Bivariate identities related to Chebyshev and Dickson polynomials over $\mathbb{F}_q$

Ron Evans
Department of Mathematics
University of California at San Diego
La Jolla, CA 92093-0112
revans@ucsd.edu

and

Mark Van Veen
Varasco LLC
2138 Edinburg Avenue
Cardiff by the Sea, CA 92007
mark@varasco.com

July 2017

2010 *Mathematics Subject Classification.* 11T06, 12E10, 13P05.
Key words and phrases. reversed Dickson polynomials over finite fields, Chebyshev polynomial, bivariate polynomial factorization, polynomial splitting field, quadratic residuacity.

Abstract

Let $\mathbb{F}_q$ be a field of q elements, where q is a power of an odd prime p. The polynomial $f(y) \in \mathbb{F}_q[y]$ defined by

$$f(y) := (1+\sqrt{y})^{(q+1)/2} + (1-\sqrt{y})^{(q+1)/2}$$

has the property that

$$f(1-y) = \rho(2) f(y),$$

where ρ is the quadratic character on $\mathbb{F}_q$. This univariate identity was applied to prove a recent theorem of N. Katz. We formulate and prove a bivariate extension, and give an application to quadratic residuacity.

1 Introduction

Let $\mathbb{F}_q$ be a field of q elements, where q is a power of an odd prime p. Fix

$$n = (q+1)/2, \tag{1.1}$$

and define a polynomial $f(y) \in \mathbb{F}_q[y]$ of degree $[n/2]$ by

$$f(y) := (1+\sqrt{y})^n + (1-\sqrt{y})^n.$$

The leading coefficient of f is

$$\tau = \begin{cases} 1, & \text{if } q \equiv 1 \bmod 4 \\ 2, & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

In $\mathbb{F}_q[y]$,

$$f(y) = D_n(2, 1-y),$$

where $D_n(2, 1-y)$ is a reversed Dickson polynomial [2, p. 436], and

$$f(y) = 2z^n \, T_n(1/z), \qquad z = \sqrt{1-y},$$

where T_n is the Chebyshev polynomial of the first kind [4, (1.49)].

By virtue of our choice of n in (1.1), the polynomial f has some interesting number-theoretic properties; for example [3, Lemma 16.6],

$$f(1-y) - \rho(2) f(y) = 0, \tag{1.2}$$

where ρ is the quadratic character on $\mathbb{F}_q$. Identity (1.2) was instrumental in the proof of a recent theorem of Katz [3, Theorem 16.3]. The purpose of this paper is to extend (1.2) by proving the following pair of bivariate polynomial identities in $\mathbb{F}_q[x, y]$:

$$(f(y) + f(x))/\tau \equiv \begin{cases} \prod_{c\in\mathcal{A}} g(x, y, c), & \text{if } q \equiv \pm 1 \bmod 8, \\ (y + x - 1) \prod_{c\in\mathcal{A}} g(x, y, c), & \text{if } q \equiv \pm 3 \bmod 8, \end{cases} \tag{1.3}$$

and

$$(f(y) - f(x))/\tau \equiv \begin{cases} (y - x)(y + x - 1) \prod_{c\in\mathcal{B}} g(x, y, c), & \text{if } q \equiv \pm 1 \bmod 8, \\ (y - x) \prod_{c\in\mathcal{B}} g(x, y, c), & \text{if } q \equiv \pm 3 \bmod 8. \end{cases} \tag{1.4}$$

where

$$g(x, y, c) := (x + y - c)^2 + 4xy(c - 1),$$

$$\mathcal{A} = \{c \in \mathbb{F}_q : \rho(c) = 1,\ \rho(1 + \sqrt{c}) = \rho(1 - \sqrt{c}) = -1\},$$

and

$$\mathcal{B} = \{c \in \mathbb{F}_q : \rho(c) = 1,\ \rho(1 + \sqrt{c}) = \rho(1 - \sqrt{c}) = 1\}.$$

Here the symbol $\equiv$ signifies that the polynomials on both sides are identical. Substitution of $1 - y$ for x in these identities immediately yields (1.2), since $\rho(2)$ equals 1 or -1 according as q is ± 1 or ± 3 modulo 8.

