A NEW FAMILY OF EXCEPTIONAL POLYNOMIALS IN CHARACTERISTIC TWO

ROBERT M. GURALNICK, JOEL E. ROSENBERG, AND MICHAEL E. ZIEVE

ABSTRACT. We produce a new family of polynomials $f(X)$ over fields k of characteristic 2 which are exceptional, in the sense that $f(X)-f(Y)$ has no absolutely irreducible factors in $k[X,Y]$ except for scalar multiples of $X-Y$; when k is finite, this condition is equivalent to saying that the map $\alpha \mapsto f(\alpha)$ induces a bijection on an infinite algebraic extension of k. Our polynomials have degree $2^{e-1}(2^e-1)$, where $e>1$ is odd. We also prove that this completes the classification of indecomposable exceptional polynomials of degree not a power of the characteristic.

1. INTRODUCTION

Let k be a field of characteristic $p \geq 0$, let $f(X) \in k[X] \setminus k$, and let $\overline{k}$ be an algebraic closure of k. A polynomial in $k[X,Y]$ is called *absolutely irreducible* if it is irreducible in $\overline{k}[X,Y]$. We say f is *exceptional* if $f(X)-f(Y)$ has no absolutely irreducible factors in $k[X,Y]$ except for scalar multiples of $X-Y$. If k is finite, this condition is equivalent to saying that the map $\alpha \mapsto f(\alpha)$ induces a bijection on an infinite algebraic extension of k [3, 6]. Via this property, exceptional polynomials have been used to construct remarkable examples of various types of objects: curves whose Jacobians have real multiplication [33], Galois extensions of number fields with group $\mathrm{PSL}_2(q)$ [5], maximal curves over finite fields [2, 28], families of character sums with small average value [6], difference sets [9, 11], binary sequences with ideal autocorrelation [9], almost perfect nonlinear power functions [13, 14, 10], bent functions [35, 11], and double-error correcting codes [10].

Trivially any linear polynomial is exceptional. The simplest nontrivial examples are the multiplicative polynomials X^d (which are exceptional when k contains no d-th roots of unity except 1) and the additive polynomials $\sum \alpha_i X^{p^i}$ (which are exceptional when they have no nonzero root in k). Dickson [7] showed that certain variants of these polynomials are also exceptional in some situations: the Dickson polynomials $D_d(X,\alpha)$ (with $\alpha \in k$), which are defined by $D_d(Y+\alpha/Y,\alpha) = Y^d + (\alpha/Y)^d$; and the subadditive polynomials $S(X)$, which satisfy $S(X^m) = L(X)^m$ with L an additive polynomial and m a positive integer. For nearly 100 years, the only known exceptional polynomials were compositions of these classical examples.

We thank the referee for useful advice on notation. The first author was partially supported by NSF grant DMS 0653873.

Klyachko [21] showed that compositions of these polynomials yield all exceptional polynomials of degree not divisible by p, and also all exceptional polynomials of degree p. A vast generalization of this result was proved by Fried, Guralnick and Saxl [15], which greatly restricted the possibilities for the *monodromy groups* of exceptional polynomials. We recall the relevant terminology: let x be transcendental over k. We say $f(X) \in k[X] \setminus k$ is *separable* if the field extension $k(x)/k(f(x))$ is separable, or equivalently $f'(X) \neq 0$. For a separable $f(X) \in k[X]$, let E be the Galois closure of $k(x)/k(f(x))$. The arithmetic monodromy group of f (over k) is $\mathrm{Gal}(E/k(f(x)))$; the geometric monodromy group of f is $\mathrm{Gal}(E/\ell(f(x)))$, where ℓ is the algebraic closure of k in E. If k is finite, then the composition $b \circ c$ of two polynomials $b, c \in k[X]$ is exceptional if and only if both b and c are exceptional [6]. Thus, the study of exceptional polynomials over finite fields reduces to the case of *indecomposable* polynomials, i.e., polynomials which are not compositions of lower-degree polynomials. For extensions of these results to infinite fields and to maps between other varieties, see [18, 19, 22, 24]. Fried, Guralnick and Saxl proved the following result about the monodromy groups of an indecomposable exceptional polynomial [15, 18]:

Theorem 1.1. *Let k be a field of characteristic p, and let $f(X) \in k[X]$ be separable, indecomposable, and exceptional of degree $d > 1$. Let A be the arithmetic monodromy group of f. Then one of the following holds.*

(i) *$d \neq p$ is prime, and A is solvable.*
(ii) *$d = p^e$ and A has a normal elementary abelian subgroup V of order p^e.*
(iii) *$p \in \{2, 3\}$, $d = p^e(p^e - 1)/2$ with $e > 1$ odd, and $A \cong \mathrm{P\Gamma L}_2(p^e) = \mathrm{PGL}_2(p^e) \rtimes \mathrm{Gal}(\mathbb{F}_{p^e}/\mathbb{F}_p)$.*

It remains to determine the polynomials corresponding to these group theoretic possibilities. Case (i) is completely understood: up to compositions with linear polynomials, one just gets the Dickson polynomials $D_d(X, \alpha)$ (see [26, Appendix] or [21]). In case (ii), we have $G = VG_1$ for some G_1; this case includes the additive polynomials (where $G_1 = 1$) and the subadditive polynomials (where G_1 is cyclic). In joint work with Müller [16, 17], we have found families of case (ii) examples in which G_1 is dihedral [16, 17]. Moreover, in all known examples in case (ii), the fixed field E^V has genus zero; conversely, we show in [17] that there are no further examples in which E^V has genus zero or one. We suspect there are no other examples in case (ii): for if E^V has genus $g > 1$ then G_1 will be a group of automorphisms of E^V whose order is large compared to g, and there are not many possibilities for such a field E^V. We hope to complete the analysis of case (ii) in a subsequent paper. The present paper addresses case (iii).

In the two years following [15], examples were found in case (iii) for each $p \in \{2, 3\}$ and each odd $e > 1$ [4, 23, 25]. In the companion paper [20], we show that twists of these examples comprise all examples in case (iii),

except possibly in the following situation: $p = 2$, $G = \mathrm{SL}_2(2^e)$, and the extension $k(x)/k(f(x))$ is wildly ramified over at least two places of $k(f(x))$. In the present paper we conclude the treatment of case (iii) by handling this final ramification setup. In particular, we find a new family of exceptional polynomials. Our main result is the following, in which we say polynomials $b, c \in k[X]$ are *k-equivalent* if there are linear polynomials $\ell_1, \ell_2 \in k[X]$ such that $b = \ell_1 \circ c \circ \ell_2$:

Theorem 1.2. *Let k be a field of characteristic 2. Let $q = 2^e > 2$. For $\alpha \in k \setminus \mathbb{F}_2$, define*

$$f_\alpha(X) := \left(\frac{\mathbb{T}(X) + \alpha}{X}\right)^q \cdot \left(\mathbb{T}(X) + \frac{\mathbb{T}(X) + \alpha}{\alpha + 1} \cdot \mathbb{T}\Big(\frac{X(\alpha^2 + \alpha)}{(\mathbb{T}(X) + \alpha)^2}\Big)\right),$$

where $\mathbb{T}(X) = X^{q/2} + X^{q/4} + \cdots + X$. Then the map $\alpha \mapsto f_\alpha$ defines a bijection from $k \setminus \mathbb{F}_2$ to the set of k-equivalence classes of separable polynomials $f \in k[X]$ of degree $q(q-1)/2$ satisfying

(i) *the geometric monodromy group of f is $\mathrm{SL}_2(q)$; and*
(ii) *the extension $k(x)/k(f(x))$ is wildly ramified over at least two places of $k(f(x))$.*

Every f_α is indecomposable. Moreover, f_α is exceptional if and only if e is odd and $k \cap \mathbb{F}_q = \mathbb{F}_2$.

The strategy of our proof is to identify the curve $\mathcal{C}$ corresponding to the Galois closure E of $k(x)/k(f(x))$, for f a polynomial satisfying (i) and (ii). It turns out that $\mathcal{C}$ is geometrically isomorphic to the smooth plane curve $y^{q+1} + z^{q+1} = \mathbb{T}(yz) + \alpha$.

A key step in our proof is the computation of the automorphism groups of curves of the form $v^q + v = h(w)$, with h varying over a two-parameter family of rational functions. Our method for this computation is rather general, and applies to many families of rational functions h.

As noted above, Theorem 1.2 completes the classification of non-affine indecomposable exceptional polynomials:

Corollary 1.3. *Let k be a field of characteristic $p \geq 0$. Up to k-equivalence, the separable indecomposable exceptional polynomials over k which lie in cases (i) or (iii) of Theorem 1.1 are precisely:*

(i) *for any p, the polynomial X^d where $d \neq p$ is prime and k contains no d-th roots of unity except 1;*
(ii) *for any p, the polynomial*

$$D_d(X, \alpha) := \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-\alpha)^i X^{d-2i}$$

where $d \neq p$ is prime, $\alpha \in k^*$, and k contains no elements of the form $\zeta + 1/\zeta$ with ζ being a primitive d-th root of unity in $\overline{k}$;
(iii) *for $p = 2$ and $q = 2^e > 2$ with e odd and $k \cap \mathbb{F}_q = \mathbb{F}_2$, the polynomial $f_\alpha(X)$ where $\alpha \in k \setminus \mathbb{F}_2$;*

(iv) *for $p = 2$ and $q = 2^e > 2$ with e odd and $k \cap \mathbb{F}_q = \mathbb{F}_2$, the polynomial*

$$X\Big(\sum_{i=0}^{e-1}(\alpha X^n)^{2^i-1}\Big)^{(q+1)/n}$$

where n divides $q+1$ and $\alpha \in k^*$;

(v) *for $p = 3$ and $q = 3^e > 3$ with e odd and $k \cap \mathbb{F}_q = \mathbb{F}_3$, the polynomial*

$$X(X^{2n}-\alpha)^{(q+1)/(4n)}\left(\frac{(X^{2n}-\alpha)^{(q-1)/2}+\alpha^{(q-1)/2}}{X^{2n}}\right)^{(q+1)/(2n)}$$

where n divides $(q+1)/4$ and $\alpha \in k^*$ has image in $k^*/(k^*)^{2n}$ of even order.

The contents of this paper are as follows. In the next section we prove some useful results about ramification groups. In Section 3 we record results from [20] which describe the ramification (including the higher ramification groups) in $E/k(f(x))$. In Section 4 we classify curves which admit B, the group of upper triangular matrices in $\mathrm{SL}_2(q)$, as a group of automorphisms with our desired ramification configuration. There is a two-parameter family of such curves. In Sections 5 and 6 we determine the automorphism groups of the curves in this family (which turn out to be either B or $\mathrm{SL}_2(q)$). The curves with automorphism group $\mathrm{SL}_2(q)$ form a one-parameter subfamily. The group theoretic data yields the existence and uniqueness of the desired polynomials. In particular, it shows we cannot have $k = \mathbb{F}_2$; in Section 9 we give a different, more direct proof of this fact. In the final two sections we consider different forms of the curves, and in particular we determine a smooth plane model. We then use this model to explicitly compute the polynomials, and we conclude the paper by proving Theorem 1.2 and Corollary 1.3.

Notation. Throughout this paper, all curves are assumed to be smooth, projective, and geometrically irreducible. We often define a curve by giving an affine plane model, in which case we mean the completion of the normalization of the stated model. Also, in this case we describe points on the curve by giving the corresponding points on the plane model.

A *cover* is a separable nonconstant morphism between curves. If $\rho\colon \mathcal{C} \to \mathcal{D}$ is a cover of curves over a field k, by a 'branch point' of ρ we mean a point of $\mathcal{D}(\overline{k})$ which is ramified in $\rho \times_k \overline{k}$ (for $\overline{k}$ an algebraic closure of k). In particular, branch points need not be defined over k, but the set of branch points is preserved by the absolute Galois group of k. If $f \in k[X]$ is a separable polynomial, then we refer to the branch points of the corresponding cover $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ as the branch points of f.

If $\rho\colon \mathcal{C} \to \mathcal{D}$ is a Galois cover, and P is a point of $\mathcal{C}$, then the ramification groups at P (in the lower numbering, as in [30]) are denoted $I_0(P), I_1(P), \ldots$, or simply $I_0, I_1, \ldots$. Here I_0 is the inertia group and I_1 is its Sylow p-subgroup. We refer to I_1 as the first ramification group, I_2 as the second, and so on.

We reserve the letter x for an element transcendental over the field k. Throughout this paper we write $q = 2^e$ where $e > 1$. We use the following notation for subgroups of $\mathrm{SL}_2(q)$. The group of diagonal matrices is denoted T. The group of upper triangular matrices is denoted B. The group of elements of B with 1's on the diagonal is denoted U. The two-element group generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is denoted W. Finally, $\mathbb{T}(X)$ denotes the polynomial $X^{q/2} + X^{q/4} + \cdots + X$.

2. Ramification in Galois p-power covers

In this section we prove a useful result (Corollary 2.2) about ramification groups in Galois covers of degree a power of the characteristic. We give two proofs, each of which provides additional information. Throughout this section, $\overline{\ell}$ is an algebraically closed field of characteristic $p > 0$.

Proposition 2.1. *Let $\rho\colon \mathcal{C} \to \mathcal{D}$ and $\rho'\colon \mathcal{C} \to \mathcal{B}$ be Galois covers of curves over $\overline{\ell}$. Let n and r be positive integers. Suppose that $\mathcal{B} \cong \mathbb{P}^1$ and the degree of ρ' is p^r. If all n-th ramification groups of ρ' are trivial, then the same is true of ρ.*

Proof. Since $\mathbb{P}^1$ has no nontrivial unramified covers, and any ramified Galois cover of p-power degree has a nontrivial first ramification group, the hypotheses imply $n \geq 2$. Without loss, we may assume ρ has degree p. First assume $\mathcal{C}$ has genus greater than 1, so that $\operatorname{Aut}\mathcal{C}$ is finite. Let H be a Sylow p-subgroup of $\operatorname{Aut}\mathcal{C}$ which contains $\mathrm{Gal}(\rho')$. By replacing ρ by one of its $(\operatorname{Aut}\mathcal{C})$-conjugates, we may assume that H contains $\mathrm{Gal}(\rho)$ as well. Then the cover $\mathcal{B} \to \mathcal{C}/H$ induced from $\mathcal{C} \to \mathcal{C}/H$ and $\mathcal{C} \to \mathcal{B}$ is the composition of a sequence of Galois degree-p covers $\mathcal{B} = \mathcal{B}_0 \to \mathcal{B}_1 \to \cdots \to \mathcal{B}_m = \mathcal{C}/H$. Since $\mathcal{B} \cong \mathbb{P}^1$, each $\mathcal{B}_i \to \mathcal{B}_{i+1}$ has trivial second ramification groups (by Riemann-Hurwitz). Thus, each n-th ramification group of $\mathcal{C} \to \mathcal{B}_{i+1}$ is also an n-th ramification group of $\mathcal{C} \to \mathcal{B}_i$ (by [30, Prop. IV.3]). By induction, $\mathcal{C} \to \mathcal{B}_m = \mathcal{C}/H$ has trivial n-th ramification groups, whence the same is true of $\mathcal{C} \to \mathcal{D}$.

