On Belyi's Theorems in positive characteristic

Nurdagül ANBAR
Johannes Kepler University, Altenberger St. 69, 4040, Linz, Austria
nurdagulanbar2@gmail.com

Seher TUTDERE
Department of Mathematics, Gebze Technical University, Gebze, Kocaeli, Turkey
stutdere@gmail.com

Abstract

There are two types of Belyi's Theorem for curves defined over finite fields of characteristic p, namely the Wild and Tame p-Belyi Theorems. In this paper, we discuss them in the language of function fields. We provide a self-contained proof for the Wild p-Belyi Theorem for any prime p, and Tame 2-Belyi Theorem.

Keywords: Belyi's Theorems, function field, finite field, tame and wild ramification, pseudo-tame.
Mathematics Subject Classification(2010): 11R58, 11G32, 14H05.

1 Introduction

Let $\mathcal{X}$ be a connected, smooth, projective curve defined over the field of algebraic numbers $\bar{\mathbb{Q}}$. The main theorem of Belyi states that there exists a morphism f from $\mathcal{X}$ to the projective line $\mathbb{P}^1$ such that the branch points of f lie in the set $\{0, 1, \infty\}$. The morphism f satisfying this property is called a *Belyi map* for $\mathcal{X}$. Belyi gave two elementary proofs for his theorem, see [1, 2]. In fact, the converse of the statement also holds, and was known before Belyi's result [13]. In other words, $\mathcal{X}$ is a curve defined over $\bar{\mathbb{Q}}$ if and only if there exists a morphism $f : \mathcal{X} \mapsto \mathbb{P}^1$ whose branch points of f lie in the set $\{0, 1, \infty\}$. However, the connection with different areas of mathematics, such as the arithmetic and modularity of elliptic curves, ABC conjecture and moduli spaces of pointed curves, makes Belyi's statement more interesting, for details see the excellent paper [5] and references therein.

In this paper we investigate Belyi's Theorem in positive characteristic p. We denote by $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime p, and by $\bar{\mathbb{F}}_p$ the algebraic closure of $\mathbb{F}_q$. The dichotomy of wild and tame ramification in positive characteristic leads to two types of Belyi's Theorem as follows:

Theorem 1 (Wild p-Belyi Theorem)**.** *Let $\mathcal{X}$ be a connected, smooth, projective curve defined over $\mathbb{F}_q$. Then there exists a morphism $\phi : \mathcal{X} \to \mathbb{P}^1$ admitting at most one branch point.*

Theorem 2 (Tame p-Belyi Theorem)**.** *Let $\mathcal{X}$ be a connected, smooth, projective curve defined over $\bar{\mathbb{F}}_p$. Then there exists a tamely ramified morphism $\phi : \mathcal{X} \to \mathbb{P}^1$ admitting at most three branch points.*

To the best of our knowledge, a first proof of Theorem 2 for odd characteristic is given in [12]. Moreover, in [5], the proofs of Theorem 1 for any positive characteristic and Theorem 2 for odd characteristic are given by using the results of [9, 14] and [4], respectively. The conjecture of the Tame p-Belyi Theorem for even characteristic has been recently proved in [8].

It is a well-known fact that the theory of algebraic curves and the theory of algebraic function fields are equivalent [6, 10]. As a consequence of this equivalence, we here discuss Belyi's theorems in positive characteristic in the language of function fields. In fact, this significantly simplifies the proof of the Tame 2-Belyi Theorem given in [8].

The paper is organized as follows. In Section 2 we fix notations and give some basic facts regarding function fields. In Section 3 we give a self-contained proof for the Wild p-Belyi Theorem. In Section 4 we discuss the Tame p-Belyi Theorem. In particular, for $p > 2$ we give the Tame p-Belyi Theorem by using the result [4] and give a self contained proof of the Tame 2-Belyi Theorem.

2 Preliminaries

For the notations and well-known facts, as a general reference, we refer to [7, 11]. Let F be a function field over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ or $\mathbb{F} = \bar{\mathbb{F}}_p$, and let F'/F be a finite separable extension of function fields. We write $P'|P$ for a place P' of F' lying over a place P of F, and denote by $e(P'|P)$ the ramification index of $P'|P$. Recall that when the ramification index $e(P'|P) > 1$, it is said that $P'|P$ is ramified. Moreover, if the characteristic p does not divide $e(P'|P)$ it is called *tamely* ramified; otherwise it is called *wildly* ramified. We call F'/F a tame extension if there is no wild ramification. For a rational function field $\mathbb{F}(y)$ and $\alpha \in \mathbb{F}$, we denote by $(y = \alpha)$ and $(y = \infty)$ the places corresponding to the zero and the pole of $y - \alpha$, respectively.