The difference of Dickson polynomials $D_n(y, a) - D_n(x, a) \in \mathbb{F}_q[x, y]$ has been factored by Bhargava and Zieve [1]. In contrast, for $n = (q+1)/2$, (1.4) yields a factorization of the difference of *reversed* Dickson polynomials

$$D_n(2, y) - D_n(2, x) \in \mathbb{F}_q[x, y],$$

in view of (1.2).

Identities (1.3) and (1.4) will follow from Theorem 3.1, whose proof depends on a series of lemmas in Section 2. Theorem 3.1 has an application to quadratic residuacity: for example, Corollary 3.2 shows that when $q \equiv \pm 1 \bmod 8$ and $c \in \mathcal{A}$ and $d \in \mathcal{B}$, then

$$\rho(1 + \sqrt{c - cd} + \sqrt{d - cd}) = -1$$

for every possible choice of signs of the square roots. Our demonstration of Theorem 3.1, though intricate, is elementary and entirely self-contained.

2 Lemmas

Lemma 2.1 appears in [3, Lemma 16.6], but we include it here for completeness.

Lemma 2.1. *We have* $f(y)^2 \equiv 2(1+y^n+(1-y)^n)$ *and* $f(y) \equiv \rho(2)f(1-y)$.

Proof. Let $x \in \mathbb{F}_q$. By the definition of f,

$$f(1-x)^2 = (1+\sqrt{1-x})^{q+1} + (1-\sqrt{1-x})^{q+1} + 2x^n.$$

If $\rho(1-x) = 1$, then

$$f(1-x)^2 = (1+\sqrt{1-x})^2 + (1-\sqrt{1-x})^2 + 2x^n = 2(2-x+x^n).$$

If $\rho(1-x) = -1$, then since $(\sqrt{1-x})^q = -\sqrt{1-x}$,

$$f(1-x)^2 = 2(x+x^n).$$

Thus if $x \neq 1$,

$$\begin{aligned} f(1-x)^2 &= (1+(1-x)^{n-1})(2-x+x^n) + (1-(1-x)^{n-1})(x+x^n) \\ &= 2 + 2x^n + (1-x)^{n-1}(2-2x) = 2(1+x^n+(1-x)^n). \end{aligned} \tag{2.1}$$

This holds as well for $x = 1$, so it holds for all $x \in \mathbb{F}_q$. Since the polynomials on both sides of (2.1) have degree less than q, it follows that

$$f(1-y)^2 \equiv 2(1+y^n+(1-y)^n) \equiv f(y)^2.$$

Therefore $f(y) \equiv \pm f(1-y)$. The constant terms of $f(y)$ and $f(1-y)$ are 2 and $2\rho(2)$ respectively, which proves that $f(y) \equiv \rho(2)f(1-y)$. □

Define

$$\mathcal{S} := \{0,1\} \cup \{u \in \mathbb{F}_q : \rho(u-u^2) = 1\}.$$

Lemma 2.2. *We have*

$$|\mathcal{S}| = 2[n/2] + 1,$$

$$|\mathcal{A}| = \begin{cases} [n/2]/2, & q \equiv \pm 1 \bmod 8 \\ ([n/2]-1)/2, & q \equiv \pm 3 \bmod 8, \end{cases}$$

and

$$|\mathcal{B}| = \begin{cases} ([n/2]-2)/2, & q \equiv \pm 1 \bmod 8 \\ ([n/2]-1)/2, & q \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. We give only the proof for $|\mathcal{A}|$, since the other proofs are similar. The cardinality $|\mathcal{A}|$ is given by the quadratic character sum

$$|\mathcal{A}| = \frac{1}{8}\sum (1-\rho(1+x))(1-\rho(1-x)),$$

where the sum is over all $x \in \mathbb{F}_q$ with $x \notin \{-1, 0, 1\}$. Thus

$$|\mathcal{A}| = \frac{2\rho(2)-2}{8} + \frac{1}{8}\sum_{x\in\mathbb{F}_q} (1-\rho(1+x))(1-\rho(1-x)).$$

Since $q = 2n-1$, this yields

$$|\mathcal{A}| = \frac{2\rho(2)+2n-3}{8} + \frac{1}{8}\sum_{x\in\mathbb{F}_q} \rho(1+x)\rho(1-x).$$

With the change of variable $x = 2t-1$, the sum on x becomes

$$\sum_{t\in\mathbb{F}_q^*} \rho(t)\rho(1-t) = \sum_{t\in\mathbb{F}_q^*} \rho(t^{-1}-1) = -\rho(-1).$$

Thus

$$|\mathcal{A}| = \frac{2\rho(2)+2n-3-\rho(-1)}{8}.$$

Lemma 2.2 for $|\mathcal{A}|$ now easily follows. □

Lemma 2.3 is the special instance $x = 0$ of our identities (1.3) and (1.4).

