On Belyi's Theorems in Positive Characteristic

Nurdagül Anbar[1], Seher Tutdere[2]

[1] *SabancıUniversity, MDBF, Orhanlı, Tuzla, 34956, İstanbul, Turkey*
Email: nurdagulanbar2@gmail.com
[2] *Balıkesir University, Department of Mathematics, 10245 Altıeylül, Balıkesir, Turkey*
Email: 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 the Tame p-Belyi Theorems. In this paper, we discuss them in the language of function fields. In particular, we provide a constructive proof for the existence of a pseudo-tame element introduced in [13], which leads to a self-contained proof for the Tame 2-Belyi Theorem. Moreover, we provide unified and simple proofs for Belyi Theorems unlike the known ones that use technical results from Algebraic Geometry.

Keywords Belyi's Theorem, function field, finite field, tame and wild ramification, pseudo-tame

Mathematics Subject Classification (2010) 11R58, 11G20, 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 [14]. In other words, $\mathcal{X}$ is a curve defined over $\bar{\mathbb{Q}}$ if and only if there exists a morphism $f : \mathcal{X} \to \mathbb{P}^1$ whose branch points of f lie in the set $\{0, 1, \infty\}$. 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 [4] 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 1.1 (Wild p-Belyi Theorem)**.** *Let $\mathcal{X}$ be a connected, smooth, projective curve defined over $\mathbb{F}_q$. Then there exists a morphism $\phi : \mathcal{X} \to \mathbb{P}^1$ over $\mathbb{F}_q$ which admits at most one branch point.*

Theorem 1.2 (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.*

We remark that the converse of the Tame p-Belyi Theorem also holds. That is, a curve $\mathcal{X}$ is defined over a finite field if and only if there exists a tamely ramified morphism $\phi : \mathcal{X} \to \mathbb{P}^1$ admitting at most three branch points. However, as we mentioned above we are interested in "only if" part of the theorem.
To the best of our knowledge, a first proof of Theorem 1.2 for odd characteristic is given in [11]. Moreover, in [4], the proofs of Theorem 1.1 for any positive characteristic and Theorem 1.2 for odd characteristic are given by using the results of [8, 15] and [3], respectively. Even though the generalization of Theorem 1.1 to higher dimensional varieties has been known for a long time [9], the proof of the Tame 2-Belyi Theorem is a very recent result. It has been proved in [13] by using the existence of a pseudo-tame element for which the authors used the Serre duality theorem.
It is a well-known fact that the theory of algebraic curves and the theory of algebraic function fields are equivalent [5, 10]. As a consequence of this equivalence, here we discuss Belyi's theorems in positive characteristic in the language of function fields. This consideration results in unified and simple proofs for Belyi Theorems unlike the known ones that use technical results from Algebraic Geometry.
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, we give the constructive proof for the existence of a pseudo-tame element by using Riemann-Roch spaces, which significantly simplifies the proof of the Tame 2-Belyi Theorem given in [13].

2 Preliminaries

For the notations and well-known facts, as a general reference, we refer to [6, 12]. 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, i.e., $P = P' \cap F$, 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 of $\mathbb{F}$ does not divide $e(P'|P)$, then 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 1.1 and 1.2 in the language of function fields as follows.

Theorem 2.1 (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 2.2 (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 the reader, we now fix some notations. We denote by

$g(F)$	the genus of F,
$\mathbb{P}_F$	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 non-zero element $z \in F$,
$\mathcal{L}(A)$	the Riemann-Roch space associated to a divisor A of F,
$\ell(A)$	the $\mathbb{F}$-dimension of $\mathcal{L}(A)$,
$\mathrm{supp}(A)$	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 [12, 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 [12, 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.
One of the main tools in our proof of the Tame 2-Belyi Theorem is the Strong Approximation Theorem [12, Theorem 1.6.5], and hence we state it for the sake of the reader.

Lemma 2.3. *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 2.4. *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 $P \notin \mathrm{supp}(D)$ and $n \in \mathbb{N}$.*

In fact, we obtain a stronger conclusion by using the Riemann-Roch Theorem [12, Theorem 1.5.15].

