COMPOSITIO MATHEMATICA

Belyi's theorem in characteristic two

Yusuke Sugiyama and Seidai Yasuda

Compositio Math. **156** (2020), 325–339.

doi:10.1112/S0010437X19007723

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
EST. 1865

Compositio Math. 156 (2020) 325–339
doi:10.1112/S0010437X19007723

Belyi's theorem in characteristic two

Yusuke Sugiyama and Seidai Yasuda

Abstract

We prove an analogue of Belyi's theorem in characteristic two. Our proof consists of the following three steps. We first introduce a new notion called *pseudo-tameness* for morphisms between curves over an algebraically closed field of characteristic two. Secondly, we prove the existence of a 'pseudo-tame' rational function by showing the vanishing of an obstruction class. Finally, we construct a tamely ramified rational function from the 'pseudo-tame' rational function.

1. Introduction

Belyi's theorem (cf. [Bel79]) states that a proper smooth curve X defined over the field of complex numbers is defined over a number field if and only if X admits a rational function f on X such that f has at most three branch points when regarded as a morphism from X to the projective line. In [Saï97], Saïdi remarked that the following analogue of Belyi's theorem holds in odd positive characteristics.

Theorem 1.1 (Saïdi). *A proper smooth curve C defined over a field of odd characteristic is defined over a finite field if and only if C admits a rational function f such that f is tamely ramified everywhere and has at most three branch points when regarded as a morphism from C to the projective line.*

In characteristic two, it is easy to see that the 'if' part of the same statement holds true; however, the 'only if' part has remained open. In this paper we give a proof of the 'only if' part by proving the following statement, which is well known when the base field k is not of characteristic two (cf. [Ful69]).

Theorem 1.2. *Let X be a proper smooth curve over an algebraically closed field k. Then X admits a morphism $f : X \to \mathbb{P}^1_k$ which is tamely ramified everywhere.*

After the first draft of this paper had appeared in arXiv, Nurdagül Anbar and Seher Tutdere [AT18] gave an alternative proof of the theorem above in the language of function fields. We note that their proof is based on some of our key results (Theorems 2.11 and 2.10) and the argument using Tsen's theorem in our proof of Lemma 3.4 below.

Let us give an outline of our proof of Theorem 1.2. Let $k(X)$ be the function field of a curve X over an algebraically closed field k of characteristic two. We set $\mathcal{H} = k(X)\backslash k(X)^2$. This can be identified with the set of finite separable morphisms from X to $\mathbb{P}^1_k$. Our aim is to find an element $f \in \mathcal{H}$ which is tamely ramified at every closed point of X. The first step is to introduce a

Received 5 June 2018, accepted in final form 26 August 2019, published online 18 December 2019.
2010 Mathematics Subject Classification 11G20 (primary), 11G32, 14G17, 14H05 (secondary).
Keywords: Belyi's theorem, algebraic curves, characteristic two, tame covering.

new notion of 'pseudo-tameness' by weakening the condition of tameness of a morphism between curves. We use this notion for morphisms from X to $\mathbb{P}^1_k$. In this case, a precise definition can be given as follows: a rational function $f \in \mathcal{H}$ is called pseudo-tame at a closed point $x \in X$ if it becomes tame at x by adding a fourth power of some $h \in k(X)$. A rational function f is said to be pseudo-tame on X when f is pseudo-tame at every closed point of X. As we see from Lemma 2.4, pseudo-tameness is stable under the action of $\Gamma = \mathrm{PGL}_2(k(X)^4)$ on $\mathcal{H}$ given by fractional linear transformations. The key step is to prove the existence of an element $f \in \mathcal{H}$ which is pseudo-tame on X. We explain more about this step in the next paragraph. In the final step, we show that any pseudo-tame rational function can be made tame everywhere on X when translated by some element of Γ using the Riemann–Roch theorem.

We prove the existence of a pseudo-tame rational function on X in the following way. We start by introducing a map

$$a(-,-) : \mathcal{H} \times \mathcal{H} \to k(X)/k(X)^2.$$

See Definition 2.8 for the definition of $a(-,-)$. The map $a(-,-)$ has the following nice properties. First, it follows from the construction that $a(-,-)$ is symmetric and bi-Γ-invariant. Second, we have a criterion for pseudo-tameness in terms of the map $a(-,-)$. We refer to Theorem 2.10 for a precise statement. Third, as we will see in Proposition 2.11, the map $a(-,-)$ satisfies a certain cocycle condition. These properties and Tsen's theorem allow us to introduce an obstruction class $\beta(X) \in H^1(X, \mathcal{O}_X/\mathcal{O}_X^2)$ to the existence of a pseudo-tame rational function on X. Finally, we use the Serre duality to prove that the obstruction class $\beta(X)$ always vanishes, that is, a pseudo-tame rational function on X always exists.

Let us explain the organization of this paper. In § 2 we first introduce a new notion of 'pseudo-tameness' for morphisms between curves over an algebraically closed field of characteristic two, and observe their basic properties. In Definition 2.8 we introduce the map $a(-,-)$ mentioned in the previous paragraph, and then study its properties. As we will see in Theorem 2.10, the map $a(-,-)$ turns out to be closely related to pseudo-tameness. In § 3 we define the obstruction class $\beta(X)$ to the existence of a pseudo-tame rational function on a curve X in characteristic two using $a(-,-)$. Then we prove that this obstruction class always vanishes. As a consequence, we have a pseudo-tame rational function on any curve in characteristic two. In § 4 we construct a tamely ramified rational function from any pseudo-tame rational function. In § 5 we give an explicit upper bound, for any given curve X in characteristic two, of the minimum of the degrees of pseudo-tamely ramified rational functions on X and those of tamely ramified rational functions on X.

2. Pseudo-tame morphisms

We fix an algebraically closed field k of characteristic two. By a 'curve' we mean a one-dimensional integral scheme which is proper and smooth over k. For a curve X, we denote by $k(X)$ the field of rational functions on X.

2.1 Basic facts on curves

We recall some basic facts on curves over an algebraically closed field of characteristic two (cf. [Har77]).

Let X be a curve. Since the relative Frobenius on X over k is of degree two and k is algebraically closed (in particular, perfect), the function field $k(X)$ is a two-dimensional $k(X)^2$-vector space, where

$$k(X)^2 = \{f^2 \mid f \in k(X)\}.$$

Note that the differential dg vanishes on X if and only if $g \in k(X)^2$. Thus, for any $g \in k(X)$ with $dg \neq 0$, the function field $k(X)$ is the direct sum $k(X)^2 \oplus k(X)^2 g$ as a $k(X)^2$-vector space.

We denote by B_X the sheaf $\mathcal{O}_X/\mathcal{O}_X^2$ of $\mathcal{O}_X^2$-modules on X. Let $X^{(1)} = X \times_{\mathrm{Spec}(k),\mathrm{Frob}_2} \mathrm{Spec}(k)$ be the Frobenius twist of X. As we explain in § 3.3, we may identify the $\mathcal{O}_X^2$-module B_X on X with Raynaud's $\mathcal{O}_{X^{(1)}}$-module B on $X^{(1)}$ introduced by Raynaud [Ray82] via the canonical isomorphism of ringed spaces

$$X^{(1)} \xrightarrow{\sim} (X, \mathcal{O}_X^2).$$

Moreover, the Jacobian of X is ordinary if and only if $H^0(X, B_X) = 0$. Note that for an open subset $U \subset X$, we may identify $H^0(U, B_X)$ with the set of elements of $k(X)/k(X)^2$ that are regular at every closed point of U.