Lemma 2.3. *We have*

$$(f(y)+2)/\tau \equiv \begin{cases} \prod_{c\in\mathcal{A}} (y-c)^2, & \text{if } q \equiv \pm 1 \bmod 8 \\ (y-1)\prod_{c\in\mathcal{A}} (y-c)^2, & \text{if } q \equiv \pm 3 \bmod 8, \end{cases} \tag{2.2}$$

and

$$(f(y)-2)/\tau \equiv \begin{cases} y(y-1)\prod_{c\in\mathcal{B}} (y-c)^2, & \text{if } q \equiv \pm 1 \bmod 8 \\ y\prod_{c\in\mathcal{B}} (y-c)^2, & \text{if } q \equiv \pm 3 \bmod 8. \end{cases} \tag{2.3}$$

Proof. By Lemma 2.2, the products in (2.2) and (2.3) each have degree $\deg f = [n/2]$. Since $f(1) = 2\rho(2)$ and the derivatives $f'(0)$ and $f'(1)$ do not vanish, the factors y and $y-1$ occur with the correct multiplicities in (2.2) and (2.3).

Let $\epsilon = \pm 1$ and choose $c \in \mathbb{F}_q$ such that

$$\rho(c) = 1, \quad \rho(1+\sqrt{c}) = \rho(1-\sqrt{c}) = \epsilon.$$

By definition of f,

$$f(c) = \rho(1+\sqrt{c})(1+\sqrt{c}) + \rho(1-\sqrt{c})(1-\sqrt{c}) = 2\epsilon,$$

so c is a zero of $f(y) - 2\epsilon$. Each such zero c has multiplicity greater than 1, since the derivative $f'(c)$ equals

$$f'(c) = \frac{n}{2\sqrt{c}}\big(\rho(1+\sqrt{c}) - \rho(1-\sqrt{c})\big) = 0.$$

Therefore the products in (2.2) and (2.3) divide the polynomials $f(y)+2$ and $f(y)-2$, respectively. Thus equality holds in (2.2) and (2.3) , since the polynomials on both sides are monic with the same degree. □

Remark 1. *Lemma 2.3 and* (1.2) *together yield the nontrivial facts that*

$$c \in \mathcal{A} \text{ if and only if } 1-c \in \mathcal{A}, \text{ when } q \equiv \pm 1 \bmod 8,$$

and

$$c \in \mathcal{A} \text{ if and only if } 1-c \in \mathcal{B}, \text{ when } q \equiv \pm 3 \bmod 8.$$

Remark 2. *For a fixed x algebraic over $\mathbb{F}_q$ with $f(x) \neq \pm 2$, the zeros of the polynomials $f(y) \pm f(x)$ are all distinct. This is because Lemmas 2.3 and 2.2 together show that the zeros of the derivative $f'(y)$ are precisely the $[n/2]-1$ elements in $\mathcal{A} \cup \mathcal{B}$.*

For each c in the set

$$\{0,1\} \cup \mathcal{A} \cup \mathcal{B} = \{0,1\} \cup \{c \in \mathbb{F}_q : \rho(c) = \rho(1-c) = 1\},$$

define the pair of functions

$$\alpha_c(x) = \left(\sqrt{c}\sqrt{1-x} + \sqrt{1-c}\sqrt{x}\right)^2,\ \alpha_c'(x) = \left(\sqrt{c}\sqrt{1-x} - \sqrt{1-c}\sqrt{x}\right)^2.$$

If $x \in \mathcal{S}$, then $\alpha_c(x)$ and $\alpha_c'(x)$ are in $\mathcal{S}$, because

$$\alpha_c(x) - \alpha_c(x)^2 = \left((2c-1)\sqrt{x-x^2} + (2x-1)\sqrt{c-c^2}\right)^2$$

and

$$\alpha_c'(x) - \alpha_c'(x)^2 = \left((2c-1)\sqrt{x-x^2} - (2x-1)\sqrt{c-c^2}\right)^2.$$

