2007

Generalized Reciprocals, Factors of Dickson Polynomials and Generalized Cyclotomic 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*, 13, 492-515. doi: 10.1016/j.ffa.2006.03.002

Generalized Reciprocals, Factors of Dickson Polynomials and Generalized Cyclotomic Polynomials over Finite Fields

Robert W. Fitzgerald
and
Joseph L. Yucas

Abstract

We give new descriptions of the factors of Dickson polynomials over finite fields in terms of cyclotomic factors. To do this generalized reciprocal polynomials are introduced and characterized. We also study the factorization of generalized cyclotomic polynomials and their relationship to the factorization of Dickson polynomials.

1 Introduction

Throughout, $q = p^e$ will denote an odd prime power and $\mathbf{F_q}$ will denote the finite field containing q elements. Let n be a positive integer, set $s = \lfloor n/2 \rfloor$ and let a be a non-zero element of $\mathbf{F_q}$. In his 1897 PhD Thesis, Dickson introduced a family of polynomials

$$D_{n,a}(x) = \sum_{i=0}^{s} \frac{n}{n-i} \left(\begin{array}{c} n-i \\ i \end{array} \right) (-a)^i x^{n-2i}.$$

These are the unique polynomials satisfying Waring's identity

$$D_{n,a}(x + \frac{a}{x}) = x^n + (\frac{a}{x})^n.$$

In recent years these polynomials have received an extensive examination. In fact, a book [9] 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 these Dickson polynomials over $\mathbf{F_q}$ is given. We summarize their results as follows:

Theorem 1.1. *$D_{n,a}(x)$ 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 $\phi(4d)/(2N_d)$ irreducible factors, each of which has the form*

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

where ζ is a primitive $4d^{th}$ root of unity, ϕ is Euler's totient function, k_d is the least positive integer such that $q^{k_d}\equiv\pm1$ (mod 4d) and

$$N_d=\begin{cases} k_d/2 & \text{if } \sqrt{a}\notin\mathbf{F_q},\ k_d\equiv 2 \text{ (mod 4) and } q^{k_d/2}\equiv 2d\pm1 \text{ (mod 4d)};\\ 2k_d & \text{if } \sqrt{a}\notin\mathbf{F_q} \text{ and } k_d \text{ is odd};\\ k_d & \text{otherwise.}\end{cases}$$

Notice that the factors appearing in the above result are in $\mathbf{F_q}[\mathbf{x}]$, 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 generalizes the results of [7] where the case $a=1$ was considered. To do this we need the notion of generalized reciprocals. This is introduced in section 2. Here we characterize polynomials which equal their generalized reciprocals in terms of their orders. This generalizes Theorem 11 of [14]. Section 3 is a rather straight-forward generalization of results from [7] and section 4 provides the factorization of the Dickson polynomials. In section 5 we introduce cyclotomic factors and provide an algorithm for factoring Dickson polynomials. Section 6 provides some computational aids and in section 7 we introduce generalized cyclotomic polynomials and study their factorization and their relationship to Dickson factors. Section 8 provides a long and tedious proof of our result on the order of generalized cyclotomic polynomials.

2 Generalized reciprocals of polynomials

Recall that q is an odd prime power and $0\neq a\in\mathbf{F_q}$. For $f(x)\in\mathbf{F_q}[\mathrm{x}]$ monic of degree n, with $f(0)\neq0$, define the *a-reciprocal* of $f(x)$ by

$$\hat{f}_a(x) = \frac{x^n}{f(0)} f(a/x).$$

That is, if

$$f(x) = \sum_{i=0}^{n} b_i x^i$$

then

$$\hat{f}_a(x) = \frac{1}{b_0} \sum_{i=0}^{n} b_i a^i x^{n-i}.$$

Notice that $\hat{f}_a(x)$ is monic and if α is a root of $f(x)$ then a/α is a root of $\hat{f}_a(x)$. Also notice that $\hat{f}_a(0) = a^n/f(0)$ thus the a-reciprocal of $\hat{f}_a(x)$ is $f(x)$. Consequently, $\hat{f}_a(x)$ is irreducible over $\mathbf{F_q}$ if and only if $f(x)$ is. However, $\hat{f}_a(x)$ may not have the same order as $f(x)$. For example, consider $f(x) = x^3 + 3$ over $\mathbf{F_7}$. $f(x)$ has order 9 while $\hat{f}_3(x) = x^3 + 2$ has order 18.

A monic polynomial $f(x)$ of degree $n = 2m$ is said to be *a-self reciprocal* if $\hat{f}_a(x) = f(x)$. Notice that $f(x) = \sum_{i=0}^{n} b_i x^i$ is a-self reciprocal if and only if $b_{n-i} b_0 = b_i a^i$. When $i = n$ we see that $f(0)^2 = a^n$ so there are two types of a-self reciprocal polynomials:

1. ($f(0) = -a^m$). Here, $f(\sqrt{a}) = -f(\sqrt{a})$ hence $f(\sqrt{a}) = 0$ and $f(x)$ is a multiple of $x^2 - a$. We will refer to a-self reciprocal polynomials of this type as being *trivial* .

2. ($f(0) = a^m$). Here $b_{n-i} a^m = b^i a^i$ hence $b_i = b_{n-i} a^{m-i}$ and $f(x)$ has the form

$$f(x) = b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i} x^i)$$

for some $b_j \in \mathbf{F_q}$ and $b_{2m} = 1$. We will refer to a-self reciprocal polynomials of this type as being *non-trivial* . As an example, it is easy to check that $f(x)\hat{f}_a(x)$ is a non-trivial a-self reciprocal polynomial for every monic polynomial $f(x)$.

Notice that the only irreducible trivial a-self reciprocal polynomial is $x^2 - a$ when a is not a square in $\mathbf{F_q}$. The following Theorem gives a characterization of non-trivial a-self reciprocal polynomials.

Theorem 2.1. *Suppose $a \in \mathbf{F_q}$ with $a \neq 0$. For a monic irreducible polynomial $f(x)$ over $\mathbf{F_q}$ of degree $n = 2m$, the following statements are equivalent.*

1. $f(x)$ is a non-trivial a-self reciprocal polynomial.

2. $f(x)$ has a root $\alpha \in \mathbf{F_{q^n}}$ with $a/\alpha \neq \alpha$ also being a root of $f(x)$.
3. $\alpha^{q^m} = a/\alpha$ for every root α of $f(x)$.

Proof: 1⇒2. By 1.,

$$f(x) = \frac{x^n}{f(0)} f(\frac{a}{x}).$$

Hence, if α is a root of $f(x)$ then so is a/α. If $\alpha = a/\alpha$ then $\alpha^2 - a = 0$ which implies that $f(x) = x^2 - a$, a contradiction.

2⇒3. By 2., f has a root α with $\alpha^{q^j} = a/\alpha$ for some j with $1 \leq j \leq n-1$. Hence

$$\alpha^{q^{2j}} = (\alpha^{q^j})^{q^j} = a/\alpha^{q^j} = a/(a/\alpha) = \alpha.$$

Consequently, n divides $2j$. But $1 \leq j \leq n-1$ and $n > 1$, so $n = 2j$ and $m = j$. If β is any other root of $f(x)$ then $\beta = \alpha^{q^i}$ for some i. We have

$$\beta^{q^m} = (\alpha^{q^i})^{q^m} = (\alpha^{q^m})^{q^i} = (\frac{a}{\alpha})^{q^i} = \frac{a}{\beta}.$$

3⇒1. By 3., $f(x)$ and $g(x) = (x^n/f(0))f(\frac{a}{x})$ are monic polynomials having the same roots and same degree hence they are equal. If $f(x) = x^2 - a$ then by 3., $\sqrt{a}^{q+1} = a$ hence $a^{\frac{q+1}{2}} = a$ and $a^{\frac{q-1}{2}} = 1$ implying $\sqrt{a} \in \mathbf{F_q}$ and contradicting the irreducibility of $f(x)$. □

Define

$$D_n = \{r : r \text{ divides } q^n - 1 \text{ but } r \text{ does not divide } q^s - 1 \text{ for } s < n\}.$$

For $r \in D_n$, write $r = d_r t_r$ where $d_r = (r, q^m + 1)$. We next characterize a-self reciprocal polynomials in terms of their orders.

Theorem 2.2. *Suppose $f(x)$ is an irreducible polynomial of degree n over $\mathbf{F_q}$ and let t be a divisor of $q-1$. The following statements are equivalent:*
1. $f(x)$ is a-self reciprocal for some $a \in \mathbf{F_q^*}$ with $ord(a) = t$.
2. $f(x)$ has order $r \in D_n$ with $t_r = t$.

Proof: 1 ⇒ 2. Let β be a root of $f(x)$. Since $f(x)$ is a-self reciprocal, $\beta^{q^m+1} = a$ and hence $\beta^{(q^m+1)t} = 1$. Let $r = ord(f)$. Then $r \in D_n$ since $f(x)$ is an irreducible polynomial of degree n. Write $r = d_r t_r$ where $d_r = (r, q^m+1)$ and write $q^m + 1 = d_r d$. Then $(t_r, d) = 1$. Since $\beta^{(q^m+1)t} = 1$, we see that $d_r t_r$ divides $d_r d t$ and thus t_r divides t. On the other hand,

$$a^{t_r} = \beta^{(q^m+1)t_r} = \beta^{d_r d t_r} = \beta^{rd} = 1.$$

Consequently, t divides t_r and hence $t_r = t$.

$2 \Rightarrow 1$. Let β be a root of $f(x)$ and write $r = d_r t_r$ where $d_r = (r, q^m + 1)$. Then $\beta^{d_r t_r} = 1$. Let $a = \beta^{q^m+1}$. Since d_r divides $q^m + 1$ and $t_r = t$ divides $q - 1$ we see that $a^{q-1} = 1$ thus $a \in \mathbf{F}_\mathbf{q}^*$ and $f(x)$ is a-self reciprocal. Also notice that $a^{t_r} = 1$. Again write $r = d_r t_r$ where $d_r = (r, q^m + 1)$ and write $q^m + 1 = d_r d$. Suppose $a^s = 1$. Then

$$1 = \beta^{(q^m+1)s} = \beta^{d_r ds}.$$

Since β has order r, we see that $d_r t_r$ divides $d_r ds$. Finally, $(d, t_r) = 1$ implies that t_r divides s. □

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

Corollary 2.3. *Let $r \in D_n$ and suppose t_r divides $q-1$. Then $Q_r(x)$ factors into all a-self reciprocal monic irreducible polynomials of degree n and order r where a ranges over all elements of F_q of order t_r.*

Proof: By Theorem 2.47 of [10], the irreducible factors of Q_r are all the irreducible polynomials of degree n and order r. The result now follows from the previous Theorem. □

Our next goal is to give a description of the a appearing in Theorem 2.1.

