), so by Proposition 3.4, it suffices to show \( \{v \in K^\times \mid r(v) \in K^p\} \) is finite and computable.

Apply Lemma 4.1 and Remark 4.2 to compute elements \( \alpha_i, \beta_j \in K^\times \) such that \( v = \alpha_i\beta_jw^p \) if \( p|\text{ord}_\xi v \) for all \( \xi \notin S \). Choose specific \( i \) and \( j \), and define \( g_{ij} : \mathbb{P}^1 \rightarrow \mathbb{P}^1 \) by \( u \mapsto \alpha_i\beta_ju \). Using Proposition 3.8 with \( Z := \mathbb{P}^1_{K_0} \) and \( f := g_{ij} \circ F \), compute

\[
\{v = \alpha_i\beta_jw^p \in K^\times \mid r(v) \in K^p\}.
\]

Doing this for each of the finitely many \( i \) and \( j \) finishes the proof.

5 Curves of absolute genus one

Proposition 5.1. Let $k$ be an algebraically closed field with finite transcendence degree over its prime field and $C$ and $D$ be smooth, geometrically connected curves over $k$. Let $J_C$ and $J_D$ denote the Jacobians of $C$ and $D$ respectively. Then there exists an algorithm to compute a (finite) set of generators for $\text{Hom}(J_C, J_D)$.

Proof. The Tate conjecture is known for products of curves, so by ([7], Theorem 8.33 and Remark 8.35), one can compute a set of curves $E_1, E_2, \ldots, E_n$ on $C \times D$ whose classes generate $\text{NS}(C \times D)$. Choose closed points $P_0 \in C(k)$ and $Q_0 \in D(k)$ and embeddings $\iota_C: C \to J_C$ and $\iota_D: D \to J_D$ sending $P_0$ and $Q_0$ to the respective identity elements. Let $\pi_C$ and $\pi_D$ denote the projections from $C \times D$ to $C$ and to $D$ respectively.

We define a homomorphism $\phi: \text{NS}(C \times D) \to \text{Hom}(J_C, J_D)$ as follows. Let $K := k(C)$, and let $\varepsilon \in C(K)$ be the generic point. Let $E$ be an integral curve on $C \times D$. If $E$ is a fiber of $\pi_C$, then $\phi(E)$ is the constant map to the identity of $J_D$. Otherwise, compute the finite $K$-subscheme $\theta := \pi_D(\pi_C^{-1}(\varepsilon))$ of $D$. List the $K$-points $\{Q_1, \ldots, Q_m\}$ of $D_K$ and their multiplicities $d_1, \ldots, d_m$ such that $\theta$ is the Weil divisor $d_1Q_1 + \cdots + d_mQ_m$, and then compute

$$Q_E := d_1\iota_D(Q_1) + \cdots + d_m\iota_D(Q_m) \in J_D(K).$$

Lastly, spread out this $K$-point $Q_E$: Spec $K \to J_D$ to a $k$-morphism $\psi_E: C \to J_D$. Then, set $\phi(E)$ to be the unique morphism $J_C \to J_D$ such that $\phi(E)(\iota_C(P)) = \psi_E(P) - \psi_E(P_0)$ for $P \in C(k)$.

This homomorphism $\phi$ agrees with the projection map $\text{NS}(C \times D) \to \text{Hom}(J_C, J_D)$ in the following factorization described in [14], Section 8.4:

$$\text{NS}(C \times D) \cong \text{NS}(C) \times \text{NS}(D) \times \text{Hom}(J_C, J_D) \cong \mathbb{Z}^2 \times \text{Hom}(J_C, J_D).$$

Hence, $\phi$ is surjective, so $\phi(E_1), \ldots, \phi(E_n)$ generate $\text{Hom}(J_C, J_D)$. \hfill \square

Lemma 5.2. Let $k$ be an algebraically closed field of characteristic $p$ and $K := k(C)$ for some smooth integral curve $C$ over $k$. Let $Y$ be an ordinary elliptic curve over $K$ that has either good reduction or multiplicative reduction at every $v \in C$. Let $V: Y^{(p)} \to Y$ be the Verschiebung isogeny, and assume that $\ker V \subset Y^{(p)}(K)$. Then an isomorphism of $K$-group schemes $\mathbb{Z}/p\mathbb{Z} \to \ker V$ induces a group isomorphism $H^1_b(C, \mathbb{Z}/p\mathbb{Z}) \to \text{Sel}(K, V)$.

Proof. Let $v \in C$ be a place at which $Y$ has good reduction. Thus, there exists a smooth proper model $\mathcal{Y}$ over $\mathcal{O}_v$, the ring of integers of $K_v$, whose generic fiber is isomorphic to $Y$ over $K_v$. By the valuative criterion for properness, $Y(K_v)/V(Y^{(p)}(K_v)) \cong \mathcal{Y}(\mathcal{O}_v)/V(\mathcal{Y}^{(p)}(\mathcal{O}_v))$, and we have

$$\mathcal{Y}(\mathcal{O}_v)/V(\mathcal{Y}^{(p)}(\mathcal{O}_v)) < H^1(\mathcal{O}_v, \mathbb{Z}/p\mathbb{Z}) \cong \mathcal{O}_v/\mathcal{Y}(\mathcal{O}_v),$$

where $\phi$ is the Artin-Schreier function $\alpha \mapsto \alpha^p - \alpha$. By Hensel’s lemma and the fact that $k$ is algebraically closed, $\phi: \mathcal{O}_v \to \mathcal{O}_v$ is surjective. Thus, $Y(K_v)/V(Y^{(p)}(K_v)) = 0$.

Now, let $v$ be a place at which $Y$ has multiplicative reduction. In this case, we have parameterizations $Y(K_v) \cong K_v^\times/q^\mathbb{Z}$ and $Y^{(p)}(K_v) \cong K_v^\times/q^{p\mathbb{Z}}$, where $q \in K_v^\times$ (REF). Furthermore, $V$ induces the natural projection map $K_v^\times/q^{p\mathbb{Z}} \to K_v^\times/q^\mathbb{Z}$, which is surjective. Thus,
Y(K_v)/V(Y^{(p)}(K_v)) = 0 in this case as well. This shows that

\[ \text{Sel}(K, V) \cong \ker \left( H^1(K, \mathbb{Z}/p\mathbb{Z}) \to \prod_{v \in C} H^1(K_v, \mathbb{Z}/p\mathbb{Z}) \right) \cong \ker \left( K/\mathfrak{p}(K) \to \prod_{v \in C} K_v/\mathfrak{p}(K_v) \right). \]

The group on the right hand side of the above expression parameterizes degree \( p \) separable, unramified covers \( C' \to C \), so \( \text{Sel}(K, V) \) is the image of the map \( H^1_{\text{ét}}(C, \mathbb{Z}/p\mathbb{Z}) \to H^1(K, \mathbb{Z}/p\mathbb{Z}) \cong H^1(K, V) \).