If $\mathcal{C}$ has genus 0, then ρ is a degree-p cover between genus-0 curves and hence has trivial second ramification groups.

Finally, assume $\mathcal{C}$ has genus 1. Pick a point of $\mathcal{C}$ with nontrivial inertia group under ρ', and let J be an order-p subgroup of this inertia group. Then $\mathcal{C}/J \cong \mathbb{P}^1$, so by replacing $\mathcal{B}$ by $\mathcal{C}/J$ we may assume ρ' has degree p. If $p > 3$ then no such ρ' exists (e.g., by Riemann-Hurwitz). If $p = 3$ then any Galois degree-p map $\mathcal{C} \to \mathcal{D}$ is either unramified (with $\mathcal{D}$ of genus 1) or has a unique branch point (with $I_2 \neq I_3$ and $\mathcal{D}$ of genus 0). Henceforth assume $p = 2$. Then a degree-p map $\mathcal{C} \to \mathcal{D}$ is either unramified (with $\mathcal{D}$ of genus 1) or has precisely two branch points (each with $I_1 \neq I_2$ and $\mathcal{D}$ of genus 0) or has a unique branch point (with $I_3 \neq I_4$ and $\mathcal{D}$ of genus 0). If there is a unique branch point then $\mathcal{C}$ is isomorphic to the curve $y^2 + y = z^3$. Since the corresponding elliptic curve has trivial 2-torsion, it follows that a degree-2

function on this curve cannot have two branch points. This completes the proof. □

We will use the following result, which follows from Proposition 2.1 and standard results about ramification groups (cf. [30, §IV2]).

Corollary 2.2. *Let $\rho\colon \mathcal{C} \to \mathcal{D}$ and $\rho'\colon \mathcal{C} \to \mathbb{P}^1$ be Galois covers of curves over $\overline{\ell}$. Suppose that ρ' has degree a power of p, and that all second ramification groups of ρ' are trivial. If I_1 and I_2 are the first and second ramification groups of ρ at some point of $\mathcal{C}$, then I_1 is elementary abelian, $I_2 = 1$, and I_1 is its own centralizer in I.*

We now give a different proof of this corollary, which generalizes the corollary in a different direction than does Proposition 2.1. For a curve $\mathcal{C}$ over $\overline{\ell}$, let $p_{\mathcal{C}}$ denote the p-rank of $\mathcal{C}$ (i.e., the rank of the p-torsion subgroup of the Jacobian of $\mathcal{C}$). Let $g_{\mathcal{C}}$ denote the genus of $\mathcal{C}$. These quantities are related by $p_{\mathcal{C}} \le g_{\mathcal{C}}$. Recall that $\mathcal{C}$ is called *ordinary* if $p_{\mathcal{C}} = g_{\mathcal{C}}$. We first record a standard basic fact.

Lemma 2.3. *Let $\theta\colon \mathcal{C} \to \mathcal{D}$ be a cover of curves over $\overline{\ell}$. If $\mathcal{C}$ is ordinary, then $\mathcal{D}$ is ordinary.*

This lemma and the next one are proved in [29, Thm. 1.2]. The strategy for proving the next lemma comes from [27, Thm. 2].

Lemma 2.4. *Let $\theta\colon \mathcal{C} \to \mathcal{D}$ be a Galois cover (of curves over $\overline{\ell}$) whose Galois group H is a p-group. Then $\mathcal{C}$ is ordinary if and only if both*

(i) *$\mathcal{D}$ is ordinary; and*
(ii) *every branch point of θ has trivial second ramification group.*

Proof. We use the Deuring-Shafarevich formula ([31, Thm. 4.2]):

$$\frac{p_{\mathcal{C}} - 1}{|V|} = p_{\mathcal{D}} - 1 + \sum_{Q \in \mathcal{D}} \Big(1 - \frac{1}{e_Q}\Big),$$

where e_Q is the ramification index of θ at the point Q.

The Riemann-Hurwitz formula yields

$$\frac{g_{\mathcal{C}} - 1}{|V|} = g_{\mathcal{D}} - 1 + \sum_{Q \in \mathcal{D}} \Big(1 - \frac{1}{e_Q}\Big) + s,$$

where s is the contribution from the second and higher ramification groups. Note that $s \ge 0$, with equality if and only if all second ramification groups are trivial.

Since $p_{\mathcal{D}} \le g_{\mathcal{D}}$, we conclude that $p_{\mathcal{C}} = g_{\mathcal{C}}$ holds if and only if $p_{\mathcal{D}} = g_{\mathcal{D}}$ and $s = 0$. □

Alternate proof of Corollary 2.2. By applying the previous result with $\theta = \rho'$, we see that $\mathcal{C}$ is ordinary. Applying it with $\theta = \rho$ shows that $I_2 = 1$, and then the remaining assertions follow from standard properties of the higher ramification groups. □

Remark. It would be interesting to refine the above alternate proof of Corollary 2.2 to prove Proposition 2.1. Such a refinement would likely require a refinement of the Deuring-Shafarevich formula that involves finer invariants than just the p-rank. However, we do not know such a refined formula. We thank Hendrik Lenstra for suggesting this possibility.

3. Previous results

We will use the following result from the companion paper [20, Lemma 2.7]. Recall our convention that x is transcendental over k; also B is the group of upper triangular matrices in $\mathrm{SL}_2(q)$, and $W = B \cap \mathrm{SL}_2(2)$.

Lemma 3.1. *Let k be a perfect field of characteristic 2, and let $q = 2^e$ with $e > 1$. Suppose $f \in k[X]$ is a separable polynomial of degree $q(q-1)/2$ which satisfies conditions* (i) *and* (ii) *of Theorem 1.2. Let E be the Galois closure of $k(x)/k(f(x))$, and let ℓ be the algebraic closure of k in E. Then $E/\ell(f(x))$ has precisely two ramified places, both of degree one, and the corresponding inertia groups are B and W (up to conjugacy). Moreover, the second ramification group over each ramified place is trivial, and f is indecomposable. The degree $[\ell : k]$ divides e, and f is exceptional if and only if e is odd and $[\ell : k] = e$. Finally, there is a curve $\mathcal{C}_0$ over k such that $\ell.k(\mathcal{C}_0) \cong_\ell E$.*

The following consequence of Lemma 3.1 describes the ramification in $\mathcal{C} \to \mathcal{C}/B$, where $\mathcal{C} = \mathcal{C}_0 \times_k \ell$. This too was proved in the companion paper [20, Cor. 2.8]. Here T is the group of diagonal matrices in $\mathrm{SL}_2(q)$.

Corollary 3.2. *If $\mathcal{C}$ is a curve over ℓ for which $\ell(\mathcal{C}) = E$, then the following hold:*

(i) *B acts as a group of ℓ-automorphisms on $\mathcal{C}$;*
(ii) *the quotient curve $\mathcal{C}/B$ has genus zero;*
(iii) *the cover $\mathcal{C} \to \mathcal{C}/B$ has exactly three branch points;*
(iv) *the inertia groups over these branch points are B, T, and W (up to conjugacy); and*
(v) *all second ramification groups in the cover $\mathcal{C} \to \mathcal{C}/B$ are trivial.*

We now record some standard facts about subgroups of $\mathrm{SL}_2(q)$; see for instance [8, §260], [32, §3.6], or [20, App.]. Here U is the group of elements of B whose diagonal entries are 1.

Lemma 3.3. *$B = U \rtimes T$ is the semidirect product of the normal subgroup U by the cyclic subgroup T. All involutions in B are conjugate. All subgroups of B of order $q-1$ are conjugate. For $j \in \{1, -1\}$, all subgroups of $\mathrm{SL}_2(q)$ of order $2(q+j)$ are conjugate, and these subgroups are dihedral and are maximal proper subgroups of $\mathrm{SL}_2(q)$. The normalizer of W in $\mathrm{SL}_2(q)$ is U. There is no group strictly between B and $\mathrm{SL}_2(q)$.*

4. B-curves

Let ℓ be a perfect field of characteristic 2. In this section we describe the curves $\mathcal{C}$ over ℓ which admit a B-action as in Corollary 3.2. We will show that the only such curves $\mathcal{C}$ are the curves $\mathcal{C}_{\alpha,\beta}$ defined as follows. For any $\alpha, \beta \in \ell^*$, let $\mathcal{C}_{\alpha,\beta}$ be the curve defined by

$$v^q + v = (\alpha+\beta)w + w^q\,\mathbb{T}\Big(\frac{\beta}{1+w^{q-1}}\Big), \tag{4.1}$$

where $\mathbb{T}(X) := X^{q/2} + X^{q/4} + \cdots + X$. Note that $\mathcal{C}_{\alpha,\beta}$ is geometrically irreducible, since the left side of (4.1) is a polynomial in v and the right side is a rational function in w with a simple pole (at $w=\infty$, with residue α).

Theorem 4.2. *Suppose $\mathcal{C}$ is a curve over ℓ satisfying the five properties in Corollary 3.2. Then $\ell \supseteq \mathbb{F}_q$ and $\mathcal{C} \cong \mathcal{C}_{\alpha,\beta}$ for some $\alpha, \beta \in \ell^*$.*

Indeed, suppose $\mathcal{C}$ satisfies the properties of Corollary 3.2. Since the inertia groups B, T, and W are not conjugate, the corresponding branch points are ℓ-rational, so for a suitably chosen coordinate t on $\mathcal{C}/B$ they are ∞, 0, and 1, respectively. Note that $\mathcal{C}/U \to \mathcal{C}/B$ is a cyclic cover of degree $q-1$ which is totally ramified over ∞ and 0, and unramified elsewhere. By Riemann-Hurwitz, $\mathcal{C}/U$ has genus zero. Each of the $q-1$ order-2 subgroups of U is conjugate to W, and is thus an inertia group in $\mathcal{C} \to \mathcal{C}/B$, hence also in $\mathcal{C} \to \mathcal{C}/U$. Thus there must be at least $q-1$ distinct places of $\mathcal{C}/U$ lying over the place $t=1$ of $\mathcal{C}/B$, so all of these places must be rational. Choose a coordinate w on $\mathcal{C}/U$ such that, in the cover $\mathcal{C}/U \to \mathcal{C}/B$, the points ∞, 0, and 1 map to ∞, 0, and 1, respectively. Then $\ell(\mathcal{C}/U) = \ell(w)$ and $\ell(\mathcal{C}/B) = \ell(t)$ where $t = w^{q-1}$. Since $\mathcal{C}/U \to \mathcal{C}/B$ is Galois, ℓ contains $\mathbb{F}_q$.

In these coordinates, the branch points of the cover $\mathcal{C} \to \mathcal{C}/U$ are ∞ and the $q-1$ elements of $\mathbb{F}_q^*$ (i.e., the points over $t=1$) with the corresponding inertia groups being U and its $q-1$ subgroups of order 2.

Let $\mathcal{C}_1 = \mathcal{C}/H$, where H is a maximal subgroup of U. Since $\mathcal{C} \to \mathcal{C}/U$ has no nontrivial second ramification groups, the same is true of $\mathcal{C}_1 \to \mathcal{C}/U$, so (since ℓ is perfect) $\mathcal{C}_1$ is defined by an equation of the form

$$y^2 + y = \alpha w + \sum_{\zeta \in \mathbb{F}_q^*} \frac{\beta_\zeta \zeta}{w+\zeta} + \gamma \tag{4.3}$$

for some $y \in \ell(\mathcal{C})$ and $\alpha, \beta_\zeta, \gamma \in \ell$. Note that $\alpha \neq 0$ (since $w=\infty$ is a branch point). Clearly $\beta_\zeta \neq 0$ if and only if $w = \zeta$ is a branch point of the cover $\mathcal{C}_1 \to \mathcal{C}/U$, and the latter holds if and only if H does not contain the inertia group of $w=\zeta$ in $\mathcal{C} \to \mathcal{C}/U$. Thus, β_ζ is nonzero for precisely $q/2$ values ζ.

Let Γ be the set of elements $z \in \ell(\mathcal{C})$ for which

$$z^2 + z = \overline{\alpha}(z)w + \sum_{\zeta \in \mathbb{F}_q^*} \frac{\overline{\beta}_\zeta(z)\zeta}{w+\zeta} + \overline{\gamma}(z)$$

with $\overline{\alpha}(z), \overline{\beta}_\zeta(z), \overline{\gamma}(z) \in \ell$. Note that $\overline{\alpha}(z)$, $\overline{\beta}_\lambda(z)$, and $\overline{\gamma}(z)$ are uniquely determined by z, and each of them defines a homomorphism $\Gamma \to \ell$. Let $\Gamma_0 = \Gamma \cap \ell(w)$; considering orders of poles, we see that $\Gamma_0 = \ell$.

Since $B = UT$, restriction to $\mathcal{C}/U$ induces an isomorphism $T \cong B/U$, so $T = \{\phi_\eta : \eta \in \mathbb{F}_q^*\}$ where $\phi_\eta(w) = \eta w$. Clearly Γ is T-invariant. The following lemma enables us to choose y so that $Ty \cup \{0\}$ is a group.

Lemma 4.4. *There exists an order-q subgroup Γ_1 of Γ such that $\Gamma = \Gamma_0 \oplus \Gamma_1$ and the nonzero elements of Γ_1 comprise a single T-orbit.*

Proof. The map $\theta\colon z + \Gamma_0 \mapsto \ell(w, z)$ defines a surjective T-set homomorphism between $\Gamma/\Gamma_0 \setminus \{0\}$ and the set Λ of degree-2 extensions of $\ell(\mathcal{C}/U)$ contained in $\ell(\mathcal{C})$. We first prove injectivity of θ: suppose $z_1, z_2 \in \Gamma \setminus \Gamma_0$ satisfy $\ell(w, z_1) = \ell(w, z_2)$. Then the nonidentity element of $\mathrm{Gal}(\ell(w, z_1)/\ell(w))$ maps $z_1 \mapsto z_1 + 1$ and $z_2 \mapsto z_2 + 1$, hence fixes $z_1 + z_2$, so $z_1 + z_2 \in \Gamma_0 = \ell$. Hence θ is injective. Since Λ is a transitive T-set of size $q-1$, it follows that $|\Gamma/\Gamma_0| = q$ and T acts transitively on $\Gamma/\Gamma_0 \setminus \{0\}$. Finally, since $|T|$ is odd and both Γ and Γ_0 are T-invariant elementary abelian 2-groups, Maschke's theorem ([1, 12.9]) implies there is a T-invariant group Γ_1 such that $\Gamma = \Gamma_0 \oplus \Gamma_1$, and $|\Gamma_1| = |\Gamma/\Gamma_0| = q$. □

By replacing y by $y + \delta$ for some $\delta \in \Gamma_0$, we may assume that y is in Γ_1. Applying ϕ_η to (4.3), we see that $y_\eta := \phi_\eta(y)$ satisfies

$$y_\eta^2 + y_\eta = \alpha\eta w + \sum_{\zeta \in \mathbb{F}_q^*} \frac{\beta_\zeta \eta^{-1}\zeta}{w + \eta^{-1}\zeta} + \gamma.$$

Thus, $\overline{\gamma}(y_\eta) = \gamma$ and $\overline{\alpha}(y_\eta) = \alpha\eta$ and $\overline{\beta}_{\eta^{-1}\zeta}(y_\eta) = \beta_\zeta$. Since the homomorphism $z \mapsto \overline{\gamma}(z)$ is constant on the nonzero elements of the group Γ_1, it follows that $\gamma = 0$.

