ON THE NUMBER OF SOLUTIONS OF EQUATIONS OF DICKSON POLYNOMIALS OVER FINITE FIELDS

Wun-Seng Chou, Gary L. Mullen and Bertram Wassermann

Dedicated to Professor Ko-Wei Lih on the occasion of his 60th birthday.

Abstract. Let $k, n_1, \ldots, n_k$ be fixed positive integers, $c_1, \ldots, c_k \in GF(q)^*$, and $a_1, \ldots, a_k, c \in GF(q)$. We study the number of solutions in $GF(q)$ of the equation $c_1 D_{n_1}(x_1, a_1) + c_2 D_{n_2}(x_2, a_2) + \cdots + c_k D_{n_k}(x_k, a_k) = c$, where each $D_{n_i}(x, a_i), 1 \leq i \leq k$, is the Dickson polynomial of degree $n_i$ with parameter $a_i$. We also employ the results of the $k = 1$ case to recover the cardinality of preimages and images of Dickson polynomials obtained earlier by Chou, Gomez-Calderon and Mullen [1].

1. Introduction

Let $q$ be a prime power. A diagonal equation over the finite field $GF(q)$ is defined to be an equation of the form

$$c_1 x_1^{n_1} + c_2 x_2^{n_2} + \cdots + c_k x_k^{n_k} = c,$$

where $c, c_1, \ldots, c_k$ are elements of $GF(q)$ with $c_1 \cdots c_k \neq 0$ and $n_1, \ldots, n_k$ are positive integers. The diagonal equation has been studied extensively; see Chapter 6 of Lidl and Niederreiter’s book [4]. Following the method used in [4], we are going to extend this equation to the equation over $GF(q)$ defined as

$$c_1 D_{n_1}(x_1, a_1) + c_2 D_{n_2}(x_2, a_2) + \cdots + c_k D_{n_k}(x_k, a_k) = c,$$

where $n_1, \ldots, n_k$ are positive integers, $c_1, \ldots, c_k$ are non-zero, $c, a_1, \ldots, a_k$ are elements in $GF(q)$, and $D_{n_1}(x, a_1), \ldots, D_{n_k}(x, a_k)$ are Dickson polynomials defined as follows.
Let $n$ be a positive integer and let $a \in GF(q)$. The Dickson polynomial over $GF(q)$ of degree $n$ with parameter $a$ is defined to be

$$D_n(x, a) = \sum_{i=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$ 

Dickson polynomials have been studied extensively because they play very important roles in both theoretical work as well as in various applications; see Lidl, Mullen and Turnwald’s book [3]. Dickson polynomials have many properties which are closely related to properties of power polynomials and are defined in Section 2. The number $D_n(x, a)$ is defined to be

$$D_n(x, a) = \sum_{i=0}^{\left[\frac{n}{2}\right]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$ 

For example, for $a \in GF(q^2) = GF(q) \setminus \{0\}$, $D_n(x, a)$ induces a permutation on $GF(q)$ if and only if $\gcd(n, q^2 - 1) = 1$.

In this paper, we will employ the method used in [4] to estimate the number $N_k$ of solutions of the equation (1.1) in $GF(q)$. At first, we consider the case $k = 1$ in Section 2. In fact, we will give a formula for $N_1$ in terms of characters on $GF(q^2)$. From now on, we write $N(D_n(x, a) = c)$ instead of $N_1$ to emphasize the Dickson polynomial $D_n(x, a)$ and the fixed value $c \in GF(q)$. In Section 3, we will use the formulas from Section 2 to recover results in [1] about cardinalities of preimages and images of Dickson polynomials. Finally, we will estimate $N_k$ in Section 4.