Lemma 2.4. *Suppose $\beta \in \mathbf{F}_{\mathbf{q}^\mathbf{n}}$ and $c = \beta^{q^m+1} \in \mathbf{F}_\mathbf{q}$. Then*

$$\beta^{q^j} = \frac{c}{\beta^{q^{m+j}}}.$$

Proof: $(\beta^{q^m+1})^{q-1} = 1$ hence $\beta^{q^{m+1}-q^m+q-1} = 1$. Then

$$\beta^q = \frac{\beta^{q^m+1}}{\beta^{q^{m+1}}} = \frac{c}{\beta^{q^{m+1}}}$$

and

$$\beta^{q^j} = (\beta^q)^{q^{j-1}} = \frac{c}{\beta^{q^{m+j}}}.$$

□

Lemma 2.5. *Suppose $\beta \in \mathbf{F}_{\mathbf{q}^\mathbf{n}}$ and $c = \beta^{q^m+1} \in \mathbf{F}_\mathbf{q}$. If $tr(\beta^{-1}) \neq 0$ then*

$$c = \frac{tr(\beta)}{tr(\beta^{-1})}.$$

Proof:

$$tr(\beta^{-1}) = \sum_{j=0}^{n-1} \frac{1}{\beta^{q^j}} = \frac{1}{\beta^{\frac{q^n-1}{q-1}}} \sum_{j=0}^{n-1} \beta^{\frac{q^n-1}{q-1}-q^j} = \frac{\beta^{\frac{q^n-1}{q-1}-q^{n-1}}}{\beta^{\frac{q^n-1}{q-1}}} \sum_{j=0}^{n-1} \beta^{q^{n-1}-q^j}.$$

Hence

$$\frac{tr(\beta)}{tr(\beta^{-1})} = \frac{\beta^{\frac{q^n-1}{q-1}} tr(\beta)}{\beta^{\frac{q^n-1}{q-1}-q^{n-1}} \sum_{j=0}^{n-1} \beta^{q^{n-1}-q^j}} = c(\frac{\beta^{q^{n-1}-q^m-1} tr(\beta)}{\sum_{j=0}^{n-1} \beta^{q^{n-1}-q^j}}).$$

Thus it suffices to show

$$tr(\beta) = \frac{\sum_{j=0}^{n-1} \beta^{q^{n-1}-q^j}}{\beta^{q^{n-1}-q^m-1}},$$

that is we show

$$tr(\beta) = \sum_{j=0}^{n-1} \beta^{q^m-q^j+1}.$$

$\beta^{q^m-q^j+1} = c/\beta^{q^j} = \beta^{q^{m+j}}$ by Lemma 2.4 thus

$$\sum_{j=0}^{n-1} \beta^{q^m-q^j+1} = \sum_{j=0}^{n-1} \beta^{q^{m+j}} = \sum_{j=0}^{n-1} \beta^{q^j} = tr(\beta).$$

□

For an irreducible polynomial $f(x)$ over $\mathbf{F_q}$, the *inverse trace* of $f(x)$ is the coefficient of x in $f(x)$ divided by the constant term of $f(x)$. Equivalently, if β is a root of $f(x)$ and $K = \mathbf{F_q}(\beta)$ then the inverse trace of $f(x)$ is $\mathrm{tr}_{K/\mathbf{F_q}}(1/\beta)$. For $f \in \mathbf{F_q}[\mathbf{x}]$, let $itr(f)$ denote the inverse trace of f.

Theorem 2.6. *Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of degree $n = 2m$. If $ord(f)|(q^m+1)(q-1)$ and $tr(f) = a \cdot itr(f) \neq 0$ then $f(x)$ is a-self reciprocal.*

Proof: Let $\beta \in \mathbf{F_{q^n}}$ be a root of $f(x)$. We show that $\beta^{q^m+1} = a$. Since $ord(f)|(q^m+1)(q-1)$, we see that $(\beta^{q^m+1})^{q-1} = 1$ hence $\beta^{q^m+1} \in F_q$. Let $c = \beta^{q^m+1}$. By Lemma 2.5,

$$c = \frac{tr(\beta)}{tr(\beta^{-1})} = \frac{tr(f)}{itr(f)} = a.$$

□

3 The mappings Φ_a and Ψ_a

Let P_m be the collection of all monic polynomials over $\mathbf{F_q}$ of degree m and let $S_{m,a}$ denote the family of all monic non-trivial a-self reciprocal polynomials over $\mathbf{F_q}$ of degree m.

We define

$$\Phi_a : P_m \to S_{2m,a}$$

by

$$f(x) \to x^m f(x + \frac{a}{x}).$$

This transformation Φ_a has been studied extensively when $a = 1$. The first occurrence is Carlitz [3]. Other authors writing about Φ_1 are Miller [12], Andrews [1], Meyn [11], Cohen [6], Scheerhorn [13], Chapman [4] and Kyuregyan [8].

Recall that a non-trivial monic a-self reciprocal polynomial $b(x)$ of degree $2m$ can be written as

$$f(x) = b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i)$$

for some $b_j \in \mathbf{F_q}$ and $b_{2m} = 1$. Define

$$\Psi_a : S_{2m,a} \to P_m$$

by

$$b(x) \to b_m + \sum_{i=0}^{m-1} b_{2m-i} D_{m-i,a}(x).$$

The following theorem is nearly a straight-forward generalization of [7]. We include a proof here for completeness.

Theorem 3.1. *(a) $\Phi_a \circ \Psi_a = id_{S_{2m,a}}$ and $\Psi_a \circ \Phi_a = id_{P_m}$.*

(b) Φ_a and Ψ_a are multiplicative.

(c) If $b(x)$ is a monic irreducible non-trivial a-self reciprocal polynomial of degree $2m$ then $\Psi_a(b(x))$ is irreducible. If $f(x)$ is an irreducible polynomial of degree m and not a-self reciprocal then $\Psi_a(f(x)\hat{f}_a(x))$ is irreducible.

Proof: We first check that the codomains are correct. For $f(x) = x^m + a_{m-1}x^{m-1} + \cdots$, we have $\Phi_a(f(x)) = x^m[(x + \frac{a}{x})^m + a_{m-1}(x + \frac{a}{x})^{m-1} + \cdots]$

which is monic of degree $2m$. Since the constant term of $\Phi_a(f(x))$ is a^m we see that the a-reciprocal of $\Phi_a(f(x))$ is

$$\frac{x^{2m}}{a^m}\frac{a^m}{x^m}f(\frac{a}{x}+x) = x^m f(x+\frac{a}{x}) = \Phi_a(f(x)).$$

Thus $\Phi_a(P_m) \subset S_{2m,a}$. And

$$\Psi_a(b(x)) = b_{2m}D_{m,a}(x) + b_{2m-1}D_{m-1,a}(x) + \cdots$$

is monic of degree m since $b_{2m} = 1$ and $D_{j,a}$ is monic of degree j. So $\Psi_a(S_{2m,a}) \subset P_m$.

We now prove (a). Write $b(x) = b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i)$.

$$\begin{aligned}
\Phi_a \circ \Psi_a(b(x)) &= \Phi_a\Bigg(b_m + \sum_{i=0}^{m-1} b_{2m-i}D_{m-i,a}(x)\Bigg) \\
&= x^m\left[b_m + \sum_{i=0}^{m-1} b_{2m-i}D_{m-i,a}(x+\frac{a}{x})\right] \\
&= x^m\left[b_m + \sum_{i=0}^{m-1} b_{2m-i}(x^{m-i} + (\frac{a}{x})^{m-i})\right] \\
&= b_m x^m + \sum_{i=0}^{m-1} b_{2m-i}(x^{2m-i} + a^{m-i}x^i) = b(x),
\end{aligned}$$

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

Now in P_m the coefficient of x^m is 1 and the others are arbitrary so that $|P_m| = p^m$. And for $b(x) \in S_{2m,a}$, $b_{2m-1}, \cdots, b_m$ are arbitrary and the other coefficients are determined so that $|S_{2m,a}| = p^m$. Hence $\Psi_a \circ \Phi_a$ is also the identity.

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

$$\begin{aligned}
\Phi_a((fg)(x)) &= x^{r+s}(fg)(x+\frac{a}{x}) \\
&= x^r f(x+\frac{a}{x}) \cdot x^s g(x+\frac{a}{x}) \\
&= \Phi_a(f(x))\Phi_a(g(x)).
\end{aligned}$$

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

$$\begin{aligned}\Phi_a(\Psi_a(b(x)c(x)) &= b(x)c(x) \\ &= (\Phi_a \circ \Psi_a)(b(x)) \cdot (\Phi_a \circ \Psi_a)(c(x)) \\ &= \Phi_a[\Psi_a(b(x))\Psi_a(c(x))] \quad \text{by the first part.}\end{aligned}$$

Consequently,

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

as Φ_a is injective by (a).

For (c), let $b(x) \in S_{2m,a}$ be irreducible. Suppose $\Psi_a(b(x)) = f(x)g(x)$, with $\deg f, \deg g \geq 1$. Then using (a) and (b)

$$b(x) = (\Phi_a \circ \Psi_a)(b(x)) = \Phi_a(f(x))\Phi_a(g(x)),$$

a contradiction. Next suppose $f(x)$ is irreducible and $\Psi_a(f(x)\hat{f}_a(x)) = u(x)v(x)$, with $\deg u(x), \deg v(x) \geq 1$. Then, taking Φ_a, we have $f(x)\hat{f}_a(x) = \Phi_a(u(x))\Phi_a(v(x))$. Since $f(x)$ is irreducible, it divides one of $\Phi_a(u(x))$ or $\Phi_a(v(x))$. Say $f(x)$ divides $\Phi_a(u(x))$. Since $\Phi_a(u(x))$ is a-self reciprocal, $\hat{f}_a(x)$ also divides $\Phi_a(u(x))$. Further, since $\hat{f}_a(x)$ is irreducible and $f(x) \neq \hat{f}_a(x)$ we see that $f(x)\hat{f}_a(x)$ divides $\Phi_a(u(x))$. But then the degree of $\Phi_a(v(x))$ is less than 1, a contradiction. □

4 Factors of Dickson polynomials

If $n = pk$ then $D_{n,a}(x) = [D_{k,a}(x)]^p$ so we assume that $(n, p) = 1$.

