Factorization of Dickson polynomials over finite fields

Nelcy Esperanza Arévalo Baquero¹ † · Fabio Enrique Brochero Martinez²

Accepted: 15 May 2021 / Published online: 2 June 2021
© Instituto de Matemática e Estatística da Universidade de São Paulo 2021

Abstract
Let \( D_n(x; a) \) and \( E_n(x; a) \) be Dickson polynomials of first and second kind respectively, where \( \mathbb{F}_q \) is a finite field with \( q \) elements. In this article we show explicitly the irreducible factors of these polynomials in the case that every prime divisor of \( n \) divides \( q - 1 \). This result generalizes the results found in (Finite Fields Appl. 3:84–96, 1997; Explicit factorization of cyclotomic and Dickson polynomials over finite fields, Springer, Berlin, 2007; Finite Fields Appl. 38:40-56, 2016; Discrete Math. 342:111618, 2019).

Keywords Irreducible polynomial · Irreducible factors · Factorization · Dickson polynomials

Mathematics subject classification Primary · 12E20 · Secondary · 11T30

1 Introduction
The Dickson polynomials \( D_n(x; a) \) over finite fields was introduce in the nineteenth century by Leonard E. Dickson as part of his PhD thesis. These polynomials have several interesting applications and properties, being mainly examples of families of permutation polynomials. Actually, the polynomials \( D_n(x; a) \in \mathbb{F}_q[x] \) are called Dickson polynomials of the first kind, to distinguish them from their variations

Communicated by Francisco Cesar Polcino Milies.

† Nelcy Esperanza Arévalo Baquero
nearevalob@unal.edu.co

Fabio Enrique Brochero Martinez
fbrocher@mat.ufmg.br

¹ Departamento de Matemática, Universidade Federal do Rio Grande do Sul UFRGS,
Porto Alegre, RS 91509-900, Brazil

² Departamento de Matemática, Universidade Federal de Minas Gerais UFMG, Belo Horizonte,
MG 31270-901, Brazil
introduced by Schur in 1923, which are now called the Dickson polynomials of the second kind $E_n(x, a) \in \mathbb{F}_q[x]$. When $a = 0$, $D_n(x;0) = x^n$ is a permutation polynomial (PP) in $\mathbb{F}_q$ if and only if $\gcd(n, q - 1) = 1$. In the case that $a \in \mathbb{F}_q^*$, it is known that the Dickson polynomial $D_n(x, a)$ induces a permutation of $\mathbb{F}_q$ if and only if $\gcd(n, a^q - 1) = 1$ (see [14, Theorem 7.16] or [13, Theorem 3.2]). This simple condition provides a very effective test for determining which polynomials $D_n(x, a)$ induce permutations of $\mathbb{F}_q$, and furthermore, once the condition is satisfied, we obtain $q - 1$ different permutations, one for each of the elements $a \in \mathbb{F}_q^*$. These polynomials have several applications and interesting properties. Indeed, with the digital advances, practical applications of permutation polynomials can be found in cryptography, combinatorial designs, error-correcting codes, as well as hardware implementation of turbo decoders, feedback shift-register, linear-feedback shift register, among other applications, as well as pure theoretical results.

In the field of complex numbers, Dickson polynomials are essentially equivalent, with a simple change of variable, to the classical Chebyshev polynomials $T_n(x)$. Actually, Dickson polynomials are sometimes referred as Chebyshev polynomials in mathematical literature. They were rediscovered by Brewer, who used certain Dickson polynomials of the first kind to calculate Brewer sums (see [1] and [4]). The Dickson polynomials are also related in some way to Kloosterman sum; in [16] Moisio proved that, if Kloosterman sum $K_q(a) \neq 0$, then the minimal polynomial $f(x)$ of $K_q(a)$ over $\mathbb{Z}$ must be a factor of $D_n(x; q) + (-1)^{n-1}$.

In recent years, these polynomials have been object of intense studies; in [13] the authors give a comprehensive survey about Dickson polynomials, including applications such as Dickson cryptosystems, Dickson pseudoprimes analogous to Carmichael numbers, etc. In particular, the problem of factorization of these polynomials has been studied by several authors. For example, in [12] Gao and Mullen studied the irreducibility of $D_n(x; a) + b$, where $n$ is odd (see also [19]). Their argument is based on a well-known irreducibility criterion for binomial $x^t - a$ over finite fields. Chou [8] and later Bhargava and Zieve [2] studied the factorization of the Dickson polynomials of the first kind on $\mathbb{F}_q$ using methods more complicated than those we use here, because even though the factorization found by Bhargava and Zieve is made in $\mathbb{F}_q$, the factors contain elements outside $\mathbb{F}_q$. Fitzgerald and Yucas [10] gave the irreducible factors of cyclotomic polynomials $Q_{3,2^n}(x)$ for all $\mathbb{F}_q$ of characteristic different to 2 and 3. They applied that result to get explicit factorization of Dickson polynomials $D_{3,2^n}(x)$ and $E_{3,2^n-1}(x)$. Tosun [17] extended the previous one by obtaining explicit factors of Dickson polynomials of the first and second kind $D_{3,2^n}(x, a)$ and $E_{3,2^n-1}(x, a)$ over $\mathbb{F}_q$, where $a$ be an arbitrary element of $\mathbb{F}_q$ odd characteristic.

