two isotopism classes, so that there are sound reasons for considering the strong isotopism problem on planar DO polynomials instead of the more difficult isotopism problem.

9.5.28 Theorem (Strong isotopy and planar equivalence) [722] Let $f, g \in \mathbb{F}_q[x]$ be planar DO polynomials with corresponding commutative presemifields $\mathcal{S}_f$ and $\mathcal{S}_g$. There is a strong isotopism (N, N, L) between $\mathcal{S}_f$ and $\mathcal{S}_g$ if and only if $f(N(x)) \equiv L(g(x)) \bmod (x^q - x)$.

See Also

§9.2 For APN functions that are closely related to planar functions.

§9.3 For bent functions that are closely related to planar functions.

§14.3 For affine and projective planes; the seminal paper [802] clearly outlines the main properties of the planes constructed via planar functions.

§14.6 Discusses difference sets. Ding and Yuan [868] used the examples of Proposition 9.5.11 Part 3 to disprove a long-standing conjecture on skew Hadamard difference sets; see also [865, 2953].

[271] Construct further classes of planar DO polynomials; see also [272], [446], [447], [2368], [3036], [3037]. The problem of planar (in)equivalence between these constructions is not completely resolved at the time of writing. An incredible new class, which combines Albert's twisted fields with Dickson's semifields, was very recently discovered by Pott and Zhou [2410].

[722] Classifies planar DO polynomials over fields of order p^2 and p^3. This does not constitute a classification of planar polynomials over fields of these orders.

[723] Applies Theorem 9.4.22 to commutative presemifields of odd order to restrict both the form of the DO polynomials and the isotopisms that need to be considered; see also [1786]. A promising alternative approach (which applies also to APN functions, see Section 9.2) is outlined in [272], while a third approach was given recently in [2954].

[1496] For results on possible forms of planar functions not defined over finite fields.

[1786] Gives specific forms for planar DO polynomials corresponding to the Dickson semifields [841], the Cohen-Ganley semifields [683], the Ganley semifields [1164], and the Penttila-Williams semifield [2368].

References Cited: [261, 271, 272, 324, 446, 447, 683, 720, 722, 723, 725, 726, 728, 781, 802, 805, 841, 865, 868, 1164, 1278, 1495, 1496, 1599, 1746, 1786, 1805, 2368, 2378, 2410, 2465, 2953, 2954, 3036, 3037]

9.6 Dickson polynomials

Qiang Wang, *Carleton University*
Joseph L. Yucas, *Southern Illinois University*

9.6.1 Basics

9.6.1 Definition Let n be a positive integer. For $a \in \mathbb{F}_q$, we define the *n-th Dickson polynomial of the first kind* $D_n(x,a)$ over $\mathbb{F}_q$ by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

9.6.2 Theorem (Waring's formula, [1927, Theorem 1.76]) Let $\sigma_1, \dots, \sigma_k$ be elementary symmetric polynomials in the variables $x_1, \dots, x_k$ over a ring R and $s_n = s_n(x_1, \dots, x_k) = x_1^n + \cdots + x_k^n \in R[x_1, \dots, x_k]$ for $n \geq 1$. Then we have

$$s_n = \sum (-1)^{i_2+i_4+i_6+\cdots} \frac{(i_1+i_2+\cdots+i_k-1)!n}{i_1!i_2!\cdots i_k!} \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_k^{i_k},$$

for $n \geq 1$, where the summation is extended over all tuples $(i_1, i_2, \dots, i_n)$ of nonnegative integers with $i_1 + 2i_2 + \cdots + ki_k = n$. The coefficients of the $\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_k^{i_k}$ are integers.

9.6.3 Theorem Dickson polynomials of the first kind are the unique monic polynomials satisfying the functional equation

$$D_n\left(y + \frac{a}{y}, a\right) = y^n + \frac{a^n}{y^n},$$

where $a \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^2}$. Moreover, they satisfy the recurrence relation

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a),$$

for $n \geq 2$ with initial values $D_0(x,a) = 2$ and $D_1(x,a) = x$.

