Bivariate factorizations via Galois theory, with application to exceptional polynomials

Michael Zieve[*]
Hill Center, Department of Mathematics, Rutgers University,
110 Frelinghuysen Road, Piscataway NJ 08854
zieve@math.rutgers.edu

Abstract

We present a method for factoring polynomials of the shape $f(X)-f(Y)$, where f is a univariate polynomial over a field k. We then apply this method in the case when f is a member of the infinite family of exceptional polynomials we discovered jointly with H. Lenstra in 1995; factoring $f(X)-f(Y)$ in this case was posed as a problem by S. Cohen shortly after the discovery of these polynomials.

1 Introduction

Factoring polynomials is one of the classical problems in algebra. There is of course an algorithmic aspect to this problem, but our concern is a more theoretical one: how can one factor each member of an infinite family of polynomials? It seems that the literature contains rather little about this problem in the case of polynomials in more than one variable, and in fact contains few examples. In this paper we describe a general method for factoring polynomials of the shape $f(X) - f(Y)$, where f is a univariate polynomial over a field k, which is often successful even when f varies over an infinite family of polynomials. More precisely, we expose a connection with group theory which reduces the problem of factoring $f(X) - f(Y)$ to

[*] The author's work supported by an NSF postdoctoral fellowship

certain computations in the Galois group of $f(X) - t$ over $k(t)$, where t is an indeterminate. Our results are related to work of Abhyankar (cf. [1]–[3] among various other papers) in which he goes in the opposite direction, deriving information about Galois groups of polynomials from the shapes of factorizations such as the ones in the present paper.

To illustrate our method, we use it to factor $f(X)-f(Y)$ for a certain family of polynomials for which these factorizations are particularly important, namely certain *exceptional polynomials* f. Here a polynomial $f(X) \in k[X]$ is called *exceptional* if there are no irreducible factors of $f(X)-f(Y)$ in $k[X,Y]$, other than (multiples of) $X-Y$, which remain irreducible over the algebraic closure of k (i.e. which are absolutely irreducible). Exceptional polynomials have a rich theory and possess several interesting properties. For instance, a polynomial f over a finite field k is exceptional if and only if there is an infinite algebraic extension ℓ of k for which the map $f\colon \ell \to \ell$ given by $a \mapsto f(a)$ is bijective (i.e. f is a permutation polynomial over ℓ). A primer on exceptional polynomials is included as an appendix to this paper. Over the years numerous authors have contributed to the theory of exceptional polynomials, with steady success, but a radical change in perspective came in 1993. This was due to the work of Fried, Guralnick and Saxl [9], who used hard group theory (including the classification of finite simple groups) in order to severely restrict the possibilities for the Galois group $\mathrm{Gal}(f(X) - t, k(t))$ of an exceptional polynomial. Their work provided hope for a complete classification of exceptional polynomials, something which previously had not been dreamt possible. The thrust of their result is that the Galois group is typically an affine group (that is, a group of invertible affine transformations of a vector space), except for certain unexpected possibilities over fields of characteristic two and three. Every exceptional polynomial known in 1993 had affine Galois group; but following [9] there was a flurry of activity which saw the construction of new (non-affine) exceptional polynomials in characteristics two and three. In fact, in recent work Guralnick and I have completely classified the non-affine exceptional polynomials [13]. However, for the non-affine exceptional polynomials in characteristic three (which were discovered jointly with Lenstra [15]), the exceptionality property was proven indirectly, without deriving the factorization of $f(X) - f(Y)$, and up to now this factorization has not been known (although it is clearly important, since it is the main ingredient in the definition of exceptionality; also it is used in the above-mentioned paper [13]). In this paper we produce this factorization by applying our general method for factoring bivariate polynomials of this shape.

Let us sketch the method. Consider a monic polynomial $f(X) \in k[X]$, where to ease the exposition we make the minor assumption that $f'(X) \neq 0$. Assume that we know the normal closure Ω of the field extension $k(y)/k(t)$, where $t = f(y)$ and y is transcendental over k, and that we know the group $G = \mathrm{Gal}(\Omega/k(t))$. First we compute the subdegrees of G, namely the indices $[G_y : G_{xy}]$ where x varies over the G-conjugates of y and G_y denotes the subgroup of G fixing y. Next, for each x we produce a polynomial over $k(y)$, having x as a root, which has degree $[G_y : G_{xy}]$; this polynomial will be the minimal polynomial of x over $k(y)$, and as such is an irreducible factor of $f(X) - f(y)$ in $k[X, y]$. Then $f(X) - f(y)$ is the product of the distinct irreducibles gotten in this manner (since polynomials of this shape cannot have multiple roots). The second step will provide the most difficulties in general: it requires us to produce a polynomial of prescribed degree having x as a root. In our example this arises in Section 6, where the shape of the roots x in our case suggests the form of the desired polynomials; this is certainly the prettiest part of the argument.

Since it is significant for the theory of exceptional polynomials, we now describe the explicit factorization we produce as an illustration of our method. We work with the infinite family of (indecomposable) exceptional polynomials over $\mathbb{F}_3$ from [15]; these are members of a more general family of polynomials having fairly uniform properties, defined as follows: if $q \equiv 3 \pmod 4$ is a power of a prime p, and d divides $(q+1)/4$, there is a corresponding polynomial in $\mathbb{F}_p[X]$,

$$f_{q,d} = X(X^{2d}+1)^{(q+1)/(4d)} \left(\frac{(X^{2d}+1)^{(q-1)/2} - 1}{X^{2d}} \right)^{(q+1)/(2d)}.$$

We present the factorization of $f_{q,d}(X) - f_{q,d}(Y)$ over $\overline{\mathbb{F}}_p[X, Y]$ for arbitrary d and $q > 3$; from these factorizations one immediately sees that $f_{q,d}$ is exceptional over $\mathbb{F}_p$ precisely when $p = 3$, and one can also read off various other properties of the $f_{q,d}$.

In his talk at the Third International Conference on Finite Fields and Applications (Glasgow 1995), S. Cohen asked for the factorization of $f_{q,d}(X) - f_{q,d}(Y)$; this motivated the present work. In that talk Cohen also presented two polynomials of degree $(q+1)/4$ which he conjectured should be factors of $f_{q,(q+1)/4}$ (based on evidence from a computer search); the validation of his conjecture is one consequence of our work.

The factorizations involve the Dickson polynomials, which are defined as follows: for any positive integer n, any field k, and any $a \in k$, the Dickson polynomial of degree n having parameter a is the unique polynomial $D_n(X, a) \in k[X]$ for which $D_n(Y + (a/Y),\, a) = Y^n + (a/Y)^n$. Now put $e = (q+1)/(4d)$. The polynomial $f_{q,d}(X) - f_{q,d}(Y) \in \overline{\mathbb{F}}_p[X, Y]$ is the product of $X - Y$ and several other distinct irreducibles $R(X, Y) \in \overline{\mathbb{F}}_p[X, Y]$, of which two have degree $(q+1)/4$, and $(q-3)/2$ have degree $(q+1)/2$, and $(q-3)/4$ have degree $q+1$. The two factors $R(X, Y)$ of degree $(q+1)/4$ are determined by the choice of $\sqrt{-1}$; these R satisfy

$$R(X^e, Y^e) = \prod_{\zeta^e = 1} \left(Y^{(q+1)/4} D_{(q+1)/4}\left(\zeta X/Y \ + 1/2, 1/16\right) + \sqrt{-1} \right).$$

The factors $R(X, Y)$ of degree $(q+1)/2$ are determined by the choices of ϕ and μ, where ϕ is a nonsquare in $\mathbb{F}_q$ of the form $\theta^2 + \theta$ with $\theta \in \mathbb{F}_q \setminus \{-1/2\}$, and $\mu \in \mathbb{F}_{q^2}$ satisfies $\mu^2 = \phi$; these R satisfy

$$R(X^{2e}, Y^{2e}) = \prod_{\zeta^{2e} = 1} \left(Y^{(q+1)/2} D_{(q+1)/2}\left(\zeta X/Y \ - 1 - 2\theta, \phi\right) + 2\mu \right).$$

Here the choice of θ is irrelevant. The factors $R(X, Y)$ of degree $q+1$ are determined by the choice of a nonzero square $\phi \in \mathbb{F}_q$ having the form $\theta^2 + \theta$ for some $\theta \in \mathbb{F}_q$; here we have

$$R(X^{2e}, Y^{2e}) = \prod_{\zeta^{2e} = 1} \left(Y^{q+1} D_{q+1}\left(\zeta X/Y \ - 1 - 2\theta, \phi\right) - \phi(2Y^{q+1} + 4) \right).$$

Again, the choice of θ is irrelevant.

