2005

Factors of Dickson Polynomials over Finite Fields

Robert W. Fitzgerald
Southern Illinois University Carbondale, rfitzg@math.siu.edu

Joseph L. Yucas
Southern Illinois University Carbondale

Published in *Finite Fields and Their Applications*, 11, 724-737.

Factors of Dickson Polynomials over Finite Fields

Robert W. Fitzgerald
and
Joseph L. Yucas

Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, Email: rfitzg@math.siu.edu, jyucas@math.siu.edu

Abstract

We give new descriptions of the factors of Dickson polynomials over finite fields.

KEYWORDS: Dickson polynomials, finite fields, cyclotomic polynomials

1 Introduction

We let $\mathbf{F_q}$ denote the finite field of characteristic p containing q elements. Let n be a positive integer and write $t = \lfloor n/2 \rfloor$. In his 1897 PhD Thesis, Dickson introduced a family of polynomials

$$D_n(x) = \sum_{i=0}^{t} \frac{n}{n-i} \left(\begin{array}{c} n-i \\ i \end{array} \right) x^{n-2i}.$$

These are the unique polynomials satisfying Waring's identity

$$D_n(x + x^{-1}) = x^n + x^{-n}.$$

In recent years these polynomials have received an extensive examination. In fact, a book [8] has been written about them. They have become known as the *Dickson polynomials* (of the first kind).

In [5] and then later simplified in [2] a factorization of the Dickson polynomials over $\mathbf{F_q}$ is given. We summarize their results as follows:

Theorem 1.1. *If q is even, then $D_n(x)$ is the product of irreducible polynomials in $\mathbf{F_q}[\mathbf{x}]$ which occur in cliques corresponding to the divisors d of n, $d > 1$. To each such d there corresponds $\phi(d)/(2k_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1} (x - (\zeta^{q^i} + \zeta^{-q^i}))$$

where ζ is a d^{th} root of unity, ϕ is Euler's totient function and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1$ (mod d).

Theorem 1.2. *If q is odd, then $D_n(x)$ is the product of irreducible polynomials in $\mathbf{F_q}[\mathbf{x}]$ which occur in cliques corresponding to the divisors d of n for which n/d is odd. To each such d there corresponds $\phi(4d)/(2k_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1} (x - (\zeta^{q^i} + \zeta^{-q^i}))$$

where ζ is a $4d^{th}$ root of unity and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1$ (mod 4).

We remark that these results were given in more generality then we use here.

Notice that the factors appearing in the above results are in $\mathbf{F_q[x]}$, although their description uses elements from outside of $\mathbf{F_q}$. The purpose of this paper is to better understand these factors. In this regard, we show that these factors can be obtained from the factors of certain cyclotomic polynomials. This in turn gives a relationship between self-reciprocal polynomials and these Dickson factors. We also obtain a recursion for these factors. In the final section of this paper we record a few identities that we discovered in this pursuit which appear to be new.

2 General results

For a polynomial $f(x)$ over $\mathbf{F_q}$, $f(x)^*$ denotes the reciprocal of $f(x)$, namely, $f(x)^* = x^n f(1/x)$, where $n = \deg f$. We say that $f(x)$ is *self-reciprocal* if $f(x) = f(x)^*$. Let P_n be the collection of all polynomials over $\mathbf{F_q}$ of degree n and let S_n denote the family of all self-reciprocal polynomials over $\mathbf{F_q}$ of degree n.

We define

$$\Phi : P_n \to S_{2n}$$

by

$$f(x) \to x^n f(x + x^{-1}),$$

where $n = \deg f$. This transformation Φ has been studied previously. The first occurrence is Carlitz [3]. Other authors writing about Φ are Miller [10], Andrews [1], Meyn [9], Cohen [6], Scheerhorn [11], Chapman [4] and Kyuregyan [7].

A self-reciprocal polynomial $b(x)$ of degree $2n$ can be written as

$$b(x) = \sum_{i=0}^{n-1} b_i(x^{2n-i} + x^i) + b_n x^n.$$

Define

$$\Psi : S_{2n} \to P_n$$

by

$$b(x) \to \sum_{i=0}^{n-1} b_i D_{n-i}(x) + b_n.$$

Theorem 2.1. *(a)* $\Phi \circ \Psi = id_{S_{2n}}$ *and* $\Psi \circ \Phi = id_{P_n}$.