9.6.4 Remark The Dickson polynomial $D_n(x,a)$ of the first kind satisfies a commutative type of relation under composition. That is, $D_{mn}(x,a) = D_m(D_n(x,a), a^n)$. Hence the set of all Dickson polynomials $D_n(x,a)$ of even degree over $\mathbb{F}_q$ are closed under composition if and only if $a = 0$ or $a = 1$. In particular, if $a = 0$ or 1 then $D_m(x,a) \circ D_n(x,a) = D_n(x,a) \circ D_m(x,a)$. Moreover, the set of all Dickson polynomials $D_n(x,a)$ of odd degree over $\mathbb{F}_q$ is closed under composition if and only if $a = 0$, $a = 1$ or $a = -1$. See [1924, 1927] for more details.

9.6.5 Definition For $a \in \mathbb{F}_q$, we define the *n-th Dickson polynomial of the second kind* $E_n(x,a)$ over $\mathbb{F}_q$ by

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

9.6.6 Theorem Dickson polynomials of the second kind have a functional equation

$$E_n(x,a) = E_n\left(y + \frac{a}{y}, a\right) = \frac{y^{n+1} - a^{n+1}/y^{n+1}}{y - a/y},$$

for $y \neq \pm\sqrt{a}$; for $y = \pm\sqrt{a}$, we have $E_n(2\sqrt{a}, a) = (n+1)(\sqrt{a})^n$ and $E_n(-2\sqrt{a}, a) = (n+1)(-\sqrt{a})^n$; here $a \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^2}$. Moreover, they satisfy the recurrence relation

$$E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a),$$

for $n \geq 2$ with initial values $E_0(x,a) = 1$ and $E_1(x,a) = x$.

9.6.7 Remark In the case $a = 1$, denote Dickson polynomials of degree n of the first and the second kinds by $D_n(x)$ and $E_n(x)$, respectively. These Dickson polynomials are closely related over the complex numbers to the Chebyshev polynomials through the connections $D_n(2x) = 2T_n(x)$ and $E_n(2x) = U_n(x)$, where $T_n(x)$ and $U_n(x)$ are Chebyshev polynomials of degree n of the first and the second kind, respectively. In recent years these polynomials have received an extensive examination. The book [1924] is devoted to a survey of the algebraic and number theoretic properties of Dickson polynomials.

9.6.8 Remark Suppose q is odd and a is a nonsquare in $\mathbb{F}_q$. Then

$$(x + \sqrt{a})^n = r_n(x) + s_n(x)\sqrt{a},$$

where

$$r_n(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i} a^i x^{n-2i}, s_n(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n}{2i+1} a^i x^{n-2i-1}.$$

The *Rédei function* is the rational function $R_n(x) = \frac{r_n(x)}{s_n(x)}$. It is shown in [1110] that $2r_n(x) = D_n(2x, x^2 - a)$.

9.6.9 Remark Permutation properties of Dickson polynomials are important; see Section 8.1. The famous Schur conjecture postulating that every integral polynomial that is a permutation polynomial for infinitely many primes is a composition of linear polynomials and Dickson polynomials was proved by Fried [1103]. We refer readers to Section 9.7.

9.6.2 Factorization

9.6.10 Remark The factorization of the Dickson polynomials of the first kind over $\mathbb{F}_q$ was given [620] and simplified in [264].

9.6.11 Theorem [264, 620] If q is even and $a \in \mathbb{F}_q^*$ then $D_n(x,a)$ is the product of squares of irreducible polynomials over $\mathbb{F}_q$ which occur in cliques corresponding to the divisors d of n, $d > 1$. Let k_d be the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$. To each such d there corresponds $\phi(d)/(2k_d)$ irreducible factors of degree k_d, each of which has the form

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

where ζ is a d-th root of unity and ϕ is Euler's totient function.