2. The Number $N(D_n(x, a) = c)$

Let $n > 0$ be a fixed integer. Let $a \in GF(q)^*$. Every element $u$ of $GF(q)$ can be expressed as $u = \alpha + \frac{\delta}{y}$, where either $\alpha \in GF(q)^*$ or $\alpha \in GF(q^2)$ satisfying $\alpha^{q+1} = a$. Let $M(a) = \{\zeta \in GF(q^2) | \zeta^{q+1} = a\}$. Then, either $\alpha \in GF(q^2)$ or $\alpha \in M(a)$. Moreover, if $\alpha_1, \alpha_2 \in M(a)$, there is an element $w \in GF(q^2)$ of multiplicative order a divisor of $q + 1$ satisfying $\alpha_2 = \alpha_1 w$. So, if we set $U$ to be the subset of $GF(q^2)$ containing all elements of multiplicative order dividing $q + 1$, then $M(a) = \alpha U = \{\alpha u | u \in U\}$ for any $\alpha \in M(a)$.

Throughout this section, let $a, c \in GF(q)$ be fixed with $a \neq 0$. Write $x = y + \frac{\delta}{y}$. It is well-known that

$$D_n(x, a) = y^n + \frac{\alpha^n}{y^n}.$$ 

This functional equation is very useful in studying Dickson polynomials over finite fields.

We now define a new equation which will be very useful in studying $N(D_n(x, a) = c)$. For $\theta \in GF(q^2)$, we set an equation

$$y^n = \theta \quad \text{with the constraint} \quad y + \frac{\alpha}{y} \in GF(q).$$
If the equation has a solution, then its solutions belong to $GF(q^2) \cup M(a)$ because of the constraint. Let $N_a(y^n = \theta)$ be the number of solutions in $GF(q^2)$ of the equation (2.3). This equation has a very close relation with the equation $D_n(x, a) = c$ as we are going to see in the following two lemmas.

**Lemma 1.** Let $a, c \in GF(q)$ with $a \neq 0$ and let $\theta \in GF(q^2)$. Then $N_a(y^n = \theta) \neq 0$ if and only if $\theta$ is a solution of $x^2 - cx + a^n = 0$ and $N(D_n(x, a) = c) \neq 0$.

**Proof.** Assume first that $y_0$ is a root of the equation (2.3). Then $x_0 = y_0 + \frac{\alpha}{y_0} \in GF(q)$ and $c = y_0^2 + \frac{\alpha^n}{y_0} \in GF(q)$. This implies that $x_0$ is a solution of the equation $D_n(x, a) = c$ and $\theta$ is a solution of $x^2 - cx + a^n = 0$ because $y_0^n = \theta$.

For the sufficiency, assume that $\theta$ is a solution of $x^2 - cx + a^n = 0$ and $N(D_n(x, a) = c) \neq 0$. Let $x_0$ be a solution of $D_n(x, a) = c$. Write $x_0 = y_1 + \frac{\alpha}{y_1}$ with $y_1 \in GF(q^2) \cup M(a)$. From (2.2), $y_1^n + \frac{\alpha^n}{y_1} = c$. So, we take either $y_0 = y_1$ or $y_0 = y_1$ according to whether $\theta = y_1^n$ or $\theta = \left(\frac{\alpha}{y_1}\right)^n$, respectively. This completes the proof.

**Lemma 2.** Let $n$ be a positive integer. Let $a, c \in GF(q)$ with $a \neq 0$ and let $\theta \in GF(q^2)$ be a solution of $x^2 - cx + a^n = 0$. Let $r$ be the number of solutions of (2.3) with $y = \pm \sqrt{a}$. Then

$$N(D_n(x, a) = c) = \begin{cases} N_a(y^n = \theta) & \text{if } \theta^2 \neq a^n \\ N_a(y^n = \theta) + r & \text{if } \theta^2 = a^n \end{cases}$$

**Proof.** In the second part of the proof of Lemma 1, $y_0$ is chosen uniquely except for $\theta = y_1^n = \left(\frac{\alpha}{y_1}\right)^n$ and $y_1 \neq \frac{\alpha}{y_1}$. This exceptional case implies that $\theta^2 = \alpha^n$ (and so $c = \pm 2\sqrt{a^n}$) and $y_1^2 \neq a$ (and so $x_0 \neq \pm 2\sqrt{a}$). Moreover, both choices of $y_0 = y_1$ and $y_0 = \frac{\alpha}{y_1}$ generate only one solution $x_0$ of $D_n(x, a) = c$ in $GF(q)$. So, the lemma follows.