2.2 Pseudo-tame morphisms

In this subsection we introduce the notion of pseudo-tameness for morphisms between curves.

Let X, Y be curves and $f : X \to Y$ be a finite morphism. For a closed point $x \in X$, the morphism f induces the local homomorphism $f^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$, where $y = f(x) \in Y$. We denote by $t \in \mathcal{O}_{Y,y}$ a uniformizer at y and let v_x be the normalized valuation of $\mathcal{O}_{X,x}$.

DEFINITION 2.1. Let the notation be as above. We say that the morphism f is *pseudo-tame* at x if there exists an element $h \in \mathcal{O}_{X,x}$ such that $v_x(f^*t + h^4)$ is an odd number.

In particular, if the morphism $f : X \to Y$ is at most tamely ramified at a closed point $x \in X$, then f is pseudo-tame at x. One can check easily that pseudo-tameness is independent of the choice of a uniformizer t. For a nonempty open subset $U \subset X$, we say that f is pseudo-tame on U if f is pseudo-tame at every closed point of U.

In this paper we mainly deal with the case where $Y = \mathbb{P}_k^1$, that is, f is a rational function on X. We remark that in [Hos17], Hoshi recently gave a natural interpretation of pseudo-tame rational functions in terms of certain rank-two vector bundles.

DEFINITION 2.2. We say that a rational function $f \in k(X)$ is *pseudo-tame* at a closed point $x \in X$ if $f : X \to \mathbb{P}_k^1$ is pseudo-tame at x. For a nonempty open subset $U \subset X$, we say that a rational function f is *pseudo-tame on* U if f is pseudo-tame at every closed point of U.

2.3 Paraphrasing pseudo-tameness

Let us fix a curve X and let

$$\mathcal{H} = k(X) \backslash k(X)^2$$

denote the set of finite separable rational functions on X. In this subsection we give some equivalent conditions for a rational function on X to be pseudo-tame at a given closed point. These conditions are given in terms of the action of the group $\Gamma = \mathrm{PGL}_2(k(X)^4)$ on $\mathcal{H}$ by fractional linear transformations.

Let us remark that the completion of the local ring $\mathcal{O}_{X,x}$ helps us to understand the pseudo-tameness of $f : X \to Y$.

Remark 2.3. Let $s \in \mathcal{O}_{X,x}$ and $t \in \mathcal{O}_{Y,y}$ be uniformizers at closed points $x \in X$ and $y = f(x) \in Y$, respectively. Let us consider the power series expansion of $f^*(t) \in \mathcal{O}_{X,x}$ with respect to s. Then, by definition, the following conditions are equivalent:

- f is pseudo-tame at x;
- for any nonvanishing term in the power series expansion of $f^*(t)$ with degree smaller than $\mathrm{ord}_x(df^*t)+1$, the degree is a multiple of four.

Now let X, x, and s be as above and let $f \in \mathcal{H}$ be a rational function. Let us consider the Laurent series expansion $f = \sum_{n \gg -\infty} c_n s^n$ of f at x with respect to s. Then, as the consequence of the equivalence above, f is pseudo-tame at x if and only if any integer n with $n < \mathrm{ord}_x(df)+1$ and $c_n \neq 0$ is a multiple of four.

Set $\Gamma = \mathrm{PGL}_2(k(X)^4)$. Then the group Γ acts on $\mathcal{H}$ freely by fractional linear transformations. The following lemma describes the pseudo-tameness of a rational function $f \in \mathcal{H}$ in terms of the Γ-orbit of f.

Lemma 2.4. *A rational function $f \in \mathcal{H}$ is pseudo-tame at $x \in X$ if and only if there exists $\gamma \in \Gamma$ such that $v_x(\gamma f) = 1$.*

Proof. Let us check that for any $f \in \mathcal{H}$, we have an element $\gamma \in \Gamma$ such that $v_x(\gamma f) \in \{1,2\}$. By adding some element of $k(X)^4$ to f, we may assume $v_x(f) \not\equiv 0 \bmod 4$. If $v_x(f) \equiv 1,2 \bmod 4$ (respectively, $v_x(f) \equiv 3 \bmod 4$), then it is easy to find an element $g \in k(X)^\times$ such that the element $f' = g^4 f$ (respectively, $f' = g^4/f$) satisfies $v_x(f') \in \{1,2\}$. Note that f' is a fractional linear transformation of f by some element of Γ. Hence the assertion follows from Remark 2.3 on the pseudo-tameness of a rational function $f \in \mathcal{H}$ since we have

$$\{\gamma \in \Gamma \mid v_x(\gamma f) = 1\} \cap \{\gamma \in \Gamma \mid v_x(\gamma f) = 2\} = \emptyset. \qquad \square$$

Corollary 2.5. *For a rational function $f \in \mathcal{H}$, the following conditions are equivalent:*

(1) *f is pseudo-tame at x;*
(2) *f belongs to the Γ-orbit of a uniformizer at x;*
(3) *for any $\gamma \in \Gamma$, the rational function γf is pseudo-tame at x.*

2.4 The obstruction $A(f,g)$

Let X be a curve. Corollary 2.5 implies that the pseudo-tameness of a rational function f at a closed point of X depends only on the Γ-orbit of f. In this subsection we give some criteria when two functions $f, g \in \mathcal{H}$ are in the same Γ-orbit. These lead to the definition of $A(f,g) \in k(X)^2$ for $f, g \in \mathcal{H}$, which serves as the obstruction class for f and g to be the same Γ-orbit. At the end of this subsection we give some basic properties of $A(f,g)$.

Note that since $k(X) = k(X)^2 \oplus k(X)^2 g$, we may write a rational function f as

$$f = F_0^2 + F_1^2 g = f_0^4 + f_1^4 g + f_2^4 g^2 + f_3^4 g^3$$

with some rational functions $F_i, f_j \in k(X)$.

Lemma 2.6. *Let the notation be as above. Then the following conditions are equivalent:*

(1) *f and g are in the same Γ-orbit;*
(2) *$1, f, g$ and fg are linearly dependent over $k(X)^4$;*
(3) *$f_1 f_3 + f_2^2 = 0$.*

Proof. It is clear that assertion (1) implies assertion (2). Let us prove the converse is also true. Assertion (2) gives a nontrivial $k(X)^4$-linear relation $a^4 + b^4 f + c^4 g + d^4 fg = 0$. It suffices to show $a^4d^4 \neq b^4c^4$. Note that we have $(b^4, d^4) \neq (0,0)$ since 1 and $g \in \mathcal{H}$ are linearly independent over $k(X)^2$ (especially over $k(X)^4$). Then we have

$$f = \frac{a^4 + c^4 g}{b^4 + d^4 g}.$$

Now $f \notin k(X)^4$ implies $a^4d^4 \neq b^4c^4$ as desired.

