Math. Res. Lett.
Volume 21, Number 06, 1389–1406, 2014

Separated Belyi maps

Zachary Scherr and Michael E. Zieve

We construct Belyi maps having specified behavior at finitely many points. Specifically, for any curve C defined over $\overline{\mathbb{Q}}$, and any disjoint finite subsets $S, T \subset C(\overline{\mathbb{Q}})$, we construct a finite morphism $\varphi\colon C \to \mathbb{P}^1$ such that φ ramifies at each point in S, the branch locus of φ is $\{0, 1, \infty\}$, and $\varphi(T) \cap \{0, 1, \infty\} = \emptyset$. This refines a result of Mochizuki's. We also prove an analogous result over fields of positive characteristic, and in addition we analyze how many different Belyi maps φ are required to imply the above conclusion for a single C and S and all sets $T \subset C(\overline{\mathbb{Q}}) \setminus S$ of prescribed cardinality.

1. Introduction

Let C be a (smooth, projective, geometrically irreducible) algebraic curve defined over $\mathbb{C}$. Belyi [2] gave an unexpected necessary and sufficient condition for C to be isomorphic to a curve defined over $\overline{\mathbb{Q}}$: namely, that there should exist a finite morphism $\varphi\colon C \to \mathbb{P}^1$ which has exactly three branch points. We refer to such a map φ as a *Belyi map*, and write $\mathrm{Br}(\varphi)$ for its branch locus. Belyi maps have had important consequences to topics ranging from Galois theory [7] to physics [1]; see for instance [3, 5, 6, 12–15] for various other consequences of Belyi maps. In some applications, one needs Belyi maps φ which satisfy additional properties. One prominent example is Mochizuki's inter-universal Teichmüller theory [10], which relies on his earlier results on Belyi maps [11].

We are interested in studying the amount of flexibility there is in the choice of a Belyi map φ on a prescribed curve C. One way to measure this is through the preimage $\varphi^{-1}(\mathrm{Br}(\varphi))$. We will show in Proposition 3.4 that, for any curve C of genus at least 2, only finitely many subsets of $C(\mathbb{C})$ of any prescribed cardinality can occur as $\varphi^{-1}(\mathrm{Br}(\varphi))$ for a Belyi map φ on C. These distinguished finite subsets of $C(\mathbb{C})$ are the focus of this paper.

We now state our first main result. Throughout this paper, we view all curves as coming equipped with a fixed embedding into projective space,

so that if a curve C is defined over a field K then we can speak of the coordinatewise action of the absolute Galois group of K on points of $C(\overline{K})$.

Theorem 1.1. *Let K be a number field, let C be a curve over K, and let S and T be finite subsets of $C(\overline{K})$ such that S is disjoint from the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements of T. Then there exists a finite morphism $\varphi\colon C \to \mathbb{P}^1$ defined over K such that*

- $\mathrm{Br}(\varphi) = \{0, 1, \infty\}$,
- *φ is ramified at every point in S,*
- $\varphi(T) \cap \{0, 1, \infty\} = \emptyset$.

In this result, the set $\{0, 1, \infty\}$ could be replaced by any prescribed three-element subset of K, since there are linear fractional transformations over K which map any such subset to $\{0, 1, \infty\}$. In [11, Theorem 2.5], Mochizuki proved a similar result in which the condition that φ be ramified on S is replaced by the weaker condition that $\varphi(S) = \{0, 1, \infty\}$. It is natural to attempt to deduce our result from Mochizuki's by replacing Mochizuki's map φ_0 with the composition $\psi \circ \varphi_0$ where $\psi\colon \mathbb{P}^1 \to \mathbb{P}^1$ is ramified at each point in $\{0, 1, \infty\}$ and also $\mathrm{Br}(\psi) = \{0, 1, \infty\}$ and $\psi^{-1}(\{0, 1, \infty\}) = \{0, 1, \infty\}$; however, in fact no such map ψ exists, so one must use a different argument. Our proof of Theorem 1.1 is quite different from Mochizuki's proof of [11, Theorem 2.5], and uses ideas from [4], although both our proof and Mochizuki's follow the general outline of all known proofs of Belyi's theorem.

Positive characteristic analogues of Belyi maps seem to have been considered for the first time by Katz [8, Lemma 16] in the context of the Langlands correspondence for function fields. In positive characteristic, every curve admits a finite morphism to $\mathbb{P}^1$ having just one branch point. We prove the following analogue of Theorem 1.1 in this setting.

Theorem 1.2. *Let K be a perfect field of characteristic $p > 0$, let C be a curve over K, and let S, T be finite subsets of $C(\overline{K})$ such that S is disjoint from the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements of T. Then there exists a finite morphism $\varphi\colon C \to \mathbb{P}^1$ defined over K such that*

- $\mathrm{Br}(\varphi) = \{\infty\}$,
- *φ is ramified at every point in S,*
- $\infty \notin \varphi(T)$.

Now we fix a set S and let T vary over all subsets of $C(\overline{\mathbb{Q}}) \setminus S$ of prescribed cardinality n. In Theorem 1.1, we produced a Belyi map corresponding to any such T; our next result shows that in fact only $n+1$ Belyi maps are needed to account for all T.