(b) Φ *and* Ψ *are multiplicative.*

(c) If deg $f_1 = d_1$ *and deg* $f_2 = d_2$ *with* $d_1 > d_2$ *then*

$$\Phi(f_1 + f_2) = \Phi(f_1) + x^{d_1 - d_2}\Phi(f_2).$$

(d) If $b(x)$ *is irreducible of degree* $2n$ *and self-reciprocal then* $\Psi(b(x))$ *is irreducible. If* $a(x)$ *is irreducible of degree* n *and not self-reciprocal then* $\Psi(a(x)a(x)^*)$ *is irreducible.*

Proof: We first check that the codomains are correct. For $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots$, with $a_n \neq 0$, we have $\Phi(f(x)) = x^n[a_n(x + x^{-1})^n + a_{n-1}(x + x^{-1})^{n-1} + \cdots]$ which has degree $2n$. The reciprocal of $\Phi(f(x))$ is

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

Thus $\Phi(P_n) \subset S_{2n}$. And

$$\Psi(b(x)) = b_0 D_n(x) + b_1 D_{n-1}(x) + \cdots$$

has degree n as $b_0 \neq 0$ and $\deg D_j = j$. So $\Psi(S_{2n}) \subset P_n$.

We now prove (a). Write $b(x) = \sum_{i=0}^{n-1} b_i(x^{2n-i} + x^i) + b_n x^n$.

$$\begin{aligned}
\Phi \circ \Psi(b(x)) &= \Phi\left(\sum_{i=0}^{n-1} b_i D_{n-i}(x) + b_n\right) \\
&= x^n \left[\sum_{i=0}^{n-1} b_i D_{n-i}(x + x^{-1}) + b_n\right] \\
&= x^n \left[\sum_{i=0}^{n-1} b_i (x^{n-i} + x^{-(n-i)}) + b_n\right] \\
&= \sum_{i=0}^{n-1} b_i(x^{2n-i} + x^i) + b_n x^n = b(x),
\end{aligned}$$

where we have used Waring's identity in the third line. Thus $\Phi \circ \Psi$ is the identity.

Now in P_n the coefficient of x^n is non-zero and the others are arbitrary so that $|P_n| = (p-1)p^n$. And for $b(x) \in S_{2n}$, $b_0 \neq 0$ and the other coefficients are arbitrary so that $|S_{2n}| = (p-1)p^n$. Hence $\Psi \circ \Phi$ is also the identity.

We now prove (b). Say $\deg f(x) = r$ and $\deg g(x) = s$. Then

$$\Phi((fg)(x)) = x^{r+s}(fg)(x + x^{-1})$$

$$= x^r f(x + x^{-1}) \cdot x^s g(x + x^{-1})$$

$$= \Phi(f(x))\Phi(g(x)).$$

Now suppose $b(x)$ and $c(x)$ are self-reciprocal polynomials. From (a)

$$\Phi(\Psi(b(x)c(x)) = b(x)c(x)$$

$$= (\Phi \circ \Psi)(b(x)) \cdot (\Phi \circ \Psi)(c(x))$$

$$= \Phi[\Psi(b(x))\Psi(c(x))] \quad \text{by the first part.}$$

Consequently,

$$\Psi(b(x)c(x)) = \Psi(b(x))\Psi(c(x))$$

as Φ is injective by (a).

For (c) notice that

$$\Phi((f_1 + f_2)(x)) = x^{d_1}((f_1 + f_2)(x + x^{-1}))$$

$$= x^{d_1} f_1(x + x^{-1}) + x^{d_1 - d_2} x^{d_2} f_2(x + x^{-1})$$

$$= \Phi(f_1(x)) + x^{d_1 - d_2}\Phi(f_2(x)).$$

We now prove (d). Let $b(x) \in S_{2n}$ be irreducible. Suppose $\Psi(b(x)) = f(x)g(x)$, with $\deg f, \deg g \geq 1$. Then using (a) and (b)

$$b(x) = (\Phi \circ \Psi)(b(x)) = \Phi(f(x))\Phi(g(x)),$$

a contradiction. Next suppose $a(x)$ is irreducible and $\Psi(a(x)a(x)^*) = u(x)v(x)$, with $\deg u(x), \deg v(x) \geq 1$. Then, taking Φ, we have $a(x)a(x)^* = \Phi(u(x))\Phi(v(x))$. Since $a(x)$ is irreducible, it divides one of $\Phi(u(x))$ or $\Phi(v(x))$. Say $a(x)$ divides $\Phi(u(x))$. Since $\Phi(u(x))$ is self-reciprocal, $a(x)^*$ also divides $\Phi(u(x))$. Further, since $a(x)^*$ is irreducible and $a(x) \neq a(x)^*$ we see that $a(x)a(x)^*$ divides $\Phi(u(x))$. But then the degree of $\Phi(v(x))$ is less than 1, a contradiction. □

Lemma 2.2. $\Phi(D_n(x)) = x^{2n} + 1$.