Finally, let us consider the $k(X)^4$-linear endomorphism $T_{f,g}$ of $k(X)$ which maps the elements $1, g, g^2, g^3$ to the elements $1, g, f$ and fg, respectively. Note that we have $f \equiv f_2^4 g^2 + f_3^4 g^3$ and $fg \equiv f_1^4 g^2 + f_2^4 g^3$ modulo the $k(X)^4$-linear subspace of $k(X)$ spanned by 1 and g. These relations show that the endomorphism $T_{f,g}$ has the determinant $(f_1f_3 + f_2^2)^4$, which proves that assertions (2) and (3) are equivalent. □

Let $f, g \in \mathcal{H}$. It follows from Lemma 2.6 that the element $A(f,g) = f_1^2 f_3^2 + f_2^4 \in k(X)^2$ serves as the obstruction for f and g to be in the same Γ-orbit. For later use, we note the following formula:

$$A(f,g) = \left(\frac{dF_0}{dg}\right)^2 + \left(\frac{dF_1}{dg}\right)^2 g + \left(\frac{dF_1}{dg}\right) F_1, \tag{2.1}$$

which we can check easily from the definition of $A(f,g)$. We note that $A(f,g)$ is neither symmetric in f and g nor bi-Γ-invariant. Indeed, we have our next lemma.

Lemma 2.7. *For $f, g \in \mathcal{H}$, we have the following:*

(1) $A(a^4 f, g) = a^4 A(f,g)$ *for any* $a \in k(X)^\times$;
(2) $A(f + b^4, g) = A(f,g)$ *for any* $b \in k(X)$;
(3) $A(f, 1/g) = g^4 A(f,g)$;
(4) $A(f,g) = (df/dg)^3 A(g,f)$.

Proof. We give a proof of property (4). The other properties can be checked easily.

In the proof of Lemma 2.6 we have seen that the $k(X)^4$-linear endomorphism $T_{f,g}$ of $k(X)$ has determinant $A(f,g)^2$. Hence it suffices to show that the $k(X)^4$-linear automorphism P of $k(X)$ that takes the basis $1, g, g^2, g^3$ to the basis $1, f, f^2, f^3$ has the determinant $(df/dg)^6$.

Let us consider another basis $1, g, f^2, gf^2$ of $k(X)$. Then P is the composite of the following two automorphisms P_1 and P_2:

$$P_1 : 1, g, g^2, g^3 \mapsto 1, g, f^2, gf^2,$$
$$P_2 : 1, g, f^2, gf^2 \mapsto 1, f, f^2, f^3.$$

Observe that P_1 preserves the direct sum decomposition $k(X) = k(X)^2 \oplus k(X)^2 g$ and that P_2 is $k(X)^2$-linear. Using these observations and by noting that $df/dg = F_1^2$ is equal to the determinant of the $k(X)^2$-linear automorphism of $k(X)$ that takes the basis $1, g$ to the basis $1, f$, we can easily check that $\det P_1 = (df/dg)^4$ and $\det P_2 = (df/dg)^2$. Thus we have $\det P = (df/dg)^6$ as desired. □

2.5 The modified obstruction $a(f,g)$

Let X be a curve and let $f, g \in \mathcal{H}$. Lemma 2.7 tells us how to modify $A(f,g)$ to make it better behaved. The modified obstruction is given in Definition 2.8 and is denoted by $a(f,g)$. It is an element of $k(X)/k(X)^2$. After summarizing basic properties of $a(f,g)$, we prove that,

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

roughly speaking, the regularity of $a(f,g)$ reflects the pseudo-tameness of f and g (Theorem 2.10). In Proposition 2.11 we prove that $a(f,g)$ has a beautiful cocycle condition. Using this cocycle condition, we will introduce in Definition 3.2 an obstruction for X to admit a pseudo-tame rational function on X.

DEFINITION 2.8. For $f,g\in\mathcal{H}$, we set

$$\begin{aligned} a(f,g) &= \frac{A(f,g)g}{(df/dg)} \bmod k(X)^2 \\ &= \frac{(f_1^2f_3^2+f_2^4)g}{f_3^4g^2+f_1^4} \bmod k(X)^2 \in k(X)/k(X)^2. \end{aligned}$$

We summarize basic properties of $a(f,g)$.

PROPOSITION 2.9. *The element $a(f,g)$ is a symmetric, bi-Γ-invariant obstruction for $f,g\in\mathcal{H}$ to be in the same Γ-orbit. That is, the following hold for any $f,g\in\mathcal{H}$:*

(1) *the two functions f and g are in the same Γ-orbit if and only if $a(f,g)=0$;*
(2) *$a(f,g)=a(g,f)$;*
(3) *$a(f,g)=a(f,\gamma g)$ for any $\gamma\in\Gamma$.*

Proof. Property (1) follows from the fact that $A(f,g)$ is the obstruction for f,g to be in the same Γ-orbit. Property (4) in Lemma 2.7 implies property (2). Property (3) follows from properties (1), (2) and (3) in Lemma 2.7 together with property (2). □

The next theorem states that the regularity of $a(f,g)$ reflects the pseudo-tameness of f and g.

THEOREM 2.10. *Let $f,g\in\mathcal{H}$. Suppose that g is pseudo-tame at a closed point $x\in X$. Then the following two conditions are equivalent:*

(1) *$a(f,g)$ is regular at x, or equivalently, the differential form $A(f,g)dg/(df/dg)$ associated with $a(f,g)$ is regular at x;*
(2) *f is pseudo-tame at x.*

Proof. From Lemma 2.4, we recall that $f\in\mathcal{H}$ is pseudo-tame at $x\in X$ if and only if there exists $\gamma\in\Gamma$ satisfying $v_x(\gamma f)=1$ and that $f\in\mathcal{H}$ is not pseudo-tame at $x\in X$ if and only if there exists $\gamma\in\Gamma$ satisfying $v_x(\gamma f)=2$. Since $a(f,g)$ is bi-Γ-invariant (Proposition 2.9), we may assume that g is a uniformizer at x.

First, we prove that condition (2) implies condition (1). Since f is pseudo-tame at x, we may assume f is a uniformizer at x. Writing f as $f=F_0^2+F_1^2g$, we have $F_1\in\mathcal{O}_{X,x}^{\times}$ and $F_0\in\mathfrak{m}_{X,x}$. Then it suffices to prove that $A(f,g)dg/(df/dg)$ is regular at x. Since $dg\in\Omega_X$ are regular at x and $df/dg=F_1^2\in\mathcal{O}_{X,x}^{\times}$, this follows from the formula (2.1).

Next, we prove that condition (1) implies condition (2). Suppose f is not pseudo-tame at x. By replacing f with γf for some suitable $\gamma\in\Gamma$, we may assume $v_x(f)=2$. Write f as $f=F_0^2+F_1^2g=f_0^4+f_1^4g+f_2^4g^2+f_3^4g^3$. Then we have

$$F_0=f_0^2+f_2^2g\in\mathfrak{m}_{X,x}\backslash\mathfrak{m}_{X,x}^2$$

and

$$F_1=f_1^2+f_3^2g\in\mathfrak{m}_{X,x}.$$

This implies that $f_2\in\mathcal{O}_{X,x}^{\times}$ and $f_1\in\mathfrak{m}_{X,x}$. Thus we have $A(f,g)=f_1^2f_3^2+f_2^4\in\mathcal{O}_{X,x}^{\times}$ and $df/dg=F_1^2\in\mathfrak{m}_{X,x}^2$. As a result, $A(f,g)\,dg/(df/dg)$ is not regular at x, which contradicts (2). □

Surprisingly, it turns out that the obstruction $a(f,g)$ satisfies the following cocycle condition.