Theorem 1.3. *Let $n \geq 1$ be an integer, and let C be a curve defined over a number field K. For any finite $\mathrm{Gal}(\overline{K}/K)$-stable subset S of $C(\overline{K})$, there exist finite morphisms*

$$\varphi_1, \ldots, \varphi_{n+1} \colon C \to \mathbb{P}^1$$

defined over K such that

- $\mathrm{Br}(\varphi_i) = \{0, 1, \infty\}$ *for* $1 \leq i \leq n+1$,
- *each φ_i is ramified at every point in S,*
- *every n-element subset $T \subset C(\overline{K}) \setminus S$ satisfies $\varphi_i(T) \cap \{0, 1, \infty\} = \emptyset$ for at least one $i \in \{1, 2, \ldots, n+1\}$ (where i may depend on T).*

This refines a result of Mochizuki's [11, Corrollary 3.1], which shows the existence of a finite set of Belyi maps satisfying the above properties, except with our condition on the ramification of φ_i replaced by the weaker condition $\varphi_i(S) = \{0, 1, \infty\}$. Mochizuki's proof uses a compactness argument which does not provide control on the number of maps required; we use a different argument which enables us to determine the minimum number of maps possible. In Theorem 5.1, we give an analogous result in positive characteristic. We note that these results have a topological interpretation. For any curve C defined over $\overline{\mathbb{Q}}$, we say that a *Belyi open* subset of $C(\overline{\mathbb{Q}})$ is any set of the form $C(\overline{\mathbb{Q}}) \setminus \varphi^{-1}(\mathrm{Br}(\varphi))$ where $\varphi \colon C \to \mathbb{P}^1$ is a Belyi map. Theorem 1.1 implies that, for any disjoint finite $S, T \subset C(\overline{\mathbb{Q}})$, there is a Belyi open set which contains T but is disjoint from S. Theorem 1.3 implies that, for any finite $S \subset C(\overline{\mathbb{Q}})$, there are $n+1$ Belyi open sets $U_1, \ldots, U_{n+1}$ such that any n-element subset T of $C(\overline{\mathbb{Q}}) \setminus S$ satisfies $T \subset U_i \subseteq C(\overline{\mathbb{Q}}) \setminus S$ for some i.

Belyi constructed a Belyi map φ on any curve C over $\overline{\mathbb{Q}}$ by writing $\varphi = \varphi_3 \circ \varphi_2 \circ \varphi_1$, where $\varphi_1 \colon C \to \mathbb{P}^1$ is any finite morphism defined over $\overline{\mathbb{Q}}$, $\varphi_2 \colon \mathbb{P}^1 \to \mathbb{P}^1$ satisfies $B := \mathrm{Br}(\varphi_2) \cup \varphi_2(\mathrm{Br}(\varphi_1)) \subset \mathbb{Q}$, and $\varphi_3 \colon \mathbb{P}^1 \to \mathbb{P}^1$ satisfies $\mathrm{Br}(\varphi_3) \cup \varphi_3(B) = \{0, 1, \infty\}$. His argument shows that there exist Belyi maps φ for which $\varphi^{-1}(\mathrm{Br}(\varphi))$ contains any prescribed subset of $C(\overline{\mathbb{Q}})$. Both Mochizuki's proof and our proof have a similar structure to Belyi's proof, in that φ is constructed as the composition of three maps. The difference is

that we require some points to be outside the branch loci of the maps φ_i, as in the following diagram (where we assume $T \neq \emptyset$):

$$\begin{array}{ccccc}
C & & T & & \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow & & \\
\mathbb{P}^1 & \alpha = \infty & \notin & A = \varphi_1(S) \cup \mathrm{Br}(\varphi_1) \\
\downarrow{\scriptstyle \varphi_2} & & \downarrow & & \\
\mathbb{P}^1 & \beta = \varphi_2(\infty) & \notin & B = \varphi_2(A) \cup \mathrm{Br}(\varphi_2) \\
\downarrow{\scriptstyle \varphi_3} & & \downarrow & & \\
\mathbb{P}^1 & \varphi_3(\beta) & \notin & \varphi_3(B) \cup \mathrm{Br}(\varphi_3) = \{0, 1, \infty\}.
\end{array}$$

We will construct the map φ_1 in the next section, treating the case of positive characteristic at the same time as the case of characteristic zero. The maps φ_2 and φ_3 are constructed for fields of characteristic zero in the section after that, and then we construct them over fields of positive characteristic. Then in the last section we treat collections of Belyi maps.

2. Reduction to $\mathbb{P}^1$

Our goal is to show that every curve C defined over a suitable field admits a Belyi map $C \to \mathbb{P}^1$ with prescribed behavior at finitely many points. In this section, we show that it suffices to do this when $C = \mathbb{P}^1$.

Proposition 2.1. *Let C be a curve defined over a perfect field K. If S and T are disjoint finite $\mathrm{Gal}(\overline{K}/K)$-stable subsets of $C(\overline{K})$ then there exists a finite morphism*

$$\varphi\colon C \to \mathbb{P}^1$$

defined over K such that $\varphi(T) \subseteq \{\infty\}$ and $\infty \notin \varphi(S) \cup \mathrm{Br}(\varphi)$.

Before proving this we recall some terminology. A divisor on C (over $\overline{K}$) is said to be *defined over K* if it is fixed by $\mathrm{Gal}(\overline{K}/K)$. For any divisor D on C which is defined over K, the associated Riemann–Roch space is the K-vector space

$$\mathcal{L}(D) := \{f \in K(C)\colon (f) \geq -D\} \cup \{0\},$$

and the dimension of this vector space is denoted $\ell(D)$.

Proof. We may (and will) assume that T is nonempty, since the result for empty T follows from the result for nonempty T. Let $O_1, O_2, \ldots, O_n$ be the $\mathrm{Gal}(\overline{K}/K)$-orbits of points in T, and for each i let D_i be the divisor

$$D_i = \sum_{P \in O_i} P.$$

Note that D_i is defined over K. Let g be the genus of C, and let R be a finite $\mathrm{Gal}(\overline{K}/K)$-stable subset of $C(\overline{K})$ such that $|R| \geq 2g-1$ and $R \cap (S \cup T) = \emptyset$. Let D be the divisor

$$D = \sum_{P \in R} P,$$

so that D is defined over K and $\deg(D) = |R| \geq 2g-1$. By the following lemma, there is an element $f \in \mathcal{L}(D + \sum_{i=1}^{n} D_i)$ which is not in $\mathcal{L}(D + \sum_{i \neq j} D_i)$ for any j. Then $f \in K(C)$ has simple poles at all the points of T, at most simple poles at the points in R, and no other poles. Because R is disjoint from S, we see that f extends to a morphism φ satisfying the requirements of the proposition. □