Let \( S \) be a scheme and \( A \) be a commutative fppf group scheme over \( S \). If \( A \) is affine over \( S \), then \( H^1_{\text{fppf}}(S, A) \) can be identified with isomorphism classes of \( A \)-torsors over \( S \) (see, for example, REF). Suppose \( f: A \to B \) is a morphism of affine fppf group schemes over \( S \), and let \( f_* \) denote the induced homomorphism \( H^1_{\text{fppf}}(S, A) \to H^1_{\text{fppf}}(S, B) \). Let \( T \) be a \( A \)-torsor over \( S \) also thought of as an element of \( H^1_{\text{fppf}}(S, A) \). Then the \( B \)-torsor corresponding to \( f_*(T) \) is the contracted product \( T \times_A B \), i.e., the quotient of \( T \times_S B \) by the \( A \) action \( a \cdot (t, b) \mapsto (a^{-1} \cdot t, ab) \). There exists a natural \( S \)-morphism \( T \to f_*(T) \) defined by \( t \mapsto (t, 1) \).

**Lemma 5.3.** Let \( S \) be a scheme and

\[
0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0
\]

be a short exact sequence of affine commutative group schemes over \( S \). We then have the exact sequence

\[
H^1_{\text{fppf}}(S, A) \xrightarrow{f_*} H^1_{\text{fppf}}(S, B) \xrightarrow{g_*} H^1_{\text{fppf}}(S, C)
\]

Let \( T \) be a \( B \)-torsor over \( S \) such that \( g_*(T) \) is the trivial \( C \)-torsor. Let \( \sigma: S \to g_*(T) \) be any section, and consider the Cartesian square

\[
\begin{array}{ccc}
T_\sigma & \longrightarrow & S \\
\downarrow \sigma' & & \downarrow \sigma \\
T & \longrightarrow & g_*(T)
\end{array}
\]

Then \( T_\sigma \) is an \( A \)-torsor over \( S \) such that \( f_*(T_\sigma) = T \).

**Proof.** One can check that the \( S \)-morphism \( \mu: A \times_S T_\sigma \to T \) defined by \( (a, t) \mapsto a \cdot \sigma'(t) \) lifts to a morphism \( A \times_S T_\sigma \to T_\sigma \) and that this defines an \( A \)-action on \( T_\sigma \). There is a well defined \( S \)-morphism

\[ \phi: T_\sigma \times B \to T, \quad (t, b) \mapsto b \cdot \sigma'(t), \]

which has the property that

\[ \phi(t, b'b) = b'b \cdot \sigma'(t) = b' \cdot \phi(t, b). \]
So, if we can verify that $T_\sigma$ is an $A$-torsor, then $\phi$ must be an isomorphism of $B$-torsors. For this, replace $S$ by some fppf cover $S'$ of $S$ to assume $T_\sigma$ has an $S$-point. This means $T$ has an $S$-point as well, which forces $T$ to be the trivial torsor, so we can assume $T$ is $B$, $g_*(T)$ is $C$, and $\sigma$ is the identity section. This then means $T_\sigma$ is the kernel of $g$, which is $A$.

For the following lemma, we introduce some background on the Hasse-Witt matrix and the Cartier operator; see [9], Sections 8-10, for more details. Let $k$ be an algebraically closed field of characteristic $p$, and let $C$ be a smooth connected projective curve over $k$ with function field $K := k(C)$. Let $\mathcal{R}$ denote the ring of repartitions on $C$, i.e., the elements $r = (r_P) \in \prod_{P \in C(k)} K$ such that $r_P$ is regular at $P$ for all but finitely many $P \in C(k)$. Let $\mathcal{R}(0)$ denote the subring of repartitions such that $r_P$ is regular at all $P \in C(k)$. There is an isomorphism
\[
\phi: \frac{\mathcal{R}}{\mathcal{R}(0) + K} \to H^1(C, \mathcal{O}_C)
\]
that goes as follows. Let $r \bmod \mathcal{R}(0) + K$ be an element of the group on the left hand side. We can assume that $r_P \neq 0$ only for $P$ in some finite set of points $\{P_1, \ldots, P_n\}$. For $1 \leq i \leq n$, let $U_i$ be the open subset of $C$ containing $P_i$ and all points other than $P_1, \ldots, P_n$ at which $r_{P_i}$ is regular, and let $U_{n+1} := C \setminus \{P_1, \ldots, P_n\}$. Then $\phi(r)$ is the Čech 1-cocycle for the open cover $U_1, \ldots, U_{n+1}$ of $C$ whose value on $U_i \cap U_j$ for $1 \leq i < j \leq n + 1$ is
\[
f_{ij} := \begin{cases} r_{P_i} - r_{P_j} & \text{if } 1 \leq i, j \leq n, \\ r_{P_i} & \text{if } j = n + 1. \end{cases}
\]
Let $F$ denote the Frobenius operator on $\mathcal{R}$ sending $r$ to $(r^p_P)$. If $F_*$ is the operator on $H^1(C, \mathcal{O}_C)$ induced by the $p$th power Frobenius map on $\mathcal{O}_C$, then $\phi$ satisfies $\phi(F(r)) = F_*(\phi(r))$.

Let $t$ be an element of $K \setminus K^p$. Then any $s \in K$ can be written as
\[
s = s_0^p + s_1^p t + \cdots + s_{p-1}^p t^{p-1}.
\]
The Cartier operator $\mathcal{C}$ is defined on differential forms on $C$ by $\mathcal{C}(s \, dt) := s_{p-1} \, dt$. Serre duality is explicitly described by the pairing
\[
\langle \cdot, \cdot \rangle: \frac{\mathcal{R}}{\mathcal{R}(0) + K} \times H^0(C, \Omega_C) \to k, \quad \langle r, \omega \rangle = \sum_{P \in C(k)} \text{res}_P(r_P \omega).
\]
The Frobenius operator on $\mathcal{R}/(\mathcal{R}(0) + K)$ and the Cartier operator on $H^0(C, \Omega_C)$ are related by the following formula:
\[
\langle F(r), \omega \rangle = \langle r, \mathcal{C}(\omega) \rangle^p.
\]
If $r_1, \ldots, r_g$ is a basis for $\mathcal{R}/(\mathcal{R}(0) + K)$, then the Hasse-Witt matrix with respect to this basis is a $g$-by-$g$ matrix $(a_{ij})$ such that $F(r_i) = \sum_j a_{ij} r_j$. Suppose $P_1, \ldots, P_g$ are $g$ distinct points on $C$ such that the divisor $D := P_1 + \cdots + P_g$ is non-special, i.e., $\dim H^0(C, \Omega_C(D)) = 1$. 

Campbell Hewett
If \( u_1, \ldots, u_g \) are respective uniformizers for \( P_1, \ldots, P_g \), then the repartitions \( r_1, \ldots, r_g \) defined by

\[
(r_i)_P := \begin{cases} 
0 & \text{if } P \neq P_i \\
1/u_i & \text{if } P = P_i 
\end{cases}
\]

form a basis for \( R/(R(0) + K) \).

**Lemma 5.4.** There exists an algorithm that takes in (i)-(iii) of Input 3.14 and computes coset representatives for the image of \( H^1_{\text{ét}}(C, \mathbb{Z}/p\mathbb{Z}) \) in \( K/\wp(K) \).