We can state Belyi's theorems given in Theorems 1 and 2 in the language of function fields as follows:

Theorem 3 (Wild p-Belyi Theorem)**.** *Let F be a function field over $\mathbb{F}_q$. Then there exists a rational subfield $\mathbb{F}_q(y)$ of F such that there exists at most one ramified place of $\mathbb{F}_q(y)$, namely $(y = \infty)$, in $F/\mathbb{F}_q(y)$.*

Theorem 4 (Tame p-Belyi Theorem)**.** *Let F be a function field over $\bar{\mathbb{F}}_p$. Then there exists a rational subfield $\bar{\mathbb{F}}_p(y)$ of F such that $F/\bar{\mathbb{F}}_p(y)$ is a tame extension, and there exist at most three ramified places of $\bar{\mathbb{F}}_p(y)$ in $F/\bar{\mathbb{F}}_p(y)$ lying in the set $\{(y = 0), (y = 1), (y = \infty)\}$.*

For the convenience of reader, we now fix some notations. We denote by

$\mathbb{P}_F$	the set of all places of $F/\mathbb{F}$,
$[F' : F]$	the extension degree of F'/F,
$f(P'\|P)$	the relative degree of $P'\|P$,
$d(P'\|P)$	the different exponent of $P'\|P$,
v_P	the valuation of F associated to the place P,

$(z)_\infty$ (resp. $(z)_0$) the pole divisor (resp. the zero divisor) of a nonzero element $z \in F$,

$\mathcal{L}(A)$ the Riemann-Roch space associated to a divisor A,

$\ell(A)$ the $\mathbb{F}$-dimension of $\mathcal{L}(A)$,

supp(A) the support of A, i.e., the set of places $P \in \mathbb{P}_F$ for which $v_P(A) \neq 0$.

Dedekind's Different Theorem [11, Theorem 3.5.1] states that $d(P'|P) \geq e(P'|P) - 1$, and the equality holds if and only if $P'|P$ is tame. Furthermore, $P'|P$ is ramified if and only if $d(P'|P) > 0$. By the Fundamental Equality [11, Theorem 3.1.11], we have $\sum e(P'|P) f(P'|P) = [F' : F]$, where P' ranges over the places of F' lying over P.

The Strong Approximation Theorem [11, Theorem 1.6.5] is one of the main tool for the Tame 2-Belyi Theorem, and hence we state it for the sake of the reader.

Lemma 1. *Let $S \subset \mathbb{P}_F$ be a proper subset, and $P_1, \dots P_r \in S$. For given $x_1, \dots x_r \in F$ and $n_1, \dots, n_r \in \mathbb{Z}$, there exists $x \in F$ such that*

$$v_{P_i}(x - x_i) = n_i \ \text{ for } i = 1, \dots r, \quad \text{ and } \quad v_P(x) \geq 0 \ \text{ for all } P \in S \setminus \{P_1, \dots P_r\} \ .$$

Corollary 1. *Let $D = \sum n_i P_i$, $n_i \geq 0$, be a positive divisor. Then the Strong Approximation Theorem implies the existence of $x \in F$ with $D \leq (x)_0$ and $(x)_\infty = nP$ for some place $P \notin \operatorname{supp}(D)$ and $n \in \mathbb{N}$.*

In fact, we obtain a stronger conclusion by using the Riemann-Roch Theorem [11, Theorem 1.5.15].

Lemma 2. *Let $D = \sum n_i P_i$, $n_i \geq 0$, a divisor of degree d. Then for any $n \geq 2g + d$ there exists $x \in F$ with $D \leq (x)_0$ and $(x)_\infty = nP$ for some place $P \notin \operatorname{supp}(D)$.*

Proof. Consider the Riemann-Roch spaces $\mathcal{L}(nP - D)$ and $\mathcal{L}((n-1)P - D)$. Since $n \geq 2g + d$, by the Riemann-Roch Theorem we have $\ell(nP - D) > \ell((n-1)P - D)$. Therefore, there exists $x \in \mathcal{L}(nP - D) \setminus \mathcal{L}((n-1)P - D)$, which is an element with desired properties. □

2.1 Ramification in the rational function field extensions

Let $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ be the rational function field extension given by the equation $t = \frac{g(x)}{h(x)}$ for some relatively prime polynomials $g(T), h(T) \in \mathbb{F}_q[T]$ such that not both g, h lie in $\mathbb{F}_q[T^p]$. Without loss of generality, we assume that $\deg(g) > \deg(h)$; otherwise we consider the extension $\mathbb{F}_q(x)/\mathbb{F}_q(1/(t+\alpha))$ for some proper $\alpha \in \mathbb{F}_q$. Let P be a place of $\mathbb{F}_q(x)$ of degree r, which is not the pole of x or a zero of $h(x)$. Consider the constant field extensions $\mathbb{F}_q(t)F_{q^r} \subseteq \mathbb{F}_q(x)\mathbb{F}_{q^r}$, see Figure 1. We have $[\mathbb{F}_q(x)\mathbb{F}_{q^r} : \mathbb{F}_q(x)] = [\mathbb{F}_q(t)\mathbb{F}_{q^r} : \mathbb{F}_q(t)] = r$ and the extension $\mathbb{F}_q(x)\mathbb{F}_{q^r}/\mathbb{F}_q(t)\mathbb{F}_{q^r}$ is defined by the same equation $t = \frac{g(x)}{h(x)}$. Note that any place $P' \in \mathbb{P}_{\mathbb{F}_q(x)F_{q^r}}$ lying over P is of degree one, i.e., $P' = (x = \alpha)$ for some $\alpha \in \mathbb{F}_{q^r}$. We set $Q' := P' \cap \mathbb{F}_q(t)\mathbb{F}_{q^r}$ and $Q := P' \cap \mathbb{F}_q(t)$. Then $Q' = (t = \beta)$, where $\beta = g(\alpha)/h(\alpha)$. Since there is no ramification in a constant field extension [11, Theorem

