

2007

Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields

Robert W. Fitzgerald

Southern Illinois University Carbondale, rfitzg@math.siu.edu

Joseph L. Yucas

Southern Illinois University Carbondale

Follow this and additional works at: http://opensiuc.lib.siu.edu/math_articles

Published in *Arithmetic of Finite Fields 2007*, Lecture Notes in Computer Science, vol. 4547, Berlin: Springer, 1-10. doi:[10.1007/978-3-540-73074-3_1](https://doi.org/10.1007/978-3-540-73074-3_1). The original publication is available at www.springerlink.com

Recommended Citation

Fitzgerald, Robert W. and Yucas, Joseph L., "Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields" (2007). *Articles and Preprints*. Paper 19.

http://opensiuc.lib.siu.edu/math_articles/19

This Article is brought to you for free and open access by the Department of Mathematics at OpenSIUC. It has been accepted for inclusion in Articles and Preprints by an authorized administrator of OpenSIUC. For more information, please contact opensiuc@lib.siu.edu.

Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields

Robert W. Fitzgerald and Joseph L. Yucas

Southern Illinois University Carbondale

Abstract. We give, over a finite field F_q , explicit factorizations into a product of irreducible polynomials, of the cyclotomic polynomials of order $3 \cdot 2^n$, the Dickson polynomials of the first kind of order $3 \cdot 2^n$ and the Dickson polynomials of the second kind of order $3 \cdot 2^n - 1$.

KEYWORDS: finite field, cyclotomic polynomial, Dickson polynomial

1 Introduction

Explicit factorizations, into a product of irreducible polynomials, over F_q of the cyclotomic polynomials $Q_{2^n}(x)$ are given in [4] when $q \equiv 1 \pmod{4}$. The case $q \equiv 3 \pmod{4}$ is done in [5]. Here we give factorizations of $Q_{2^n r}(x)$ where r is prime and $q \equiv \pm 1 \pmod{r}$. In particular, this covers $Q_{2^n 3}(x)$ for all F_q of characteristic not 2, 3. We apply this to get explicit factorizations of the first and second kind Dickson polynomials of order $2^n 3$ and $2^n 3 - 1$ respectively.

Explicit factorizations of certain Dickson polynomials have been used to compute Brewer sums [1]. But our basic motivation is curiosity, to see what factors arise. Of interest then is how the generalized Dickson polynomials $D_n(x, b)$ arise in the factors of the cyclotomic polynomials and how the Dickson polynomials of the first kind appear in the factors of both kinds of Dickson polynomials.

Let q be a power of an odd prime and let $v_2(k)$ denote the highest power of 2 dividing k . We will only consider the case where r is prime and $q \equiv \pm 1 \pmod{r}$. We recall the general form of the factors of cyclotomic polynomials in this case (see [4] 3.35 and 2.47).

Proposition 1. *Let $L = v_2(q^2 - 1)$, and work over F_q .*

1. *Suppose $q \equiv 1 \pmod{r}$. Then:*
 - (a) *For $0 \leq n \leq v_2(q - 1)$, $Q_{2^n r}(x)$ is a product of linear factors.*
 - (b) *For $v_2(q - 1) < n \leq L$, $Q_{2^n r}(x)$ is a product of irreducible quadratic polynomials.*
 - (c) *For $n > L$, $Q_{2^n r}(x) = \prod f_i(x^{2^{n-L}})$, where $Q_{2^L r}(x) = \prod f_i(x)$.*
2. *Suppose $q \equiv -1 \pmod{r}$. Then:*
 - (a) *For $0 \leq n \leq L$, $Q_{2^n r}(x)$ is a product of irreducible quadratic factors.*
 - (b) *For $n > L$, $Q_{2^n r}(x) = \prod f_i(x^{2^{n-L}})$, where $Q_{2^L r}(x) = \prod f_i(x)$.*

2 Factors of cyclotomic polynomials

As before, $L = v_2(q^2 - 1)$ and $r = 2s + 1$ be a prime. Let $\Omega(k)$ denote the primitive k th roots of unity in F_{q^2} .