Since $\Gamma_1 = \{y_\eta\} \cup \{0\}$ is closed under addition, $y_\eta + y_{\eta'} = y_{\eta''}$ for some η''. Comparing images under $\overline{\alpha}$ yields that

$$y_\eta + y_{\eta'} = y_{\eta+\eta'}.$$

Thus,

$$\beta_\zeta + \beta_\eta = \overline{\beta}_1(y_\zeta) + \overline{\beta}_1(y_\eta) = \overline{\beta}_1(y_{\zeta+\eta}) = \beta_{\zeta+\eta}.$$

Since $\beta_\zeta = 0$ for exactly $q/2 - 1$ choices of $\zeta \in \mathbb{F}_q^*$, this implies that $\beta_\zeta = 0$ for ζ in some hyperplane (i.e., index-2 subgroup) $\mathcal{H}$ of $\mathbb{F}_q$, and $\beta_\zeta = \beta_{\zeta'}$ for $\zeta, \zeta' \notin \mathcal{H}$. Hence, $\overline{\beta}_\zeta(y_\eta) = 0$ for $\zeta \in \eta^{-1}\mathcal{H}$. The hyperplanes $\eta^{-1}\mathcal{H}$ comprise all $q-1$ hyperplanes in $\mathbb{F}_q$, so there is some η for which $\eta^{-1}\mathcal{H}$ is the set of

roots of $\mathbb{T}(X) := X^{q/2} + X^{q/4} + \cdots + X$. Replacing y by y_η, the equation for $\mathcal{C}_1$ becomes

$$y^2 + y = \alpha w + \beta \sum_{\zeta \in \mathbb{F}_q^*} \frac{\mathbb{T}(\zeta)\zeta}{w + \zeta}.$$

Note that α and β are nonzero elements of ℓ.

Since $\ell(\mathcal{C})$ is the Galois closure of $\ell(\mathcal{C}_1)/\ell(w^{q-1})$, it is uniquely determined by the choice of α and β. Thus, to conclude the proof of Theorem 4.2, it suffices to show that (for each choice of $\alpha, \beta \in \ell^*$) the curve $\mathcal{C}_{\alpha,\beta}$ satisfies the hypotheses of the theorem, and that the quotients of $\mathcal{C}_{\alpha,\beta}$ by B and by some order-$q/2$ subgroup induce the above cover $\mathcal{C}_1 \to \mathbb{P}^1_{w^{q-1}}$. The following lemma is clear:

Lemma 4.5. *If ℓ contains $\mathbb{F}_q(\alpha, \beta)$, then for any $\left(\begin{smallmatrix} \gamma^{-1} & \delta \\ 0 & \gamma \end{smallmatrix}\right) \in B$ there is a unique ℓ-automorphism of $\mathcal{C}_{\alpha,\beta}$ mapping $w \mapsto \gamma^2 w$ and $v \mapsto \gamma^2 v + \gamma\delta$. This correspondence defines an embedding $B \hookrightarrow \mathrm{Aut}_\ell(\mathcal{C}_{\alpha,\beta})$.*

We now show that $\mathcal{C}_{\alpha,\beta}$ (together with this action of B) has the desired properties.

Lemma 4.6. *The curve $\mathcal{C} := \mathcal{C}_{\alpha,\beta}$ has genus $q(q-1)/2$. Moreover, the fixed fields $\ell(\mathcal{C})^U$ and $\ell(\mathcal{C})^B$ equal $\ell(w)$ and $\ell(w^{q-1})$, and the cover $\mathcal{C} \to \mathcal{C}/B$ has precisely three branch points. The inertia groups over these points are (up to conjugacy) B, T, and W. Also, the second ramification groups at all three points are trivial. Finally, if $H = \{\left(\begin{smallmatrix} 1 & \delta \\ 0 & 1 \end{smallmatrix}\right) : \mathbb{T}(\delta) = 0\}$, then $\ell(\mathcal{C})^H = \ell(w, y)$ where*

$$y^2 + y = \alpha w + \beta \sum_{\zeta \in \mathbb{F}_q^*} \frac{\mathbb{T}(\zeta)\zeta}{w - \zeta}. \tag{4.7}$$

Proof. It is clear that $\ell(\mathcal{C})^U = \ell(w)$ and $\ell(\mathcal{C})^B = \ell(t)$, where $t := w^{q-1}$. Also, both w and $\overline{y} := \mathbb{T}(v)$ are fixed by H, and a straightforward calculation yields

$$\overline{y}^2 + \overline{y} = (\alpha + \beta)w + w^q\, \mathbb{T}\Big(\frac{\beta}{t+1}\Big) = \alpha w + \beta \sum_{\zeta \in \mathbb{F}_q^*} \frac{\mathbb{T}(\zeta)\zeta}{w - \zeta} + h + h^2$$

for an appropriate $h \in \ell(w)$. Thus, H fixes w and $y := \overline{y} + h$, and y satisfies (4.7). Since $y \notin \ell(w)$, it follows that $\ell(\mathcal{C})^H = \ell(w, y)$. Note that the genus of $\ell(w, y)$ is $q/2$, since the right hand side of (4.7) has precisely $1 + q/2$ poles and they are all simple.

Let $\mathcal{D} = \mathcal{C}/U$ and $\mathcal{B} = \mathcal{C}/B$, so $\ell(\mathcal{D}) = \ell(w)$ and $\ell(\mathcal{B}) = \ell(t)$. The cover $\mathcal{D} \to \mathcal{B}$ is only ramified at $w = 0$ and $w = \infty$, and is totally ramified at both of these points. The cover $\mathcal{C} \to \mathcal{D}$ can only be ramified at points with $v = \infty$, hence at points with $w \in \mathbb{F}_q^*$ or $w = \infty$. The point $w = \infty$ of $\mathcal{D}$ is totally ramified in $\mathcal{C} \to \mathcal{D}$, since w is a simple pole of the right hand side of (4.1). The points $w \in \mathbb{F}_q^*$ of $\mathcal{D}$ all lie over the point $t = 1$ of $\mathcal{B}$, and precisely $q/2$ of these points are ramified in $\mathcal{C}/H \to \mathcal{D}$. Since T permutes transitively both the $q-1$ points in $\mathcal{D}$ over $t = 1$ and the $q-1$ index-2 subgroups of U, we see

that each such point ramifies in precisely $q/2$ of the covers $\mathcal{C}/V \to \mathcal{D}$ as V ranges over the $q-1$ index-2 subgroups of U. This implies that each $w \in \mathbb{F}_q^*$ has ramification index 2 in $\mathcal{C} \to \mathcal{D}$. Thus, the only branch points of the cover $\mathcal{C} \to \mathcal{C}/B$ are ∞, 0, and 1, and the corresponding ramification indices are $q(q-1)$, $q-1$, and 2. Hence, up to conjugacy, the corresponding inertia groups are B, T, and W. Moreover, since the second ramification groups of $\mathcal{C}/H \to \mathcal{D}$ are trivial, the same is true of every $\mathcal{C}/V \to \mathcal{D}$, and hence of $\mathcal{C} \to \mathcal{D}$. It follows from Riemann-Hurwitz that $\mathcal{C}$ has genus $q(q-1)/2$. □

This concludes the proof of Theorem 4.2.

5. Automorphism groups of B-curves

Let $\overline{\ell}$ be an algebraically closed field of characteristic 2, let $\alpha, \beta \in \overline{\ell}^*$, and put $\mathcal{C} := \mathcal{C}_{\alpha,\beta}$ as in (4.1). By Lemma 4.6, $\mathcal{C}$ admits an action of B satisfying the five properties of Corollary 3.2. In this section we prove that the automorphism group of $\mathcal{C}$ is either B or $\mathrm{SL}_2(q)$.

Let P_1, P_2, and P_3 be points of $\mathcal{C}$ whose stabilizers (in B) are B, W, and T, respectively. Let $\mathcal{G}$ be the automorphism group of $\mathcal{C}$.

Lemma 5.1. *Let $V \le U$ be a subgroup with $|V| > 2$. Then $N_{\mathcal{G}}(V) \le B$ and $|\mathcal{G} : B|$ is odd. Moreover, B is the stabilizer of P_1 in $\mathcal{G}$.*

Proof. Let $\overline{B}$ be the stabilizer of P_1 in $\mathcal{G}$, and let $\overline{U}$ be the Sylow 2-subgroup of $\overline{B}$. Corollary 2.2 implies that $\overline{U}$ is elementary abelian and that $\mathcal{C} \to \mathcal{C}/\overline{U}$ has trivial second ramification groups.

Write $|\overline{U}| = q\overline{q}$. Since the $q-1$ order-2 subgroups of U are all conjugate under B, they are all inertia groups in $\mathcal{C} \to \mathcal{C}/U$. These subgroups are nonconjugate in the abelian group $\overline{U}$, so $\mathcal{C} \to \mathcal{C}/\overline{U}$ has at least $q-1$ distinct branch points not lying under P_1. By Riemann-Hurwitz, $2(q\overline{q} + q(q-1)/2 - 1) = \sum_Q \mathrm{ind}(Q)$ where Q varies over the branch points of $\mathcal{C} \to \mathcal{C}/\overline{U}$ and $\mathrm{ind}(Q)$ is the sum of the different exponents (in the cover $\mathcal{C} \to \mathcal{C}/\overline{U}$) of the points over Q. If Q lies under P_1, then Q is totally ramified so $\mathrm{ind}(Q) = 2(q\overline{q}-1)$. Any branch point satisfies $\mathrm{ind}(Q) \ge q\overline{q}$ (since $\mathcal{C} \to \mathcal{C}/\overline{U}$ is a Galois cover with Galois group a 2-group). Thus,

$$2\Big(q\overline{q} + \frac{q(q-1)}{2} - 1\Big) \ge 2(q\overline{q} - 1) + (q-1)q\overline{q},$$

or $q(q-1) \ge (q-1)q\overline{q}$. Hence $\overline{q} = 1$, so $\overline{U} = U$.

By Corollary 2.2, U is its own centralizer in $\overline{B}$, so conjugation induces a faithful action of $\overline{B}/U$ on U and thus also on $U \setminus \{0\}$. Since $\overline{B}/U$ is cyclic, it follows that $|\overline{B}/U| \le |U \setminus \{0\}| = |B/U|$, so $\overline{B} = B$.

Since we know the inertia groups of $\mathcal{C} \to \mathcal{C}/B$, we see that P_1 is the only point of $\mathcal{C}$ fixed by V. Thus, $N_{\mathcal{G}}(V)$ fixes P_1, so $N_{\mathcal{G}}(V) \le B$. In particular, $N_{\mathcal{G}}(U) = N_B(U) = B$. If U is not a full Sylow 2-subgroup of $\mathcal{G}$, then (since 2-groups are nilpotent) $|N_{\mathcal{G}}(U) : U|$ is even, a contradiction. Thus, $|\mathcal{G} : B|$ is odd. □

Lemma 5.2. *The following are equivalent:*

(i) $\mathcal{G} = B$;
(ii) P_1 *and* P_3 *are in distinct* $\mathcal{G}$*-orbits;*
(iii) $T = N_{\mathcal{G}}(T)$*; and*
(iv) $|N_{\mathcal{G}}(T) : T| \neq 2$.

Proof. By Lemma 5.1, the intersection of the stabilizers (in $\mathcal{G}$) of P_1 and P_3 is T. Since distinct B-conjugates of T intersect trivially, any nontrivial element of T fixes precisely two points of $\mathcal{C}$ (namely P_1 and P_3). Thus, $N_{\mathcal{G}}(T)$ preserves $\Lambda := \{P_1, P_3\}$, so either it acts transitively on Λ (and $|N_{\mathcal{G}}(T) : T| = 2$) or else $N_{\mathcal{G}}(T) = T$. Hence conditions (iii) and (iv) are equivalent, and they both follow from (ii). If $\nu P_3 = P_1$ with $\nu \in \mathcal{G}$, then T^ν is contained in B, so $T^\nu = T^\mu$ for some $\mu \in B$; but then $\mu^{-1}\nu \in N_{\mathcal{G}}(T) \setminus T$. Hence (ii) and (iii) are equivalent.

Clearly if $\mathcal{G} = B$, all the remaining conditions are true. So we assume the last three conditions and show that $\mathcal{G} = B$.

Suppose P_1 and P_3 are in distinct $\mathcal{G}$-orbits. Let I be the stabilizer of P_3 in $\mathcal{G}$, so $I = V\overline{T}$ where V is a normal 2-subgroup and $\overline{T}$ is a cyclic group of odd order. Since I contains T, by Schur-Zassenhaus T is contained in an I-conjugate $\overline{T}'$ of $\overline{T}$, so $I = V\overline{T}'$. Since $\overline{T}'$ is cyclic, it normalizes T, so (by (iii)) $\overline{T}' = T$. Since U is a Sylow 2-subgroup of $\mathcal{G}$ (Lemma 5.1), some conjugate V' of V is contained in U; by our hypothesis on the inertia groups of $\mathcal{C} \to \mathcal{C}/B$, either $|V| \leq 2$ or $V' = U$. But $V' \neq U$ because P_1 and P_3 are in distinct $\mathcal{G}$-orbits, and $|V| \neq 2$ since $|I : T| = 2$ contradicts (iii). Hence $I = T$. Since any nontrivial element of T fixes no point of $\mathcal{G}P_3 \setminus \{P_3\}$, it follows that $\mathcal{G}$ acts on $\mathcal{G}P_3$ as a Frobenius group with Frobenius complement T; let K be the Frobenius kernel. Since K is a normal subgroup of $\mathcal{G}$ that contains a Sylow 2-subgroup, K contains every Sylow 2-subgroup, so $U \leq K$. By Lemma 5.1, $N_{\mathcal{G}}(U) = B$, so $N_K(U) = B \cap K = U$. Nilpotence of the Frobenius kernel implies $K = U$, so $\mathcal{G} = KT = B$. □

Lemma 5.3. W *is the stabilizer of* P_2 *in* $\mathcal{G}$.