Lemma 2.4. *If $\alpha_c(x) = 0$ or $\alpha_c'(x) = 0$, then $x = c$. If $\alpha_c(x) = 1$ or $\alpha_c'(x) = 1$, then $x = 1 - c$.*

Proof. If $\alpha_c(x) = 0$ or $\alpha_c'(x) = 0$, then $\sqrt{c - cx} = \pm\sqrt{x - cx}$, so that $x = c$. Now suppose that $\alpha_c(x) = 1$ or $\alpha_c'(x) = 1$. Then

$$\sqrt{c - cx} = \pm\sqrt{x - cx} \pm 1$$

so that squaring both sides yields $c - x - 1 = \pm 2\sqrt{x - cx}$. Squaring both sides again yields $(c + x - 1)^2 = 0$ so that $x = 1 - c$. □

Lemma 2.5. *For each $x \in \mathcal{S}$ and each $c \in \{0,1\} \cup \mathcal{A} \cup \mathcal{B}$,*

$$f(\alpha_c(x))^2 = f(\alpha_c'(x))^2 = f(x)^2.$$

Proof. We consider just $\alpha_c(x)$, since the argument for $\alpha_c'(x)$ is the same. It follows from (1.2) and Lemma 2.3 that

$$f(c)^2 = f(1-c)^2 = f(0)^2 = f(1)^2 = 4.$$

Therefore by Lemma 2.4, Lemma 2.5 holds when $x \in \{0,1\}$ or $\alpha_c(x) \in \{0,1\}$. Thus we may assume that $x \notin \{0,1\}$ and $\alpha_c(x) \notin \{0,1\}$. By Lemma 2.1,

$$f(x)^2 = 2(1 + x\rho(x) + (1-x)\rho(1-x)) = 2(1 + \rho(x)),$$

since $\rho(1-x)=\rho(x)$. Since $\alpha_c(x)\in\mathcal{S}$, we similarly have

$$f(\alpha_c(x))^2 = 2(1+\rho(\alpha_c(x))).$$

Thus

$$f(x)^2 - f(\alpha_c(x))^2 = 2(\rho(x)-\rho(\alpha_c(x))).$$

Finally, the right side above vanishes because

$$\frac{\alpha_c(x)}{x} = c\Big(\frac{\sqrt{x-x^2}}{x}+\frac{\sqrt{c-c^2}}{c}\Big)^2$$

is a square in $\mathbb{F}_q$. □

Lemma 2.6 proves the nontrivial fact that $f(\alpha_c(y))$ is a polynomial in $\mathbb{F}_q[y]$. Since $\alpha_1(y)=1-y$, (1.2) is the special case $c=1$ of Lemma 2.6.

Lemma 2.6. *For each fixed $c\in\{0,1\}\cup\mathcal{A}\cup\mathcal{B}$,*

$$f(\alpha_c(y)),\ f(\alpha_c'(y))\in\mathbb{F}_q[y]$$

and

$$f(\alpha_c(y)) \equiv f(\alpha_c'(y)) \equiv \rho(1+\sqrt{c})f(y),$$

where $\sqrt{c}$ is interpreted as 1 in the case $c=1$.

Proof. For some polynomials $g,h\in\mathbb{F}_q[y]$,

$$f(\alpha_c(y)) = g+\sqrt{y-y^2}\ h \tag{2.4}$$

and

$$f(\alpha_c'(y)) = g-\sqrt{y-y^2}\ h. \tag{2.5}$$

Thus

$$f(\alpha_c(y))^2 + f(\alpha_c'(y))^2 = 2g^2+2(y-y^2)h^2$$

and

$$f(\alpha_c(y))^2 - f(\alpha_c'(y))^2 = 4\sqrt{y-y^2}\ gh.$$

Then by Lemma 2.5,

$$f(x)^2 = g(x)^2+(x-x^2)h(x)^2, \quad \text{for all } x\in\mathcal{S} \tag{2.6}$$

and

$$(x - x^2)g(x)h(x) = 0, \quad \text{for all } x \in \mathcal{S}. \tag{2.7}$$

We proceed to show that the polynomials $f(y)^2$ and $g(y)^2$ have the same leading term.

Case 1: $q \equiv 3 \bmod 4$, so 2 divides n.