9.6.12 Theorem [264, 620] If q is odd and $a \in \mathbb{F}_q^*$ then $D_n(x,a)$ is the product of irreducible polynomials over $\mathbb{F}_q$ which occur in cliques corresponding to the divisors d of n for which n/d is odd. Let m_d is the least positive integer satisfying $q^{m_d} \equiv \pm 1 \pmod{4d}$. To each such d there corresponds $\phi(4d)/(2N_d)$ irreducible factors of degree N_d, 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 $4d$-th root of unity and

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

9.6.13 Example Let $(q, n) = (5, 12)$. Then $D_{12}(x, 2) = x^{12} + x^{10} + x^8 + 4x^6 + 3x^2 + 3$ is the product of irreducible polynomials over $\mathbb{F}_5$ which occur in cliques corresponding to the divisors $d = 4$ and $d = 12$ of $n = 12$. By direct computation, $m_4 = N_4 = 4$ and $m_{12} = N_{12} = 4$. For $d = 4$, there corresponds one irreducible factor of degree 4, while there are two irreducible factors of degree 4 for $d = 12$, 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 $4d$-th root of unity.

9.6.14 Remark Similar results hold for Dickson polynomials of the second kind and they can be found in [264] and [620]. Dickson polynomials of other kinds are defined in [2926] and the factorization of the Dickson polynomial of the third kind is obtained similarly in [2926]. We note that the factors appearing in the above results are over $\mathbb{F}_q$, although their description uses elements in an extension field of $\mathbb{F}_q$. In [1073] Fitzgerald and Yucas showed that these factors can be obtained from the factors of certain cyclotomic polynomials. This in turn gives a relationship between a-self-reciprocal polynomials and these Dickson factors. In the subsequent subsections we explain how this works. These results come mainly from [1073].

9.6.2.1 a-reciprocals of polynomials

9.6.15 Definition Let q be an odd prime power and fix $a \in \mathbb{F}_q^*$. For a monic polynomial f over $\mathbb{F}_q$ of degree n, with $f(0) \neq 0$, define the *a-reciprocal* of f by

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

The polynomial f is *a-self-reciprocal* if $f(x) = \hat{f}_a(x)$.

9.6.16 Remark We note that the notion of a 1-self-reciprocal is the usual notion of a self-reciprocal.

9.6.17 Lemma

1. If α is a root of f then a/α is a root of $\hat{f}_a$.
2. The polynomial f is irreducible over $\mathbb{F}_q$ if and only if $\hat{f}_a$ is irreducible over $\mathbb{F}_q$.

9.6.18 Remark The a-reciprocal of an irreducible polynomial f may not have the same order as f. For example, consider $f(x) = x^3 + 3$ when $q = 7$. Then f has order 9 while $\hat{f}_3(x) = x^3 + 2$ has order 18.

9.6.19 Theorem [1073] Suppose f is a polynomial of even degree $n = 2m$ over $\mathbb{F}_q$. The following statements are equivalent:

1. f is a-self-reciprocal;
2. $n = 2m$ and f 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 $b_j \in \mathbb{F}_q$.

9.6.20 Definition Let n be an even integer. 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 $r \in D_n$ and even n, we write $r = d_r t_r$ where $d_r = (r, q^m + 1)$ and $m = n/2$.

9.6.21 Theorem [1073] Suppose f is an irreducible polynomial of degree $n = 2m$ over $\mathbb{F}_q$. The following statements are equivalent:

1. f is a-self-reciprocal for some $a \in \mathbb{F}_q^*$ with $\text{ord}(a) = t$,
2. f has order $r \in D_n$ and $t_r = t$.

9.6.22 Theorem [1073] Let $r \in D_n$ and suppose t_r divides $q - 1$. Then the cyclotomic polynomial $Q(r, x)$ factors into all a-self-reciprocal monic irreducible polynomials of degree n and order r where a ranges over all elements of $\mathbb{F}_q$ of order t_r.