Lemma 2.5. *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 $P \notin \mathrm{supp}(D)$.*

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. □

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 suitable $\alpha \in \mathbb{F}_q$. 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 $\mathbb{F}_q(t)\mathbb{F}_{q^r} \subseteq \mathbb{F}_q(x)\mathbb{F}_{q^r}$, 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 $P' \in \mathbb{P}_{\mathbb{F}_q(x)\mathbb{F}_{q^r}}$ 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 [12, Theorem 3.6.3], by the transitivity of ramification indices, we have $e(P|Q) = e(P'|Q')$. Write $g(T) - \beta h(T) = (T - \alpha)^m s(T)$ for some positive integer m and $s(T) \in \mathbb{F}_{q^r}[T]$ such that $s(\alpha) \neq 0$. 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 in $\bar{\mathbb{F}}_p$. 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

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

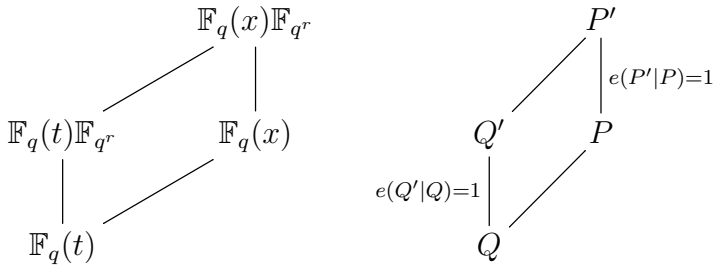

Figure 1: Constant field extensions of rational function fields

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

Lemma 2.6. *Let $\mathbb{F}_q(x)$ be a rational function field, and let $S = \{P_1, \ldots, P_n\}$ be a finite set of places of $\mathbb{F}_q(x)$ with $P_i \notin \{(x = 0), (x = \infty)\}$ for all $i = 1, \ldots, n$. Then there exists a subfield $\mathbb{F}_q(t)$ of $\mathbb{F}_q(x)$ with the following properties.*

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

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

(iii) the extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is tame.

Proof. We denote by r_i the degree of P_i for $i = 1, \ldots, n$, and set $r = \mathrm{lcm}(r_1, \ldots, r_n)$, 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 the above discussion on the ramification in the extension of rational function fields, all the places P_i 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). In other words, they are totally ramified. As the polynomial $T^{q^r-1} + \beta$ has no multiple roots for any non-zero $\beta \in \bar{\mathbb{F}}_p$, there is no other ramification. In particular, $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is a tame extension.

□

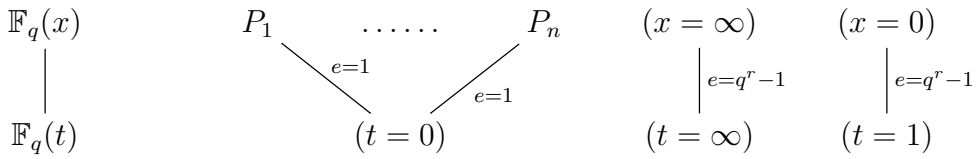

Figure 2: Ramification structure in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$

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. We recall the statement of the theorem: a function field F over $\mathbb{F}_q$ has a rational subfield $\mathbb{F}_q(y)$ such that at most one place of $\mathbb{F}_q(y)$, namely $(y=\infty)$, is ramified in $F/\mathbb{F}_q(y)$.

Proof of Theorem 2.1. 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 $S = \{(x=0), (x=\infty), P_1, \ldots, P_n\} \subset \mathbb{P}_{\mathbb{F}_q(x)}$ for some $n \geq 1$. By Lemma 2.6, we can find an element $t \in \mathbb{F}_q(x) \subseteq F$ such that any ramified place of F in $F/\mathbb{F}_q(t)$ lies over a place in 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 $(u=\infty)$. Moreover, the place $(t=1)$ lies over $(u=2)$. (Note that this is $(u=0)$ in characteristic 2.) We have seen in the above discussion 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.
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 $(u=\infty)$ 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 $F/\mathbb{F}_q(y)$.

□

Remark 3.1. We note that in the proof of Theorem 2.1 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 [12, Theorem 3.4.13] that both ramification have different exponents $2p$.