Lemma 2.2. *Let C be a curve of genus g defined over a perfect field K. Let T be a non-empty finite $\mathrm{Gal}(\overline{K}/K)$-stable subset of $C(\overline{K})$. Let $O_1, \ldots, O_n$ be the $\mathrm{Gal}(\overline{K}/K)$-orbits in T, and let D_i be the divisor $D_i = \sum_{P \in O_i} P$. If D is a divisor defined over K of degree at least $2g-1$, then*

$$\mathcal{L}\left(D + \sum_{i=1}^{n} D_i\right) \supsetneq \bigcup_{j=1}^{n} \mathcal{L}\left(D + \sum_{i \neq j} D_i\right).$$

Proof. For each $j \in \{1, 2, \ldots, n\}$, we have

$$\deg\left(D + \sum_{i=1}^{n} D_i\right) > \deg\left(D + \sum_{i \neq j} D_i\right) \geq 2g-1,$$

so the Riemann–Roch theorem implies that

$$\ell\left(D + \sum_{i=1}^{n} D_i\right) = \deg(D) + |T| + 1 - g > \ell\left(D + \sum_{i \neq j} D_i\right).$$

Since a vector space over an infinite field cannot be written as the union of finitely many proper subspaces, it follows that if K is infinite then

$$\mathcal{L}\left(D+\sum_{i=1}^{n} D_i\right) \supsetneq \bigcup_{j=1}^{n} \mathcal{L}\left(D+\sum_{i\neq j} D_i\right).$$

Henceforth assume that K is finite, and write

$$\begin{aligned} m_i &:= \deg(D_i) = |O_i|\,, \\ m &:= |T|\,, \\ q &:= |K|\,, \\ r &:= \deg(D) + 1 - g. \end{aligned}$$

The Riemann–Roch theorem implies that $\ell(D+\sum_{i=1}^{n} D_i) = r+m$, and thus

$$\left|\mathcal{L}\left(D+\sum_{i=1}^{n} D_i\right)\right| = q^{r+m}.$$

For distinct $j_1, j_2, \ldots, j_k \in \{1,2,\ldots,n\}$, we have

$$\bigcap_{t=1}^{k} \mathcal{L}\left(D+\sum_{i\neq j_t} D_i\right) = \mathcal{L}\left(D+\sum_{i\neq j_1,\ldots,j_k} D_i\right).$$

Riemann–Roch implies that

$$\begin{aligned} \ell\left(D+\sum_{i\neq j_1,\ldots,j_k} D_i\right) &= r+\sum_{i\neq j_1,\ldots,j_t} m_i \\ &= r+m-m_{j_1}-\cdots-m_{j_k}, \end{aligned}$$

so that

$$\left|\mathcal{L}\left(D+\sum_{i\neq j_1,\ldots,j_k} D_i\right)\right| = q^{r+m-m_{j_1}-\cdots-m_{j_k}}.$$

It follows by inclusion–exclusion that

$$\left|\bigcup_{j=1}^{n} \mathcal{L}\left(D+\sum_{i\neq j} D_i\right)\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1\leq j_1<\ldots<j_k\leq n} q^{r+m-\sum_{t=1}^{k} m_{j_t}}.$$

This cardinality equals

$$q^{r+m}\left(1-\prod_{i=1}^{n}\left(1-\frac{1}{q^{m_{j_i}}}\right)\right),$$

which is strictly smaller than q^{r+m}. Thus our union of subspaces is a proper subset of $\mathcal{L}(D+\sum_{i=1}^{n} D_i)$, as desired. □

3. Characteristic 0

In this section, we prove that for any finite subset $A \subset \mathbb{P}^1(\overline{\mathbb{Q}})$, and any element $\alpha \in \mathbb{P}^1(\overline{\mathbb{Q}}) \setminus A$, there is a Belyi map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ with $\varphi(\alpha) \notin \mathrm{Br}(\varphi) = \{0, 1, \infty\}$ such that all points in A ramify under φ. We do this in two steps. The first step produces a map φ_2 which allows us to reduce to the case that A and α are in $\mathbb{P}^1(\mathbb{Q})$. The second step produces a map φ_3 for which $\varphi = \varphi_3 \circ \varphi_2$ has the required properties.

To proceed, fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and let $|\cdot| : \overline{\mathbb{Q}} \to \mathbb{R}$ be the induced absolute value. The following lemma enables us to control the absolute values of α and of the elements of A.

Lemma 3.1. *Let A be a finite subset of $\mathbb{P}^1(\overline{\mathbb{Q}})$, and pick any $\alpha \in \mathbb{P}^1(\mathbb{Q}) \setminus A$. Then for any real number $c > 1$, there exists a linear fractional transformation $\psi \in \mathbb{Q}(x)$ such that $\psi(\alpha) \in \mathbb{Q}$ with $\max_{\beta\in A}\{|\psi(\beta)|\} < 1$ and $|\psi(\alpha)| > c$.*

Proof. Upon replacing A and α by their images under a suitably chosen linear fractional transformation in $\mathbb{Q}(x)$, we may assume that $\alpha = 0$ and $\infty \notin A$. Because $0 = \alpha \notin A$, we can choose $r \in \mathbb{Q}$ with $0 < r < \min_{\beta\in A} \frac{|\beta|}{c+1}$. It follows that every $\beta \in A$ satisfies

$$rc < |\beta| - r,$$

so the triangle inequality yields

$$rc < |\beta| - r \leq |\beta - r|\,.$$

Choose a rational number s such that $rc < s < \min_{\beta\in A} |\beta - r|$. Now the linear fractional transformation

$$\psi(x) := \frac{s}{x - r}$$

satisfies

$$|\psi(0)| = \frac{s}{r} > c$$

and, for β in A,

$$|\psi(\beta)| = \frac{s}{|\beta - r|} < 1.$$

Since s and r are rational, ψ satisfies the conditions of the lemma. □

Our next result enables us to reduce from the case of a finite subset of $\mathbb{P}^1(\overline{\mathbb{Q}})$ to a finite subset of $\mathbb{P}^1(\mathbb{Q})$.