By Lemma 2.3, $f(y)$ has leading term $2y^{n/2}$, so by (2.4), the leading term of $g(y)$ must appear among the terms in the expansion of $2\alpha_c(y)^{n/2}$. By definition of $\alpha_c(y)$, for some choice of the square roots,

(2.8)

$$2\alpha_c(y)^{n/2} = 2(\sqrt{c - cy} + \sqrt{y - cy})^n = 2\sum_{j=0}^{n} \binom{n}{j} (\sqrt{c - cy})^{n-j} (\sqrt{y - cy})^j.$$

Only the terms with even j can contribute to the polynomial $g(y)$, so the leading term of $g(y)$ must appear among the terms in the expansion of

$$2\sum_{i=0}^{n/2} \binom{n}{2i} (c - cy)^{n/2-i} (y - cy)^i.$$

The leading term of $g(y)$ is thus

$$(-y)^{n/2} c^{n/2} 2 \sum_{i=0}^{n/2} \binom{n}{2i} (1 - 1/c)^i.$$

By the definition of f and (1.2),

$$2\sum_{i=0}^{n/2} \binom{n}{2i} (1 - 1/c)^i = f(1 - 1/c) = \rho(2) f(1/c).$$

By the definition of f and Lemma 2.3,

$$c^{n/2} f(1/c) = (1 + \sqrt{c})^n + (1 - \sqrt{c})^n = f(c) = \pm 2.$$

Thus $g(y)^2$ has leading term $4y^n$, and this matches the leading term of $f(y)^2$.

Case 2: $q \equiv 1 \bmod 4$, so 2 divides $n - 1$.

By Lemma 2.3, $f(y)$ has leading term $y^{(n-1)/2}$, so the leading term of $g(y)$ must appear among the terms in the expansion of $\alpha_c(y)^{(n-1)/2}$. Arguing as in Case 1, we see that the leading term of $g(y)$ is

$$(-y)^{(n-1)/2} c^{(n-1)/2} \sum_{i=0}^{(n-1)/2} \binom{n-1}{2i} (1-1/c)^i.$$

Now,

$$\begin{aligned} 2 \sum_{i=0}^{(n-1)/2} \binom{n-1}{2i} (1-1/c)^i &= (1+\sqrt{1-1/c})^{n-1} + (1-\sqrt{1-1/c})^{n-1} \\ &= \rho(1+\sqrt{1-1/c}) + \rho(1-\sqrt{1-1/c}) = 2\rho(1+\sqrt{1-1/c}). \end{aligned}$$

Since $c^{(n-1)/2} = \rho(\sqrt{c})$, $g(y)$ has leading term $\pm\rho(\sqrt{c}+\sqrt{c-1})y^{(n-1)/2}$. Hence both $g(y)^2$ and $f(y)^2$ have the leading term y^{n-1}. This completes the demonstration that $f(y)^2$ and $g(y)^2$ have the same leading term in all cases.

Assume for the purpose of contradiction that the polynomial $h(y)$ is not identically zero. By (2.7), every $x \in \mathcal{S}$ with $x \notin \{0,1\}$ is a zero of $g(y)h(y)$. By Lemma 2.2, $|\mathcal{S}| = 2[n/2]+1$, so that $\deg h \geq [n/2]-1$. On the other hand, one sees that $\deg h \leq [n/2]-1$ by looking at the expansion of $\alpha_c(y)^{[n/2]}$; for example, in Case 1, one looks at the terms in (2.8) with odd j, for they are the terms that can contribute to h. Consequently, $\deg h = [n/2]-1$. Thus the polynomial $f(y)^2 - g(y)^2 - (y-y^2)h(y)^2$ has degree less than or equal to $2[n/2]$. However, by (2.6), this polynomial has $|\mathcal{S}| > 2[n/2]$ zeros, so

$$f(y)^2 - g(y)^2 \equiv (y-y^2)h(y)^2.$$

The right side is a polynomial of degree $2[n/2]$, but the left side has degree less than $2[n/2]$, because $f(y)^2$ and $g(y)^2$ have the same leading term. This contradiction shows that h is identically zero.