In fact, the number of solutions of the equation (2.3) can be expressed as a character sum over $GF(q^2)$.

**Lemma 3.** Let $0 \neq a \in GF(q)$ and let $\theta \in GF(q^2)$. Let $\alpha \in M(a)$. Write $m = \gcd(n, q - 1)$ and $\ell = \gcd(n, q + 1)$. Let $r$ be the number of solutions of (2.3) with $y = \pm \sqrt{a}$. Then

$$N_a(y^n = \theta) = \begin{cases} 1 + \sum_{i=0}^{m(q+1)-1} \frac{1}{q+1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}), & \text{if } \theta^2 \neq a^n \\ 1 + \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}) - r, & \text{if } \theta^2 = a^n \end{cases}$$
where $\lambda$ and $\mu$ are multiplicative characters of orders $m(q + 1)$ and $\ell(q - 1)$, respectively.

Proof. Suppose first that $\theta \in GF(q^2)$ is not a root of $x^2 - cx + a^n = 0$ for any $c \in GF(q)$. Then $N_a(y^n = \theta) = 0$ from Lemma 1. Moreover, $\theta \notin GF(q)$ and $\theta\alpha^{-n}$ has multiplicative order not dividing $q + 1$. These facts imply

$$
\sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) = 0 = \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n})
$$

and so the lemma holds.

In what follows, we suppose that $\theta \in GF(q^2)$ is a root of $x^2 - cx + a^n = 0$ for some $c \in GF(q)$. Note that every solution of the equation (2.3) belongs to $GF(q)^* \cup M(a)$. Note also that any solution in $GF(q)^*$ of (2.3) is a gcd($n(q+1), q^2 - 1) = m(q + 1)$ power of some element in $GF(q^2)$. So, the total number of solutions in $GF(q)^*$ of the equation (2.3) equals $\frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta)$. Furthermore, $u \in M(a)$ is a solution of the equation (2.3) if and only if $u\alpha^{-1}$ has order dividing $q + 1$ and is a solution of the equation $y^n = \theta\alpha^{-n}$. The last statement is equivalent to the fact that $\theta\alpha^{-n}$ is a gcd($n(q-1), q^2 - 1) = \ell(q - 1)$ power of some element in $GF(q^2)$. So, the total number of solutions in $M(a)$ of (2.3) equals $\frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n})$.

Finally, if $u \in GF(q)^* \cap M(a)$ is a solution of the equation (2.3), then $u^2 = u^{q+1} = a$. This case holds if and only if $\theta^2 = a^n$. Combining all of these results together, we have that $N_a(y^n = \theta) = \frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n})$ if $\theta^2 \neq a^n$, and $N_a(y^n = \theta) = \frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n}) - r$ if $\theta^2 = a^n$, because we count $u \in GF(q)^* \cap M(a)$ twice in the latter case.

We are now ready to express $N(D_n(x, a) = c)$ in terms of character sums over a finite field.