Proposition 3.2. *Let A be a finite subset of $\mathbb{P}^1(\overline{\mathbb{Q}})$, and let $\alpha \in \mathbb{P}^1(\mathbb{Q}) \setminus A$. There exists a rational function $f \in \mathbb{Q}(x)$ such that*

$$f(A), \mathrm{Br}(f), f(\alpha) \subseteq \mathbb{P}^1(\mathbb{Q}) \quad \text{and} \quad f(\alpha) \notin f(A) \cup \mathrm{Br}(f).$$

Proof. For any $\alpha \in \mathbb{P}^1(\mathbb{Q})$ and any finite subsets A_0, A_1 of $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \{\alpha\}$ with $A_0 \subset A_1$, the conclusion of the Proposition holds for $A = A_0$ if it holds for $A = A_1$. Therefore we may assume without loss that A is nonempty. Moreover, the hypothesis $\alpha \in \mathbb{P}^1(\mathbb{Q}) \setminus A$ implies that α is not in the image of A under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so (since this image is finite) we may assume that A is preserved by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $c > 1$ be a constant whose value will be chosen later. Then Lemma 3.1 produces a degree-one rational function $\psi(x) \in \mathbb{Q}(x)$ for which $\psi(\alpha) \in \mathbb{Q}$, $|\psi(\alpha)| > c$, and $\max_{\beta \in \overline{A}}\{|\psi(\beta)|\} < 1$. It follows that $\hat{A} := \psi(A)$ is a subset of $\overline{\mathbb{Q}}$ which does not contain the rational number $\hat{\alpha} := \psi(\alpha)$, and moreover (since $\psi(x) \in \mathbb{Q}(x)$) that $\hat{A}$ is preserved by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that $|\hat{A}| \le |A|$ is bounded by a constant which does not depend on the choice of c. If $\hat{f} \in \mathbb{Q}(x)$ satisfies $\hat{f}(\hat{A}), \mathrm{Br}(\hat{f}), \hat{f}(\hat{\alpha}) \subseteq \mathbb{P}^1(\mathbb{Q})$ and $\hat{f}(\hat{\alpha}) \notin \hat{f}(\hat{A}) \cup \mathrm{Br}(\hat{f})$, then $\hat{f} \circ \psi$ satisfies all the properties required of f. Thus, there is no loss in replacing A and α by $\hat{A}$ and $\hat{\alpha}$, so we may assume that $\alpha \in \mathbb{Q}$, that A is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subset of $\overline{\mathbb{Q}}$, and in addition that $\max_{\beta \in A}\{|\beta|\} < 1$ and $|\alpha| > c$.

Writing $n := |A|$ (which is bounded by a constant which does not depend on the choice of c), we will define polynomials $f_0, f_1, \ldots, f_{n-1} \in \mathbb{Q}[x]$ such that

(1) $\deg(f_i) = n - i$ for $0 \le i \le n-1$,

(2) $f_i(\mathrm{Br}(f_{i-1})) = \{0, \infty\}$ for $1 \le i \le n-1$,

(3) $f_0(A) = \{0\}$,

(4) the leading coefficient of f_i is an integer,

(5) all coefficients of f_i have absolute value bounded by an absolute constant (independent of the choice of c) for $0 \leq i \leq n-1$.

Suppose for the moment that such f_i have been constructed. By properties (1) and (5) there is a constant N, independent of c, such that for each i all coefficients of $f_{n-1} \circ f_{n-2} \circ \cdots \circ f_i$ have absolute value at most N. We now show that if c is sufficiently large then $f := f_{n-1} \circ f_{n-2} \circ \cdots \circ f_1 \circ f_0$ satisfies the conclusion of the Proposition. For $\beta \in A$ we have $f_0(\beta) = 0$ and thus $f(\beta) = f_{n-1} \circ \cdots \circ f_1(0)$ is a rational number of absolute value at most N. Next, any $\delta \in \mathrm{Br}(f) \setminus \{\infty\}$ has the form $\delta = f_{n-1} \circ f_{n-2} \circ \cdots \circ f_i(\gamma)$ where $0 \leq i \leq n-2$ and $f_i'(\gamma) = 0$. Property (2) implies that $f_{i+1}(f_i(\gamma)) = 0$, so that δ equals $f_{n-1} \circ f_{n-2} \circ \cdots \circ f_{i+2}(0)$ and hence is a rational number of absolute value at most N. Since the leading coefficient of $f(x)$ has absolute value at least 1, and all other coefficients have absolute value at most N, it follows that if c is sufficiently large then $|f(\alpha)| > N$. But we have shown that $f(A) \cup \mathrm{Br}(f)$ consists of rational numbers of absolute value at most N, so we must have $f(\alpha) \notin f(A) \cup \mathrm{Br}(f)$. Finally, since $f(x) \in \mathbb{Q}[x]$ and $\alpha \in \mathbb{Q}$, we see that $f(\alpha) \in \mathbb{Q}$, which implies the conclusion of the proposition.