Lemma 4.1. *Let $g(x)$ be a separable a-self reciprocal polynomial over $\mathbf{F_q}$. Then $g(x)$ factors as*

$$g(x) = \prod f(x)\hat{f}_a(x) \prod b(x),$$

where each $f(x)$ is irreducible and not a-self reciprocal, each $b(x)$ is irreducible and a-self reciprocal and the $f(x)$ and $b(x)$ are distinct.

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

Lemma 4.2. $\Phi_a(D_{n,a}(x)) = x^{2n} + a^n$.

Proof;

$$\Phi_a(D_{n,a}(x)) = x^n D_{n,a}(x + \frac{a}{x}) = x^n(x^n + (\frac{a}{x})^n) = x^{2n} + a^n,$$

where we have again used Waring's identity. □

Proposition 4.3. *$x^{2n} + a^n$ is separable and a-self reciprocal. Factor as in Lemma 4.1*

$$x^{2n} + a^n = \prod f(x)\hat{f}_a(x) \prod b(x),$$

Then

$$D_{n,a}(x) = \prod \Psi(f(x)\hat{f}_a(x)) \prod \psi(b(x)),$$

is the factorization of $D_{n,a}(x)$ into irreducible polynomials over $\mathbf{F_q}$.

Proof: The first statement is clear. By Lemma 4.2, $\Phi(D_{n,a}(x)) = x^{2n} + a^n$. Applying Ψ using Theorem 2.1(b) we see that each $\Psi(f(x)\hat{f}_a(x))$ and $\Psi(b(x))$ is irreducible by Theorem 2.1(c). □

Example 4.4. *We factor $D(18, 2)$ over $\mathbf{F_7}$.*

Here $n = 18, a = 2, q = 7$ and $a^n = 1$.

$$x^{36} + 1 = [(x^6 + 5x^3 + 2)(x^6 + 6x^3 + 4)][(x^6 + 2x^3 + 2)(x^6 + x^3 + 4)]$$

$$[(x^2+4x+1)(x^2+x+4)][(x^2+3x+1)(x^2+6x+4)](x^2+5x+2)(x^2+2x+2).$$

Now (x^2+5x+2) and (x^2+2x+2) are 2-self reciprocal; the other factors are not but they have been paired with their 2-reciprocals. Consequently, the factors of $D_{18,2}(x)$ are

$$\begin{aligned}
(1)\ \Psi_2((x^6 + 5x^3 + 2)(x^6 + 6x^3 + 4)) &= \Psi_2(x^{12} + 4x^9 + x^6 + 4x^3 + 1) \\
&= D_{6,2}(x) + 4D_{3,2}(x) + 1 \\
&= (x^6 + 2x^4 + x^2 + 5) + 4(x^3 + x) + 1 \\
&= x^6 + 2x^4 + 4x^3 + x^2 + 4x + 6. \\
(2)\ \Psi_2((x^6 + 2x^3 + 2)(x^6 + x^3 + 4)) &= x^6 + 2x^4 + 3x^3 + x^2 + 3x + 6
\end{aligned}$$

$$\begin{aligned}
(3)\quad \Psi_2((x^2+4x+1)(x^2+x+4)) &= \Psi_2(x^4+5x^3+2x^2+3x+4)\\
&= D_{2,2}(x)+5D_{1,2}(x)+2\\
&= (x^2+3)+5(x)+2 = x^2+5x+5\\
(4)\quad \Psi_2((x^2+3x+1)(x^2+6x+4)) &= x^2+2x+5\\
(5)\quad \Psi_2((x^2+5x+2)) &= D_{1,2}(x)+5 = x+5\\
(6)\quad \Psi_2((x^2+2x+2)) &= D_{1,2}(x)+2 = x+2.
\end{aligned}$$

□

5 Cyclotomic factors

As seen in the previous section, to factor $D_{n,a}(x)$ it suffices to factor $x^{2n}+a^n$. In this section we derive the factors of $x^{2n}+a^n$ from factors of cyclotomic polynomials and we provide an algorithm for factoring $D_{n,a}(x)$ for all $a \in \mathbf{F_q}$ with $o(-a^n) = t$.

Proposition 5.1. *Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ which divides $x^{2n}+a^n$. Then either f or $\hat{f}_a$ has order $2dt$ for some divisor d of n with n/d odd and $t = o(-a^n)$.*

Proof: Let β be a root of f. Since f divides $x^{2n}+a^n$, $\beta^{2n} = -a^n$ and $(a/\beta)^{2n} = -a^n$. Hence both $o(\beta)$ and $o(a/\beta)$ divide $2nt$. Now, $(-a^n)^{o(\beta)} = (\beta^{2n})^{o(\beta)} = 1$ so t divides $o(\beta)$. Similarly, t divides $o(a/\beta)$. Write $o(\beta) = s_1t$ and $o(a/\beta) = s_2t$. Then s_1 and s_2 both divide $2n$. Assume that s_1 and s_2 both divide n. Then $\beta^{nt} = 1$ and $(a/\beta)^{nt} = 1$ thus $1 = \beta^{nt} = a^{nt}$. Since $(-a^n)^t = 1$, t must be even. Write $t = 2m$. Then $1 = \beta^{nt} = \beta^{2nm} = (\beta^{2n})^m = (-a^n)^m$. Consequently, t divides m. But $t = 2m > m$, a contradiction. Hence s_1 and s_2 both do not divide n. Suppose s_1 does not divide n. Since s_1 divides $2n$ we can write $s_1 = 2d$ for some d dividing n. Notice that $n/d = 2n/s_1$. Assume that n/d is even and write $2n/s_1 = 2r$. Here we see that $2n = 2rs_1$ and s_1 divides n, a contradiction. Thus n/d is odd. A similar argument will work if s_2 does not divide n. □

Proposition 5.2. *Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of order $2dt$ where d divides n with n/d odd and t divides $q-1$. Then x^{2n} mod $f(x)$ is in $\mathbf{F_q}$.*

Proof: Let β be a root of $f(x)$. Since $\beta^{2dt} = 1$ and d divides n, we see that $(\beta^{2n})^t = 1$ and thus $\beta^{2n} \in \mathbf{F_q}$. Let $c = \beta^{2n}$. Write $x^{2n} = f(x)g(x) + r(x)$ with the degree of $r(x)$ less than the degree of $f(x)$. Then

$$c = \beta^{2n} = f(\beta)g(\beta) + r(\beta) = r(\beta),$$

thus β satisfies $r(x) - c$ and $f(x)$ divides $r(x) - c$. Since the degree of $r(x) - c$ is less than the degree of $f(x)$ we must have $r(x) = c$. □

For a monic irreducible polynomial $f(x)$ over $\mathbf{F_q}$ set

$$r_n(f) = x^{2n} \bmod f(x).$$

The following algorithm is not efficient. The algorithm works best for factoring $D_{n,a}(x)$ for various a's. But still it is simpler to apply one of the standard factorization algorithms to each $D_{n,a}(X)$. We present the algorithm only to illustrate how the previous results combine to factor the Dickson polynomials $D_{n,a}(x)$.

Algorithm for factoring $D_{n,a}(x)$ when $o(-a^n) = t$: For each divisor d of n with n/d odd, factor Q_{2dt}. For each factor f of Q_{2dt} compute $r_n(f)$. If $r_n(f) = -a^n$ then compute $\hat{f}_a$. If $f = \hat{f}_a$ then $\Psi(f)$ is a factor of $D(n, a)$. If $f \neq \hat{f}_a$ then $\Psi(f\hat{f}_a)$ is a factor of $D(n, a)$.

Example 5.3. *We factor $D_{13,2}(x)$ and $D_{13,3}(x)$ over $\mathbf{F_5}$.*

Let $q = 5$, $n = 13$ and $t = 4$. The elements a of $\mathbf{F_5}$ with $o(-a^n) = t$ are 2 and 3. The divisors d of n with n/d odd are 1 and 13. Further, $-2^n = 3$ and $-3^n = 2$.

1. $d = 1$.

Factor f of $Q_{2dt}(x)$	$r_n(f)$	a	a-reciprocal of f	
$x^2 + 3$	2	3	$x^2 + 3$	.
$x^2 + 2$	3	2	$x^2 + 2$	

We see that both factors are a-self reciprocal for their respective a. Consequently, $\Psi_2(x^2 + 2) = x$ is a factor of $D_{13,2}(x)$ and $\Psi_3(x^2 + 3) = x$ is a factor of $D_{13,3}(x)$.

2. $d = 13$.

Factor f of $Q_{2dt}(x)$	$r_n(f)$	a	a-reciprocal of f
$x^4+x^3+2x^2+3x+4$	3	2	$x^4+4x^3+2x^2+2x+4$
x^4+2x^3+x+4	3	2	x^4+3x^3+4x+4
$x^4+2x^3+4x^2+x+4$	3	2	$x^4+3x^3+4x^2+4x+4$.
x^4+4x^3+3x+4	2	3	x^4+x^3+2x+4
$x^4+2x^3+3x^2+4x+4$	2	3	$x^4+3x^3+3x^2+x+4$
$x^4+4x^3+x^2+3x+4$	2	3	$x^4+x^3+x^2+2x+4$

Here we omitted factors of Q_{2dt} that are a-reciprocals of other factors already considered. Notice that the first three factors will contribute to $D_{13,2}(x)$ and the last three factors will contribute to $D_{13,3}(x)$. None of the factors are a self reciprocal, Consequently,

$$\Psi_2((x^4+x^3+2x^2+3x+4)(x^4+4x^3+2x^2+2x+4)) = x^4+2,$$

$$\Psi_2((x^4+2x^3+x+4)(x^4+3x^3+4x+4)) = x^4+3x^2+3$$

and

$$\Psi_2((x^4+2x^3+4x^2+x+4)(x^4+3x^3+4x^2+4x+4)) = x^4+x^2+2$$

are factors of $D_{13,2}(x)$.

$$\Psi_3((x^4+4x^3+3x+4)(x^4+x^3+2x+4)) = x^4+2x^2+3,$$

$$\Psi_3((x^4+2x^3+3x^2+4x+4)(x^4+3x^3+3x^2+1x+4)) = x^4+2$$

and

$$\Psi_3((x^4+4x^3+x^2+3x+4)(x^4+x^3+x^2+2x+4)) = x^4+4x^2+2$$

are factors of $D_{13,3}(x)$ We have

$$D_{13,2}(x) = x(x^4+2)(x^4+3x^2+3)(x^4+x^2+2)$$

and

$$D_{13,3}(x) = x(x^4+2)(x^4+2x^2+3)(x^4+4x^2+2).$$

□

6 Computing $r_n(f)$

In some cases it is not necessary to compute $r_n(f)$ in the algorithm of the previous section as the next two results illustrate.

