SEPARATED BELYI MAPS

ZACHARY SCHERR AND MICHAEL E. ZIEVE

ABSTRACT. 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, 13, 14, 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 [11], which relies on his earlier results on Belyi maps [10].

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 [10, Thm. 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 [10, Thm. 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 $\overline{\mathbb{Q}}$. If $S \subset C(\overline{\mathbb{Q}})$ is a finite set of points, then there exist finite morphisms*

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

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*

- *for any subset $T \subset C(\overline{\mathbb{Q}})$ of cardinality n for which $S \cap T = \emptyset$, there exists an $i \in \{0, 1, \ldots, n+1\}$ such that $\varphi_i(T) \cap \{0, 1, \infty\} = \emptyset$.*

This refines a result of Mochizuki's [10, Cor. 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 $T \subset U_i \subset C(\overline{\mathbb{Q}}) \setminus S$ for some i.

Belyi proved his theorem by constructing φ as the composition $\varphi_3 \circ \varphi_2 \circ \varphi_1$, 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 stay away from the branch locus, as in the following diagram:

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

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 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. $\qquad\square$

Lemma 2.2. *Let C be a curve of genus g defined over a perfect field K. Let T be a finite, non-empty $\mathrm{Gal}(\overline{K}/K)$-stable set of points 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

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

so the Riemann–Roch theorem implies that

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

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

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

Henceforth assume that K is finite, and put

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

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

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

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

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

Riemann–Roch implies that

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

so that

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

It follows by inclusion-exclusion that

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

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 $\mathcal{L}(D+\sum_{i=1}^{n}D_i)$. □

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 $|.| \colon \overline{\mathbb{Q}} \to \mathbb{R}$ 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 suppose $\alpha \in \mathbb{P}^1(\mathbb{Q}) \setminus A$. Then for any real number $c > 1$, there exists a fractional linear 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. By applying an appropriate fractional linear transformation with rational coefficients, we may assume without loss of generality that $\alpha = 0$ and $\infty \notin A$. Because $\alpha = 0$ is not in A, we can choose an $r \in \mathbb{Q}$ with $0 < r < \min_{\beta \in A}\dfrac{|\beta|}{c+1}$. Rewriting this inequality, we have that for any $\beta \in A$

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

Thus the triangle inequality yields

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

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

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

we see that

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

and that for β in A we have

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

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*

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

Proof. If $A = \emptyset$, then we lose nothing by replacing A with $\{\beta\}$ for some $\beta \in \mathbb{Q}$ different from α. Thus for the remainder of the proof we assume that A is nonempty. Let $\overline{A}$ be the set of all Galois conjugates of elements of A. Since $\alpha \in \mathbb{P}^1(\mathbb{Q}) \setminus A$ we know that $\alpha \notin \overline{A}$ as well. Applying a fractional linear transformation from Lemma 3.1, we may assume without loss of generality that $|\beta| < 1$ for all $\beta \in \overline{A}$, and that $c < |\alpha| < \infty$ for some positive constant c to be chosen later. Note that the fractional linear transformation has rational coefficients so the image of $\overline{A}$ is still Galois stable. Writing $n := \#\overline{A}$, we will define polynomials $f_0, f_1, \dots, f_{n-1} \in \mathbb{Q}[x]$ such that

(1) $\deg(f_i) = n - i$ for $0 \le i \le n - 1$
(2) $f_i(\mathrm{Br}(f_{i-1})) = \{0\}$ for $1 \le i \le n - 1$
(3) $f_0(\overline{A}) = \{0\}$
(4) the leading coefficient of f_i is an integer
(5) all coefficients of f_i have absolute value bounded by a function of n (independent of the choice of c) for $0 \le i \le n - 1$.

Supposing for the moment that such f_i have been constructed, we now show that if c is sufficiently large compared to n then $f := f_{n-1} \circ f_{n-2} \circ \cdots \circ f_1 \circ f_0$ satisfies the conclusion of the Proposition. For $\beta \in \overline{A}$ we have $f_0(\beta) = 0$ and thus $f(\beta) = f_{n-1} \circ \cdots \circ f_1(0)$ is a rational number whose absolute value is bounded by a function of n. Next, any finite element δ of $\mathrm{Br}(f)$ has the form $\delta = f_{n-1} \circ f_{n-2} \circ \cdots \circ f_i(\gamma)$ where $0 \le i \le n - 2$ and $f_i'(\gamma) = 0$. Then $f_{i+1}(f_i(\gamma)) = 0$, so $\delta = f_{n-1} \circ f_{n-2} \circ \cdots \circ f_{i+2}(0)$ is a rational number whose absolute value is bounded by a function of n. Finally, since $\alpha \in \mathbb{Q}$ and $c < |\alpha| < \infty$, we see that $f(\alpha) \in \mathbb{Q}$ and that $|f(\alpha)|$ is larger than any prescribed function of n whenever c is sufficiently large; since $f(A)$ and $\mathrm{Br}(f) \setminus \{\infty\}$ are bounded by a function of n, the statement of the result follows.