Proposition 2.11. *For $f,g,h \in \mathcal{H}$, the following Čech 1-cocycle condition holds:*

$$a(f,g)+a(g,h)+a(h,f)=0 \in k(X)/k(X)^2.$$

Proof. We note that an element $F \in k(X)$ belongs to $k(X)^2$ if and only if $dF = 0 \in \Omega_X$ and that $A(f,g), df/dg \in k(X)^2$. Hence, it suffices to show

$$\frac{A(f,g)}{df/dg}\,dg+\frac{A(g,h)}{dg/dh}\,dh+\frac{A(h,f)}{dh/df}\,df=0\in\Omega_X.$$

The relation $A(f,g)=(df/dg)^3A(g,f)$ reduces us to showing the equality

$$A(g,f)+\left(\frac{dh}{df}\right)^2A(g,h)+\left(\frac{dg}{dh}\right)A(h,f)=0\in k(X).$$

Write g,h as $g=G_0^2+G_1^2f$, $h=H_0^2+H_1^2f$, and $g=g_0^2+g_1^2h$. By formula (2.1) we have

$$\begin{aligned} A(g,f)&=\left(\frac{dG_0}{df}\right)^2+\left(\frac{dG_1}{df}\right)^2f+\frac{dG_1}{df}G_1, \\ \left(\frac{dh}{df}\right)^2A(g,h)&=\left(\frac{dg_0}{df}\right)^2+\left(\frac{dg_1}{df}\right)^2h+\frac{dg_1}{df}g_1H_1^2, \end{aligned} \tag{2.2}$$

and

$$\frac{dg}{dh}A(h,f)=\left(\frac{dH_0}{df}\right)^2g_1^2+\left(\frac{dH_1}{df}\right)^2g_1^2f+\frac{dH_1}{df}g_1^2H_1.$$

Hence, by applying the equalities $G_0=g_0+g_1H_0$ and $G_1=g_1H_1$ to (2.2), we obtain the desired equality. □

2.6 Stability under the composition

In this last part of this section we would like to mention, although we do not use it in the rest of the paper, that pseudo-tameness is stable under the composition of morphisms.

Proposition 2.12. *Let X,Y,Z be curves and $f:X\to Y$, $g:Y\to Z$ be finite morphisms. Let $x\in X$ be a closed point and set $y=f(x)$. Suppose f,g are pseudo-tame at x,y, respectively. Then $g\circ f$ is pseudo-tame at x.*

Proof. By Remark 2.3, we may prove the assertion by passing to the formal completions at the closed points. Let $S\subset tk[[t]]$ denote the subset of formal power series f in t such that $f+h^4$ has an odd vanishing order at $t=0$ for some $h\in tk[[t]]$. It suffices to show that S is closed under the composition of formal power series. Let $f_1,f_2\in S$ and let us write $f_i=g_i+h_i^4$ for $i=1,2$, where $h_i\in tk[[t]]$ and g_i has an odd vanishing order at $t=0$. Since $f_1(f_2(t))=g_1(f_2(t))+h_1(f_2(t))^4$, it suffices to show that $g_1(f_2(t))\in S$. Let m denote the vanishing order of g_1 at $t=0$. Since $f_2=g_2+h_2^4$, the vanishing order n of $f_2^m-h_2^{4m}$ at $t=0$ is odd and the vanishing order of $f_2^i-h_2^{4i}$ at $t=0$ is greater than n for any $i>m$. This implies that $g_1(f_2(t))-g_1(h_2^4(t))$ has an odd vanishing order at $t=0$. Since $g_1(h_2^4(t))$ belongs to $(tk[[t]])^4$, we have $g_1(f_2(t))\in S$, as desired. □

3. Existence of a pseudo-tame rational function

3.1 Construction of an obstruction class $\beta(X)$

For a curve X, we introduce a cohomology class $\beta(X) \in H^1(X, B_X)$ which turns out to be an obstruction for X to have a pseudo-tame rational function on X. First, we introduce a notion of a certain class of coverings of X.

Definition 3.1. For a curve X, an open covering $\mathcal{U} = (U_i)_{i \in I}$ of X is called *sufficiently refined* if each $U_i \subset X$ is nonempty and affine, and there exists a pseudo-tame rational function on U_i.

We remark that any curve X admits a sufficiently refined open covering of X. For example, we can construct it as follows. Take I as the set of closed points of X. For each closed point $x \in X$, take a uniformizer t_x at x and let U_x be an affine open neighborhood at x on which the rational function t_x is unramified. Then the covering $\mathcal{U} = (U_i)_{i \in I}$ is a sufficiently refined open covering of X. Note that for any quasi-coherent $\mathcal{O}_X^2$-module, its cohomology groups coincide with the corresponding Čech cohomology groups with respect to the covering $\mathcal{U}$ since U_i is affine for each $i \in I$.

Definition 3.2. For a curve X, let $\mathcal{U} = (U_i)_{i \in I}$ be a sufficiently refined open covering of X with a pseudo-tame rational function f_i on U_i. We set $\beta_{i,j} = a(f_i, f_j)$. Theorem 2.10 implies $\beta_{i,j} \in H^0(U_i \cap U_j, B_X)$. Thus Proposition 2.11 tells us that the family $(\beta_{i,j})$ defines an element of $H^1(X, B_X)$. We denote this element by $\beta(X, \mathcal{U}, (f_i)) \in H^1(X, B_X)$.

Proposition 3.3. *The element $\beta(X, \mathcal{U}, (f_i)) \in H^1(X, B_X)$ is independent of the choices of $\mathcal{U}$ and (f_i). Therefore we denote it by $\beta(X)$.*

Proof. First, we prove that, for any fixed sufficiently refined open covering $\mathcal{U} = (U_i)_{i \in I}$ of X, the cohomology class $\beta(X, \mathcal{U}, (f_i))$ is independent of the choice of (f_i). Let us take any two families (f_i) and (g_i) such that $f_i, g_i \in k(X)$ are pseudo-tame on U_i for each $i \in I$. We check that the two families $(a(f_i, f_j))_{i,j}$ and $(a(g_i, g_j))_{i,j}$ define the same element of $H^1(\mathcal{U}, B_X)$. Set $H_i = a(f_i, g_i) \in k(X)/k(X)^2$ for each i. Since the rational functions f_i and g_i are pseudo-tame on U_i, it follows from Theorem 2.10 that H_i belongs to $H^0(U_i, B_X)$. By Proposition 2.11, we have $a(f_i, f_j) = H_i + a(g_i, f_j)$ and $a(g_i, g_j) = a(g_i, f_j) + H_j$. Hence we have $a(f_i, f_j) - a(g_i, g_j) = H_i - H_j$, which implies that the Čech 1-cocycle $a(f_i, f_j) - a(g_i, g_j)$ is a 1-coboundary. Therefore $(a(f_i, f_j))_{i,j}$ and $(a(g_i, g_j))_{i,j}$ define the same element of $H^1(\mathcal{U}, B_X)$. In particular, they define the same element of $H^1(X, B_X)$. Thus we may denote the element $\beta(X, \mathcal{U}, (f_i))$ by $\beta(X, \mathcal{U})$.