By (2.6), the polynomial $f(y)^2 - g(y)^2$ has $|\mathcal{S}| > 2[n/2]$ zeros, so we have $f(y)^2 - g(y)^2 \equiv 0$. Thus $g(y) \equiv \pm f(y)$. By definition of f, its constant term is $f(0) = 2$. Since $f(\alpha_c(y)) = f(\alpha_c'(y)) = g(y)$ by (2.4) and (2.5), the constant term of g is

$$g(0) = f(\alpha_c(0)) = f(c) = 2\rho(1+\sqrt{c}),$$

by Lemma 2.3. Thus $g(y) \equiv \rho(1+\sqrt{c})f(y)$, which yields the desired result. □

Lemma 2.7. *Let $c_1, c_2, \ldots$ run through all the elements of $\mathcal{A} \cup \mathcal{B}$. For a fixed $x \in \mathbb{F}_q$, let L denote the list*

$$\alpha_0(x), \alpha_1(x), \alpha_{c_1}(x), \alpha'_{c_1}(x), \alpha_{c_2}(x), \alpha'_{c_2}(x), \ldots \ .$$

Then no three separate entries in L can be equal. Moreover, at most one entry in L can equal 0, and at most one entry in L can equal 1.

Proof. We first show that at most two entries of L can be equal to some fixed element u. Suppose that $\alpha_c(x) = u$ or $\alpha'_c(x) = u$ for some $c \in \{0,1\} \cup \mathcal{A} \cup \mathcal{B}$. Then solving for c, we find that

$$c = u + (1-2u)x \pm 2\sqrt{(u-u^2)(x-x^2)}.$$

If $x \in \{0,1\}$ or $u \in \{0,1\}$, then the square root vanishes and there is only one solution c, so no three entries in L can equal u in this case. Thus it suffices to assume that neither x nor u is in $\{0,1\}$ and that there are two distinct solutions $c \in \{0,1\} \cup \mathcal{A} \cup \mathcal{B}$, say $c = i$ and $c = j$.

Suppose for the purpose of contradiction that there exist three entries in L equal to u. Then without loss of generality, these three entries are $\alpha_i(x)$, $\alpha'_i(x)$, and $\alpha_j(x)$, where necessarily $i \notin \{0,1\}$ since L does not contain a pair of entries of the form $\alpha_i(x)$, $\alpha'_i(x)$ when i equals 0 or 1. This yields the desired contradiction, since $\alpha_i(x)$ cannot equal $\alpha'_i(x)$ when $i \notin \{0,1\}$. Thus at most two entries in L can equal u.

Suppose that $\alpha_c(x) = 0$ or $\alpha'_c(x) = 0$. Then $c = x$ by Lemma 2.4. Thus if two entries of L were to vanish, they would have to be $\alpha_x(x)$ and $\alpha'_x(x)$ with $x \notin \{0,1\}$. But $\alpha_x(x)$ cannot equal $\alpha'_x(x)$, so at most one entry of L can vanish.

Finally, suppose that $\alpha_c(x) = 1$ or $\alpha'_c(x) = 1$. Then $c = 1 - x$ by Lemma 2.4. Thus if two entries of L were to equal 1, they would have to be $\alpha_{1-x}(x)$ and $\alpha'_{1-x}(x)$ with $x \notin \{0,1\}$. But $\alpha_{1-x}(x)$ cannot equal $\alpha'_{1-x}(x)$, so at most one entry of L can equal 1. □

3 Main results

The following theorem immediately yields identities (1.3) and (1.4), since

$$g(x,y,c) = (y - \alpha_c(x))(y - \alpha'_c(x)), \quad \alpha_0(x) = x, \ \alpha_1(x) = 1 - x.$$

Theorem 3.1.

$$(f(y)+f(x))/\tau \equiv$$

$$\begin{cases} \prod_{c\in\mathcal{A}} (y-\alpha_c(x))(y-\alpha_c'(x)), & \text{if } q \equiv \pm 1 \bmod 8, \\ (y-\alpha_1(x)) \prod_{c\in\mathcal{A}} (y-\alpha_c(x))(y-\alpha_c'(x)), & \text{if } q \equiv \pm 3 \bmod 8, \end{cases} \tag{3.1}$$

and

(3.2)

$$(f(y)-f(x))/\tau \equiv$$

$$\begin{cases} (y-\alpha_0(x))(y-\alpha_1(x)) \prod_{c\in\mathcal{B}} (y-\alpha_c(x))(y-\alpha_c'(x)), & \text{if } q \equiv \pm 1 \bmod 8, \\ (y-\alpha_0(x)) \prod_{c\in\mathcal{B}} (y-\alpha_c(x))(y-\alpha_c'(x)), & \text{if } q \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. View both sides of (3.1) and (3.2) as polynomials in y. For brevity, refer to the left and right sides of these equations as $M(y)$ and $N(y)$, respectively. We begin by proving that $M(y) \equiv N(y)$ for each fixed $x \in \{0,1\} \cup \mathcal{A} \cup \mathcal{B}$.