Proposition 6.1. *Let $a \in \mathbf{F}_\mathbf{q}^*$. Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of degree ω and order $r = 2dt$ where $t = o(-a^n)$. A necessary condition for $r_n(f) = -a^n$ is*

$$(f(0))^{\frac{(q-1)n}{td}} = (-1)^{\frac{\omega(q-1)}{t}} (-a^n)^{\frac{q^\omega-1}{r}}.$$

If $(\frac{q^\omega-1}{r}, q-1) = 1$, this condition is sufficient.

Proof: Let β be a root of f in $\mathbf{F_{q^d}}$ and write $q^\omega - 1 = 2dts$. Recall that $r_n(f) = \beta^{2n}$. If $\beta^{2n} = -a^n$ then

$$\beta^{2d\frac{n}{d}s} = (-a^n)^s$$

$$\beta^{\frac{q^\omega-1}{t}\frac{n}{d}} = (-a^n)^{\frac{q^\omega-1}{r}}$$

$$(-1)^{\frac{\omega(q-1)}{t}} \beta^{\frac{q^\omega-1}{t}\frac{n}{d}} = (-1)^{\frac{\omega(q-1)}{t}} (-a^n)^{\frac{q^\omega-1}{r}}.$$

But

$$f(0) = (-1)^\omega \beta^{\frac{q^\omega-1}{q-1}}$$

thus

$$(f(0))^{\frac{(q-1)n}{td}} = (-1)^{\frac{\omega(q-1)}{t}} \beta^{\frac{q^\omega-1}{t}\frac{n}{d}}$$

since n/d is odd.

Conversely, if β is a root of f then since d divides n we have $(\beta^{2n})^t = 1$ so $\beta^{2n} \in \mathbf{F_q}$. Write again $q^\omega - 1 = 2dts$.

$$(f(0))^{\frac{(q-1)n}{td}} = ((-1)^\omega \beta^{\frac{q^\omega-1}{q-1}})^{\frac{(q-1)n}{td}} = (-1)^{\frac{\omega(q-1)}{t}} \beta^{\frac{q^\omega-1}{t}\frac{n}{d}}.$$

Thus

$$\beta^{\frac{q^\omega-1}{t}\frac{n}{d}} = (-a^n)^{\frac{q^\omega-1}{r}}$$

and

$$(\beta^{2n})^s = (-a^n)^s.$$

Consequently, $o(\frac{\beta^{2n}}{-a^n})$ divides s. If $(q-1, s) = 1$, we have $\beta^{2n} = -a^n$. □

Example 6.2. *We consider $a = 2$ and the polynomial $f(x) = x^4+x^3+2x^2+3x+2$ over $\mathbf{F_7}$.*

$f(x)$ is a monic irreducible polynomial over $\mathbf{F_7}$ of order $60 = 2 \cdot 5 \cdot 6$, $\hat{f}_2(x) = x^4+3x^3+4x^2+4x+1$ and $o(-2^5) = 6$. We have $q-1 = 6$, $t = 6$, $n = 5$, $d = 5$, $f(0) = 2$, $\omega = 4$ and $r = 60$.

$$(f(0))^{\frac{(q-1)n}{td}} = 2 \text{ and } (-1)^{\frac{\omega(q-1)}{t}}(-a^n)^{\frac{q^\omega-1}{r}} = 4$$

thus $r_n(f) \neq -a^n$ and $\Psi(f(x)\hat{f}_a(x))$ is not a factor of $D_{5,2}(x)$. □

Proposition 6.3. *Let $a \in \mathbf{F_q^*}$. Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of degree ω and order $r = 2dt$ where d divides n, n/d is odd and $t = o(-a^n)$. Write $q^\omega - 1 = 2dts$ and suppose there exist a positive integer y such that t divides $(sy-1)$. A necessary and sufficient condition for $r_n(f) = -a^n$ is*

$$(f(0))^{\frac{(q-1)ny}{td}} = (-1)^{\frac{\omega(q-1)y}{t}}(-a^n).$$

Proof: Suppose first that the condition holds. Let β be a root of $f(x)$ in $\mathbf{F_{q^d}}$.

$$((-1)^\omega f(0))^{\frac{(q-1)ny}{td}} = (\beta^{\frac{q^\omega-1}{q-1}})^{\frac{(q-1)ny}{td}} = \beta^{2nsy}.$$

Now, $\frac{\beta^{2nsy}}{\beta^{2n}} = \beta^{2n(sy-1)} = 1$ since t divides $(sy-1)$ and d divides n. Consequently, $\beta^{2nsy} = \beta^{2n}$ and we have

$$\beta^{2n} = ((-1)^\omega f(0))^{\frac{(q-1)ny}{td}} = -a^n$$

Conversely, by Proposition 6.1 we have

$$(f(0))^{\frac{(q-1)n}{td}} = (-1)^{\frac{\omega(q-1)}{t}}(-a^n)^s$$

$$(f(0))^{\frac{(q-1)ny}{td}} = (-1)^{\frac{\omega(q-1)y}{t}}(-a^n)^{sy}$$

$$(-1)^{\frac{\omega(q-1)y}{t}}(f(0))^{\frac{(q-1)ny}{td}} = (-a^n)^{sy} = -a^n$$

since t divides $sy-1$. □

Example 6.4. *We consider $a = 2$ and the polynomials $f(x) = x^3+9$ and $g(x) = x^3+13$ over $\mathbf{F_{43}}$.*

$f(x)$ and $g(x)$ are both monic irreducible polynomial over $\mathbf{F_{43}}$ of order $126 \cdot 9 \cdot 7$, and $o(-2^9) = 7$. We have $q-1 = 42$, $t = 7$, $n = 9$, $d = 9$, $f(0) = 9$, $g(0) = 13$, $\omega = 3$, $r = 60$,$s = 631$ and $y = 1$.

$$(f(0))^{\frac{(q-1)ny}{td}} = 4$$

$$(g(0))^{\frac{(q-1)ny}{td}} = 16$$

$$(-1)^{\frac{\omega(q-1)y}{t}} = 1$$

and

$$(-a^n)^{sy} = \frac{q^\omega - 1}{r} = 4$$

thus $r_n(f) = -a^n$ but $r_n(g) \neq -a^n$ Consequently, $\Psi(f(x)\hat{f}_a(x))$ is a factor of $D_{9,2}(x)$ and $\Psi(g(x)\hat{g}_a(x))$ is not. □

In the final result of this section we show that $r_n(f)$ can be computed using a standard recurrence.

Let $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$ be an irreducible polynomial over $\mathbf{F_q}$. Consider the recurrence given by

$$\rho_1(f) = \rho_2(f) = \cdots = \rho_{d-1}(f) = 0$$

$$\rho_d(f) = 1$$

$$\rho_k(f) = -c_{d-1}\rho_{k-1}(f) - c_{d-2}\rho_{k-2}(f) - \cdots - c_0\rho_{k-d}(f), \text{ for } k > d.$$

Proposition 6.5. *Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of degree d and order st where t divides $q-1$. Then $f(x)$ divides $x^{sk}+f(0)\rho_{sk}(f)$ for any positive integer k.*

Proof: Let β be a root of $f(x)$ in $\mathbf{F_{q^d}}$. The linear mapping $L : \mathbf{F_{q^d}} \to \mathbf{F_q}$ that sends β^j to 0 for $0 \leq j < d-1$ and which sends β^{d-1} to 1 satisfies $L(\beta^j) = \rho_{j+1}(f)$ for $0 \leq j < q^d - 1$. Since $(\beta^{sk})^t = 1$ we see that $\beta^{sk} \in \mathbf{F_q}$ and thus for $1 \leq j < d-1$, $L(\beta^{sk+j}) = L(\beta^{sk}\beta^j) = \beta^{sk}L(\beta^j) = 0$. That is, $\rho_{sk+1}(f) = \rho_{sk+2}(f) = \cdots = \rho_{sk+d-1}(f) = 0$. Let $g(x) = \sum_{i=1}^{sk} \rho_i(f)x^{sk-i}$. We will show that $x^{sk}+f(0)\rho_{sk}(f) = f(x)g(x)$. Notice that the leading term of $f(x)g(x)$ is $x^d\rho_d(f)x^{sk-d} = x^{sk}$ and the constant term of $f(x)g(x)$ is $f(0)\rho_{sk}(f)$, thus it remains to show that the other terms of $f(x)g(x)$ equal 0. For $1 \leq j \leq sk-d$, the coefficient of x^{sk-j} in $f(x)g(x)$ is $c_0\rho_j(f)+c_1\rho_{j+1}(f)+\cdots+c_{d-1}\rho_{j+d-1}(f)+\rho_{j+d}(f) = 0$ by the recurrence relation. For $1 \leq j < d$, the coefficient of x^j

in $f(x)g(x)$ is $c_0\rho_{sk-j}(f) + c_1\rho_{sk-j+1}(f) + \cdots + c_j\rho_{sk}(f)$. Recall however that $\rho_{sk+1}(f) = \rho_{sk+2}(f) = \cdots = \rho_{sk+d-1}(f) = 0$. Consequently, this coefficient can be written as $c_0\rho_{sk-j}(f)+c_1\rho_{sk-j+1}(f)+\cdots+c_{d-1}\rho_{sk+d-j-1}(f)+\rho_{sk+d-j}(f)$ and again the recurrence relation yields the result. □

Corollary 6.6. *Suppose $f(x)$ is a monic irreducible polynomial over $\mathbf{F_q}$ of order $2dt$ for some divisor d of n with n/d odd. Then $r_n(f) = f(0)\rho_{2n}(f)$.*

Proof: $f(x)$ divides $x^{2n} - r_n(f)$ by definition and $f(x)$ divides $x^{2n} + f(0)\rho_{2n}(f)$ by Proposition 6.5 hence $f(x)$ divides $-r_n(f) + f(0)\rho_{2n}(f)$ and thus $r_n(f) = f(0)\rho_{2n}(f)$. □

7 Generalized cyclotomic polynomials

Set $T_{n,a}(x) = x^{2n} + a^n$. In our pursuit of factoring $T_{n,a}(x)$, some interesting factors arose. We will call these factors *generalized cyclotomic polynomials.* In this section we derive the degree, order and invariance of these polynomials and study their relationship to Dickson factors.

