Subfield value sets over finite fields

Wun-Seng Chou *
Institute of Mathematics
Academia Sinica, and/or
Department of Mathematical Sciences
National Chengchi University
Taipei, Taiwan, ROC
Email: macws@math.sinica.edu.tw

Javier Gomez-Calderon, Gary L. Mullen†
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802, U. S. A.
Email: {jxg11,mullen}@math.psu.edu

Daniel Panario‡, and David Thomson †‡
School of Mathematics and Statistics
Carleton University
1125 Colonel By Dr., Ottawa ON Canada, K1S 5B6
Email: {daniel,dthomson}@math.carleton.ca

Abstract

Let $\mathbb{F}_{q^e}$ be a finite field, and let $\mathbb{F}_{q^d}$ be a subfield of $\mathbb{F}_{q^e}$. The *value set* of a polynomial f lying within $\mathbb{F}_{q^d}$ is defined as the set of images $\{f(c) \in \mathbb{F}_{q^d} : c \in \mathbb{F}_{q^e}\}$. This work is concerned with the cardinality of value sets of polynomials lying within subfields. In particular, we give the cardinality of subfield value sets of linearized polynomials, of power polynomials and of Dickson polynomials $D_n(x, a)$ of degree n and parameter a, where $a^n \in \mathbb{F}_{q^d}$.

*This author would like to thank the National Science Council for partial support of this work under grant number NSC 92-2115-M-001-026.

†These authors would like to sincerely thank Gary McGuire and the Claude Shannon Institute of University College Dublin, Dublin, Ireland, for their support during the Jan. - Mar., 2011 period, where part of this work took place.

‡These authors are partially supported by NSERC of Canada.

2010 *Mathematics Subject Classification*: Primary 11T06; Secondary 12F99.

Key words and phrases: Dickson polynomial, linearized polynomial, power polynomial, value set, permutation polynomial, König-Rados Theorem.

1 Introduction

Let q be a prime power, let $\mathbb{F}_q$ denote the finite field of order q, and let $\mathbb{F}_q^*$ denote the (cyclic) multiplicative group of $\mathbb{F}_q$. For integers $1 \leq d \leq e$, $\mathbb{F}_{q^d}$ is a subfield of the finite field $\mathbb{F}_{q^e}$ if and only if d divides e.

In this paper we consider the *value set* of a polynomial $f \in \mathbb{F}_{q^e}[x]$ *lying within a subfield* $\mathbb{F}_{q^d}$ *of* $\mathbb{F}_{q^e}$, or simply the *subfield value set*. The subfield value set is defined as the set of images $f(c) \in \mathbb{F}_{q^d}$, where c runs over $\mathbb{F}_{q^e}$. When the subfield is omitted, the value set of f is simply the set of images of f. Das and Mullen [2] study value sets of polynomials over finite fields; in particular, they obtain a lower bound for the cardinality of the value set of a polynomial over $\mathbb{F}_q$.

The idea of studying functions on extension fields with their images in subfields is a very natural one. For example, the *absolute trace* function defined for $\alpha \in \mathbb{F}_{q^e}$ by

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{e-1}}$$

maps onto the subfield $\mathbb{F}_q$ uniformly in the sense that it maps onto each element of the subfield $\mathbb{F}_q$ equally often. More generally, for each d dividing e, the trace function defined for $\alpha \in \mathbb{F}_{q^e}$ by

$$\mathrm{Tr}_d(\alpha) = \alpha + \alpha^{q^d} + \cdots + \alpha^{q^{e-d}}$$

maps onto the subfield $\mathbb{F}_{q^d}$ uniformly in the sense that it maps onto each element of the subfield $\mathbb{F}_{q^d}$ equally often. These subfield ideas can be used to construct sets of mutually orthogonal frequency squares (MOFS); see [7]. A connection to maximal curves is given in [3].

From now on, let $V_f(q^e; q^d) = \{f(c) \in \mathbb{F}_{q^d} \colon c \in \mathbb{F}_{q^e}\}$ denote the subfield value set of f that lies in the subfield $\mathbb{F}_{q^d}$ as c ranges over the extension field $\mathbb{F}_{q^e}$. Further let $|V_f(q^e; q^d)|$ denote the cardinality of $V_f(q^e; q^d)$, that is, the number of distinct elements in the image of f that lie in $\mathbb{F}_{q^d}$ as c ranges over the extension field $\mathbb{F}_{q^e}$. As a special case we note that $V_f(q^e; q^e)$ denotes the usual value set $\{f(c) \colon c \in \mathbb{F}_{q^e}\}$ of a polynomial f over the field $\mathbb{F}_{q^e}$.

Further let $N_f(q^e; q^d)$ denote the number of images $f(c)$ (counting multiplicities) of $f : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$ that lie in the subfield $\mathbb{F}_{q^d}$, as c ranges over the elements of the extension field $\mathbb{F}_{q^e}$. We clearly have $|V_f(q^e; q^d)| \leq N_f(q^e; q^d)$, and of course $N_f(q^e; q^e) = q^e$ for any polynomial f over the field $\mathbb{F}_{q^e}$.

In this paper, we consider subfield value sets for several classes of polynomials, namely *linearized polynomials*, *power polynomials* and *Dickson polynomials*.

The structure of the paper is as follows. Section 2 gives the value set in the subfield for linearized polynomials and includes an extension of the König-Rados Theorem which gives the distribution of zeroes of a polynomial lying within a subfield. In Section 3 we give the value set in the subfield for power polynomials. Section 4 presents the main result of this paper on the value set of Dickson polynomials within subfields. We conclude in Section 5 with an open problem on the general case of the subfield value set of a Dickson polynomial.

2 König-Rados and linearized polynomials

2.1 König-Rados theorem for subfields

Let $n > 0$, let $f \in \mathbb{F}_q[x]$ and consider the equation $f(x) = 0$. The distinct roots of f can be found as the roots of $\gcd(f, x^q - x)$, which have multiplicity 1. Thus, the number of distinct solutions of $f(x) = 0$ is equal to the degree of $\gcd(f, x^q - x)$. It is trivial to determine if $f(0) = 0$ and so we consider only the solutions to $\gcd(f, x^{q-1} - 1)$. Furthermore, since $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q$, we may assume, without loss of generality, that $n \leq q - 2$ when we consider the number of nonzero solutions of $f(x) = 0$.

The König-Rados Theorem expresses the number of nonzero roots of a polynomial in terms of the rank of a coefficient matrix.

Theorem 2.1. [6, Theorem 6.1] *Let q be a power of a prime, let*

$$f(x) = \sum_{s=0}^{q-2} a_s x^s \in \mathbb{F}_q[x]$$

and denote by C the left circulant matrix

$$C = \begin{bmatrix} a_0 & a_1 & \cdots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \cdots & a_{q-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q-2} & a_0 & \cdots & a_{q-4} & a_{q-3} \end{bmatrix}.$$

The number of nonzero solutions of the equation $f(x) = 0$ in $\mathbb{F}_q$ is equal to $q - 1 - \mathrm{rk}(C)$, where $\mathrm{rk}(C)$ is the rank of the matrix C.