It remains to show that $\beta(X, \mathcal{U})$ is independent of $\mathcal{U}$. Let $\mathcal{U} = (U_i)_{i \in I}$ and $\mathcal{V} = (V_j)_{j \in J}$ be two sufficiently refined open coverings of X. It suffices to show $\beta(X, \mathcal{U}) = \beta(X, \mathcal{V})$. First, suppose that $\mathcal{V}$ is a refinement of $\mathcal{U}$. Fix a map $\iota : J \to I$ such that $V_j \subset U_{\iota(j)}$. We choose a family $(f_i)_{i \in I}$ such that f_i is pseudo-tame on U_i. For each $j \in J$, we set $g_j = f_{\iota(j)}|_{V_j}$. Then the families $(a(f_{i_1}, f_{i_2}))_{i_1, i_2 \in I}$ and $(a(g_{j_1}, g_{j_2}))_{j_1, j_2 \in J}$ define the elements $\beta(X, \mathcal{U})$ and $\beta(X, \mathcal{V})$, respectively. Hence by the definition of $H^1(X, B_X)$, we have $\beta(X, \mathcal{U}) = \beta(X, \mathcal{V})$. In general, let us choose a common refinement $\mathcal{U}'$ of $\mathcal{U}$ and $\mathcal{V}$. Then we have $\beta(X, \mathcal{U}) = \beta(X, \mathcal{U}') = \beta(X, \mathcal{V})$ as desired. □

3.2 $\beta(X)$ as an obstruction class

Let K be a field. Recall from [Ser79, X, § 7] that K is called quasi-algebraically closed if K satisfies the following condition: if $F \in K[\mathbf{T}]$ is a homogeneous polynomial of n variables with $\deg(F) < n$, then F has a nontrivial root in $K^{\oplus n}$. Suppose that K is of transcendental degree one over an algebraically closed field. Then Tsen's theorem (cf. [Ser79, X, § 7]) states that K is quasi-algebraically closed. In particular, for any curve X, its function field is quasi-algebraically closed.

Lemma 3.4. *For any $g, a \in \mathcal{H}$, there exists $f \in \mathcal{H}$ such that*

$$a(f,g) = a \bmod k(X)^2 \in k(X)/k(X)^2.$$

Proof. Since $k(X) = k(X)^2 \oplus k(X)^2 g$, there exists a unique element $b \in k(X)$ satisfying $a \equiv b^2 g \bmod k(X)^2$. For any $f \in \mathcal{H}$, let us write f as $f = f_0^4 + f_1^4 f + f_2^4 g^2 + f_3^4 g^3$. Recall that $a(f,g)$ is defined as

$$a(f,g) = (f_1^2 f_3^2 + f_2^4)g/(f_3^4 g^2 + f_1^4) \bmod k(X)^2 \in k(X)/k(X)^2.$$

Thus it suffices to show that there exists $f_i \in k(X)$ such that

$$(f_1, f_3) \neq (0,0), \quad b = \frac{f_1 f_3 + f_2^2}{f_3^2 g + f_1^2}.$$

Set $F(T_1, T_2, T_3) = T_1 T_3 + T_2^2 + bg T_3^2 + b T_1^2 \in k(X)[T_1, T_2, T_3]$. Then F is a homogeneous quadratic polynomial in three variables with coefficients in $k(X)$. Tsen's theorem implies F has a nontrivial root in $k(X)^{\oplus 3}$. Then the root gives (f_1, f_2, f_3) as desired. □

The following theorem ensures that the cohomology class $\beta(X)$ is the obstruction class for X to admit a pseudo-tame rational function on X.

Theorem 3.5. *Let X be a curve. The following are equivalent:*

(1) $\beta(X) = 0 \in H^1(X, B_X)$;

(2) *there exists a pseudo-tame rational function on X.*

Proof. First, we prove that condition (2) implies condition (1). Let $f \in k(X)$ be a pseudo-tame rational function on X. Then $\beta(X) = 0 \in H^1(X, B_X)$ follows from $a(f,f) = 0$ (Proposition 2.9).

Next, we prove that condition (1) implies condition (2). Take a pair $(\mathcal{U} = (U_i)_{i\in I}, (f_i)_{i \in I})$ defining $\beta(X)$. Since $\beta(X) = 0 \in H^1(X, B_X)$, there exists a family $(a_i)_{i\in I}$ with $a_i \in H^0(U_i, B_X)$ satisfying $a(f_i, f_j) = a_i - a_j$. Lemma 3.4 implies that for each $i \in I$, there exists $g_i \in \mathcal{H}$ satisfying $a(f_i, g_i) = a_i$. Since a_i is regular on U_i, it follows from Theorem 2.10 that the function g_i is pseudo-tame on U_i. On the other hand, the cocycle condition shows

$$\begin{aligned} a(g_i, g_j) &= a(g_i, f_i) + a(f_i, g_j) \\ &= a_i + (a(f_i, f_j) + a(f_j, g_j)) \\ &= a_i + (a_i - a_j) + a_j \\ &= 0. \end{aligned}$$

Therefore $a(g_i, g_j)$ is clearly regular on U_j. That is, g_i is pseudo-tame on U_j. Since j is arbitrary, g_i is pseudo-tame on X. □

3.3 Vanishing of $\beta(X)$

Our next aim is to prove the following vanishing theorem for $\beta(X)$.

Theorem 3.6. *For any curve X, we have $\beta(X) = 0$.*

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

Our main tool for the proof of Theorem 3.6 is the duality of cohomology groups for the sheaf B_X. This duality follows from the duality of Raynaud's sheaf B (cf. [Ray82, § 4]) since we may identify B with B_X as follows. Since the base field k is algebraically closed (in particular, perfect), we have the canonical isomorphism of ringed spaces

$$X^{(1)} = X \times_{\mathrm{Spec}(k),\mathrm{Frob}_2} \mathrm{Spec}(k) \xrightarrow{\sim} (X, \mathcal{O}_X^2)$$

which makes the diagram

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X^{(1)} \\ \Vert & & \downarrow \cong \\ X & \xrightarrow{\iota} & (X, \mathcal{O}_X^2) \end{array}$$

commutative, where the map π is the relative Frobenius on X over k and the map ι denotes the morphism given by the identity map on the underlying space of X and the inclusion $\mathcal{O}_X^2 \hookrightarrow \mathcal{O}_X$. Via the isomorphism, we identify Raynaud's sheaf B with the $\mathcal{O}_X^2$-module B_X on X.