In this study, we consider the problem of splitting $D_n(x; a)$ and $E_n(x; a)$ into irreducible factors over $\mathbb{F}_q^*$, where $\mathbb{F}_q$ is a finite field with $q$ elements, $n$ is a positive integer such that every prime divisor of $n$ divides $q - 1$ for Dickson polynomials of the first kind $D_n(x; a)$, and every prime divisor of $n + 1$ divide $q - 1$ for Dickson polynomials of the second kind $E_n(x; a)$. The result will be divide in several cases depending essentially on the class of $q$ modulo 4 and also if $a$ is a square in $\mathbb{F}_q$.

We observe that when $n$ is a power of 2, the condition $\text{rad}(n)|(q - 1)$ is trivial and then the results in [17] are particular case of our results.
The structure of this paper is as follows. In Sect. 2, we give a formal definition of Dickson polynomials with parameter \( a \), some useful properties of that polynomials, in particular, the \( a \)-self reciprocal property. In addition, we show without proof some results about the factorization of polynomial of the form \( x^m \pm 1 \). The factorization of Dickson polynomials of the first kind in odd characteristic is determined in Sect. 3. In Sect. 4, we give the factorization of Dickson polynomials of the second kind in odd characteristic. In Sect. 5, we provide the factorization of Dickson polynomials in even characteristic.

2 Preliminaries

Throughout this paper, \( \mathbb{F}_q \) denotes the finite field with \( q \) elements, where \( q \) is a power of a prime \( p \). For any \( a \in \mathbb{F}_q^* \), \( \text{ord}_q(a) \) denotes the order of \( a \) in the cyclic group \( \mathbb{F}_q^* \) and for each positive integer \( n \geq 2 \), \( \text{rad}(n) \) denotes the product of the prime factors that divides \( n \). The Dickson polynomials of first and second kind are defined as:

**Definition 2.1** Let \( n \geq 1 \) be an integer and \( a \in \mathbb{F}_q^* \). The polynomial \( D_n(x;a) \in \mathbb{F}_q[x] \) defined as

\[
D_n(x;a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}
\]

is called the \( n \)-th Dickson polynomial of the first kind with parameter \( a \).

**Definition 2.2** Let \( n \geq 1 \) be an integer and \( a \in \mathbb{F}_q^* \). The polynomial \( E_n(x;a) \in \mathbb{F}_q[x] \) defined as

\[
E_n(x;a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i}
\]

is called the \( n \)-th Dickson polynomial of the second kind with parameter \( a \).

The \( n \)-th Dickson polynomials \( D_n(x;a) \) and \( E_n(x;a) \) are the unique degree \( n \) polynomials satisfying the formal relations

\[
D_n\left(y + \frac{a}{y};a\right) = y^n + \frac{a^n}{y^n} \quad \text{and} \quad E_n\left(y + \frac{a}{y};a\right) = \frac{y^n - a^n}{y - a},
\]

respectively. These equalities are known as Waring’s identities.

In the case when \( a = 1 \), we denote the polynomials \( D_n(x;1) \) and \( E_n(x;1) \) as \( D_n(x) \) and \( E_n(x) \), respectively. In this case, these polynomials can be see as polynomials with integer coefficients and then \( D_{pn}(x) = (D_n(x))^p \) and \( E_{pn}(x) = (E_n(x))^p \), where \( p \) is the characteristic of the field.
The following lemma shows some interesting properties of Dickson polynomials, that will be useful in the next sections.

**Lemma 2.3** ([13], Lemma 2.6) The Dickson polynomials $D_n(x;a)$ and $E_n(x;a)$ satisfy the following properties:

(i) $D_{mn}(x;a) = D_n(D_m(x;a);a^n)$ for $m \geq 0$ and $n \geq 0$,

(ii) $D_{n^p}(x;a) = [D_n(x;a)]^{p^2}$ for $n \geq 0$, where $p$ is the characteristic of $\mathbb{F}_q$,

(iii) $b^p D_n(x;a) = D_n(bx;b^2a)$ for $n \geq 0$,

(iv) $b^p D_n(b^{-1}x;a) = D_n(x;b^2a)$ for $n \geq 0$ and $b \neq 0$.

(v) $E_n(x;a) = [E_m(x;a)]^{p^2}(x^2 - 4a)^{\frac{n}{2}}$ for $n \geq 0$ and $r \geq 0$, where $p$ is the characteristic of $\mathbb{F}_q$ and $n + 1 = (m + 1)p^r$,

(vi) $b^p E_n(x;a) = E_n(bx;b^2a)$ for $n \geq 0$,

(vii) $b^p E_n(b^{-1}x;a) = E_n(x;b^2a)$ for $n \geq 0$ and $b \neq 0$.

The following definition is borrowed from [9] and [11], that is also a possible generalization of the notion of reciprocal polynomial.