We further extend the König-Rados Theorem to determine the number of roots of the polynomials occurring within a subfield.

Theorem 2.2. *Let q be a power of a prime, and let e, d be positive integers with d dividing e. Let*

$$f(x) = \sum_{s=0}^{q^e-2} a_s x^s \in \mathbb{F}_{q^e}[x],$$

and denote by C and B_d the matrices

$$C = \begin{bmatrix} a_0 & a_1 & \cdots & a_{q^e-3} & a_{q^e-2} \\ a_1 & a_2 & \cdots & a_{q^e-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q^e-2} & a_0 & \cdots & a_{q^e-4} & a_{q^e-3} \end{bmatrix}, \quad B_d = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ c_1 & c_2 & \cdots & c_{q^d-1} \\ c_1^2 & c_2^2 & \cdots & c_{q^d-1}^2 \\ \vdots & \vdots & & \vdots \\ c_1^{q^e-2} & c_2^{q^e-2} & \cdots & c_{q^d-1}^{q^e-2} \end{bmatrix},$$

where $c_1, c_2, \ldots, c_{q^d-1}$ are the distinct elements of $\mathbb{F}_{q^d}^*$. Then, the number of non-zero solutions of the equation $f(x) = 0$ in $\mathbb{F}_{q^d}$ is equal to $q^d - 1 - \mathrm{rk}(CB_d)$.

Proof. Let N_d be the number of solutions of $f(x) = 0$ occurring within $\mathbb{F}_{q^d}^*$. Let $c_1, c_2, \ldots, c_{q^d-1}$ be ordered so that $f(c_i) \neq 0$ for $1 \leq i \leq q^d - 1 - N_d$ and $c_{q^d-N_d}, c_{q^d-N_d+1}, \ldots, c_{q^d-1} \in \mathbb{F}_{q^d}^*$. Let the columns of B_d be ordered in this way. Since the elements of $\mathbb{F}_{q^d}^*$ which are solutions of $f(x) = 0$ appear in the final columns of B_d, the final N_d columns of CB_d are equal to 0 and the rank of CB_d is at most $q^d - 1 - N_d$.

Now consider the submatrix E of CB_d

$$E = \begin{bmatrix} f(c_1) & f(c_2) & \cdots & f(c_{q^d-1-N_d}) \\ c_1^{-1} f(c_1) & c_2^{-1} f(c_2) & \cdots & c_{q^d-1-N_d}^{-1} f(c_{q^d-1-N_d}) \\ c_1^{-2} f(c_1) & c_2^{-2} f(c_2) & \cdots & c_{q^d-1-N_d}^{-2} f(c_{q^d-1-N_d}) \\ \vdots & \vdots & & \vdots \\ c_1^{-(q^d-2-N_d)} f(c_1) & c_2^{-(q^d-2-N_d)} f(c_2) & \cdots & c_{q^d-1-N_d}^{-(q^d-2-N_d)} f(c_{q^d-1-N_d}) \end{bmatrix}.$$

The matrix E is non-singular since $\det(E) = f(c_1)f(c_2)\cdots f(c_{q^d-1-N_d}) \cdot \det(E')$, where E' is Vandermonde with defining row $(c_1^{-1}, c_2^{-1}, \ldots, c_{q^d-1-N_d}^{-1})$. Thus, $\mathrm{rk}(CB_d) = q^d - 1 - N_d$. □

We comment that if $e = d$, then $B_d = B$. Since B_d has full rank, $\mathrm{rk}(CB_d) = \mathrm{rk}(C)$, and Theorem 2.2 reduces to Theorem 2.1.

2.2 Linearized polynomials

Let $\mathbb{F}_{q^e}$ be the finite field with q^e elements. A *linearized polynomial* over $\mathbb{F}_{q^e}$ is a polynomial of the form

$$L(x) = \sum_{i=0}^{e-1} \alpha_i x^{q^i} \in \mathbb{F}_{q^e}[x].$$

An *affine polynomial over* $\mathbb{F}_{q^e}$ is given by $A(x) = L(x) + \alpha$, where $L(x)$ is a linearized polynomial over $\mathbb{F}_{q^e}$ and $\alpha \in \mathbb{F}_{q^e}$.

Note that every linearized polynomial L over $\mathbb{F}_{q^e}$ is indeed linear over $\mathbb{F}_q$. We can consider L as a linear operator $\mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$, when $\mathbb{F}_{q^e}$ is seen as a vector space over $\mathbb{F}_q$. For the remainder of this paper we use the notation $\mathbb{F}_{q^e}$ both to denote the finite field of degree e over $\mathbb{F}_q$ and to denote the vector space $\mathbb{F}_q^e$ over $\mathbb{F}_q$. In addition, we do not make the distinction between a linearized polynomial $L \in \mathbb{F}_{q^e}[x]$ and the linear operator $\mathbb{F}_q^e \to \mathbb{F}_q^e$.

It is well known when linearized polynomials define permutations over finite fields, see [6, Theorem 7.9]. We use a technique similar to an alternate discussion, given in [6, Page 362], to determine the value set of a linearized polynomial.

Theorem 2.3. *Let q be a power of a prime, and let e be a positive integer. Denote by $\mathbb{F}_{q^e}$ the finite field with q^e elements and let $L(x) = \sum_{s=0}^{e-1} \alpha_i x^{q^i}$ be a linearized polynomial over $\mathbb{F}_{q^e}$. Denote by M the $e \times e$ matrix*

$$\begin{bmatrix} \alpha_0 & \alpha_{e-1}^q & \cdots & \alpha_1^{q^{e-1}} \\ \alpha_1 & \alpha_0^q & \cdots & \alpha_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_{e-1} & \alpha_{e-2}^q & \cdots & \alpha_0^{q^{e-1}} \end{bmatrix}.$$

Then, L is a permutation polynomial if and only if $\det(M) \neq 0$, where $\det(M)$ denotes the determinant of the matrix M. Furthermore, the value set of L, denoted V_L, satisfies $|V_L| = q^{\mathrm{rk}(M)}$.

Proof. The statement of the theorem is proven in [6, Page 362], except for the final line. For the final assertion, we fix a basis $\{\beta_0, \beta_1, \ldots, \beta_{e-1}\}$ of $\mathbb{F}_{q^e}$ over $\mathbb{F}_q$ and let $\gamma_i = L(\beta_i)$, $i = 0, 1, \ldots, e-1$.