We will often use the following, which is equation 7.10 in [4]. For $m \geq 0$

$$D_{2m}(x, c) = D_m(x^2 - 2c, c^2).$$

Lemma 1. *Suppose $q \equiv -1 \pmod{r}$. Let N denote the norm $F_{q^2} \rightarrow F_q$.*

1. *If $q \equiv 3 \pmod{4}$ and $\rho \in \Omega(2^n)$, for $n \leq L$, then*

$$N(\rho) = \begin{cases} 1, & \text{if } 2 \leq n < L \\ -1, & \text{if } n = L. \end{cases}$$

2. *If $\omega \in \Omega(r)$ then $N(\omega) = 1$.*

3. *If $\alpha \in F_{q^2}$ and $N(\alpha) = a$ then $\alpha + a/\alpha \in F_q$.*

Proof. (1) Since $q - 1 \equiv 2 \pmod{4}$, $L - 1$ is the highest power of 2 dividing $q + 1$. Let $\rho \in \Omega(2^L)$. Now $N(\rho) = \rho^{q+1}$ so that $N(\rho)^2 = \rho^{2(q+1)} = 1$ and $N(\rho) = \pm 1$. If $N(\rho) = 1$ then $\rho^{q+1} = 1$ and $2^L = o(\rho)$ divides $q + 1$, a contradiction. Hence $N(\rho) = -1$. If $\omega \in \Omega(2^n)$ for $n < L$, then ω is an even power of ρ and so $N(\omega) = 1$.

(2) $N(\omega)^r = N(\omega^r) = 1$ and, as r is prime, the only r th root of unity in F_q is 1. So $N(\omega) = 1$.

(3) We have $\alpha\alpha^q = a$ so that $\alpha + a/\alpha = \text{tr}(\alpha) \in F_q$. □

Theorem 1. 1. *Suppose $q \equiv -1 \pmod{r}$ and $q \equiv 3 \pmod{4}$.*

(a) $Q_r(x) = \prod_{a \in S_1} (x^2 - ax + 1)$ and $Q_{2r}(x) = \prod_{a \in S_1} (x^2 + ax + 1)$, where S_1 is the set of roots of $1 + \sum_{i=1}^s D_i(x, 1)$

(b) For $2 \leq n < L$, $Q_{2^n r}(x) = \prod_{a \in S_n} (x^2 + ax + 1)$, where S_n is the set of roots of $1 + \sum_{i=1}^s (-1)^s D_{2^{n-1}i}(x, 1)$.

(c) For $n \geq L$, $Q_{2^n r}(x) = \prod_{b \in T_L} (x^{2^{n-L+1}} + bx^{2^{n-L}} - 1)$, where T_L is the set of roots of $1 + \sum_{i=1}^s (-1)^s D_{2^{L-1}i}(x, -1)$.

2. *Suppose $q \equiv -1 \pmod{r}$ and $q \equiv 1 \pmod{4}$.*

(a) $Q_r(x) = \prod_{a \in S_1} (x^2 - ax + 1)$ and $Q_{2r}(x) = \prod_{a \in S_1} (x^2 + ax + 1)$.

(b) For $2 \leq n \leq L$,

$$Q_{2^n r}(x) = \prod_{\rho \in \Omega(2^{n-1})} \prod_{b \in T(\rho)} (x^2 + bx + \rho),$$

where $T(\rho)$ is the set of roots in F_q of $1 + \sum_{i=1}^s (-1)^i D_{2^{n-1}i}(x, \rho)$.

(c) For $n > L$, $Q_{2^n r}(x) = \prod_{\rho \in \Omega(2^{L-1})} \prod_{b \in T(\rho)} (x^{2^{n-L+1}} + bx^{2^{n-L}} + \rho)$.