3.6.3], by the transitivity of ramification indices, we have $e(P|Q) = e(P'|Q')$. Write $g(T) - \beta h(T) = (T - \alpha)^m r(T)$ for some positive integer m and $r \in \mathbb{F}[T]$ such that $r(\alpha) \neq 0$. We then have

$$e(P'|Q') = v_{P'}(t - \beta) = v_{P'}(g(x) - \beta h(x)) = m \ . \tag{2.1}$$

In particular, Equation (2.1) implies that $P|Q$ is ramified if and only if $g(T) - \beta h(T)$ has multiple roots. Note that any zero of $h(x)$ is a pole of t. Let $h(T) = \prod p_i(T)^{e_{p_i}}$ be the factorization of $h(T)$ in $\mathbb{F}_q[T]$, where $p_i(T)$'s are distinct irreducible polynomials and $e_{p_i} \geq 1$. We denote by P_i the place of $\mathbb{F}_q(x)$ corresponding to $p_i(x)$. Then the conorm of $(t = \infty)$ with respect to $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is given by

$$\mathrm{Con}_{\mathbb{F}_q(x)/\mathbb{F}_q(t)}\left((t = \infty)\right) = e((x = \infty)|(t = \infty))(x = \infty) + \sum e(P_i|(t = \infty))P_i \ .$$

with

$$e((x = \infty)|(t = \infty)) = \deg(g(T)) - \deg(h(T)) \quad \text{and} \quad e(P_i|(t = \infty)) = e_{p_i} \ .$$

$$\begin{tikzcd}
 & \mathbb{F}_q(x)\mathbb{F}_{q^r} \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{F}_q(t)\mathbb{F}_{q^r} \arrow[d, dash] & \mathbb{F}_q(x) \arrow[dl, dash] \\
\mathbb{F}_q(t) &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & P' \arrow[dl, dash] \arrow[d, dash, "e(P'|P)=1"] \\
Q' \arrow[d, dash, "e(Q'|Q)=1"'] & P \arrow[dl, dash] \\
Q &
\end{tikzcd}$$

Figure 1: Constant field extensions of rational function fields

We finish this section with the following lemma, which is required for the proofs of both p-Belyi theorems in the subsequent sections.

Lemma 3. *Let $\mathbb{F}_q(x)$ be a rational function field, and let $S = \{P_1, \cdots, P_n\}$ be a finite set of places of $\mathbb{F}_q(x)$ with $P_i \notin \{(x = 0), (x = \infty)\}$ for all $i = 1, \cdots, n$. Then there exists a subfield $\mathbb{F}_q(t)$ of $\mathbb{F}_q(x)$ with the following properties:*

(i) The extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is tame,

(ii) P_i lies over $(t = 0)$ for all $i = 1, \cdots, n$, and

(iii) $(t = 1)$ and $(t = \infty)$ are the only ramified places of $\mathbb{F}_q(t)$ in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$.

Proof. We denote by r_i the degree of P_i for $i = 1, \cdots, n$, and set $r := \mathrm{lcm}(r_1, \cdots, r_n)$, where lcm is the least common multiple. Consider the subfield $\mathbb{F}_q(t)$ of $\mathbb{F}_q(x)$ given by the equation $t = 1 - x^{q^r - 1}$. Then $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is an extension of degree $q^r - 1$. Since r is divisible by the degree of P_i, by above discussion on ramification in the rational function fields extension, all the places P_i's lie over $(t = 0)$. Furthermore, $(x = \infty)$ and $(x = 0)$ are the only places lying over $(t = \infty)$ and $(t = 1)$, respectively, with ramification indices $e((x = \infty)|(t = \infty)) = e((x = 0)|(t = 1)) = q^r - 1$ (see Figure 2). As the polynomial $T^{q^r - 1} + \beta$ has no multiple roots for any nonzero $\beta \in \bar{\mathbb{F}}_p$, these is no other ramification. In particular, $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is a tame extension.

$\square$

$$\begin{tikzcd}
\mathbb{F}_q(x) \arrow[d, dash] & P_1 \arrow[dr, dash, "e=1"] & \cdots\cdots & P_n \arrow[dl, dash, "e=1"] & (x=\infty) \arrow[d, dash, "e=q^r-1"] & (x=0) \arrow[d, dash, "e=q^r-1"] \\
\mathbb{F}_q(t) & & (t=0) & & (t=\infty) & (t=1)
\end{tikzcd}$$

Figure 2: Ramification structure in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$

3 The Wild p-Belyi Theorem

In this section, we give a self-contained proof for the Wild p-Belyi Theorem for any positive characteristic p.