We will also use our method to derive the factorization of $f(X) - f(Y)$, where $f(X)$ is one of the non-affine exceptional polynomials in characteristic two which were discovered by Cohen and Matthews following examples of Müller. This factorization appeared in [5], where it was verified by entirely different methods after having been conjectured based on bits of evidence coming from a number of different directions. Our approach, based on the Galois-theoretic information from [12], provides new insight into this factorization; for instance, we resolve a mystery from [5]. This mystery is that the factors of $f(X) - f(Y)$ can be expressed in terms of Dickson polynomials (just as is true for the odd characteristic polynomials above); in [5], the Dickson polynomials entered only at the very last step, as a way of rewriting the factorization after all proofs had been completed. In our approach the Dickson polynomials arise naturally out of the dihedral groups which are point-stabilizers of the Galois groups. Another advantage of our approach is that the factorization is derived rather than verified; this differs from [5], where the proofs will only work if the factorization has been conjectured at the outset (our approach produces the factors themselves by pure reasoning, with no need for guesswork).

We now describe the contents of this paper in more detail. In the next section we explain the general factorization method. In Section 3 we recall known facts about the specific polynomials $f_{q,d}$, which we require in order to factor $f_{q,d}(X)-f_{q,d}(Y)$. Then in the next three sections we apply our method to produce this bivariate factorization, first computing the subdegrees of the appropriate group, next computing the roots of $f_{q,d}(X)-t$, and then producing the factors themselves. Section 7 contains some consequences of the factorization, and discusses the role of the factorization in the theory of the $f_{q,d}$. After giving a quick primer on exceptional polynomials in Appendix A, we conclude in Appendix B by applying our method to derive the bivariate factorizations associated to the Müller-Cohen-Matthews exceptional polynomials.

It is a pleasure to thank Hendrik W. Lenstra, Jr. for several valuable conversations, and Stephen D. Cohen for comments on an earlier version of this manuscript.

Notation. In the various sections of this paper (but not in the appendices) we keep certain notational conventions. As above, $q \equiv 3 \pmod 4$ is a power of a prime p. For $E \in \mathbb{F}_{q^2}$, we let $\bar{E} := E^q$ denote the conjugate of E in the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. The algebraic closure of a field k is denoted $\overline{k}$. Finally, we reserve α for a fixed square root of -1 in $\mathbb{F}_{q^2}$, and d for a divisor of $(q+1)/4$, and put $e=(q+1)/(4d)$.

2 General method

In this section we explain our approach to factoring polynomials $f(X)-f(Y)$. We start by reformulating the problem via some easy reductions. Let $f(X)$ be a polynomial in $k[X]$; without loss we assume f monic. We reserve the letters X, Y for indeterminates, transcendental over every field under consideration; to avoid confusion, we will write y for Y whenever we want to view it as an element of a prescribed field (but always y is transcendental over k, so the factorizations of $f(X) - f(y)$ and $f(X) - f(Y)$ over k differ only by the substitution of Y for y). When viewed as a member of $k[y][X]$, the polynomial $f(X) - f(y)$ is monic (in X), so we may assume that each of its irreducible factors in $k[y][X]$ is also monic in X. Then each of these factors is irreducible in $k(y)[X]$ (by Gauss' lemma), so it suffices to find the factorization of $f(X) - f(y)$ into monic irreducible polynomials $R(X, y) \in k(y)[X]$ (each such R will necessarily lie in $k[y][X]$).

Next we reduce to the case where the factors R are distinct. Note that $f'(X) = 0$ if and only if f is a polynomial in X^p, where $p = \mathrm{char}(k)$; equivalently, $f(X) = h(X)^p$ for some polynomial $h(X) \in \overline{k}[X]$ (where $h(X) \in k[X]$ if k perfect), i.e. $f(X) - f(y) = (h(X) - h(y))^p$. It follows that, at least in the case of perfect fields k, in order to factor $f(X) - f(y)$ it is sufficient to perform the factorization under the assumption that $f'(X) \neq 0$ (and for imperfect k we can first perform the factorization over the perfect field $\overline{k}$ and then piece together the factorization over k). Henceforth, to simplify the exposition, we assume $f'(X) \neq 0$; this implies that $f(X) - f(y)$ has no multiple roots (as any such root x would satisfy $f'(x) = 0$, so $x \in \overline{k}$, whence $f(y) = f(x) \in \overline{k}$, contradicting the fact that y is transcendental over k). Thus, $f(X) - f(y)$ is the product of its distinct monic irreducible factors $R(X, y) \in k(y)[X]$, and we have only to find these factors.

Now put $t = f(y)$, so that $f(X) - f(y) = f(X) - t$. As above, this polynomial over $k(t)$ is separable (since $f'(X) \neq 0$) and irreducible (by Gauss' lemma). Let $G = \mathrm{Gal}(f(X) - t, k(t))$ be its Galois group. One root of $f(X) - t$ is y; the other roots are the $k(t)$-conjugates of y, namely the values $\tau(y)$ for $\tau \in G$. Thus, the monic irreducible factors of $f(X) - t$ in $k(y)[X]$ are precisely the minimal polynomials over $k(y)$ of the various $\tau(y)$.

Our first step in the construction of these minimal polynomials will be the computation of their degrees. We translate this to a group theoretic calculation. Let H be the subgroup of G consisting of elements fixing y. For any $\tau \in G$, the subgroup of G consisting of elements fixing $\tau(y)$ is $H^\tau := \tau H \tau^{-1}$. By Galois theory, the degree of the minimal polynomial of $\tau(y)$ over $k(y)$, or $[k(\tau(y), y) : k(y)]$, equals the index $[H : H \cap H^\tau] = \#H/\#(H \cap H^\tau)$. (In group theoretic terms, these indices are the subdegrees of the transitive permutation group G.) Thus, to compute the degrees, we must determine the sizes of the various intersections $H \cap H^\tau$.

In the example considered in this paper, we perform this computation in Section 4. Then we explicitly compute the various $\tau(y)$, after which we produce their minimal polynomials. But first, in the next section, we recall the details of this example.