9.6.2.2 The maps Φ_a and Ψ_a

9.6.23 Definition Define the mapping $\Phi_a : P_m \to S_n$ from the polynomials over $\mathbb{F}_q$ of degree m to the a-self-reciprocal polynomials over $\mathbb{F}_q$ of degree $n = 2m$ by

$$\Phi_a(f(x)) = x^m f(x + a/x).$$

9.6.24 Remark In the case $a = 1$ this transformation has appeared often in the literature. The first occurrence is Carlitz [544]. Other authors writing about Φ are Chapman [584], Cohen [673], Fitzgerald-Yucas [1073], Kyuregyan [1808], Miller [2086], Meyn [2077] and Scheerhorn [2521].

9.6.25 Definition Define $\Psi_a : S_n \to P_m$ by

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

9.6.26 Theorem Maps Φ_a and Ψ_a are multiplicative and are inverses of each other.

9.6.2.3 Factors of Dickson polynomials

9.6.27 Theorem [1073] The polynomial $D_n(x, a)$ is mapped to $x^{2n} + a^n$ by the above defined Φ_a, namely, $\Phi_a(D_n(x, a)) = x^{2n} + a^n$.

9.6.28 Theorem [1073] The polynomial $x^{2n} + a^n$ factors over $\mathbb{F}_q$ as

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

where each f is either an irreducible a-self-reciprocal polynomial or a product of an irreducible polynomial and its a-reciprocal over $\mathbb{F}_q$.

9.6.29 Theorem [1073] The polynomial $D_n(x, a)$ factors over $\mathbb{F}_q$ as

$$D_n(x, a) = \prod \Psi_a(f(x)),$$

where $x^{2n} + a^n = \prod f(x)$ such that f is either an irreducible a-self-reciprocal polynomial or a product of an irreducible polynomial and its a-reciprocal.

9.6.30 Theorem The following is an algorithm for factoring $D_n(x, a)$ over $\mathbb{F}_q$.

1. Factor $x^{2n} + a^n$.
2. For each factor f of $x^{2n} + a^n$ which is not a-self-reciprocal, multiply f with $\hat{f}_a$.
3. Apply Ψ_a.

9.6.31 Example We factor $D_{12}(x, 2) = x^{12} + x^{10} + x^8 + 4x^6 + 3x^2 + 3$ when $q = 5$.

$$\begin{aligned} x^{24} + 2^{12} &= [(x^4 + x^2 + 2)(x^4 + 2x^2 + 3)][(x^4 + 3)(x^4 + 2)][(x^4 + 4x^2 + 2)(x^4 + 3x^2 + 3)] \\ &= (x^8 + 3x^6 + 2x^4 + 2x^2 + 1)(x^8 + 1)(x^8 + 2x^6 + 2x^4 + 3x^2 + 1). \end{aligned}$$

Then apply Ψ_2 to obtain

$$\begin{aligned} D_{12}(x, 2) &= (D_4(x, 2) + 3D_2(x, 2) + 2)D_4(x, 2)(D_4(x, 2) + 2D_2(x, 2) + 2) \\ &= (x^4 + 3)(x^4 + 2x^2 + 3)(x^4 + 4x^2 + 2). \end{aligned}$$

9.6.32 Definition For $a \in \mathbb{F}_q^*$, define $\eta(n, a)$ by

$$\eta(n, a) = \begin{cases} n \cdot \operatorname{ord}(a^n) & \text{if } n \text{ is odd and } a \text{ is a non-square,} \\ 4n \cdot \operatorname{ord}(a^n) & \text{otherwise.} \end{cases}$$

9.6.33 Theorem [1073] For a monic irreducible polynomial f over $\mathbb{F}_q$ and $a \in \mathbb{F}_q^*$, the following statements are equivalent:

1. f divides $D_n(x, a)$.
2. There exists a divisor d of n with n/d odd and $\operatorname{ord}(\Phi_a(f)) = \eta(d, a)$, where Φ_a is defined in Definition 9.6.23.