Proof of Theorem 3. Let $x \in F$ be a separating element. Then there exist finitely many ramified places of $\mathbb{F}_q(x)$ in $F/\mathbb{F}_q(x)$. Assume that the ramified places lie in the set $S = \{(x=0), (x=\infty), P_1, \cdots, P_n\} \subset \mathbb{P}_{\mathbb{F}_q(x)}$ for some $n \geq 1$. By Lemma 3, we can find an element $t \in \mathbb{F}_q(x) \subseteq F$ such that all the ramified places of F in $F/\mathbb{F}_q(t)$ lie over the set $\{(t=0), (t=1), (t=\infty)\}$.

We first consider the extension $\mathbb{F}_q(t)/\mathbb{F}_q(u)$ given by the equation $u = \frac{t^{p+1}+1}{t}$. The places $(t=0)$ and $(t=\infty)$ lie over $(u=\infty)$ with ramification indices $e((t=0)|(u=\infty)) = 1$ and $e((t=\infty)|(u=\infty)) = p$ (see Figure 3). Hence, by the Fundamental Equality $(t=0)$ and $(t=\infty)$ are the only places lying over $(u=\infty)$. We have seen in Subsection 2.1 that there is no other ramification in $\mathbb{F}_q(t)/\mathbb{F}_q(u)$ if $f_\beta(T) = T^{p+1} - \beta T + 1$ is a polynomial without multiple root for all $\beta \in \bar{\mathbb{F}}_p$. Suppose that α is a multiple root of $f_\beta(T)$ for some $\beta \in \bar{\mathbb{F}}_p$. Then α is also a root of $f'_\beta(T) = T^p - \beta$, and hence α is a p-th root of β. However, this means that $f_\beta(\alpha) = 1$, which gives a contradiction. Moreover, the place $(t=1)$ lies over $(u=2)$. (Note that this is $(u=0)$ in characteristic 2.)

Next, we consider the extension $\mathbb{F}_q(u)/\mathbb{F}_q(y)$ given by the equation $y = \frac{(u-2)^{p+1}+1}{u-2}$. Similarly, we can show that the places $(u=\infty)$ and $(u=2)$ are all places lying over $(y=\infty)$, and the ramification occurs only at $(y=\infty)$. Consequently, $(y=\infty)$ is the only ramified place in the extension $F/\mathbb{F}_q(y)$.

$$\begin{tikzcd}
\mathbb{F}_q(t) \arrow[d, dash, "u=\frac{t^{p+1}+1}{t}"'] \\
\mathbb{F}_q(u) \arrow[d, dash, "y=\frac{(u-2)^{p+1}+1}{u-2}"'] \\
\mathbb{F}_q(y)
\end{tikzcd}
\qquad
\begin{tikzcd}
(t=0) \arrow[d, dash, "e=1"'] & (t=\infty) \arrow[dl, dash, "e=p"] & (t=1) \arrow[d, dash, "e=1"] \\
(u=\infty) \arrow[dr, dash, "e=p"] & & (u=2) \arrow[dl, dash, "e=1"] \\
& (y=\infty) &
\end{tikzcd}$$

Figure 3: The Wild p-Belyi Theorem

□

Remark 1. We note that in the proof of Theorem 3 the ramified places in $\mathbb{F}_q(t)/\mathbb{F}_q(u)$ and $\mathbb{F}_q(u)/\mathbb{F}_q(y)$ have ramification indices p, i.e., they are wild, see Figure 3. It follows from the Hurwitz Genus Formula [11, Theorem 3.4.13] that both ramification have different exponents $2p$.

4 The Tame p-Belyi Theorem

As mentioned in [5], a proof of Theorem 4 for $p > 2$ can be given as an application of the following technical result of Fulton.

Proposition 1. *[4, Proposition 8.1] If F is a function field with constant field $\bar{\mathbb{F}}_p$ with $p > 2$, then there exists a rational subfield $\bar{\mathbb{F}}_p(x)$ of F such that $e(Q|P) = 2$ or 1 for any $Q \in \mathbb{P}_F$ and $P \in \mathbb{P}_{\bar{\mathbb{F}}_p(x)}$ with $Q|P$.*

Therefore, we first prove the existence of a tame rational subfield of a function field F over $\bar{\mathbb{F}}_p$ for $p = 2$. We will then give a proof of Theorem 4.

4.1 The Tame 2-Belyi Theorem

Throughout this subsection, we assume that F is a function field over $\mathbb{F} = \bar{\mathbb{F}}_2$. An element $x \in F$ is called *pseudo-tame at* $P \in \mathbb{P}_F$ if there exists $z \in F$ such that $x + z^4$ is tame at P. Moreover, we say x is a *pseudo-tame element* if x is pseudo-tame at P for all $P \in \mathbb{P}_F$.

Lemma 4. *(i) x is pseudo-tame at P if and only if, for any non-vanishing term in the Laurent series expansion of x with degree smaller than $v_P(dx) + 1$, the degree is a multiple of four.*

(ii) x is pseudo-tame at P if and only if $\gamma(x)$ is pseudo-tame at P for any $\gamma \in \Gamma$, where Γ is the projective general linear group over F^4.