3 Galois theory of the $f_{q,d}$

In this section we review some known properties (from [15]) of the special class of polynomials $f_{q,d}$ to be considered in this paper. We begin with the polynomials $f = f_{q,1}$. Recall that $q \equiv 3 \pmod 4$ is a power of a prime p, and that $f(X) \in \mathbb{F}_p[X]$ is given by

$$f(X) = X(X^2+1)^{(q+1)/4}\left(\frac{(X^2+1)^{(q-1)/2}-1}{X^2}\right)^{(q+1)/2}.$$

We take a 'top-down' approach to the Galois-theoretic setup of f, as done in [15] and similar to Serre's appendix to [1]; this means that we start with the largest field to be considered, which will turn out to be the splitting field of $f(X)-t$, and produce all smaller fields as fixed fields of groups of automorphisms of the large field. In our case, we begin with the field $\overline{\mathbb{F}}_p(v)$, where v is transcendental over $\overline{\mathbb{F}}_p$ (and $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$). The group $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ acts as a group of automorphisms of $\overline{\mathbb{F}}_p(v)$, with the matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ corresponding to the $\overline{\mathbb{F}}_p$-automorphism of $\overline{\mathbb{F}}_p(v)$ sending v to $(Av+C)/(Bv+D)$; in fact, any $\overline{\mathbb{F}}_p$-automorphism of $\overline{\mathbb{F}}_p(v)$ has this form. The subfield of $\overline{\mathbb{F}}_p(v)$ fixed (elementwise) by the group $G' = \mathrm{PSL}_2(\mathbb{F}_q)$ is $\overline{\mathbb{F}}_p(t)$, where

$$t = (-1)^{(q+1)/4}\alpha\frac{(v^{q^2}-v)^{(q+1)/2}}{(v^q-v)^{(q^2+1)/2}};$$

here α denotes a square root of -1. Let H' be the subgroup of G' given by

$$H' = \left\{\begin{pmatrix} A & B \\ -\epsilon B & \epsilon A \end{pmatrix} : A, B \in \mathbb{F}_q,\ \epsilon \in \{\pm 1\},\ A^2+B^2 = \epsilon\right\}/\{\pm I\},$$

where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the identity; then H' is a dihedral group of order $q+1$. The subfield of $\overline{\mathbb{F}}_p(v)$ fixed by H' is $\overline{\mathbb{F}}_p(y)$, where

$$y = \alpha\frac{(v^2+1)^{(q+1)/2}}{v^q-v}.$$

Then $\overline{\mathbb{F}}_p(v)$ is the Galois closure of the separable extension $\overline{\mathbb{F}}_p(y)/\overline{\mathbb{F}}_p(t)$, and moreover $t = f(y)$. By Galois theory, G' (respectively, H') is the subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p) \cong \mathrm{Aut}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(v))$ consisting of elements fixing t (respectively, y); also $\overline{\mathbb{F}}_p(v)$ is the splitting field of $f(X) - t$ over $\overline{\mathbb{F}}_p(t)$.

For the purposes of the present paper, it is convenient to modify the above expressions in order to simplify the form of H'. We do this in the following result; recall that, for $E \in \mathbb{F}_{q^2}$, we put $\bar{E} := E^q$. In particular, $\bar{\alpha} = -\alpha$.

Theorem 1 *For $u = (-\alpha v + 1)/(\alpha v + 1)$, we have $\overline{\mathbb{F}}_p(u) = \overline{\mathbb{F}}_p(v)$, and $y = -2/(u^{(q+1)/2} - u^{-(q+1)/2})$, and*

$$f(y) = t = (-2)^{(p-1)/2} \frac{(u^{q^2} - u)^{(q+1)/2}}{(u^{q+1} - 1)^{(q^2+1)/2}}.$$

The extension $\overline{\mathbb{F}}_p(u)/\overline{\mathbb{F}}_p(t)$ is Galois with group

$$G = \left\{ \begin{pmatrix} E & \bar{F} \\ F & \bar{E} \end{pmatrix} \, : \, E, F \in \mathbb{F}_{q^2},\, E\bar{E} - F\bar{F} = 1 \right\} / \{\pm I\},$$

where the matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ corresponds to the $\overline{\mathbb{F}}_p$-automorphism of $\overline{\mathbb{F}}_p(u)$ sending u to $(Au + C)/(Bu + D)$. The extension $\overline{\mathbb{F}}_p(u)/\overline{\mathbb{F}}_p(y)$ is Galois with group

$$H = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}, \begin{pmatrix} 0 & \beta \\ \bar{\beta} & 0 \end{pmatrix} \, : \, \zeta^{q+1} = 1,\, \beta^{q+1} = -1 \right\} / \{\pm I\}.$$

Proof. We start with the first sentence. It is immediate that $\overline{\mathbb{F}}_p(u) = \overline{\mathbb{F}}_p(v)$; we now compute y and t. First, $v = (\alpha u - \alpha)/(u+1)$, so $v^2 + 1 = 4u/(u+1)^2$ and

$$v^q - v = \frac{(-\alpha u^q + \alpha)(u+1) - (\alpha u - \alpha)(u^q + 1)}{(u+1)^{q+1}} = -2\alpha \frac{u^{q+1} - 1}{(u+1)^{q+1}}.$$

Hence $y = -2u^{(q+1)/2}/(u^{q+1} - 1) = -2/(u^{(q+1)/2} - u^{-(q+1)/2})$. Likewise

$$v^{q^2} - v = \alpha \frac{(u^{q^2} - 1)(u+1) - (u-1)(u^{q^2} + 1)}{(u+1)^{q^2+1}} = 2\alpha \frac{u^{q^2} - u}{(u+1)^{q^2+1}},$$

so

$$t = \frac{(-1)^{(q+1)/4}\, \alpha\, (2\alpha)^{(q+1)/2} (u^{q^2} - u)^{(q+1)/2}}{(-2\alpha)^{(q^2+1)/2} (u^{q+1} - 1)^{(q^2+1)/2}} = (-2)^{(p-1)/2} \frac{(u^{q^2} - u)^{(q+1)/2}}{(u^{q+1} - 1)^{(q^2+1)/2}}.$$

From the discussion preceding the Theorem, $\overline{\mathbb{F}}_p(u)/\overline{\mathbb{F}}_p(t)$ is Galois, and its Galois group, viewed as a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p) \cong \mathrm{Aut}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(u))$, is $G := \left(\begin{smallmatrix} \alpha/2 & 1/2 \\ -\alpha/2 & 1/2 \end{smallmatrix}\right) G' \left(\begin{smallmatrix} -\alpha & \alpha \\ 1 & 1 \end{smallmatrix}\right)$. The product

$$\begin{pmatrix} \alpha/2 & 1/2 \\ -\alpha/2 & 1/2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} -\alpha & \alpha \\ 1 & 1 \end{pmatrix}$$

equals

$$\frac{1}{2} \begin{pmatrix} A + D + (B - C)\alpha & -A + D + (B + C)\alpha \\ -A + D - (B + C)\alpha & A + D - (B - C)\alpha \end{pmatrix},$$

so

$$G = \left\{ \begin{pmatrix} E & \bar{F} \\ F & \bar{E} \end{pmatrix} \ : \ E, F \in \mathbb{F}_{q^2},\, E\bar{E} - F\bar{F} = 1 \right\} / \{\pm I\}.$$

Similarly, $\overline{\mathbb{F}}_p(u)/\overline{\mathbb{F}}_p(y)$ is Galois, and its Galois group, viewed as a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p) \cong \mathrm{Aut}_{\overline{\mathbb{F}}_p}(\overline{\mathbb{F}}_p(u))$, is $H := \left(\begin{smallmatrix} \alpha/2 & 1/2 \\ -\alpha/2 & 1/2 \end{smallmatrix}\right) H' \left(\begin{smallmatrix} -\alpha & \alpha \\ 1 & 1 \end{smallmatrix}\right)$, i.e.

$$H = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}, \begin{pmatrix} 0 & \beta \\ \bar{\beta} & 0 \end{pmatrix} \ : \ \zeta^{q+1} = 1,\, \beta^{q+1} = -1 \right\} / \{\pm I\}.$$