**Definition 2.4** Let $a$ be an element in $\mathbb{F}_q^*$. For each monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n$ with $f(0) \neq 0$, let define $f_a^*(x)$, the $a$-reciprocal of $f(x)$, by

$$f_a^*(x) = \frac{x^n}{f(0)} f\left(\frac{a}{x}\right).$$

In the case when $f(x) = f_a^*(x)$ we say that $f(x)$ is $a$-self-reciprocal.

It is easy to prove that $f_a^*(x)$ is a monic polynomial and if $\alpha \in \overline{\mathbb{F}_q}$ is a root of $f(x)$, then $\frac{a}{\alpha}$ is a root of $f_a^*(x)$. In addition

$$(f \cdot g)_a^*(x) = f_a^*(x) \cdot g_a^*(x) \quad \text{and} \quad (f_a^*)_a^*(x) = f(x),$$

for any $f$ and $g$ monic polynomials with $(f \cdot g)(0) \neq 0$. In particular, the polynomial $f(x)$ is irreducible in $\mathbb{F}_q[x]$ if and only if $f_a^*(x)$ is also irreducible.

**Lemma 2.5** Let $f(x)$ be an $a$-self-reciprocal polynomial of degree $n = 2m$ in $\mathbb{F}_q$. Then $f(x)$ can be write as

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

where $b_j \in \mathbb{F}_q$ for every $j = 0, 1, \ldots, m$.

**Proof** The result follows directly from comparing the coefficients of $f$ and $f_a^*$. \qed
Definition 2.6 Let $P_m$ be the family of monic polynomials of degree $m$ in $\mathbb{F}_q$ and $S_{2m,a}$ be the family of monic polynomials $a$-self-reciprocal of degree $2m$ in $\mathbb{F}_q$. For each positive integer $m$, let

$$
\Phi_a : P_m \to S_{2m,a} \quad \text{and} \quad \Psi_a : S_{2m,a} \to P_m
$$

be the applications defined as

$$
\Phi_a(f(x)) = x^m f\left(x + \frac{a}{x}\right)
$$

and

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

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

Theorem 2.7 ([11] Theorem 3.1.) Let $a$ be an element in $\mathbb{F}_q^*$ and $\Phi_a$ and $\Psi_a$ be as in Definition 2.6. Then

a) $\Phi_a \circ \Psi_a = \text{Id}_{S_{2m,a}}$ and $\Psi_a \circ \Phi_a = \text{Id}_{P_m}$.

b) $\Phi_a$ and $\Psi_a$ are multiplicative functions.

c) If $f(x)$ is a monic irreducible non-trivial $a$-self-reciprocal polynomial of degree $2m$, then $\Psi_a(f(x))$ is an irreducible polynomial. If $g(x)$ is an irreducible polynomial of degree $m$ and non $a$-self-reciprocal, then $\Psi_a(g(x)g_a^*(x))$ is irreducible.

Corollary 2.8 Let $\Phi_a$ be as in Definition 2.6. Then

$$
\Phi_a(D_n(x;a)) = x^{2n} + a^n.
$$

$$
\Phi_a(D_n(x';a)) = x'^{2n}D_n\left(x + \frac{a}{x'};a\right) = x'^n\left(x^n + \left(\frac{a}{x'}\right)^n\right) = x^{2n} + a^n.
$$

Proof

From this corollary, in order to find the irreducible factors of $D_n(x;a)$, it is enough to split the polynomial $x^{2n} + a^n$ into irreducible factors. The factorization of this last polynomial has been extensively studied (see [3, 5–7, 10]). Then we exhibit without proof some results that will be useful in the following section.

Theorem 2.9 ([5] Theorem 1) Let $\mathbb{F}_q$ be a finite field and $n \in \mathbb{N}$ such that

a) $q \equiv 1 \pmod{4}$ or $8 \nmid n$,
b) \( \text{rad}(n) \) divides \( q - 1 \).

Then every irreducible factor of \( x^n - 1 \) is of the form \( x^t - a \), where \( t \) divides \( \frac{n}{\gcd(n,q-1)} \), \( a \in \mathbb{F}_q \) and \( \text{ord}_q(a) \) divides \( \gcd(\frac{n}{t}, q - 1) \).

**Theorem 2.10** ([5] Theorem 2) Let \( q \) and \( n \) such that \( q \equiv 3 \pmod{4} \), \( 8 \mid n \) and \( \text{rad}(n) \mid (q - 1) \), then every irreducible factor of \( x^n - 1 \) in \( \mathbb{F}_q[x] \) is one of the following types

i) \( x^t - a \), where \( a \in \mathbb{F}_q^* \), \( t \) divides \( \frac{n}{\gcd(n,q-1)} \) and \( \text{ord}_q(a) \) divides \( \gcd(\frac{n}{t}, q - 1) \),

ii) \( x^t - (b + b^t)x + b^{q+1} \), where \( b \in \mathbb{F}_q^2 \setminus \mathbb{F}_q^* \), \( t \) divides \( \frac{n}{\gcd(n,q-1)} \) and \( \text{ord}_q(b) \) divides \( \gcd(\frac{n}{t}, q^2 - 1) \).