Proof. (i) The proof is straightforward by the definition of being pseudo-tame.

(ii) It is enough to observe that if x is pseudo-tame at P, then $a^4x + b^4$ and $1/x$ are also pseudo-tame at P by (i).

□

For $x, y \in \mathcal{H} = F \setminus F^2$, we write $x = x_0^4 + x_1^4 y + x_2^4 y^2 + x_3^4 y^3$ for some $x_0, x_1, x_2, x_3 \in F$ and define

$$a(x, y) = \frac{(x_1^2 x_3^2 + x_2^4)y}{x_3^4 y^2 + x_1^4} \ . \tag{4.1}$$

The notion $a(x, y)$ is introduced in [8]. We can summarize the required properties of $a(x, y)$ as follows.

Lemma 5. *(i) For any $x, y, t \in \mathcal{H}$*

$$a(x, y) + a(y, t) + a(t, x) \equiv 0 \mod F^2 \ . \tag{4.2}$$

(ii) Let $a(x, y) \equiv a \mod F^2$ and y be pseudo-tame at P. Then x is pseudo-tame at P if and only if a is regular at P, i.e., there exits $\tilde{a} \in F$ with $\tilde{a} \equiv a \mod F^2$ and $v_P(\tilde{a}) \geq 0$.

One of the main tools to show the existence of a pesudo-tame element is *Tsen's Theorem* stated as follows:
A function field F over $\bar{\mathbb{F}}_p$ is quasi-algebraically closed, i.e, any homogeneous polynomial over F of n variables whose degree is less than n has a non-trivial solution.

Proposition 2. *For any $x, a \in \mathcal{H}$, there exists $y \in \mathcal{H}$ such that $a(x,y) \equiv a \mod F^2$.*

Proof. Since $F = F^2 \oplus xF^2$, there exists unique $b \in F$ such that $a \equiv b^2 x \mod F^2$. Write $y = y_0^4 + y_1^4 x + y_2^4 x^2 + y_3^4 x^3$. Note that by Equation (4.2), $a(x,y) \equiv a(y,x) \mod F^2$, and hence

$$a(x,y) \equiv \frac{(y_1^2 y_3^2 + y_2^4)x}{y_3^4 x^2 + y_1^4} \equiv b^2 x \mod F^2 \ . \tag{4.3}$$

This holds if and only if $b \equiv (y_1 y_3 + y_2^2)/(y_3^2 x + y_1^2) \mod F^2$. By Tsen's Theorem, there exists an element $y \in F$ satisfying Equation (4.3). $\square$

We need the following two lemmata, which will be used in the proof of the existence of a pseudo-tame element.

Lemma 6. *Let $x \in F$ and $P, Q \in \mathbb{P}_F \setminus \operatorname{supp}(x)_\infty$. Then there exists $z \in F$ such that z has simple poles, $v_Q(x) \geq k$ for some positive integer k, and $x + z^2$ is tame at P.*

Proof. Let $u \in F$ be a prime element at P, and $x = a_0 + a_1 u + a_2 u^2 + \cdots$ be the Laurent series expansion of x. Let j be the integer such that a_j is the first non-vanishing term in the expansion. If j is odd, then it is enough to choose z has zero at P sufficiently large. Otherwise, say $j = 2n$. Then for a divisor $R = R_1 + \cdots + R_t$, where t is sufficiently large and R_i's are pairwise distinct and $P, Q \notin \operatorname{supp}(R)$, by the Riemann Roch Theorem there exists $z \in F$ such that

$$z \in \mathcal{L}(R - kQ - nP) \setminus \mathcal{L}(R - kQ - (n-1)P) \ .$$

Then z has simple poles, sufficiently large zero at Q, and $v_P(z) = n$. There exists $\alpha \in \mathbb{F}$ with $v_P(x + \alpha z^2) > 2n$. Then inductively we obtain an element satisfying the desired properties. $\square$

Lemma 7. *Let $R = R_1 + \cdots + R_t$, and $P_1, \ldots, P_n, Q \in \mathbb{P}_F \setminus \operatorname{supp}(R)$, where t is sufficiently large and R_i's are pairwise distinct. Then there exists $y \in F$ such that $(y)_\infty = R$, $P_i \notin \operatorname{supp}(y)_0$, and $v_Q(y) \geq k$ for some positive integer k.*

Proof. By the Riemann Roch Theorem, there exist z_j, x_i such that

$$z_j \in \mathcal{L}(R - kQ) \setminus \mathcal{L}(R - kQ - R_j) \quad \text{and} \quad x_i \in \mathcal{L}(R - kQ) \setminus \mathcal{L}(R - kQ - P_i)$$

for all $i = 1, \ldots, t$ and $j = 1, \ldots n$. Note that z_j, x_i have simple poles in the $\operatorname{supp}(R)$ with $v_{P_i}(x_i) = 0$ and $v_{R_j}(z_j) = -1$. As $\mathbb{F}$ is algebraically closed, there exist $\alpha_j, \beta_i \in \mathbb{F}$ such that

$$y = \sum_{j=1}^{t} \alpha_j z_j + \sum_{j=1}^{n} \beta_i x_i$$

has the desired properties. $\square$

Proposition 3. *Let F be a function field over $\mathbb{F} = \bar{\mathbb{F}}_2$. Then there exists a pseudo-tame element $x \in F$.*

Proof. We first show the existence of $x_i, a_i \in F$ for $i = 1, 2$ such that x_i is pseudo-tame, a_i is regular at P for all $P \in U_i$ with $\mathbb{P}_F = U_1 \cup U_2$ and $a(x_1, x_2) \equiv a_1 + a_2 \mod F^2$.