Lemma 7.1. *If $k|n$ and n/k is odd then $T_{k,a}(x)|T_{n,a}(x)$ and $D_{k,a}(x)|D_{n,a}(x)$.*

Proof: Note that $y + z$ divides $y^m + z^m$ if m is odd. Set $y = x^{2k}$ and $z = a^k$ to get the result for $T_{n,a}(x)$. Apply Ψ to get the result for $D_{n,a}(x)$. □

Set

$$Q_{n,a}(x) = \frac{T_{n,a}(x)}{\operatorname{lcm}\{T_{k,a}(x) : k|n, \quad n/k \quad \text{odd and} \quad k < n\}}$$

and set

$$H_{n,a}(x) = \frac{D_{n,a}(x)}{\operatorname{lcm}\{D_{k,a}(x) : k|n, \quad n/k \quad \text{odd and} \quad k < n\}}.$$

Thus $Q_{n,a}(x)$ consists of the factors of $T_{n,a}(x)$ which have not occurred as factors of $T_{k,a}(x)$, $k < n$, and similarly for $H_{n,a}(x)$. We call the $Q_{n,a}(x)$ the *a-cyclotomic* polynomials.

Let Δ_m denote the set of primitive mth roots of unity.

Lemma 7.2. 1. *$Q_{n,a}(x)$ is a-self reciprocal, separable and we have that $\Psi(Q_{n,a}(x)) = H_{n,a}(x)$.*

2. We have

$$Q_{n,a}(x) = a^{\phi(2n)} Q_{2n}(x^2/a) = \prod_{\rho \in \Delta_{2n}} (x^2 - a\rho).$$

3. $\deg Q_{n,a}(x) = 2\phi(2n)$*.*

Proof: (1) The first two statements follow from $Q_{n,a}(x)$ being a quotient of separable, a-self reciprocal polynomials. The third follows form Ψ_a being multiplicative, Theorem 3.1.

(2) We begin with

$$\begin{aligned} x^n + 1 &= \prod_{d|n,\ \frac{n}{d}\ odd} Q_{2d}(x) \\ x^{2n} + a^n &= a^n \prod_{d|n,\ \frac{n}{d}\ odd} Q_{2d}(x^2/a). \end{aligned}$$

And so the new part of $x^{2n} + a^n$ is

$$Q_{n,a}(x) = a^{\phi(2n)} Q_{2n}(x^2/a) = \prod_{\rho \in \Delta_{2n}} (x^2 - a\rho).$$

This proves (2) and (3) follows immediately from (2). □

Let w denote the order of q modulo $2n$. Then $Q_{2n}(x)$ factors, over $\mathbf{F_q}$, as a product of irreducible polynomials, each of degree w. Let ρ_0 be a particular primitive $(2n)$th root of unity. The factorization of $Q_{2n}(x)$ is $\prod c_i(x)$ where for each i

$$c_i(x) = \prod_{\rho \in S_i} (x - \rho)$$

over a subset S_i of Δ_{2n}, an orbit under the automorphism group of $F(\rho_0)/F$. Fix a $\rho_i \in S_i$ for each i. Let w' denote the order of q modulo $4n$.

Lemma 7.3. *Either* $w' = w$ *or* $w' = 2w$*.*

Proof: Since $q^{w'} \equiv 1 \pmod{2n}$ we get $w|w'$. And $q^{w'} - 1 = (q^w - 1)(q^w + 1)$, $q^w + 1$ is even, so $q^{2w} \equiv 1 \pmod{4n}$. Hence $w'|2w$. □

Lemma 7.4. *1. All irreducible factors of* $Q_{n,a}(x)$ *have the same degree.*

2. *The degree of an irreducible factor of $Q_{n,a}(x)$ is w iff one of the following holds:*

   (a) w is even and $w' = w$.

   (b) w is odd, $w' = w$ and a is a square.

   (c) w is odd, $w' = 2w$ and a is a non-square.

3. *In all other cases, the degree of an irreducible factor of $Q_{n,a}(x)$ is $2w$.*

Proof: Set

$$h_i(x) = \prod_{\rho \in S_i} (x^2 - a\rho).$$

Then $h_i(x) = a^w c_i(x^2/a) \in \mathbf{F_q}[\mathrm{x}]$ and $Q_{n,a}(x) = \prod h_i(x)$, by Lemma 7.2. Note that the automorphisms of $\mathbf{F_q}(\rho_0)/\mathbf{F_q}$ permute the $x^2 - a\rho$, over $\rho \in S_i$. Hence if $x^2 - a\rho_i$ is irreducible over $\mathbf{F_q}(\rho_0)$ then $h_i(x)$ is irreducible, of degree $2w$. If $x^2 - a\rho_i$ splits as $(x + u(\rho_i))(x + v(\rho_i))$, for polynomials u, v over $\mathbf{F_q}$, then $h_i(x) = k)i(x)m_i(x)$ where

$$k_i(x) = \prod_{\rho \in S_i} (x + u(\rho)) \quad \text{and} \quad m_i(x) = \prod_{\rho \in S_i} (x + v(\rho)),$$

are irreducible over $\mathbf{F_q}$ of degree w.

(1) Fix a primitive $(2n)$th root of unity ρ_0. Suppose one irreducible factor of $Q_{n,a}(x)$ has degree w. Then for some primitive $(2n)$th root of unity ρ_1, $x^2 - a\rho_1$ splits in $\mathbf{F_q}(\rho_{\mathbf{0}})$. Thus $a\rho_1 = u^2$ for some $u \in \mathbf{F_q}(\rho_0)$.

Let ρ_i be another primitive $(2n)$th root of unity. Then $\rho_i = \rho_1^s$ for some s prime to $2n$. In particular, s is odd. Then $a^s\rho_i = u^{2s} = a^s\rho_1^s$ and so $a\rho_i = [u^s a^{-(s-1)/2}]^2 \in \mathbf{F_q}(\rho_0)^2$. Thus all $x^2 - a\rho_i$ split in $\mathbf{F_q}(\rho_{\mathbf{0}})$ and all factors have degree w. Otherwise, no $x^2 - a\rho_i$ split in $\mathbf{F_q}(\rho_{\mathbf{0}})$ and all factors have degree $2w$.

(2), (3) Let ρ be a primitive $(2n)$th root of unity. Note that $\mathbf{F_q}(\rho) = \mathbf{F_{q^w}}$ and $\mathbf{F_q}(\sqrt{\rho}) = \mathbf{F_{q^{w'}}}$. Thus $\sqrt{\rho} \in \mathbf{F_q}(\rho)$ iff $w = w'$. And $\sqrt{a} \in \mathbf{F_q}(\rho)$ iff w is even or a is a square (in $\mathbf{F_q}$).

We check the cases. If $w' = w$ is even then $\sqrt{a}$ and $\sqrt{\rho}$ are in $\mathbf{F_q}(\rho)$. So $x^2 - a\rho$ splits in $\mathbf{F_q}(\rho)$ and all factors have degree w.

If $w' = w$ is odd then $\sqrt{\rho} \in \mathbf{F_q}(\rho)$ and $\sqrt{a} \in \mathbf{F_q}(\rho)$ iff a is a square in $\mathbf{F_q}$. So if a is a square then $x^2 - a\rho$ splits in $\mathbf{F_q}(\rho)$ and all factors have degree w. If a is not a square then $x^2 - a\rho$ does not split in $\mathbf{F_q}(\rho)$ and the factors have degree $2w$.

If $w' = 2w$ with w even then $\sqrt{a} \in \mathbf{F_q}(\rho)$ and $\sqrt{\rho} \notin \mathbf{F_q}(\rho)$. Hence $x^2 - a\rho$ does not split in $\mathbf{F_q}(\rho)$ and the factors have degree $2w$.

Lastly, suppose $w' = 2w$ and w is odd. Then neither $\sqrt{a}, \sqrt{\rho}$ are in $\mathbf{F_q}(\rho)$. Both have degree 2 over $\mathbf{F_q}(\rho)$ and so $\sqrt{a} = \beta\sqrt{\rho}$ for some $\beta \in \mathbf{F_q}(\rho)$. Then $a\rho = \beta^2\rho^2 \in \mathbf{F_q}(\rho)^2$. Hence $x^2 - a\rho$ splits and the irreducible factors of $Q_{n,a}(x)$ have degree w. □

Proposition 7.5. *Let $g(x)$ be an irreducible factor of $Q_{n,a}(x)$. If $g(x)$ is a-self reciprocal of degree $d = 2e$ then $2n|q^e + 1$.*

Proof: Let α be a root of $g(x)$. Then we have that $\alpha^{q^e} = a/\alpha$ by Theorem 2.1, and α^2/a is a primitive $2n$th root of unity, by Lemma 7.2. Now

$$(\alpha^2/a)^{q^e+1} = (\alpha^{q^e})^2\alpha^2/a^2 = 1.$$

And so $2n$ divides $q^e + 1$. □

Lemma 7.6. *1. Either every irreducible factor of $Q_{n,a}(x)$ is a-self reciprocal or none are.*

2. An irreducible factor $g(x)$ of $Q_{n,a}(x)$ is a-self reciprocal iff $\deg g$ is even (say $\deg g = 2e$), $2n|q^e + 1$ (say $q^e + 1 = 2ns$) and one of the following holds:

(a) s is odd, e is odd and a is a non-square.

(b) s is even and a is a square.

Proof: Let $g(x)$ be an irreducible factor of $Q_{n,a}(x)$. Suppose $g(x)$ is a-self reciprocal. Now $\deg g$ is even, say $\deg g = 2e$. Also, by Proposition 7.5, $2n|q^e + 1$. Write $q^e + 1 = 2ns$. Let α be a root of $g(x)$. As $g(x)$ divides $Q_{n,a}(x)$ which divides $T_{n,a}(x) = x^{2n} + a^n$, we have that $\alpha^{2n} = -a^n$. Theorem 2.1 gives $\alpha^{q^e} = a/\alpha$. So

$$a = \alpha^{q^e+1} = \alpha^{2ns} = (-1)^s a^{ns}.$$

Then $a^{(q^e-1)/2} = (-1)^s$. Write

$$\frac{q^e - 1}{2} = \frac{q-1}{2}(1 + q + q^2 + \cdots + q^{e-1})$$

and let Q be the second factor. Then we have

$$a^{\frac{q-1}{2}Q} = (-1)^s, \tag{1}$$

Conversely, suppose irreducible g has degree $2e$ and that $q^e + 1 = 2ns$. We still have $\alpha^{2n} = -a^n$ as g divides $T_{n,a}(x)$. If Equation 1 holds then

$$\alpha^{q^e+1} = \alpha^{ns} = (-1)^s a^{ns} = a,$$

and g is self reciprocal.