Proof. Let $\hat{W}$ be the stabilizer of P_2 in $\mathcal{G}$. Let $\overline{W}$ be the Sylow 2-subgroup of $\hat{W}$. By Corollary 2.2, $\overline{W}$ is elementary abelian and is its own centralizer in $\hat{W}$. Thus, $\hat{W}/\overline{W}$ embeds in $\mathrm{Aut}(\overline{W})$. If $\overline{W} = W$, this implies that $\hat{W} = W$. Now assume that $\overline{W}$ strictly contains W; we will show that this leads to a contradiction. Note that Lemma 5.2 implies $P_3 \in \mathcal{G}P_1$.

Let C be the centralizer of W in $\mathcal{G}$. Then C contains U and $\overline{W}$, where $\overline{W} \cap U = W$. Let $\Lambda = CP_2$. Since W and C commute, W acts trivially on Λ, so $\Lambda \subseteq \{P_1\} \cup UP_2$. But U is a Sylow 2-subgroup of $\mathcal{G}$, so it contains a conjugate $\overline{W}^\nu$ of $\overline{W}$ in $\mathcal{G}$, and since $|\overline{W}| > 2$ we must have $\nu P_2 = P_1$. Hence $\Lambda = \{P_1\} \cup UP_2$. The stabilizer of P_1 in $\mathcal{G}$ is B, and the stabilizer in B of any element of UP_2 is W. Thus any two-point stabilizer of C on Λ is conjugate in C to W, hence equals W, so C/W is a Frobenius group on Λ. A Frobenius complement is U/W (since $B \cap C = U$). It is well known (and

elementary in this case: cf. [12, Thm. 3.4A]) that an abelian subgroup of a Frobenius complement must be cyclic. Hence U/W is cyclic, so $q = 4$. In this case C/W is dihedral of order 6, so (since C contains U) the group C is dihedral of order 12.

Let T' be the order-3 subgroup of C. Since T' is normal in C, no subgroup of C properly containing T' can be an inertia group in $\mathcal{C} \to \mathcal{C}/C$ (by Corollary 2.2). Thus, every orbit of C/T' on the set Γ of fixed points of T' is regular, so $|\Gamma|$ is divisible by 4. Since T fixes precisely two points of $\mathcal{C}$, it follows that T' and T are not conjugate in $\mathcal{G}$, so a Sylow 3-subgroup of $\mathcal{G}$ is noncyclic, and thus contains an elementary abelian subgroup of order 9 [1, 23.9]. By Lemma 4.6, $\mathcal{C}$ has genus $q(q-1)/2 = 6$. But Riemann-Hurwitz shows that (in characteristic not 3) an elementary abelian group of order 9 cannot act on a genus-6 curve, contradiction. □

Theorem 5.4. *If $\mathcal{G} \neq B$ then $\mathcal{G} = \mathrm{SL}_2(q)$ and $\mathcal{C} \to \mathcal{C}/\mathcal{G}$ has precisely two branch points, with inertia groups B and W.*

Proof. Assume that $\mathcal{G} \neq B$. Consider the cover $\mathcal{C} \to \mathcal{C}/\mathcal{G}$. By Lemmas 5.1 and 5.3, the inertia groups of P_1 and P_2 in this cover are B and W, respectively. Since these groups are nonconjugate, P_1 and P_2 lie over distinct branch points Q_1 and Q_2. By Lemma 4.6 and Corollary 2.2, every branch point of $\mathcal{C} \to \mathcal{C}/\mathcal{G}$ has trivial second ramification group.

For a point Q of $\mathcal{C}/\mathcal{G}$, let $\mathrm{ind}(Q)$ denote the sum of the different exponents (in the cover $\mathcal{C} \to \mathcal{C}/\mathcal{G}$) of the points lying over Q. Note that $\mathrm{ind}(Q_1)/|\mathcal{G}| = 1 - 2/|B| + |U|/|B| = 1 + (q-2)/|B|$ and $\mathrm{ind}(Q_2) = |\mathcal{G}|$. The Riemann-Hurwitz formula gives

$$\begin{aligned} q(q-1) - 2 &= -2|\mathcal{G}| + \mathrm{ind}(Q_1) + \mathrm{ind}(Q_2) + \sum_{Q \notin \{Q_1, Q_2\}} \mathrm{ind}(Q) \\ &= (q-2)|\mathcal{G} : B| + \sum_{Q} \mathrm{ind}(Q); \end{aligned}$$

since any branch point Q satisfies $\mathrm{ind}(Q) \geq 2|\mathcal{G}|/3 > q(q-1)$, it follows that Q_1 and Q_2 are the only branch points in $\mathcal{C} \to \mathcal{C}/\mathcal{G}$, and we must have $|\mathcal{G} : B| = q + 1$.

By Lemma 5.2, T has index 2 in $H := N_{\mathcal{G}}(T)$. Thus H preserves the set $\{P_1, P_3\}$ of fixed points of T. Lemma 5.2 implies $P_1 \in \mathcal{G}P_3$, so $|\mathcal{G}P_3| = |\mathcal{G}P_1| = |\mathcal{G} : B| = q + 1$. Since $|BP_3| = q$, it follows that $\mathcal{G}P_3 = BP_3 \cup \{P_1\}$. Pick an involution $\nu \in H$. If ν fixes P_1 then Lemma 5.1 implies $\nu \in B$; but ν must also fix P_3, which is impossible since the stabilizer of P_3 in B is T (and T contains no involutions). Thus ν must swap P_1 and P_3. By Lemma 5.1, U is a Sylow 2-subgroup of $\mathcal{G}$; since all involutions of U are conjugate in B, it follows that ν is conjugate in $\mathcal{G}$ to the nonidentity element of W, and thus fixes a unique point of $\mathcal{G}P_1$.

The orbits of B on $\Lambda := \mathcal{G}P_1$ are the fixed point P_1 and the q-element orbit BP_3. Since B has a unique conjugacy class of index-q subgroups, this

determines Λ as a B-set. The same orbit sizes occur in the action of B on $\mathbb{P}^1(\mathbb{F}_q)$ induced by the usual action of $\mathrm{PSL}_2(q)$ on $\mathbb{P}^1(\mathbb{F}_q)$. Thus, Λ and $\mathbb{P}^1(\mathbb{F}_q)$ are isomorphic B-sets. We will show below that, up to T-conjugacy, there is a unique involution in the symmetric group of Γ which normalizes T and has a unique fixed point. Since $\mathrm{SL}_2(q)$ contains such an involution, we can extend our isomorphism of B-sets $\Lambda \cong_B \mathbb{P}^1(\mathbb{F}_q)$ to an isomorphism of $\langle B, \nu\rangle$-sets, and in particular $\mathrm{SL}_2(q)$ has a subgroup isomorphic to $\langle B, \nu\rangle$. Since B is a maximal subgroup of $\mathrm{SL}_2(q)$, we have $\langle B, \nu\rangle \cong \mathrm{SL}_2(q)$, whence (since $|\mathcal{G}| \le |\mathrm{SL}_2(q)|$) we conclude $\mathcal{G} \cong \mathrm{SL}_2(q)$.

It remains to show that, up to T-conjugacy, there is a unique involution $\hat{\nu}$ in the symmetric group of Λ which normalizes T and has a unique fixed point. Note that T fixes P_1 and P_3, and T is transitive on the other $q-1$ points of Λ. Thus $\hat{\nu}$ permutes $\{P_1, P_3\}$, and the fixed point hypothesis implies $\hat{\nu}$ interchanges P_1 and P_3. Hence $\hat{\nu}$ fixes a unique point of TP_3, so we may may identify this orbit with T and assume the fixed point is $1 \in T$. The only order-2 automorphism of T with no nontrivial fixed points is the automorphism inverting all elements of T, whence $\hat{\nu}$ is unique up to T-conjugacy. □

6. G-curves and hyperelliptic quotients

Let $\overline{\ell}$ be an algebraically closed field of characteristic 2, let $\alpha, \beta \in \overline{\ell}^*$, and let $\mathcal{C} := \mathcal{C}_{\alpha,\beta}$ be as in (4.1). We use the embedding $B \to \mathrm{Aut}\,\mathcal{C}$ from Lemma 4.5. By Theorem 5.4, the automorphism group of $\mathcal{C}$ is either B or $G := \mathrm{SL}_2(q)$. In this section we determine when the latter occurs.

Proposition 6.1. *$\mathcal{C}$ has automorphism group G if and only if $\beta^2 = \alpha + \alpha^2$.*

Set $t := w^{q-1}$ and $y := v/w$. Since T fixes t and y, we have $\overline{\ell}(t,y) \subseteq \overline{\ell}(v,w)^T = \overline{\ell}(\mathcal{C}/T)$. Clearly w has degree at most $q-1$ over $\overline{\ell}(t,y)$, and also $\overline{\ell}(v,w) = \overline{\ell}(y,w)$. Thus, $\overline{\ell}(\mathcal{C}/T) = \overline{\ell}(t,y)$.

The curve $\mathcal{C}/T$ is defined by the equation

$$y^q + \frac{y}{t} = \frac{\alpha+\beta}{t} + \mathbb{T}\Big(\frac{\beta}{t+1}\Big),$$

which is irreducible because $[\overline{\ell}(y,t) : \overline{\ell}(t)] = q$. Putting

$$z := y^2 + y + \frac{\beta}{t+1},$$

we compute

$$\mathbb{T}(z) = y^q + y + \mathbb{T}\Big(\frac{\beta}{t+1}\Big) = y\Big(1 + \frac{1}{t}\Big) + \frac{\alpha+\beta}{t},$$

and thus

$$y = \frac{t\,\mathbb{T}(z) + \alpha + \beta}{t+1}.$$

It follows that

Lemma 6.2. *$\overline{\ell}(\mathcal{C}/T) = \overline{\ell}(t,z)$ and $\overline{\ell}(\mathcal{C}) = \overline{\ell}(w,z)$.*

Our next result gives further information about $\mathcal{C}/T$.

Lemma 6.3. *$\mathcal{C}/T$ is hyperelliptic of genus $q/2$, and the hyperelliptic involution ν fixes z and maps $t \mapsto (\alpha^2+\alpha+\beta^2+z)/(z^q t)$.*

Proof. Substituting our expression for y (in terms of t and $\mathbb{T}(z)$) into the definition of z gives

$$z = \frac{(t\,\mathbb{T}(z)+\alpha+\beta)^2 + (t\,\mathbb{T}(z)+\alpha+\beta)(t+1) + \beta(t+1)}{(t+1)^2},$$

so $0 = t^2 z^q + t(\mathbb{T}(z)+\alpha) + (z+\alpha^2+\alpha+\beta^2)$. By considering the order of the pole at the point $z=\infty$ in this equation, we see that $t \notin \overline{\ell}(z)$. Thus, $[\overline{\ell}(t,z) : \overline{\ell}(z)] = 2$. Our hypothesis on the ramification in $\mathcal{C} \to \mathcal{C}/B$ implies that $\overline{\ell}(t,z)$ has genus $q/2$. Hence $\mathcal{C}/T$ is hyperelliptic, and the hyperelliptic involution ν fixes z and maps $t \mapsto (\alpha^2+\alpha+\beta^2+z)/(z^q t)$. □

Suppose in this paragraph that $\mathrm{Aut}_{\overline{\ell}}(\mathcal{C}) \cong G$, and choose the isomorphism so that it extends our previous embedding $B \hookrightarrow \mathrm{Aut}_{\overline{\ell}}(\mathcal{C})$. By Theorem 5.4, there are points P_1, P_2 on $\mathcal{C}$ whose stabilizers in G are B and W, respectively, and moreover the corresponding points Q_1, Q_2 on $\mathcal{C}/G$ are the only two branch points of $\mathcal{C} \to \mathcal{C}/G$. By Lemma 5.2, $H := N_G(T)$ has order $2(q-1)$, so Lemma 3.3 implies H is dihedral, hence contains $q-1$ involutions. But all involutions in G are conjugate, and each fixes $q/2$ points of GP_2, so $\mathcal{C}/T \to \mathcal{C}/H$ is ramified over $q/2$ points lying over Q_2. Likewise, $\mathcal{C}/T \to \mathcal{C}/H$ is ramified over a unique point lying over Q_1, so $\mathcal{C}/T \to \mathcal{C}/H$ has $1+q/2$ branch points and thus (since $\mathcal{C}/T$ has genus $q/2$) we find that $\mathcal{C}/H$ has genus zero. By uniqueness of the hyperelliptic involution, we must have $\overline{\ell}(\mathcal{C})^H = \overline{\ell}(z)$, and each element $\mu \in H \setminus T$ is an involution whose restriction to $\mathcal{C}/T$ is the hyperelliptic involution ν. Now, $(w\mu(w))^{q-1} = t\rho(t) = (\alpha^2+\alpha+\beta^2+z)/z^q$ is in $\overline{\ell}(z)$, so $\overline{\ell}(w\mu(w), z)/\overline{\ell}(z)$ is cyclic of order dividing $q-1$; but the dihedral group of order $2(q-1)$ has no proper normal subgroups of even order, so $w\mu(w) \in \overline{\ell}(z)$. Thus $(\alpha^2+\alpha+\beta^2+z)/z^q$ is a $(q-1)$-th power in $\overline{\ell}(z)$, so $\beta^2 = \alpha+\alpha^2$.

Conversely, we now assume that $\beta^2 = \alpha^2+\alpha$ (with $\alpha \notin \mathbb{F}_2$, since $\beta \neq 0$). By Lemma 6.2, there are precisely $q-1$ extensions of ν to an embedding of $\overline{\ell}(\mathcal{C})$ into its algebraic closure, one for each $(q-1)$-th root of $\rho(t)$ (this root will be $\rho(w)$). Since $t\rho(t) = 1/z^{q-1}$, each of these extensions maps $w \mapsto \zeta/(zw)$ with $\zeta \in \mathbb{F}_q^*$ and so in particular leaves $\overline{\ell}(\mathcal{C}) = \overline{\ell}(w,z)$ invariant (and thus is an automorphism of $\overline{\ell}(\mathcal{C})$). Since $\mathrm{Aut}_{\overline{\ell}}(\mathcal{C})$ properly contains B, Theorem 5.4 implies that $\mathrm{Aut}_{\overline{\ell}}(\mathcal{C}) \cong \mathrm{SL}_2(q)$. This completes the proof of Proposition 6.1.

7. Forms of $\mathcal{C}_{\alpha,\beta}$

In this section we study isomorphisms between curves of the shape $\mathcal{C}_{\alpha,\beta}$, and isomorphisms between these curves and other curves.