To finish the proof, we must construct polynomials $f_i \in \mathbb{Q}[x]$ satisfying the stated properties. Define

$$f_0(x) := \prod_{\beta \in A} (x - \beta).$$

Since A is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable, f_0 must be in $\mathbb{Q}[x]$. Moreover, f_0 is monic of degree n and $f_0(A) = \{0\}$. Since $|\beta| < 1$ for all $\beta \in A$, and every coefficient of f_0 is the sum of several products of distinct β's (or the negative of such a sum), it follows that every coefficient of f_0 has absolute value less than 2^n. Therefore f_0 satisfies the required properties. Inductively, suppose we have defined f_{i-1} for some i with $1 \leq i \leq n-1$, and that f_{i-1} satisfies the required properties. Then define

$$f_i(x) := \mathrm{Res}_y(f_{i-1}'(y), f_{i-1}(y) - x),$$

where $\mathrm{Res}_y(*, *)$ is the resultant with respect to the variable y. Since the resultant is the determinant of the Sylvester matrix, it follows that f_i has rational coefficients and that all its coefficients have absolute value at most some function of n (independent of c). Let ax^d be the leading term of $f_{i-1}(x)$, where we know that $d = n - i + 1$. Let $r_1, r_2, \ldots, r_{d-1}$ be the roots of f_{i-1}',

counted with multiplicity. Then we have

$$f_i(x) = (ad)^d \prod_{j=1}^{d-1} (f_{i-1}(r_j) - x).$$

It follows that the leading term of f_i is $(-x)^{d-1}(ad)^d$, and that the roots of f_i are precisely the finite branch points of f_{i-1}. Thus f_i satisfies Properties (1)–(5), so by induction these properties hold for $f_0, f_1, \ldots, f_{n-1}$, which implies the result. □

We now construct the desired Belyi map in case the curve is $\mathbb{P}^1$ and all distinguished points are in $\mathbb{P}^1(\mathbb{Q})$.

Proposition 3.3. *Let B be a finite subset of $\mathbb{P}^1(\mathbb{Q})$, and pick any $\beta \in \mathbb{P}^1(\mathbb{Q}) \setminus B$. Then there exists a rational function $f \in \mathbb{Q}(x)$ such that*

- *f is ramified at every point in B,*
- *$\mathrm{Br}(f) = \{0, 1, \infty\}$,*
- *$f(\beta) \notin \{0, 1, \infty\}$.*

Proof. Upon replacing B and β by their images under $\frac{1}{x-a}$ for any prescribed $a \in \mathbb{Q} \setminus (B \cup \{\beta\})$, we may assume that $B \subset \mathbb{Q}$ and $\beta \in \mathbb{Q}$. Upon replacing B and β by their images under ax for a suitable $a \in \mathbb{Z} \setminus \{0\}$, we may assume that $B \subset \mathbb{Z}$ and $\beta \in \mathbb{Z}$. By adjoining to B a sufficiently large finite subset of $\mathbb{Z} \setminus (B \cup \{\beta\})$, we may assume that $|B| \geq 2$. Let p be a prime which does not divide $\gamma - \beta$ for any $\gamma \in B$, and put $\delta := \beta + p$. Let $B' := B \cup \{\delta\}$, and write the elements of B' as

$$B' = \{b_1, b_2, \ldots, b_m\}$$

with $b_m = \delta$.

We now construct the desired rational function $f(x)$. Let

$$c := \prod_{1 \leq i < j \leq m} (b_i - b_j),$$

and note that $c \neq 0$. Partial fraction decomposition ensures that there are unique $n_1, \ldots, n_m \in \mathbb{Q}$ such that

$$\sum_{i=1}^{m} \frac{n_i}{x - b_i} = \frac{c}{\prod_{j=1}^{m}(x - b_j)},$$

namely

$$n_i := \frac{c}{\prod\limits_{\substack{1\le j\le m\\ j\ne i}} (b_i - b_j)}.$$

Our choice of c ensures that the n_i are nonzero integers. Finally, we define

$$f(x) := \prod_{i=1}^{m} (x - b_i)^{2n_i}.$$

It remains to check that $f(x)$ has the required properties. Since each n_i is nonzero, the elements of B' are critical points of f. Every finite critical point of f must be either a zero or a pole of

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^{m} \frac{2n_i}{x - b_i}.$$

Our construction of the n_i's ensures that the right side equals

$$\frac{2c}{\prod_{j=1}^{m}(x - b_j)},$$

so f cannot have any critical points outside of $B' \cup \{\infty\}$. Since $f(B') \subseteq \{0, \infty\}$ and $f(\infty) \in \{0, 1, \infty\}$, it follows that $\mathrm{Br}(f) \subseteq \{0, 1, \infty\}$. Moreover, since f ramifies at each element of B' and we know that $|B'| \ge 3$, Riemann–Hurwitz implies that f must have at least three branch points, whence $\mathrm{Br}(f) = \{0, 1, \infty\}$. Finally, we show that $f(\beta) \notin \{0, 1, \infty\}$. Since $\beta \notin B'$, we know a priori that $f(\beta) \notin \{0, \infty\}$. Our choice of the prime p ensures that $p \nmid (\beta - b_i)$ for $i < m$, yet $p \mid (\beta - b_m)$. Thus the p-adic valuation of

$$f(\beta) = \prod_{i=1}^{m} (\beta - b_i)^{2n_i}$$

is nonzero, so that $f(\beta) \ne 1$. □

With all the ingredients in place, we can now prove Theorem 1.1.

Proof of Theorem 1.1. By adjoining to S the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements of S, we may assume that S is preserved by $\mathrm{Gal}(\overline{K}/K)$. Likewise we may assume that T is preserved by $\mathrm{Gal}(\overline{K}/K)$. By adjoining to T a finite $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-stable set of points in $C(\overline{\mathbb{Q}}) \setminus S$ if necessary, we may assume that T is nonempty. Let $\varphi_1 \colon C \to \mathbb{P}^1$ be the map produced by Proposition 2.1

for this choice of S and T. Then φ_1 is defined over K, the set $A := \varphi_1(S) \cup \mathrm{Br}(\varphi_1)$ does not contain $\alpha := \infty$, and $\varphi_1(T) = \{\infty\}$. Let $\varphi_2 \colon \mathbb{P}^1 \to \mathbb{P}^1$ be the map produced by Proposition 3.2 for A and α. Then φ_2 is defined over $\mathbb{Q}$, both $\beta := \varphi_2(\alpha)$ and $B := \varphi_2(A) \cup \mathrm{Br}(\varphi_2)$ are contained in $\mathbb{P}^1(\mathbb{Q})$, and $\beta \notin B$. Lastly, let $\varphi_3 \colon \mathbb{P}^1 \to \mathbb{P}^1$ be the map produced by Proposition 3.3 for B and β. Then φ_3 is defined over $\mathbb{Q}$, every point in B ramifies under φ_3, and $\varphi_3(\beta) \notin \{0, 1, \infty\} = \mathrm{Br}(\varphi_3)$. Pictorially, we have