Proof;

$$\Phi(D_n(x)) = x^n D_n(x + x^{-1}) = x^n(x^n + x^{-n}) = x^{2n} + 1,$$

where we have again used Waring's identity. □

Lemma 2.3. *Let $g(x)$ be separable and self-reciprocal. Then $g(x)$ factors as*

$$a_1(x)a_1(x)^* a_2(x)a_2(x)^* \cdots a_r(x)a_r(x)^* b_1(x)b_2(x)\cdots b_s(x),$$

for some $r, s \geq 0$. Here each $a_i(x)$ is irreducible and not self-reciprocal, each $b_j(x)$ is irreducible and self-reciprocal and the a_i and b_j are distinct.

Proof: Let $p(x)$ be an irreducible factor of $g(x)$ and let β be a root of $p(x)$. Then $1/\beta$ is also a root of $g(x)$ as $g(x)$ is self-reciprocal. If $1/\beta$ is a root of $p(x)$ then $p(x)$ is self-reciprocal. Otherwise, the minimal polynomial of $1/\beta$, namely $p(x)^*$, also divides $g(x)$, and $p(x) \neq p(x)^*$. The factors are distinct as $g(x)$ has no multiple roots. □

Let $Q_d(x)$ be the dth cyclotomic polynomial, namely the product of $(x-\gamma)$ over all primitive dth roots of unity γ.

Lemma 2.4. *If $(p, n) = 1$ then*

$$x^n + 1 = \prod_{d|n} Q_{2d}(x).$$

Proof:

$$\begin{aligned}(x^n - 1)(x^n + 1) = x^{2n} - 1 &= \prod_{d|2n} Q_d(x) \\ &= (\prod_{d|n} Q_d(x))(\prod_{d|n} Q_{2d}(x)) \\ &= (x^n - 1)(\prod_{d|n} Q_{2d}(x)).\end{aligned}$$

Consequently,

$$x^n + 1 = \prod_{d|n} Q_{2d}(x).$$

□

3 Characteristic 2

Here we assume $p = 2$. Since $D_{2m}(x) = D_m(x)^2$ we need only factor $D_n(x)$ for odd n. Consequently, we assume that n is odd throughout this entire section.

Lemma 3.1. *Let $n = 2m + 1$.*
(a) $D_n(x) = xF_n(x)^2$, for some polynomial $F_n(x)$ of degree m.
(b) $(x + 1)\Phi(F_n(x)) = x^n + 1$.

Proof: For (a), let

$$F_n(x) = \sum_{i=0}^{t} \frac{n}{n-i} \left(\begin{array}{c} n-i \\ i \end{array} \right) x^{m-i}.$$

For (b), we use Lemma 2.2 and Theorem 2.1(b).

$$x^{2n} + 1 = \Phi(D_n(x)) = \Phi(x)\Phi(F_n(x))^2 = (x^2 + 1)\Phi(F_n(x))^2.$$

So $(x^n + 1)^2 = [(x + 1)\Phi(F_n(x))]^2$, giving (b). □

Proposition 3.2. *x^n+1 is separable and self-reciprocal. Factor as in Lemma 2.3*

$$x^n + 1 = a_1(x)a_1(x)^* \cdots a_r(x)a_r(x)^* b_1(x) \cdots b_s(x).$$

Then

$$F_n(x) = \Psi(a_1(x)a_1(x)^*) \cdots \Psi(a_r(x)a_r(x)^*)\Psi(b_1(x)) \cdots \Psi(b_s(x)),$$

is the factorization of $F_n(x)$ into irreducible polynomials over $\mathbf{F_q}$.