This completes the proof. ■

Remark. This proof demonstrates an explicit conjugacy between two subgroups of $\mathrm{SL}_2(q^2)$, namely $\mathrm{SL}_2(q)$ and $G = \mathrm{SU}(q, \hat{H})$, the subgroup preserving the Hermitian form $\hat{H}(\theta, \theta) = \theta_1^{q+1} - \theta_2^{q+1}$. Both of these subgroups are conjugate to $\mathrm{SU}_2(q)$, which is the subgroup preserving the Hermitian form $\theta_1^{q+1} + \theta_2^{q+1}$. The latter conjugacy was known to Dickson [8, §144] but seems to have been forgotten over the years: it is not in [10] or [17] and is given incorrectly in [14]. Specifically, Suzuki proves only that $\mathrm{SU}_2(q) \cong \mathrm{SL}_2(q)$, by first computing all subgroups of $\mathrm{SL}_2(q^2)$, then noting that any such subgroup of the same order as $\mathrm{SL}_2(q)$ must be isomorphic to $\mathrm{SL}_2(q)$ [17, (6.22)]. In the proof of [14, Hilfssatz 8.8], Huppert exhibits a skew-Hermitian form $[\cdot, \cdot]$ over $\mathbb{F}_{q^2}$, then claims that $[u_1, u_2] = -[u_2, u_1] \notin \mathbb{F}_q$ for some u_1, u_2, which is false and invalidates the entire proof.

Next we recall from [15] the relationship between the Galois theory of the polynomials $g = f_{q,d}$ and that of $f = f_{q,1}$. Here f and g are monic polynomials related by $f(X^d) = g(X)^d$, and d is a divisor of $(q+1)/4$. Let r satisfy $r^d = y$, and put $s = g(r)$. From [15] we know that the Galois closure of $\overline{\mathbb{F}}_p(r)/\overline{\mathbb{F}}_p(s)$ is the field $\Omega = \overline{\mathbb{F}}_p(u, s)$, and moreover the permutation groups

$\hat{G} = \mathrm{Gal}(\Omega/\overline{\mathbb{F}}_p(s)) = \mathrm{Gal}(g(X) - s, \overline{\mathbb{F}}_p(s))$ and $G = \mathrm{Gal}(\overline{\mathbb{F}}_p(u)/\overline{\mathbb{F}}_p(t)) = \mathrm{Gal}(f(X) - t, \overline{\mathbb{F}}_p(t))$ are isomorphic (via the restriction map); also $\overline{\mathbb{F}}_p(r) = \overline{\mathbb{F}}_p(y, s)$, so the subgroup $\hat{H}$ of $\hat{G}$ consisting of elements fixing r corresponds to H. For $\sigma \in \hat{G}$, the subgroup of $\hat{G}$ fixing $\sigma(r)$ is $\hat{H}^\sigma = \sigma\hat{H}\sigma^{-1}$; if $\tau \in G$ is the projection of σ, then this group corresponds to H^τ. It follows that the intersection $\hat{H} \cap \hat{H}^\sigma$ has the same size as $H \cap H^\tau$, so the minimal polynomial of $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$ has the same degree as the minimal polynomial of $\tau(y)$ over $\overline{\mathbb{F}}_p(y)$. In the next section we compute these degrees for the various roots $\tau(y)$ of $f(X) - t$, thereby finding them for the roots $\sigma(r)$ of $g(X) - s$; after that we compute the minimal polynomials for the various $\sigma(r)$ to produce the desired bivariate factorization.

4 Subdegrees

In this section we compute the degrees of the irreducible factors of $f(X)-f(y)$ over $\overline{\mathbb{F}}_p(y)$, where $f = f_{q,1}$. The result is as follows, where, as in Theorem 1, G consists of the $\overline{\mathbb{F}}_p$-automorphisms τ of $\overline{\mathbb{F}}_p(u)$ mapping u to $(Eu+F)/(\bar{F}u+\bar{E})$ for some $E, F \in \mathbb{F}_{q^2}$ with $E\bar{E} - F\bar{F} = 1$, and the choice of (E, F) is unique up to replacing (E, F) by $(-E, -F)$; we write $\tau = \left(\begin{smallmatrix} E & \bar{F} \\ F & \bar{E} \end{smallmatrix}\right)$ for short.

Proposition 2 *The polynomial $f(X) - f(y)$ has $3(q + 1)/4$ distinct monic irreducible factors in $\overline{\mathbb{F}}_p(y)[X]$, of which*

- *one has degree 1, namely $X - y$;*
- *two have degree $(q + 1)/4$, with roots $\tau(y)$ where $F\bar{F} = -1/2$;*
- *$(q-3)/2$ have degree $(q+1)/2$, with roots $\tau(y)$ where $(E\bar{E}F\bar{F})^{(q-1)/2} = -1$ but $F\bar{F} \neq -1/2$; and*
- *$(q - 3)/4$ have degree $q + 1$, with roots $\tau(y)$ where $(E\bar{E}F\bar{F})^{(q-1)/2} = 1$.*

Proof. From Section 2, the degrees of the irreducible factors of $f(X) - f(y)$ over $\overline{\mathbb{F}}_p(y)$ are precisely the values $(q + 1)/\#(H \cap H^\tau)$, where $\tau \in G$. Theorem 1 expresses H in coordinates especially suited to the calculation of these values.

To start with, if $\tau \in H$ then $\tau(y) = y$, so the minimal polynomial for $\tau(y)$ over $\overline{\mathbb{F}}_p(y)$ is just $X - y$. Henceforth we assume $\tau \notin H$. Let $\tau = \left(\begin{smallmatrix} E & \bar{F} \\ F & \bar{E} \end{smallmatrix}\right)$, where $E, F \in \mathbb{F}_{q^2}$ with $E\bar{E} - F\bar{F} = 1$; then our assumption simply asserts that $EF \neq 0$.

We now compute $H \cap H^\tau$ for $\tau \notin H$. One easily checks that no nonidentity diagonal matrices in H have diagonal conjugate by τ; that no diagonal matrix in H has antidiagonal conjugate by τ, unless $F\bar{F} = -1/2$ (in which case there is one such diagonal matrix); and that no antidiagonal matrix in H has antidiagonal conjugate, unless $(E\bar{E}F\bar{F})^{(q-1)/2} = -1$, in which case there are two such antidiagonal matrices. Hence, $\#H \cap H^\tau$ is 4 if $F\bar{F} = -1/2$, is 2 if $(E\bar{E}F\bar{F})^{(q-1)/2} = -1$ and $F\bar{F} \neq -1/2$, and is 1 if $(E\bar{E}F\bar{F})^{(q-1)/2} = 1$. Thus the degree of the minimal polynomial for $\tau(y)$ over $\overline{\mathbb{F}}_p(y)$ in these cases is $(q+1)/4$ or $(q+1)/2$ or $q+1$, respectively.