Theorem 4. Let $n$ be a positive integer. Write $m = \gcd(n, q - 1)$ and $\ell = \gcd(n, q + 1)$. Let $a, c \in GF(q)$ with $a \neq 0$ and let $\theta \in GF(q^2)$ be a solution of $x^2 - cx + a^n = 0$. Choose an arbitrary element $\alpha \in M(a)$, and finally, choose two multiplicative characters $\lambda$ and $\mu$ of orders $m(q + 1)$ and $\ell(q - 1)$ respectively. Then

$$
N(D_n(x, a) = c) = \begin{cases} 
\left(1 + \frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n})\right), & \text{if } \theta^2 \neq a^n, \\
\left(1 + \frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n})\right) \cdot \frac{1}{2}, & \text{if } \theta^2 = a^n.
\end{cases}
$$

Proof. The theorem follows immediately by Lemmas 2 and 3.
The formula in the last theorem is a formula for computing the number of preimages of a fixed element \( c \in GF(q) \) under the Dickson polynomial \( D_n(x, a) \). Sometimes we only need to know whether or not the equation \( D_n(x, a) = c \) has a solution in \( GF(q) \). We only need to modify this formula a little bit for this purpose. Namely, let \( I(D_n(x, a) = c) = 1 \) if the equation \( D_n(x, a) = c \) has a solution in \( GF(q) \), while \( I(D_n(x, a) = c) = 0 \) if the equation \( D_n(x, a) = c \) does not have any solution in \( GF(q) \). We are going to express the number \( I(D_n(x, a) = c) \) in terms of character sums in the following.

**Theorem 5.** Let \( n \) be a positive integer. Write \( m = \gcd(n, q - 1) \) and \( \ell = \gcd(n, q + 1) \). Let \( a, c \in GF(q) \) with \( a \neq 0 \) and let \( \theta \in GF(q^2) \) be a solution of \( x^2 - cx + a^n = 0 \) with \( \theta^2 \neq a^n \). Choose an arbitrary element \( \alpha \in M(a) \), and finally, choose two multiplicative characters \( \lambda \) and \( \mu \) of orders \( m(q + 1) \) and \( \ell(q - 1) \) respectively. Then

\[
I(D_n(x, a) = c) = \frac{1}{m(q + 1)} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{\ell(q - 1)} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n}).
\]

**Proof.** Note that \( \theta \notin GF(q)^* \cap M(a^n) \) since \( \theta^2 \neq a^n \). So, if one of the summations in the statement of the theorem is non-zero, then the other summation is zero. Moreover, \( \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) \) equals either \( m(q+1) \) or \( 0 \) depending on whether \( \theta \) either an \( m(q+1) \)th power in \( GF(q^2) \) or not, respectively, and \( \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta\alpha^{-n}) \) equals either \( \ell(q-1) \) or \( 0 \) depending on \( \theta\alpha^{-n} \) either an \( \ell(q-1) \)th power in \( GF(q^2) \) or not, respectively. From the definition of \( I(D_n(x, a) = c) \), the theorem follows. \( \blacksquare \)

### 3. Cardinalities of Preimages and Images

Using results in Section 2, we are going to give a new proof of results obtained by Chou, Gomez-Calderon and Mullen [1]. In this section, \( n \geq 2 \) is an integer, \( a \in GF(q)^* \), and \( \eta \) denotes the quadratic character of \( GF(q) \). Moreover, \( d \mid t \) means that \( d^j \) divides \( t \) but \( d^{j+1} \) does not divide \( t \). The following theorem includes both Theorems 9 and 9′ in [1].

**Theorem 6.** (Theorems 9 and 9′, [1]). Let \( a \in GF(q)^* \), \( x_0 \in GF(q) \) and let \( D_n^{-1}(D_n(x_0, a)) \) be the preimage of \( D_n(x_0, a) \). If \( q \) is even, then