For $0 \leq i, j \leq e-1$ we have

$$\gamma_i^{q^j} = \sum_{s=0}^{e-1} \alpha_s^{q^j} \beta_i^{q^{s+j}},$$

and taking subscripts (mod e), we have

$$\gamma_i^{q^j} = \sum_{s=0}^{e-1} \alpha_{s-j}^{q^j} \beta_i^{q^s}.$$

We therefore have a matrix equation relating the conjugates of the γ_i, β_i and α_{s-j} of the following form

$$\begin{bmatrix} \gamma_0 & \gamma_0^q & \cdots & \gamma_0^{q^{e-1}} \\ \gamma_1 & \gamma_1^q & \cdots & \gamma_1^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \gamma_{e-1} & \gamma_{e-1}^q & \cdots & \gamma_{e-1}^{q^{e1}} \end{bmatrix}$$

$$= \begin{bmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{e-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{e-1} & \beta_{e-1}^q & \cdots & \beta_{e-1}^{q^{e-1}} \end{bmatrix} \begin{bmatrix} \alpha_0 & \alpha_{e-1}^q & \cdots & \alpha_1^{q^{e-1}} \\ \alpha_1 & \alpha_0^q & \cdots & \alpha_2^{q^{e-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_{e-1} & \alpha_{e-2}^q & \cdots & \alpha_0^{q^{e-1}} \end{bmatrix}.$$

Labelling the corresponding matrices Γ, B and M, respectively, by [6, Corollary 2.38], the matrix B is non-singular and thus the rank of Γ is equal to the rank of M. Since the value set of the linearized polynomial L is equal to the image set of the linear operator, we have $|V_L| = q^{\mathrm{rk}(M)}$. □

Corollary 2.4. *Let $L \in \mathbb{F}_{q^e}[x]$ be a linearized polynomial with value set of cardinality $q^{\mathrm{rk}(M)}$, as given in Theorem 2.3. Every image is repeated $q^{e-\mathrm{rk}(M)}$ times. Furthermore, $N_L(q^e; q^d) = |V_L(q^e; q^d)| q^{e-\mathrm{rk}(M)}$, where $N_L(q^e; q^d)$ denotes the total number of images of L in $\mathbb{F}_{q^d}$, including repetitions.*

Proof. Since L defines a linear operator $\mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$, we have, by the first isomorphism theorem, $\mathbb{F}_{q^e}/\ker(L) \cong V_L$. Since $\dim(\ker(L)) = e - \mathrm{rk}(M)$, the claim follows. □

Suppose $L \in \mathbb{F}_{q^e}[x]$ is a linearized polynomial and let $A(x) = L(x) + \alpha$, for some $\alpha \in \mathbb{F}_{q^e}$. Consider the subfield value set of A, $V_A(q^e; q^d)$, for any d dividing e. We have trivially that $|V_A(q^e; q^e)| = |V_L(q^e; q^e)|$. If $\alpha \in \mathbb{F}_{q^d}$, then $|V_A(q^e; q^d)| = |V_L(q^e; q^d)|$.

Example 2.5. *Let $L(x) = Tr_d(x)$. Then L is a linearized polynomial and L maps $\mathbb{F}_{q^e}$ onto $\mathbb{F}_{q^d}$. Let $\alpha \in \mathbb{F}_{q^e}$ with $\alpha \notin \mathbb{F}_{q^d}$ and let $A(x) = L(x) + \alpha$. Then $V_A(q^e; q^d) = \emptyset$.*

If $\alpha \in V_L(q^e; q^e)$, that is, if α is an image of L, then for all $\beta \in \mathbb{F}_{q^e}$, $A(\beta) = L(\beta) + \alpha = L(\beta + \gamma)$, where $\alpha = L(\gamma)$. Thus, running over all $\beta \in \mathbb{F}_{q^e}$, we have that $V_L(q^e; q^d) = V_A(q^e; q^d)$ for all d dividing e. If α is not an image of L, then the subfield value set of A depends on the additive cosets of the subfield value set of L. It can be easily verified with a computer algebra program, such as SAGE or Maple, that the cardinalities of subfield value sets of affine polynomials most often vary from the subfield value sets of their corresponding linearized polynomials.

Lemma 2.6. *Let q be a power of a prime, and let e be a positive integer. Let $\mathbb{F}_{q^e}$ be the finite field with q^e elements and let L be a linearized polynomial over $\mathbb{F}_{q^e}$ defined by $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$. Then*

$$N_L(q^e; q^d) = \left| \left\{ \beta : \sum_{i=0}^{e-1} \left(a_{e-d+i}^{q^d} - a_i \right) \beta^{q^i} = 0 \right\} \right|$$

and

$$|V_L(q^e; q^d)| = N_L(q^e; q^d)/q^{e-\mathrm{rk}(M)},$$

where M is the matrix given in Theorem 2.3.

Proof. Let

$$L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$$

and suppose that $L(\alpha)$ lies in $\mathbb{F}_{q^d}$. That is,

$$L(\alpha)^{q^d} = \sum_{i=0}^{e-1} a_i^{q^d} \alpha^{q^{i+d}} = L(\alpha) = \sum_{i=0}^{e-1} a_i \alpha^{q^i}.$$

Rearranging, we find

$$\sum_{i=0}^{e-1} a_i^{q^d} \alpha^{q^{i+d}} - \sum_{i=0}^{e-1} a_i \alpha^{q^i} = \sum_{i=0}^{e-1} (a_{e-d+i}^{q^d} - a_i) \alpha^{q^i} = 0,$$

where the subscripts are taken $\pmod e$. Thus $L(\alpha)$ lies in the subfield $\mathbb{F}_{q^d}$ of $\mathbb{F}_{q^e}$ if and only if α is a root of the polynomial

$$b(x) = \sum_{i=0}^{e-1} (a_{e-d+i}^{q^d} - a_i) x^{q^i}. \tag{2.1}$$

The final expression for $|V_L(q^e; q^d)|$ is given by Corollary 2.4. $\square$

Counting the number of zeroes of the polynomial b in Equation (2.1) can be done by the König-Rados theorem, see Theorem 2.1.

Theorem 2.7. *Let L be a linearized polynomial over $\mathbb{F}_{q^e}$ given by $L(x) = \sum_{i=0}^{q^e-1} a_i x^i$, that is $a_j = 0$ for $j \neq 1, q, q^2, \ldots, q^{e-1}$. Let C be the left-circulant matrix of size $q^e - 1$ with defining row*

$$\left[0 \; b_0 \; \underbrace{0 \cdots 0}_{q-2 \text{ times}} \; b_1 \; \underbrace{0 \cdots 0}_{q^2-q-1 \text{ times}} \; b_2 \cdots b_{e-2} \; \underbrace{0 \cdots 0}_{q^{e-1}-q^{e-2}-1 \text{ times}} \; b_{e-1} \; \underbrace{0 \cdots 0}_{q^e-q^{e-1}-2 \text{ times}}\right],$$

where b_0 are the coefficients of b in Equation (2.1). *Then,*

$$|V_L(q^e; q^d)| = \frac{q^e - \mathrm{rk}(C)}{q^{e-\mathrm{rk}(M)}},$$

where M is given by Corollary 2.4.