3. *Suppose $q \equiv 1 \pmod{r}$ and $q \equiv 3 \pmod{4}$.*

(a) $Q_r(x) = \prod(x - \omega)$, $Q_{2r}(x) = \prod(x + \omega)$ and $Q_{4r}(x) = \prod(x^2 + \omega)$, with each product over $\Omega(r)$.

(b) For $3 \leq n < L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{c \in U_n} (x^2 + c\omega x + \omega^2)$$

where U_n is the set of roots in F_q of $D_{2^{n-2}}(x, 1)$.

(c) For $n \geq L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{d \in V_L} (x^{2^{n-L+1}} + d\omega x - \omega^2)$$

where V_L is the set of roots in F_q of $D_{2^{L-2}}(x, -1)$.

4. Suppose $q \equiv 1 \pmod{r}$ and $q \equiv 1 \pmod{4}$.

(a) $Q_r(x) = \prod_{\omega \in \Omega(r)} (x - \omega)$.

(b) For $1 \leq n < L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{\rho \in \Omega(2^n)} (x + \omega\rho)$$

(c) For $n \geq L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{\rho \in \Omega(2^{L-1})} (x^{2^{n-L+1}} + \omega\rho).$$

Proof. (1) If $\omega \in \Omega(r)$ then $N(\omega) = 1$ and $\omega + 1/\omega \in F_q$ by Lemma 1. So

$$Q_r(x) = \prod_{\omega \in \Omega(r)} (x - \omega) = \prod (x^2 - ax + 1),$$

is a factorization over F_q , where a runs over all distinct $\omega + \omega^{-1}$. The quadratic factors are irreducible by Corollary 1. Also,

$$\begin{aligned} 1 + \sum_{i=1}^s D_i(a, 1) &= 1 + \sum_{i=1}^s (\omega^i + \omega^{-i}) \\ &= \omega^{-s} \left(\sum_{j=0}^{2s} \omega^j \right) = 0. \end{aligned}$$

As $\deg(1 + \sum D_i(x, 1)) = s$, the a are all of the roots. Further,

$$Q_{2r}(x) = Q_r(-x) = \prod (x^2 + ax + 1),$$

which completes the proof of (1)(a).

For (1)(b), the case $n = 2$ can be checked directly. So suppose $3 \leq n < L$. Note that $a_2 = \rho\omega + (\rho\omega)^{-1}$ as $\rho^{-1} = -\rho$. Let $\rho_n \in \Omega(2^n)$ and set $a_n = \rho\rho_n\omega + (\rho\rho_n\omega)^{-1}$. We claim that $a_n \in F_q$ and that $a_n^2 = 2 - a_{n-1}$ (with a_{n-1}

defined via a different choice of ω). Namely, $N(\rho\rho_n\omega) = 1$ as $n < L$ and so $a_n \in F_q$. And

$$\begin{aligned} a_n^2 &= \rho^2 \rho_n^2 \omega^2 + (\rho^2 \rho_n^2 \omega^2)^{-1} + 2 \\ &= -\rho_{n-1} \omega^2 - (\rho_{n-1} \omega^2)^{-1} + 2 = 2 - a_{n-1}. \end{aligned}$$

Then inductively,

$$Q_{2^n r}(x) = \prod (x^4 + a_{n-1}x^2 + 1) = \prod (x^2 + a_n x + 1)(x^2 - a_n x + 1),$$

where again the quadratic factors are irreducible over F_q . Lastly, again by induction, the a_n are roots of

$$1 + \sum_{i=1}^s (-1)^i D_{2^{n-2}i}(-(x^2 - 2), 1) = 1 + \sum_{i=1}^s (-1)^i D_{2^{n-1}i}(x, 1).$$

This has degree $2^{n-1}s$ and there are $2^{n-1}s = \frac{1}{2} \deg Q_{2^n r}(x)$ many a_n 's. So the a_n 's are all of the roots of the above polynomial.