**Proof.** Consider the Artin-Schreier short exact sequence on the étale site of \( C \):

\[
\begin{array}{cccccccccc}
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{G}_a & \xrightarrow{\wp} & \mathbb{G}_a & \longrightarrow & 0 \\
\end{array}
\]

The map \( \wp : k \rightarrow k \) is surjective, so we have the exact sequence

\[
\begin{array}{cccccccccc}
0 & \longrightarrow & H^1_{\text{ét}}(C, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & H^1_{\text{ét}}(C, \mathbb{G}_a) & \xrightarrow{\wp_*} & H^1_{\text{ét}}(C, \mathbb{G}_a) & \longrightarrow & 0
\end{array}
\]

Furthermore, we have the canonical isomorphism \( H^1(C, \mathcal{O}_C) \cong H^1_{\text{ét}}(C, \mathbb{G}_a) \). The first step is to find a basis \( r_1, \ldots, r_g \) for \( H^1(C, \mathcal{O}_C) \) and compute the Hasse-Witt matrix with respect to this basis. One way to do this is as follows.

Compute a basis \( \omega_1, \ldots, \omega_g \) for \( H^0(C, \Omega_C) \) and a matrix \((c_{ij})\) for the Cartier operator with respect to this basis as outlined in [12]. Now choose points \( P_1, \ldots, P_g \) inductively as follows. For each \( 1 \leq j \leq g \), set \( \omega_{0,j} := \omega_j \). For each \( i \geq 1 \), choose a point \( P_i \) on which \( \omega_{i-1,1} \) does not vanish and compute a basis \( \omega_{i,1}, \ldots, \omega_{i,g-i} \) for \( H^0(C, \Omega_C(P_1 + \cdots + P_i)) \). By construction, \( P_1 + \cdots + P_g \) is a nonspecial divisor. Compute respective uniformizers \( u_1, \ldots, u_g \) for these points to get a basis \( r_1, \ldots, r_g \) for \( R/(R(0) + K) \) as described above. Using (5.1) and the matrix \((c_{ij})\), compute the Hasse-Witt matrix \( H := (a_{ij}) \) with respect to \( r_1, \ldots, r_g \).

The choice of basis \( r_1, \ldots, r_g \) lets us represent elements of \( R/(R(0) + K) \) by column vectors. For such a vector \((\beta_i)\), the Artin-Schreier operator is given by

\[
(\beta_i) \mapsto H(\beta_i^p) - (\beta_i).
\]

Computing its kernel is just a matter of finding the finitely many solutions of \( g \) polynomials in the variables \( \beta_1, \ldots, \beta_g \). Thus, compute the kernel \( \{s_1, s_2, \ldots, s_N\} \subset R/(R(0) + K) \) and lift each \( s_\ell \) to some \( s_\ell \in R \). To get from \( s_\ell \) to an element of \( K \), first determine the Čech 1-cocycle \( \phi(s_\ell) \) as described above, with cover \( U_1, \ldots, U_{n+1} \) and values \( f_{ij} \) on \( U_i \cap U_j \). Let \( T_\ell \) be the \( \mathbb{G}_a \)-torsor corresponding to \( s_\ell \). Above \( U_1, T_\ell \) and \( \wp_* (T_\ell) \) are both isomorphic to \( U_1 \times_k \mathbb{A}^1_k \), and the morphism \( T_\ell \rightarrow \wp_* (T_\ell) \) is given by \((P, x) \mapsto (P, x^p - x)\). Determine elements \( g_\ell \in \mathcal{O}_C(U_1) \) and \( h_\ell \in \mathcal{O}_C(U_2) \) such that \( f_{12}^\ell - f_{12} = h_\ell - g_\ell \). There is a section \( \sigma : C \rightarrow \wp_* (T_\ell) \) given on \( U_1 \) by \( P \mapsto (P, g_\ell(P)) \). Thus, by Lemma 5.3, a \( \mathbb{Z}/p\mathbb{Z} \)-torsor \( T_\gamma \) corresponding to \( s_\ell \) restricted to \( U_1 \) has equation \( x^p - x = g_\ell \). Thus, the desired elements of \( K \) are \( g_1, \ldots, g_N \). \( \square \)
Lemma 5.5. Assume the same hypotheses as in Lemma 5.2. Let $S$ be a finite set of $v \in C$ containing all places with bad reduction, and let $O_{K,S}$ be the ring of $S$-integers in $K$. Then a $K$-group scheme isomorphism $\mu_p \to \ker F$ induces an inclusion

$$Y^{(p)}(K)/F(Y(K)) \subset H^1_{fppf}(O_{K,S}, \mu_p) \subset H^1_{fppf}(K, \mu_p),$$

and $H^1_{fppf}(O_{K,S}, \mu_p)$ maps isomorphically to $K(S,p)$ (see Lemma 4.1 and Remark 4.2) via the isomorphism $H^1_{fppf}(K, \mu_p) \cong K^\times/K^{\times p}$.

Proof. Let $\mathcal{Y}$ be a proper, smooth scheme over $O_{K,S}$ whose generic fiber is isomorphic to $Y$ over $K$. By properness,

$$Y^{(p)}(K)/F(Y(K)) \cong \mathcal{Y}^{(p)}(O_{K,S})/F(\mathcal{Y}(O_{K,S})) \subset H^1_{fppf}(O_{K,S}, \ker F) \cong H^1_{fppf}(O_{K,S}, \mu_p).$$

If $v \in C$ is a closed point, then we have an exact sequence

$$0 \to O_{C,v}^\times/O_{C,v}^{\times p} \to H^1_{fppf}(O_{C,v}, \mu_p) \to H^1_{fppf}(O_{C,v}, \mathbb{G}_m).$$

But, $H^1_{fppf}(O_{C,v}, \mathbb{G}_m) \cong \text{Pic } O_{C,v} \cong 0$. This shows that every $\mu_p$-torsor over $O_{C,v}$ is of the form

$$\text{Spec } O_{C,v}[x]/(x^p - \alpha)$$

for some $\alpha \in O_{C,v}^\times$ defined uniquely modulo $O_{C,v}^{\times p}$.

Now, take any element $\xi \in H^1_{fppf}(O_{K,S}, \mu_p)$ and consider its corresponding $\mu_p$-torsor $T$ over $O_{K,S}$. By the above paragraph, there exists an open cover $\mathcal{U}$ of $C \setminus S$ and elements $\alpha_U \in O_{C(U)}^\times$ for $U \in \mathcal{U}$ such that

$$T_U \cong \text{Spec } O_{C(U)}[x]/(x^p - \alpha_U).$$

If $U, V \in \mathcal{U}$ and $v \in U \cap V$, then $\alpha_U/\alpha_V \in O_{C,v}^{\times p}$, so in particular, $\alpha_U/\alpha_V \in K^{\times p}$. Therefore, there is a well defined homomorphism $\phi: H^1_{fppf}(O_{K,S}, \mu_p) \to K(S,p)$ defined by $\xi \mapsto \overline{\alpha}^\mu_U$, where $U$ is any element of $\mathcal{U}$. Note that we also have a commutative diagram

$$\begin{array}{ccc}
H^1_{fppf}(O_{K,S}, \mu_p) & \longrightarrow & H^1_{fppf}(K, \mu_p) \\
\phi \downarrow & & \cong \\
K(S,p) & \longrightarrow & K^\times/K^{\times p}
\end{array}$$