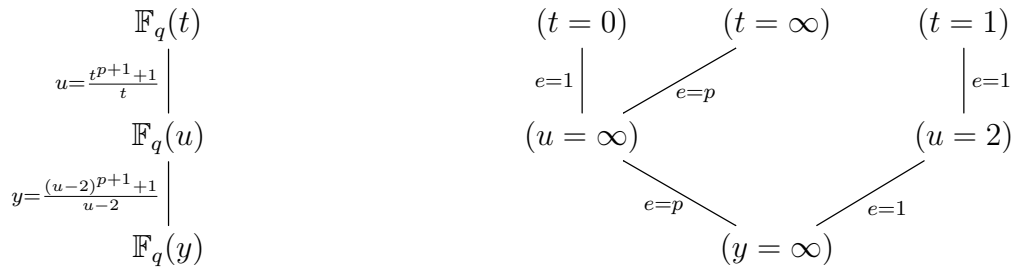

Figure 3: The Wild p-Belyi Theorem

4 The Tame p-Belyi Theorem

As mentioned in [4], a proof of Theorem 2.2 for $p > 2$ can be given as an application of the following technical result of Fulton, which shows the existence of a tame rational subfield of a function field.

Proposition 4.1. *[3, 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 discuss 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 2.2.

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 tame at $P \in \mathbb{P}_F$ if P is tame in the extension $F/\mathbb{F}(x)$. That is, $e(P|Q)$ is relatively prime to the characteristic p of $\mathbb{F}$, where $Q = P \cap \mathbb{F}(x)$. We say $x \in F$ is *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 that x is a *pseudo-tame element* of F if x is pseudo-tame at P for all $P \in \mathbb{P}_F$. We remark that the concept of "pseudo-tame" is introduced in [13], and for the properties of being pseudo-tame we refer to [13].
Let $P \in \mathbb{P}_F$, and t be a P-prime element of F, i.e., $v_P(t) = 1$. It is well known fact that any element $x \in F$ has a unique representation of the form

$$x = \sum_{i=n}^{\infty} a_i t^i \quad \text{with } n \in \mathbb{Z} \text{ and } a_i \in \mathbb{F}\ , \tag{4.1}$$

which is called power series expansion of x at P with respect to t. Moreover, we have $v_P(x) = \min\{i \mid a_i \neq 0\}$, see [12, Theorem 4.2.6].

Lemma 4.2. *Let $x \in F$ and Γ be the projective general linear group over F^4.*

(i) x is pseudo-tame at P if and only if the degree of any non-vanishing term in Equation 4.1 smaller than $v_P(dx) + 1$ is multiple of four.

(ii) x is pseudo-tame at P if and only if $\gamma(x)$ is pseudo-tame at P for any $\gamma \in \Gamma$.

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

$$a(x, y) = \frac{(x_1^2 x_3^2 + x_2^4)y}{x_3^4 y^2 + x_1^4} \ . \tag{4.2}$$

The notion $a(x, y)$ is introduced in [13]. We summarize the required properties of $a(x, y)$, which are given in Proposition 2.7 and Theorem 2.10 in [13], as follows.

Lemma 4.3. *(i) For any $x, y, t \in \mathcal{H}$,*

$$a(x, y) + a(y, t) + a(t, x) \equiv 0 \mod F^2 \ . \tag{4.3}$$

(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 exists $\tilde{a} \in F$ with $\tilde{a} \equiv a \mod F^2$ and $v_P(\tilde{a}) \geq 0$.

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

Lemma 4.4. *Let $x \in \mathcal{H}$ and $P, Q \in \mathbb{P}_F \setminus \mathrm{supp}(x)_\infty$. Then there exists $z \in F$ such that z has simple poles, $v_Q(z) \geq 0$, and $x + z^2$ is tame at P.*

Proof. Let $u \in F$ be a prime element at P, and

$$x = a_0 + a_1 u + a_2 u^2 + \dots$$

be the power series expansion of x. Let j be the integer such that a_j is the first non-vanishing term in the expansion. Note that $j \geq 0$ as $P \notin \mathrm{supp}(x)_\infty$. If j is odd, then it is enough to choose a non-zero $z \in \mathbb{F}$. Suppose that $j = 2n$. Then consider a divisor $R = R_1 + \dots + R_t$,

where t is sufficiently large, the R_i's are pairwise distinct, and $P, Q \notin \mathrm{supp}(R)$. By the Riemann Roch Theorem, there exists $z \in F$ such that