Raynaud [Ray82, § 4] gave a pairing

$$B \times B \to \Omega^1_{X^{(1)}/k}$$

by using the Cartier isomorphism. Under the above identification of B and B_X, the pairing

$$B_X \times B_X \to \Omega^1_{(X,\mathcal{O}_X^2)/k}$$

can be written as

$$([f],[g]) \mapsto (df/dg)\, d(g^2) \tag{3.1}$$

if $[g] \neq 0$, where $[f]$ and $[g]$ denote the classes of local sections f, g of $\mathcal{O}_X$, respectively. Here, we regard the ringed space $(X, \mathcal{O}_X^2)$ as a k-scheme via the isomorphisms

$$\Gamma(X, \mathcal{O}_X^2) \underset{\iota^*}{\xrightarrow{\cong}} \Gamma(X, \mathcal{O}_X) \xrightarrow{\cong} k,$$

where the isomorphism ι^* is induced by ι. We regard the cohomology groups $H^i(X, B_X)$ $(i = 0, 1)$ as k-vector spaces via the k-scheme structure of $(X, \mathcal{O}_X^2)$. Then the Serre duality gives a k-bilinear perfect pairing

$$(\ ,\ ) : H^0(X, B_X) \times H^1(X, B_X) \to k. \tag{3.2}$$

In order to prove the vanishing of $\beta(X)$, we give an explicit description of the pairing (3.2). For $f \in k(X)/k(X)^2$, take a representative $\widetilde{f} \in k(X)$ of f and write df for the meromorphic differential 1-form $d\widetilde{f} \in \Omega_X$. Note that df depends only on f and is independent of the choice of $\widetilde{f}$. For a nonempty open subset $U \subset X$, we have

$$H^0(U, B_X) = \{f \in k(X)/k(X)^2 \mid df \in \Omega_X \text{ is regular on } U\}.$$

Let $X = U \cup V$ be an affine open covering. The Mayer–Vietoris exact sequence

$$H^0(U, B_X) \oplus H^0(V, B_X) \to H^0(U \cap V, B_X) \to H^1(X, B_X) \to 0$$

gives the surjection

$$H^0(U \cap V, B_X) \to H^1(X, B_X)$$

which we denote by $\Psi_{B_X,U,V}$.

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

Then the pairing (3.2) can be explicitly written as follows. Take any $f \in H^0(X, B_X)$ and $\alpha \in H^1(X, B_X)$. Given an affine open covering $X = U \cup V$, we write $\alpha = \Psi_{B_X,U,V}(g)$ for some $g \in H^0(U \cap V, B_X)$. Let us take representatives $\widetilde{f}$, $\widetilde{g} \in k(X)$ of $f, g \in k(X)/k(X)^2$. We may assume $f \neq 0$. Then we have $g_0, g_1 \in k(X)$ such that $\widetilde{g} = g_0^2 + g_1^2 \widetilde{f}$. By (3.1), we have

$$(f, \alpha) = \left(\sum_{x \in X \setminus U} \mathrm{Res}_x(g_1 \, d\widetilde{f}) \right)^2.$$

Here $\mathrm{Res}_x(g_1 \, d\widetilde{f})$ is the residue of $g_1 \, d\widetilde{f} \in \Omega_x$ at a closed point x.

We are now ready to prove Theorem 3.6.

Proof of Theorem 3.6. Let X be a curve. It suffices to show that $(f, \beta(X)) = 0 \in k$ for any $f \in H^0(X, B_X)$. We can assume that $f \neq 0 \in k(X)/k(X)^2$. Take a representative $\widetilde{f} \in k(X)$ of f. Let S be the set of closed points of X at which $\widetilde{f}$ is not tame. Then there exists $g \in k(X)$ such that $g^2 + \widetilde{f}$ is tame on S. Let T be the set of closed points of X at which $g^2 + \widetilde{f}$ is not tame and we set $U = X \setminus S$, $V = X \setminus T$. By definition of $\beta(X)$, we have $\beta(X) = \Psi_{B_X,U,V}(a)$ for $a = a(\widetilde{f}, g^2 + \widetilde{f}) \in H^0(U \cap V, B_X)$. Recall that we have

$$a = \left(\frac{dg}{d\widetilde{f}} \right)^2 \widetilde{f} \bmod k(X)^2.$$

Then we have

$$(f, \beta(X)) = \left(\sum_{x \in S} \mathrm{Res}_x \left(\left(\frac{dg}{d\widetilde{f}} \right) \cdot d\widetilde{f} \right) \right)^2.$$

Since $\mathrm{Res}_x((dg/d\widetilde{f}) \cdot d\widetilde{f}) = \mathrm{Res}_x(dg) = 0$ at any closed point $x \in X$, we have $(f, \beta(X)) = 0$. □

Thus we conclude that we have a pseudo-tame rational function for any curve.

Corollary 3.7. *For any curve X, there exists a rational function $f \in \mathcal{H}$ which is pseudo-tame on X.*

Remark 3.8. We remark that the set of Γ-orbits of pseudo-tame rational functions on X has the following $H^0(X, B_X)$-torsor structure: if S is the Γ-orbit of a pseudo-tame rational function $f \in k(X)$ and $a \in H^0(X, B_X)$, then $a \cdot S$ is the set of $g \in H$ satisfying $a(f, g) = a$. It follows from Lemma 3.4 that this set is nonempty and it follows from Proposition 2.9 that it consists of a single Γ-orbit. The cocycle condition in Proposition 2.11 implies that $a \cdot (b \cdot S) = (a + b) \cdot S$ for any $a, b \in H^0(X, B_X)$.

In particular, if the Jacobian of X is ordinary, then the pseudo-tame rational functions on X form a single Γ-orbit.

4. Existence of a tamely ramified rational function

In the previous section we proved the existence of a pseudo-tame rational function on any curve. The aim of this section is to prove Theorem 4.1, which states that any Γ-orbit of a pseudo-tame rational function contains a tamely ramified rational function. Our main idea of the proof of Theorem 4.1 is to consider the cube f^3 of a certain pseudo-tame rational function f on X instead of f itself.

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

We fix and recall some notation. For a curve X over k, we identify the rational functions on X with the morphisms from X to the projective line $\mathbb{P}^1_k$ over k. We say that a rational function on X is tamely ramified if it is, as a morphism from X to $\mathbb{P}^1_k$, at most tamely ramified at every closed point of X. With this notation, our main result can be stated as follows.

Theorem 4.1. *Let X be a curve. Let us fix a closed point $x \in X$ and set $A = \Gamma(X\backslash\{x\}, \mathcal{O}_X)$. Let f_0 be a pseudo-tame rational function on X. Then there exists an element $\gamma \in \Gamma = \mathrm{PGL}_2(k(X)^4)$ such that $f = \gamma f_0 \in A$ and that f is a tamely ramified rational function.*

We give a proof of the theorem at the end of this section. Let g denote the genus of X. For an element $f \in k(X)$, we denote the order of pole at x by $\deg(f)$, that is, $\deg(f) = -\mathrm{ord}_x(f)$.