### 3 Factorization of Dickson polynomials of the first kind

Throughout this section, \( q \) is a power of an odd prime, \( n \) represents a positive integer such that \( \text{rad}(n) \) divides \( q - 1 \), i.e., every prime divisor of \( n \) also divides \( q - 1 \). In the case that \( a \) is a square in \( \mathbb{F}_q^* \), we can see that, by a linear change of the variable, the factorization of \( D_n(x;\alpha) \) and \( D_n(x) \) are equivalent. In addition, the factorization of \( D_n(x) \) also depend on the class of \( q \) modulo 4. In addition, we notice that \( x \) is a factor of \( D_n(x;\alpha) \) if and only if \( n \) is odd. We divide the result in three cases.

**Theorem 3.1** Let \( a \in \mathbb{F}_q^* \) be a square in \( \mathbb{F}_q \) and assume that either \( q \equiv 1 \pmod{4} \) or \( n \) is an odd positive integer. If \( \text{rad}(n)|(q - 1) \), then every irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_q^* \), different from \( x \), is of the form \( D_t(x;\alpha) = b^t(\alpha + q^{-1}) \), where \( b^2 = a \), \( \alpha \in \mathbb{F}_q^* \) and \( t \) is a divisor of \( \frac{4n}{\gcd(4n,q-1)} \) such that the following conditions are satisfied

i) \( \alpha^{2t} = -1 \),

ii) \( \text{rad}(t) \mid \text{ord}_q(\alpha) \),

iii) \( \gcd(t, \frac{q-1}{\text{ord}_q(\alpha)}) = 1 \).

**Proof** From Lemma 2.3 item (iv), we know that \( D_n(x;\alpha) = b^tD_n(b^{-1}x;1) \) for \( n \geq 0 \) and \( b \neq 0 \). Therefore the factorization of \( D_n(x;\alpha) \) can be obtained from the factorization of \( D_n(y) \) where \( y = b^{-1}x \). In addition, by Corollary 2.8 we know that \( \Phi_1(D_n(y)) = y^{2n} + 1 \) and since \( y^{4n} - 1 = (y^{2n} - 1)(y^{2n} + 1) \), if we find the irreducible factors of \( y^{2n} - 1 \), in particular we obtain the irreducible factors of \( y^{2n} + 1 \).

It follows from Theorem 2.9 that every irreducible factor of \( y^{4n} - 1 \) is of the form \( y^t - \alpha \), where \( t \) divides \( \frac{4n}{\gcd(4n,q-1)} \) and \( \alpha \) is an appropriate element of \( \mathbb{F}_q^* \). Indeed \( y^t - \alpha \) divides \( y^{2n} + 1 \) is equivalent to \( y^{2n} \equiv -1 \pmod{y^t - \alpha} \), and therefore \( y^{2n} \equiv (y^t)^t \equiv -1 \pmod{y^t - \alpha} \). Consequently \( \alpha^{2n/t} = -1 \).
Let suppose that $f(y)$ is an irreducible factor of $D_n(y)$ and $h(y)$ be the image of $f(y)$ by the map $\Phi_t$. Hence, $h(x)$ is a factor of $x^{2n} + 1$, not necessarily irreducible in $\mathbb{F}_q[y]$. There exists an irreducible factor of the form $x' - \alpha$ that divides $h(x)$. Since $h(x)$ is self-reciprocal polynomial, it follows that the reciprocal $x' - \alpha^{-1}$ also divides $h(x)$.

At this point, we have two cases to consider.

(a) If $\alpha \neq \alpha^{-1}$, then $(y' - \alpha)(y' - \alpha^{-1}) \mid h(y)$. Since

$$ (y' - \alpha)(y' - \alpha^{-1}) = y'(y' + \frac{1}{y'} - (\alpha + \alpha^{-1})) = y'(D_t(y + \frac{1}{y'}) - (\alpha + \alpha^{-1})) $$

we get that $\Psi_1((y' - \alpha)(y' - \alpha^{-1})) = D_t(y) - (\alpha + \alpha^{-1})$ divides $f(y)$. Now, using the fact that $f(y)$ is a monic irreducible polynomial, we conclude that $f(y) = D_t(y) - (\alpha + \alpha^{-1})$. Finally, rewriting this identity using the original variable we obtain

$$ f(b^{-1}x) = D_t(b^{-1}x;1) - (\alpha + \alpha^{-1}) = b^{-1}D_t(x;a) - (\alpha + \alpha^{-1}) $$

and therefore

$$ b'f(b^{-1}x) = D_t(x;a) - b'(\alpha + \alpha^{-1}) $$

is a monic irreducible factor of $D_n(x;a)$ in $\mathbb{F}_q[x]$. (b) In the case when $\alpha = \alpha^{-1}$, we have that $\alpha = \pm 1$ and $y' - \alpha = y' \pm 1$. It is clear that this polynomial is irreducible if $t = 1$ and in this case $y \pm 1$ divides $y^{2n} + 1$, thus

$$ y^{2n} + 1 \equiv (\mp 1)^{2n} + 1 \equiv 2 \equiv 0 \pmod{y \pm 1} $$

implies that $\text{char}(\mathbb{F}_q) = 2$, which is a contradiction. In the case that $t \neq 1$, we have that $y' - 1$ is always reducible and $y' + 1$ is reducible if $t$ has an odd prime divisor. Lastly, if $t$ is a power of 2, we have to consider the following cases.