Proof. Theorem 2.1 gives the number of non-zero roots of b is $q^e - 1 - \mathrm{rk}(C)$. Since 0 is a root of b, the claim follows. □

3 Power polynomials

We now consider the subfield value set $V_{x^n}(q^e; q^d)$ of the polynomial $f(x) = x^n$. Power polynomials are a special case of Dickson polynomial $D_n(x, a)$ with $a = 0$, as we will see in the next section. It is well known and easy to see that

$$|V_{x^n}(q^e; q^e)| = \frac{q^e - 1}{(n, q^e - 1)} + 1.$$

We first show the number of preimages of the subfield value set of a power polynomial.

Theorem 3.1. *The number of preimages of the power polynomial x^n is given by $N_{x^n}(q^e; q^d) = (n(q^d - 1), q^e - 1)) + 1$.*

Proof. Recall that if $\alpha \in \mathbb{F}_{q^e}$, then $\alpha \in \mathbb{F}_{q^d}$ if and only if $\alpha^{q^d} = \alpha$. For $c \in \mathbb{F}_{q^e}^*$, if $(c^n)^{q^d} = c^n$, we have $c^{n(q^d-1)} = 1$. The number of solutions of this equation for $c \in \mathbb{F}_{q^e}^*$, is given by $(n(q^d - 1), q^e - 1)$, and the result follows. □

Since the multiplicative group $\mathbb{F}_{q^e}^*$ is cyclic, we have in $\mathbb{F}_{q^e}^*$

$$|V_{x^n}(q^e; q^d)| = \frac{N_{x^n}(q^e; q^d)}{(n, q^e - 1)} + 1 = \frac{(n(q^d - 1), q^e - 1)}{(n, q^e - 1)} + 1.$$

We note that if $(n, q^e - 1) = 1$ so that x^n is a permutation polynomial on $\mathbb{F}_{q^e}$, then $|V_{x^n}(q^e; q^d)| = N_{x^n}(q^e; q^d) = q^d$ since x^n must map $\mathbb{F}_{q^d}$ onto itself. In fact, if $(n, q^d - 1) = 1$, then x^n is a permutation polynomial on $\mathbb{F}_{q^d}$ and so $|V_{x^n}(q^e; q^d)| = q^d$.

4 Dickson polynomials

For $a \in \mathbb{F}_{q^e}$, the Dickson polynomial $D_n(x,a)$ of degree n and parameter a is defined by

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

Dickson polynomials have been studied extensively since they play very important roles in the theory of permutation polynomials over finite fields, and in the Schur conjecture; see [5]. In [4], the use of Dickson polynomials in cryptographic systems, particularly over finite fields, is generalized by considering Dickson polynomials over Galois rings. Dickson polynomials have many properties which are closely related to properties of the power polynomial $x^n = D_n(x,0)$, see [5]. For example, for $a \in \mathbb{F}_q^*$, $D_n(x,a)$ induces a permutation on the field $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$. Moreover, from [1] we have

$$|V_{D_n(x,a)}(q;q)| = \frac{q-1}{2(n,q-1)} + \frac{q+1}{2(n,q+1)} + \alpha,$$

where α can be explicitly stated and is usually 0. In [3], if n is odd and n divides $q-1$, it was shown that $N_{D_n(x,1)}(q^2;q) = (q(n+1)-(n-1))/2$, and $N_{D_{q-1}(x,1)}(q^2;q) = (q^2+1)/2$.

Let $a \in \mathbb{F}_{q^e}^*$. If $c \in \mathbb{F}_{q^e}$, then we can write $c = y + a/y$ for some $y \in \mathbb{F}_{q^{2e}}$, and we obtain a functional equation for Dickson polynomials, $D_n(c,a) = y^n + a^n/y^n$. Thus, in order to have the image $D_n(c,a)$ in the subfield $\mathbb{F}_{q^d}$, we must have

$$\left(y^n + \frac{a^n}{y^n}\right)^{q^d} = y^n + \frac{a^n}{y^n}. \tag{4.1}$$

If $a^n \in \mathbb{F}_{q^d}$, Equation (4.1) becomes, after simplification,

$$(y^{n(q^d-1)} - 1)(y^{n(q^d+1)} - a^n) = 0; \tag{4.2}$$

that is, either $y^{n(q^d-1)} = 1$ or $y^{n(q^d+1)} = a^n$. The following lemma is essential but has an elementary proof which is omitted.

Lemma 4.1. *For $a \in \mathbb{F}_{q^e}^*$, let C_a be the set $C_a = \{y + a/y : y \in \mathbb{F}_{q^e}^*$ or $y^{q^e+1} = a\}$. Then, $C_a = \mathbb{F}_{q^e}$.*

We consider only the case $a^n \in \mathbb{F}_{q^d}$, for otherwise, when $a^n \notin \mathbb{F}_{q^d}$, Equation (4.1) does not seem to lead to a convenient factorization as in Equation (4.2); see Section 5. We derive $|V_{D_n(x,a)}(q^e;q^d)|$ in detail for q odd and note that the derivation for q even is similar and therefore omitted.

Let q be odd. In the following lemma, η_{q^ℓ} is the quadratic character on $\mathbb{F}_{q^\ell}$, so that $\eta_{q^\ell}(a) = 1$ if $a \in \mathbb{F}_{q^\ell}^*$ is a non-zero square and $\eta_{q^\ell}(a) = -1$ if $a \in \mathbb{F}_{q^\ell}^*$ is not a square. Moreover $\sqrt{a}$ is a square root in $\mathbb{F}_{q^{2\ell}}$ of $a \in \mathbb{F}_{q^\ell}^*$. For any number m, let r_m be the non-negative integer satisfying $2^{r_m}||m$, that is, r_m is the highest non-negative power of 2 dividing m.

Lemma 4.2. *Let $\mathbb{F}_{q^d}$ be a subfield of $\mathbb{F}_{q^e}$ with q odd. If $a^n \in \mathbb{F}_{q^d}^*$, then $c \in V_{D_n(x,a)}(q^e; q^d)$ if and only if $c = y^n + a^n/y^n$, where y satisfies at least one of the following requirements:*