On the other hand, take any $\overline{\alpha} \in K(S,p)$ with coset representative $\alpha \in K^\times$. For any $v \in C \setminus S$, we have $v(\alpha) = 0 \pmod{p}$, so $\alpha^\beta \in O_{C,v}^\times$ for some $\beta \in K^\times$. This means there exists an open cover $\mathcal{U}$ of $C \setminus S$ and elements $\alpha_U \in O_{C(U)}^\times$ such that $\alpha_U = \alpha \pmod{K^{\times p}}$ for all $U \in \mathcal{U}$. Define

$$T_U := \text{Spec } O_{C(U)}[x]/(x^p - \alpha_U)$$

for each $U \in \mathcal{U}$. For $U, V \in \mathcal{U}$, we have $\alpha_U/\alpha_V \in K^{\times p} \cap O_{C(U \cap V)}^\times = O_{C(U \cap V)}^{\times p}$, so there are $O_{C(U \cap V)}$-isomorphisms

$$\text{Spec } O_{C(U \cap V)}[x]/(x^p - \alpha_V) \to \text{Spec } O_{C(U \cap V)}[x]/(x^p - \alpha_U)$$
Proof of Theorem 1.1, assuming \( \tilde{g} = 1 \). Assume Input 3.14. We will invoke Remark 3.5 multiple times and replace \( K_0 \) by finite separable extensions. First, replace \( K_0 \) by such an extension to assume that \( Y \) has a \( K_0 \)-point, making \( Y_{K_0} \) into an elliptic curve as in the proof of Proposition 3.15. Next, use Proposition 3.15 to determine if \( Y \) is isotrivial. First, consider the case where \( Y \) is isotrivial. Replace \( k_0 \) by \( \ell_0, \ K_0 \) by \( L_0 \), and \( Y \) by \( \overline{Y}_{k_0} \) via the isomorphism \( \phi \) as in the statement of the proposition. Thus, we have

\[
Y_0(K)/Y_0(k) = \{ \text{k-morphisms Spec } K \rightarrow Y_0 \}/Y_0(k)
\]

\[
= \{ \text{k-morphisms } C \rightarrow Y_0 \}/\{ \text{constant k-morphisms } C \rightarrow Y_0 \}
\]

\[
= \text{Hom}(J_C, Y_0).
\]

Using Proposition 5.1, compute a set of generators for \( Y_0(K)/Y_0(k) \), and then compute the finite group

\[
\frac{Y_0(K)/Y_0(k)}{p(Y_0(K)/Y_0(k))} = \frac{Y_0(K)}{pY_0(K)}
\]

(note that in the proof of Proposition 5.1, we first construct the k-morphisms \( C \rightarrow Y_0 \) themselves, which are all we need in this case). We now have points \( Q_1, \ldots, Q_n \in Y_0(K) \) such that all elements of \( Y_0(K) \) are of the form \( Q_i + pP \) for \( P \in Y_0(K) \) for some \( i \). Apply Proposition 3.8 with \( Z = Y \) and \( f(P) = Q_i + pP \) for every \( i \) to compute \( X(K) \).

Now, consider the case where \( Y \) is nonisotrivial (in fact, the proof in this case only assumes \( Y \) is ordinary). Replace \( K_0 \) by a finite separable extension such that \( \ker V \subset Y^{(p)}(K_0) \), \( \ker F \subset Y(K_0) \), and \( Y \) has either good reduction or multiplicative reduction at every \( v \in C \). Compute a \( K_0 \)-group scheme isomorphism \( \mathbb{Z}/p\mathbb{Z} \rightarrow \ker V \) as well as the image of \( H^1_{\text{fppf}}(C, \mathbb{Z}/p\mathbb{Z}) \) in \( K/\varphi(K) \) as in Lemma 5.4. By Lemma 5.2, this is the same as \( \text{Sel}(K, V) \) as a subgroup of \( H^1(K, \ker V) \). For every \( \eta \in \text{Sel}(K, V) \), compute a corresponding \( \ker V \)-torsor \( V_\eta : Y_\eta \rightarrow Y \). Now, every \( P \in Y(K) \) is of the form \( V_\eta(Q) \) for some \( \eta \in \text{Sel}(K_0, V) \) and \( Q \in Y_\eta(K) \).

Let \( X_\eta := X \times_Y Y_\eta \) with morphism \( g_\eta : X_\eta \rightarrow X \). Note that \( V_\eta \) is separable and \( \pi \) is purely inseparable, so \( \overline{Y}(Y_\eta) \) and \( \overline{X}(X) \) are linearly disjoint over \( \overline{K}(Y) \). This implies \( X_\eta \) is geometrically integral. Furthermore, \( X \) is regular and \( g_\eta \) is étale because \( V_\eta \) is étale, so \( X_\eta \) is regular. On the other hand, \( X_\eta \) maps to \( X \), so \( X_\eta \) cannot be smooth ([11], Lemma 0CCW). Now, because

\[
\bigcup_{\eta \in \text{Sel}(K, V)} g_\eta(X_\eta(K)) = \bigcup_{\eta \in \text{Sel}(K, V)} g_\eta\left( \{(P, Q) \in X \times Y_\eta(K) \mid \pi(P) = V_\eta(Q)\} \right)
\]

\[
= \bigcup_{\eta \in \text{Sel}(K, V)} \{ P \in X(K) \mid \pi(P) = V_\eta(Q) \text{ for some } Q \in Y_\eta(K) \}
\]

\[
= X(K),
\]
it suffices to compute $X_\eta(K)$ for each $\eta \in \text{Sel}(K,V)$. Note that $Y_\eta$ is a twist of $Y^{(p)}$, which can be defined over $K_0^p$. It follows that $Y_\eta$ can be defined over $K_0^p$, so $Y_\eta^{(1/p)}$ is defined over $K_0$. For simplicity, we may replace $X$ and $Y$ by $X_\eta$ and $Y_\eta$.

Now, using Lemma 5.5 and Remark 4.2, compute a finite subgroup $H := H^1_{fppf}(\mathcal{O}_{K,S}, \mu_p) \subset H^1_{fppf}(K, \mu_p) \cong K^*/K^{*p}$ isomorphic to $K(S,p)$ for some finite set of places $S$ of $K$ such that $H$ contains the image of $Y(K)$. Therefore, every $h \in H$ gives a ker-$F$-torsor $F_h : Y_h \to Y$ such that every $P \in Y(K)$ is of the form $F_h(Q)$ for some $h \in H$ and $Q \in Y_h(K)$. The morphism $F_h$ is inseparable, so apply Proposition 3.8 with $Z = Y_h$ and $f = F_h$ for every $h$ to compute $X(K)$.

\[ \square \]

\section{Curves of absolute genus at least two}

In the case where $Y_K$ is isotrivial, we make use of the de Franchis-Severi Theorem. The proof of a computable version of the de Franchis-Severi Theorem over a number field or $\mathbb{Q}$ was given in [2], Theorem 5.5. We show that it can be slightly modified to work over any field $k_0$ finitely generated over its prime field.

\textbf{Theorem 6.1.} There exists an algorithm that takes as input a field $k_0$ finitely generated over its prime field, with $k := \overline{k_0}$, and a smooth projective integral curve and computes the set of pairs $(Y, \pi)$ where $Y$ is a smooth curve over $k$ with $g(Y) \geq 2$ and $\pi : X \to Y$ is a separable morphism, up to isomorphism (pairs $(Y, \pi)$ and $(Y', \pi')$ are considered isomorphic if and only if there is a $k$-isomorphism $\theta : Y \to Y'$ with $\theta \circ \pi = \pi'$).