We finish the proof of (1) by checking the case $n = L$ (the cases $n > L$ then follow from Corollary 1). Now $N(\rho\rho_L\omega) = -1$ by Lemma 1, so that $b = \rho\rho_L\omega - (\rho\rho_L\omega)^{-1} \in F_q$. And $b^2 = -a_{L-1} - 2$. Hence

$$x^4 + a_{L-1}x^2 + 1 = (x^2 + bx - 1)(x^2 - bx - 1)$$

is an irreducible factorization over F_q . Lastly, b is a root of

$$1 + \sum_{i=1}^s (-1)^i D_{2^{L-2}i}(-(x^2 + 2), 1) = 1 + \sum_{i=1}^s (-1)^i D_{2^{L-1}i}(x, -1).$$

As before, the b 's are all of the roots.

(2) First note that $L = v_2(q-1) + 1$ so that $\Omega(2^n) \subset F_q$ for $n < L$. The factorization of $Q_r(x)$ and $Q_{2^n r}(x)$ is the same as in (1). For (2)(b), again the case $n = 2$ can be checked directly. For $2 < n < L$ we work by induction. Set $b_n = \rho_n(\omega + \omega^{-1})$, for $\rho_n \in \Omega(2^n)$. Then $b_n \in F_q$ and $b_n^2 = b_{n-1} + 2\rho_{n-1}$. Note that the set of b_{n-1} 's is closed under multiplication by -1 . Hence we need only check that

$$x^4 - a_{n-1}x^2 + \rho_{n-1} = (x^2 + b_n x + \rho_n)(x^2 - b_n x + \rho_n).$$

Further, b_n is a root of

$$1 + \sum_{i=1}^s (-1)^i D_{2^{n-2}i}(x^2 - 2\rho_{n-1}, \rho_{n-2}) = 1 + \sum_{i=1}^s (-1)^i D_{2^{n-1}i}(x, \rho_{n-1}).$$

Set $\delta_{\rho_{n-1}}(x) = 1 + \sum_{i=1}^s (-1)^i D_{2^{n-1}i}(x, \rho_{n-1})$. Fix a ρ_{n-1} and pick a ρ_n with $\rho_n^2 = \rho_{n-1}$. To complete the proof of (2)(b) we need to check that the b_n 's are all of the roots of $\delta_{\rho_{n-1}}(x)$ in F_q .

For $n = 2$, $\deg \delta_{\rho_1} = 2s$ which is the number of b_2 's so δ_{ρ_1} has no other roots. Inductively assume that

$$\delta_{\rho_{n-1}}(x) = \prod (x - b_n) \cdot h(x),$$

where $h(x)$ is a product of non-linear factors. Then

$$\delta_{\rho_n}(x) = \delta_{r h \circ \rho_{n-1}}(x^2 - 2\rho_n) = \prod (x^2 - 2\rho_n - b_n) \cdot h(x^2 - 2\rho_n).$$

Now $x^2 - 2\rho_n - b_n$ splits in F_q iff $2\rho_n + b_n$ is a square in F_q . The b_n 's in $T(\rho_n)$ are $\pm\rho_n(\omega + \omega^{-1})$. And $2\rho_n + \rho_n(\omega + \omega^{-1}) = \rho_n(\omega^r + \omega^{-r})^2$ is a square (in fact, the square of a b_{n+1}) while $2\rho_n - \rho_n(\omega + \omega^{-1}) = -\rho_n(\omega^r - \omega^{-r})^2$ is not a square (as $\omega^r - \omega^{-r} \notin F_q^2$). Hence the roots of δ_{ρ_n} in F_q are precisely the b_{n+1} 's.