Proposition 7.1. *Let $\overline{\ell}$ be an algebraically closed field of characteristic 2. For $\alpha, \beta, \alpha', \beta' \in \overline{\ell}^*$, the curves $\mathcal{C}_{\alpha,\beta}$ and $\mathcal{C}_{\alpha',\beta'}$ are isomorphic if and only if $\alpha = \alpha'$ and $\beta = \beta'$.*

Proof. Let $\mathcal{C} = \mathcal{C}_{\alpha,\beta}$ and $\mathcal{C}' = \mathcal{C}_{\alpha',\beta'}$, and let $\mathcal{G} = \operatorname{Aut}\mathcal{C}$ and $\mathcal{G}' = \operatorname{Aut}\mathcal{C}'$. Write the equations of $\mathcal{C}$ and $\mathcal{C}'$ as $v^q+v = (\alpha+\beta)w+w^q\,\mathbb{T}(\beta/(1+w^{q-1}))$ and $(v')^q+v' = (\alpha'+\beta')w'+(w')^q\,\mathbb{T}(\beta'/(1+(w')^{q-1}))$, respectively. Suppose there is an isomorphism $\rho\colon \mathcal{C} \to \mathcal{C}'$. Conjugation by ρ induces an isomorphism $\theta\colon \mathcal{G} \to \mathcal{G}'$. By replacing ρ by its compositions with automorphisms of $\mathcal{C}$ and $\mathcal{C}'$, we can replace θ by its compositions with arbitrary inner automorphisms of $\mathcal{G}$ and $\mathcal{G}'$.

We use the embeddings $B \to \mathcal{G}$ and $B \to \mathcal{G}'$ from Lemma 4.5. By Lemma 5.1, U is a Sylow 2-subgroup of $\mathcal{G}$ and $\mathcal{G}'$, so (by composing ρ with automorphisms) we may assume $\theta(U) = U$. Since all index-2 subgroups of U are conjugate under B, we may assume in addition that $\theta(H) = H$ where H is a prescribed index-2 subgroup of U. Then ρ induces an isomorphism between $\mathcal{C}/U$ and $\mathcal{C}'/U$ which maps the set of branch points of $\mathcal{C}/H \to \mathcal{C}/U$ to the corresponding set in $\mathcal{C}'/U$. For definiteness, choose H to be the subgroup defined in Lemma 4.6, and choose the coordinates w and w' on $\mathcal{C}/U$ and $\mathcal{C}'/U$. The branch points of each of $\mathcal{C}/H \to \mathcal{C}/U$ and $\mathcal{C}'/H \to \mathcal{C}'/U$ (in the coordinates w and w') are $\{\delta : \mathbb{T}(\delta) = 1\} \cup \{\infty\}$.

Since B is the normalizer of U in both $\mathcal{G}$ and $\mathcal{G}'$ (by Lemma 5.1), it follows from $\theta(U) = U$ that $\theta(B) = B$. The only points of $\mathcal{C}/U$ which ramify in $\mathcal{C}/U \to \mathcal{C}/B$ are $w = 0$ and $w = \infty$, so ρ must map these to $w' = 0$ and $w' = \infty$ in some order. Thus, $\rho(w)$ is a constant times either w' or $1/w'$. Since also ρ preserves $\{\delta : \mathbb{T}(\delta) = 1\} \cup \{\infty\}$, we must have $\rho(w) = w'$. Since $\theta(H) = H$ and the right hand side of (4.7) has only simple poles, by applying ρ to this equation we see that $\alpha = \alpha'$ and $\beta = \beta'$. □

Proposition 7.2. *Let k be a perfect field of characteristic 2, and let $\overline{k}$ be an algebraic closure of k. Let $\mathcal{C} = \mathcal{C}_{\alpha,\beta}$ where $\alpha, \beta \in \overline{k}^*$. Let $\mathcal{C}'$ be a curve over k which is isomorphic to $\mathcal{C}$ over $\overline{k}$. Let ℓ be an extension of k such that $\operatorname{Aut}_\ell(\ell(\mathcal{C}')) \cong \operatorname{Aut}_{\overline{k}}(\overline{k}(\mathcal{C}'))$. Then:*

(i) *k contains $\mathbb{F}_2(\alpha, \beta)$;*
(ii) *$\mathcal{C}$ is defined over k; and*
(iii) *$\mathcal{C}$ is isomorphic to $\mathcal{C}'$ over ℓ.*

Proof. Note that $\overline{k}(\mathcal{C}) = \overline{k}(v, w)$ where v, w satisfy

$$v^q + v = (\alpha + \beta)w + w^q\,\mathbb{T}\Big(\frac{\beta}{1 + w^{q-1}}\Big).$$

If ρ is any k-automorphism of $\overline{k}(\mathcal{C})$, then $\overline{k}(\mathcal{C}) = \overline{k}(v_1, w_1)$ where $v_1 := \rho(v)$ and $w_1 := \rho(w)$ satisfy

$$v_1^q + v_1 = (\rho(\alpha) + \rho(\beta))w_1 + w_1^q\,\mathbb{T}\Big(\frac{\rho(\beta)}{1 + w_1^{q-1}}\Big).$$

Thus, $\mathcal{C}_{\alpha,\beta} \cong \mathcal{C}_{\rho(\alpha),\rho(\beta)}$, whence (by the previous result) ρ fixes α and β. Hence $\mathbb{F}_2(\alpha,\beta)$ is fixed by the full group of k-automorphisms of $\overline{k}(\mathcal{C})$.

By hypothesis, there is a $\overline{k}$-isomorphism θ between $\overline{k}(\mathcal{C})$ and $\overline{k}(\mathcal{C}')$. Conjugation by θ induces an isomorphism $\mathrm{Aut}_k(\overline{k}(\mathcal{C})) \cong \mathrm{Aut}_k(\overline{k}(\mathcal{C}'))$, so in particular both of these groups fix the same subfield of $\overline{k}$. Since k is perfect and $\mathcal{C}'$ is defined over k, the subfield of $\overline{k}$ fixed by $\mathrm{Aut}_k(\overline{k}(\mathcal{C}'))$ is just k, so $\mathbb{F}_2(\alpha,\beta) \subseteq k$.

Clearly $\mathcal{C}$ is defined over $\mathbb{F}_2(\alpha,\beta)$, hence over k. Finally, by Theorem 4.2 and Proposition 7.1 there is an ℓ-isomorphism $\ell(\mathcal{C}) \cong \ell(\mathcal{C}')$. □

8. Existence and uniqueness of polynomials

Let k be a perfect field of characteristic 2, and let $q = 2^e > 2$. In this section we prove a preliminary version of Theorem 1.2, in which we describe the Galois closure of $k(x)/k(f(x))$ rather than describing the polynomials f. Here x is transcendental over k, and we say $b, c \in k[X]$ are *k-equivalent* if there are linear polynomials $\ell_1, \ell_2 \in k[X]$ such that $b = \ell_1 \circ c \circ \ell_2$.

Theorem 8.1. *If $f \in k[X]$ is a separable polynomial of degree $(q^2-q)/2$ such that*

(i) *the geometric monodromy group of f is $\mathrm{SL}_2(q)$; and*
(ii) *the extension $k(x)/k(f(x))$ is wildly ramified over at least two places of $k(f(x))$,*

then there is a unique pair $(\alpha,\beta) \in k^* \times k^*$ with $\beta^2 = \alpha + \alpha^2$ for which the Galois closure of $k(x)/k(f(x))$ is isomorphic to $(k.\mathbb{F}_q)(\mathcal{C}_{\alpha,\beta})$. Conversely, each such pair (α,β) actually occurs for some f with these properties, and two such polynomials are k-equivalent if and only if they correspond to the same pair (α,β). Finally, every such f is indecomposable, and f is exceptional if and only if e is odd and $k \cap \mathbb{F}_q = \mathbb{F}_2$.

Our proof uses a corollary of the following simple lemma (cf. [12, Thm. 4.2A]):

Lemma 8.2. *Let G be a transitive permutation group on a set Δ, and let G_1 be the stabilizer of a point $\pi \in \Delta$. Let C be the centralizer of G in the symmetric group on Δ. Then $C \cong N_G(G_1)/G_1$, and C acts faithfully and regularly on the set of fixed points of G_1. In particular, C is trivial if G_1 is self-normalizing in G.*

Proof. Note that an element $\tau \in C$ is determined by the value $\tau(\pi)$ (since $\tau(\nu(\pi)) = \nu(\tau(\pi))$ for every $\nu \in G$).

If G acts regularly on Δ, then we can identify the action of G on Δ with the action of G on itself by left multiplication. Clearly right multiplication commutes with this action, so the map $\tau \mapsto \tau(1)$ induces an isomorphism $C \cong G$, and C acts regularly on Δ.

Let Λ be the set of fixed points of G_1. Then $N_G(G_1)/G_1$ acts regularly on Λ. Letting $\hat{C}$ be the centralizer of $N_G(G_1)$ in $\mathrm{Sym}(\Lambda)$, the previous paragraph shows that $\hat{C} \cong N_G(G_1)/G_1$ acts regularly on Λ. Since C acts

on Λ and C centralizes $N_G(G_1)$, restriction to Λ induces a homomorphism $\theta\colon C \to \hat{C}$. We see that θ is injective, since $\tau \in C$ is determined by $\tau(\pi)$. It remains only to prove that θ is surjective. For $\mu \in \hat{C}$, $\nu \in G$ and $\lambda \in G_1$, note that $\nu(\lambda(\mu(\pi))) = \nu(\mu(\lambda(\pi))) = \nu(\mu(\pi))$; hence the image of $\mu(\pi)$ is constant on each coset in G/G_1, so the map $\nu(\pi) \mapsto \nu(\mu(\pi))$ defines a permutation ϕ of Δ. Plainly ϕ centralizes G and $\theta(\phi) = \mu$, so the proof is complete. □

Corollary 8.3. *Let $f \in k[X]$ be a separable polynomial, let E be the Galois closure of $k(x)/k(f(x))$, and let ℓ be the algebraic closure of k in E. Put $A := \mathrm{Gal}(E/k(f(x)))$, $G := \mathrm{Gal}(E/\ell(f(x)))$, and $G_1 := \mathrm{Gal}(E/\ell(x))$. If $N_G(G_1) = G_1$, then $C_A(G) = 1$.*

Proof of Theorem 8.1. Suppose $f \in k[X]$ is a separable polynomial of degree $(q^2 - q)/2$ which satisfies conditions (i) and (ii) of Theorem 8.1. Let E be the Galois closure of $k(x)/k(f(x))$, and let ℓ be the algebraic closure of k in E. Then there is an ℓ-isomorphism between E and $\ell(\mathcal{C}_{\alpha,\beta})$ for some $\alpha, \beta \in \ell^*$, and also $\ell \supseteq \mathbb{F}_q$ (by Corollary 3.2 and Theorem 4.2). This uniquely determines the pair (α, β) (Proposition 7.1). By Theorem 5.4, the geometric monodromy group $G := \mathrm{Gal}(E/\ell(f(x)))$ equals $\mathrm{Aut}_\ell\, \ell(\mathcal{C}_{\alpha,\beta})$, so Proposition 6.1 implies $\beta^2 = \alpha^2 + \alpha$. By Lemma 3.1 and Proposition 7.2, both α and β are in k. By Lemma 3.3, the hypotheses of the above corollary are satisfied, so no nontrivial element of $\mathrm{Gal}(E/k(f(x)))$ centralizes G. Since every ℓ-automorphism of $\ell(\mathcal{C}_{\alpha,\beta})$ is defined over $k.\mathbb{F}_q$, we see that G commutes with $\mathrm{Gal}(E/(k.\mathbb{F}_q)(\mathcal{C}_{\alpha,\beta}))$, so $L = (k.\mathbb{F}_q)(\mathcal{C}_{\alpha,\beta})$. We have proven the first sentence of Theorem 8.1.

Conversely, suppose $\alpha, \beta \in k^*$ satisfy $\beta^2 = \alpha + \alpha^2$, and put $\ell := k\mathbb{F}_q$. Let $E = \ell(\mathcal{C}_{\alpha,\beta})$. We have shown that $G := \mathrm{Aut}_\ell\, E$ satisfies $G \cong \mathrm{SL}_2(q)$, and that there are degree-one places P_1 and P_2 of E whose stabilizers in G are B and W, respectively. Moreover, E has genus $q(q-1)/2$, and the second ramification groups at P_1 and P_2 are trivial. By Riemann-Hurwitz, the only places of E^G which ramify in E/E^G are the places Q_1 and Q_2 which lie under P_1 and P_2. Let G_1 be a subgroup of G of index $q(q-1)/2$. Then G_1 is dihedral of order $2(q+1)$, and hence contains $q+1$ involutions. Each of the $q+1$ conjugates of U contains precisely one of these involutions. Hence there is a unique place of E^{G_1} lying over Q_1, and its ramification index in E/E^{G_1} is 2. Also there are precisely $q/2$ places of E^{G_1} which lie over Q_2 and ramify in E/E^{G_1}, and each has ramification index 2. Thus E^{G_1} has genus zero, and Q_1 is totally ramified in E^{G_1}/E^G. Next, $A := \mathrm{Aut}_k\, E$ satisfies $A = G.\,\mathrm{Gal}(E/k(\mathcal{C}_{\alpha,\beta}))$. Since G is normal in A, and G_1 is conjugate (in G) to all $(q^2 - q)/2$ subgroups of G having order $2q + 2$, it follows that $|N_A(G_1) : G_1| = |\ell : k|$ and $N_A(G_1)G = A$. Thus, $E^{N_A(G_1)}$ is a genus-zero function field over k which contains a degree-one place that is totally ramified over E^A. We can write $E^{N_A(G_1)} = k(x)$ and $E^A = k(u)$, and by making linear fractional changes in x and u we may assume that the unique place of

$k(x)$ lying over the infinite place of $k(u)$ is the infinite place. In other words, $u = f(x)$ for some $f \in k[X]$. Separability of f follows from separability of $k(x)/k(u)$. The degree of f is $(q^2-q)/2$, and its geometric monodromy group is $\mathrm{SL}_2(q)$ (since G_1 contains no nontrivial normal subgroup of $\mathrm{SL}_2(q)$). The extension $k(x)/k(f(x))$ is totally ramified over infinity, and also is wildly ramified over another place of $k(f(x))$.

