Factoring Dickson polynomials over finite fields

Manjul Bhargava
Department of Mathematics, Princeton University. Princeton NJ 08544
manjul@math.princeton.edu

Michael Zieve
Department of Mathematics, University of Southern California.
Los Angeles CA 90089
zieve@math.usc.edu

Abstract

We derive the factorizations of the Dickson polynomials $D_n(X, a)$ and $E_n(X, a)$, and of the bivariate Dickson polynomials $D_n(X, a) - D_n(Y, a)$, over any finite field. Our proofs are significantly shorter and more elementary than those previously known.

1. Introduction. Let $\mathbb{F}_q$ be the field containing q elements, and let p be the characteristic of $\mathbb{F}_q$. Let n be a nonnegative integer and $a \in \mathbb{F}_q$. The Dickson polynomial of the first kind, of degree n and parameter a, is defined to be the unique polynomial $D_n(X, a) \in \mathbb{F}_q[X]$ for which $D_n(Y + (a/Y), a) = Y^n + (a/Y)^n$; the Dickson polynomial of the second kind, of degree n and parameter a, is defined to be the unique polynomial $E_n(X, a) \in \mathbb{F}_q[X]$ for which $E_n(Y + (a/Y), a) = \frac{Y^{n+1}-(a/Y)^{n+1}}{Y-(a/Y)}$. The uniqueness of these polynomials is clear; there are several ways to prove their existence, e.g. see [1] or [5, Lemma 1.1] or [4, (2.2)]. These polynomials have been extensively studied, and in fact a book has been written in their honor [4]. In this note we shall derive the factorizations of the Dickson polynomials $D_n(X, a)$ and $E_n(X, a)$, and of the bivariate Dickson polynomial $D_n(X, a) - D_n(Y, a)$, over any finite field $\mathbb{F}_q$. In each case, our strategy will be to first write down the factorization over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, then determine how to put together certain factors over $\overline{\mathbb{F}}_q$ in order to get the irreducible factors over $\mathbb{F}_q$.

The factorizations of $D_n(X, a)$ and $E_n(X, a)$ have been carried out using much lengthier methods by W.-S. Chou [2]. The purpose of this note is to exhibit a simpler approach. Our methods can also be used to provide simple proofs of various other factorization results; as an example we include the factorization of $D_n(X, a) - D_n(Y, a)$ over any finite field, which seems to be new. Previously the factorization of this polynomial over the algebraic closure of a finite field was known, due to K. S. Williams for n odd [7] and to G. Turnwald for n even [5, Prop. 1.7]; we give simpler proofs of these results as well. We are grateful to G. Turnwald for informing us that our proof of this last result is similar to an argument of S. D. Cohen and R. W. Matthews [3, p. 67].

We shall retain the notation of the first paragraph throughout this note. Also, for any $\xi \in \overline{\mathbb{F}}_q$, by $\sqrt{\xi}$ we shall mean a fixed square root of ξ in $\overline{\mathbb{F}}_q$; for any positive integer d coprime to p, we will use ζ_d to denote a primitive d-th root of unity in $\overline{\mathbb{F}}_q$.

2. The Dickson polynomial of the first kind, $D_n(X, a)$. Write $n = p^r m$ with $(p, m) = 1$. Then it follows from the functional equation of D_n that $D_n(X, a) = D_m(X, a)^{p^r}$; thus, in order to factor D_n, it suffices to factor D_m. Our first result gives the factorization of D_m over $\overline{\mathbb{F}}_q$.

Theorem 1 *For q odd,*

$$D_m(X, a) = \prod_{\substack{i=1 \\ i \text{ odd}}}^{2m-1} \left(X - \sqrt{a}\,(\zeta_{4m}^i + \zeta_{4m}^{-i})\right);$$

for q even,

$$D_m(X, a) = X \prod_{i=1}^{\frac{m-1}{2}} \left(X - \sqrt{a}\,(\zeta_m^i + \zeta_m^{-i})\right)^2.$$