- If $q \equiv 1 \pmod{4}$, we have that $-1$ is a square in $\mathbb{F}_q$ and hence $y' + 1$ is reducible.
- If $q \equiv 3 \pmod{4}$ and $n$ is odd, since $t$ divides $2n$ it follows that $t = 2$ and $x^2 + 1$ is an irreducible factor of $x^{2n} + 1$. Therefore $\Psi_1(x^2 + 1) = x$ divides $D_n(x;1)$.

In the previous theorem, we consider the case when $a \in \mathbb{F}_q$ is a square in $\mathbb{F}_q$ and either $q \equiv 1 \pmod{4}$ or $n$ is an odd integer. In the following theorems, we use Theorem 3.1 in order to understand the complementary cases of that conditions.

**Theorem 3.2** Let $a$ be a square in $\mathbb{F}_q$, $q \equiv 3 \pmod{4}$ and $n$ an even integer such that $\text{rad}(n)|(q - 1)$. Let $b \in \mathbb{F}_q$ such that $b^2 = a$, $\alpha \in \mathbb{F}_q^*$ and $t$ be a divisor of $\frac{4n}{\gcd(4n,q^2-1)}$, such that $t$ and $\alpha$ satisfy the conditions (i), (ii) and (iii) of Theorem 3.1 in the finite field $\mathbb{F}_q$. Then every irreducible factor of $D_n(x;a)$ in $\mathbb{F}_q$ is of the following types
(a) \( D_t(x;\alpha) - b'(\alpha + \alpha^{-1}) \) when \( \alpha \in \mathbb{F}_q^* \) or \( \alpha^{q+1} = 1 \),
(b) \( (D_t(x;\alpha) - b'(\alpha + \alpha^{-1})) (D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q})) \) otherwise.

**Proof** We observe that every irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_q[x] \) is also a factor, not necessarily irreducible, in \( \mathbb{F}_{q^2}[x] \). Consequently, at first we consider the Dickson polynomial \( D_n(x;\alpha) \) as a polynomial in \( \mathbb{F}_{q^2}[x] \). Since \( q^2 \equiv 1 \pmod{4} \), by Theorem 3.1, every irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_{q^2}[x] \) is of the form \( D_t(x;\alpha) - b'(\alpha + \alpha^{-1}) \) \( \in \mathbb{F}_{q^2}[x] \).

Some of these factors are also in \( \mathbb{F}_q[x] \), but that happens when \( \alpha + \alpha^{-1} \in \mathbb{F}_q \). This condition is equivalent to \( \alpha + \alpha^{-1} = (\alpha + \alpha^{-1})^q \) and that equation is equivalent to \( (\alpha^{q+1} - 1)(\alpha^{q-1} - 1) = 0 \). Therefore \( \alpha \in \mathbb{F}_q^* \) or \( \alpha^{q+1} = 1 \).

In the case when none of these conditions are satisfied, \( D_t(x;\alpha) - b'(\alpha + \alpha^{-1}) \in \mathbb{F}_q[x] \) is a factor of \( D_n(x;\alpha) \), that is not in \( \mathbb{F}_q[x] \). From the fact that the coefficients of \( D_n(x;\alpha) \) is invariant by Frobenius automorphism

\[
\tau : \mathbb{F}_q^* \rightarrow \mathbb{F}_{q^2}
\]
\[
\beta \mapsto \beta^q,
\]

we conclude that \( D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q}) \) is also an irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_{q^2}[x] \). In addition, since \( \alpha + \alpha^{-1} \neq \alpha^q + \alpha^{-q} \), we conclude that \( (D_t(x;\alpha) - b'(\alpha + \alpha^{-1})) (D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q})) \) is a factor of \( D_n(x;\alpha) \).

Finally, the coefficients of \( (D_t(x;\alpha) - b'(\alpha + \alpha^{-1})) (D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q})) \) are invariant by \( \tau \), then

\[
(D_t(x;\alpha) - b'(\alpha + \alpha^{-1})) (D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q})) \in \mathbb{F}_q[x]
\]

is an irreducible factor of \( D_n(x;\alpha) \) in the polynomial ring \( \mathbb{F}_q[x] \).

**Theorem 3.3** Let \( a \in \mathbb{F}_q \) be a non-square in \( \mathbb{F}_q \), \( b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \) such that \( b^2 = a \) and \( n \) be a positive integer such that \( \text{rad}(n)(q-1) \). Let \( \alpha \in \mathbb{F}_q^* \) and \( t \) be a divisor of \( \frac{4n}{\gcd(4n,q^2-1)} \) satisfied the conditions (i), (ii) and (iii) of Theorem 3.1 in the field \( \mathbb{F}_{q^2} \). Then every irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_q \) is one of the following types

(a) \( D_t(x;\alpha) - b'(\alpha + \alpha^{-1}) \) when \( t \) is even and either \( \alpha \in \mathbb{F}_q^* \) or \( \alpha^{q+1} = 1 \), or \( t \) is odd and either \( \alpha^{q-1} = -1 \) or \( \alpha^{q+1} = -1 \),
(b) \( (D_t(x;\alpha) - b'(\alpha + \alpha^{-1})) (D_t(x;\alpha) - b'(\alpha^q + \alpha^{-q})) \) otherwise.