Next we show that the Galois closure of $k(x)/k(f(x))$ is E, or equivalently that $N_A(G_1)$ contains no nontrivial normal subgroup of A. Let J be a proper normal subgroup of A. Since G is normal in A (and simple), J must intersect G trivially. Thus each element of J has shape $\nu\sigma$, where $\nu \in G$ and $\sigma \in \mathrm{Gal}(E/k(\mathcal{C}_{\alpha,\beta}))$ satisfy $|\langle\nu\sigma\rangle| = |\langle\sigma\rangle|$. In particular, J is cyclic; let $\nu\sigma$ be a generator of J. Since G and J normalize one another and intersect trivially, they must commute. Write $E = \ell(v, w)$ where $v^q + v = (\alpha+\beta)w + w^q\,\mathbb{T}(\beta/(1+w^{q-1}))$. Let $\tau \in G$ map $(v, w) \mapsto (v+1, w)$. Since τ commutes with both J and σ, it also must commute with ν. Hence ν maps $(v, w) \mapsto (v+\alpha, w)$ for some $\alpha \in \mathbb{F}_q$. For $\zeta \in \mathbb{F}_q^*$, let $\lambda_\zeta \in G$ map $(v, w) \mapsto (\zeta v, \zeta w)$. Then $\lambda_\zeta\nu\sigma(w) = \zeta w$, but $\nu\sigma\lambda_\zeta(w) = \sigma(\zeta)w$, so σ fixes ζ. Hence σ fixes both $\mathbb{F}_q$ and $k(\mathcal{C}_{\alpha,\beta})$, so it fixes E, whence $J = 1$. Thus the arithmetic monodromy group of f is A. Since G has a unique conjugacy class of subgroups of index $(q^2-q)/2$, all of which are self-normalizing, any two index-$(q^2-q)/2$ subgroups of A which surject onto A/G are conjugate. Since $A = \mathrm{Aut}_k E$, it follows that there is a unique k-equivalence class of polynomials f which satisfy all our hypotheses for a given pair (α, β). Conversely, k-equivalent polynomials have isomorphic Galois closures, hence correspond to the same pair (α, β). Finally, the indecomposability and exceptionality criteria follow from Lemma 3.1. □

Corollary 8.4. *There exists a separable polynomial $f \in k[X]$ of degree $q(q-1)/2$ with two wild branch points and geometric monodromy group $\mathrm{SL}_2(q)$ if and only if k properly contains $\mathbb{F}_2$.*

Corollary 8.5. *There exists a separable exceptional polynomial $f \in k[X]$ of degree $q(q-1)/2$ with two wild branch points and geometric monodromy group $\mathrm{SL}_2(q)$ if and only if e is odd, $k \cap \mathbb{F}_q = \mathbb{F}_2$, and k properly contains $\mathbb{F}_2$.*

9. Another nonexistence proof over $\mathbb{F}_2$

One consequence of Corollary 8.4 is that there is no separable polynomial f over $\mathbb{F}_2$ of degree $q(q-1)/2$ such that the cover $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ has at least two wildly ramified branch points and has geometric monodromy group $\mathrm{SL}_2(q)$. In this section we give a more direct proof of this fact, by showing that the Galois closure of such a cover $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ would be a curve having more rational points than is permitted by the Weil bound.

Theorem 9.1. *There is no separable polynomial $f \in \mathbb{F}_2[X]$ of degree $q(q-1)/2$ satisfying the following conditions:*

(i) *the geometric monodromy group of f is $G := \mathrm{SL}_2(q)$;*
(ii) *the extension $\mathbb{F}_2(x)/\mathbb{F}_2(f(x))$ has precisely two branch points, and in the Galois closure $E/\mathbb{F}_2(f(x))$ their ramification indices are $q(q-1)$ and 2; and*
(iii) *all second ramification groups in $E/\mathbb{F}_2(f(x))$ are trivial.*

Remark. By Lemma 3.1, conditions (ii) and (iii) follow from (i) if we assume that f has two wild branch points. Thus, the combination of Theorem 9.1 and Lemma 3.1 implies the 'only if' implication in Corollary 8.4.

Proof. Suppose there is an f satisfying the above conditions. The Riemann-Hurwitz formula implies that the genus of E is $q(q-1)/2$.

Since the two branch points of $E/\mathbb{F}_2(f(x))$ have nonconjugate inertia groups, these points must be $\mathbb{F}_2$-rational. Let Q be the point with ramification index 2.

Let $A := \mathrm{Gal}(E/\mathbb{F}_2(f(x)))$ be the arithmetic monodromy group of f. By Corollary 8.3, $G \le A \le \mathrm{Aut}(G) = \mathrm{SL}_2(q).e$. Thus, $A = G.e'$ for some $e' \mid e$. It follows that the algebraic closure of $\mathbb{F}_2$ in E is $\ell := \mathbb{F}_{2^{e'}}$. Let P be a place of E lying over Q. Let H be the decomposition group of P in the extension $E/\mathbb{F}_2(f(x))$. We know that the inertia group W of P has order 2, so $U := N_G(W)$ has order q. Thus, $H \le N_A(W) = \langle U, \nu \rangle$, where $\nu \in A$ has order e' and maps to a generator of A/G. Since Q is $\mathbb{F}_2$-rational, H/W surjects onto A/G, or equivalently $A = GH$. Since H/W is cyclic, it follows that $|H/W|$ is either e' or $2e'$.

Suppose that $e' < e$. Let $\hat{\ell}$ be the quadratic extension of ℓ. Then $|\hat{\ell}| \le q$. Let $\hat{P}$ be a place of $\hat{\ell}E$ lying over P (there are one or two such places). Since $|H/W|$ divides $[\hat{\ell} : \mathbb{F}_2]$, the place $\hat{P}$ is rational over $\hat{\ell}$. Moreover, the ramification index of $\hat{P}$ in $\hat{\ell}E/\hat{\ell}(f(x))$ is 2. Thus, Q lies under $|G|/2$ rational places of $\hat{\ell}E$. Since $\hat{\ell}E$ has genus $q(q-1)/2$, this violates the Weil bound for the number of rational points on a curve over a finite field.

Now suppose that $e' = e$. As noted above, $H \le N_A(W) = \langle U, \nu \rangle$. For any $\mu \in U$, the element $(\mu\nu)^e \in H$ lies in U and centralizes $\mu\nu$, hence it centralizes ν. However, the centralizer of ν in U is W. Since $|\mathcal{C}_U(\nu)| = 2$, it follows that no element of $N_A(W)/W$ has order $2e$, so H/W is cyclic of order e. Now, as in the previous case, we obtain a contradiction by counting points. □

10. Construction of polynomials

In this section we use the results proved so far in order to compute explicit forms of the polynomials whose existence was proved in Theorem 8.1.

Let k be a perfect field of characteristic 2, and let $q = 2^e > 2$. Let $\alpha, \beta \in k^*$ satisfy $\beta^2 = \alpha + \alpha^2$.

Theorem 10.1. *The polynomial*

$$\hat{f}(X) := (\mathbb{T}(X) + \alpha + 1) \prod_{\substack{\zeta^{q-1}=1 \\ \zeta \neq 1}} \Big(\sum_{i=0}^{e-1} \frac{\zeta^{2^i} + \zeta}{\zeta^{2^i} + 1} X^{2^i} + \zeta\alpha + 1 \Big) \tag{10.2}$$

is in the k-equivalence class corresponding to (α, β) in Theorem 8.1.

Proof. Let $\ell = k.\mathbb{F}_q$ and $E = \ell(\mathcal{C}_{\alpha,\beta})$. Write $E = \ell(v, w)$, where $v^q + v = (\alpha + \beta)w + w^q\, \mathbb{T}(\beta/(1 + w^{q-1}))$.

Let $\hat{w} = 1/w$ and $\hat{v} = v^2/w + v + \beta w/(1 + w^{q-1})$. Then

$$\begin{aligned} \mathbb{T}(\hat{v}\hat{w}) &= \Big(\frac{v}{w}\Big)^q + \frac{v}{w} + \mathbb{T}\Big(\frac{\beta}{1 + w^{q-1}}\Big) \\ &= v\Big(\frac{1}{w} + \frac{1}{w^q}\Big) + \frac{\alpha + \beta}{w^{q-1}}, \end{aligned}$$

so $k(\hat{v}, \hat{w}) = k(v, w)$. Next,

$$\begin{aligned} \hat{v}^q\hat{w} &= \frac{v^{2q}}{w^{q+1}} + \frac{v^q}{w} + \frac{\beta^q w^{q-1}}{1 + w^{q^2-q}} \\ &= \frac{v^2}{w^{q+1}} + \frac{\alpha^2 + \beta^2}{w^{q-1}} + w^{q-1}\, \mathbb{T}\Big(\frac{\beta}{1 + w^{q-1}}\Big)^2 + \frac{v}{w} + \alpha + \beta \\ &\qquad + w^{q-1}\, \mathbb{T}\Big(\frac{\beta}{1 + w^{q-1}}\Big) + \frac{\beta^q w^{q-1}}{1 + w^{q^2-q}} \\ &= \frac{v^2}{w^{q+1}} + \frac{\alpha}{w^{q-1}} + \frac{w^{q-1}\beta}{1 + w^{q-1}} + \frac{v}{w} + \alpha + \beta \\ &= \mathbb{T}(\hat{v}\hat{w}) + \hat{w}^q\hat{v} + \alpha. \end{aligned}$$

Since $[\ell(\hat{v}, \hat{w}) : \ell(\hat{w})] = [\ell(v, w) : \ell(w)] = q$, the polynomial $\hat{w}X^q + \mathbb{T}(\hat{w}X) + \hat{w}^q X + \alpha$ is irreducible over $\ell(\hat{w})$, so also $\hat{v}X^q + \mathbb{T}(\hat{v}X) + \hat{v}^q X + \alpha$ is irreducible over $\ell(\hat{v})$. Let $\hat{\ell} = \mathbb{F}_{q^2}.\ell$, and $\hat{E} = \hat{\ell}.E$. Pick $\gamma \in \hat{\ell}^*$ of multiplicative order $q + 1$, and let $\delta = \gamma + 1/\gamma \in \mathbb{F}_q^* \subseteq \ell^*$. Let $y = (\hat{v}\gamma + \hat{w}/\gamma + 1)/\delta$ and $z = (\hat{v}/\gamma + \hat{w}\gamma + 1)/\delta$. Then $\hat{E} = \hat{\ell}(\hat{v}, \hat{w}) = \hat{\ell}(y, z)$.

Lemma 10.3. *We have $[\hat{\ell}(y, z) : \hat{\ell}(z)] = q + 1$ and*

$$y^{q+1} + z^{q+1} = \mathbb{T}(yz) + \alpha + 1. \tag{10.4}$$

For $\eta \in \mathbb{F}_{q^2}$ with $\eta^{q+1} = 1$, there is a unique element $\hat{\nu}_\eta \in \mathrm{Aut}_{\hat{\ell}}\, \hat{E}$ which maps $(y, z) \mapsto (y\eta, z/\eta)$. Moreover, $\nu_\eta := \hat{\nu}_\eta|_E$ is in $\mathrm{Aut}_\ell\, E$.

Proof. We compute

$$\begin{aligned} y^{q+1}+z^{q+1} &= \frac{(\hat{v}\gamma+\frac{\hat{w}}{\gamma}+1)(\frac{\hat{v}^q}{\gamma}+\hat{w}^q\gamma+1)}{\delta^{q+1}} + \frac{(\frac{\hat{v}}{\gamma}+\hat{w}\gamma+1)(\hat{v}^q\gamma+\frac{\hat{w}^q}{\gamma}+1)}{\delta^{q+1}} \\ &= \hat{w}^q\hat{v}+\hat{w}\hat{v}^q+\frac{\hat{w}^q+\hat{v}^q+\hat{w}+\hat{v}}{\delta} \\ &= \mathbb{T}(\hat{w}\hat{v})+\alpha+\frac{\hat{w}^q+\hat{v}^q}{\delta^q}+\frac{\hat{w}+\hat{v}}{\delta} \\ &= \mathbb{T}\left(\hat{w}\hat{v}+\frac{\hat{w}+\hat{v}}{\delta}+\frac{\hat{w}^2+\hat{v}^2+1}{\delta^2}\right)+\alpha+\mathbb{T}\Big(\frac{1}{\delta^2}\Big) \\ &= \mathbb{T}(yz)+\alpha+\mathbb{T}\Big(\frac{1}{\delta^2}\Big). \end{aligned}$$

Since $1/\delta = \gamma/(\gamma^2+1) = \gamma/(\gamma+1)+\gamma^2/(\gamma^2+1)$, we have

$$\begin{aligned} \mathbb{T}\Big(\frac{1}{\delta^2}\Big) = \mathbb{T}\Big(\frac{1}{\delta}\Big) &= \frac{\gamma^q}{\gamma^q+1}+\frac{\gamma}{\gamma+1} \\ &= \frac{\frac{1}{\gamma}}{\frac{1}{\gamma}+1}+\frac{\gamma}{\gamma+1}=1. \end{aligned}$$

Since $\hat{E}=\hat{\ell}(y,z)$ has genus $q(q-1)/2$ where y and z satisfy equation (10.4) of total degree $q+1$, this equation must define a smooth (projective) plane curve, and in particular must be irreducible. Thus $[\hat{\ell}(y,z):\hat{\ell}(z)]=q+1$. Now existence and uniqueness of $\hat{\nu}_\eta$ are clear. A straightforward computation yields that $\hat{\nu}_\eta$ maps

$$\begin{aligned} \hat{w} &\mapsto \frac{1}{\delta^2}\left(\delta+\Big(\frac{\gamma}{\eta}+\frac{\eta}{\gamma}\Big)+\hat{w}\Big(\frac{\eta}{\gamma^2}+\frac{\gamma^2}{\eta}\Big)+\hat{v}\Big(\eta+\frac{1}{\eta}\Big)\right) \\ \hat{v} &\mapsto \frac{1}{\delta^2}\left(\delta+\Big(\gamma\eta+\frac{1}{\gamma\eta}\Big)+\hat{w}\Big(\eta+\frac{1}{\eta}\Big)+\hat{v}\Big(\gamma^2\eta+\frac{1}{\gamma^2\eta}\Big)\right). \end{aligned}$$

Since $\ell(\hat{\nu}_\eta(\hat{v}),\hat{\nu}_\eta(\hat{w}))=E$, it follows that $\hat{\nu}_\eta$ induces an automorphism of E. □

We now compute the subfield of E fixed by an index-$(q^2-q)/2$ subgroup of $G := \mathrm{Aut}_\ell E \cong \mathrm{SL}_2(q)$. There is a unique element $\tau \in \mathrm{Aut}_\ell E$ such that $\tau\colon (\hat{v},\hat{w}) \mapsto (\hat{w},\hat{v})$. Note that τ maps (y,z) to (z,y), and the group $G_1 := \langle \tau, \{\nu_\eta : \eta^{q+1}=1\}\rangle$ is dihedral of order $2q+2$. Hence the subfield of $\hat{E}$ fixed by G_1 contains $\hat{\ell}(yz)$. Multiplying equation (10.4) by y^{q+1}, we see that $[\hat{\ell}(y,z):\hat{\ell}(yz)] = [\hat{\ell}(y,yz):\hat{\ell}(yz)] \le 2q+2$, so $\hat{\ell}(yz)$ is the subfield of $\hat{E}$ fixed by G_1. Moreover, since

$$yz = \left(\frac{\hat{v}+\hat{w}}{\delta}\right)^2+\frac{\hat{v}+\hat{w}}{\delta}+\hat{v}\hat{w}+\frac{1}{\delta^2}$$

lies in E, the subfield of E fixed by G_1 is $\ell(yz)$.