(2)(c) The case $n = L$ must be done separately as $\rho_L \notin F_q$. Set $b_L = \rho\rho_L(\omega - \omega^{-1})$. As in the proof of (a), $(\omega - \omega^{-1})^2 \in F_q \setminus F_q^2$. And $\rho_{L-1} \in F_q \setminus F_q^2$. Hence $\rho_{L-1}(\omega - \omega^{-1})^2 \in F_q^2$ and its square root, b_L , is in F_q . Also $b_L^2 = -b_{L-1} + 2\rho_{L-1}$. Then

$$x^4 + b_{L-1}x^2 + \rho_{L-2} = (x^2 + b_Lx + \rho_{L-1})(x^2 - b_Lx + \rho_{L-1}),$$

giving the desired factorization. Further, $b_{L-1} = -b_L^2 + 2\rho_{L-1}$ so that b_L is a root of

$$1 + \sum_{i=1}^s (-1)^i D_{2L-2i}(-(x^2 - 2\rho_{L-1}), \rho_{L-2}) = 1 + \sum_{i=1}^s (-1)^i D_{2L-1i}(x, \rho_{L-1}).$$

As before, these are all of the roots in F_q . Finally, the cases $n > L$ follow from Corollary 1.

(3) As $q \equiv 1 \pmod{r}$, we have $\Omega(r) \subset F_q$. The factorizations for Q_r and Q_{2r} are clear and that of Q_{4r} follows from Corollary 1. We do the case $n = 3 < L$ (the case $n = 3 = L$ will follow from the case $n = L$ to be done later). Let $\rho_3 \in \Omega(2^3)$. Then $\rho_3 \in F_{q^2} \setminus F_q$, $N(\rho_3) = 1$ as $n < L$, and $c_3 = \rho_3 + \rho_3^{-1} \in F_q$. Also $c_3^2 = \rho + \rho^{-1} + 2 = 2$. A typical factor of Q_{4r} can be written as $x^2 + \omega^4$ and we have

$$x^4 + \omega^4 = (x^2 + c_2\omega x + \omega^2)(x^2 - c_2\omega x + \omega^2),$$

giving the desired factorization of $Q_{2^3r}(x)$. Note that $c_3 = \pm\sqrt{2}$, the roots of $D_2(x, 1) = x^2 - 2$.

Now suppose $3 < n < L$ and work inductively. We have $N(\rho_n) = 1$ so that $c_n = \rho_n + \rho_n^{-1} \in F_q$. And $c_n^2 = c_{n-1} + 2$. A typical factor of $Q_{2^{n-1}r}(x)$ can be written as $x^2 - c_{n-1}\omega^2 x + \omega^4$ and we have

$$x^4 - c_{n-1}\omega^2 x^2 + \omega^4 = (x^2 + c_n\omega x + \omega^2)(x^2 - c_n\omega x + \omega^2),$$

giving the desired factorization. Further, c_n is a root of $D_{2^{n-3}}(x^2 - 2, 1) = D_{2^{n-2}}(x, 1)$. A counting argument shows the c_n 's are all of the roots.

Next suppose $n = L$. We have $N(\rho_L) = -1$ so that $c_L = \rho_L - \rho_L^{-1} \in F_q$. And $c_L^2 = c_{L-1} - 2$. Then

$$x^4 - c_{L-1}\omega^2x^2 + \omega^4 = (x^2 + c_L\omega x - \omega^2)(x^2 - c_L\omega x - \omega^2),$$

giving the desired factorization. Further, The c_L 's are all of the roots of $D_{2^{L-3}}(x^2 + 2, 1) = D_{2^{L-2}}(x, -1)$. The cases $n > L$ follow from Corollary 1.

(4) Note that $L = v_2(q-1) + 1$. Hence here $\Omega(r), \Omega(2^n) \subset F_q$, for $n < L$. The factorizations of $Q_{2^n r}(x)$ for $n < L$ are clear and the rest follows from Corollary 1. □

3 Cyclotomic polynomials in the case $r = 3$

We work out the case $r = 3$ (so that all F_q not of characteristic 2, 3 are covered). By way of comparison, we first recall the result for $r = 1$. L continues to denote $v_2(q^2 - 1)$.