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

Then z has simple poles, $v_Q(z) \geq 0$, and $v_P(z) = n$. There exists $\alpha \in \mathbb{F}$ with $v_P(x + \alpha z^2) > 2n$. Then after finitely many steps we obtain an element satisfying the desired properties by Strict Triangle Inequality ([12, Lemma 1.1.11]). □

Lemma 4.5. *Let $x \in \mathcal{H}$ and $P_1, \ldots, P_t, Q \in \mathbb{P}_F \setminus \mathrm{supp}(x)_\infty$. Then there exists $z \in F$ such that z has simple poles, $v_Q(z) \geq 0$, and $x + z^2$ is tame at P_i for all $i = 1, \ldots, t$*

Proof. The proof is induction on t. We know that the claim holds for $t = 1$ by Lemma 4.4. Suppose that the claim holds for $t - 1 \geq 1$. That is, for $x \in \mathcal{H}$ and $P_1, \ldots, P_t, Q \in \mathbb{P}_F \setminus \mathrm{supp}(x)_\infty$, there exits z_1 such that z_1 has simple poles, $v_Q(z_1) \geq 0$ and $x + z_1^2$ is tame at P_i for all $i = 1, \ldots, t-1$. By the Riemann Roch Theorem, we can find z_2 such that z_2 has simple poles, $v_Q(z_2) \geq 0$, $v_{P_i}(z_2) > v_{P_i}(x + z_1^2)$ for all $i = 1, \ldots, t-1$ and $x + z_1^2 + z_2^2$ is tame at P_t. Set $z := z_1 + z_2$. Then the following holds.

(i) z has simple poles.

(ii) $v_Q(z) \geq 0$.

(iii) $x + z^2$ is tame for all P_i for all $i = 1, \ldots, t$ since $v_{P_i}(z_2) > v_{P_i}(x + z_1^2)$ implies that

$$v_{P_i}(x + z^2) = v_{P_i}(x + z_1^2 + z_2^2) = v_{P_i}(x + z_1^2) \quad \text{for all } i = 1, \ldots, t-1 \ .$$

□

Lemma 4.6. *Let $R = R_1 + \ldots + R_t$, and $P_1, \ldots, P_n, Q \in \mathbb{P}_F \setminus \mathrm{supp}(R)$, where t is sufficiently large and the R_i's are pairwise distinct. Then there exists $y \in F$ such that $(y)_\infty = R$, $P_i \notin \mathrm{supp}(y)_0$, 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 $j = 1, \ldots, t$ and $i = 1, \ldots n$. Note that z_j, x_i have simple poles in $\mathrm{supp}(R)$ 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. □

One of the main tools to show the existence of a pseudo-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 in n variables whose degree is less than n has a non-trivial solution. By using Tsen's Theorem, the following result is given in [13, Lemma 3.5]. The proof of the result is quite short and straightforward, and hence we give it here for the completeness.

Lemma 4.7. *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 $a \equiv b^2 x \mod F^2$. For $y \in F$, write $y = y_0^4 + y_1^4 x + y_2^4 x^2 + y_3^4 x^3$ for some $y_0, y_1, y_2, y_3 \in F$. Note that by Equation (4.3), $a(x, y) \equiv a(y, x) \mod F^2$, and hence

$$a(x, y) \equiv \frac{(y_1^2 y_3^2 + y_2^4)x}{y_3^4 x^2 + y_1^4} \equiv b^2 x \mod F^2 \ . \tag{4.4}$$

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 (4.4). □

Proposition 4.8. *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 $U_i \subseteq \mathbb{P}_F$ and $x_i, a_i \in F$ for $i = 1, 2$ such that $\mathbb{P}_F = U_1 \cup U_2$, x_i is pseudo-tame and a_i is regular at P for all $P \in U_i$, 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. Otherwise, we can replace x_1 by $x_1 + \alpha$ for some $\alpha \in \mathbb{F}$. Suppose $Q, P_1, \ldots, P_t$ 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 $\mathrm{supp}((x_1)_0) \cap \mathrm{supp}((z)_\infty) = \emptyset$, and
- $x_2 := x_1 + z^2$ is tame at $P_1, \ldots, P_t$.