Proof. Note that

$$D_m\big(Y + \frac{a}{Y}, a\big) = Y^m + (a/Y)^m = \prod_{\xi^m=-1} \big(Y - \xi \frac{a}{Y}\big);$$

in order to express the right-hand side as a function of $Y + (a/Y)$, we pair the terms corresponding to ξ and $1/\xi$, which gives

$$\left(Y - \xi\frac{a}{Y}\right)\left(Y - \frac{a}{\xi Y}\right) = Y^2 - \left(\xi + \frac{1}{\xi}\right)a + \frac{a^2}{Y^2} = \left(Y + \frac{a}{Y}\right)^2 - a\left(\sqrt{\xi} + \frac{1}{\sqrt{\xi}}\right)^2.$$

Thus, $D_m(X, a)$ is the product of monic linear factors corresponding to the $\xi \in \overline{\mathbb{F}}_q$ for which $\xi^m = -1$, where the factors corresponding to ξ and $1/\xi$ are $X \pm \sqrt{a}(\sqrt{\xi} + (1/\sqrt{\xi}))$. The result for q even follows at once; for q odd, the result follows from the fact that the numbers $\pm\sqrt{\xi}$ with $\xi^m = -1$ are precisely the numbers ζ_{4m}^i with i odd and $0 < i < 4m$. ■

For $a = 0$, the factorization of $D_m(X, a) = X^m$ is trivial; our next two results give the factorization of $D_m(X, a)$ over $\mathbb{F}_q$ when $a \neq 0$.

Theorem 2 *If q is odd and $a \neq 0$, then $D_m(X, a)$ is the product of several distinct irreducible polynomials in $\mathbb{F}_q[X]$, which occur in cliques corresponding to the divisors d of m for which m/d is odd. To each such d there correspond $\varphi(4d)/(2N_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{N_d-1} \left(X - \sqrt{a}^{q^i}\left(\zeta_{4d}^{q^i} + \zeta_{4d}^{-q^i}\right)\right)$$

for some choice of ζ_{4d}; here φ denotes Euler's totient function, k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{4d}$, and

$$N_d = \begin{cases} k_d/2 & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } k_d \equiv 2 \pmod 4 \text{ and } q^{k_d/2} \equiv 2d \pm 1 \pmod{4d}; \\ 2k_d & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } k_d \text{ is odd;} \\ k_d & \text{otherwise.} \end{cases}$$

Proof. The previous result describes the roots of $D_m(X, a)$; clearly these roots are distinct, since ξ and ξ^{-1} are the only roots of the quadratic equation $Z + Z^{-1} = \xi + \xi^{-1}$. Thus $D_m(X, a)$ is the product of its distinct monic irreducible factors over $\mathbb{F}_q$, and each such factor is the minimal polynomial over $\mathbb{F}_q$ of a root α of D_m. These roots are given by $\alpha = \sqrt{a}\,(\zeta_{4d} + \zeta_{4d}^{-1})$ where d is a divisor of m with m/d odd, and ζ_{4d} is a primitive $4d$-th root of unity. The minimal polynomial of α over $\mathbb{F}_q$ has the form $\prod_{i=0}^{N-1}(X - \alpha^{q^i})$, where N denotes the least positive integer such that $\alpha^{q^N} = \alpha$. We will show that $N = N_d$; since for fixed d there are $\varphi(4d)/2$ choices for α, the theorem follows.

We now show $N = N_d$. Note that $\left(\sqrt{a}\,(\zeta_{4d}+\zeta_{4d}^{-1})\right)^{q^s} = \sqrt{a}^{q^s}\left(\zeta_{4d}^{q^s}+\zeta_{4d}^{-q^s}\right)$; thus, N is the least positive integer s such that

$$\sqrt{a}^{q^s}\left(\zeta_{4d}^{q^s}+\zeta_{4d}^{-q^s}\right) = \sqrt{a}\left(\zeta_{4d}+\zeta_{4d}^{-1}\right). \tag{$*$}$$

If $\sqrt{a} \in \mathbb{F}_q$ or s is even, then $\sqrt{a}^{q^s} = \sqrt{a}$, so $(*)$ just asserts that $\zeta_{4d}^{q^s}+\zeta_{4d}^{-q^s} = \zeta_{4d}+\zeta_{4d}^{-1}$, or equivalently $\zeta_{4d}^{q^s} = \zeta_{4d}^{\pm 1}$, i.e. $q^s \equiv \pm 1 \pmod{4d}$. If $\sqrt{a} \notin \mathbb{F}_q$ and s is odd, then $\sqrt{a}^{q^s} = -\sqrt{a}$, so $(*)$ is equivalent to $\zeta_{4d}^{q^s} = -\zeta_{4d}^{\pm 1}$, i.e. $q^s \equiv 2d \pm 1 \pmod{4d}$. The result follows at once by inspection. ∎