\[
|D_n^{-1}(D_n(x_0, a))| =
\begin{cases}
\gcd(n, q - 1) & \text{if } x^2 + x_0x + a \text{ is reducible over } GF(q) \text{ and } D_n(x_0, a) \neq 0, \\
\gcd(n, q + 1) & \text{if } x^2 + x_0x + a \text{ is irreducible over } GF(q) \text{ and } D_n(x_0, a) \neq 0, \\
\gcd(n, q - 1) + \gcd(n, q + 1) \quad & \text{if } D_n(x_0, a) = 0.
\end{cases}
\]
If \( q \) is odd and \( 2^r | (q^2 - 1) \), then
\[
|D_n^{-1}(D_n(x_0, a))| = \begin{cases} 
\gcd(n, q - 1) & \text{if } \eta(x_0^2 - 4a) = 1 \text{ and } D_n(x_0, a) \neq \pm 2a^{n/2}, \\
\gcd(n, q + 1) & \text{if } \eta(x_0^2 - 4a) = -1 \text{ and } D_n(x_0, a) \neq \pm 2a^{n/2}, \\
\gcd(n, q - 1) & \text{if } \eta(x_0^2 - 4a) = 1 \text{ and condition } A \text{ holds}, \\
\frac{\gcd(n, q + 1)}{2} & \text{if } \eta(x_0^2 - 4a) = -1 \text{ and condition } A \text{ holds}, \\
\frac{\gcd(n, q - 1) + \gcd(n, q + 1)}{2} & \text{otherwise},
\end{cases}
\]
where condition \( A \) holds if either
\[
2^t | n \text{ with } 1 \leq t \leq r - 1, \eta(a) = -1 \text{ and } D_n(x_0, a) = \pm 2a^{n/2}
\]
or
\[
2^t | n \text{ with } 1 \leq t \leq r - 2, \eta(a) = 1 \text{ and } D_n(x_0, a) = -2a^{n/2}.
\]

**Proof.** Write \( c = D_n(x_0, a) \). Then \( 0 \neq |D_n^{-1}(D_n(x_0, a))| = N(D_n(x, a) = c) \). Let \( \theta \in GF(q^2) \) be a root of \( x^2 - cx + a^n = 0 \) and let \( \alpha \in M(a) \). Note that if \( u \in GF(q^2) \) is a root of \( x^2 - x_0x + a = 0 \), then either \( u \) or \( \frac{1}{u} \) is a root of \( y^n = \theta \) with \( u \in GF(q)^* \cup M(a) \).

We first consider \( \theta^2 \neq a^n \). From Theorem 4,
\[
|D_n^{-1}(D_n(x_0, a))| = \frac{1}{q + 1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q - 1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}),
\]
where \( \lambda \) and \( \mu \) are multiplicative characters of orders \( m(q+1) \) and \( \ell(q-1) \), respectively. Since \( \theta^2 \neq a^n \), either \( \theta \in GF(q) \) or \( \theta \in M(a^n) \), but cannot be both. This implies either \( \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) = 0 \) or \( \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}) = 0 \), but cannot be both zero simultaneously. Precisely, if \( x^2 - x_0x + a \) is reducible (or \( \eta(x_0^2 - 4a) = 1 \) when \( q \) odd) over \( GF(q) \), then \( \theta \in GF(q) \) is an \( m \)th power and so \( \sum_{i=0}^{m(q+1)-1} \mu^i(\theta \alpha^{-n}) = 0 \) and \( |D_n^{-1}(D_n(x_0, a))| = \frac{1}{q + 1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) = m \); while if \( x^2 - x_0x + a \) is irreducible (or \( \eta(x_0^2 - 4a) = -1 \) when \( q \) odd) over \( GF(q) \), then \( \theta \alpha^{-n} \in U \) is an \( \ell \)th power and so \( \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}) = 0 \) and \( |D_n^{-1}(D_n(x_0, a))| = \frac{1}{q - 1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}) = \ell \). This proves the first two situations for any prime power \( q \).
In the remaining part of this proof, assume \( \theta^2 = a^n \). Then \( c = 0 \) if \( q \) is even while \( c \in GF(q)^* \cap M(a^n) = \{ \pm \sqrt{a^n} \} \) if \( q \) is odd. In this case, there is only one choice for \( \theta \). From Theorem 4,

\[
|D_n^{-1}(D_n(x_0, a))| = \frac{1}{2} \left[ \frac{1}{q+1} \sum_{i=0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell(q-1)-1} \mu^i(\theta a^{-n}) \right].
\]