Let $x_1 \in F$ such that $(x_1)_\infty = (2n+1)Q$ for sufficiently large n and $Q \in \mathbb{P}_F$. Moreover, we can suppose that x_1 has simple zeros. Suppose $P_1, \ldots, P_t$ are ramified places of F in $F/\mathbb{F}(x_1)$. Let $z \in F$ such that

- $v_Q(z) \geq 0$,
- z has simple poles such that $\operatorname{supp}((x_1)_0) \cap \operatorname{supp}((z)_\infty) = \emptyset$, and
- $x_2 = x_1 + z^2$ is tame at $P_1, \ldots, P_t$.

Such an element exists by Lemma 6. We set $U_1 := \mathbb{P}_F \setminus \{P_1, \ldots, P_t\}$ and $U_2 := \{P_1, \ldots, P_t\}$. Observe that

$$a = a(x_1, x_2) = \left(\frac{dz}{dx_1}\right)^2 x_1 \ .$$

As $v_Q(z) \geq 0$, we have $v_Q(a) \geq 0$. Also, it is easy to observe that $v_P(a) \geq 0$ for any $P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_t\} \cup \operatorname{supp}((z)_\infty)$ since dx has zeros only at P_i for $i = 1, \ldots, t$ and dz has only poles in $\operatorname{supp}((z)_\infty)$. Say $\operatorname{supp}((z)_\infty) = R_1 + \cdots + R_k$, where R_i's are pairwise distinct places of F. As k is sufficiently large, by Lemma 7 there exits $y \in \mathcal{L}(R_1 + \cdots + R_k)$ such that

- y has sufficiently large zero at Q,
- $v_{R_i}(y) = -1$ for all $i = 1, \ldots, k$,
- y has no zero at $P_1, \ldots, P_t$

Set $u := \frac{1}{y}$, then we can write

$$\frac{dz}{dx} = \alpha_{-2} \frac{1}{u^2} + \alpha_{-1} \frac{1}{u} + \alpha_0 + \cdots$$

Note that the Laurent series expansion of $\frac{dx}{du}$ and $\frac{dz}{du}$ with respect to u has only even powers of u, and hence we have $\alpha_{-1} = 0$. Then

$$v_{R_i}\left(\frac{dz}{dx} + \alpha_{-2} \frac{1}{u^2}\right) \geq 0 \quad \text{for all } i = 1, \ldots, k$$

and $\frac{dz}{dx} + \alpha_{-2} \frac{1}{u^2}$ has sufficiently large zero at Q. Set

$$a_1 := \left(\frac{dx}{dz} + \alpha_{-2} \frac{1}{u^2}\right)^2 x \ \text{ and } \ a_2 := \frac{\alpha_{-2}^2 x}{u^4}$$

so that $a = a_1 + a_2$. Then a_1 is regular for all $P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_t\}$. Furthermore, since u has no pole at P_i, a_2 is regular at P_i for all $i = 1, \ldots, k$.

The rest of the proof is similar to the one given in [8, Theorem 3.6], but we give it here for the completeness. By Proposition 2, for any a_i there exists $y_i \in F$ such that $a(x_i, y_i) \equiv a_i \mod F^2$ for $i = 1, 2$. Then Equation (4.2) implies that $a(y_1, y_2) \equiv 0 \mod F^2$. In particular, $a(y_1, y_2)$ is regular at P for all $P \in U_j$. By Lemma 5/(ii), this shows that y_i is pseudo-tame at P for all $P \in U_j$ and $j = 1, 2$. In other words, y_i is pseudo-tame at P for all $P \in \mathbb{P}_F$. □

We fix a place $Q \in \mathbb{P}_F$, and set $R = \bigcup_{n\in\mathbb{N}} \mathcal{L}(nQ)$, i.e., R is the set of all elements which have poles only at Q.