9.6.2.4 a-cyclotomic polynomials

9.6.34 Definition For $a \in \mathbb{F}_q^*$, define the *a-cyclotomic polynomial* $Q_a(n, x)$ over $\mathbb{F}_q$ by

$$Q_a(n, x) = \prod_{\substack{d \mid n \\ d \text{ even}}} (x^d - a^{d/2})^{\mu(n/d)}.$$

9.6.35 Remark When $n \equiv 0 \pmod 4$, we have $Q_1(n, x) = Q(n, x)$, the n-th cyclotomic polynomial over $\mathbb{F}_q$. When $n \equiv 2 \pmod 4$, we have $Q_1(n, x) = Q(n/2, -x^2)$. Similar to the factorization of $x^n - 1 = \prod_{d \mid n} Q(d, x)$ [1927], we can reduce the factorization of $x^{2n} \pm a^n$ to the factorization of a-cyclotomic polynomials.

9.6.36 Theorem [1073] We have

1. $x^{2n} - a^n = \prod_{d \mid n} Q_a(2d, x)$;
2. $x^{2n} + a^n = \prod_{\substack{d \mid n \\ d \text{ odd}}} Q_a(4d, x)$.

9.6.37 Remark A factorization of these a-cyclotomic polynomials $Q_a(m, x)$ is also given in [1073].

9.6.3 Dickson polynomials of the $(k+1)$-st kind

9.6.38 Definition [2926] For $a \in \mathbb{F}_q$, any integers $n \geq 0$ and $0 \leq k < p$, we define the *n-th Dickson polynomial of the $(k+1)$-st kind* $D_{n,k}(x,a)$ over $\mathbb{F}_q$ by $D_{0,k}(x,a) = 2-k$ and

$$D_{n,k}(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

9.6.39 Definition [2926] For $a \in \mathbb{F}_q$, any integers $n \geq 0$ and $0 \leq k < p$, we define the *n-th reversed Dickson polynomial of the $(k+1)$-st kind* $D_{n,k}(a,x)$ over $\mathbb{F}_q$ by $D_{0,k}(a,x) = 2-k$ and

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-1)^i a^{n-2i} x^i.$$

9.6.40 Remark [2926] It is easy to see that $D_{n,0}(x,a) = D_n(x,a)$ and $D_{n,1}(x,a) = E_n(x,a)$. Moreover, if $\mathrm{char}(\mathbb{F}_q) = 2$, then $D_{n,k}(x,a) = D_n(x,a)$ if k is even and $D_{n,k}(x,a) = E_n(x,a)$ if k is odd.

9.6.41 Theorem [2926] For any integer $k \geq 1$, we have

$$D_{n,k}(x,a) = kD_{n,1}(x,a) - (k-1)D_{n,0}(x,a) = kE_n(x,a) - (k-1)D_n(x,a).$$

9.6.42 Theorem [2926] The fundamental functional equation for $D_{n,k}$ is

$$\begin{aligned} D_{n,k}(y+ay^{-1},a) &= \frac{y^{2n} + yax^{2n-2} + \cdots + ka^{n-1}y^2 + a^n}{y^n} \\ &= \frac{y^{2n}+a^n}{y^n} + \frac{ka}{y^n}\frac{y^{2n} - a^{n-1}y^2}{y^2-a}, \quad \text{for } y \neq 0, \pm\sqrt{a}. \end{aligned}$$

9.6.43 Theorem [2926] The Dickson polynomial of the $(k+1)$-st kind satisfies the following recurrence relation

$$D_{n,k}(x,a) = xD_{n-1,k}(x,a) - aD_{n-2,k}(x,a),$$

for $n \geq 2$ with initial values $D_{0,k}(x,a) = 2-k$ and $D_{1,k}(x,a) = x$.

9.6.44 Theorem [2926] The generating function of $D_{n,k}(x,a)$ is

$$\sum_{n=0}^{\infty} D_{n,k}(x,a)z^n = \frac{2-k+(k-1)xz}{1-xz+az^2}.$$

9.6.45 Remark The Dickson polynomial $D_{n,k}(x,a)$ of the $(k+1)$-st kind satisfies a second order differential equation; see [2706, 2926] for more details.