I. $y^{(q^e-1,n(q^d-1))} = 1$,

II. *a. for* $\eta_{q^e}(a) = 1$ *and* $\eta_{q^d}(a^n) = 1$,

1. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d-1))} = 1$,
2. $(\frac{y}{\sqrt{a}})^{(q^e-1,n(q^d+1))} = 1$,
3. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d+1))} = 1$,

b. for $\eta_{q^e}(a) = -1$ *and* $\eta_{q^d}(a^n) = 1$,

1. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d-1))} = -1$ *and* $r_{q^e+1} < r_{n(q^d-1)}$,
2. $(\frac{y}{\sqrt{a}})^{(q^e-1,n(q^d+1))} = -1$ *and* $r_{q^e-1} < r_{n(q^d+1)}$,
3. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d+1))} = -1$ *and* $r_{q^e+1} < r_{n(q^d+1)}$,

c. for $\eta_{q^e}(a) = 1$ *and* $\eta_{q^d}(a^n) = -1$,

1. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d-1))} = -1$ *and* $r_{n(q^d-1)} < r_{q^e+1}$,
2. $(\frac{y}{\sqrt{a}})^{(q^e-1,n(q^d+1))} = -1$ *and* $r_{n(q^d+1)} < r_{q^e-1}$,
3. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d+1))} = -1$ *and* $r_{n(q^d+1)} < r_{q^e+1}$,

d. for $\eta_{q^e}(a) = -1$ *and* $\eta_{q^d}(a^n) = -1$,

1. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d-1))} = -1$ *and* $r_{q^e+1} = r_{n(q^d-1)}$,
2. $(\frac{y}{\sqrt{a}})^{(q^e-1,n(q^d+1))} = -1$ *and* $r_{q^e-1} = r_{n(q^d+1)}$,
3. $(\frac{y}{\sqrt{a}})^{(q^e+1,n(q^d+1))} = -1$ *and* $r_{q^e+1} = r_{n(q^d+1)}$.

Proof. By Lemma 4.1, $\{D_n(c,a) : c \in \mathbb{F}_{q^e}\} = \{y^n + (a/y)^n \colon y \in \mathbb{F}_{q^e}$ or $y^{q^e+1} = a\}$. Since $a^n \in \mathbb{F}_{q^d}$, $y^n + (a/y)^n \in V_{D_n(x,a)}(q^e; q^d)$ if and only if $y^{q^e-1} = 1$ or $y^{q^e+1} = a$ and $y^{n(q^d-1)} = 1$ or $y^{n(q^d+1)} = a^n$ by Equation (4.2).

If $y^{q^e-1} = 1$ and $y^{n(q^d-1)} = 1$, then $y^{\left(q^e-1,n(q^d-1)\right)} = 1$ and Case **I.** holds. In Case **II**, we prove only (b.1). All other cases can be proved in similar ways.

Suppose $\eta_{q^d}(a^n) = 1$ and $\eta_{q^e}(a) = -1$. Then $(\sqrt{a})^{n(q^d-1)} = 1$ and $(\sqrt{a})^{q^e-1} = -1$. The last equality is equivalent to $(\sqrt{a})^{q^e+1} = -a$.

(Case II.b.1). Suppose $y^{q^e+1} = a$ and $y^{n(q^d-1)} = 1$. These two equations are equivalent to $\left(\frac{y}{\sqrt{a}}\right)^{q^e+1} = -1$ and $\left(\frac{y}{\sqrt{a}}\right)^{n(q^d-1)} = 1$, respectively. Thus, $\left(\frac{y}{\sqrt{a}}\right)^{(2(q^e+1),n(q^d-1))} = 1$ but $\left(\frac{y}{\sqrt{a}}\right)^{(q^e+1,n(q^d-1))} = -1$, and so $r_{q^e+1} < r_{n(q^d-1)}$. □

We can now evaluate $N_{D_n(x,a)}(q^e; q^d)$.

Theorem 4.3. *Let q be odd and let $a \in \mathbb{F}_{q^e}$ with $a^n \in \mathbb{F}_{q^d}$. For integers m and k, let $\delta_{m<k} = 1$, if $m < k$, and $\delta_{m<k} = 0$, if $m \geq k$. Also, let $\delta_{m=k} = 1$, if $m = k$, and $\delta_{m=k} = 0$, if $m \neq k$.*

a. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = 1$, then*

$$\begin{aligned}
&N_{D_n(x,a)}(q^e; q^d)\\
&= \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1)) - (q^e-1, 2n)}{2}\\
&+ \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1)) - (q^e+1, 2n)}{2}.
\end{aligned}$$

b. *If $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = 1$, then*

$$\begin{aligned}
&N_{D_n(x,a)}(q^e; q^d)\\
&= \frac{(q^e-1, n(q^d-1)) + \delta_{r_{q^e-1}<r_{n(q^d+1)}}(q^e-1, n(q^d+1))}{2}\\
&+ \frac{-(1-\delta_{r_n<r_{q^e-1}})(q^e-1, n) + \delta_{r_{q^e+1}<r_{n(q^d-1)}}(q^e+1, n(q^d-1))}{2}\\
&+ \frac{\delta_{r_{q^e+1}<r_{n(q^d+1)}}(q^e+1, n(q^d+1)) - (1-\delta_{r_n<r_{q^e+1}})(q^e+1, n)}{2}.
\end{aligned}$$

c. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = -1$, then*

$$\begin{aligned}
&N_{D_n(x,a)}(q^e; q^d)\\
&= \frac{(q^e-1, n\left(q^d-1\right)) + \delta_{r_{n(q^d+1)}<r_{q^e-1}}(q^e-1, n(q^d+1))}{2}\\
&+ \frac{\delta_{r_{n(q^d-1)}<r_{q^e+1}}(q^e+1, n(q^d-1)) + \delta_{r_{n(q^d+1)}<r_{q^e+1}}(q^e+1, n(q^d+1))}{2}.
\end{aligned}$$

d. *If $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = -1$, then*

$$\begin{aligned}
&N_{D_n(x,a)}(q^e; q^d)\\
&= \frac{(q^e-1, n(q^d-1)) + \delta_{r_{q^e-1}=r_{n(q^d+1)}}(q^e-1, n(q^d+1))}{2}\\
&+ \frac{\delta_{r_{q^e+1}=r_{n(q^d-1)}}(q^e+1, n(q^d-1)) + \delta_{r_{q^e+1}=r_{n(q^d+1)}}(q^e+1, n(q^d+1))}{2}.
\end{aligned}$$

Proof. We prove this theorem according to the cases in Lemma 4.2. We only prove Case **b.** and comment that the proof of this case is a typical example of the proofs of the remaining cases.

(Case b.) $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = 1$. Let

$$E_1 = \left\{ y \in \mathbb{F}_{q^e} : y^{\left(q^e-1, n(q^d-1)\right)} = 1 \right\},$$
$$E_2 = \left\{ y \in \mathbb{F}_{q^{2e}} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e+1, n(q^d-1)\right)} = -1 \text{ and } r_{q^e+1} < r_{n(q^d-1)} \right\},$$
$$E_3 = \left\{ y \in \mathbb{F}_{q^e} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e-1, n(q^d+1)\right)} = -1 \text{ and } r_{q^e-1} < r_{n(q^d-1)} \right\}, \text{ and}$$
$$E_4 = \left\{ y \in \mathbb{F}_{q^{2e}} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e+1, n(q^d+1)\right)} = -1 \text{ and } r_{q^e+1} < r_{n(q^d+1)} \right\}.$$

The definition of E_1 comes from Case **I.** of Lemma 4.2. We note that $|E_1| = (q^e-1, n(q^d-1))$, $|E_2| = (q^e+1, n(q^d-1))$, $|E_3| = (q^e-1, n(q^d+1))$, and $|E_4| = (q^e+1, n(q^d+1))$.