By Lemma 2.3, $M(y) \equiv N(y)$ when $x = 0$. Also, since $f(1) = 2\rho(2)$ and $\alpha_c(1) = \alpha_c'(1) = 1 - c$, Lemma 2.3 and Remark 1 show that $M(y) \equiv N(y)$ for $x = 1$ as well. Now fix $x \in \mathcal{A} \cup \mathcal{B}$.

By Lemma 2.6, every zero of $N(y)$ is a zero of $M(y)$. Since $x \in \mathcal{A} \cup \mathcal{B}$, we have $f(x) = \pm 2$ by Lemma 2.3. Also by Lemma 2.3, each zero of $M(y)$ equal to 0 or 1 has multiplicity 1, while every other zero of $M(y)$ has multiplicity 2. By Lemma 2.7, each zero of $N(y)$ equal to 0 or 1 has multiplicity 1, and every other zero of $N(y)$ has multiplicity at most 2. Therefore $N(y)$ divides $M(y)$. Since $M(y)$ and $N(y)$ are both monic of degree $[n/2]$, they are equal. Thus we've proved that $M(y) \equiv N(y)$ for each $x \in \{0,1\} \cup \mathcal{A} \cup \mathcal{B}$.

Each monomial of $M(y) - N(y)$ has the form $G_j(x)y^j$, where $G_j(x)$ is a polynomial in x with $\deg G_j \le [n/2]$. Since each of the $1 + [n/2]$ elements in $\{0,1\} \cup \mathcal{A} \cup \mathcal{B}$ is a zero of G_j, we have $G_j \equiv 0$. This completes the proof that $M(y) \equiv N(y)$. □

Fix an algebraic x over $\mathbb{F}_q$. Since

$$\alpha_c(x) = c + x(1-2c) + 2\sqrt{c-c^2}\sqrt{x-x^2},$$

Theorem 3.1 shows that the splitting field of $f(y)^2 - f(x)^2$ is $\mathbb{F}_q(x, \sqrt{x - x^2})$. In particular, if $x - x^2$ is a square in $\mathbb{F}_q(x)$, then $f(y)^2 - f(x)^2$ splits completely in $\mathbb{F}_q(x)$.

We next consider some consequences of Theorem 3.1 when $x - x^2$ is a nonsquare in $\mathbb{F}_q(x)$. When $q \equiv \pm 3 \bmod 8$, the only value of $y \in \mathbb{F}_q(x)$ for which $f(y) = f(x)$ is $y = x$. When $q \equiv \pm 1 \bmod 8$, the only values of $y \in \mathbb{F}_q(x)$ for which $f(y) = f(x)$ are $y = x$ and $y = 1 - x$. When $q \equiv \pm 1 \bmod 8$, there is no value of $y \in \mathbb{F}_q(x)$ for which $f(y) = -f(x)$. When $q \equiv \pm 3 \bmod 8$, the only value of $y \in \mathbb{F}_q(x)$ for which $f(y) = -f(x)$ is $y = 1 - x$.

Here is an example for $q = 23$. First take $x = 11 + 20I$, where I is a zero of the polynomial $u^2 + 1 \in \mathbb{F}_q[u]$. Then $\mathbb{F}_q(x) = \mathbb{F}_q(I)$ is a field of 529 elements, and $x - x^2$ equals the square $(4 + 5I)^2$. We have

$$f(y) = f(x) \text{ for } y \in \{13 + 3I, 11 + 20I, 10 + 7I, 15 + 19I, 9 + 4I, 14 + 16I\}$$

and

$$f(y) = -f(x) \text{ for } y \in \{8 + 18I, 22 + 15I, 18 + 10I, 16 + 5I, 6 + 13I, 2 + 8I\}.$$

In contrast, take $x = 18 + 9I$, so that $x - x^2 = 5 + 7I$ is a nonsquare in $\mathbb{F}_q(x)$. Then $y = x$ and $y = 1 - x$ are the only values of $y \in \mathbb{F}_q(x)$ for which $f(x)$ equals $f(y)$, while there are no values of $y \in \mathbb{F}_q(x)$ for which $f(x)$ equals $-f(y)$.