Assume first that \( \theta = \sqrt{a^n} \). There are two cases to consider. (1) \( a \) is a square in \( GF(q) \) so that \( \sqrt{a} \in GF(q)^* \cap M(a^n) \) is a solution of \( y^n = \theta \). This implies that \( \theta \) is an \( m \)th power in \( GF(q) \) and \( \theta a^{-n} \) is an \( \ell \)th power in \( U \). So we have that if \( a \) is a square in \( GF(q) \), then \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) from the equation (3.4). This proves the third situation for \( q \) even and part of the last situation for \( q \) odd. (2) \( a \) is a non-square in \( GF(q) \). So \( q \) must be odd. For a positive integer \( u \), write \( \omega(u) \) to be the non-negative integer satisfying \( 2^{\omega(u)} \mid u \). If \( \eta(x_0^2 - 4a) = 1 \), then \( y^n = \sqrt{a^n} \) has a solution in \( GF(q) \) and so \( \theta = \sqrt{a^n} \) is an \( m \)th power in \( GF(q) \). This implies that \( n \) is even and \( t = \omega(n) > \omega(q-1) \). Now \( (\theta a^{-n})^{\frac{1}{m}} = (a^\frac{1}{2^{\omega(n)}}(a^{q+1})^{-\frac{1}{2^{t}}} = (a^{\frac{1}{2^{\omega(n)}-\frac{1}{2}}})^\frac{1}{2^{t}} = (-1)^{\frac{1}{2^{t}}}. \) This implies that \( \theta a^{-n} \) is an \( \ell \)th power in \( U \) if and only if \( t = \omega(n) > \omega(\ell) = \omega(q+1) \). Combining together, we have, from the equation (3.4), that \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( \eta(x_0^2 - 4a) = 1 \) and \( 1 \leq t \leq r - 1 \), while \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( \eta(x_0^2 - 4a) = 1 \) and \( t \geq r \). If \( \eta(x_0^2 - 4a) = -1 \), then \( y^n = \sqrt{a^n} \) has a solution in \( M(a) \) and so \( \theta a^{-n} \) is an \( \ell \)th power in \( U \). Hence, \( t = \omega(n) > \omega(\ell) = \omega(q+1) \) in this case. Now \( \theta a^{-n} = (a^\frac{1}{2^{\omega(n)}-\frac{1}{2}}) \) \( \frac{1}{2^{t}} = (-1)^{\frac{1}{2^{t}}}. \) This implies that \( \theta \) is an \( m \)th power in \( GF(q) \) if and only if \( t = \omega(n) > \omega(\ell) = \omega(q+1) \). So, from the equation (3.4) again, we have that \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( \eta(x_0^2 - 4a) = -1 \) and \( 1 \leq t \leq r - 1 \), while \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( \eta(x_0^2 - 4a) = -1 \) and \( t \geq r \).