Theorem 3 *If q is even and $a \neq 0$, then $D_m(X,a)/X$ is the product of the squares of several distinct irreducible polynomials in $\mathbb{F}_q[X]$, which occur in cliques corresponding to the divisors d of m with $d > 1$. To each such d there correspond $\varphi(d)/(2k_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1}\left(X - \sqrt{a}\bigl(\zeta_d^{q^i}+\zeta_d^{-q^i}\bigr)\right)$$

for some choice of ζ_d; here k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

Proof. By Theorem 1, the roots of the polynomial $\sqrt{D_n(X,a)/X}$ are the elements $\alpha = \sqrt{a}\,(\zeta_d+\zeta_d^{-1})$ where $d \mid m$ and $d \neq 1$. As in the proof of Theorem 2, we conclude $\sqrt{D_m(X,a)/X}$ is the product of its distinct monic irreducible factors over $\mathbb{F}_q$, and each such factor is of the form $\prod_{i=0}^{N-1}(X-\alpha^{q^i})$, where N denotes the degree of α over $\mathbb{F}_q$. Since q is even, $a \in \mathbb{F}_q$ implies $\sqrt{a} \in \mathbb{F}_q$; thus N is the least positive integer s such that $\zeta_d^{q^s}+\zeta_d^{-q^s} = \zeta_d+\zeta_d^{-1}$, i.e., $q^s = \pm 1 \pmod{d}$. Hence $N = k_d$. Since for fixed d there are $\varphi(d)/2$ choices for α, we have the theorem. ∎

3. The Dickson polynomial of the second kind, $E_n(X,a)$. Write $n+1$ in the form $p^r(m+1)$, where $(p, m+1) = 1$. Using the functional equation for E_n, we find

$$E_n(Y+a/Y,a) = \frac{(Y^{m+1}-(a/Y)^{m+1})^{p^r}}{Y-\,a/Y} = E_m(Y+a/Y,a)^{p^r}(Y-a/Y)^{p^r-1},$$

and it follows that

$$E_n(X,a) = E_m(X,a)^{p^r}(X^2-4a)^{\frac{p^r-1}{2}}.$$

Thus, to factor E_n, it suffices to factor E_m. Our first result gives the factorization of E_m over $\overline{\mathbb{F}}_q$; we omit the proof since it is nearly identical to that of Theorem 1.

Theorem 4 *For q odd,*

$$E_m(X,a) = \prod_{i=1}^{m}\bigl(X - \sqrt{a}\,(\zeta^{i}_{2(m+1)} + \zeta^{-i}_{2(m+1)})\bigr);$$

for q even,

$$E_m(X,a) = \prod_{i=1}^{m/2}\bigl(X - \sqrt{a}\,(\zeta^{i}_{m+1} + \zeta^{-i}_{m+1})\bigr)^2.$$

When $a=0$, the factorization of $E_m(X,a)=X^m$ is trivial. In Theorems 5 and 6, we present the factorization of $E_m(X,a)$ over the finite field $\mathbb{F}_q$ in the case $a \neq 0$.

Theorem 5 *If q is odd and $a \neq 0$, then $E_m(X,a)$ is the product of several distinct irreducible polynomials in $\mathbb{F}_q[X]$. These occur in cliques corresponding to the divisors d of $2(m+1)$ with $d>2$. To each such d there correspond $\varphi(d)/(2N_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{N_d-1}\Bigl(X - \sqrt{a}^{\,q^i}\,(\zeta_d^{q^i} + \zeta_d^{-q^i})\Bigr)$$

for some choice of ζ_d, unless a is a nonsquare in $\mathbb{F}_q$ and $4 \nmid d$; in this exceptional case there are $\varphi(d)/N_d$ factors corresponding to each of $d=d_0$ and $d=2d_0$, where $d_0>1$ is an odd divisor of $m+1$, and the factors corresponding to d_0 are identical to the factors corresponding to $2d_0$. Here k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$, and

$$N_d = \begin{cases} k_d/2 & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } d \equiv 0 \pmod 2 \text{ and } k_d \equiv 2 \pmod 4 \\ & \quad \text{and } q^{k_d/2} \equiv \frac{d}{2} \pm 1 \pmod{d}; \\ 2k_d & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } k_d \text{ is odd;} \\ k_d & \text{otherwise.} \end{cases}$$

We omit the proof since it is similar to that of Theorem 2. We remark that the corresponding result in [2], namely Thm. 3.1, is false in case a is a square in $\mathbb{F}_q$ and $4 \nmid d$; this case should be included in item (5) of that result rather than item (6).