Now that we know the possible sizes of $H \cap H^\tau$, we compute the number of τ's for which each size occurs. Note that the preimage of any element of $\mathbb{F}_q^*$ under the $(q+1)$-th power map $\mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ has size $q+1$. Thus the first case occurs for $(q+1)^2/2$ choices of τ (equivalently, choices of (E, F) up to the equivalence $(E, F) \sim (-E, -F)$); dividing by $\#H = q+1$ gives $(q+1)/2$ conjugates of t having minimal polynomial of degree $(q+1)/4$, and since all the roots of any such minimal polynomial are conjugates of t, we find that there are two polynomials in this case. To count the polynomials in the other cases, note that $\theta := F\bar{F} = E\bar{E} - 1$ is an arbitrary element of $\mathbb{F}_q \backslash \{0, -1, -1/2\}$, and $E\bar{E}F\bar{F} = \theta^2 + \theta$ is a square in $\mathbb{F}_q$ for precisely half of all such values θ (as can be proven by classical elementary arguments involving the quadratic character). Thus, the second case occurs for $(q-3)(q+1)^2/4$ choices of τ, hence for $(q-3)(q+1)/4$ conjugates of t and finally there are $(q-3)/2$ polynomials in this case. The third case occurs for the same number of τ's as does the second, hence occurs for $(q-3)/4$ polynomials. This completes the proof. ∎

5 Computation of roots

In this section we compute the values $\sigma(r)$ where $\sigma \in \hat{G}$. As before, $e = (q+1)/(4d)$. Let σ correspond to $\left(\begin{smallmatrix} E & \bar{F} \\ F & \bar{E} \end{smallmatrix}\right) \in G$, where $E, F \in \mathbb{F}_{q^2}$ satisfy $E\bar{E} - F\bar{F} = 1$; the result is as follows.

Proposition 3 *We have $\sigma(r) = rw^{2e}$ and $\sigma(y) = yw^{(q+1)/2}$, where*

$$w = E\bar{F}u + \bar{E}Fu^{-1} + E\bar{E} + F\bar{F}.$$

Proof. We start with $\sigma(y)$. Theorem 1 implies $y = -2/(u^{(q+1)/2} - u^{-(q+1)/2})$; it follows that

$$\sigma(y) = \frac{-2\left((Eu+F)(\bar{F}u+\bar{E})\right)^{(q+1)/2}}{(Eu+F)^{q+1} - (\bar{F}u+\bar{E})^{q+1}}.$$

We compute $(Eu+F)^{q+1} = (\bar{E}u^q + \bar{F})(Eu+F) = E\bar{E}u^{q+1} + \bar{E}Fu^q + E\bar{F}u + F\bar{F}$; since $(\bar{F}u+\bar{E})^{q+1}$ is gotten by switching E and $\bar{F}$ in the above expression, we find that $(Eu+F)^{q+1} - (\bar{F}u+\bar{E})^{q+1} = u^{q+1} - 1$. Thus

$$\sigma(y) = \frac{-2\left(E\bar{F}u + (E\bar{E}+F\bar{F}) + \bar{E}Fu^{-1}\right)^{(q+1)/2}}{u^{(q+1)/2} - u^{-(q+1)/2}} = yw^{(q+1)/2}.$$

Since $\sigma(r)^d = \sigma(y) = yw^{(q+1)/2} = r^d w^{(q+1)/2}$, we have $\sigma(r) = rw^{2e}\eta$ where $\eta^d = 1$; we must show that $\eta = 1$ (note that this is certainly true when $EF = 0$; henceforth we assume $EF \neq 0$). Since $s = g(r)$ is fixed by σ, we have $g(r) = g(\sigma(r))$, so

$$r(r^{2d}+1)^e \left(\frac{(r^{2d}+1)^{(q-1)/2} - 1}{r^{2d}}\right)^{2e} = \\ \sigma(r)\cdot(\sigma(r)^{2d}+1)^e \left(\frac{(\sigma(r)^{2d}+1)^{(q-1)/2} - 1}{\sigma(r)^{2d}}\right)^{2e};$$

substituting $\sigma(r)^d = r^d w^{(q+1)/2}$ and $\sigma(r) = rw^{2e}\eta$ (and $r^d = y$) gives

$$(y^2+1)^e \left(\frac{(y^2+1)^{(q-1)/2} - 1}{y^2}\right)^{2e} = \\ \eta w^{2e}(y^2w^{q+1}+1)^e \left(\frac{(y^2w^{q+1}+1)^{(q-1)/2} - 1}{y^2w^{q+1}}\right)^{2e}.$$

Thus for some ξ with $\xi^e = \eta$ we have

$$(y^2+1)\left(\frac{(y^2+1)^{(q-1)/2} - 1}{y^2}\right)^2 = \xi w^2(y^2w^{q+1}+1)\left(\frac{(y^2w^{q+1}+1)^{(q-1)/2} - 1}{y^2w^{q+1}}\right)^2;$$

multiplying by y^4w^{2q} gives

$$(*) \quad w^{2q}\left((y^2+1)^q - 2(y^2+1)^{(q+1)/2} + (y^2+1)\right) \\ = \xi\left((y^2w^{q+1}+1)^q - 2(y^2w^{q+1}+1)^{(q+1)/2} + (y^2w^{q+1}+1)\right).$$

Recall that $w = (E\bar{F}u^2 + (E\bar{E} + F\bar{F})u + \bar{E}F)/u$ and $y = -2u^{(q+1)/2}/(u^{q+1}-1)$; when we make these substitutions in $(*)$, and multiply both sides by the quantity $u^{2q}(u^{q+1}-1)^{2q}$, we get an equality of elements of $\overline{\mathbb{F}}_p[u]$. To determine ξ, it suffices to compare the leading coefficients of the resulting polynomials. After a straightforward computation one finds that these leading coefficients are $4(E\bar{F})^2$ and $4\xi(E\bar{F})^2$, so $\xi = 1$ and thus $\eta = \xi^e = 1$ as desired. Finally, $\sigma(r) = rw^{2e}$. ■

6 Minimal polynomials

For each $\sigma \in \hat{G} \setminus \hat{H}$, we can now determine a monic polynomial in $\overline{\mathbb{F}}_p(r)[X]$, of the appropriate degree, which has $\sigma(r)$ as a root; this will be the minimal polynomial for $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$. Once we have computed these minimal polynomials, the factorization stated in the introduction will follow at once from the discussion in Section 2.

As in the previous section, let σ correspond to $\left(\begin{smallmatrix} E & \bar{F} \\ F & \bar{E} \end{smallmatrix}\right) \in G$, where $E, F \in \mathbb{F}_{q^2}$ satisfy $E\bar{E} - F\bar{F} = 1$, and let $\gamma = E\bar{E}F\bar{F}$. By Proposition 3, we have $r^d = y = -2/(u^{(q+1)/2} - u^{-(q+1)/2})$ and $\sigma(r) = rw^{2e}$ and $w = E\bar{F}u + \bar{E}Fu^{-1} + (E\bar{E} + F\bar{F})$. The shape of w is suggestive of the Dickson polynomials; we clarify this in each of the cases of Proposition 2. For each choice of σ, that result tells us the degree n of $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$; for each σ we produce three polynomials over $\overline{\mathbb{F}}_p(r)$, each of degree n. The first polynomial has w as a root, the second has w^{2e} as a root, and the third has $\sigma(r)$ as a root (and the third is monic). The first has the shape $P(X) = bD_n(X - (E\bar{E} + F\bar{F}), \gamma) + c$, where $D_n(Z, \gamma)$ is a Dickson polynomial and $b, c \in \overline{\mathbb{F}}_p(r)$. The second is defined by $Q(X^{2e}) = \prod_{\zeta^{2e}=1} P(\zeta X)$. The third is just $R(X) = Q(X/r)$. Actually, for the two factors of degree $(q+1)/4$, we will have to deviate slightly from this plan, but we still follow the same general strategy. In the next three paragraphs we implement this plan for each of the three nontrivial cases in Proposition 2.