$$\begin{array}{ccccc}
C & & T & & \\
\big\downarrow{\scriptstyle \varphi_1} & & \big\downarrow & & \\
\mathbb{P}^1 & \alpha = \infty & \notin & A = \varphi_1(S) \cup \mathrm{Br}(\varphi_1) \\
\big\downarrow{\scriptstyle \varphi_2} & & \big\downarrow & & \\
\mathbb{P}^1 & \beta = \varphi_2(\infty) & \notin & B = \varphi_2(A) \cup \mathrm{Br}(\varphi_2) \\
\big\downarrow{\scriptstyle \varphi_3} & & \big\downarrow & & \\
\mathbb{P}^1 & \varphi_3(\beta) & \notin & \mathrm{Br}(\varphi_3) \cup \varphi_3(B) = \{0, 1, \infty\}.
\end{array}$$

Thus $\varphi := \varphi_3 \circ \varphi_2 \circ \varphi_1$ is a finite morphism $C \to \mathbb{P}^1$ defined over K, and $\varphi(T) = \varphi_3(\beta) \notin \{0, 1, \infty\}$. Since $\varphi_2(\varphi_1(S)) \subseteq B$ and every point of B ramifies under φ_3, it follows that every point of S ramifies under φ. Finally, $\mathrm{Br}(\varphi)$ is the union of the three sets $\mathrm{Br}(\varphi_3)$, $\varphi_3(\mathrm{Br}(\varphi_2))$, and $\varphi_3(\varphi_2(\mathrm{Br}(\varphi_1)))$, and hence equals $\{0, 1, \infty\}$. □

We conclude this section by showing that, if C is a complex curve of genus at least 2, then only finitely many subsets of $C(\mathbb{C})$ of any prescribed cardinality can occur as $\varphi^{-1}(\mathrm{Br}(\varphi))$ where $\varphi \colon C \to \mathbb{P}^1$ is a Belyi map. In fact, we will show at the same time that only finitely many curves C of any prescribed genus admit a Belyi map $\varphi \colon C \to \mathbb{P}^1$ for which $\varphi^{-1}(\mathrm{Br}(\varphi))$ has prescribed cardinality.

Proposition 3.4. *Fix integers $n, g \geq 1$. There are only finitely many isomorphism classes of complex curves C of genus g for which there exists a Belyi map $\varphi \colon C \to \mathbb{P}^1$ such that $\left|\varphi^{-1}(\mathrm{Br}(\varphi))\right| = n$. Moreover, if $g \geq 2$ and C is a curve of genus g, then there are only finitely many n-element subsets of $C(\mathbb{C})$ which occur as $\varphi^{-1}(\mathrm{Br}(\varphi))$ for a Belyi map $\varphi \colon C \to \mathbb{P}^1$.*

Proof. Let $\varphi \colon C \to \mathbb{P}^1$ be a degree-d Belyi map on a genus-g curve C, and let $B := \varphi^{-1}(\mathrm{Br}(\varphi))$. For any $P \in B$, write $e(P)$ for the ramification index

of P under φ. The Riemann–Hurwitz formula implies that

$$2g-2 = -2d + \sum_{P\in B}(e(P)-1) = -2d + 3d - |B|\,,$$

so that $d = 2g-2+|B|$. Thus, d is determined by g and $n := |B|$.

For any Belyi map $\varphi\colon C \to \mathbb{P}^1$, there is a linear fractional transformation $\mu \in \mathbb{C}(x)$ for which $\mu(\mathrm{Br}(\varphi)) = \{0,1,\infty\}$. Thus $\overline{\varphi} := \mu\circ\varphi$ is a Belyi map with branch locus $\{0,1,\infty\}$, and $\varphi^{-1}(\mathrm{Br}(\varphi)) = \overline{\varphi}^{-1}(\{0,1,\infty\})$. So there is no loss in restricting to Belyi maps with branch locus $\{0,1,\infty\}$. A classical result (see for instance, [9, Prop. 3.1]) implies that, for any fixed d, there are only finitely many isomorphism classes of pairs (C,φ) where C is a complex curve and $\varphi\colon C\to\mathbb{P}^1$ is a degree-d Belyi map with branch locus $\{0,1,\infty\}$. Thus, for fixed n and g, there are only finitely many isomorphism classes of corresponding curves C. Since any curve of genus at least 2 has only finitely many automorphisms, it follows that for fixed n, g with $g\geq 2$ and a fixed genus-g curve C there are only finitely many n-element sets of the form $\varphi^{-1}(\{0,1,\infty\})$, where $\varphi\colon C\to\mathbb{P}^1$ is a Belyi map with branch locus $\{0,1,\infty\}$. □

4. Characteristic p

In this section, we prove Theorem 1.2. The key tool is the following result:

Proposition 4.1. *Let K be a perfect field of characteristic $p>0$, and let $B\subset\mathbb{P}^1(\overline{K})$ be a finite set such that $0\notin B$. Then there exists $f\in K(x)$ such that*

- *f is ramified at every point in B*
- $\mathrm{Br}(f) = \{\infty\}$
- $f(0)\neq\infty$.