Note that such an element z exists by Lemma 4.5. We set $U_1 = \mathbb{P}_F \setminus \{P_1, \ldots, P_t\}$ and $U_2 = \{P_1, \ldots, P_t\}$. By the definition of $a(x_1, x_2)$, see Equation (4.2), and the fact that $a(x_1, x_2) \equiv a(x_2, x_1) \mod F^2$, we 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 $P \in \mathbb{P}_F \setminus \{P_1, \ldots, P_t\} \cup \mathrm{supp}((z)_\infty)$ since dx_1 has zeros only at P_i for $i = 1, \ldots, t$ and dz has only poles in $\mathrm{supp}((z)_\infty)$. Say $\mathrm{supp}((z)_\infty) = R_1 + \ldots + R_k$, where the R_i's are pairwise distinct places of F. As we can choose z so that k is sufficiently large, by Lemma 4.6, there exists $y \in \mathcal{L}(R_1 + \ldots + R_k)$ such that

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

Set $u = \frac{1}{y}$, i.e., u is a prime element at R_i for all $i = 1, \ldots, k$. Since $v_{R_i}(dx_1) = 0$ and $v_{R_i}(dz) \geq -2$, we can write

$$\frac{dz}{dx_1} = \alpha_{-2}\frac{1}{u^2} + \alpha_{-1}\frac{1}{u} + \alpha_0 + \ldots$$

Note that the power series expansion of $\frac{dx_1}{du}$ and $\frac{dz}{du}$ with respect to u has only even powers of u, and hence we have $\alpha_{-1} = 0$. Then

$$v_{R_i}\left(\frac{dz}{dx_1} + \alpha_{-2}\frac{1}{u^2}\right) \geq 0 \quad \text{for all } i = 1, \ldots, k$$

and $\frac{dz}{dx_1} + \alpha_{-2}\frac{1}{u^2}$ has zero at Q. Set

$$a_1 = \left(\frac{dz}{dx_1} + \alpha_{-2}\frac{1}{u^2}\right)^2 x_1 \text{ and } a_2 = \frac{\alpha_{-2}^2 x_1}{u^4}$$

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 $v_{P_i}(u) = 0$, a_2 is regular at P_i for all $i = 1, \ldots, t$.
The rest of the proof is similar to the one given in [13, Theorem 3.5], but we give it here for completeness. By Proposition 4.7, for any a_i there exists $y_i \in F$ such that $a(x_i, y_i) \equiv a_i \mod F^2$ for $i = 1, 2$. Note that a_i is regular and x_i is pseudo-tame on U_i implies that y_i is pseudo-tame on U_i for $i = 1, 2$ by Lemma 4.3/(ii). Then Equation (4.3) implies that $a(y_1, y_2) \equiv 0 \mod F^2$, i.e., $a(y_1, y_2)$ is regular at P for all $P \in \mathbb{P}_F$. Therefore, by Lemma 4.3/(ii), we conclude that y_i is pseudo-tame at P for all $P \in U_j$ and $i, j = 1, 2$. In other words, y_i is pseudo-tame at P for all $P \in \mathbb{P}_F$ for $i = 1, 2$. □

Now we continue with the proof of the Tame p-Belyi Theorem, and leave the existence of tame extension obtained from a pseudo-tame element in Appendix 4.1. The proof is similar to the one given in [13], but it is more elegant and easier to follow.

Remark 4.9. Even though the proof that the existence of a pseudo-tame element implies the existence of tame extension is similar to the one in [13], we remark that Prof Japp Top and Roos Westerbeek were pointing out a mistake in the original version of [13]. Therefore, our proof corrects the error, which has also been independently corrected in the new version of [13].

We recall the statement of the theorem: a function field F over $\bar{\mathbb{F}}_p$ has a rational subfield $\bar{\mathbb{F}}_p(y)$ such that $F/\bar{\mathbb{F}}_p(y)$ is tame and at most there places of $\bar{\mathbb{F}}_p(y)$, namely $(y=0),(y=1),(y=\infty)$, are ramified in $F/\bar{\mathbb{F}}_p(y)$.