First assume $F\bar{F} = -1/2$ (so $E\bar{E} = 1/2$). Then

$$\begin{aligned} D_{(q+1)/2}(w, -1/4) &= D_{(q+1)/2}\left(E\bar{F}u - (4E\bar{F}u)^{-1}, -1/4\right) \\ &= (E\bar{F}u)^{(q+1)/2} + (4E\bar{F}u)^{-(q+1)/2}; \end{aligned}$$

since $(E\bar{F})^{q+1} = -1/4$, this last expression equals

$$(E\bar{F})^{(q+1)/2}(u^{(q+1)/2} - u^{-(q+1)/2}) = -2(E\bar{F})^{(q+1)/2}/r^d.$$

Thus w is a root of $\hat{P}(X) = r^d D_{(q+1)/2}(X, -1/4) + 2(E\bar{F})^{(q+1)/2} \in \overline{\mathbb{F}}_p(r)[X]$; to get a polynomial of degree $(q+1)/4$ from this, we note that $\hat{P}(X) = P(X^2)$ for some $P(X) \in \overline{\mathbb{F}}_p(r)[X]$, where $P(w^2) = 0$. Define $Q(X) \in \overline{\mathbb{F}}_p(r)[X]$ by $Q(X^e) = \prod_{\zeta^e=1} P(\zeta X)$, so w^{2e} is a root of Q; then $R(X) = Q(X/r) \in \overline{\mathbb{F}}_p(r)[X]$ vanishes at $rw^{2e} = \sigma(r)$. Here R is monic of degree $(q+1)/4$, so indeed R is the minimal polynomial for $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$. The polynomials P, Q, R are determined by the value of $2(E\bar{F})^{(q+1)/2} = \pm\alpha$, yielding at most two polynomials R; since there are indeed two factors in this case, these polynomials are distinct.

Next assume $\gamma^{(q-1)/2} = -1$ but $F\bar{F} \neq -1/2$. Then

$$D_{(q+1)/2}\left(w - (E\bar{E} + F\bar{F}), \gamma\right) = (E\bar{F}u)^{(q+1)/2} + \frac{\gamma^{(q+1)/2}}{(E\bar{F}u)^{(q+1)/2}};$$

this last is just $(E\bar{F})^{(q+1)/2}(u^{(q+1)/2} - u^{-(q+1)/2}) = -2(E\bar{F})^{(q+1)/2}/r^d$. Thus w is a root of $P(X) = r^d D_{(q+1)/2}\left(X - (E\bar{E} + F\bar{F}), \gamma\right) + 2(E\bar{F})^{(q+1)/2}$, so w^{2e} is a root of the polynomial $Q(X)$ defined by $Q(X^{2e}) = \prod_{\zeta^{2e}=1} P(\zeta X)$. Finally, $\sigma(r) = rw^{2e}$ is a root of $R(X) = Q(X/r)$. Here R is a monic polynomial in $\overline{\mathbb{F}}_p(r)[X]$ of degree $(q+1)/2$, so R is the minimal polynomial for $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$. The polynomials P, Q, R are determined by the values of $F\bar{F}$ and $(E\bar{F})^{(q+1)/2}$; here $\theta := F\bar{F} \in \mathbb{F}_q \setminus \{-1/2\}$ satisfies $(\theta^2 + \theta)^{(q-1)/2} = -1$, and $(E\bar{F})^{(q+1)/2}$ is a square root of $\theta^2 + \theta$. Thus there are $(q-3)/2$ choices for θ, each of which corresponds to two values of $(E\bar{F})^{(q+1)/2}$; however, the polynomials Q corresponding to θ and $-\theta - 1$ are identical, so there are at most $(q-3)/2$ distinct polynomials R in this case. Again, we know there are precisely this many factors in this case, so these polynomials are distinct.

Now assume $\gamma^{(q-1)/2} = 1$. Then

$$D_{q+1}\left(w - (E\bar{E} + F\bar{F}), \gamma\right) = \gamma\left(u^{q+1} + u^{-(q+1)}\right) = \gamma(4r^{-2d} + 2),$$

so w is a root of $P(X) = r^{2d} D_{q+1}\left(X - (E\bar{E} + F\bar{F}), \gamma\right) - \gamma(2r^{2d} + 4)$. Put $Q(X^{2e}) = \prod_{\zeta^{2e}=1} P(\zeta X)$, so $Q(w^{2e}) = 0$, and thus $\sigma(r)$ is a root of $R(X) = Q(X/r)$. Since R is a monic polynomial in $\overline{\mathbb{F}}_p(r)[X]$ of degree $q+1$, again it is the minimal polynomial for $\sigma(r)$ over $\overline{\mathbb{F}}_p(r)$. The polynomials P, Q, R are determined by the value of $\theta := F\bar{F}$; this is an element of $\mathbb{F}_q$ satisfying $(\theta^2 + \theta)^{(q-1)/2} = 1$. There are $(q-3)/2$ such values θ; however, replacing θ by $-\theta - 1$ leaves Q and R unchanged, so there are at most $(q-3)/4$ distinct polynomials R in this case. As above, since this equals the number of factors in this case, these polynomials are distinct.

In summary, the polynomial $g(X)-g(r) \in \overline{\mathbb{F}}_p(r)[X]$ is the product of $X-r$ and several other distinct irreducibles, two of which have degree $(q+1)/4$, $(q-3)/2$ of which have degree $(q+1)/2$, and $(q-3)/4$ of which have degree $q+1$. The two factors $R(X)$ of degree $(q+1)/4$ are determined by the choice of $\sqrt{-1}$; for $z^e = r$ these R satisfy

$$R(X^e) = \prod_{\zeta^e=1} \left(z^{(q+1)/4} D_{(q+1)/2} \left(\sqrt{\zeta X/z}, -1/4 \right) + \sqrt{-1} \right).$$

Here the choice of $\sqrt{\zeta X/z}$ is irrelevant, since $D_{(q+1)/2}$ is an even function. The factors $R(X)$ of degree $(q+1)/2$ are determined by the choices of a nonsquare element $\phi \in \mathbb{F}_q$ of the form $\theta^2 + \theta$ with $\theta \in \mathbb{F}_q \setminus \{-1/2\}$, and $\mu \in \mathbb{F}_{q^2}$ with $\mu^2 = \phi$; here, for $z^{2e} = r$,

$$R(X^{2e}) = \prod_{\zeta^{2e}=1} \left(z^{(q+1)/2} D_{(q+1)/2} \left(\zeta X/z \, - 1 - 2\theta, \phi \right) + 2\mu \right).$$

Here the choice of θ is irrelevant. The factors $R(X)$ of degree $q+1$ are determined by the choice of a nonzero square $\phi \in \mathbb{F}_q$ having the form $\theta^2 + \theta$ for some $\theta \in \mathbb{F}_q$; for $z^{2e} = r$ we have

$$R(X^{2e}) = \prod_{\zeta^{2e}=1} \left(z^{q+1} D_{q+1} \left(\zeta X/z \, - 1 - 2\theta, \phi \right) - \phi(2z^{q+1} + 4) \right).$$

Again, the choice of θ is irrelevant. Finally, one can make use of the well-known trivial relation $D_{mn}(X, a) = D_n(D_m(X, a), a^m)$ to rewrite the degree $(q+1)/4$ factors in the form given in the introduction.