Proof: The first statement is clear. By Lemma 2.2, $\Phi(D_n(x)) = x^{2n} + 1$. Applying Ψ using Theorem 2.1(b) we see that each $\Psi(aa^*)$ and $\Psi(b)$ is irreducible by Theorem 2.1(d). □

We now give a recursive description of the factors of $F_n(x)$ in Proposition 3.2. Recall that if $m|n$ then $D_m(x)|D_n(x)$ (since $p = 2$) and so $F_m(x)|F_n(x)$. Set

$$G_n(x) = \text{lcm}\{F_m(x) : m|n \quad \text{and} \quad m < n\}$$

and set

$$H_n(x) = F_n(x)/G_n(x).$$

Thus $H_n(x)$ consists of the factors of $F_n(x)$ which have not occurred as factors of $F_m(x)$, $m < n$.

Let $Q_d(x)$ be the dth cyclotomic polynomial over $\mathbf{F_q}$, namely the product of $(x - \gamma)$ over all primitive dth roots of unity γ.

Lemma 3.3. *$H_n(x) = \Psi(Q_n(x))$.*

Proof: Suppose $d|n$ and $d < n$. Then

$$x^d + 1 = \prod_{e|d} Q_e(x)$$

$$F_d(x) = \prod_{e|d} \Psi(Q_d(x)).$$

Thus

$$G_n(x) = \mathrm{lcm}\{F_d(x) : d|n, d < n\} = \prod_{d|n, d<n} \Psi(Q_d(x)).$$

Now

$$x^n + 1 = \prod_{d|n} Q_d(x)$$

$$F_n(x) = \prod_{d|n, d<n} \Psi(Q_d(x)) \cdot \Psi(Q_n(x)).$$

So $H_n(x) = F_n(x)/G_n(x) = \Psi(Q_n(x))$. $\square$

Let $\langle q \rangle_n$ denote the subgroup generated by q in $\mathbb{Z}_n^*$, the group of units of $\mathbb{Z}_n$. We always consider two cases:

(i) $-1 \in \langle q \rangle_n$. Here we let v be the least positive integer such that $n|q^v+1$.

(ii) $-1 \notin \langle q \rangle_n$. Here we let w be the least positive integer such that $n|q^w - 1$.

Lemma 3.4. *(a) Suppose that $-1 \in \langle q \rangle_n$. Then $Q_n(x)$ is the product of all self-reciprocal polynomials of degree $2v$ and order n.*

(b) Suppose that $-1 \notin \langle q \rangle_n$. Then $Q_n(x)$ is the product of all irreducible, not self-reciprocal, polynomials of degree w and order n.

Proof: (a) In the notation of [12], we have $n \in D_v$. The result is then [12], Theorem 11.

(b) By the definition of w, all primitive nth roots of unity lie in $GF(2^w)$ and no smaller field. Hence if $p(x)$ is an irreducible factor of $Q_n(x)$ then $\deg p(x) = w$. Clearly $p(x)$ has order n as its roots are primitive nth roots of unity. And $p(x)$ is not self-reciprocal by [12], Theorem 8. Conversely, if $p(x)$ has order n then $p(x)$ divides $Q_n(x)$. □

Theorem 3.5. *(a) Suppose $-1 \in \langle q \rangle_n$. The irreducible factors of $H_n(x)$ are the $\Psi(b(x))$, over all irreducible, self-reciprocal polynomials of degree $2v$ and order n.*

(b) Suppose $-1 \notin \langle q \rangle_n$. The irreducible factors of $H_n(x)$ are the $\Psi(a(x)a(x)^*)$ where $\cup\{a(x), a(x)^*\}$ is all irreducible, not self-reciprocal, polynomials of degree w and order n.

Proof: (a) follows from Lemma 3.3 and Lemma 3.4. For (b), note that if γ is a primitive nth root of unity then so is $1/\gamma$. Hence if $a(x)$ divides $Q_n(x)$ so does $a(x)^*$. Pair the factors of $Q_n(x)$ as $a(x)a(x)^*$ before applying Ψ. □

Example: Consider the cyclotomic polynomials

$$Q_3(x) = x^2 + x + 1$$

$$Q_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

and

$$Q_{21}(x) = x^{12} + +x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$$

over $\mathbf{F_2}$.

$$F_{21}(x) = \Psi(Q_3(x))\Psi(Q_7(x))\Psi(Q_{21}(x))$$

$$= (D_1(x)+1)(D_3(x)+D_2(x)+D_1(x)+1)(D_6(x)+D_5(x)+D_3(x)+D_2(x)+1)$$

$$= (x + 1)(x^3 + x^2 + 1)(x^6 + x^5 + 1).$$

Hence

$$D_{21}(x) = xF(x)^2 =$$

$$= x(x + 1)^2(x^3 + x^2 + 1)^2(x^6 + x^5 + 1)^2.$$

Chou [5] showed that any irreducible $f(x)$ over $GF(q)$ divides some $D_n(x)$. The next result describes precisely when this happens.