**Proof** As in the previous theorem, we consider the Dickson polynomial \( D_n(x;\alpha) \) as a polynomial in \( \mathbb{F}_{q^2}[x] \). We have that \( q^2 \equiv 1 \pmod{4} \) and \( a \) is a square in \( \mathbb{F}_{q^2} \). It follows from Theorem 3.1 that every irreducible factor of \( D_n(x;\alpha) \) in \( \mathbb{F}_{q^2}[x] \) is of the form \( D_t(x;\alpha) - b'(\alpha + \alpha^{-1}) \in \mathbb{F}_{q^2}[x] \).

At this point, we need to determine which factors are in \( \mathbb{F}_q[x] \). Since \( D_t(x;\alpha) \in \mathbb{F}_q[x] \), we need to find conditions in order that \( b'(\alpha + \alpha^{-1}) \in \mathbb{F}_q \), which is equivalent to \( b'(\alpha + \alpha^{-1}) = b'(\alpha^q + \alpha^{-q}) \). This equation can be rewritten as \( b'(\alpha^q + \alpha^{-q}) = \alpha + \alpha^{-1} \).

\( \square \) Springer
Since $a$ is not a square in $\mathbb{F}_q$ then $b^{q-1} = \left( b^2 \right)^{\frac{q-1}{2}} = a^{\frac{q-1}{2}} = -1$. Now, we have two cases to consider.

(a) If $t$ is even, $b^{q(q-1)}(a^q + a^{-q}) = a + a^{-1}$ if and only if $a^q + a^{-q} = a + a^{-1}$, and hence $a \in \mathbb{F}_q^*$ or $a^{q+1} = 1$.

(b) If $t$ is odd, $b^{q(q-1)}(a^q + a^{-q}) = a + a^{-1}$ if and only if $-a^q - a^{-q} = a + a^{-1}$, that is equivalent to $(a^{q-1} + 1)(a^{q+1} + 1) = 0$.

Finally, in the case when none of the conditions are satisfied, the factor $D_t(x; a) - b'(a + a^{-1}) \in \mathbb{F}_q[x]$ of $D_n(x; a)$ is not in $\mathbb{F}_q[x]$. Applying Frobenius automorphism on that polynomial we also conclude that $D_t(x; a) - b''(a^q + a^{-q})$ is an irreducible factor of $D_n(x; a)$ in $\mathbb{F}_q[x]$ and

$$
\left( D_t(x; a) - b'(a + a^{-1}) \right) \left( D_t(x; a) - b''(a^q + a^{-q}) \right)
$$

is an irreducible factor of $D_n(x; a)$ in $\mathbb{F}_q[x]$.

\[ \square \]

4 Dickson polynomials of the second kind

Throughout this section, $n$ represents a positive integer such that $\text{rad}(n + 1)$ divides $q - 1$, i.e., every prime divisor of $n + 1$ also divides $q - 1$.

Lemma 4.1 Let $\Phi_a$ be the function defined at 2.6. Then

$$
\Phi_a(E_n(x; a)) = \frac{x^{2(n+1)} - a^{n+1}}{x^2 - a}.
$$

Proof Applying Waring’s identity on $E_n$, we have

$$
\Phi_a(E_n(x; a)) = x^nE_n\left(x + \frac{a}{x}; a\right) = x^n\left( \frac{x^{n+1} - a^{n+1}}{x^{n+1}} \right) = \frac{x^{2(n+1)} - a^{n+1}}{x^2 - a},
$$

as we want to prove. \[ \square \]

Using the previous lemma and essentially the same steps of the proof of Theorems 3.1, 3.2 and 3.3, we obtain the following result, enunciated without proof.

Theorem 4.2 Let $a$ be a square in $\mathbb{F}_q^*$ with $q \equiv 1 \pmod{4}$ or $n$ an even integer. In addition, $n$ satisfies that $\text{rad}(n + 1)$ divides $q - 1$. Then every irreducible factor of $E_n(x; a)$ in $\mathbb{F}_q[x]$, different from $x$, is of the form $D_t(x; a) - b'(a + a^{-1})$, where $b^2 = a$, $a \in \mathbb{F}_q^*$ and $t$ is a divisor of $\frac{2(n+1)}{\gcd(2(n+1), q-1)}$, satisfying the following conditions.
(i) \( \alpha = \frac{2(n+1)}{r} = 1 \),
(ii) \( \text{rad}(t) \mid \text{ord}_q(\alpha) \),
(iii) \( \gcd \left( t, \frac{q-1}{\text{ord}_a(\alpha)} \right) = 1 \),
(iv) \( (\alpha, t) \not\in \{(1, 1), (1, -1)\} \).