(1) We have shown that $g(x)$ being a-self reciprocal depends only on $\deg g$. By Lemma 7.4, all irreducible factors of $Q_{n,a}(x)$ have the same degree. Hence either all factors are a-self reciprocal or none are.

(2) We need only check when Equation 1 holds. Note that with Q is odd iff e is odd and

$$a^{\frac{q-1}{2}} = \begin{cases} 1, & \text{if } a \text{ is a square} \\ -1, & \text{if } a \text{ is not a square.} \end{cases}$$

Both sides of Equation 1 are -1 iff s is odd, e is odd and a is a non-square. This is case (a). Both sides of Equation 1 are $+1$ iff s is even and either e is even or a is a square. But s and e cannot both be even. Namely, e even implies that $q^e \equiv 1 \pmod 4$ and so $q^e + 1 \equiv 2 \pmod 4$. But then $q^e + 1 = 2ns$ with s odd. Thus both sides of Equation 1 are $+1$ iff s is even and a is a square, which is case (b). □

Proposition 7.7. *Let α be a root of an irreducible factor $g(x)$ of $Q_{n,a}(x)$. Set $\beta = a/\alpha$ and let $t = o(-a^n)$. We have $lcm(o(\alpha), o(\beta)) = 2nt$. In particular, if $g(x)$ is a-self reciprocal then $o(g(x)) = 2nt$ and if $g(x)$ is not a-self reciprocal then $o(g(x)\hat{g}_a(x)) = 2nt$.*

The proof is long and technical. It is postponed to the last section.

Theorem 7.8. *Suppose $n > 1$. Let $t = o(-a^n)$.*

1. *Suppose that $w' = w$ is even (say $w = 2v$), $2n|q^v+1$ (say $q^v+1 = 2ns$) and one of the following holds:*

   (a) s is odd, v is odd and a is not a square,

   (b) s is even and a is a square.

Then each irreducible factor of $Q_{n,a}(x)$ has degree w, order $2nt$ and is a-self-reciprocal.

2. *Suppose that $w' = w$ is even but Case 1 does not hold. Then each irreducible factor $g(x)$ of $Q_{n,a}(x)$ has degree w, is not a-self reciprocal and $g(x)\hat{g}_a(x)$ has order $2nt$.*

3. *Suppose that $w' = w$ is odd and a is a square. Then each irreducible factor $g(x)$ of $Q_{n,a}(x)$ has degree w, is not a-self reciprocal and $g(x)\hat{g}_a(x)$ has order $2nt$.*

4. *Suppose that $w' = 2w$, w is odd, and a is not a square. Then each irreducible factor $g(x)$ of $Q_{n,a}(x)$ has degree w, is not a-self reciprocal and $g(x)\hat{g}_a(x)$ has order $2nt$.*

5. *In all other cases, each irreducible factor $g(x)$ of $Q_{n,a}(x)$ has degree $2w$, is not a-self reciprocal and $g(x)\hat{g}_a(x)$ has order $2nt$.*

Proof: First suppose $w = w' = 2v$ is even and $2n|q^v + 1$, with $q^v + 1 = 2ns$. Then the degree of an irreducible factor is w, by Lemma 7.4. Apply Lemma 7.6, with $e = v$, to get each factor is a-self reciprocal. The order follows from Proposition 7.7.

The other cases follow even more easily from Proposition 7.7, Lemma 7.4 and Lemma 7.6. □

Example 7.9. Each of the cases of Theorem 7.8 does occur.

1. Let $q = 5$ and $n = 7$. Then $w = w' = 6$ so $v = 3$. And $5^3 + 1 = 14 \cdot 9$ so that $s = 9$. If $a = 2$, a non-square, then we are in Case 1a. Here $t = o(-2^7) = 4$. The irreducible factors of $Q_{7,2}(x)$ all have degree 6, order 56 and are 2-self-reciprocal. If $a = 4$, a square, then we are in Case 2 and the factors still have degree 6, but none are 4-self-reciprocal. Here $t = 1$ so for each factor $g(x)$, $g(x)\hat{g}_4(x)$ has order 14.

2. Let $q = 7$ and $n = 11$. Then $w = w' = 10$ so $v = 5$. And $7^5+1 = 22\cdot 764$ so that $s = 764$. If $a = 2$, a square, then we are in Case 1b. Here $t = o(-2^{11}) = 6$. The irreducible factors of $Q_{11,2}(x)$ all have degree 10, order 132 and are 2-self-reciprocal. If $a = 3$, a non-square, then we are in Case 2 and the degree of the factors is still 10 but none of them

are 3-self-reciprocal. Here $t = 3$ so for each factor $g(x)$, $g(x)\hat{g}_3(x)$ has order 66.

3. Let $q = 5$ and $n = 11$. Then $w = w' = 5$. If $a = 4$ then we are in Case 3. The irreducible factors of $Q_{11,4}(x)$ have degree 5 and none are 2-self-reciprocal. Here $t = 1$ so for each factor $g(x)$, $g(x)\hat{g}_4(x)$ has order 22. If $a = 2$ then we are in Case 5. The degree of the factors is now 10 and each $g(x)\hat{g}_2(x)$ has order $22t = 88$.

4. Let $q = 7$ and $n = 9$. Then $w = 3$ and $w' = 6$. If $a = 3$ we are in Case 4. Here $t = o(-3^9) = 1$. The irreducible factors of $Q_{9,3}(x)$ all have degree 3 and are not 3-self-reciprocal. The order of $g(x)\hat{g}_3(x)$ is 18. If $a = 2$ then we are in Case 5 and the factors now have degree 6 and each $g(x)\hat{g}_2(x)$ has order 36.

Each of these examples may be easily verified with MAPLE.

The following corollary appeared, with different notation, in [2].

Corollary 7.10. *The irreducible factors of $H_{n,a}(x)$ all have the same degree. This degree is (referring to the Cases of Theorem 7.8)*

1. *$w/2$ in Case 1,*
2. *w in Cases 2, 3, and 4,*
3. *$2w$ in Case 5.*

Proof: Combine Theorem 3.1, Lemma 7.2 and Theorem 7.8. □

Example 7.11. Let $n = 45$, $q = 29$ and $a = 12$, a non-square. Then $t = 4$, $w = w' = 6$ and $q^3 + 1 = 90 \cdot 271$, so we are in Case 1(a). Factoring $Q_{360}(x)$ gives 16 polynomials of degree 6, all of the form $x^6 + bx^3 + c$ with $c = 12$ or 17. These are:

$$\begin{array}{lcl} c = 12 \qquad b & = & 1, 2, 4, 11, 18, 25, 27, 28 \\ c = 17 \qquad b & = & 5, 10, 12, 13, 16, 17, 19, 24. \end{array}$$

Computation shows that $r_{45}(f) = 17 = -12^{45}$ precisely for the factors with $c = 17$ (see after Proposition 6.3 for an explanation of this). Each of these factors is 12-self reciprocal and

$$\Psi_{12}(x^6 + bx^3 + 17) = \Psi_{12}(x^3(x^3 + (12/x)^3 + b) = D_{3,12}(x) + b = x^3 + 22x + b.$$

The product of these $\Psi_{12}(f)$, over the $(b, 17)$, is $H_{45,12}(x)$.

Example 7.12. Let $n = 45$, $q = 31$ and $a = 3$, a non-square.Then $t = 1$, $w = 3$ and $w' = 6$ so we are in Case 4. The only divisors d of 45 with the order of q modulo $2dt$ equal to 3 are $d = 9, 45$. The factors of both $Q_{18}(x)$ and $Q_{90}(x)$ have the form $x^3 + b$. These are

$$\begin{array}{lcl} Q_{18}(x) & b & = & 5, 25 \\ Q_{90}(x) & b & = & 7, 9, 10, 14, 18, 19, 20, 28. \end{array}$$

We get $r_{45}(f) = 1 = -a^{45}$ for all of these factors. But $r_9(f) = 2 = -a^9$ for $a = 10, 19$ so these two values must be omitted. Each of the remaining $f\hat{f}_3$ has the form $x^6+cx^3+27 = x^3(x^3+(3/x)^3+c)$ for $c = 2, 4, 5, 12, 19, 26, 27, 29$. Hence

$$\Psi_3(f\hat{f}_3) = D_{3,3,}(x) + c = x^3 + 22x + c$$

and their product is $H_{45,3}(x)$.

Note that the discarded factors, $x^3 + b$ for $b = 10, 19$, have the same degree, order and invariance as the factors of $Q_{45,3}(x)$ (given by Theorem 7.8), but are not factors of $Q_{45,3}(x)$.

8 Proof of Proposition 7.7

We begin with three not quite obvious lemmas about cyclic groups.

Lemma 8.1. *Let $b, c \in GF(q)^*$ and let π be an odd prime. Let $e = v_\pi(q-1)$, the highest power of π dividing $q-1$. If $c^{\pi^{e+1}} = -b^{\pi^{e+1}}$ then $c^{\pi^e} = -b^{\pi^e}$.*

Proof: We have $c^{\pi^{e+1}} = (-b)^{\pi^{e+1}}$ and so $x^{\pi^{e+1}} = 1$ for $x = c/(-b)$. Then $o(x)|\pi^{e+1}$. Also $o(x)|(q-1)$. Hence $o(x)$ divides $(\pi^{e+1}, q-1) = \pi^e$. So $x^{\pi^e} = 1$ and we are done. □

Lemma 8.2. *Let G be a cyclic group of even order and let ϵ be the unique element of order 2. Let $a \in G$.*

1. *$o(a) = 2^m$ iff $a^{2^{m-1}} = \epsilon$.*

2. *If $o(a^{2^n}) = 2^m$ then $o(a) = 2^{n+m}$.*

3. *If $o(\epsilon a) = n$ then*

$$o(a) = \begin{cases} n/2, & \text{if } n \equiv 2 \pmod 4 \\ n, & \text{if } n \equiv 0 \pmod 4 \\ 2n, & \text{if } n \equiv 1, 3 \pmod 4). \end{cases}$$

Proof: (1) If $o(a) = 2^m$ then $a^{2^{m-1}}$ has order 2 and so equals ϵ. Conversely, assume that $a^{2^{m-1}} = \epsilon$. Then $o(a)|2^m$. Suppose $o(a) = 2^k$ with $k < m$. Then

$$\epsilon = a^{2^{m-1}} = (a^{2^k})^{2^{m-1-k}} = 1,$$

a contradiction. Thus $o(a) = 2^m$.

(2) We have from (1) that

$$a^{2^{n+m-1}} = (a^{2^n})^{2^{m-1}} = \epsilon.$$

Hence, by the other direction of (1), $o(a) = 2^{n+m}$.