\textbf{Proof.} Because $2 \leq g(Y) \leq g(X)$, it suffices to show that, for fixed $g \geq 2$, the set $\mathcal{C}_g$ of isomorphism classes of $(Y, \pi)$ with $g(Y) = g$ is computable. Embed $X$ in $\mathbb{P}^n_k$ via the tricanonical embedding. Let $(Y, \pi) \in \mathcal{C}_g$, and embed $Y$ in $\mathbb{P}^n_k$ via the tricanonical embedding. Then, if $R$ is the ramification divisor of $\pi$, then $3K_X - \pi^*(3K_Y)$ is linearly equivalent to $3R$, which is an effective divisor. Thus, $H^0(X, \pi^*(3K_Y)) = H^0(X, 3K_X - 3R) \subset H^0(X, 3K_X)$, so $\pi$ is the restriction to $X$ of a projection $\pi_L : \mathbb{P}^n_k \dashrightarrow \mathbb{P}_k^{n}$ with respect to a linear subspace $L \subset \mathbb{P}_k^n$ of dimension $n-m-1$. Let $G$ be the Grassmannian variety of $(n-m-1)$-dimensional subspaces of $\mathbb{P}^n_k$. If $\theta$ is an isomorphism from $(Y, \pi)$ to $(Y', \pi')$, then $\pi^*(3K_Y) = 3\pi^*(\theta^*K_{Y'}) = \pi'^*(3K_{Y'})$. Thus, $(Y, \pi) \mapsto L$ is a well defined function $\iota : \mathcal{C}_g \to G(k)$. If $\iota(Y, \pi) = \iota(Y', \pi')$, then $Y$ and $Y'$ map isomorphically to the same curve in $\mathbb{P}^m_k$ such that $\pi$ and $\pi'$ are induced by the same projection. Hence, $\iota$ is injective.

Conversely, if $s \in G_k$ with residue field $k(s)$, then let $L$ be the corresponding subspace of $\mathbb{P}^n_{k(s)}$, let $Y_s$ be the Zariski closure of $\pi_L(X_{k(s)} - L)$ in $\mathbb{P}^m_{k(s)}$, and let $\pi_s : X_{k(s)} \to Y_s$ denote the morphism induced by $\pi_L$. The $s \in G(k)$ that are in the image of $\iota$ are precisely the points that satisfy the following three conditions:

(i) $Y_s$ is a smooth curve over $k$,
(ii) $\pi_s$ is a separable morphism, and
(iii) the subspace $L \subset \mathbb{P}^m_k$ is equal to the linear subspace $L' \subset \mathbb{P}^n_k$ defined as the common zeros of the sections in the image of $H^0(Y_s, 3K_{Y_s}) \to H^0(X, 3K_X)$.
[2] first prove the following claim:

**Claim 1.** \( G \) can be computably partitioned into a finite number of irreducible locally closed subsets \( H_i \) such that for each \( i \), either

1. for all \( s \in H_i \), the curve \( Y_s \) is not smooth over the residue field of \( s \), or
2. there is a smooth family \( \mathcal{Y} \to H_i \) of curves, and an \( H_i \)-morphism \( X \times_k H_i \to \mathcal{Y} \) whose fiber above \( s \in H_i \) is \( \pi_s : X \to Y_s \).

Assuming this, we prove the following claim:

**Claim 2.** Let \( H \) be a locally closed subset of \( G \) satisfying (2) in Claim 1. Then, \( H \) can be computably partitioned into a finite number of irreducible locally closed subsets \( H'_i \) such that for all \( i \), either (1) \( \pi_s \) is inseparable for all \( s \in H'_i \) or (2) \( \pi_s \) is separable for all \( s \in H'_i \).

To prove this claim, we use induction on the dimension of \( H \). First, compute the irreducible components of \( H \) to reduce to the case where \( H \) is irreducible. The claim is clearly true if \( \dim H = 0 \). Suppose \( \dim H \geq 1 \), and let \( \eta \in H \) be the generic point of \( H \). By assumption, \( Y_\eta \) is smooth over \( \kappa := k(\eta) \), so in particular, it is geometrically reduced. Thus, there exists some \( f \in \kappa(Y_\eta) \) such that \( \kappa(Y_\eta) \) is a separable finite extension of \( \kappa(f) \). But, \( \kappa(Y_\eta) \) is the function field of \( \mathcal{Y} \), so we may compute a nonempty open subset \( V \subset \mathcal{Y} \) on which \( f \) is a well defined \( k \)-morphism \( V \to \mathbb{A}^1_k \). Let \( U \subset H \) be the image of \( V \) under \( \mathcal{Y} \to H \). Then, \( f \) is a well defined element of \( k(s)(Y_s) \) for all \( s \in U \). Now, \( df \neq 0 \in \Omega_{k(s)} \) because \( \kappa(Y_\eta) \) is separable over \( \kappa(f) \), so we may replace \( U \) by a smaller nonempty open set to assume \( df \neq 0 \in \Omega_{k(s)(Y_s)} \) for all \( s \in U \). If \( d(\pi_s^*f) = 0 \in \Omega_{k(s)}(X_s) \), then \( d(\pi_s^*f) = 0 \in \Omega_{k(s)}(X_{k(s)}) \) for all \( s \in U \), meaning \( \pi_s \) is inseparable for all \( s \in U \). If \( d(\pi_s^*f) \neq 0 \in \Omega_{k(s)}(X_s) \), we may again replace \( U \) by a smaller nonempty open set such that \( d(\pi_s^*f) \neq 0 \in \Omega_{k(s)}(X_{k(s)}) \) for all \( s \in U \), meaning \( \pi_s \) is separable for all \( s \in U \). The irreducible components of \( H \setminus U \) have smaller dimension than \( H \), so, by induction, we have proved Claim 2.

[2] then prove the following (because they work over \( \overline{\mathbb{Q}} \), there is no mention of separability of \( \pi_s \), but the proof of the claim stated here is exactly the same):

**Claim 3.** Let \( H \) be a locally closed subset of \( G \) satisfying (2) in Claim 1 and (2) in Claim 2. Let \( J \) be the set of \( s \in H \) for which the linear subspace \( L \subset \mathbb{P}^{\alpha}_{k(s)} \) is equal to the linear subspace \( L' \subset \mathbb{P}^{\alpha}_{k(s)} \) defined as the common zeros of the sections in the image \( H^0(Y_s, 3K_{Y_s}) \to H^0(X_{k(s)}, 3K_{X_{k(s)}}) \). Then, \( J \) is constructible and computable.

Claims 1, 2, and 3 together tell us that the set of \( s \in G(k) \) satisfying (i), (ii), and (iii) above are the closed points of a computable subvariety \( J \) of \( G \). By the de Franchis-Severi Theorem, there are finitely many such \( s \), so \( \dim J = 0 \). Thus, its set of points is computable and therefore \( C_g \) is as well.

\[ \blacksquare \]

**Remark 6.2.** If we are given smooth curves \( X \) and \( Y \) over \( k \) with \( g(Y) \geq 2 \), then for there to exist a separable morphism \( X \to Y \), we must have \( g(X) \geq g(Y) \geq 2 \). Thus, computing the finite set of separable morphisms \( (Y', \pi') \) described by the theorem and determining which \( Y' \) are isomorphic to \( Y \) shows that the set of separable morphisms from \( X \) is to \( Y \) is finite and computable.