Next we compute an invariant of G. Recall that $\mathrm{SL}_2(q)$ can be written as CTU, where T is the diagonal subgroup, U is a unipotent subgroup, and C

is a cyclic subgroup of order $(q+1)$. We can choose U to be the set of maps $\sigma_\xi\colon (v,w)\mapsto (v+\xi,w)$ with $\xi\in\mathbb{F}_q$, so $E^U=\ell(w)$. We can choose T to be the set of maps $\mu_\zeta\colon (v,w)\mapsto(\zeta^{-1}v,\zeta^{-1}w)$ with $\zeta^{q-1}=1$, and C to be the set of maps ν_η defined in the above lemma. Hence the product

$$\prod_{\eta^{q+1}=1}\prod_{\zeta^{q-1}=1}\prod_{\xi\in\mathbb{F}_q}\nu_\eta\mu_\zeta\sigma_\xi\Big(\frac{\delta}{w}+1\Big)$$

is G-invariant. Since this product is the q-th power of

$$u:=\prod_{\eta^{q+1}=1}\prod_{\zeta^{q-1}=1}\nu_\eta\mu_\zeta\Big(\frac{\delta}{w}+1\Big),$$

also G fixes u. Since $1/w=(z\gamma+1+y\gamma^{-1})/\delta$, we have

$$u=\prod_{\zeta^{q-1}=1}\prod_{\eta^{q+1}=1}(\eta\zeta y\gamma^{-1}+\zeta+1+\eta^{-1}\zeta\gamma z).$$

By the following lemma,

$$\begin{aligned}
u&=\prod_{\zeta^{q-1}=1}\prod_{\eta^{q+1}=1}(\eta\zeta y+\zeta+1+\eta^{-1}\zeta z)\\
&=(y^{q+1}+z^{q+1})\prod_{\substack{\zeta^{q-1}=1\\ \zeta\neq1}}\Big(\zeta^2(y^{q+1}+z^{q+1})+\\
&\qquad\qquad(\zeta^2+1)\Big(1+\mathbb{T}\Big(yz\frac{\zeta^2}{\zeta^2+1}\Big)\Big)\Big)\\
&=(\mathbb{T}(yz)+\alpha+1)\prod_{\zeta\in\mathbb{F}_q\smallsetminus\mathbb{F}_2}\Big(\zeta\big(\mathbb{T}(yz)+\alpha+1\big)+\\
&\qquad\qquad(\zeta+1)\Big(1+\mathbb{T}\Big(yz\frac{\zeta}{\zeta+1}\Big)\Big)\Big)\\
&=(\mathbb{T}(yz)+\alpha+1)\prod_{\zeta\in\mathbb{F}_q\smallsetminus\mathbb{F}_2}\Big(\sum_{i=0}^{e-1}\frac{\zeta^{2^i}+\zeta}{\zeta^{2^i}+1}(yz)^{2^i}+\zeta\alpha+1\Big).
\end{aligned}$$

Thus $u=\hat f(yz)$ where $\hat f$ is the polynomial defined in (10.2). It follows that $[\ell(yz):\ell(u)]=\deg(\hat f)=(q^2-q)/2$. Since $E^{G_1}=\ell(yz)$ and $E^G\supseteq\ell(u)$ and $[E^{G_1}:E^G]=(q^2-q)/2$, it follows that $E^G=\ell(u)$. Now, G_1 contains no nontrivial normal subgroup of G, so E is the Galois closure of $\ell(yz)/\ell(u)$, whence G is the geometric monodromy group of $\hat f$. Clearly $\hat f$ is fixed by $\mathrm{Gal}(\ell/k)$, so $\hat f\in k[X]$. By Theorem 5.4, the extension E/E^G has two wildly ramified branch points, so Theorem 8.1 implies that $\hat f$ is in the k-equivalence class corresponding to the pair (α,β). □

Lemma 10.5. *The following identity holds in $k[Y,Z]$:*

$$\prod_{\omega^{q+1}=1} (\omega Y + 1 + \omega^{-1} Z) = Y^{q+1} + Z^{q+1} + \mathbb{T}(YZ) + 1.$$

Proof. By applying the transformation $(Y,Z) \mapsto (\omega Y, Z/\omega)$, we see that $\prod(\omega Y + 1 + \omega^{-1}Z) - Y^{q+1} - Z^{q+1}$ is a polynomial $h(YZ) \in k[YZ]$, with degree at most $q/2$ and constant term 1. If we substitute $Y = Z = \omega/(\omega^2+1)$ (where $\omega^{q+1} = 1$ and $\omega \neq 1$), we see that $YZ = \omega^2/(\omega^4+1)$ is a root of h. These roots of h are precisely the trace 1 elements of $\mathbb{F}_q$, namely the roots of $\mathbb{T}(YZ)+1$. Hence $h(YZ)$ and $\mathbb{T}(YZ)+1$ have the same roots and the same constant term, and $\mathbb{T}(YZ)+1$ is squarefree with $\deg(\mathbb{T}+1) \geq \deg(h)$, so $h(YZ) = \mathbb{T}(YZ)+1$. □

Remark. Once one knows 'where to look' for these polynomials – especially, what should be the Galois closure E of $k(x)/k(f(x))$ – one can give direct proofs of their properties. But such proofs would seem unmotivated, since we know no way to guess what E should be besides appealing to the results in this paper.

11. Another form for the polynomials

In the previous section we computed the polynomials whose existence was proved in Theorem 8.1. Our expression for the polynomials was concise, but involved a product. In this section we prove Theorem 1.2 and Corollary 1.3 by writing the polynomials without any sums or products other than the usual $\mathbb{T}(X) = X^{q/2} + X^{q/4} + \cdots + X$. Here $q = 2^e > 2$ and k is a perfect field of characteristic 2. Also $\alpha, \beta \in k^*$ satisfy $\beta^2 = \alpha^2 + \alpha$.

Theorem 11.1. *The expression*

$$f(X) := \left(\frac{\mathbb{T}(X)+\alpha}{X}\right)^q \cdot \left(\mathbb{T}(X) + \frac{\mathbb{T}(X)+\alpha}{\alpha+1} \cdot \mathbb{T}\Big(\frac{X(\alpha^2+\alpha)}{(\mathbb{T}(X)+\alpha)^2}\Big)\right)$$

defines a polynomial which lies in the k-equivalence class corresponding to $(\alpha+1, \beta)$ in Theorem 8.1.

Proof. First we show that f is a polynomial. Writing $h(X) := X^q f(X)$, we have

$$\begin{aligned} h &= (\mathbb{T}(X)+\alpha)^q \cdot \mathbb{T}(X) + \frac{(\mathbb{T}(X)+\alpha)^{q+1}}{\alpha+1} \cdot \mathbb{T}\Big(\frac{X(\alpha^2+\alpha)}{(\mathbb{T}(X)+\alpha)^2}\Big) \\ &= (\mathbb{T}(X)+\alpha)^q \cdot \mathbb{T}(X) + \frac{1}{\alpha+1} \sum_{i=0}^{e-1} X^{2^i} (\alpha^2+\alpha)^{2^i} (\mathbb{T}(X)+\alpha)^{q+1-2^{i+1}}. \end{aligned}$$

Thus h is a polynomial divisible by $X \cdot (\mathbb{T}(X)+\alpha)$, and moreover h is monic of degree $q(q+1)/2$. We now determine the multiplicity of X as a divisor of h. This multiplicity is unchanged if we replace h by

$$\hat{h} := h \cdot \Big(h + \frac{(\mathbb{T}(X)+\alpha)^{q+1}}{\alpha+1}\Big);$$

writing $c := X(\alpha^2+\alpha)/(\mathbb{T}(X)+\alpha)^2$, we compute

$$\begin{aligned}\hat{h} &= h^2 + h\cdot\frac{(\mathbb{T}(X)+\alpha)^{q+1}}{\alpha+1}\\ &= (\mathbb{T}(X)+\alpha)^{2q}\cdot\mathbb{T}(X)^2 + \mathbb{T}(X)\cdot\frac{(\mathbb{T}(X)+\alpha)^{2q+1}}{\alpha+1} + \frac{(\mathbb{T}(X)+\alpha)^{2q+2}}{\alpha^2+1}\cdot\mathbb{T}(c^2+c).\end{aligned}$$

Substituting $\mathbb{T}(c^2+c) = c^q + c$, and reducing mod X^{2q}, we find that

$$\begin{aligned}\hat{h} &\equiv \alpha^{2q}\,\mathbb{T}(X)^2 + \frac{\alpha^{2q}}{\alpha+1}(\mathbb{T}(X)^2+\alpha\,\mathbb{T}(X)) + \frac{(\mathbb{T}(X)+\alpha)^2}{\alpha^2+1}X^q(\alpha^2+\alpha)^q\\ &\qquad + \frac{\alpha^{2q}}{\alpha^2+1}X(\alpha^2+\alpha) \pmod{X^{2q}}\\ &= \frac{\alpha^{2q}}{\alpha+1}\left(\mathbb{T}(X)^2(\alpha+1) + \mathbb{T}(X)^2 + \alpha\,\mathbb{T}(X) + \alpha X\right) + \frac{(\mathbb{T}(X)+\alpha)^2}{\alpha^2+1}X^q(\alpha^2+\alpha)^q\\ &= \frac{\alpha^q}{\alpha^2+1}X^q\left(\alpha^{q+1}(\alpha+1) + (\mathbb{T}(X)+\alpha)^2(\alpha+1)^q\right),\end{aligned}$$

so X^q divides $\hat{h}$, whence f is a polynomial divisible by $(\mathbb{T}(X)+\alpha)$. Furthermore, X divides f (equivalently X^{q+1} divides $\hat{h}$) precisely when $\alpha\in\mathbb{F}_q$, in which case X^2 exactly divides f. Since h is monic of degree $q(q+1)/2$, it follows that f is monic of degree $q(q-1)/2$.

We now show that $f/(\mathbb{T}(X)+\alpha)$ is in $k[X^2]$. It suffices to show that $\overline{f} := X^q f/(\mathbb{T}(X)+\alpha)$ is in $k[X^2]$. We compute

$$\begin{aligned}\overline{f} &= \mathbb{T}(X)(\mathbb{T}(X)+\alpha)^{q-1} + \frac{(\mathbb{T}(X)+\alpha)^q}{\alpha+1}\cdot\mathbb{T}\Big(\frac{X(\alpha^2+\alpha)}{(\mathbb{T}(X)+\alpha)^2}\Big)\\ &= (\mathbb{T}(X)+\alpha)^q + \alpha(\mathbb{T}(X)+\alpha)^{q-1} + \frac{1}{\alpha+1}\sum_{i=0}^{e-1}(X(\alpha^2+\alpha))^{2^i}(\mathbb{T}(X)+\alpha)^{q-2^{i+1}}.\end{aligned}$$

The summands with $i>0$ are polynomials in X^2. Thus, there exists $b\in k[X]$ such that

$$\begin{aligned}\overline{f} &= b(X^2) + \alpha(\mathbb{T}(X)+\alpha)^{q-1} + \alpha X(\mathbb{T}(X)+\alpha)^{q-2}\\ &= b(X^2) + \alpha(\mathbb{T}(X)+\alpha)^{q-2}(\mathbb{T}(X)+\alpha+X),\end{aligned}$$

so indeed $\overline{f}\in k[X^2]$, whence $f/(\mathbb{T}(X)+\alpha)$ is in $k[X^2]$.

By Theorem 10.1, the polynomial

$$\hat{f}(X) := (\mathbb{T}(X)+\alpha)\prod_{\substack{\zeta^{q-1}=1\\ \zeta\neq 1}}\Big(\sum_{i=1}^{e-1}\frac{\zeta^{2^i}+\zeta}{\zeta^{2^i}+1}X^{2^i} + \zeta(\alpha+1)+1\Big)$$

is in the k-equivalence class corresponding to $(\alpha+1,\beta)$ in Theorem 8.1. By Lemma 3.1, the extension $k(x)/k(\hat{f}(x))$ has precisely two branch points; one of these points is totally ramified, and the ramification index at any point of $k(x)$ lying over the other branch point is at most 2. Since $k(x)/k(\hat{f}(x))$ is totally ramified over the infinite place, there is a unique finite branch point.

But plainly $\hat{f}(X) = (\mathbb{T}(X) + \alpha)\hat{b}(X)^2$ for some nonconstant $\hat{b} \in k[X]$, so $\hat{f}(x) = 0$ is the finite branch point, and thus $\hat{b}(X)$ is squarefree and coprime to $(\mathbb{T}(X) + \alpha)$. We will show that every root δ of $\hat{f}$ is a root of f; it follows that the multiplicity of δ as a root of f is at least as big as the corresponding multiplicity for $\hat{f}$. Since f and $\hat{f}$ have the same degree and the same leading coefficient, we conclude that $f = \hat{f}$.

It remains to prove that every root of $\hat{f}$ is a root of f. Recall that, in the function field $\overline{k}(y, z)$ where $y^{q+1} + z^{q+1} = \mathbb{T}(yz) + \alpha$, we have the identity

$$\begin{aligned}\hat{f}(yz) &= \prod_{\zeta^{q-1}=1} \prod_{\eta^{q+1}=1} (\eta\zeta y + \zeta + 1 + \frac{\zeta}{\eta} z) \\ &= (y^{q+1} + z^{q+1}) \prod_{\substack{\zeta^{q-1}=1 \\ \zeta \neq 1}} \prod_{\eta^{q+1}=1} (\eta\zeta y + \zeta + 1 + \frac{\zeta}{\eta} z).\end{aligned}$$

Let δ be a root of $\hat{f}$. Pick $\hat{y} \in \overline{k}^*$ and $\hat{z} \in \overline{k}$ such that $\delta = \hat{y}\hat{z}$ and $\hat{y}^{q+1} + \hat{z}^{q+1} = \mathbb{T}(\hat{y}\hat{z}) + \alpha$: such $\hat{y}, \hat{z}$ exist because substituting $\hat{z} = \delta/\hat{y}$ into the latter equation (and clearing denominators) gives a polynomial in $\hat{y}$ which is not a monomial, and thus has a nonzero root. If $\mathbb{T}(\delta) = \alpha$ then we already know that $f(\delta) = 0$. If $\delta = 0$ then $\hat{z} = 0$ and $\hat{y}^{q+1} = \alpha$, so

$$\begin{aligned}0 = \hat{f}(0) &= \prod_{\zeta^{q-1}=1} \prod_{\eta^{q+1}=1} (\eta\zeta\hat{y} + \zeta + 1) \\ &= \prod_{\zeta^{q-1}=1} (\zeta^{q+1}\hat{y}^{q+1} + (\zeta + 1)^{q+1}) \\ &= \prod_{\zeta^{q-1}=1} (\zeta^2\alpha + \zeta^2 + 1) \\ &= (\alpha + 1)^{q-1} + 1.\end{aligned}$$

Thus $\alpha \in \mathbb{F}_q$, so X^2 divides f.