Proof. Since the result in case $B=\emptyset$ follows from the result in case $B=\{1\}$, we may assume that B is nonempty. Let $\overline{B}\subset\mathbb{P}^1(\overline{K})$ be the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements in $B\setminus\{\infty\}$, and let $V\subset\overline{K}$ be the $\mathbb{F}_p$-span of $\overline{B}$. Then V is a finite set which is preserved by $\mathrm{Gal}(\overline{K}/K)$, and its minimal polynomial

$$T(x) := \prod_{\alpha\in V}(x-\alpha)$$

has the form

$$T(x) = \sum_{i=0}^{n} a_i x^{p^i},$$

where $a_i \in K$ and $a_0 \neq 0$. Let

$$S(x) := \frac{T(x)^p}{x^p} = \sum_{i=0}^{n} a_i^p x^{p(p^i-1)}$$

and

$$g(x) := x^p + \frac{1}{T(x) + S(x)}.$$

The rational function $g(x)$ is well defined since $S(0) = a_0^p \neq 0$, while $T(0) = 0$. Plainly $g(\infty) = \infty$. Since $0 \notin B$ by hypothesis, for β in $B \setminus \{\infty\}$ we have

$$T(\beta) + S(\beta) = T(\beta) + \frac{T(\beta)^p}{\beta^p} = 0,$$

so that $g(\beta) = \infty$. Thus $g(B) \subseteq \{\infty\}$, and furthermore

$$g(0) = \frac{1}{T(0) + S(0)} = \frac{1}{a_0^p} \neq \infty.$$

Since $T'(x) = a_0$ and $S'(x) = 0$, we compute

$$g'(x) = \frac{-a_0}{(T(x) + S(x))^2},$$

so that $g'(x)$ has no roots in $\overline{K}$ since $a_0 \neq 0$. Therefore $g(x)$ has no finite critical points which are not poles, and since $g(\infty) = \infty$, it follows that $\mathrm{Br}(g) \subseteq \{\infty\}$. The polynomial $x^p + x \in K[x]$ has ∞ as its unique critical point and its unique branch point. Thus $f := g^p + g$ satisfies the requirements of the proposition. □

Proof of Theorem 1.2. By adjoining to S the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements of S, we may assume that S is preserved by $\mathrm{Gal}(\overline{K}/K)$. Likewise we may assume that T is preserved by $\mathrm{Gal}(\overline{K}/K)$. By adjoining to T a finite $\mathrm{Gal}(\overline{K}/K)$-stable set of points in $C(\overline{K}) \setminus S$ if necessary, we may assume that T is nonempty. Let $\varphi_1 \colon C \to \mathbb{P}^1$ be the map constructed in Proposition 2.1 for this choice of S and T. Then φ_1 is defined over K, the set $A := \varphi_1(S) \cup \mathrm{Br}(\varphi_1)$ does not contain $\alpha := \infty$, and $\varphi_1(T) = \{\infty\}$. Let $\varphi_2 \colon \mathbb{P}^1 \to \mathbb{P}^1$ be the map $x \mapsto 1/x$, and put $B := \varphi_2(A)$, so that B does not contain $\varphi_2(\alpha) = 0$. Let $\varphi_3 \colon \mathbb{P}^1 \to \mathbb{P}^1$ be the map constructed in Proposition 4.1 for this choice

of B. Then φ_3 is defined over K, ramifies at every point in B, and satisfies $\varphi_3(0) \neq \infty$ and $\mathrm{Br}(\varphi_3) = \{\infty\}$. This yields the diagram

$$\begin{array}{ccccc}
C & & T & & \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow & & \\
\mathbb{P}^1 & \alpha = \infty & \notin & A = \varphi_1(S) \cup \mathrm{Br}(\varphi_1) \\
\downarrow{\scriptstyle \frac{1}{x}} & \downarrow & & \\
\mathbb{P}^1 & \beta = 0 & \notin & B = \{1/\gamma \colon \gamma \in A\} \\
\downarrow{\scriptstyle \varphi_3} & \downarrow & & \\
\mathbb{P}^1 & \varphi_3(\beta) & \notin & \varphi_3(B) \cup \mathrm{Br}(\varphi_3) = \{\infty\}.
\end{array}$$

Then $\varphi := \varphi_3 \circ \varphi_2 \circ \varphi_1$ is a finite morphism $C \to \mathbb{P}^1$ defined over K, and $\varphi(T) = \varphi_3(\beta) \neq \infty$. Since φ_3 ramifies at every point in B, and B contains $\varphi_2(\varphi_1(S))$, we see that φ ramifies at every point in S. Finally, since φ_2 is unramified, $\mathrm{Br}(\varphi)$ is the union of $\mathrm{Br}(\varphi_3)$ and $\varphi_3(\varphi_2(\mathrm{Br}(\varphi_1)))$, and hence equals $\{\infty\}$. □

5. Collections of Belyi maps

Finally, we consider collections of Belyi maps, and prove Theorem 1.3.

Proof of Theorem 1.3. Let $T_0 = \emptyset$, and use the following inductive procedure to define finite subsets T_i of $C(\overline{\mathbb{Q}}) \setminus S$ and morphisms $\varphi_i \colon C \to \mathbb{P}^1$ for each $i = 1, 2, \ldots, n+1$. For any $i \in \{1, 2, \ldots, n+1\}$ such that T_{i-1} has been defined, let $\varphi_i \colon C \to \mathbb{P}^1$ be the morphism produced by Theorem 1.1 for the sets S and $T := T_{i-1}$. Then φ_i is a finite morphism defined over K such that

- $\mathrm{Br}(\varphi_i) = \{0, 1, \infty\}$,
- φ_i is ramified at every point in S,
- $\varphi_i(T_{i-1}) \cap \{0, 1, \infty\} = \emptyset$.

Define

$$T_i := T_{i-1} \cup \varphi_i^{-1}(\{0, 1, \infty\}) \setminus S,$$

and note that T_i is a finite subset of $C(\overline{\mathbb{Q}}) \setminus S$. This procedure yields morphisms $\varphi_1, \ldots, \varphi_{n+1} \colon C \to \mathbb{P}^1$. For each $i \in \{1, 2, \ldots, n+1\}$, note that

$$\varphi_i^{-1}(\{0, 1, \infty\}) = S \cup (T_i \setminus T_{i-1}).$$

Since $T_1 \subseteq T_2 \subseteq \cdots \subseteq T_{n+1}$, the sets

$$T_1 \setminus T_0,\ T_2 \setminus T_1,\ \ldots,\ T_{n+1} \setminus T_n$$

are pairwise disjoint. Thus any n-element subset T of $C(\overline{\mathbb{Q}})$ must be disjoint from at least one set $T_i \setminus T_{i-1}$, so if $T \cap S = \emptyset$ then $\varphi_i(T) \cap \{0, 1, \infty\} = \emptyset$. □

The following positive characteristic analogue of Theorem 1.3 can be shown by a similar argument.