For $y \in E_2$, y can be written as $y = u\sqrt{a}$ with $u^{\left(2(q^e+1), n(q^d-1)\right)} = 1$ and $u^{q^e+1} = -1$. This implies that $2^{r_{2(q^e+1)}}$ divides the order of u. Moreover, if $y \in E_3$, then $2^{r_{2(q^e-1)}}$ divides the order of u. Since either $q^e - 1 \equiv 0 \pmod 4$ or $q^e + 1 \equiv 0 \pmod 4$, 8 divides the order of u. However $u^{2(q^e+1)} = 1 = u^{2(q^e-1)}$ would imply $u^4 = 1$, a contradiction. So, $E_2 \bigcap E_3 = \varnothing$. Similar arguments show that $E_1 \bigcap E_2 = E_1 \bigcap E_4 = E_3 \bigcap E_4 = \varnothing$.

Let $y = u\sqrt{a}$. Then $y \in E_2 \bigcap E_4$ if and only if $u^{\left(2(q^e+1), n(q^d-1)\right)} = 1$, $u^{q^e+1} = -1$ and $u^{(2(q^e+1), n(q^d+1))} = 1$. These are equivalent to $u^{(2(q^e+1), 2n)} = 1$ and $u^{q^e+1} = -1$. So, if $r_{q^e+1} > r_n$, then $|E_2 \bigcap E_4| = 0$, while if $r_{q^e+1} \le r_n$, then $|E_2 \bigcap E_4| = (q^e+1, n)$. By similar arguments, we have that $|E_1 \bigcap E_3| = 0$ if $r_{q^e-1} > r_n$, and $|E_1 \bigcap E_3| = (q^e-1, n)$ if $r_{q^e-1} \le r_n$.

Combining all of the results above together, we have, by the inclusion-exclusion principle,

$$N_{D_n(x,a)}(q^e; q^d) = \frac{|E_1 \bigcup E_2 \bigcup E_3 \bigcup E_4|}{2}$$
$$= \frac{(q^e-1, n(q^d-1)) + \delta_{r_{q^e-1} < r_{n(q^d-1)}}(q^e-1, n(q^d+1))}{2}$$
$$+ \frac{-(1-\delta_{r_n < r_{q^e-1}})(q^e-1, n) + \delta_{r_{q^e+1} < r_{n(q^d-1)}}(q^e+1, n(q^d-1))}{2}$$
$$+ \frac{\delta_{r_{q^e+1} < r_{n(q^d+1)}}(q^e+1, n(q^d+1)) - (1-\delta_{r_n < r_{q^e+1}})(q^e+1, n)}{2}.$$

This completes the proof. □

The result of Theorem 4.3, Case **a**. is a generalization of the results in [3] stated before. Indeed, if n is an odd divisor of $q-1$ (and so n properly divides $q-1$), then $(q^2-1, n(q-1)) = (q-1)(q+1, n) = q-1$, $(q^2-1, n(q+1)) = n(q+1)$, $(q^2-1, 2n) = 2n$, and $(q^2+1, n(q-1)) = 2 = (q^2+1, n(q+1)) = (q^2+1, 2n)$. So, $N_{D_n(x,1)}(q^2; q) = (q(n+1)-(n-1))/2$. Moreover, in the case $n = q-1$, we obtain $N_{D_{q-1}(x,1)}(q^2; q) = (q^2+1)/2$ using similar arguments.

We are now ready to compute $|V_{D_n(x,a)}(q^e; q^d)|$ with $a^n \in \mathbb{F}_{q^d}$.

Theorem 4.4. *Let q be odd and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. For integers m and k, let $\delta_{m<k} = 1$, if $m < k$, and $\delta_{m<k} = 0$, if $m \geq k$. Also, let $\delta_{m=k} = 1$, if $m = k$, and $\delta_{m=k} = 0$, if $m \neq k$. Suppose that $2^r || (q^{2e}-1)$.*

a. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = 1$, then $|V_{D_n(x,a)}(q^e; q^d)| =$*

$$\frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - \frac{3+(-1)^{n+1}}{2}.$$

b. *If $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = 1$, then $|V_{D_n(x,a)}(q^e; q^d)| =$*

$$-\delta_{r-1<r_n} + \frac{(q^e-1, n(q^d-1)) + \delta_{r_{q^e-1}<r_{n(q^d+1)}}(q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{\delta_{r_{q^e+1}<r_{n(q^d-1)}}(q^e+1, n(q^d-1)) + \delta_{r_{q^e+1}<r_{n(q^d+1)}}(q^e+1, n(q^d+1))}{2(q^e+1, n)}.$$

c. *If $\eta_{q^e}(a) = 1$ and $\eta_{q^d}(a^n) = -1$, then $|V_{D_n(x,a)}(q^e; q^d)| =$*

$$\frac{(q^e-1, n(q^d-1)) + \delta_{r_{n(q^d+1)}<r_{q^e-1}}(q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{\delta_{r_{n(q^d-1)}<r_{q^e+1}}(q^e+1, n(q^d-1)) + \delta_{r_{n(q^d+1)}<r_{q^e+1}}(q^e+1, n(q^d+1))}{2(q^e+1, n)}.$$

d. *If $\eta_{q^e}(a) = -1$ and $\eta_{q^d}(a^n) = -1$, then $|V_{D_n(x,a)}(q^e; q^d)| =$*

$$\frac{(q^e-1, n(q^d-1)) + \delta_{r_{q^e-1}=r_{n(q^d+1)}}(q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{\delta_{r_{q^e+1}=r_{n(q^d-1)}}(q^e+1, n(q^d-1)) + \delta_{r_{q^e+1}=r_{n(q^d+1)}}(q^e+1, n(q^d+1))}{2(q^e+1, n)}.$$

Proof. We prove only Case **a.** The proofs of the remaining cases are similar.

Let

$$E_1 = \left\{ y \in \mathbb{F}_{q^e} : y^{\left(q^e-1, n(q^d-1)\right)} = 1 \right\},$$

$$E_2 = \left\{ y \in \mathbb{F}_{q^{2e}} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e+1, n(q^d-1)\right)} = 1 \right\},$$

$$E_3 = \left\{ y \in \mathbb{F}_{q^e} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e-1, n(q^d+1)\right)} = 1 \right\}, \text{ and}$$

$$E_4 = \left\{ y \in \mathbb{F}_{q^{2e}} : \left(\frac{y}{\sqrt{a}}\right)^{\left(q^e+1, n(q^d+1)\right)} = 1 \right\}.$$

Similar to the proof of Theorem 4.3, we have $y = u\sqrt{a} \in E_1 \bigcap E_3$ if and only if the order of u divides $(q^e - 1, 2n)$ and $y = u\sqrt{a} \in E_2 \bigcap E_4$ if and only if the order of u divides $(q^e + 1, 2n)$. In both situations, we have $y^n = (a/y)^n$. From [1, Lemma 7], for $x_0 = y_0 + a/y_0$, $y_0 \in (E_1 \bigcap E_3) \bigcup (E_2 \bigcap E_4)$ if and only if $D_n(x_0, a) = \pm 2a^{n/2}$.