(3) First, suppose $n = 2m$ with m odd. Note that $(\epsilon a)^m$ has order two and so $(\epsilon a)^m = \epsilon$, $\epsilon a^m = \epsilon$ and $a^m = 1$. Let $k = o(a)$. Then $k|m$ and so k is odd. We have $a^k = 1$, $(\epsilon a)^k = \epsilon$ and $(\epsilon a)^{2k} = 1$. Thus $n|2k$, $m|k$ and so $k = m$.

Next, suppose $n = 4m$. Note that $a^n = (\epsilon a)^n = 1$. Further, $(\epsilon a)^{2m} = \epsilon$ and so $a^{2m} + \epsilon$. Let $k = o(a)$. Then $k|4m$. If $k|2m$ then $1 = a^k = a^{2m} = \epsilon$, a contradiction. So $k = 4m'$ where $m'|m$. We have $1 = a^{4m'} = (\epsilon a)^{4m'}$ so that $n = 4m$ divides $4m'$. Thus $m = m'$ and $k = n$.

Lastly, suppose n is odd. Then $(\epsilon a)^n = 1$ implies $a^n = \epsilon$ and $a^{2n} = 1$. Let $k = o(a)$. Then $k|2n$. If $k|n$ then $1 = a^k = a^n = \epsilon$, a contradiction. Thus $k = 2n'$ where $n'|n$. Then $a^{n'}$ has order two and so $a^{n'} = \epsilon$. As n' is odd, we have $(\epsilon a)^{n'} = 1$ and $n|n'$. Thus $n = n'$ and $k = 2n$. □

Lemma 8.3. *Let G be a finite cyclic group and let $a, b \in G$.*

1. *If $o(a^k) = t$ then $o(a) = ts$ for some s that divides k such that (k/s) is prime to t.*

2. *If $o(a) = n$ and $o(b) = m$ then $o(ab) = n'm's$ where $d = (n, m)$, $n' = n/d$, $m' = m/d$, and for some s dividing d such that (d/s) is prime to $n'm'$.*

Proof: (1) Note $\langle a^k \rangle < \langle a \rangle$ so t divides $o(a)$. And $a^{kt} = 1$ so $o(a)|tk$. Hence $o(a) = ts$, for some s dividing k. Write $k = sk'$. We also have

$$o(a^k) = \frac{ts}{(ts, k)} = \frac{t}{(t, k')},$$

so that $(t, k') = 1$.

(2) We have $(ab)^d = a^d b^d$, $o(a^d) = n'$ and $o(b^d) = m'$. As $(n', m') = 1$, we get $o((ab)^d) = n'm'$. Apply (1). $\square$

Let $t = o(-a^n)$. Let $g(x)$ be an irreducible factor of $Q_{n,a}(x)$ and let α be a root of $g(x)$.

Note that as $-a^n \in F$, t divides $q-1$. We set up notation:

$$n = 2^e AB,$$

where A is the largest common odd factor of n and $q-1$, and B is odd. Write

$$q - 1 = 2AA_1,$$

$$t_1 = (t, A_1) \qquad t = t_1 t_2 \qquad A_1 = t_1 A_2 \qquad 2A = t_2 A_3.$$

Note that $(t_2, A_2) = 1$. Further, let $e_2 = v_2(A_2)$ and write

$$A_2 = 2^{e_2} A_4.$$

Lastly, set $f = \max\{0, e - e_2\}$. Note that $e_2 + f \geq e$.

Lemma 8.4. *Let k be the least positive integer with $\alpha^k \in F$. Then $k = 2^f B t_2$.*

Proof: We proceed in four steps.

Step 1. $k | 2^f B t_2$.

We wish to calculate $(\alpha^{2^f B t_2})^{q-1}$. Now

$$\begin{aligned} 2^f B t_2 (q-1) &= 2^f B t_2 (2A)(t_1 2^{e_2} A_4) \\ &= 2(2^{f+e_2} AB) t A_4 \\ &= 2(2^e AB) t 2^{f+e_2-e} A_4 \\ &= 2nt(2^{f+e_2-e} A_4). \end{aligned}$$

Since $\alpha^{2nt} = (-a^n)^t = 1$, we get $(\alpha^{2^f B t_2})^{q-1} = 1$. Thus $\alpha^{2^f B t_2} \in F$ and $k | 2^f B t_2$.

Step 2. $B | k$.

We first introduce yet more notation. As $\alpha^{2n} = -a^n \in F$, we have $k | 2n$. Write $2n = km$.

Let B_1 be a factor (greater than 1) of B that is prime to $q-1$. Suppose, if possible, that $B_1 | m$; write $m = B_1 m_1$. Note that km is even as is km_1, since B_1 is odd. In this notation, we have

$$\alpha^{km} = -a^n = -a^{km/2}.$$

Let $c = \alpha^k$; $c \in F$. Then

$$c^m = c^{B_1 m_1} = -a^{kB_1 m_1/2} = (-1)^{B_1} a^{kB_1 m_1/2}.$$

The map $x \mapsto x^{B_1}$ is an isomorphism of F, since B_1 is prime to $q-1$, so we have

$$c^{m_1} = -a^{km_1/2}.$$

But then

$$\alpha^{km_1} = (-a)^{km_1/2} = -a^{km_1/2},$$

and α is a root of $T_{km_1/2,a}(x)$. Now n divided by $km_1/2$ is $(2n)/(km_1) = m/m_1 = B_1$ is odd. But α, a root of $Q_{n,a}$, is not a root of any T_i with $i|n$, $i \neq n$ and n/i odd. Hence $2n = km_1$, $m = m_1$, $B_1 = 1$, a contradiction. Hence B_1 divides k.

Next we consider factors of B that are not prime to $q-1$. Suppose π is a prime dividing B and $q-1$. Note that B is odd, so π is odd. Let $e = v_\pi(A)$ and $f = v_\pi(B) \geq 1$ so that $v_\pi(n) = e + f$. Note that $v_\pi(q-1) = e$ as $A = (n, q-1)$.

We want to show π^f divides k. Suppose instead that $v_\pi(k) \leq f - 1$. Then $v_\pi(m) \geq e + 1$. Write $m = \pi^{e+1} m_2$. We have

$$\begin{aligned} c^m &= -a^{km/2} \\ (c^{m_2})^{\pi^{e+1}} &= -(a^{km_2/2})^{\pi^{e+1}} \\ (c^{m_2})^{\pi^e} &= -(a^{km_2/2})^{\pi^e}, \end{aligned}$$

using Lemma 8.1. But then

$$\alpha^{km/\pi} = c^{m/\pi} = c^{m_2 \pi^e} = -a^{km/(2\pi)},$$

contradicting the fact that α is not a root of T_i for $i < n$ and n/i odd. Hence $\pi^f | k$. This completes that proof that $B|k$.

Step 3. $Bt_2|k$.

By Step 2, we have that $k = B\ell$, for some ℓ dividing t_2. Then

$$\begin{aligned} 1 = (\alpha^k)^{2^e(q-1)} &= \alpha^{B\ell \cdot 2^e \cdot 2AA_1} \\ &= (\alpha^{2 \cdot 2^e AB})^{\ell A_1} \\ &= (-a^n)^{\ell A_1}. \end{aligned}$$

Thus t divides ℓA_1. So $t_2 = t/t_1$ divides $\ell A_1/t_1 = \ell A_2$. Since $(t_2, A_2) = 1$ we have that $t_2|\ell$. So $Bt_2|k$ as desired.

Step 4. Finish.

Combining Steps 1 and 3 shows we can write $k = 2^h B t_2$ for some $h \leq f \leq e$. Let $\alpha^k = c \in F$. Now

$$\begin{aligned} c^{2^{e-h}A_3} &= \alpha^{2^{e-h}A_3 2^f B t_2} \\ &= \alpha^{2^e(2A)B} = \alpha^{2n} = -a^n, \end{aligned}$$

has order t. Write $t = 2^{v_2(t)}t'$ and $A_3 = 2^{v_2(A_3)}A_3'$, with t' and A_3' odd. Then

$$(-a^n)^{t'} = c^{2^{e-h}t'A_3} = c^{2^{e-h+v_2(A_3)}t'A_3'},$$

has order $2^{v_2(t)}$. By Lemma 8.2, the order of $c^{t'A_3'}$ is 2 to the power of $e - h + v_2(A_3) + v_2(t)$. This must divide $q-1$, as $c \in F$. So

$$v_2(q-1) \geq e - h + v_2(A_3) + v_2(t).$$

Now $q - 1 = 2AA_1 = t_2A_3 \cdot t_1A_2 = tA_2A_3$. Thus

$$\begin{aligned} v_2(t) + v_2(A_2) + v_2(A_3) &\geq e - h + v_2(A_3) + v_2(t) \\ h &\geq e - v_2(A_2) = e - e_2. \end{aligned}$$

As h is non-negative, we have $h \geq \max\{0, e - e_2\} = f$. But $h \leq f$ by Step 1, so $h = f$ and $k = 2^f B t_2$. □

As above, set:

$$c_\alpha = \alpha^{2^f B t_2} \in F.$$

Lemma 8.5. *1. $o(\alpha) = 2^f B t_2 o(c_\alpha)$.*

2. $c_\alpha^{2^{e-f}A_3} = -a^n$.

3. Suppose $2^f t_2$ is even. Then $c_\alpha = xy$, where $o(x) = 2 \cdot 2^{e-f}A_3$ and $y = a^{2^f B t_2/2}$. Further, $o(-y^{2^{e-f}A_3}) = t$.

4. Suppose $2^f t_2$ is odd. Then $c_\alpha^2 = xy$, where $o(x) = 2^e A_3$ and $y = b^{Bt_2}$. Further, $o(-y^{2^e A_3/2}) = t$.

Proof: (1) Just for this proof, let $d = o(\alpha)$. Then $\alpha^d = 1 \in F$ so that $k = 2^f B t_2$ divides d, using the value of k from Lemma 8.4. Write $d = 2^f B t_2 d_2$. Then

$$1 = \alpha^d = \alpha^{2^f B t_2 d_2} = c_\alpha^{d_2}$$

and so $o(c_\alpha)$ divides d_2.

Also $\alpha^{2^f Bt_2 o(c_\alpha)} = c_\alpha^{o(c_\alpha)} = 1$ so $d = 2^f Bt_2 d_2$ divides $2^f Bt_2 o(c_\alpha)$. Thus we have the converse that $d_2 | o(c_\alpha)$. So $d_2 = o(c_\alpha)$.