7 Consequences of the factorization

In this section we note some consequences of the factorization proved above. In particular, we show that certain known properties of the $f_{q,d}$ follow at once from the bivariate factorization; this factorization provides new perspective on the known results, and we hope that this new perspective might lead to new results in the future. We begin by determining when $f_{q,d}$ is exceptional (over $\mathbb{F}_p$). To this end, note that each of the factors $R(X, Y)$ we have presented is monic in X (that is, monic when viewed as a member of $\overline{\mathbb{F}}_p[Y][X]$); thus, if no $R(X, Y)$ lies in $\mathbb{F}_p[X, Y]$, then also no scalar multiple of any $R(X,Y)$ lies in $\mathbb{F}_p[X,Y]$. So, when testing whether $f_{q,d}$ is exceptional, it suffices to check whether any $R(X,Y)$ lies in $\mathbb{F}_p[X,Y]$. Neither of the factors $R(X,Y)$ of degree $(q+1)/4$ lies in $\mathbb{F}_p[X,Y]$, since the coefficient of $X^{(e-1)(q+1)/4}$ in $R(X^e,Y^e)$ is $e\sqrt{-1} \notin \mathbb{F}_p$. The factors $R(X,Y)$ of degree $(q+1)/2$ do not lie in $\mathbb{F}_p[X,Y]$, since the coefficient of $X^{(2e-1)(q+1)/2}$ in $R(X^{2e},Y^{2e})$ is $4e\mu \notin \mathbb{F}_p$. But, for $p > 3$, there are factors of degree $q+1$ lying in $\mathbb{F}_p[X,Y]$: namely, choose any $\theta \in \mathbb{F}_p$ for which $\phi := \theta^2 + \theta$ is a nonzero square in $\mathbb{F}_p$; then the corresponding factor $R(X,Y)$ has coefficients in $\mathbb{F}_p$. This shows that $f_{q,d}$ is not exceptional when $p > 3$. If $p = 3$ there is no $\theta \in \mathbb{F}_p$ for which $\theta^2 + \theta$ is a nonzero square in $\mathbb{F}_p$. For any factor $R(X,Y)$ of degree $q+1$, the coefficient of $X^{(2e-1)(q+1)}$ in $R(X^{2e},Y^{2e})$ is $-8e\phi$; if this coefficient lies in $\mathbb{F}_p$, then ϕ and consequently θ lies in $\mathbb{F}_p$ as well, a contradiction when $p = 3$. Thus, for $p = 3$ the polynomial $f_{q,d}$ is exceptional.

Another consequence of the factorization is that $f_{q,d}(X)$ is indecomposable (over $\overline{\mathbb{F}}_p$) for $q \neq 7$ (i.e. it is not the (functional) composition of two lower-degree polynomials in $\overline{\mathbb{F}}_p[X]$). For, if $f_{q,d}(X) = g(h(X))$ with $g, h \in \overline{\mathbb{F}}_p[X]$, then $h(X) - h(Y)$ divides $\Delta := f_{q,d}(X) - f_{q,d}(Y)$, hence is the product of (a scalar and) $X - Y$ and several of the irreducible factors $R(X,Y)$ of Δ. In particular, the degree of h is simultaneously a divisor of the degree of $f_{q,d}$, namely $n = q(q-1)/2$, and a sum of 1 and several multiples of $(q+1)/4$; but, for $q \neq 7$, one easily checks that 1 and $q(q-1)/2$ are the only divisors of n congruent to 1 modulo $(q+1)/4$, whence f is indecomposable. We remark that the polynomials $f_{7,1}$ and $f_{7,2}$ have the unusual property of being indecomposable over $\mathbb{F}_7$ but decomposable over $\overline{\mathbb{F}}_7$; in fact, any indecomposable polynomial over a field which decomposes over a larger field, and which has degree not a power of the characteristic, must be a twist of one of $f_{7,1}$ or $f_{7,2}$ or either of two other polynomials (of degree 55 over $\mathbb{F}_{11}$), see [13].

There is more to be done along these lines. It would be very nice if one could recover from the factorization that the Galois group of $f_{q,d}(X) - s$ over $\overline{\mathbb{F}}_p(s)$ is $\mathrm{PSL}_2(q)$: the known approaches to these polynomials begin by conjecturing this Galois group and then produce the polynomials, but perhaps one can proceed in a converse manner by beginning with the factorization and deriving from it all known properties of the $f_{q,d}$. Hopefully these two approaches could somehow be combined to yield a direct approach which produces the $f_{q,d}$ without any hints. As a first step, now that we know the factorization, it should be possible to give a quick elementary verification of it. It could also be hoped that a study of the factorization would lead to the discovery of new properties of the polynomials $f_{q,d}$.

Appendix A: Exceptional polynomials

In this appendix we briefly review the theory of exceptional polynomials; see [9] for more details. Following [6], we say a univariate polynomial $f(X)$ over a field k is an exceptional polynomial (over k) if the only absolutely irreducible factors of $f(X)-f(Y)$ in $k[X,Y]$ are the scalar multiples of $X-Y$. If f is exceptional, then the mapping $k \to k$ given by $a \mapsto f(a)$ is injective outside a finite set; a major open problem is to determine whether in fact this mapping is always injective. This is true, for instance, when k is finite, in which case there is an equivalent description of exceptional polynomials: they are precisely the polynomials inducing bijective mappings $\ell \to \ell$ for infinitely many finite extensions ℓ of k (the proof relies on the Riemann hypothesis for curves over finite fields (Weil's theorem)). This property makes exceptional polynomials over finite fields valuable for applications in coding theory and cryptography. One consequence of the property is that, if $f(X) \in \mathbb{F}_q[X]$ induces bijections on $\mathbb{F}_{q^n}$ for infinitely many n, then these values n include all numbers coprime to some fixed $N > 0$. It follows that, for $g, h \in \mathbb{F}_q[X]$, the composition $g(h)$ is exceptional if and only if both g and h are exceptional. Hence, the study of exceptional polynomials over finite fields k reduces to the case of indecomposable exceptional polynomials.

There are extremely few known examples of indecomposable exceptional polynomials. The classical examples trace back to Dickson's 1897 thesis [7]; these include certain cyclic polynomials X^n, certain additive polynomials $\sum a_i X^{p^i}$ (with $p = \mathrm{char}(k)$), and certain modifications of these two families (where, for instance, the modified cyclic polynomials are the Dickson polynomials). These classical families are surveyed in [4]. No essentially new examples were found between 1897 and 1993. Then came the seminal work of Fried, Guralnick, and Saxl [9], which showed that for any indecomposable exceptional polynomial f over a finite field k, either $\mathrm{Gal}(f(X)-t, k(t))$ is an affine group (in which case f has prime power degree), or k has characteristic 2 or 3 in which case certain other possibilities could not be ruled out. All the classical examples resided in the affine case, so it was not known whether non-affine examples would occur. However, in a sense [9] showed where to look for these, and in the ensuing two years examples were produced in characteristic 2 by Müller, Cohen and Matthews, and in characteristic 3 by Lenstra and the author. Recently Guralnick and I have classified all non-affine indecomposable exceptional polynomials over any finite field; they are all 'twists' of the previously known examples. But much work remains to be done in the affine case; new examples were exhibited by Guralnick and Müller [11], but there will probably be many further examples and it is not clear whether it is feasible to classify them all.

Appendix B: Factorizations in characteristic 2

In this appendix we sketch how our general method for factoring $f(X) - f(Y)$ applies when f is one of the (non-affine) indecomposable exceptional polynomials over fields of characteristic 2 discovered by Müller, Cohen, and Matthews. As noted in the introduction, our derivation of this factorization is very different from the verification found in [5]; in particular, we are able to explain the previously mysterious occurrence of Dickson polynomials in the factorization. The polynomials in question are defined as follows: for any $\ell \geq 2$ and any divisor d of $2^\ell + 1$, put $q = 2^\ell$ and

$$g_{\ell,d}(X) = X \left(\sum_{i=0}^{\ell-1} X^{(2^i-1)d} \right)^{(q+1)/d}.$$

Then $g_{\ell,d}(X) \in \mathbb{F}_2[X]$ is indecomposable (even over $\overline{\mathbb{F}}_2$) and, when ℓ is odd, it is exceptional over $\mathbb{F}_2$. In [5] these properties of the $g_{\ell,d}$ are shown to be immediate consequences of the factorization of $g_{\ell,d}(X) - g_{\ell,d}(Y)$ (over $\overline{\mathbb{F}}_2[X,Y]$); alternately one can prove these properties group theoretically, without mentioning the factorization [12].