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

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

Since $\overline{A}$ is Galois stable, we see that f_0 is a monic polynomial in $\mathbb{Q}[x]$ of degree n. Moreover, $f_0(\overline{A}) = \{0\}$ and all coefficients of f_0 have absolute value bounded by a function of n. Inductively, suppose for any $1 \le i \le n-1$ that f_{i-1} has been defined and satisfies the stated properties. Then put

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

where $\mathrm{Res}_y()$ is the resultant with respect to the variable y. Since the resultant is the determinant of the Sylvester matrix, we see that f_i has

rational coefficients and that all its coefficients are bounded by a function of n. 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}. This concludes the proof. $\square$

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 suppose $\beta \in \mathbb{P}^1(\mathbb{Q}) \setminus B$. 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. By applying a fractional linear transformation of the form $\frac{1}{x-a}$ if necessary (with $a \in \mathbb{Q}$), we may assume that $B \subseteq \mathbb{Q}$ and $\beta \in \mathbb{Q}$. We may also apply a fractional linear transformation of the form ax with $a \in \mathbb{Z} \setminus \{0\}$ to ensure that $B \subseteq \mathbb{Z}$ 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

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

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

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

namely

$$n_i = \frac{c}{\displaystyle\prod_{\substack{1 \leq j \leq m \\ j \neq i}} (b_j - b_i)}.$$

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 f ensures that the right side equals

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

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 $\#B' \geq 3$, 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 $f(\beta) \neq 1$. $\qquad\square$

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

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

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 iso-morphism classes of complex curves C of genus g for which there exists a Belyi map $\varphi \colon C \to \mathbb{P}^1$ such that $\#\varphi^{-1}(\mathrm{Br}(\varphi)) = n$. 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 fractional linear 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 $\{0, 1, \infty\}$. $\qquad\square$

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 $B \subseteq \mathbb{P}^1(\overline{K})$ 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. Let $\overline{B} \subseteq \mathbb{P}^1(\overline{K})$ be the set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of elements in $B \setminus \{\infty\}$, and let $V \subseteq \overline{K}$ be the $\mathbb{F}_p$-span of $\overline{B}$. This 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

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

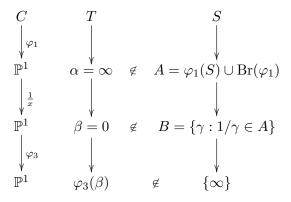so that $g(\beta) = \infty$. Thus $g(B) \subseteq \{\infty\}$, and furthermore

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

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

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

which has no finite roots since $a_0 \neq 0$. Therefore $g(x)$ has no finite critical points which are not poles, and since $g(\infty) = \infty$, we see 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. $\qquad\square$

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 $\varphi(T) = \{\infty\}$. 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

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

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 $\{\infty\}$. $\qquad\square$

5. Collections of Belyi maps

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

Proof of Theorem 1.3. Let $T_0 = \emptyset$. For each $i = 1, 2, \ldots, n+1$, if T_{i-1} is a finite subset of $C(\overline{\mathbb{Q}}) \setminus S$ then we define a morphism $\varphi_i \colon C \to \mathbb{P}^1$ and a finite subset T_i of $C(\overline{\mathbb{Q}}) \setminus S$ as follows. 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 satisfies

- $\mathrm{Br}(\varphi_i) = \{0, 1, \infty\}$
- 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 finite morphisms $\varphi_1, \ldots, \varphi_{n+1} \colon C \to \mathbb{P}^1$. For $i = 1, 2, \ldots, n+1$, note that

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

Since $T_1 \subseteq T_2 \subseteq \ldots \subseteq T_{n+1}$, 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 $\varphi_i(T) \cap \{0, 1, \infty\} = \emptyset$. $\square$

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 $S \subset C(K)$, 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 $1 \leq i \leq n+1$*
- *each φ_i is ramified at every point in S*
- *for any n-element subset $T \subset C(\overline{K}) \setminus S$ there exists $i \in \{1, \ldots, n+1\}$ such that $\varphi_i(T) \cap \{\infty\} = \emptyset$.*

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 $S \subsetneq \varphi_i^{-1}(\{0, 1, \infty\})$, then pick some $t_i \in \varphi_i^{-1}(\{0, 1, \infty\}) \setminus S$, and note that

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

satisfies $|T| \leq n$ and

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

for every i.

References

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

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

[3] I. I. Bouw, S. Wewers and L. Zapponi, *Deformation data, Belyi maps, and the local lifting problem*, Trans. Amer. Math. Soc. **361** (2009), 6645–6659. 1

[4] E. H. Brooks, J. H. Rosen, Z. Scherr, B. L. Weiss and M. E. Zieve, *A classification of certain Belyi maps*, preprint. 2

[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, Springer, Berlin (2006), 302–316. 1

[6] W. Goldring, *Unifying themes suggested by Belyi's theorem*, in: Number Theory, Analysis and Geometry: In Memory of Serge Lang, Springer–Verlag (2012), 181–214. 1

[7] A. Grothendieck, *Esquisse d'un programme*, in: Geometric Galois Actions, 1, Cambridge Univ. Press, Cambridge (1997), 5–48. 1

[8] N. M. Katz, *Travaux de Laumon*, *Séminaire N. Bourbaki*, 1987–1988, exp. no. 691, 105–132. 2

[9] B. Köck, *Belyi's theorem revisited*, Beiträge Algebra Geom. **45** (2004), 253–264. 10

[10] S. Mochizuki, *Noncritical Belyi maps*, Math. J. Okayama Univ. **46** (2004), 105–113. 1, 2, 3

[11] S. Mochizuki, *Inter-universal Teichmüller theory IV: log-volume computations and set-theoretic foundations*, preprint. 1

[12] K. Nakanishi, *Lamé operators with projective octahedral and icosahedral monodromies*, Rend. Sem. Mat. Univ. Padova **114** (2005), 109–129. 1

[13] L. Schneps (ed.), The Grothendieck theory of dessins d'enfants, Cambridge Univ. Press, Cambridge (1994). 1

[14] L. Schneps and P. Lochak (eds.), Geometric Galois actions. 1. Around Grothendieck's "Esquisse d'un Programme", Cambridge Univ. Press, Cambridge (1997). 1

[15] L. Schneps and P. Lochak (eds.), Geometric Galois actions. 2. The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups, Cambridge Univ. Press, Cambridge (1997). 1

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/