Theorem 6 *If q is even and $a \neq 0$, then $E_m(X,a)$ is the product of the squares of several distinct irreducible polynomials in $\mathbb{F}_q[X]$, which occur in cliques corresponding to the divisors d of $m+1$ with $d > 1$. To each such d there correspond $\varphi(d)/(2k_d)$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1} \Big(X - \sqrt{a}\big(\zeta_d^{q^i} + \zeta_d^{-q^i}\big)\Big)$$

for some choice of ζ_d; here k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

Proof. When the characteristic is 2, we observe that

$$E_m(Y + a/Y, a) = \frac{Y^{m+1} - (a/Y)^{m+1}}{Y - a/Y} = \frac{D_{m+1}(Y + a/Y, a)}{Y + a/Y};$$

hence $E_m(X,a) = D_{m+1}(X,a)/X$, so the desired factorization follows immediately from Theorem 3. ■

4. The bivariate Dickson polynomial, $D_n(X,a) - D_n(Y,a)$. Write $n = p^r m$, where $(m,p) = 1$. Then the functional equation implies $D_n(X,a) - D_n(Y,a) = [D_m(X,a) - D_m(Y,a)]^{p^r}$; thus, to factor $D_n(X,a) - D_n(Y,a)$, it suffices to factor $D_m(X,a) - D_m(Y,a)$. As the factorization of $D_m(X,0) - D_m(Y,0) = X^m - Y^m$ is trivial, we shall assume $a \neq 0$ throughout. Our first result gives the factorization of $D_m(X,a) - D_m(Y,a)$ over $\overline{\mathbb{F}}_q$.

Theorem 7 *Let $\alpha_i = \zeta_m^i + \zeta_m^{-i}$ and $\beta_i = \zeta_m^i - \zeta_m^{-i}$. Then for m odd,*

$$D_m(X,a) - D_m(Y,a) = (X - Y) \prod_{i=1}^{(m-1)/2} \big(X^2 - \alpha_i XY + Y^2 + \beta_i^2 a\big),$$

and for m even,

$$D_m(X,a) - D_m(Y,a) = (X - Y)(X + Y) \prod_{i=1}^{(m-2)/2} \big(X^2 - \alpha_i XY + Y^2 + \beta_i^2 a\big).$$

Proof. Observe that

$$\begin{aligned} D_m\big(W+\frac{a}{W},a\big)-D_m\big(Z+\frac{a}{Z},a\big) &= W^m+(a/W)^m-Z^m-(a/Z)^m \\ &= [W^m-Z^m]\Big[1-\Big(\frac{a}{WZ}\Big)^m\Big] \\ &= \prod_{\xi^m=1}\Big[\big(W-\xi Z\big)\Big(1-\xi\frac{a}{WZ}\Big)\Big]. \end{aligned}$$

In order to express the last expression as a function solely of $W + a/W$ and $Z + a/Z$, we pair the terms corresponding to ξ and $1/\xi$; writing $\alpha = \xi + \xi^{-1}$ and $\beta = \xi - \xi^{-1}$, this gives

$$\begin{aligned} &\Big(W-\xi Z\Big)\Big(1-\xi\frac{a}{WZ}\Big)\Big(W-\frac{Z}{\xi}\Big)\Big(1-\frac{a}{\xi WZ}\Big) \\ =\ &\Big(W+\frac{a}{W}\Big)^2-\alpha\Big(W+\frac{a}{W}\Big)\Big(Z+\frac{a}{Z}\Big)+\Big(Z+\frac{a}{Z}\Big)^2+\beta^2 a \end{aligned}$$

if $\xi \neq 1/\xi$ (i.e. $\xi \neq \pm 1$), and

$$\Big(W-\xi Z\Big)\Big(1-\xi\frac{a}{WZ}\Big)=\Big(W+\frac{a}{W}\Big)-\xi\Big(Z+\frac{a}{Z}\Big)$$

otherwise. The factorization given in the theorem follows at once. Moreover, one can immediately check that the given linear and quadratic factors are irreducible over $\overline{\mathbb{F}}_q$; hence the stated factorization is complete. ■

Our next result gives the factorization of $D_m(X, a) - D_m(Y, a)$ over $\mathbb{F}_q$.