9.6.46 Theorem [2926] Suppose ab is a square in $\mathbb{F}_q^*$. Then $D_{n,k}(x,a)$ is a PP of $\mathbb{F}_q$ if and only if $D_{n,k}(x,b)$ is a PP of $\mathbb{F}_q$. Furthermore,

$$D_{n,k}(\alpha,a) = (\sqrt{a/b})^n D_{n,k}((\sqrt{b/a})\alpha, b).$$

9.6.47 Definition Define S_{q-1}, S_{q+1}, and S_p by

$$S_{q-1} = \{\alpha \in \mathbb{F}_q : u_\alpha^{q-1} = 1\}, \quad S_{q+1} = \{\alpha \in \mathbb{F}_q : u_\alpha^{q+1} = 1\}, \quad S_p = \{\pm 2\},$$

where $u_\alpha \in \mathbb{F}_{q^2}$ satisfies $\alpha = u_\alpha + \frac{1}{u_\alpha} \in \mathbb{F}_q$.

9.6.48 Theorem [2926] As functions on $\mathbb{F}_q$, we have

$$D_{n,k}(\alpha) = \begin{cases} D_{(n)_{2p},k}(\alpha) & \text{if } \alpha \in S_p, \\ D_{(n)_{q-1},k}(\alpha) & \text{if } \alpha \in S_{q-1}, \\ D_{(n)_{q+1},k}(\alpha) & \text{if } \alpha \in S_{q+1}, \end{cases}$$

where for positive integers n and r we use the notation $(n)_r$ to denote $n \pmod r$, the smallest positive integer congruent to n modulo r.

9.6.49 Theorem [2926] Let $\alpha = u_\alpha + \frac{1}{u_\alpha}$ where $u_\alpha \in \mathbb{F}_{q^2}$ and $\alpha \in \mathbb{F}_q$. Let $\epsilon_\alpha = u_\alpha^c \in \{\pm 1\}$ where $c = \frac{p(q^2-1)}{4}$. As functions on $\mathbb{F}_q$ we have

$$D_{c+n,k}(\alpha) = \epsilon_\alpha D_{n,k}(\alpha).$$

Moreover, $D_{n,k}(x)$ is a PP of $\mathbb{F}_q$ if and only if $D_{c+n,k}(x)$ is a PP of $\mathbb{F}_q$.

9.6.50 Theorem [2926] For $k \neq 1$, let $k' = \frac{k}{k-1} \pmod p$ and $\epsilon_\alpha = u_\alpha^c \in \{\pm 1\}$ where $c = \frac{p(q^2-1)}{4}$. For $n < c$, as functions on $\mathbb{F}_q$ we have

$$D_{c-n,k'}(\alpha) = \frac{-\epsilon_\alpha}{k-1} D_{n,k}(\alpha).$$

Moreover, $D_{n,k}(x)$ is a PP of $\mathbb{F}_q$ if and only if $D_{c-n,k'}(x)$ is a PP of $\mathbb{F}_q$.

9.6.4 Multivariate Dickson polynomials

9.6.51 Definition [1924] The Dickson polynomial of the first kind $D_n^{(i)}(x_1, \ldots, x_t, a)$, $1 \le i \le t$, is given by the functional equations

$$D_n^{(i)}(x_1, \ldots, x_t, a) = s_i(u_1^n, \ldots, u_{t+1}^n), \; 1 \le i \le t,$$

where $x_i = s_i(u_1, \ldots, u_{t+1})$ are elementary symmetric functions and $u_1 \cdots u_{t+1} = a$. The vector $D(t, n, a) = (D_n^{(1)}, \ldots, D_n^{(t)})$ of the t Dickson polynomials is a *Dickson polynomial vector.*