As in the case \( \tilde{g} = 1 \), we break the proof of 1.1 into the cases where \( Y_K \) is isotrivial and \( Y_K \) is nonisotrivial. Which case we are in can be detected using Proposition 3.15.
Proof of Theorem 1.1, assuming \( \tilde{g} \geq 2 \) and \( Y_0 \) is isotrivial. Assume Input 3.14. Using Proposition 3.15 and Remark 3.5, replace \( k_0 \) by \( \ell_0 \), \( K_0 \) by \( L_0 \), and \( Y \) by \( (Y_0)_{K_0} \) via the isomorphism \( \phi \). Thus,

\[
Y_0(K) = \{ \text{morphisms } \text{Spec } K \to Y_0 \} = \{ k\text{-morphisms } C \to Y_0 \} = Y_0(k) \cup \{ \text{nonconstant } k\text{-morphisms } C \to Y_0 \}.
\]

Using Theorem 6.1, compute the finitely many separable \( k \)-morphisms \( g_1, \ldots, g_n : C \to Y_0 \), and let \( Q_1, \ldots, Q_n \) denote the corresponding elements of \( Y_0(K) \). Choose \( z \) and \( r \) as in Proposition 3.4 so that \( r \) is defined on all of the \( Q_i \). We claim that a point \( P \in Y_0(K) \) falls into one of the following cases:

(i) \( P = Q_i \) for some \( i \), or

(ii) \( P = F(Q) \) for some \( Q \in Y_0^{(1/p)}(K) \).

To see this, suppose \( P \in Y_0(K) \). If \( P \in Y_0(k) \), then because \( k \) is algebraically closed, \( P \) satisfies (ii). Now, assume \( P \notin Y_0(k) \) and \( P \) does not satisfy (i). Then, \( P \) can be identified with a nonconstant inseparable \( k \)-morphism \( f : C \to Y_0 \). Because \( C \) is smooth, this implies \( f \) factors as \( g \circ F \) for some \( k \)-morphism \( g : C^{(p)} \to Y_0 \). Taking the \( p \)th root of all coefficients in \( g \) gives us a \( k \)-morphism \( g^{(1/p)} : C \to Y_0^{(1/p)} \), corresponding to a point \( Q \in Y_0^{(1/p)}(K) \). Furthermore,

\[
f = g \circ F = F \circ g^{(1/p)},
\]

meaning \( P = F(Q) \).

The set of \( P \) satisfying (i) is finite, so determine which ones satisfy \( r(P) \in K^p \). Lastly, compute the set of \( P \) satisfying (ii) such that \( r(P) \in K^p \) using Proposition 3.8, taking \( Z = (Y_0^{(1/p)})_K \) and \( f = F \).

Let \( k \) be a field, \( Y \) be a smooth connected projective surface over \( k \), and \( C \) be a smooth connected projective curve over \( k \) together with a morphism \( \phi : Y \to C \). Then we say \( \phi \) is semistable if

(i) the generic fiber of \( \phi \) is a smooth geometrically connected projective curve over \( K \),

(ii) the geometric fibers of \( \phi \) are reduced with at worst normal crossing singularities, and

(iii) the fibers of \( \phi \) contain no \((-1)\)-curves.

**Theorem 6.3.** Let \( k \) be a field of characteristic \( p \) and \( K = k(C) \), where \( C \) is a smooth integral curve over \( k \). Let \( Y \) be a smooth connected projective curve over \( K \) with genus \( g(Y) \geq 2 \). Let \( \ell > 768g(Y) \) be a prime not equal to \( p \), and assume \( Y(K) \neq \emptyset \) and \( \text{Pic } Y[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2g(Y)} \). Let \( \phi : Y \to C \) be a minimal regular model for \( Y \). Then \( \phi \) is semistable.

**Proof.** See [11], Theorem 0CDN. \( \square \)
Let $Y$ and $\phi: Y \to C$ be as in Theorem 6.3. There is an induced morphism $\alpha: C \to \overline{M}_g$, where $\overline{M}_g$ is the coarse moduli space of stable curves of genus $g$ over $k$. The image of $\alpha$ will be a projective curve over $k$ if $Y$ is nonisotrivial. In this case, the inseparable degree of $\alpha$ is equal to $p^e$ for some integer $e \geq 0$, which Szpiro ([13]) defines as the modular inseparability exponent of $\phi$. Note that we have a commutative diagram

$$
\begin{array}{ccc}
\text{Spec } K & \longrightarrow & \text{Spec } F \\
\downarrow & & \downarrow \\
C & \longrightarrow & \overline{M}_g
\end{array}
$$

(6.1)

where $F$ is the residue field of the image of Spec $K$ and has transcendence degree one over $k$, and $p^e$ is the inseparable degree of $K/F$. This means that $e$ depends only on $Y$, so we will also refer to $e$ as the modular inseparability exponent of $Y$.

Let $B \subset C$ be an open subset with $Z := \phi^{-1}(B)$ such that $Z \to B$ is smooth. Consider the exact sequence of tangent sheaves on $Z$:

$$0 \to \mathcal{T}_{\mathcal{Z}/B} \to \mathcal{T}_{\mathcal{Z}} \to \phi^*\mathcal{T}_B \to 0.$$ 

The natural homomorphism $\mathcal{T}_B \to \phi_*\phi^*\mathcal{T}_B$ is an isomorphism, so we have an exact sequence

$$0 \to \phi_*\mathcal{T}_{\mathcal{Z}/B} \to \phi_*\mathcal{T}_{\mathcal{Z}} \xrightarrow{\beta} \mathcal{T}_B \xrightarrow{\gamma} R^1\phi_*\mathcal{T}_{\mathcal{Z}/B}.$$ 

(6.2)

Then $e > 0$ if and only if the Kodaira-Spencer map $\gamma$ is zero.

**Proposition 6.4.** Let $\phi: Y \to C$ be semistable with modular inseparability exponent $e$. Let $Y$ be the generic fiber of $\mathcal{Y}$, and suppose $Y$ has genus at least two. Then $e > 0$ if and only if there exists a curve $Y'$ over $kK^p$ such that $Y \simeq Y'_K$. If this is the case, then the modular inseparability exponent of $Y'$ is $e - 1$.

**Proof.** Let $\varepsilon \in C$ be the generic point. Taking stalks of (6.2) at $\varepsilon$, we get

$$0 \longrightarrow H^0(Y, \mathcal{T}_Y) \longrightarrow (\phi_*\mathcal{T}_{\mathcal{Z}})_\varepsilon \xrightarrow{\beta_\varepsilon} \mathcal{T}_{B, \varepsilon} \xrightarrow{\gamma_\varepsilon} H^1(Y, \mathcal{T}_Y).$$

Here, $\mathcal{T}_{B, \varepsilon}$ is a one-dimensional $K$-vector space and can be identified with the set of $k$-derivations on $K$. Then $e > 0$ if and only if $\gamma_\varepsilon = 0$ if and only if $\beta_\varepsilon$ is an isomorphism. Let $\delta$ be a nonzero $k$-derivation on $K$. We therefore see that $e > 0$ if and only if $\delta$ extends to a derivation on $\mathcal{O}_Y|_{\phi^{-1}(U)}$ for some open $U \subset B$ if and only if $\delta$ extends to a $k$-derivation on $\mathcal{O}_Y$. By Proposition 3.16, this is satisfied if and only if there exists a curve $Y'$ over $kK^p$ such that $Y \simeq Y'_K$.