Lemma 4.2. *For a nonzero ideal $I \subset A$, we set $d = \dim_k A/I$. Then, for any integer n with $n \geqslant 2g + d$, there exists an element $f \in I$ such that $\deg(f) = n$.*

Proof. Let D be the effective divisor on $\mathrm{Spec}(A) = X\backslash\{x\}$ associated with the ideal I. Then we have $\deg(D) = d$. The Riemann–Roch theorem implies

$$\dim_k H^0(X, \mathcal{O}(nx - D)) = n - d + 1 - g$$

and

$$\dim_k H^0(X, \mathcal{O}((n-1)x - D)) = n - d - g.$$

In particular, we have an inequality

$$\dim_k H^0(X, \mathcal{O}(nx - D)) > \dim_k H^0(X, \mathcal{O}((n-1)x - D)).$$

Thus there exists $f \in k(X)^\times$ such that $\mathrm{div}(f) + nx - D$ is effective and that $\mathrm{div}(f) + (n-1)x - D$ is not effective. Then the element f satisfies the desired condition. □

Lemma 4.3. *For an element $f \in A$, we assume that f is pseudo-tame at x and that the order of the differential df at x satisfies $-\mathrm{ord}_x(df) \geqslant 8g$. Then there exists $h \in A$ such that $\deg(f + h^4) = -\mathrm{ord}_x(df) - 1$.*

Proof. We define an integer e by $2e = -\mathrm{ord}_x(df)$. Then we prove the lemma by induction on $\deg(f) - 2e$. If $\deg(f) - 2e < 0$ then we can take $h = 0$. Otherwise, let us define an integer d by $4d = \deg(f)$. By assumption, we have an inequality $d \geqslant 2g$. Thus Lemma 4.2 implies that there exists an element $h_0 \in A$ with $\deg(h_0) = d$. Then for some $a \in k$, we have $\deg(f + (ah_0)^4) < 4d$. By the induction hypothesis, we can take $h_1 \in A$ with $\deg(f + (ah_0)^4 + h_1^4) = 2e - 1$, that is, $h = ah_0 + h_1$ is the desired element. □

Lemma 4.4. *For a nonzero ideal $I \subset A$, we set $d = \dim_k A/I$. Then, for any $a \in A$, there exists $f \in A$ satisfying $f \equiv a \bmod I$ and $\deg(f) < d + 2g$.*

Proof. Let $f \in A$ be a representative of $(a \bmod I) \in A/I$ such that $\deg(f) \leqslant \deg(f_1)$ for any other representative $f_1 \in A$ of $(a \bmod I)$. Then the element $f \in A$ satisfies $\deg(f) < d + 2g$. In fact, suppose $\deg(f) \geqslant d + 2g$. Then Lemma 4.2 gives us an element $h \in I$ with $\deg(h) = \deg(f)$. Then there exists $b \in k$ such that $\deg(f + bh) < \deg(f)$ and $f + bh \equiv a \bmod I$. This contradicts the minimality of $\deg(f)$. □

Lemma 4.5. *Let f_0 be a pseudo-tame rational function on X and r a positive integer with $r \geqslant 8g - 1$. Then there exists an element $\gamma \in \Gamma$ such that $f = \gamma f_0$ satisfies the following conditions:*

(1) *$f = \gamma f_0 \in A$;*
(2) *$\deg(f)$ is odd and $\deg(f) \geqslant r$;*
(3) *any zero of f is simple.*

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

Proof. Let us write $f_0 = h_0/h_1$ for some $h_0, h_1 \in A$. Then $f_1 = h_1^4 f_0 = h_1^3 h_0 \in A$ is a pseudo-tame rational function on X. Take $h_2 \in A$ satisfying $-\mathrm{ord}_x(df_1) + 4\deg(h_2) \geqslant r+1$ and set $f_2 = h_2^4 f_1$, $2e = -\mathrm{ord}_x(df_2)$. Since we have $2e \geqslant r+1 \geqslant 8g$, Lemma 4.3 implies that we can take $h_3 \in A$ with $\deg(f_2 + h_3^4) = 2e - 1 \geqslant r$. Then $f_3 = f_2 + h_3^4 \in A$ is a pseudo-tame rational function satisfying condition (2). Finally, by adding some constant to f_3, we obtain a rational function f satisfying the desired properties. □

Finally, we are ready to prove our main result.

Proof of Theorem 4.1. Fix a pseudo-tame rational function $f \in A$ in the Γ-orbit of f_0 as in Lemma 4.5 with $r = \max(12g - 2, 0)$ and set $2e - 1 = \deg(f)$. Let us denote by Z the set of the zeros of df. For each $z \in Z$, set $2m_z = \mathrm{ord}_z(df)$. Since $\deg(\mathrm{div}(df)) = 2g - 2$, we have $\sum_{z\in Z} m_z = e + g - 1$. Let $I \subset A$ be an ideal associated with the effective divisor

$$\sum_{\substack{z\in Z,\\ m_z>1}} (\lfloor m_z/2 \rfloor + 1)z$$

on $\mathrm{Spec}(A) = X\backslash\{x\}$. Then we have an inequality $\dim_k(A/I) \leqslant e + g - 1$. We note that condition (2) of Lemma 4.5 implies that $f(z) \neq 0$ for any $z \in Z$. In particular, we have $\mathrm{ord}_z(d(f^3)) = 2m_z$ for any $z \in Z$. Thus there exists an element $a \in A$ such that for any $h \in A$ with $h \equiv a \bmod I$, $f^3 + h^4$ is tame at any $z \in Z$.

Let us fix such $a \in A$. Then Lemma 4.4 implies that there exists an element $h \in A$ with $h \equiv a \bmod I$ and $\deg(h) < 2g + (e+g-1)$. We note that $f^3 + h^4$ is tame at any $z \in Z$. Now let us check that $f^3 + h^4$ is tame at x. By our assumption, we have $2e - 1 \geqslant 12g - 2$. Since this inequality implies $8g + 4(e + g - 1) \leqslant 3(2e - 1)$, we obtain $4\deg(h) < 3\deg(f)$. Thus $f^3 + h^4$ is tame at x. Finally, we prove that $f^3 + h^4$ is tame outside of $Z \cup \{x\}$. The equation $d(f^3 + h^4) = f^2 df$ and condition (2) in Lemma 4.5 imply that $0 \leqslant \mathrm{ord}_y(d(f^3 + h^4)) \leqslant 2$ for any $y \notin Z \cup \{x\}$. Since $f^3 + h^4$ is everywhere pseudo-tame, the inequality implies that $f^3 + h^4$ is tame at $y \notin Z \cup \{x\}$. Thus we conclude that $f^3 + h^4$ is a tamely ramified rational function on X. □

Proof of Theorem 1.2. The assertion follows from [Ful69] if the characteristic of k is not equal to 2. When k is of characteristic two, the assertion follows from Corollary 3.7 and Theorem 4.1. □

5. An upper bound of the minimum degree

THEOREM 5.1. *Let X be a curve of genus $g \geqslant 1$, and let $x \in X$ be a closed point. Let $A = \Gamma(X\backslash\{x\}, \mathcal{O}_X)$. Then there exists an element $f \in A$ such that $\deg(f) \leqslant 48g^2 + 22g - 1$ and that f is a pseudo-tame function on X.*

Proof. By Lemma 4.2, we can choose two elements $f, t \in A$ with $\deg(f) = 2g+1$ and $\deg(t) = 2g$. By adding to t a suitable element of smaller degree if necessary, we may assume that $k(X)$ is a separable extension of $k(t)$. Let Z be the set of zeros of df. For $z \in Z$, set $2m_z = \mathrm{ord}_z(df)$. Let I denote the ideal of A associated with the effective divisor $\sum_{z\in Z}(m_z + 1)z$. Then there exists an element $a \in A$ such that for any $h \in A$ with $h \equiv a \bmod I$, $f + h^2$ is tame at any $z \in Z$. The argument in the proof of Theorem 4.1 shows that $\dim_k(A/I) \leqslant 4g$. Hence it follows from Lemma 4.4 that there exists $h \in A$ with $\deg(h) < 6g$ such that $f' = f + h^2$ is tame on $U = X\backslash\{x\}$. Set $V = X\backslash Z$. It follows from the definition that $\beta(X)$ is equal to the image of $a(f, f') \in H^0(U \cap V, B_X)$ under the map $\Psi_{B_X,U,V}$ in § 3.3. Since $\beta(X) = 0$, there exists an

https://doi.org/10.1112/S0010437X19007723 Published online by Cambridge University Press

element $a \in H^0(U, B_X) = A/A^2$ such that $a + a(f, f')$ is regular at x. Choose a unique $b \in k(X)$ satisfying $a = b^2 f \bmod k(X)^2$ and let us consider the polynomial $F(T_1, T_2, T_3) = T_1T_3 + T_2^2 + bfT_3^2 + bT_1^2$. Then the argument in the proof of Lemma 3.4 and Theorem 3.5 shows that, for any nontrivial solution $(g_1, g_2, g_3) \in A^3$ of $F(T_1, T_2, T_3) = 0$, the element $g_1^4 f + g_2^4 f^2 + g_3^4 f^3 \in A$ is a pseudo-tame rational function on X.