9.6.52 Remark Let $r(c_1, \ldots, c_t, z) = z^{t+1} - c_1 z^t + c_2 z^{t-1} + \cdots + (-1)^t c_t z + (-1)^{t+1} a$ be a polynomial over $\mathbb{F}_q$ and $\beta_1, \ldots, \beta_{t+1}$ be the roots (not necessarily distinct) in a suitable extension of $\mathbb{F}_q$. For any positive integer n, we let $r_n(c_1, \ldots, c_t, z) = (z - \beta_1^n) \ldots (z - \beta_{t+1}^n)$. Then $r_n(c_1, \ldots, c_t, z) = z^{t+1} - D_n^{(1)}(c_1, \ldots, c_t, a) z^t + D_n^{(2)}(c_1, \ldots, c_t, a) z^{t-1} + \cdots + (-1)^t D_n^{(t)}(c_1, \ldots, c_t, a) z + (-1)^{t+1} a^t$.

9.6.53 Remark For the Dickson polynomial $D_n^{(1)}(x_1, \ldots, x_t, a)$, an explicit expression, a generating function, a recurrence relation, and a differential equation satisfied by $D_n^{(1)}(x_1, \ldots, x_t, a)$ can be found in [1924]. Here we only give the generating function and recurrence relation.

9.6.54 Theorem The Dickson polynomial of the first kind $D_n^{(1)}(x_1, \ldots, x_t, a)$ satisfies the generating function

$$\sum_{n=0}^{\infty} D_n^{(1)}(x_1, \ldots, x_t, a) z^n = \frac{\sum_{i=0}^{t} (t+1-i)(-1)^i x_i z^i}{\sum_{i=0}^{t+1} (-1)^i x_i z^i}, \text{ for } n \geq 0,$$

and the recurrence relation

$$D_{n+t+1}^{(1)} - x_1 D_{n+t}^{(1)} + \cdots + (-1)^t x_k D_{n+1}^{(1)} + (-1)^{t+1} a D_n^{(1)} = 0,$$

with the $t+1$ initial values

$$D_0^{(1)} = t+1, D_j^{(1)} = \sum_{r=1}^{j} (-1)^{r-1} x_r D_{j-r}^{(1)} + (-1)^j (t+1-j) x_j, \text{ for } 0 < j \leq t.$$

9.6.55 Remark Much less is known for the multivariate Dickson polynomials of the second kind. The same recurrence relation of $D_n^{(1)}(x_1, \ldots, x_t, a)$ is used to define the multivariate Dickson polynomials of the second kind $E_n^{(1)}(x_1, \ldots, x_t, a)$ with the initial condition $E_0 = 1$, $E_j = \sum_{r=1}^{j} (-1)^{r-1} x_r E_{j-r}$ for $1 \leq j \leq t$. The generating function is $\sum_{n=0}^{\infty} E_n z^n = \frac{1}{\sum_{i=0}^{t+1} (-1)^i x_i z^i}$; see [1924] for more details.

See Also

§8.1	For permutation polynomials with one variable.
§8.3	For value sets of polynomials over finite fields.
§9.7	For Schur's conjecture and exceptional covers.
[1924]	For a comprehensive book on Dickson polynomials.

References Cited: [264, 544, 584, 620, 673, 1073, 1103, 1110, 1808, 1924, 1927, 2077, 2086, 2521, 2706, 2926]

9.7 Schur's conjecture and exceptional covers

.

Michael D. Fried, *University of California Irvine*

9.7.1 Rational function definitions

9.7.1 Remark (Extend values) The historical functions of this section are polynomials and rational functions: $f(x) = N_f(x)/D_f(x)$ with N_f and D_f relatively prime (nonzero) polynomials, denoted $f \in F(x)$, F a field (almost always $\mathbb{F}_q$ or a number field). The subject takes off by including functions f – *covers* – where the domain and range are varieties of the same dimension. Still, we emphasize functions between projective algebraic curves (nonsingular), often where the target and domain are projective 1-space.