Lemma 8. *Let $x \in R$. If x is pseudo-tame at Q with $-v_Q(dx) \geq 8g$, then there exists $z \in R$ such that $-v_Q(x + z^4) = -v_Q(dx) - 1$.*

Proof. We set $2e = -v_Q(dx)$. Note that $-v_Q(x) \geq -v_Q(dx) - 1$ and equality holds only if x is tame at Q. Suppose that $-v_Q(x) > -v_Q(dx) - 1 \geq 8g - 1$. Since x is pseudo-tame at Q, $v_Q(x) = -4k$ for some integer $k \geq 2g$. By Lemma 2, there exists $z_0 \in F$ with $(z_0)_\infty = kQ$. Since $\mathbb{F}$ is algebraically closed, there exists α such that for $\tilde{x} = x + \alpha z_0^4$ we have $-v_Q(\tilde{x}) < 4k = -v_Q(x)$. Then the existence of z follows after finitely many steps. □

Lemma 9. *Let $D = \sum n_i P_i$, $n_i \geq 0$, be a divisor of degree d. Suppose that $Q \notin \operatorname{supp}(D)$ and $d > 2g$. Then for $a \in R$ there exists $x \in R$ such that $D \leq (x + a)_0$ and $(x)_\infty = nQ$ for some $n < d + 2g$.*

Proof. By the Strong Approximation Theorem, there exits $x \in R$ such that $D \leq (x+a)_0$, see Corollary 1. If $n \geq d+2g$, then there exists $z \in F$ such that $D \leq (z)_0$ and $(z)_\infty = nQ$ by Lemma 2. There exists $\alpha \in \mathbb{F}$ such that $(x + \alpha z)_\infty = kQ$ with $k < n$. Note that for $\tilde{x} = x + \alpha z \in R$ we have $D \leq (\tilde{x} + a)_0$. Then the argument follows by induction. □

Proposition 4. *Let F be a function field over $\mathbb{F} = \bar{\mathbb{F}}_2$. Then there exists $x \in F$ such that $F/\mathbb{F}(x)$ is tame.*

Proof. Let x_0 be a pseudo-tame element. As F is the quotient field of R, we can write $x_0 = z_0/z_1$ for some $z_0, z_1 \in R$. Set $y = x_0 z_1^4 = z_1^3 z_0$. Note that $y \in R$ is pseudo-tame by Lemma 4/(ii). We can assume that $-v_Q(dy) \geq 8g$; otherwise we can replace y by $z^4 y$ for some proper $z \in R$. By Lemma 8, we can assume that $-v_Q(dy) = -v_Q(y) - 1 = 2e$. Moreover, we can suppose that y has simple zeros; otherwise replace y by $y + \alpha$ for some proper $\alpha \in \mathbb{F}$. In other words, there exists a pseudo-tame element $y \in R$, which is tame at Q and having simple zeros.

Let $\mathcal{Z}$ be the set of zeros of dy. Observe that y is pseudo-tame implies that y^3 is pseudo-tame. As dy has finitely many zeros, there exits $z \in F$ such that $y^3 + z^4$ is tame at P for all $P \in \mathcal{Z}$. Moreover, by the Strong Approximation Theorem, we can assume that $z \in R$, i.e., we can assume that $y^3 + z^4$ is a pseudo-tame element in R which is tame at P for all $P \in \mathcal{Z}$. Next, we set $v_P(dy) := 2m_P$, and define

$$D := \sum_{P\in\mathcal{Z}} \left\lfloor \frac{m_P}{2} \right\rfloor Q.$$

As $\deg(dy) = 2g - 2$, we have

$$\sum_{P \in \mathcal{Z}} m_P = e + g - 1, \text{ i.e., } \deg(D) \leq \frac{e+g-1}{2}.$$

By Lemma 9, we can also assume that $z \in R$ such that

$$(z)_0 \geq D \text{ and } \deg(z)_0 = \deg(z)_\infty \leq 2g + \frac{e+g-1}{2}.$$

We set $x := y^3 + h^4$. Note that by construction $x \in R$ is pseudo-tame and tame at P for all $P \in \mathcal{Z}$. Moreover, the Strict Triangle Inequality implies that

$$v_Q(x) = 3v_P(Q) = -3(2e-1), \text{ i.e., } x \text{ is tame at } Q.$$

For $P \in \mathbb{P}_F \setminus \mathcal{Z} \cup \{Q\}$, we see that $v_P(dx) = 2v_Q(y) = 0$ or 2 (as y has only simple zeros). Note that x is unramified at P if and only if $v_P(dx) = 0$. Since x is a pseudo-tame rational function, any term in the Laurent series expansion smaller than $v_P(dx)$ is multiple of 4 by Lemma 4/(i). However, this implies that $v_P(dx) = 0$, i.e., x is tame at P.

□

Proof of Theorem 4. We consider the subfield $\bar{\mathbb{F}}_p(x)$ of F given as in Propositions 1 and 4, i.e., $F/\bar{\mathbb{F}}_p(x)$ is tame. Since $F/\bar{\mathbb{F}}_p(x)$ is a finite separable extension, there exist finitely many ramified places of $\bar{\mathbb{F}}_p(x)$ in $F/\bar{\mathbb{F}}_p(x)$. Suppose that all the ramified places of $\bar{\mathbb{F}}_p(x)$ are contained in the set $\{(x = 0), (x = \infty), P_1, \cdots, P_n\}$ for some $n \geq 1$. Note that any place of $\bar{\mathbb{F}}_p(x)$ is rational, i.e., P_i is a place corresponding to $x - \alpha_i$ for some nonzero $\alpha_i \in \bar{\mathbb{F}}_p$. Let r be a positive integer such that $\alpha_i^{q^r-1} - 1 = 0$ for all $i = 1, \ldots, n$. Then Lemma 3 also holds for the extension $\bar{\mathbb{F}}_p(x)/\bar{\mathbb{F}}_p(t)$ defined by $t = 1 - x^{q^r-1}$. In other words, all places $P_1, \ldots, P_n$ lie over $(t = 0)$. Moreover, $(x = 0), (x = \infty)$ are the only ramified places in $\bar{\mathbb{F}}_p(x)/\bar{\mathbb{F}}_p(t)$, which are totally ramified lying over $(t = 1), (t = \infty)$, respectively. Then the proof follows from the fact that $\bar{\mathbb{F}}_p(x)/\bar{\mathbb{F}}_p(t)$ is tame. □