Proposition 2. *The following are factorizations.*

1. If $q \equiv 1 \pmod{4}$ then
 - (a) For $1 \leq n < L$, $Q_{2^n}(x) = \prod(x + a)$, where a runs over all primitive 2^n roots of unity.
 - (b) For $n \geq L$, $Q_{2^n}(x) = \prod(x^{2^{n-L+1}} + a)$, where a runs over all primitive 2^{L-1} roots of unity.
2. If $q \equiv 3 \pmod{4}$ then
 - (a) For $2 \leq n < L$, $Q_{2^n}(x) = \prod(x^2 + ux + 1)$ where u runs over all roots of $D_{2^{n-2}}(x, 1)$.
 - (b) For $n \geq L$, $Q_{2^n}(x) = \prod(x^{2^{n-L+1}} + vx^{2^{n-L}} - 1)$, where v runs over all roots of $D_{2^{L-2}}(x, -1)$.

Proof. Statement (1) is from [4]. Statement (2) is by Meyn [5]. □

Proposition 3. *The following are factorizations.*

1. If $q \equiv 1 \pmod{12}$ then let $u, v \in F_q$ be the primitive cube roots of unity.
 - (a) $Q_3(x) = (x - u)(x - v)$.
 - (b) For $1 \leq n < L$, $Q_{2^n 3}(x) = \prod(x + u\rho)(x + v\rho)$, where $\rho \in \Omega(2^n)$.
 - (c) For $n \geq L$, $Q_{2^n 3}(x) = \prod(x^{2^{n-L+1}} + u\rho)(x^{2^{n-L+1}} + v\rho)$, where $\rho \in \Omega(2^L)$.
2. If $q \equiv 5 \pmod{12}$ then
 - (a) $Q_3(x) = x^2 + x + 1$ and $Q_6(x) = x^2 - x + 1$ are irreducible.
 - (b) For $2 \leq n \leq L$, $Q_{2^n 3}(x) = \prod(x^2 + cx + \rho_{n-1})$, where $\rho_{n-1} \in \Omega(2^{n-1})$ and for each ρ_{n-1} , the c 's run over all the solutions to $D_{2^{n-1}}(x, \rho_{n-1}) = 1$.
 - (c) For $n > L$, $Q_{2^n 3}(x) = \prod(x^{2^{n-L+1}} + cx^{2^{n-L}} + \rho_{L-1})$, with ρ_{L-1} and c as before.

3. If $q \equiv 7 \pmod{12}$ then again let $u, v \in F_q$ be the primitive cube roots of unity.
- (a) $Q_3(x) = (x - u)(x - v)$, $Q_6(x) = (x + u)(x + v)$ and $Q_{12}(x) = (x^2 + u)(x^2 + v)$.
 - (b) For $3 \leq n < L$, $Q_{2^n 3}(x) = \prod (x^2 + cux + v)(x^2 + cvx + u)$, where c runs over the roots of $D_{2^{n-2}}(x, 1)$.
 - (c) For $n \geq L$, $Q_{2^n 3}(x) = \prod (x^{2^{n-L+1}} + dux^{2^{n-L}} - v)(x^{2^{n-L+1}} + dvx^{2^{n-L}} - u)$, where d runs over the roots of $D_{2^{L-2}}(x, -1)$.
4. If $q \equiv 11 \pmod{12}$ then
- (a) $Q_3(x) = x^2 + x + 1$ and $Q_6(x) = x^2 - x + 1$ are irreducible.
 - (b) For $2 \leq n < L$, $Q_{2^n 3}(x) = \prod (x^2 + ax + 1)$, where the a 's run over all solutions to $D_{2^{n-1}}(x, 1) = 1$.
 - (c) For $n \geq L$, $Q_{2^n 3}(x) = \prod (x^{2^{n-L+1}} + bx^{2^{n-L}} - 1)$, where the b 's run over all solutions to $D_{2^{L-1}}(x, -1) = 1$.

4 Factors of Dickson polynomials

The results here for the Dickson polynomials of the first kind are a re-formulation of results in [2]. The results for the Dickson polynomials of the second kind are new. We have included the first kind results to illustrate how the approach taken here covers the two kinds simultaneously.