Theorem 5.1. *Let n be a positive integer, and let C be a curve defined over a perfect field K of characteristic $p > 0$. For any finite $\mathrm{Gal}(\overline{K}/K)$-stable subset S of $C(\overline{K})$, there exist finite morphisms*

$$\varphi_1, \ldots, \varphi_{n+1} \colon C \to \mathbb{P}^1$$

defined over K such that

- $\mathrm{Br}(\varphi_i) = \{\infty\}$ *for* $1 \le i \le n+1$,
- *each φ_i is ramified at every point in S,*
- *every n-element subset $T \subset C(\overline{K}) \setminus S$ satisfies $\varphi_i(T) \cap \{\infty\} = \emptyset$ for at least one $i \in \{1, 2, \ldots, n+1\}$ (where i may depend on T).*

We conclude with a remark about potential improvements of the number $n+1$ of maps in Theorem 1.3.

Remark. Let C be a curve over $\overline{\mathbb{Q}}$, and let S be a finite subset of $C(\overline{\mathbb{Q}})$. If S has the form $\varphi^{-1}(\mathrm{Br}(\varphi))$ for some Belyi map $\varphi \colon C \to \mathbb{P}^1$, then we may replace the $n+1$ maps $\varphi_1, \ldots, \varphi_{n+1}$ in the conclusion of Theorem 1.3 with the single map φ. If S does not have this form, then the $n+1$ Belyi maps in the conclusion of Theorem 1.3 cannot be replaced by a smaller set of maps. For, if $\varphi_1, \ldots, \varphi_n \colon C \to \mathbb{P}^1$ are Belyi maps with $\mathrm{Br}(\varphi_i) = \{0, 1, \infty\}$ and $S \subsetneqq \varphi_i^{-1}(\{0, 1, \infty\})$, then pick any $t_i \in \varphi_i^{-1}(\{0, 1, \infty\}) \setminus S$, and note that

$$T := \{t_1, \ldots, t_n\}$$

satisfies $|T| \le n$ and

$$\varphi_i(T) \cap \{0, 1, \infty\} \ne \emptyset$$

for every i.

Acknowledgments

The authors thank the referee for reading this paper extremely carefully and providing several helpful comments. The authors thank the NSF for support under grants EMSW21-RTG:0943832 and DMS-1162181.

References

[1] S.K. Ashok, F. Cachazo and E. Dell'Aquila, *Children's drawings from Seiberg–Witten curves*, Commun. Number Theory Phys. **1**(2) (2007), 237–305.

[2] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. **14** (1980), 247–256.

[3] I.I. Bouw, S. Wewers and L. Zapponi, *Deformation data, Belyi maps, and the local lifting problem*, Trans. Amer. Math. Soc. **361**(12) (2009), 6645–6659.

[4] E.H. Brooks, J.H. Rosen, Z. Scherr, B.L. Weiss and M.E. Zieve, *A classification of certain Belyi maps*, Preprint.

[5] N.D. Elkies, *Shimura curves for level-3 subgroups of the* $(2, 3, 7)$ *triangle group, and some other examples*, in 'Algorithmic number theory', Lecture Notes in Computer Science, **4076**, 302–316, Springer, Berlin, 2006.

[6] W. Goldring, *Unifying themes suggested by Belyi's theorem*, in 'Number theory, analysis and geometry', 181–214, Springer, New York, 2012.

[7] A. Grothendieck, *Esquisse d'un programme*, in 'Geometric Galois actions, 1', London Mathematical Society Lecture Note Series, **242**, 5–48, Cambridge University Press, Cambridge, 1997. With an English translation on pp. 243–283.

[8] N.M. Katz, *Travaux de Laumon*, Astérisque (1988), no. 161–162, Exp. No. 691, 4, 105–132 (1989). Séminaire Bourbaki, Vol. 1987/88.

[9] B. Köck, *Belyi's theorem revisited*, Beiträge Algebra Geom. **45**(1) (2004), 253–265.

[10] S. Mochizuki, *Inter-universal Teichmüller theory IV: log-volume computations and set-theoretic foundations*, Preprint. `http://www.kurims.kyoto-u.ac.jp/~motizuki/papers-english.html`

[11] ———, *Noncritical Belyi maps*, Math. J. Okayama University **46** (2004), 105–113.

[12] K. Nakanishi, *Lamé operators with projective octahedral and icosahedral monodromies*, Rend. Sem. Mat. Univ. Padova **114** (2005), 109–129 (2006).

[13] L. Schneps (ed.), *The Grothendieck theory of dessins d'enfants*, London Mathematical Society Lecture Note Series, **200**, Cambridge University Press, Cambridge, 1994, ISBN 0-521-47821-9. Papers from the Conf. on Dessins d'Enfant held in Luminy, April 19–24, 1993.

[14] L. Schneps and P. Lochak (eds.), *Geometric Galois actions*', 1, Vol. 242 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1997, ISBN 0-521-59642-4. Around Grothendieck's "Esquisse d'un programme".

[15] ———, *Geometric Galois actions*', 2, Vol. 243 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge (1997), ISBN 0-521-59641-6. The inverse Galois problem, moduli spaces and mapping class groups.

Department of Mathematics
University of Pennsylvania
209 South 33rd Street
Philadelphia, PA 19104-6395
USA
E-mail address: zscherr@math.upenn.edu
URL: http://www.math.upenn.edu/∼zscherr/

Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109-1043
USA

Mathematical Sciences Center
Tsinghua University
Beijing 100084
China
E-mail address: zieve@umich.edu
URL: http://www.math.lsa.umich.edu/∼zieve/

Received November 14, 2013