Henceforth we assume $\alpha \neq \mathbb{T}(\delta)$ and $\delta \neq 0$. This implies $\eta\zeta\hat{y} + \zeta + 1 + \hat{z}\zeta/\eta = 0$ for some ζ, η with $\zeta \in \mathbb{F}_q \setminus \mathbb{F}_2$ and $\eta^{q+1} = 1$. By replacing $\hat{y}$ and $\hat{z}$ with $\eta\hat{y}$ and $\hat{z}/\eta$, we may assume $\eta = 1$, so

$$\hat{z} = \hat{y} + 1 + \frac{1}{\zeta}.$$

Write $\hat{\zeta} := 1 + 1/\zeta$, and note that $\hat{\zeta} \in \mathbb{F}_q \setminus \mathbb{F}_2$. Since $\delta = \hat{y}\hat{z}$, we compute

$$\begin{aligned}\mathbb{T}(\delta) + \alpha &= \hat{y}^{q+1} + \hat{z}^{q+1} \\ &= \hat{y}^{q+1} + \hat{y}^{q+1} + \hat{\zeta}\hat{y}^q + \hat{\zeta}^q\hat{y} + \hat{\zeta}^{q+1} \\ &= \hat{\zeta}\hat{y}^q + \hat{\zeta}\hat{y} + \hat{\zeta}^2\end{aligned}$$

and

$$\begin{aligned}\mathbb{T}(\delta) &= \mathbb{T}(\hat{y}^2 + \hat{\zeta}\hat{y}) \\ &= \hat{\zeta}\hat{y}^q + \hat{\zeta}\hat{y} + \mathbb{T}(\hat{y}^2 + \hat{\zeta}^2\hat{y}^2).\end{aligned}$$

Thus

$$\alpha + \hat{\zeta}^2 = \mathbb{T}(\hat{y}^2 + \hat{\zeta}^2\hat{y}^2),$$

so

$$\sqrt{\alpha} + \hat{\zeta} = \mathbb{T}(\hat{y} + \hat{\zeta}\hat{y}).$$

Adding the last two equations gives

$$\alpha + \sqrt{\alpha} + \hat{\zeta}^2 + \hat{\zeta} = \hat{y}^q + \hat{y} + \hat{\zeta}\hat{y}^q + \hat{\zeta}\hat{y} = (1 + \hat{\zeta})(\hat{y}^q + \hat{y}),$$

so

$$\begin{aligned}\mathbb{T}(\delta) + \alpha &= \hat{\zeta}^2 + \hat{\zeta}(\hat{y}^q + \hat{y}) \\ &= \hat{\zeta}^2 + \frac{\hat{\zeta}}{1 + \hat{\zeta}} \left(\alpha + \sqrt{\alpha} + \hat{\zeta}^2 + \hat{\zeta}\right) \\ &= \frac{\hat{\zeta}}{1 + \hat{\zeta}} \left(\alpha + \sqrt{\alpha}\right)\end{aligned}$$

and

$$\begin{aligned}\mathbb{T}\Big(\frac{\delta}{\hat{\zeta}^2}\Big) &= \mathbb{T}\Big(\frac{\hat{y}^2}{\hat{\zeta}^2} + \frac{\hat{y}}{\hat{\zeta}}\Big) \\ &= \frac{\hat{y}^q}{\hat{\zeta}} + \frac{\hat{y}}{\hat{\zeta}} \\ &= 1 + \frac{\alpha + \sqrt{\alpha}}{\hat{\zeta}^2 + \hat{\zeta}}.\end{aligned}$$

Writing $\tilde{f}(X) := X^q f(X)/(\mathbb{T}(X) + \alpha)^q$, we have

$$\begin{aligned}\tilde{f}(\delta) &= \mathbb{T}(\delta) + \frac{\mathbb{T}(\delta) + \alpha}{\alpha + 1} \cdot \mathbb{T}\Big(\frac{\delta(\alpha^2 + \alpha)}{(\mathbb{T}(\delta) + \alpha)^2}\Big) \\ &= \frac{\alpha + \hat{\zeta}\sqrt{\alpha}}{1 + \hat{\zeta}} + \frac{\hat{\zeta}\sqrt{\alpha}}{(1 + \hat{\zeta})(\sqrt{\alpha} + 1)} \cdot \mathbb{T}\Big(\frac{\delta(\alpha^2 + \alpha)(1 + \hat{\zeta})^2}{\hat{\zeta}^2(\alpha^2 + \alpha)}\Big) \\ &= \frac{\alpha + \hat{\zeta}\sqrt{\alpha}}{1 + \hat{\zeta}} + \frac{\hat{\zeta}\sqrt{\alpha}}{(1 + \hat{\zeta})(\sqrt{\alpha} + 1)} \cdot \mathbb{T}\Big(\delta + \frac{\delta}{\hat{\zeta}^2}\Big) \\ &= \frac{\alpha + \hat{\zeta}\sqrt{\alpha}}{1 + \hat{\zeta}} + \frac{\hat{\zeta}\sqrt{\alpha}}{(1 + \hat{\zeta})(\sqrt{\alpha} + 1)} \cdot \frac{\hat{\zeta} + \alpha + \sqrt{\alpha}(1 + \hat{\zeta})}{\hat{\zeta}} \\ &= \frac{\alpha + \hat{\zeta}\sqrt{\alpha} + \sqrt{\alpha}(\sqrt{\alpha} + \hat{\zeta})}{1 + \hat{\zeta}},\end{aligned}$$

so $\tilde{f}(\delta) = 0$ and thus $f(\delta) = 0$, which completes the proof. □

Remark. The above proof is not completely satisfying, since it is a verification that $f(X)$ has the desired property, rather than a derivation of the simple expression for $f(X)$. We do not have a good explanation why the polynomial in Theorem 8.1 can be written in such a simple form.

We conclude the paper by proving the results stated in the introduction.

Proof of Theorem 1.2. In case k is perfect, the result follows from Theorem 8.1 and Theorem 11.1. For general k, let $\tilde{k}$ denote the perfect closure of k. Let $f \in k[X]$ satisfy properties (i) and (ii) of Theorem 1.2. Then f satisfies the same properties over the perfect field $\tilde{k}$, so f is $\tilde{k}$-equivalent to f_α for some $\alpha \in \tilde{k} \setminus \mathbb{F}_2$. We will show that this implies f is k-equivalent to f_α, and that $\alpha \in k$. Since the monodromy groups of f over k are the same as those over $\tilde{k}$, indecomposability and exceptionality of f over k are equivalent to the corresponding properties over $\tilde{k}$. Since $\tilde{k} \cap \mathbb{F}_q = k \cap \mathbb{F}_q$ (because $\mathbb{F}_q/\mathbb{F}_2$ is separable), the result follows.

It remains to prove that if $f(X) := \delta + \eta f_\alpha(\zeta X + \gamma)$ is in $k[X]$, where $\delta, \eta, \alpha, \zeta, \gamma \in \tilde{k}$ with $\eta\zeta \neq 0$ and $\alpha \notin \mathbb{F}_2$, then $\delta, \eta, \alpha, \zeta, \gamma$ are in k. The terms of $f_\alpha(X)$ of degree at least $(q^2-3q)/2$ are $\mathbb{T}(X)X^{(q^2-2q)/2} + \alpha X^{(q^2-3q+2)/2}$ and (if $q = 4$) $(\alpha+1)X^2$. Hence the coefficients of $X^{q^2/2-q+2}$ and $X^{q^2/2-q+1}$ in $f(X)$ are $\eta\zeta^{q^2/2-q+2}$ and $\eta\zeta^{q^2/2-q+1}$, and since these are in k^*, we must have $\zeta, \eta \in k^*$. The coefficients of $X^{(q^2-3q+2)/2}$ and $X^{(q^2-2q)/2}$ in $f(X)$ are $\alpha\eta\zeta^{(q^2-3q+2)/2}$ and $\eta\zeta^{(q^2-2q)/2}\,\mathbb{T}(\gamma)$, so $\alpha \in k^*$ and $\mathbb{T}(\gamma) \in k$, whence $\mathbb{T}(\gamma)^2 + \mathbb{T}(\gamma) = \gamma^q + \gamma$ is in k. The coefficient of $X^{(q^2-3q)/2}$ in $f(X)$ is $\eta\zeta^{(q^2-3q)/2}(\alpha\gamma + \gamma^q)$ (plus $\eta(\alpha+1)\zeta^2$ if $q = 4$), so γ is in k. Finally, we conclude that $\delta = f(0) - \eta f_\alpha(\gamma)$ is in k. □

Proof of Corollary 1.3. First assume $f \in k[X]$ is a separable indecomposable exceptional polynomial in case (i) of Theorem 1.1. Then the geometric monodromy group G of f is solvable, and the degree d of f is prime and not equal to p. By [26, Thm. 4], it follows that f is $\overline{k}$-equivalent to either X^d or $D_d(X, 1)$. By [34, Lemma 1.9], f is k-equivalent to either X^d or $D_d(X, a)$ with $a \in k^*$. These polynomials $f(X)$ are separable and indecomposable. We verify exceptionality by examining the factorization of $f(X) - f(Y)$ in $\overline{k}[X, Y]$, given for instance in [34, Prop. 1.7].

Now consider case (iii) of Theorem 1.1. In this case, Corollary 1.3 for $p = 3$ is [20, Thm. 1.3]. So suppose $p = 2$, and let $f \in k[X]$ be a separable indecomposable exceptional polynomial of degree $d = q(q-1)/2$ where $q = 2^e > 2$ with $e > 1$ odd. By Theorem 1.1, the arithmetic monodromy group A of f is $\mathrm{P\Gamma L}_2(q)$, and thus G has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(q)$. The desired result follows from [20, Thm. 4.3] if $\overline{k}(x)/\overline{k}(f(x))$ has no finite branch points, or if the Galois closure E of this extension does not have genus $(q^2-q)/2$. If neither of these conditions hold, then [20, Thm. 2.1] implies that $G = \mathrm{PSL}_2(q)$ and $E/\overline{k}(f(x))$ has precisely one finite branch point, whose inertia group has order 2 and whose second ramification group

is trivial. In particular, f satisfies conditions (i) and (ii) of Theorem 1.2, so in this case the result follows from Theorem 1.2. □

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, New York, 1986.

[2] P. Carbonne and T. Henocq, Décomposition de la Jacobienne sur les corps finis, Bull. Polish Acad. Sci. Math. **42** (1994), 207–215.

[3] S. D. Cohen, The distribution of polynomials over finite fields, Acta Arith. **17** (1970), 255–271.

[4] S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 345 (1994), 897–909.

[5] H. Darmon and J.-F. Mestre, Courbes hyperelliptiques à multiplications réelles et une construction de Shih, Canad. Math. Bull. **43** (2000), 304–311.

[6] H. Davenport and D. J. Lewis, Notes on congruences (I), Quart. J. Math. Oxford (2) **14** (1963), 51–60.

[7] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math. **11** (1896-7), 65–120 and 161–183.

[8] ———, *Linear Groups*, Teubner, Leipzig, 1901.

[9] J. F. Dillon, Multiplicative difference sets via additive characters, Des. Codes Cryptogr. **17** (1999), 225–235.

[10] J. F. Dillon, Geometry, codes and difference sets: exceptional connections, in *Codes and Designs*, de Gruyter, Berlin, 2002, pp. 73–85.

[11] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. **10** (2004), 342–389.

[12] J. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York, 1996.

[13] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Welch case, IEEE Trans. Inform. Theory **45** (1999), 1271–1275.

[14] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, in *Difference Sets, Sequences and their Correlation Properties*, Kluwer, Dordrecht, 1999, pp. 133–158.

[15] M. D. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, Israel J. Math. **82** (1993), 157–225.

[16] R. M. Guralnick and P. Müller, Exceptional polynomials of affine type, J. Algebra **194** (1997), 429–454.

[17] R. M. Guralnick, P. Müller and M. E. Zieve, Exceptional polynomials of affine type, revisited, preprint.

[18] R. M. Guralnick and J. Saxl, Exceptional polynomials over arbitrary fields, in *Algebra, Arithmetic and Geometry with Applications*, Springer, Berlin, 2004, pp. 457–472.

[19] R. M. Guralnick, T. J. Tucker and M. E. Zieve, Exceptional covers and bijections on rational points, Int. Math. Res. Not. IMRN, **2007**, art. ID rnm004, 20 pp. arXiv:math/0511276.

[20] R. M. Guralnick and M. E. Zieve, Polynomials with PSL(2) monodromy, submitted for publication. arXiv:0707.1835 [math.AG].

[21] A. A. Klyachko, Monodromy groups of polynomial mappings, in *Studies in Number Theory*, Saratov, 1975, pp. 82–91.

[22] H. W. Lenstra, Jr., D. P. Moulton, and M. E. Zieve, Exceptional maps between varieties, in preparation.

[23] H. W. Lenstra, Jr. and M. Zieve, A family of exceptional polynomials in characteristic three, in *Finite Fields and Applications*, Cambridge Univ. Press, Cambridge, 1996, pp. 209–218.

[24] C. R. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta Arith. **12** (1967), 289–299.
[25] P. Müller, New examples of exceptional polynomials, in *Finite Fields: Theory, Applications and Algorithms*, Amer. Math. Soc., Providence, 1994, pp. 245–249.
[26] ———, A Weil-bound free proof of Schur's conjecture, Finite Fields Appl. **3** (1997), 25–32.
[27] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. **303** (1987), 595–607.
[28] F. Özbudak, On maximal curves and linearized permutation polynomials over finite fields, J. Pure Appl. Algebra **162** (2001), 87–102.
[29] R. Pink, Euler-Poincaré formula in equal characteristic under ordinariness assumptions, Manuscripta Math. **102** (2000), 1–24.
[30] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.
[31] D. Subrao, The p-rank of Artin-Schreier curves, Manuscripta Math. **16** (1975), 169–193.
[32] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.
[33] W. Tautz, J. Top and A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials, Can. J. Math. **43** (1991), 1055–1064.
[34] G. Turnwald, On Schur's conjecture, J. Austral. Math. Soc. Ser. A **58** (1995), 312–357.
[35] Q. Xiang, Maximally nonlinear functions and bent functions, Des. Codes Cryptogr. **17** (1999), 211–218.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089–2532, USA
E-mail address: guralnic@usc.edu

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121–1967, USA
E-mail address: joelr@ccrwest.org

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540–1966, USA
E-mail address: zieve@math.rutgers.edu
URL: http://www.math.rutgers.edu/∼zieve/