We now state the factorization. Let $T(X) = \sum_{i=0}^{\ell-1} X^{2^i}$; the values of this polynomial on $\mathbb{F}_q$ coincide with the values of the trace map $\mathbb{F}_q \to \mathbb{F}_2$ (so the $q/2$ distinct roots of T all lie in $\mathbb{F}_q$). Then, for $e = (q+1)/d$,

$$g_{\ell,d}(X) - g_{\ell,d}(Y) = (X - Y) \prod_{\substack{T(\delta)=0 \\ \delta \neq 0}} R_\delta(X,Y), \qquad (\dagger)$$

where each $R_\delta(X,Y)$ is an irreducible polynomial in $\overline{\mathbb{F}}_2[X,Y]$ of degree $q+1$; explicitly,

$$R_\delta(X^e, Y^e) = \prod_{\zeta^e=1} \left(Y^{q+1} D_{q+1}\left(\frac{\zeta X/Y + 1}{\sqrt{\delta}}, 1 \right) + 1 \right).$$

Henceforth we write g for $g_{\ell,d}$ and f for $g_{\ell,1}$.

We begin by computing the degrees of the irreducible factors of $g(X) - g(Y)$ in $\overline{\mathbb{F}}_2[X,Y]$. As in Section 2, $g(X)-g(Y)$ is the product of several distinct irreducible factors, whose degrees are the subdegrees of the permutation group $\operatorname{Gal}(g(X)-s, \overline{\mathbb{F}}_2(s))$. This group is isomorphic to $\mathrm{PGL}_2(q)$ in its transitive permutation representation with one-point stabilizer a dihedral group of order $q+1$. One computes the subdegrees in a manner similar to that of Section 4, and finds that they are all $q+1$ except a single one which is one (corresponding to the factor $X-Y$).

Next we compute the roots of $g(X)-s$. From [12], for $t = s^d$ the splitting field of $f(X)-t$ over $\overline{\mathbb{F}}_2(t)$ is $\overline{\mathbb{F}}_2(u)$, and the splitting field of $g(X)-s$ over $\overline{\mathbb{F}}_2(s)$ is $\overline{\mathbb{F}}_2(u,s)$. The restriction map induces an isomorphism between $G := \operatorname{Gal}(\overline{\mathbb{F}}_2(u,s)/\overline{\mathbb{F}}_2(s))$ and $\operatorname{Gal}(\overline{\mathbb{F}}_2(u)/\overline{\mathbb{F}}_2(t))$, where the elements of the latter group are the $\overline{\mathbb{F}}_2$-isomorphisms of $\overline{\mathbb{F}}_2(u)$ sending u to $(Eu+F)/(\bar{F}u+\bar{E})$, for any choice of $E, F \in \mathbb{F}_{q^2}$ such that $E\bar{E}+F\bar{F}=1$ (here $\bar{E} := E^q$). One root $r \in \overline{\mathbb{F}}_2(u,s)$ of $g(X)-s$ satisfies $r^{-d} = u^{q+1} + u^{-(q+1)}$; the other roots are the images of r under G, which we compute (as in Section 5) to be rw^e for $e = (q+1)/d$ and $w = 1 + E\bar{F}u + \bar{E}Fu^{-1}$.

Finally we compute the minimal polynomials over $\overline{\mathbb{F}}_2(r)$ for these roots. Assume $rw^e \neq r$. Put $\gamma = E\bar{E}F\bar{F}$. Then w is a root of the polynomial $P(X) = D_{q+1}(X+1,\gamma) + \gamma r^{-d}$. Next, w^e is a root of $Q(X) \in \overline{\mathbb{F}}_2(r)[X]$ defined by $Q(X^e) = \prod_{\zeta^e=1} P(\zeta X)$. Thus rw^e is a root of $\hat{R}(X) = r^{q+1}Q(X/r)$, which is a monic polynomial in $\overline{\mathbb{F}}_2(r)[X]$ of degree $q+1$, hence is the minimal polynomial for rw^e over $\overline{\mathbb{F}}_2(r)$. Note that $\hat{R}$ is determined by the value of γ, and $\gamma = \theta^2+\theta$ for $\theta := F\bar{F} \in \mathbb{F}_q^*$; hence $T(\gamma)=0$. Now denoting $\hat{R}(X)$ by $\hat{R}_\delta(X)$, it follows that

$$g(X) - g(r) = (X-r) \prod_{\substack{T(\delta)=0 \\ \delta\neq 0}} \hat{R}_\delta(X).$$

It remains to recover $R_\delta(X,Y)$ from $\hat{R}_\delta(X)$. For $z^e = r$, note that $g(X^e) - g(z^e) = g(X^e) - s$ is the product of $X^e - Y^e$ and the various $\hat{R}_\delta(X^e)$, each of which is monic and irreducible in $\overline{\mathbb{F}}_2(r)[X^e]$. But

$$\hat{R}_\delta(X^e) = r^{q+1} \prod_{\zeta^e=1} P(\zeta X/z) = \prod_{\zeta^e=1} \left(z^{q+1} D_{q+1}(\zeta X/z + 1, \gamma) + \gamma \right)$$

lies in $\overline{\mathbb{F}}_2[r^e, X^e]$; substituting Y for z and X for X^e, we see that $g(X) - g(Y) = (X-Y)\prod_\delta \check{R}_\delta(X,Y)$, where $\check{R}_\delta$ is the irreducible polynomial in

$\overline{\mathbb{F}}_2[X,Y]$ defined by

$$\check{R}_\delta(X^e,Y^e)=\prod_{\zeta^e=1}\left(Y^{q+1}D_{q+1}(\zeta X/Y+1,\gamma)+\gamma\right).$$

Standard trivial properties of Dickson polynomials imply that R_δ is a scalar multiple of $\check{R}_\delta$, which completes our derivation of the factorization (†).

Note that $g_{\ell,d}(X)=X^{-q}T(X^d)^{(q+1)/d}$; such a simple expression for $g_{\ell,d}$ seems to merit a better explanation than is presently known.

References

[1] S. S. Abhyankar, Galois theory on the line in nonzero characteristic, *Bull. Amer. Math. Soc.* **27** (1992), 68–133.

[2] S. S. Abhyankar, Nice equations for nice groups, *Israel J. Math.* **88** (1994), 1–24.

[3] S. S. Abhyankar, S. D. Cohen, and M. E. Zieve, Bivariate factorizations connecting Dickson polynomials and Galois theory, *Trans. Amer. Math. Soc.*, to appear.

[4] S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseign. Math.* **36** (1990), 53–65.

[5] S. D. Cohen and R. M. Matthews, Exceptional polynomials, *Finite Fields Appl.* **1** (1995), 261–277.

[6] H. Davenport and D. J. Lewis, Notes on Congruences (I), *Quart. J. Math. Oxford, Ser. 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, *Annals Math.* **11** (1897), 65–120.

[8] L. E. Dickson, "Linear groups with an exposition of the Galois field theory," 1901 (reprinted Dover, New York, 1958).

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

[10] D. Gorenstein, "Finite groups," Harper&Row, New York, 1968.

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

[12] R. M. Guralnick and M. Zieve, Exceptional rational functions of small genus, in preparation.

[13] R. M. Guralnick and M. Zieve, Polynomials with prescribed monodromy, preprint.

[14] B. Huppert, "Endliche gruppen," Springer-Verlag, Berlin, 1967.

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

[16] H. W. Lenstra, Jr. and M. Zieve, Exceptional maps between varieties, in preparation.

[17] M. Suzuki, "Group theory. I.," Springer-Verlag, New York, 1982.