Recall that the factorization of $x^t + 1$ is

$$x^t + 1 = \prod_{\substack{d|t \\ t/d \text{ odd}}} Q_{2d}(x).$$

The following generalization is standard.

Proposition 4.

$$\sum_{i=0}^{w-1} x^{it} = \prod_{\substack{d|t, 1 \neq s|w \\ (s, t/d)=1}} Q_{ds}(x).$$

We review the transformations of [2]. Let P_n be the collection of all polynomials over a field F of degree n and let S_n denote the family of all self-reciprocal polynomials over F of degree n . Define

$$\begin{aligned} \Phi : P_n &\rightarrow S_{2n} && \text{by} \\ f(x) &\mapsto x^n f(x + x^{-1}), \end{aligned}$$

where $n = \deg f$.

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

$$\begin{aligned} \Psi : S_{2n} &\rightarrow P_n \quad \text{by} \\ b(x) &\mapsto \sum_{i=0}^{n-1} b_i D_{n-i}(x) + b_n. \end{aligned}$$

Φ and Ψ are multiplicative inverses (this was proved only for finite fields in [2], Theorem 3, and for arbitrary fields in [3], Theorem 6.1). We write $D_n(x)$ for $D_n(x, 1)$ and $E_n(x)$ for the n th order Dickson polynomial of the second kind.

Proposition 5. *Write $n = 2^k m$ with m odd. Then:*

$$\begin{aligned} \Phi(D_n(x)) &= \prod_{e|m} Q_{2^{k+2}e}(x) \\ \Phi(E_{n-1}(x)) &= \prod_{e|m} \prod_{i=0}^{k+1} Q_{2^i e}(x), \end{aligned}$$

where we exclude $e = 1, i = 0, 1$ from the second equation.

Proof. Note that by Waring's identity

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

Take $t = 2n$ and $w = 2$ (and so $s = 2$) in Lemma 4 to get the result. Similarly,

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

Take $t = 2$ and $w = n$ in Lemma 4 to get the result. □

Corollary 1. *Write $n = 2^k m$, with m odd. The factorizations over \mathbb{Q} are:*

$$\begin{aligned} D_n(x) &= \prod_{e|m} \Psi(Q_{2^{k+2}e}(x)) \\ E_{n-1} &= \prod_{e|m} \prod_{i=0}^{k+1} \Psi(Q_{2^i e}(x)), \end{aligned}$$

where we again exclude $e = 1, i = 0, 1$ from the second equation.

Proof. This follows from Proposition 5 and the properties of Φ, Ψ since each $Q_r(x)$, $r > 1$ is irreducible over \mathbb{Q} and self-reciprocal. □

5 Dickson polynomials in the case $r = 3$

We return to the case of finite fields F_q . We use the explicit factorizations of cyclotomic polynomials to get explicit factorizations of the Dickson polynomials of order $2^n r$, via Proposition 1. We begin with the case $r = 1$, where the factorizations of $Q_{2^n}(x)$ were known but the results for Dickson polynomials are new.

Proposition 6. *Set $L = v_2(q^2 - 1)$.*

1. *For $1 \leq n \leq L - 3$, $D_{2^n}(x)$ splits in F_q . For $n \geq L - 2$, we have the factorization*

$$D_{2^n}(x) = \prod (D_{2^{n-L+3}}(x) + a),$$

where a runs over all roots of $D_{2^{L-3}}(x)$.

2. *For $1 \leq n \leq L - 2$, $E_{2^{n-1}}(x)$ splits in F_q . For $n \geq L - 1$, we have the factorization*

$$E_{2^{n-1}}(x) = \prod_{i=0}^{L-3} (x + a_i) \cdot \prod_{i=1}^{n-L+2} (D_{2^i}(x) + a_{L-3}),$$

where a_i runs over all the roots of $D_{2^i}(x)$.