Observe that $a(f, f') = (dh/df)^2 f \bmod k(X)^2$ and that $\deg(dh/df) \leqslant 4g - 1$. The latter implies $\deg((dh/df)^2 f) \leqslant 10g - 1$. Since $10g - 1 \geqslant 4g$, it follows from Lemma 4.2 that there exists a lift $\widetilde{a} \in A$ of a satisfying $\deg(\widetilde{a}) \leqslant 10g - 1$. Observe that $b^2 = d\widetilde{a}/df$. This implies $\deg(b) \leqslant 4g - 1$. Since $\sum_{z \in Z} m_z = 2g$, it follows from Lemma 4.2 that there exists a nonzero $c \in A$ with $\deg(c) \leqslant 4g$ satisfying $bc \in A$. Then we have $\deg(bc) \leqslant 8g - 1$. Hence $cF(T_1, T_2, T_3)$ is a homogeneous quadratic polynomial with coefficients in A and the degree of each coefficient is at most $10g$.

Note that, for any nonzero $\phi \in k[t]$ and $i \in \{0, 1, \ldots, 2g - 1\}$, the degree of ϕf^i is congruent to i modulo $2g$. This implies that $1, f, \ldots, f^{2g-1}$ are linearly independent over $k[t]$. Let L be the Galois closure of $k(X)$ over $k(t)$ in a separable closure of $k(X)$, and let us consider the polynomial

$$G = \prod_{\sigma} \sigma(F)\left(\sum_{i=0}^{2g-1} \sigma(f)^i S_{1,i}, \sum_{i=0}^{2g-1} \sigma(f)^i S_{2,i}, \sum_{i=0}^{2g-1} \sigma(f)^i S_{3,i}\right),$$

where σ runs over the element of $\mathrm{Gal}(L/k(t))/\mathrm{Gal}(L/k(X))$, in variables $S_{1,i}$, $S_{2,i}$, $S_{3,i}$ ($i \in \{0, 1, \ldots, 2g-1\}$). Then G is a homogeneous polynomial of degree $4g$ in $6g$ variables, and the coefficients of G are polynomials in $k[t]$ whose degrees are at most $2(2g - 1)\deg f + 10g = 8g^2 + 10g - 2$. Hence the argument in the proof of Tsen's theorem (cf. [Sha10, ch. 1, 6.2, Corollary 1.11]) shows that there exists a nontrivial solution of $G = 0$ in $k[t]^{6g}$ whose all entries are polynomials in t of degree at most $4g + 2$. Since $1, f, \ldots, f^{2g-1}$ is linearly independent over $k[t]$, this shows that there exists a nontrivial solution $(g_1, g_2, g_3) \in A^3$ of $F(T_1, T_2, T_3) = 0$ satisfying $\deg(g_i) \leqslant (2g - 1)\deg(f) + (4g + 2)\deg(t) = 12g^2 + 4g - 1$. Thus we may find a pseudo-tame rational function $g' = g_1^4 f + g_2^4 f^2 + g_3^4 f^3 \in A$ on X of degree at most $4(12g^2 + 4g - 1) + 3\deg(f) = 48g^2 + 22g - 1$, as desired. □

Corollary 5.2. *Let X, x, and A be as in Theorem 5.1. Then there exists an element $f \in A$ such that $\deg(f) \leqslant 144g^2 + 66g - 3$ and that f is a tamely ramified rational function on X.*

Proof. By Theorem 5.1, we can take $f \in A$ such that $\deg(f) \leqslant 48g^2 + 22g - 1$ and that f is a pseudo-tame function on X. By replacing f with fh^4 for some suitable $h \in A$ with $\deg(h) = 3g$ if $-\mathrm{ord}_x(df) < 8g$, and then by applying Lemma 4.3, we obtain an element $f' \in A$ such that $\deg(f')$ is odd with $12g < \deg(f') \leqslant 48g^2 + 22g - 1$ and that f' is a pseudo-tame function on X. Then the argument of the proof of Lemma 4.5 and Theorem 4.1 shows that a function of the form $(f' + c)^3 + h'^4$ for some $c \in k$ and $h' \in A$ with $4\deg(h') < 3\deg(f')$ is a tamely ramified rational function on X, which proves the assertion. □

Acknowledgements

The authors thank Akio Tamagawa for discussions concerning this article. They would especially like to thank Jaap Top and Roos Westerbeek for their careful reading of the manuscript and for kindly pointing out a mistake in the proof of Theorem 4.1 in an earlier version of the paper. They also thank Jaap Top for informing them that Seher Tutdere and Nurdagül Anbar have obtained a different proof to correct the mistake mentioned above in an earlier version of the manuscript.

They thank the anonymous referee for giving many beneficial comments, especially those for improving the presentation of this paper. The authors are grateful to Benjamin Bailey and Satoshi Kondo for their various comments and suggestions to make clearer the presentation of the paper. During this research, the second author was supported by JSPS KAKENHI Grant number JP15H03610.

References

AT18 N. Anbar and S. Tutdere, *On Belyi's theorems in positive characteristic*, Preprint (2018), arXiv:1811.00773.

Bel79 G. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), 267–276.

Ful69 W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. of Math. (2) **90** (1969), 542–575.

Har77 R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52 (Springer, Berlin, 1977).

Hos17 Y. Hoshi, *Frobenius-projective structures on curves in positive characteristic*, Preprint (2017), available online at http://www.kurims.kyoto-u.ac.jp/preprint/file/RIMS1871.pdf.

Ray82 M. Raynaud, *Sections des fibres vectoriels sur une courbe*, Bull. Soc. Math. France **110** (1982), 103–125.

Saï97 M. Saïdi, *Revêtements modérés et groupe fondamental de graphe de groupes*, Compos. Math. **107** (1997), 319–338.

Ser79 J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67 (Springer, Berlin, 1979).

Sha10 I. R. Shafarevich, *Basic algebraic geometry 1*, third edition (Springer, Berlin, 2010).

Yusuke Sugiyama u.sugiyama.0811@gmail.com
Department of Mathematics, Graduate School of Science, Osaka University,
1-1 Machikaneyama Toyonaka, Osaka 560-0043, Japan

Seidai Yasuda s-yasuda@math.sci.osaka-u.ac.jp
Department of Mathematics, Graduate School of Science, Osaka University,
1-1 Machikaneyama Toyonaka, Osaka 560-0043, Japan