With the notation in (6.1), the map Spec $K \to \overline{M}_g$ factors as

$$\text{Spec } K \to \text{Spec } kK^p \to \text{Spec } F \to \overline{M}_g.$$
Then the modular inseparability exponent of $Y'$ is

$$[kK^p : F]_i = \frac{[K : F]_i}{[kK^p : F]_i} = p^{e-1}.$$ 

\[\square\]

**Proposition 6.5.** There exists an algorithm that takes in (i)-(iii) of Input 3.14 and a smooth curve $Y$ over $K_0$ of genus at least two and either computes a curve $Y'$ over $k_0K_0^p$ such that $Y \cong Y'_k$ or determines if no such $Y'$ exists.

**Proof.** First determine an affine open subset $B = \text{Spec} A$ of $C$ such that $Y$ spreads out to a smooth projective $k_0$-morphism $\phi : Y \to B$. Let $\varepsilon$ denote the generic point of $C$. Let $R$ be the homogeneous coordinate ring of $Y$ as a projective $B$-scheme, and compute an $R$-module $M$ such that $T_Y = \bar{M}$. Then compute $N := M \otimes_A K_0$, which is a module over the homogeneous coordinate ring of $Y$, as well as $H := H^0(Y, N)$. We have natural isomorphisms

$$H \cong H^0(Y, T_Y|_Y) \cong H^0(Y, T_Y) \otimes_A K_0 \cong H^0(B, \phi_* T_Y) \otimes_A K_0 \cong (\phi_* T_Y)_\varepsilon.$$ 

By the proof of Corollary 3.7, $Y'$ exists if and only if $H \neq 0$. So, if $H = 0$, then the algorithm stops here. Otherwise, choose any nonzero $\tilde{\delta} \in H$ thought of as a $k_0$-derivation on $O_Y$. Let $\delta$ be its image in $H^0(B, T_B)$. By Proposition 3.16, the kernel of $\delta$ is the structure sheaf of the desired $Y'$. From $\delta$, determine the induced $k$-derivation $\tilde{\delta}_\eta$ on $K_0(Y)$. Consider $\tilde{\delta}_\eta$ as a $k_0K_0(Y)^p$-linear operator on the $p^2$-dimensional $k_0K_0(Y)^p$-vector space $K_0(Y)$, and compute its kernel $F$. Compute a presentation $F = k_0K_0^p[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. In this way, $F$ is the function field of an affine curve $Z$ over $k_0K_0^p$. The normalization of the projective closure of $Z$ is isomorphic to $Y'$ over $k_0K_0^p$, so compute this to finish the proof. \[\square\]

**Theorem 6.6.** Let $\phi : Y \to C$ be semistable. Let $Y$ be the generic fiber of $Y$, and suppose $Y$ has genus at least two. Let $s : C \to Y$ be a section of $\phi$ with $E := s(C)$. Then

$$-E.E \leq p^e \frac{8}{3} \left[ \frac{3g(Y) + 2}{3g(Y)} \right]^2 \left( f + 1 + \frac{2g(C) - 2}{3g(Y)} + \frac{1}{3g(Y)} \right),$$

where $f$ is the number of nonsmooth fibers of $\phi$ and $e$ is the modular inseparability exponent of $\phi$.

**Proof.** See [13], Corollaire 2. \[\square\]

**Remark 6.7.** Given (i)-(iii) of Input 3.14 and a semistable morphism $\phi : Y \to C$ over $k_0$ as in Theorem 6.6, one can compute the number on the right hand side of (6.3). To compute $e$, repeatedly apply Proposition 6.5 and Proposition 6.4. There will be a curve $Y'$ over $k_0K_0^p$ such that $Y \cong Y'_k$, but there will not exist such a curve over $k_0K_0^{p+1}$.

**Theorem 6.8.** Let $k$, $K$, and $\phi : Y \to C$ be as in Theorem 6.3. The relative dualizing sheaf $\omega_{Y/C} = K_Y - \phi^* K_C$ satisfies

(i) $\omega_{Y/C} \cdot \omega_{Y/C} \geq 0$, with equality if and only if $Y$ is isotrivial, and
(ii) $\omega_{Y/C}.D \geq 0$ for all effective divisors $D$ on $Y$, with equality if and only if $D$ is supported on the rational curves of self-intersection $-2$ contained in the fibers of $\phi$.

In particular, if $Y$ is nonisotrivial, $\omega_{Y/C}$ is big.

Proof. See [13], Théorème 1 and Théorème 2. Bigness of $\omega_{Y/C}$ follows from [6], Theorem 2.2.16. \hfill \Box

**Theorem 6.9.** Let $k$ be an algebraically closed field of characteristic $p$ and $K = k(C)$, where $C$ is a smooth integral curve over $k$. If $Y$ is a smooth nonisotrivial curve over $K$ with $g(Y) \geq 2$, then the set $Y(K)$ is finite.

Proof. See [8], Théorème 4. \hfill \Box

**Theorem 6.10.** There exists an algorithm that takes in (i)-(iii) of Input 3.14 and a smooth connected projective nonisotrivial curve $Y$ over $K_0$ with genus $g(Y) \geq 2$ and computes $Y(K)$.

Proof. Compute a finite separable extension $L_0/K_0$ and a projective smooth model $\phi: Y \to C$ for $Y_{L_0}$ as in Theorem 6.3. For simplicity, replace $K_0$ by $L_0$ by Remark 3.5. For the remainder of this proof, it will be convenient to work over $k$ instead of $k_0$, so by base changing, we will consider $Y$ and $C$ as varieties over $k$. Suppose $Y$ is embedded in $\mathbb{P}^n_k$, and choose a hyperplane $H$ in $\mathbb{P}^n_k$. Compute the number $N$ on the number on the right hand side of (6.3) by Remark 6.7. By Theorem 6.8 and Kodaira’s Lemma ([6], Proposition 3.4.2.6), $H^0(Y, n\omega_{Y/C} - H|_Y)$ is nonzero for sufficiently large $n$. Thus, compute some positive integer $n$ and effective divisor $D$ on $Y$ such that $n\omega_{Y/C}$ is linearly equivalent to $H|_Y + D$. Compute the irreducible components $C_1, \ldots, C_r$ of $D$, and compute the nonnegative integer

$$M := \max\{0, -C_i.C_i\}.$$

Note that if $C'$ is an integral curve on $Y$, then $C'.D \geq -M$. A point $P \in Y(K)$ corresponds to a section $s_P$ of $\phi$. Let $E := s_P(C) \subset Y$. By Theorem 6.6,

$$E.H|_Y = E.\left(n\omega_{Y/C} - D\right) = n\left(E.K_Y - E.\phi^*K_C\right) - E.D = n\left((2g_C - 2 - E.E) - (2g_C - 2)\right) - E.D = -nE.E - E.D \leq nN + M.$$

Now, for each $1 \leq d \leq nN + M$, compute the Hilbert scheme $H$ of 1-dimensional $k$-subschemes of $\mathbb{P}^n_k$ of genus $g(C)$ and degree $d$, and let $\psi: H \to H$ be the universal family embedded in $\mathbb{P}^n_{k'} \times_k H$. If $H' \subset H$ is an irreducible component with generic point $\eta$ and $h \in H'(k)$ is such that $H_h$ is a smooth integral curve over $k$, then

(1) $h$ is a reduced point,

(2) $H_\eta$ is a smooth integral curve over $k(\eta)$, and

(3) $H_h$ has genus $g(C)$ and degree $d$ as a curve in $\mathbb{P}^n_k$.  