We note that, when $L = 3$, the statement (1) means that $D_{2^n}(x)$ is irreducible over F_q for $n \geq 1$.

Theorem 2. *Set $L = v_2(q^2 - 1)$.*

1. *Suppose $q \equiv \pm 1 \pmod{12}$. For $0 \leq n \leq L - 3$, $D_{2^{n+3}}(x)$ splits in F_q . For $n \geq L - 2$, we have the factorization*

$$D_{2^{n+3}}(x) = \prod (D_{2^{n-L+3}}(x) + a),$$

where a runs over all the roots of $D_{2^{L-3}}(x)$.

2. *Suppose $q \equiv \pm 5 \pmod{12}$. The following are factorizations.*
 - (a) *For $0 \leq n \leq L - 3$,*

$$D_{2^{n+3}}(x) = \prod (D_1(x) + a)(D_2(x) + aD_1(x) + (a^2 - 1)),$$

where a runs over all the roots of $D_{2^n}(x)$.

- (b) *For $n \geq L - 2$,*

$$D_{2^{n+3}}(x) = \prod (D_{2^{n-L+3}}(x) + b)(D_{2^{n-L+3}}(x) + uD_{2^{n-L+2}}(x) + (b + 3)),$$

where b runs over roots of $D_{2^{L-3}}(x)$ and $u^2 = 3b + 6$.

Proof. The proof is a tedious computation. Take each factor of the appropriate cyclotomic polynomial, pair it with its reciprocal and then apply Ψ . We note that in Case 2, $3 \notin F_q^{*2}$. And $b+2 \notin F_q^{*2}$ since otherwise $\sqrt{b+2}$ is a root in F_q of $D_{2^L-3}(x^2-2) = D_{2^L-2}(x)$, contradicting Proposition 6. Thus $3b+6$ has square roots u in F_q . □

The factorizations of $E_{2^{n3-1}}(x)$ follow from the previous result and the following identity:

Corollary 2. For $n \geq 1$

$$E_{2^{n3-1}}(x) = (x^2 - 1) \prod_{i=0}^{n-1} D_{2^{i3}}(x).$$

Proof. We use induction. For $n = 1$, Proposition 5 gives,

$$E_{2^{n3-1}}(x) = E_5(x) = \Psi(Q_4)\Psi(Q_3)\Psi(Q_6)\Psi(Q_{12}).$$

Then $Q_3 = x^2+x+1$ so $\Psi(Q_3) = x+1$, $Q_6 = x^2-x+1$ so $\Psi(Q_6) = x-1$ and, using Proposition 5 again, $\Psi(Q_4)\Psi(Q_{12}) = D_3$. So $E_{2^{n3-1}}(x) = (x^2-1)D_{2^{n-1}3}(x)$.

Proposition 5 gives:

$$\begin{aligned} E_{2^{n+1}3-1}(x) &= E_{2^{n3-1}}\Psi(Q_{2^{n+2}})\Psi(Q_{2^{n+2}3}) \\ &= E_{2^{n3-1}}D_{2^{n3}}, \end{aligned}$$

which gives the result by induction. □

References

1. Ş. Alaca, Congruences for Brewer sums, *Finite Fields Appl.* 13 (2007), 1–19.
2. R. W. Fitzgerald and J. L. Yucas, Factors of Dickson polynomials over finite fields, *Finite Fields Appl.* 11 (2005), 724–737.
3. R. W. Fitzgerald and J. L. Yucas, A generalization of Dickson polynomials via linear fractional transformations, *Int. J. Math. Comput. Sci.* 1 (2006), 391–416.
4. R. Lidl and H. Niederreiter, *Finite Fields* (second edition), *Encyclopedia of Mathematics and Its Applications*, vol 20, Cambridge University Press, Cambridge, 1997.
5. H. Meyn, Factorization of the cyclotomic polynomial $x^{2^n} + 1$ over finite fields, *Finite Fields Appl.* 2 (1996), 439–442.