Proof of Theorem 2.2. We consider the subfield $\bar{\mathbb{F}}_p(x)$ of F given as in Propositions 4.1 and A.3, 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 places of $\bar{\mathbb{F}}_p(x)$ that are ramified in $F/\bar{\mathbb{F}}_p(x)$. Suppose that all the ramified places of $\bar{\mathbb{F}}_p(x)$ are contained in the set $\{(x=0),(x=\infty),P_1,\ldots,P_n\}$ 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 non-zero $\alpha_i\in\bar{\mathbb{F}}_p$. Let r be a positive integer such that $\alpha_i^{q^r-1}-1=0$ for all $i=1,\ldots,n$. Then Lemma 2.6 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 $\bar{\mathbb{F}}_p(x)/\bar{\mathbb{F}}_p(t)$, and they 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 will see in Remark 4.10 that there must be at least three ramified places in Theorem 2.2 if $g(F)>0$. 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 4.10. 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 places of $\bar{\mathbb{F}}_p(y)$, which are ramified 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.

$$\begin{aligned}\deg\left(\mathrm{Diff}(F/\bar{\mathbb{F}}_p(y))\right) &= \sum_{i=1}^{k}\sum_{P\in\mathbb{P}_F,P|Q_i}(e(P|Q_i)-1)\\ &= \sum_{i=1}^{k}\sum_{P\in\mathbb{P}_F,P|Q_i}e(P|Q_i)-\sum_{i=1}^{k}N_{Q_i}\\ &= kn-\sum_{i=1}^{k}N_{Q_i} \qquad (4.5)\end{aligned}$$

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

$$\deg\left(\mathrm{Diff}(F/\bar{\mathbb{F}}_p(y))\right)=2n+2g(F)-2\ . \qquad (4.6)$$

Equations (4.5) and (4.6) imply that $k\geq 3$ if $g(F)>0$.

Remark 4.11. Since ramification does not change under a constant field extension, we conclude from Remark 4.10 that there must be wild ramification in Theorem 2.1 as noticed in Remark 3.1. Hence, it is called the Wild p-Belyi Theorem.

Acknowledgements

The authors would like to thank Prof. Dr. Henning Stichtenoth and Prof. Dr. Jaap Top for their kind help and helpful discussions, which improved the manuscript considerably. 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] Fulton W. Hurwitz schemes and the irreducibility of moduli of algebraic curves. Ann Math 1969; 90: 542–575.

[4] 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 .

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

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

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

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

[9] Kedlaya K S. Étale covers of affine spaces in positive characteristic. C. R. Math. Acad. Sci. Paris 335 (2002), no. 11, 921–926.

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

[11] Saidi M. Revêtements modérés et groupe fondamental de graphe de groupes. Compos Math 1997; 107.3: 319-338.

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

[13] Sugiyama Y, Yasuda S. Belyi's theorem in characteristic two. Compos. Math. 156 (2020), no. 2, 325–339.

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

[15] 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.

A Existence of a Tame Rational Subfield from a Pseudo-tame Element

Let F be a function field over $\bar{\mathbb{F}}_2 = \mathbb{F}$. 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 the subring of F consisting of all elements which have poles only at Q.

Lemma A.1. *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 the 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 4.3/(i). By Lemma 2.5 with $D = 0$, there exists $z_0 \in F$ with $(z_0)_\infty = kQ$. Since $\mathbb{F}$ is algebraically closed, there exists $\alpha \in \mathbb{F}$ 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 A.2. *Let $D = \sum n_i P_i$, $n_i \geq 0$, be a divisor of degree d. Suppose that $Q \notin \mathrm{supp}(D)$ 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 exists $x \in R$ such that $D \leq (x + a)_0$ and $(x)_\infty = nQ$ for a sufficiently large integer n, see Corollary 2.4. If $n \geq d + 2g$, then there exists $z \in F$ such that $D \leq (z)_0$ and $(z)_\infty = nQ$ by Lemma 2.5. 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 A.3. *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 of F. 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 4.2/(ii). We can assume that $-v_Q(dy) \geq 8g$; otherwise we can replace y by $z^4 y$ for some suitable $z \in R$. By Lemma A.1, 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 suitable $\alpha \in \mathbb{F}$. 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 exists $z \in F$ 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 $P \in \mathcal{Z}$. 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 A.2, 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 $x = y^3 + z^4$. 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

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

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 pseudo-tame, any term in the power series expansion of x at P smaller than $v_P(dx)$ is multiple of 4 by Lemma 4.2/(i). However, this implies that $v_P(dx) = 0$, i.e., x is tame at P. Hence, by above argument we observe that $F/\mathbb{F}(x)$ is a tame extension.

□