Thus, compute the reduced loci $H_1, H_2, \ldots, H_m$ of the irreducible components of $H$. Throw out any $H_i$ if the curve $H_i$ over the generic point $\eta \in H_i$ is not smooth and integral. Lastly, replace $H_i$ by the open subset of $h \in H_i$ such that $H_h$ is smooth and integral.

**Claim 1.** Let $H'$ be a reduced locally closed subvariety of one of the $H_i$, and let $H''$ be the locus of $h \in H'$ such that $H_h \subset \mathcal{Y}_{k(h)} \subset \mathbb{P}^n_{k(h)}$. Then $H''$ is a computable closed subset of $H'$.

We prove Claim 1 by induction on the dimension of $H'$. It suffices to assume $H'$ is irreducible and affine, say $H' = \text{Spec } A$. Let $H' \subset H$ be the preimage of $H'$. Let $F$ denote the fraction field of $A$. Let $S := A[x_0, \ldots, x_n]$ be the homogeneous coordinate ring of $\mathbb{P}^n_A$ and $I$ be the homogeneous ideal for $H' \subset \mathbb{P}^n_A$.

Now, consider the following procedure given a homogeneous element $f$ in $S$ of degree $e$. Compute a projection $p_F: S_e \otimes_A F \rightarrow I_e \otimes_A F$ (here $S_e$ and $I_e$ denote the graded pieces of degree $e$ in $S$ and $I$ respectively). Write $p_F$ as a matrix with entries in $F$, and compute the localization $A'$ of $A$ by inverting the denominators of these entries. Thus, $p_F$ spreads out to an $A'$-homomorphism $p_{A'}: S_e \otimes_A A' \rightarrow I_e \otimes_A A'$ that is the identity when restricted to $I_e \otimes_A A'$. Compute

$$f - p_{A'}(f) = \sum_{\alpha} a_{\alpha}(f)x^{\alpha}$$

(here we are using multi-index notation, i.e., if $\alpha = (\alpha_0, \ldots, \alpha_n)$ with $\alpha_0 + \cdots + \alpha_n = e$, then $x^\alpha := x_0^{\alpha_0} \cdots x_n^{\alpha_n}$).

Let $f_1, \ldots, f_\ell$ be homogeneous generators for the ideal for $\mathcal{Y}$ thought of as elements of $S$. Let $J$ be the radical of the ideal of $A'$ generated by all the $a_\alpha(f_i)$, and let $A' := A'/J$. A point $h \in \text{Spec } A'(k)$ is such that $H_h \subset \mathcal{Y}$ if and only if $a_\alpha(f_i)$ vanish at $h$ for all $\alpha$ and $i$. Thus, Spec $A''$ is the intersection of the desired closed subvariety $H''$ with Spec $A'$. The complement $H' \setminus \text{Spec } A'$ has dimension less than the dimension of $H'$, so by induction, we have proved Claim 1.

Apply Claim 1 to each $H_i$ to compute the locally closed subvariety $Z \subset H$ of points $h \in H(k)$ such that $H_h$ is a smooth integral curve contained in $\mathcal{Y}$, and let $Z \subset H$ be the preimage of $Z$. Let $\phi'$ be the composition of $Z$-morphisms $Z \rightarrow \mathcal{Y} \times_k Z \rightarrow C \times_k Z$. We now wish to determine the set of $h \in Z(k)$ such that $\phi'_{h|Z}: Z_h \rightarrow C$ is an isomorphism.

**Claim 2.** Let $h \in Z(k)$ be a point such that $\phi'_{h|Z}: Z_h \rightarrow C$ is an isomorphism. Then $h$ is an isolated point of $Z$.

To see this, let $h$ be such a point. Let $\varepsilon$ denote the generic point of $C$ and consider the pullback morphism $\phi'_\varepsilon: Z_\varepsilon \rightarrow \varepsilon \times Z$. Notice that the set of $h' \in Z(k)$ such that $\phi'_{h'|Z}$ is a nonconstant morphism is the set of $h' \in Z(k)$ in the image of $\phi'_\varepsilon$. But, $\phi'_\varepsilon$ is the composition of flat morphisms $Z_\varepsilon \rightarrow Z \rightarrow Z$, so the image of $\phi'_\varepsilon$ is an open subset $U$ of $Z$ containing $h$. Let $U \subset Z$ be the preimage of $U$. Then $\phi'_{\varepsilon|U}: V \rightarrow C \times_k U$ is quasi-finite. Furthermore, $\phi'_{\varepsilon|U}$ is proper because $C \times_k U \rightarrow U$ is separated and the composition $U \rightarrow C \times_k U \rightarrow U$ is proper, so $\phi'_{\varepsilon|U}$ is finite. Let $x \in Z_h$ be any point. The cardinality of fibers of $\phi'_{\varepsilon|U}$ is an upper semicontinuous function, so there exists some open $V \subset U$ containing $x$ such that $\phi'$ restricts to an isomorphism on $V$. Let $V \subset U$ be the (open) image of $V$. For every $h' \in V(k)$, the morphism $\phi'_{h'|V}: Z_{h'} \rightarrow C$ is an isomorphism. The inverse $C \rightarrow Z_{h'}$ composed with $Z_{h'} \rightarrow \mathcal{Y}$ defines a section of $\phi$. There can only by finitely many such sections by Theorem 6.9, so $V$ is 0-dimensional. This proves Claim 2.
To compute $Y(K)$, compute the 0-dimensional irreducible components $h_1, \ldots, h_s$ of $Z$ and determine which give rise to isomorphisms $Z_{h_i} \to C$. Lastly, compute their inverses $C \to Z_{h_i}$ and their corresponding elements of $Y(K)$.

Proof of Theorem 1.1, assuming $\tilde{g} \geq 2$ and $Y$ is nonisotrivial. Assume Input 3.14. Compute $Y(K)$ using Theorem 6.10, and then compute $X(K)$ as preimages of $\pi$.

Proof of Corollary 1.2. If $X(L)$ is finite for every finite separable extension $L$ of $K$, then neither of the following can be true for $X$:

(i) $X$ is smooth of genus 0 or 1,

(ii) $X$ is smooth of genus at least 2 and is isotrivial.

Thus, $X$ is either smooth of genus at least 2 and not isotrivial, in which case we use Theorem 6.10, or $X$ is not smooth, in which case we use Theorem 1.1.

References