**Theorem 4.3** Let \( a \in \mathbb{F}_q^* \) be a square in \( \mathbb{F}_q^* \) with \( q \equiv 3 \pmod{4} \) and \( n \) an odd positive integer. In addition, \( n \) satisfies that \( \text{rad}(n+1) \) divides \( q-1 \). Let \( b^2 = a, \alpha \in \mathbb{F}_q^* \) and \( t \) a divisor of \( \frac{2(n+1)}{\gcd(2(n+1), q-1)} \), satisfying the conditions (i), (ii), (iii) and (iv) of the previous theorem in the field \( \mathbb{F}_q^* \). Then every irreducible factor of \( E_n(x;a) \) in \( \mathbb{F}_q^* \), different from \( x \), is one of the following types

(a) \( D_i(x;a) - b^i(\alpha + \alpha^{-1}) \) when \( \alpha \in \mathbb{F}_q^* \) or \( \alpha^{q+1} = 1 \),
(b) \( (D_i(x;a) - b^i(\alpha + \alpha^{-1})) (D_i(x;a) - b^i(\alpha^q + \alpha^{-q})) \) otherwise.

**Theorem 4.4** Let \( a \in \mathbb{F}_q \) be a non-square in \( \mathbb{F}_q^* \) and \( n \) be an integer such that \( \text{rad}(n+1) \) divides \( q-1 \). Let \( b \in \mathbb{F}_q^* \setminus \mathbb{F}_q^* \) such that \( b^2 = a, \alpha \in \mathbb{F}_q^* \) and \( t \) be a divisor of \( 2(n+1) \), satisfying the conditions (i), (ii), (iii) and (iv) of Theorem 4.2 in \( \mathbb{F}_q^* \). Then every irreducible factor of \( E_n(x;a) \) in \( \mathbb{F}_q^* \), different from \( x \), is one of the following types

(a) \( D_i(x;a) - b^i(\alpha + \alpha^{-1}) \) then \( t \) is even and either \( \alpha \in \mathbb{F}_q^* \) or \( \alpha^{q+1} = 1 \), or \( t \) is odd and either \( \alpha^{q-1} = -1 \) or \( \alpha^{q+1} = -1 \).
(b) \( (D_i(x;a) - b^i(\alpha + \alpha^{-1})) (D_i(x;a) - b^i(\alpha^q + \alpha^{-q})) \) otherwise.

## 5 Dickson polynomial in characteristic 2

Throughout this section \( \mathbb{F}_q \) is a finite field of characteristic 2. We notice that if \( n = 2^r s \), where \( r \geq 0 \) and \( s \) is odd, then \( D_n(x) = [D_s(x)]^{2^r} \). Therefore in order to split \( D_n(x) \) into irreducible factors in \( \mathbb{F}_q[x] \), it is enough to factorize \( D_s(x) \). Hence, we assume that \( n \) is odd.

**Lemma 5.1** Let \( n = 2m + 1 \) be a positive odd integer. Then

(a) \( D_n(x) = xF_n(x)^2 \) for some polynomial \( F_n(x) \) of degree \( m \), with \( F_n(0) \neq 0 \),
(b) \( (x+1)\Phi_1(F_n(x)) = x^m + 1 \).
Proof

(a) Let define

\[ F_n(x) = \sum_{i=0}^{m} \frac{n^{-i}}{n-i} \binom{n-i}{i} m^{i}. \]

Then

\[ xF_n(x)^2 = x \left[ \sum_{i=0}^{m} \frac{n^{-i}}{n-i} \binom{n-i}{i} m^{i} \right]^2 = x \sum_{i=0}^{m} \frac{n^{-i}}{n-i} \binom{n-i}{i} m^{2i}. \]

(b) By Corollary 2.8 item (i) and Theorem 2.7 follows that

\[ x^{2n} + 1 = \Phi_1(D_n(x)) = \Phi_1(x)\Phi_1(F_n(x)^2) = (x^2 + 1)\Phi_1(F_n(x)^2). \]

Therefore \((x^n + 1)^2 = [(x + 1)\Phi_1(F_n(x))]^2. \]

\[ \square \]

Theorem 5.2 Let \( \mathbb{F}_q \) be a finite field such that \( \text{char}(\mathbb{F}_q) = 2, a \in \mathbb{F}_q^* \) and \( n \) be a positive integer such that \( \text{rad}(n)|(q-1) \). Then every irreducible factor of \( D_n(x; a) \) different from \( x \), has multiplicity 2 and is of the form \( D_n(x; a) = b^n - b(a + a^{-1}) \), where \( b^2 = a, a \in \mathbb{F}_q^* \) and \( t \) is a divisor of \( \frac{n}{\text{gcd}(n, q-1)} \), satisfying the following conditions

(i) \( a^n = 1 \),
(ii) \( \text{rad}(t) \mid \text{ord}_{q}^1(a) \),
(iii) \( \text{gcd}(t, \frac{q-1}{\text{ord}_{q}^1(a)}) = 1 \),
(iv) \( (a, t) \neq (1, 1) \).