(2) We have,

$$c_\alpha^{2^{e-f}A_3} = \alpha^{2^e Bt_2 A_3} = \alpha^{2 \cdot 2^e AB} = \alpha^{2n} = -a^n.$$

(3) We assume that $2^f t_2$ is even. Now $e_2 \geq e - f$ so that 2^{e-f} divides A_2, and so A_1. And t_2 divides $2A$. Thus $2^{e-f}t_2$ divides $2AA_1 = q-1$. We have, by (2),

$$c_\alpha^{2^{e-f}2A_3} = -a^{2^e Bt_2 A_3/2}.$$

Thus, in F, we may take roots of order $2^{e-f}A_3$, obtaining $c_\alpha = xy$ where $x^{2^{e-f}A_3} = -1$ and $y = a^{2^f Bt_2/2}$.

We check that $o(x) = 2 \cdot 2^{e-f}A_3$. Recall that $A_3 = 2^{e_3}A_5$ with A_5 odd. Then

$$(x^{A_5})^{2^{e-f+e_3}} = -1.$$

So $o(x^{A_5}) = 2 \cdot 2^{e-f+e_3}$ by Lemma 8.2 (1). Hence $o(x) = 2 \cdot 2^{e-f+e_3}\pi$ for some divisor π of A_5. Then

$$\alpha^{2^{e+e_3}Bt_2\pi} = c_\alpha^{2^{e-f+e_3}\pi} = x^{2^{e-f+e_3}\pi} y^{2^{e-f+e_3}\pi} = (-1)b^{2^{e+e_3}Bt_2\pi/2}.$$

Hence α is a root of $T_i(x)$, for $i = 2^{e+e_3}Bt_2\pi/2$ and $n/i = A_5/\pi$ is odd. Since α is a root of $Q_n^b(x)$, the new part of $T_n(x)$, we must have $\pi = A_5$ as desired.

To complete (3) note that $y^{2^{e-f}A_3} = a^{2^e Bt_2 A_3/2} = a^n$ so that $-y^{2^{e-f}A_3}$ has order t.

(4) Now assume $2^f t_2$ is odd. Note that $f = 0$, A_3 is even and $A_3/2$ is odd. We have

$$c_\alpha^{2^e A_3} = -a^{2^e Bt_2 A_3/2}.$$

Take roots of order $2^e A_3/2$ to get:

$$c_\alpha^2 = xy \qquad x^{2^e A_3/2} = 1 \qquad y = a^{t_2 B}.$$

The proof that $o(x) = 2^e A_3$ is similar to that of (3). And, also similarly, $y^{2^e A_3/2} = a^{2^e Bt_2 A_3/2} = a^n$ so that $-y^{2^e A_3/2}$ has order t □

We introduce yet more notation. Set $\beta = a/\alpha$, which is a root of $\hat{g}_a(x)$. Set

$$c_\beta = \beta^{2^f Bt_2} = \frac{a^{2^f Bt_2}}{c_\alpha}.$$

Proof of Proposition 7.7 It is enough to show $\mathrm{lcm}(o(\alpha), o(\beta)) = 2nt$. By the first part of Lemma 8.5, it suffices to show $\mathrm{lcm}(o(c_\alpha), o(c_\beta)) = 2^{e-f}A_3t$ as then

$$\mathrm{lcm}(o(\alpha), o(\beta)) = 2^f Bt_2 \cdot 2^{e-f}A_3t = 2^e(t_2A_3)Bt = 2nt.$$

Part I We first consider the case where $2^f t_2$ is even. We check that t is even in this case. If t_2 is even then $t = t_1t_2$ is even. Say $f \geq 1$. If t is odd then $o(a^n) = 2t$ by Lemma 8.2. Then $o(a^{nt}) = 2$, $o((a^{ABt})^{2^e}) = 2$ and $o(a^{ABt}) = 2^{e+1}$, by Lemma 8.2. This must divide $q-1$. So

$$\begin{array}{rcl} v_2(q-1) & \geq & e+1 \\ v_2(A_2)+1 & \geq & e+1 \\ e_2 & \geq & e. \end{array}$$

But then $f = 0$,a contradiction. Hence when $2^f t_2$ is even, t is even.

From Lemma 8.5, we have that $c_\alpha = xy$, where $o(x) = 2 \cdot 2^{e-f}A_3$ and $o(-y^{2^{e-f}}) = t$. Then, by Lemma 8.2, $o(y^{2^{e-f}}) = t/2$ if $t \equiv 2 \pmod 4$ and t, if $t \equiv 0 \pmod 4$.

Case 1 First suppose that $t \equiv 2 \pmod 4$. Then

$$o(y) = \frac{1}{2}ts_1/2 \quad \text{with} 2^{e-f}A_3 = s_1s_2, (s_2, t/2) = 1,$$

by Lemma 8.3. Then

$$(o(x), o(y)) = (2s_1s_2, \frac{1}{2}ts_1) = s_1(2s_2, \frac{1}{2}t) = s_1,$$

as s_2 is prime to $t/2$ and $t/2$ is odd. Apply Lemma 8.3 to get

$$o(c_\alpha) = (2s_2)(t/2)s_3 \quad \text{with} \quad s_1 = s_3s_4, (s_4, ts_2) = 1.$$

Now we have $c_\beta = y^2/c_\alpha$. Here $o(y^2)$ is $ts_1/2$ if s_1 is odd, and $ts_1/4$ if s_1 is even.

Case 1A We suppose s_1 is odd. Then

$$(o(c_\alpha, o(y^2)) = (ts_2s_3, \frac{1}{2}ts_3s_4/2) = (ts_3/2)(2s_2, s_4) = ts_3/2,$$

as s_4 is prime to ts_2 and t is even. Apply Lemma 8.3 once again to get

$$o(c_\beta) = s_4(2s_2)s_5, \qquad ts_3/2 = s_5s_6, (s_6, 2s_2s_4) = 1.$$

We obtain:

$$\begin{aligned}\mathrm{lcm}(o(c_\alpha), o(c_\beta)) &= \mathrm{lcm}(ts_2s_3, 2s_2s_4s_5) \\ &= \mathrm{lcm}(2s_2s_5s_6, 2s_2s_4s_5) \\ &= 2s_2s_5\mathrm{lcm}(s_6, s_4),\end{aligned}$$

where we have used $ts_3 = 2s_5s_6$ in the second line. Lastly, s_6 is prime to s_2s_4 so $\mathrm{lcm}(s_4, s_6) = s_4s_6$. We get

$$\begin{aligned}\mathrm{lcm}(o(c_\alpha), o(c_\beta)) &= 2s_2s_5s_6s_4 \\ &= 2s_2(ts_3/2)s_4 \\ &= ts_2(s_3s_4) \\ &= ts_2s_1 = t2^{e-f}A_3,\end{aligned}$$

as desired.

Case 1B Now we suppose that s_1 is even and so $o(y^2) = ts_1/4$. We compute as in Case 1A:

$$\begin{aligned}(o(c_\alpha), o(y^2)) &= ts_3/4 \\ o(c_\beta) &= s_4(4s_2)s_5, \quad \text{with} \quad ts_3 = s_5s_6, (s_6, 4s_2s_4) = 1 \\ \mathrm{lcm}(o(c_\alpha), o(c_\beta)) &= 4s_2s_5s_6s_4 \\ &= 2^{e-f}A_3t.\end{aligned}$$

This completes Case 1.

Case 2 Now suppose that $t \equiv 0 \pmod 4$. Here $o(y) = ts_1$ and $o(y^2) = ts_1/2$ as t is even. Compute as in Case 1A to get $\mathrm{lcm}(o(c_\alpha), o(c_\beta))2^{e-f}A_3t$. This completes Part I.

Part II Now we consider the case where $2^f t_2$ is odd. Note that $f = 0$ here and, from $2A = t_2A_3$, that A_3 is even, $A_3/2$ is odd. The proof is similar to the previous cases. We have $c_\alpha^2 = xy$ where $o(x) = 2^eA_3$ and $o(-y^{2^eA_3/2}) = t$. We thus have from Lemma 8.2

$$o(y^{2^eA_3/2}) = \begin{cases} t/2 & \text{if } t \equiv 2 \pmod 4 \\ t, & \text{if } t \equiv 0 \pmod 4 \\ 2t, & \text{if } t \equiv 1, 3 \pmod 4). \end{cases}$$

There are four cases, depending on t modulo 4. The computations are all similar to Part I. We present only the first case.

Suppose $t \equiv 2 \pmod 4$. Then

$$o(y) = ts_1/2 \quad \text{with} \quad 2^e A_3/2 = s_1 s_2, (s_2, t/2) = 1,$$

by Lemma 8.3. Then

$$(0(x), o(y)) = (2^e A_3, ts_1/2) = (2s_1 s_2, ts_1/2) = s_1,$$

as s_2 is prime to $t/2$ and $t/2$ is odd. So

$$o(c_\alpha^2) = (2s_2)(t/2)s_3 \quad \text{with} \quad s_1 = s_3 s_4, (s_4, s_2 t) = 1,$$

by Lemma 8.3 again. As $s_2 t s_3$ is even, $o(c_\alpha) = 2s_2 t s_3$. Now

$$c_\beta = \frac{b^{Bt_2}}{c_\alpha} = \frac{y}{c_\alpha}.$$

We have

$$(o(c_\alpha), o(y)) = (2s_2 t s_3, ts_1/2) = (2s_2 t s_3, ts_3 s_4/2) = ts_3/2,$$

s_4 is prime to s_2 and s_4 is odd (since it is also prime to t). Applying Lemma 8.3 once again gives

$$o(c_\beta) = (4s_2)s_3 s_5 \quad \text{with} \quad ts_3/2 = s_5 s_6, (s_6, 4s_2 s_3) = 1.$$

Hence

$$\begin{aligned} \mathrm{lcm}(o(c_\alpha), o(c_\beta)) &= \mathrm{lcm}((2s_2)(2s_5 s_6), 4s_2 s_3 s_5) \\ &= 4s_2 s_5 (s_6 s_4) \\ &= 2^e A_3 t, \end{aligned}$$

as desired.

□

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] R.W. Fitzgerald, J.L. Yucas, Factors of Dickson polynomials over finite fields, to appear in Finite Fields Appl.

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

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

[10] R. Lidl and H. Niederreiter, *Finite fields,* Cambridge Univ. Press, Cambridge, 1997.

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

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

[13] 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).

[14] J. Yucas and G. Mullen, Self-reciprocal polynomials over finite fields, Des. Codes Cryptogr. 33 (2004) 275-281.

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