Finally, assume \( \theta = -\sqrt{a^n} \) for \( q \) odd. We also consider two cases. (1) \( a \) is a square in \( GF(q) \). Now \( \theta \) is an \( m \)th power in \( GF(q)^* \) if and only if \( 1 = (\theta)^{\frac{1}{m}} = (-1)^{\frac{1}{m}}(a^{\frac{1}{2}})^\frac{1}{2^{t}} = (-1)^{\frac{1}{2^{t}}}. \) This is equivalent to \( t < \omega(q-1) \). On the other hand, \( \theta a^{-n} \) is an \( \ell \)th power in \( U \) if and only if \( 1 = (\theta a^{-n})^{\frac{1}{m}} = (-1)^{\frac{1}{2^{t}}}(a^{\frac{1}{2^{t}}}(a^{q+1})^{-\frac{1}{2^{t}}} = (-1)^{\frac{1}{2^{t}}}. \) The last statement is equivalent to \( t < \omega(q+1) \). So if \( \eta(x_0^2 - 4a) = 1 \) (or \( y^n = -\sqrt{a^n} \) has a solution in \( GF(q) \)), then \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( 1 \leq t < \omega(q-1) \) and \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( t = 0 \). And if \( \eta(x_0^2 - 4a) = -1 \) (or \( y^n = -\sqrt{a^n} \) has a solution in \( M(a) \)), \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( 1 \leq t < \omega(q-1) \) and \( |D_n^{-1}(D_n(x_0, a))| = \frac{m+\ell}{2} \) if \( t = 0 \). (2) \( a \) is a non-square in \( GF(q)^* \). This implies that \( n \) is even. \( \theta \) is an \( m \)th power in \( GF(q)^* \) if and only if \( 1 = (\theta)^{\frac{1}{m}} = (-1)^{\frac{1}{m}}(a^{\frac{1}{2}})^\frac{1}{2^{t}} = (-1)^{\frac{1}{2^{t}}}. \) This is equivalent to \( t = \omega(q-1) \). On the other hand, \( \theta a^{-n} \) is an \( \ell \)th power in \( U \) if and only
if \(1 = (\theta \alpha^{-n})^{\frac{q+1}{q}} = (-1)^{\frac{q+1}{q}} a^{\frac{n}{q} - 1} = (-1)^{\frac{n}{q} + 1} \). The last statement is equivalent to \(t = \omega(q + 1)\). Note that either \(t = \omega(q - 1)\) or \(t = \omega(q + 1)\), but cannot be both. So, from the equation (3.4), we have that \(\eta(x_0^2 - 4a) = 1\), while \(|D_n^{-1}(D_n(x_0, a))| = \frac{m}{q} \) if \(\eta(x_0^2 - 4a) = -1\). This completes the proof. \(\blacksquare\)

We now provide an alternate proof of one of the main result in [1] about the cardinality \(|V_{D_n(x,a)}|\) of the value set of \(D_n(x,a)\).

**Theorem 7.** (Theorems 10 and 10', [1]). Let \(a \in GF(q)^*\). Suppose that \(2^r||\langle q^2 - 1 \rangle\) and \(\eta\) is the quadratic character on \(GF(q)\) whenever \(q\) is odd. Then we have

\[
|V_{D_n(x,a)}| = \frac{q - 1}{2(n, q - 1)} + \frac{q + 1}{2(n, q + 1)} + \delta,
\]

where

\[
\delta = \begin{cases} 
1 & \text{if } q \text{ is odd, } 2^r-1||n \text{ and } \eta(a) = -1, \\
1/2 & \text{if } q \text{ is odd and } 2^t||n \text{ with } 1 \leq t \leq r - 2, \\
0 & \text{otherwise.}
\end{cases}
\]

**Proof.** Let \(S = GF(q)^* \cap M(a^n)\) and let \(\alpha \in M(a)\) be fixed. Note that every element \(\theta \in S\) satisfies \(\theta^2 = a^n\). Let \(k\) be the number of elements \(\beta \in S\) such that either \(\beta\) is an \(m\)th power in \(GF(q)^*\) or \(\beta \alpha^{-n}\) is an \(\ell\)th power in \(U\). From the definition of \(I(D_n(x,a) = c)\), we have \(|V_{D_n(x,a)}| = \sum c \in GF(q) I(D_n(x,a) = c)\). For \(c \neq \pm \sqrt{a^n}\), we take only one root \(\theta\) in Theorem 5. So, when we sum over all elements in \(GF(q)^* \cup M(a^n)\) in Theorem 5, we have

\[
|V_{D_n(x,a)}| = \frac{1}{2} \sum_{\theta \in GF(q) \setminus M(a^n)} \left[ \frac{1}{m(q+1)} \sum_{i = 0}^{m(q+1)-1} \lambda^i(\theta) + \frac{1}{\ell(q-1)} \sum_{i = 0}^{\ell(q-1)-1} \mu^i(\theta \alpha^{-n}) \right] + k
\]