Theorem 8 *The polynomial $D_m(X, a) - D_m(Y, a)$ is the product of distinct irreducible polynomials in $\mathbb{F}_q[X]$, which occur in cliques corresponding to the divisors d of m. To each such $d \neq 1, 2$ there correspond $\varphi(d)/(2k_d)$ irreducible factors of degree $2k_d$, each of which has the form*

$$\prod_{i=0}^{k_d-1}\big(X^2-\alpha_d^{q^i}XY+Y^2+\beta_d^{2q^i}a\big).$$

For $d \in \{1, 2\}$, there corresponds a single factor of the form $(X - \zeta_d Y)$. Here α_d and β_d denote $\zeta_d + \zeta_d^{-1}$ and $\zeta_d - \zeta_d^{-1}$ respectively for some choice of ζ_d, and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

Proof. Note that the quadratic factors of $D_m(X,a) - D_m(Y,a)$ over $\overline{\mathbb{F}}_q$ as given in the previous theorem are distinct, since $\alpha_1, \ldots, \alpha_{\lfloor (m-1)/2 \rfloor}$ are distinct. Hence $D_m(X,a) - D_m(Y,a)$ is the product of its distinct monic irreducible factors over $\mathbb{F}_q$, and each such factor is either of the form $(X - \zeta_d Y)$ for $d = 1$ or 2, or is of the form

$$\prod_{i=0}^{N-1} \left(X^2 - \alpha_d^{q^i} XY + Y^2 + \beta_d^{2q^i} a\right),$$

for some $d \mid m$ with $d > 2$, where N denotes the least positive integer such that both α_d and β_d^2 are elements of $\mathbb{F}_{q^N}$. However, note that $\beta_d^2 = \alpha_d^2 - 4 \in \mathbb{F}_q(\alpha_d)$, and, as before, the smallest integer M such that $\alpha_d^{q^M} = \alpha_d$ is $M = k_d$. Hence $N = k_d$, and the theorem follows. ∎

Remark. There does not appear to be an analogous way to treat the bivariate Dickson polynomial $E_n(X,a) - E_n(Y,a)$ of the second kind, and in fact little is known about this factorization, although G. Turnwald has some preliminary results [6]. Finally, we mention one further factorization involving Dickson polynomials:

$$\sum_{i=0}^{q-1} E_i(X,1) Y^{(q-1)(q-1-i)} = \prod_{a \in \mathbb{F}_q^*} [D_{q-1}(Y,a) - X].$$

Many further results along these lines can be found in [1].

Acknowledgments. That the arguments presented in [2] can be greatly simplified has been independently noticed by S. Gao (private communication). The first author acknowledges support from AT&T Research during the summer of 1997. The second author was supported by an NSF Postdoctoral Fellowship.

References

[1] S. S. Abhyankar, S. D. Cohen, and M. E. Zieve, Bivariate factorizations connecting Dickson polynomials and Galois theory, *Trans. Amer. Math. Soc.*, to appear.

[2] W. Chou, The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.* **3** (1997), 84–96.

[3] S. D. Cohen and R. W. Matthews, Monodromy groups of classical families over finite fields, *in* “Finite Fields and Applications,” LMS Lecture Note Series, Vol. 233, pp. 59–68, Cambridge, 1996.

[4] R. Lidl, G. L. Mullen, and G. Turnwald, “Dickson Polynomials,” Pitman Monographs and Surveys in Pure and Applied Math.,Longman, London/Harlow/Essex, 1993.

[5] G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc. (Ser. A)* **58** (1995), 312–357.

[6] G. Turnwald, Monodromy groups of Dickson polynomials of the second kind, preprint, 1996.

[7] K. S. Williams, Note on Dickson's permutation polynomials, *Duke Math. J.* **38** (1971), 659–665.