Remark 3. *For those x with $f(x) = 0$, the products in Theorem 3.1 can be written in simpler form. Indeed,*

$$f(y) = \prod (y - s)$$

where the product is over the $[n/2]$ values of $s \in \mathbb{F}_q$ for which $\rho(s) = \rho(1-s) = -1$. To see this, note that $\rho(1 - s) = -1$ implies that $(1 - s)^{n-1} = -1$, which in turn implies that when $\rho(s) = -1$,

$$(1 - s)^n = -(1 - s) = -(1 - \sqrt{s})^{q+1}.$$

Dividing by $(1 - \sqrt{s})^n$, we obtain $f(s) = 0$.

For the factorization of $f(y) \bmod p$ with some different values of n in place of (1.1), see [5, Section 4].

For $c, d \in \mathcal{A} \cup \mathcal{B}$, define

$$R(c,d) := \sqrt{c - cd} + \sqrt{d - cd},$$

for an arbitrary fixed choice of signs of the square roots. Note that $R(c,d)$ is in $\mathbb{F}_q$ and $R(c,d)^2 \in \{\alpha_c(d), \alpha_c'(d)\}$. The following corollary to Theorem 3.1 determines the quadratic residuacity of the nonzero values of $1 + R(c,d)$.

Corollary 3.2. *Let $c, d \in \mathcal{A} \cup \mathcal{B}$ with $1 + R(c,d) \neq 0$. Then*

$$\rho(1 + R(c,d)) = \begin{cases} 1, & \text{if } \ c,d \in \mathcal{A} \text{ or } \ c,d \in \mathcal{B}, \\ -1, & \text{otherwise.} \end{cases}$$

Proof. Apply Theorem 3.1 with fixed $x = d$, so that each $R(c,d)^2$ is a zero of the polynomials in (3.1) and (3.2). Since $f(d) = \pm 2$, it follows from Lemma 2.3 that each $R(c,d)^2$ is in $\{0,1\} \cup \mathcal{A} \cup \mathcal{B}$.

First consider the case where $R(c,d)^2 \notin \{0,1\}$. Matching up the zeros in Theorem 3.1 with those in Lemma 2.3, we see that $R(c,d)^2 \in \mathcal{B}$ if either $c, d \in \mathcal{A}$ or $\ c, d \in \mathcal{B}$, and $R(c,d)^2 \in \mathcal{A}$, otherwise. Corollary 3.2 thus follows in this case, since by definition of $\mathcal{A}$ and $\mathcal{B}$, $\rho(1 + \sqrt{u})$ and $\rho(1 - \sqrt{u})$ are both equal to -1 or both equal to 1 according as $u \in \mathcal{A}$ or $u \in \mathcal{B}$.

Next consider the case where $R(c,d) = 0$. In that case, $c = d$, so that Corollary 3.2 again holds. Finally consider the case where $R(c,d)^2 = 1$. Then $d = 1 - c$. Since $1 + R(c,d) \neq 0$, we have $R(c,d) = 1$. Since $d = 1 - c$, it follows from Remark 1 that $\rho(2) = 1$ if and only if $c, d \in \mathcal{A}$ or $\ c, d \in \mathcal{B}$. This completes the proof of the corollary in all cases. □

References

[1] M. Bhargava and M. Zieve, Factoring Dickson polynomials over finite fields, Finite Fields Appl. 5 (1999), 103–111.

[2] X.-d. Hou and T. Ly, Necessary conditions for reversed Dickson polynomials to be permutational, Finite Fields Appl. 16 (2010), 436–448.

[3] N. M. Katz, Rigid local systems on $\mathbb{A}^1$ with finite monodromy, (to appear). `https://web.math.princeton.edu/~nmk/gpconj95.pdf`

[4] J. C. Mason and D. C. Handscomb, Chebyshev polynomials, Chapman & Hall/CRC, Boca Raton, FL, 2003.

[5] M. O. Rayes, V. Trevisan, and P. S. Wang, Factorization properties of Chebyshev polynomials, Computers and Math. with Appl. 50 (2005), 1231–1240.