Proposition 3.6. *Suppose $f(x)$ is an irreducible polynomial of degree $d \geq 2$. Then $f(x)$ divides $D_n(x)$ if and only if ord $\Phi(f(x))$ divides n.*

Proof: We have $f(x)|D_n(x)$ iff $f(x)|F_n(x)$ iff $\Phi(f(x))$ divides $\Phi(F_n(x))$ iff $\Phi(f(x))$ divides $(x+1)\Phi(F_n(x)) = x^n + 1$ iff $\mathrm{ord}\Phi(f(x))$ divides n. $\square$

We now give a second description (in the case $q = 2$) of the factors of $H_n(x)$, from the point of view of their image under Φ rather than their pre-image under Ψ.

Let $p(x)$ be an irreducible polynomial over $\mathbf{F_2}$. The *inverse trace* of $p(x)$ is the coefficient of x in $p(x)$. Equivalently, if α is a root of $p(x)$ and $K = \mathbf{F_2}(\alpha)$ then the inverse trace of $p(x)$ is $\mathrm{tr}_{K/\mathbf{F_2}}(1/\alpha)$.

We first record a result of Meyn, [9].

Lemma 3.7. *Let $f(x)$ be irreducible of degree n over $\mathbf{F_2}$.*

(a) If the inverse trace of $f(x)$ is 1 then $\Phi(f(x))$ is irreducible.

(b) If the inverse trace of $f(x)$ is 0 then $\Phi(f(x))$ factors as $u(x)u(x)^*$, for some irreducible, not self-reciprocal, polynomial $u(x)$ of degree n.

Proposition 3.8. *Suppose $q = 2$.*

(a) If $-1 \in \langle 2 \rangle_n$ then the irreducible factors of $H_n(x)$ are the irreducible polynomials $f(x)$ of degree v and inverse trace 1 such that $\Phi(f(x))$ has order n.

(b) If $-1 \notin \langle 2 \rangle_n$ then the irreducible factors of $H_n(x)$ are the irreducible polynomials $f(x)$ of degree w and inverse trace 0 such that $\Phi(f(x))$ has order n.

Proof: (a) The irreducible factors of $H_n(x)$ are the $f(x) = \Psi(b(x))$ for irreducible, self-reciprocal polynomials $b(x)$ of degree $2v$ and order n. So $f(x)$ is irreducible, degree v, with inverse trace 1 by Lemma 3.7, and $\Phi(f(x)) = b(x)$ has order n. The proof of (b) is similar. $\square$

Set
$$m(f) = \min\{n : f(x)|D_n(x)\}.$$

Corollary 3.9. *Let $f(x)$ be irreducible of degree $d \geq 2$ over $\mathbf{F_2}$.*

(a) $m(f)$ divides exactly one of $2^d + 1$ or $2^d - 1$.

(b) $m(f)$ divides $2^d + 1$ iff the inverse trace of $f(x)$ is 1.

Proof: Let $n = \mathrm{ord}\Phi(f(x)) = m(f)$ by Proposition 3.6. Then $\Phi(f(x))$ divides $Q_n(x)$ and so $f(x)$ divides $\Psi(Q_n(x)) = H_n(x)$ by Lemma 3.3. Thus by Proposition 3.8 either $-1 \in \langle 2 \rangle_n$, $n|2^d + 1$ and the inverse trace of $f(x)$ is 1 or $-1 \notin \langle 2 \rangle_n$, $n|2^d - 1$ and the inverse trace of $f(x)$ is 0. $\square$

4 Odd characteristic

Here we assume that p is odd. Since $D_{pm}(x) = D_m(x)^p$ we need only factor $D_n(x)$ with $(p, n) = 1$. Thus, we assume $(p, n) = 1$ throughout this section. The results here are similar to the results when $p = 2$ except that we work with Q_{4n} instead of Q_n. The proofs are also similar and thus we will be brief.