Every element $x_0 = y_0 + a/y_0$ with $y_0 \in (E_1 \bigcup E_3) \setminus (E_1 \bigcap E_3)$ satisfies $\eta_{q^e}(x_0^2 - 4a) = 1$ and $D_n(x_0, a) \neq 2a^{n/2}$. From [1, Theorem 9], the total number I_1 of images $D_n(x_0, a)$ with $x_0 = y_0 + a/y_0$ for all $y_0 \in (E_1 \bigcup E_3) \setminus (E_1 \bigcap E_3)$ is

$$I_1 = \frac{(q^e - 1, n(q^d - 1)) + (q^e - 1, n(q^d + 1)) - 2(q^e - 1, 2n)}{2(q^e - 1, n)}.$$

Similarly, the total number I_2 of images $D_n(x_0, a)$ with $x_0 = y_0 + a/y_0$ for all $y_0 \in (E_2 \bigcup E_4) \setminus (E_2 \bigcap E_4)$ is

$$I_2 = \frac{(q^e + 1, n(q^d - 1)) + (q^e + 1, n(q^d + 1)) - 2(q^e + 1, 2n)}{2(q^e + 1, n)}.$$

We have seen that $|E_1 \bigcap E_3| = (q^e - 1, 2n)$, $|E_2 \bigcap E_4| = (q^e + 1, 2n)$, and $(E_1 \bigcap E_3) \bigcap (E_2 \bigcap E_4) = \{\pm\sqrt{a}\}$. Let t, r satisfy $2^t || n$ and $2^r || (q^{2e-1} - 1)$, respectively. If $1 \le t \le r - 2$, then either $(q^e - 1, 2n) = 2(q^e - 1, n)$ and $(q^e + 1, 2n) = (q^e + 1, n)$ or $(q^e - 1, 2n) = (q^e - 1, n)$ and $(q^e + 1, 2n) = 2(q^e + 1, n)$. Furthermore, $(q^e - 1, 2n) = 2(q^e - 1, n)$ and $(q^e + 1, 2n) = 2(q^e + 1, n)$ if $t = 0$, while $(q^e - 1, 2n) = (q^e - 1, n)$ and $(q^e + 1, 2n) = (q^e + 1, n)$ if $t \ge r - 1$.

For $x_0 = y_0 + a/y_0 \in \mathbb{F}_{q^e}$, if $y_0 \in E_1 \bigcap E_3$, then $\eta_{q^e}(x_0^2 - 4a) = 1$, while if $\pm\sqrt{a} \neq y_0 \in E_2 \bigcap E_4$, then $\eta_{q^e}(x_0^2 - 4a) = -1$. Moreover, every element $y_0 \in E_1 \bigcap E_3$ can be written as $y_0 = u\sqrt{a}$ with $u^{(q^e-1,2n)} = 1$.

So, if $x_0 = y_0 + a/y_0 \in \mathbb{F}_{q^e}$ with $y_0 \in E_1 \bigcap E_3$, then $D_n(x_0, a) = y_0^n + a^n/y_0^n = 2u^{(q^e-1,n)}(\sqrt{a})^n$. Hence, if $(q^e-1, 2n) = (q^e-1, n)$, then for all elements $y_0 \in E_1 \bigcap E_3$, $D_n(y_0 + a/y_0, a) = 2(\sqrt{a})^n$. If $(q^e-1, 2n) = 2(q^e-1, n)$, then for half of elements $y_0 \in E_1 \bigcap E_3$, $D_n(y_0 + a/y_0, a) = 2(\sqrt{a})^n$ and for all other elements $y_0 \in E_1 \bigcap E_3$, $D_n(y_0 + a/y_0, a) = -2(\sqrt{a})^n$. Similarly, if $(q^e+1, 2n) = (q^e+1, n)$ then for all elements $y_0 \in E_2 \bigcap E_4$, $D_n(y_0 + a/y_0, a) = 2(\sqrt{a})^n$, and if $(q^e+1, 2n) = 2(q^e+1, n)$ then for half of elements $y_0 \in E_2 \bigcap E_4$, $D_n(y_0 + a/y_0, a) = 2(\sqrt{a})^n$ and for all other elements $y_0 \in E_2 \bigcap E_4$, $D_n(y_0 + a/y_0, a) = -2(\sqrt{a})^n$. Combining all of these results together, we have, from [1, Theorem 9], that the total number I_3 of images $D_n(y_0 + a/y_0, a)$ with $y_0 \in (E_1 \bigcap E_3) \bigcap (E_2 \bigcap E_4)$ equals either 1 if $2^t || n$ and $t \geq r-1$, or 2 otherwise.

We have for the value set $|V_{D_n(x,a)}(q^e; q^d)| = I_1 + I_2 + I_3$. We now compute $|V_{D_n(x,a)}(q^e; q^d)|$ according to the value of t.

Case 1: $t = 0$ (n is odd). We have $(q^e-1, 2n) = 2(q^e-1, n)$, $(q^e+1, 2n) = 2(q^e+1, n)$ and $I_3 = 2$. From the result above, we have

$$\begin{aligned}
|V_{D_n(x,a)}(q^e; q^d)| =& 2 + \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1)) - 2(q^e-1, 2n)}{2(q^e-1, n)} \\
&+ \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1)) - 2(q^e+1, 2n)}{2(q^e+1, n)} \\
=& \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} \\
&+ \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - 2.
\end{aligned}$$

Case 2: $1 \leq t \leq r-2$. We have either $(q^e-1, 2n) = 2(q^e-1, n)$ and $(q^e+1, 2n) = (q^e+1, n)$, or $(q^e-1, 2n) = (q^e-1, n)$ and $(q^e+1, 2n) = 2(q^e+1, n)$. In this case, $I_3 = 2$ and

$$\begin{aligned}
I_1 + I_2 =& \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} \\
&+ \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - 3.
\end{aligned}$$

Thus,

$$\begin{aligned}
|V_{D_n(x,a)}(q^e; q^d)| =& \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} \\
&+ \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - 1.
\end{aligned}$$

Case 3: $t \geq r-1$. We have $(q^e-1, 2n) = (q^e-1, n)$, $(q^e+1, 2n) = (q^e+1, n)$ and $I_3 = 1$. Therefore, the value set satisfies

$$|V_{D_n(x,a)}(q^e; q^d)| = \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - 1.$$

This completes the proof. □

The following corollary is the most important special case, which appears as [1, Theorem 10].