We note that the statement of the Tame p-Belyi Theorem strictly holds if the genus of F is positive. More precisely, we see in Remark 2 that in Theorem 4 there must be at least three (resp., two) ramified places if $g(F) > 0$ (resp., $g(F) = 0$). That is, the places $(y = 0), (y = 1)$, and $(y = \infty)$ are all ramified in the Tame p-Belyi Theorem when $g(F)$ is positive.

Remark 2. Let F be a function field over $\bar{\mathbb{F}}_p$. Suppose that there exists a rational subfield $\bar{\mathbb{F}}_p(y)$ of F such that $F/\bar{\mathbb{F}}_p(y)$ is tame of degree n. Let $Q_1, \ldots, Q_k$ be all ramified places of $\bar{\mathbb{F}}_p(y)$ in $F/\bar{\mathbb{F}}_p(y)$. We denote by N_{Q_i} the number of places of F lying over Q_i for $i = 1, \ldots, k$. Then by Dedekind's Different Theorem the degree of the ramification divisor of $F/\bar{\mathbb{F}}_p(y)$ is given as follows.

$$\begin{aligned}
\deg\big(\mathrm{Diff}(F/\bar{\mathbb{F}}_p(y))\big) &= \sum_{i=1}^{k} \sum_{P\in\mathbb{P}_F, P|Q_i} (e(P|Q_i)-1) \\
&= \sum_{i=1}^{k} \sum_{P\in\mathbb{P}_F, P|Q_i} e(P|Q_i) - \sum_{i=1}^{k} N_{Q_i} \\
&= kn - \sum_{i=1}^{k} N_{Q_i} \qquad (4.4)
\end{aligned}$$

Note that we use the Fundamental Equality in the last equality. By the Hurwitz genus formula, we also have

$$\deg\big(\mathrm{Diff}(F/\bar{\mathbb{F}}_p(y))\big) = 2n + 2g(F) - 2\ . \qquad (4.5)$$

Equation (4.4) and (4.5) implies that $k \geq 2$. The case $k = 2$ holds only if $g(F) = 0$ and the places Q_1, Q_2 are totally ramified.

Remark 3. Since ramification does not change under the constant field extension, we conclude from Remark 2 that there must be a wild ramification in Theorem 3 as noticed in Remark 1. Hence, it is called the Wild p-Belyi Theorem.

Acknowledgment

The authors would like to thank Prof. Dr. Henning Stichtenoth and Prof. Dr. Jaap Top for helpful discussions and their kind help. Nurdagül Anbar is supported by the Austrian Science Fund (FWF): Project F5505–N26 and Project F5511–N26, which is a part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

References

[1] Belyi G V,. On Galois extensions of a maximal cyclotomic field. Math USSR Izv 1980; 14: 247–256.

[2] Belyi G V. A new proof of the three point theorem. Sb Math 2002; 193(3-4): 329–332.

[3] Husemöller D. Elliptic curves. 2nd Ed. Springer-Verlag, 2004; 111.

[4] Fulton W. Hurwitz schemes and the irreducibility of moduli of algebraic curves. Ann Math 1969; 90: 542–575.

[5] Goldring W. Unifying themes suggested by Belyi's Theorem. Number Theory. Analysis and Geometry. in: Ramakrishnan, et al. (Eds.) Springer-Verlag (S. Lang memorial volume), 2011 .

[6] Hartshorne R. Algebraic geometry. Springer Verlag, 1977; 54.

[7] Hirschfeld J W P, Korchmaros G, Torres F. Algebraic curves over a finite field. Princeton Series in Appl Math Princeton University Press, 2008.

[8] Sugiyama Y, Yasuda S. Belyi's theorem in characteristic two, arXiv:1708.03036.

[9] Katz N, de Laumon T. Séminaire Bourbaki 1987-1988; 691: 105–132.

[10] Niederreiter H, Xing C P. Algebraic geometry in coding theory and cryptography. Princeton University Press, Princeton, NJ. 2009.

[11] Stichtenoth H. Algebraic function fields and codes. 2nd Ed. Springer-Verlag, 2009; 254.

[12] Mohamed S. Revêtements modérés et groupe fondamental de graphe de groupes. Compos Math 1997; 107.3: 319-338.

[13] Weil A. The field of definition of a variety. Amer J Math 1956; 78: 509–524.

[14] Zapponi L. On the 1-pointed curves arising as étale covers of the affine line in positive characteristic. Math Z 2008; 258(4): 711–727.