Proposition 4.1. *$x^{2n} + 1$ is separable and self-reciprocal. Factor $x^{2n} + 1$ as in Lemma 2.3,*

$$x^{2n} + 1 = a_1(x)a_1(x)^* \cdots a_r(x)a_r(x)^* b_1(x) \cdots b_s(x).$$

Then

$$D_n(x) = \Psi(a_1(x)a_1(x)^*) \cdots \Psi(a_r(x)a_r(x)^*)\Psi(b_1(x)) \cdots \Psi(b_s(x)),$$

is the factorization of $D_n(x)$ into irreducible polynomials over $\mathbf{F_q}$.

Proof: Same as the proof of Proposition 3.2. □

Recall that if $m|n$ and n/m is odd then $D_m(x)|D_n(x)$. Set

$$G_n(x) = \mathrm{lcm}\{D_m(x) : m|n, n/m \quad \text{odd and} \quad m < n\}$$

and set

$$H_n(x) = D_n(x)/G_n(x).$$

Thus $H_n(x)$ consists of the factors of $D_n(x)$ which have not occurred as factors of $D_m(x)$, $m < n$.

Lemma 4.2. *$H_n(x) = \Psi(Q_{4n}(x))$.*

Proof: By By Lemma 2.4,

$$x^{2n} + 1 = \prod_{d|2n} Q_{4d}(x).$$

Now proceed as in Lemma 3.3. □

Again we consider two cases:

(i) $-1 \in \langle q \rangle_{4n}$. Here we let v be the least positive integer such that $4n|q^v + 1$.

(ii) $-1 \notin \langle q \rangle_{4n}$. Here we let w be the least positive integer such that $4n|q^w - 1$.

Lemma 4.3. *(a) Suppose that* $-1 \in \langle q \rangle_{4n}$*. Then* $Q_{4n}(x)$ *is the product of all monic self-reciprocal polynomials of degree* $2v$ *and order* $4n$*.*

(b) Suppose that $-1 \notin \langle q \rangle_{4n}$*. Then* $Q_{4n}(x)$ *is the product of all monic irreducible, not self-reciprocal, polynomials of degree* w *and order* $4n$*.*

Proof: Same as Lemma 3.4. □

Theorem 4.4. *(a) Suppose* $-1 \in \langle q \rangle_{4n}$*. The irreducible factors of* $H_n(x)$ *are the* $\Psi(b(x))$*, over all monic irreducible, self-reciprocal polynomials of degree* $2v$ *and order* $4n$*.*

(b) Suppose $-1 \notin \langle q \rangle_{4n}$*. The irreducible factors of* $H_n(x)$ *are the* $\Psi(a(x)a(x)^*)$ *where* $\cup\{a(x), a(x)^*\}$ *is all monic irreducible, not self-reciprocal, polynomials of degree* w *and order* $4n$*.*

Proof: Same as Theorem 3.5. □

Proposition 4.5. *Suppose* $f(x)$ *is a monic irreducible polynomial of degree* $d \geq 2$*. Then* $f(x)$ *divides* $D_n(x)$ *if and only if 4 divides ord* $\Phi(f(x))$*, ord* $\Phi(f(x))$ *divides* $4n$ *and* $\frac{4n}{ord\ \Phi(f(x))}$ *is odd.*

Proof: Same as Proposition 3.6. □

5 Some new identities

We can easily derive an identity over $\mathbb{Z}$. For odd p recall that $D_m(x)$ divides $D_n(x)$ if $m|n$ and n/m is odd. We can find the quotient in one case.

Corollary 5.1. *Write* $n = 2^s m$ *with* $m = 2k+1$ *odd. Then*

$$D_n(x) = D_{2^s}(x)\left(\sum_{i=0}^{k-1}(-1)^i D_{n-(2i+1)2^s}(x) + (-1)^k\right),$$

holds over $\mathbb{Z}$*.*

Proof: We first work over $F = GF(p)$. The second factor on the right is

$$\Psi\left(\sum_{i=0}^{k-1}(-1)^i(x^{2n-2^{s+1}-i2^{s+1}} + x^{i2^{s+1}}) + (-1)^k x^{k2^{s+1}}\right).$$