Corollary 4.5. *Let q be odd and let $a \in \mathbb{F}_q^*$. Suppose that $2^r || (q^2-1)$. Then we have*

$$|V_{D_n(x,a)}(q; q)| = \frac{q-1}{2(n, q-1)} + \frac{q+1}{2(n, q+1)} + \alpha,$$

where

$$\alpha = \begin{cases} 1 & \text{if } 2^{e-1} || n \text{ and } \eta_q(a) = -1, \\ \frac{1}{2} & \text{if } 2^t || n \text{ with } 1 \leq t \leq r-2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This is a special case of Theorem 4.4 with $q^e = q^d = q$. Determining the value of α depends on the parity of n and the value of $\eta_q(a)$; the details are omitted. □

We now state the results of $N_{D_n(x,a)(q^e;q^d)}$ and $|V_{D_n(x,a)}(q^e; q^d)|$ for q even. The derivation of these results is similar, but slightly simpler, to those of q odd and is therefore omitted.

Theorem 4.6. *Let q be even and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. Then*

$$N_{D_n(x,a)}(q^e; q^d) = \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1)) - (q^e-1, n)}{2} + \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1)) - (q^e+1, n)}{2}.$$

Theorem 4.7. *Let q be even and let $a \in \mathbb{F}_{q^e}^*$ with $a^n \in \mathbb{F}_{q^d}$. Then*

$$|V_{D_n(x,a)}(q^e; q^d)| = \frac{(q^e-1, n(q^d-1)) + (q^e-1, n(q^d+1))}{2(q^e-1, n)} + \frac{(q^e+1, n(q^d-1)) + (q^e+1, n(q^d+1))}{2(q^e+1, n)} - 1.$$

Corollary 4.8. *Let q be even and let $a \in \mathbb{F}_q^*$. Then we have*

$$|V_{D_n(x,a)}(q; q)| = \frac{q-1}{2(n, q-1)} + \frac{q+1}{2(n, q+1)}.$$

5 Open problem

We conclude with an open problem. In all of our work concerning Dickson polynomials, we have assumed that the parameter a has the property that $a^n \in \mathbb{F}_{q^d}$. The reason for this assumption is that in this case, Equation (4.1) leads to the simple factorization in Equation (4.2). For this equation, we are able to calculate the number of solutions to each factor as well as the number of solutions which simultaneously satisfy both factors.

For $a^n \notin \mathbb{F}_{q^d}$, we do not know how to find $\left|V_{D_n(x,a)}(q^e;q^d)\right|$ in general. However, we know that if $\gcd(n, q^{2e}-1) = 1$, then $|V_{D_n(x,a)}(q^e;q)| = q = N_{D_n(x,a)}(q^e;q)$ because $D_n(x,a)$ is a permutation polynomial over $\mathbb{F}_{q^e}$. The following is an example in the other extreme case, namely $|V_{D_n(x,a)}(q^e;q)| = 0 = N_{D_n(x,a)}(q^e;q)$.

Proposition 5.1. *Let $q \equiv 7 \pmod 8$ be a prime power and let $a \in \mathbb{F}_{q^2}^*$ be a primitive element of $\mathbb{F}_{q^2}$. Then $|V_{D_{(q-1)(q^2+1)}(x,a)}(q^2;q)| = 0$.*

Proof. Since $a \in \mathbb{F}_{q^2}^*$ is a primitive element, $a^{(q-1)(q^2+1)} \notin \mathbb{F}_q$. At first, we consider $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right)$ with $y \in \mathbb{F}_{q^2}^*$. In this case, $y^{q^2-1}=1$ and so we have $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right) = y^{(q-1)(q^2+1)} + \frac{a^{(q-1)(q^2+1)}}{y^{(q-1)(q^2+1)}} = y^{2(q-1)} + \frac{a^{2(q-1)}}{y^{2(q-1)}}$. Hence, $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right) \in \mathbb{F}_q$ if and only if

$$\begin{aligned} y^{2(q-1)} + \frac{a^{2(q-1)}}{y^{2(q-1)}} &= \left(y^{2(q-1)} + \frac{a^{2(q-1)}}{y^{2(q-1)}}\right)^q = y^{2(q^2-q)} + \frac{a^{2(q^2-q)}}{y^{2(q^2-q)}} \\ &= y^{-2(q-1)} + \frac{a^{-2(q-1)}}{y^{-2(q-1)}} = \frac{1}{a^{2(q-1)}}\left(y^{2(q-1)} + \frac{a^{2(q-1)}}{y^{2(q-1)}}\right). \end{aligned}$$

This implies that $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right) \in \mathbb{F}_q$ if and only if either $a^{2(q-1)} = 1$ or $y^{4(q-1)} = -a^{2(q-1)}$. We have that $a^{2(q-1)} = 1$ cannot hold because a is primitive in $\mathbb{F}_{q^2}$. Also, $y^{4(q-1)} = -a^{2(q-1)}$ cannot hold because a is primitive in $\mathbb{F}_{q^2}$ and $-a^{2(q-1)} = a^{(q-1)(2+(q+1)/2)}$ with the fact that $2 + \frac{q+1}{2} \equiv 2 \pmod 4$ from $q \equiv 7 \pmod 8$. So, what we have shown is that $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right) \notin \mathbb{F}_q$ in this case.

Finally, we consider $y^{q^2+1} = a$. In this case, $D_{(q-1)(q^2+1)}\left(y+\frac{a}{y},a\right) = y^{(q-1)(q^2+1)} + \frac{a^{(q-1)(q^2+1)}}{y^{(q-1)(q^2+1)}} = 2a^{q-1}$, is trivally not in $\mathbb{F}_q$. Combining this with the result above, we have $|V_{D_{(q-1)(q^2+1)}(x,a)}(q^2;q)| = 0$. □

In general, $a \in \mathbb{F}_{q^e}$ is such that $a^n \notin \mathbb{F}_{q^d}$, then Equation (4.1) seems to not yield a simple factorization like that occurring in Equation (4.2). In such a setting, how does one proceed to calculate the cardinality of the subfield value set $|V_{D_n(x,a)}(q^e; q^d)|$?

References

[1] W.-S. Chou, J. Gomez-Calderon, and G.L. Mullen, Value sets of Dickson polynomials over finite fields, *Journal of Number Theory* Vol. 30 (1988), 334-344.

[2] P. Das and G.L. Mullen, Value sets of polynomials over finite fields, *Finite Fields with Applications in Coding Theory, Cryptography and Related Areas*, edited by G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, Springer (2002), 80-85.

[3] A. Garcia and H. Stichtenoth, On Chebyshev polynomials and maximal curves, *Acta Arithmetica*, Vol. 90 (1999), 301-311.

[4] J. Gomez-Calderon and G.L. Mullen, Galois rings and algebraic cryptography, *Acta Arithmetica*, Vol. 59 (1991), 317-328.

[5] R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical, Essex, United Kingdom (1993).

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20 (2nd ed.), Cambridge University Press, Cambridge (1997).

[7] S.J. Suchower, Polynomial representation of complete sets of frequency hyperrectangles with prime power dimensions, *Journal of Combinatorial Theory, Series A*, Vol. 62 (1993), 46-65.