Proof In characteristic 2, every element of \( \mathbb{F}_q \) is a square. In addition, by Lemma 2.3 and Lemma 5.1, we have that

\[ D_n(x; a) = b^n D_n(b^{-1} x) = b^n x(F_n(b^{-1} x))^2. \]

Therefore, in order to find the factorization of \( D_n(x; a) \), it is enough to find the factorization of \( F_n(x) \). On the other hand, \( \Phi_1(F_n(x)) = \frac{x^n + 1}{x + 1} \), hence from here the proof is essentially the same of Theorem 3.1. \[ \square \]

To conclude this section, we analyse the factorization of Dickson polynomials of the second kind in characteristic 2. We shall see that it is almost
the same factorization of Dickson polynomials of the first kind. Actually, if 
\( n + 1 = 2^r(s + 1) \) with \( r \geq 0 \) and \( s \) even, then 
\( E_n(x) = [E_s(x)]^{2^r}x^{2^r - 1} \). Therefore, in order to find the factors of 
\( E_n(x) \), we need to factorize \( E_s(x) \) with \( s + 1 \) odd and then we can 
assume that \( n + 1 \) is odd. Then

\[
E_n(x) = E_n\left( y + \frac{1}{y} \right) = \frac{y^{n+1} - \left( \frac{1}{y} \right)^{n+1}}{y - \frac{1}{y}} = \frac{D_{n+1}(y + \frac{1}{y})}{y + \frac{1}{y}} = \frac{D_{n+1}(x)}{x}.
\]

From Lemma 5.1 item (1), we conclude that \( E_n(x) = F_{n+1}(x)^2 \), and consequently the 
factorization of \( E_n(x,a) \) with the condition that \( \text{rad}(n + 1)|(q - 1) \) can be found using 
Theorem 5.2.

Acknowledgements This work is part of the master’s thesis of the first author and was financed in part 
by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brazil (CAPES)—Finance Code 
001.

References

1. Alaca, S.: Congruences for Brewer sums. Finite Fields Appl. 13, 1–19 (2007)
2. Bhargava, M., Zieve, M.: Factoring Dickson polynomials over finite fields. Finite Fields Appl. 5, 
103–111 (1999)
3. Blake, I.F., Gao, S., Mullin, R.C.: Explicit factorization of \( x^{2^k} + 1 \) over \( \mathbb{F}_p \) with \( p \equiv 3 \) (mod4). Appl. 
Algebra Engrg. Comm. Comput. 4, 89–94 (1993)
4. Brewer, B.W.: On certain character sums. Trans. Amer. Math. Soc. 99, 241–245 (1961)
5. Brochero Martínez, F.E., Giraldo Vergara, C.R., de Oliveira, L.: Explicit factorization of 
\( x^n - 1 \in \mathbb{F}_p[x] \). Des. Codes Cryptogr. 77(1), 277–286 (2015)
6. Brochero Martínez, F.E.: Reis, Lucas, Silva-Jesus, Lays, Factorization of composed polynomials 
and applications. Discrete Math. 342, (2019). DOI: j.disc.2019.111603
7. Chen, B., Li, L., Tuerhong, R.: Explicit factorization of \( x^{2^mp} - 1 \) over a finite field. Finite Fields 
Appl. 24, 95–104 (2013)
8. Chou, W.S.: The Factorization of Dickson polynomials over finite fields. Finite Fields Appl. 3, 
84–96 (1997)
9. Fitzgerald, R.W., Yucas, J.L.: Factors of Dickson polynomials over finite fields. Finite Fields Appl. 
11, 724–737 (2005)
10. Fitzgerald, R. W., Yucas, J. L.: Explicit factorization of cyclotomic and Dickson polynomials over 
finite fields. Arithmetical of Finite Fields. In: Lecture Notes in Computer Science, vol. 4547, pp. 
1–10. Springer, Berlin (2007)
11. Fitzgerald, R.W., Yucas, J.L.: Generalized reciprocals, factors of Dickson polynomials and general-
ized cyclotomic polynomials over finite fields. Finite Fields Appl. 13, 492–515 (2007)
12. Gao, S., Mullin, G.: Dickson polynomials and irreducible polynomials over finite fields. J. Number 
Theory 49, 118–132 (1994)
13. Lidl, R., Mullen, G.L., Turnwald, G.: Dickson polynomials. Pitman Monogr. Surv. Pure Appl. Math, 
Essex (1993)
14. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia Math. Appl., Vol 20, Addison-Wesley (1983)
15. Meyn, H.: Factorization of the cyclotomic polynomials \( x^n + 1 \) over finite fields. Finite Fields Appl. 
2, 439–442 (1996)
16. Moisio, M.J.: On certain values of Kloosterman sums. IEEE Trans. Inform. Theory 55, 3563–3564 
(2009)
17. Tosun, S.: Explicit factorizations of generalized Dickson polynomials of order $2^m$ via generalized cyclotomic polynomials over finite fields. Finite Fields Appl. 38, 40–56 (2016)
18. Tosun, S.: Explicit factors of generalized cyclotomic polynomials and generalized Dickson polynomials of order $2^m3$ over finite fields Discrete Math. 342, 111618 (2019) DOI: j.disc.2019.111618
19. Turnwald, G.: Reducibility of translates of Dickson polynomials. Proc. Am. Math. Soc. 126, 965–971 (1998)
20. Tuxanidy, A., Wang, Q.: Composed products and factors of cyclotomic polynomials over finite fields. Des. Codes Cryptogr. 69, 203–231 (2013)
21. Wang, L., Wang, Q.: On explicit factors of cyclotomic polynomials over finite fields. Des. Codes Cryptogr. 63(1), 87–104 (2012)

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.