Note that $2n - 2^{s+1} - i2^{s+1} = 2^{s+1}(m-1-i)$. Let $j = i+1$. Then the second factor on the right is thus

$$\Psi\left(\sum_{j=1}^{m}(-1)^{j+1}x^{2^{s+1}(m-j)}\right).$$

Apply Φ to the right side of the equation to get

$$\Phi(RHS) = (x^{2^{s+1}}+1)\left(\sum_{j=1}^{m}(-1)^{j+1}x^{2^{s+1}(m-j)}\right) = x^{2^{s+1}m}+1 = x^{2n+1}+1 = \Phi(D_n(x)),$$

where we have used Lemma 2.2 twice in calculating $\Phi(D_{2^s}(x))$ and $\Phi(D_n(x))$. As Φ is injective, the identity is valid over $GF(p)$. As p is arbitrary, the identity is valid over $\mathbb{Z}$. $\square$

Proposition 5.2. *Let $q = 2$ and $n = 2m+1$.*
(a)$F_n(x) = \sum_{i=1}^{m} D_i(x) + 1$.
(b) $F_n(x) = F_{n-2}(x) + D_m(x)$.
(c) $D_n(x) = D_{n-2}(x) + xD_m(x)^2$.

Proof: We have

$$\begin{aligned} F_n(x) &= (\Psi \circ \Phi)(F_n(x)) \\ &= \Psi((x^n+1)/(x+1)) \\ &= \Psi(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \\ &= \left[\sum_{i=0}^{m-1} D_{m-i}(x) + 1\right] \\ F_n(x) &= \sum_{j=1}^{m} D_j(x) + 1. \end{aligned}$$

This is (a). (b) follows immediately from (a). For (c)

$$D_n(x) = xF_n(x)^2 = x(F_{n-2}(x)+D_m(x))^2 = xF_{n-2}(x)^2+D_m(x)^2 = D_{n-2}(x)+D_m(x)^2,$$

(since we are working over $\mathbf{F_2}$). $\square$

Proposition 5.3. *Let $q = 2$ and write $n = 2^k + s$ with $s < 2^k$.*

$$F_n(x) = x^{2^{k-2}} F_{2^{k-1}+s}(x) + F_s(x) = x^{2^{k-1}} F_s(x) + F_{2^k-s}(x).$$

Proof: Using Theorem 2.1(b)(c) and Lemma 3.1(b) we have

$$\begin{aligned}
\Phi(x^{2^{k-2}} F_{2^{k-1}+s}(x) + F_s(x)) &= \Phi(x^{2^{k-2}})\Phi(F_{2^{k-1}+s}(x)) + x^{2^{k-1}}\Phi(F_s(x)) \\
&= (x^{2^{k-1}} + 1)(\frac{x^{2^{k-1}+s} + 1}{x+1}) + (x^{k-1})(\frac{x^s + 1}{x+1}) \\
&= \frac{x^{2^k+s} + 1}{x+1} = \Phi(F_{2^k+s}(x)).
\end{aligned}$$

Similarly,

$$\begin{aligned}
\Phi(x^{2^{k-1}} F_s(x) + F_{2^k-s}(x)) &= \Phi(x^{2^{k-1}})\Phi(F_s(x)) + x^{2^s}\Phi(F_{2^k-s}(x)) \\
&= (x^{2^k} + 1)(\frac{x^s + 1}{x+1}) + (x^s)(\frac{x^{2^k-s} + 1}{x+1}) \\
&= \frac{x^{2^k+s} + 1}{x+1} = \Phi(F_{2^k+s}(x)).
\end{aligned}$$

The result now follows since Φ is injective. $\square$

References

[1] G. Andrews, Reciprocal polynomials and quadratic transformations, Utilitas Math.38 (1985), 255-264.

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

[3] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967), 212-220.

[4] R. Chapman, Completely normal elements in iterated quadratic extensions of finite fields, Finite Fields Appl. 3 (1997), 1-10.

[5] W.S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. 3 (1997), 84-96.

[6] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, Des. Codes Cryptogr. 2 (1992), 169-174.

[7] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $GF(2^s)$, Finite Fields Appl. 8 (2002), 52-68.

[8] R. Lidl, G. Mullen, G. Turnwell, Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London/Harlow/Essex, 1993.

[9] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput.1 (1990) 43-53.

[10] R. L. Miller, Necklaces, symmetries and self-rreciprocal polynomials, Discrete Math. 22 (1978), 25-33.

[11] A. Scheerhorn, Iterated constructions of normal bases over finite fields, Finite Fields: Theory, Applications and Algorithms (Las Vegas, NV, 1993), 309-325, Contemp. Math. 168, Amer. Math. Soc., Providence, RI (1994).

[12] J. Yucas and G. Mullen, Self-reciprocal polynomials over finite fields, to appear in Designs, Codes and Cryptography.