(3.5)

\[
= \frac{1}{2m(q+1)} \sum_{i = 0}^{m(q+1)-1} \sum_{\theta \in GF(q) \setminus M(a^n)} \lambda^i(\theta) + \frac{1}{2\ell(q-1)} \sum_{i = 0}^{\ell(q-1)-1} \sum_{\theta \in M(a^n) \setminus S} \mu^i(\theta \alpha^{-n}) + k,
\]

where \(\lambda\) and \(\mu\) are multiplicative characters on \(GF(q^2)\) of orders \(m(q + 1)\) and \(\ell(q - 1)\), respectively.

Since every \(\theta \in GF(q)\) is a \((q + 1)\)th power in \(GF(q^2)\) and there are exactly \(\frac{q - 1}{m}\) elements in \(GF(q)^*\) which are \(m\)th powers in \(GF(q)^*\), the first term in the equation (3.5) can be rewritten as
Equations of Dickson Polynomials

\[ E_1 = \frac{1}{2m(q+1)} \sum_{i=0}^{m(q+1)-1} \sum_{\theta \in GF(q^*) \setminus S} \lambda^i(\theta) \]

(3.6)

\[ = \frac{1}{2m} \left[ \sum_{\theta \in GF(q^*)} \sum_{i=0}^{m-1} \lambda^{(q+1)i}(\theta) - \sum_{\theta \in S} \sum_{i=0}^{m-1} \lambda^{(q+1)i}(\theta) \right] \]

\[ = \frac{1}{2m} \left[ q - 1 - \sum_{\theta \in S} \sum_{i=0}^{m-1} \lambda^{(q+1)i}(\theta) \right] . \]

Moreover, every \( u \in U \) is a \((q-1)\)th power in \( GF(q^2) \) and there are exactly \( \frac{q+1}{\ell} \) elements in \( U \) which are \( \ell \)th powers in \( U \), the second term in the equation (3.5) can be rewritten as

\[ E_2 = \frac{1}{2\ell(q-1)} \sum_{i=0}^{\ell(q-1)-1} \sum_{\theta \in M(a^n) \setminus S} \mu^i(\theta a^{-n}) \]

(3.7)

\[ = \frac{1}{2\ell} \left[ \sum_{i=0}^{\ell-1} \sum_{u \in U} \mu^{(q-1)i}(u) - \sum_{\theta \in S} \sum_{i=0}^{\ell-1} \mu^{(q-1)i}(\theta a^{-n}) \right] \]

\[ = \frac{1}{2\ell} \left[ q + 1 - \sum_{\theta \in S} \sum_{i=0}^{\ell-1} \mu^{(q-1)i}(\theta a^{-n}) \right] . \]

Suppose now that \(|S| = 0\). Then \( a \) is a non-square in \( GF(q) \) and \( n \) is odd. So \( k = 0 \), \( \sum_{\theta \in S} \sum_{i=0}^{m-1} \lambda^{(q+1)i}(\theta) = 0 \) in the equation (3.6), and \( \sum_{\theta \in S} \sum_{i=0}^{\ell-1} \mu^{(q-1)i}(\theta a^{-n}) = 0 \) in the equation (3.7). In this case, \( \delta = 0 \) and so, \( |V_{D_n(x,a)}| = \frac{q-1}{2m} + \frac{q+1}{2\ell} \) as desired.

Finally suppose \(|S| \neq 0\). Then \( S = \{ \sqrt{a^n} \} \) if \( q \) is even and \( S = \{ \pm \sqrt{a^n} \} \) if \( q \) is odd. Note that \( \theta = \pm \sqrt{a^n} \) is an \( m \)th power in \( GF(q)^* \) if and only if \( 1 = (\pm \sqrt{a^n})^{\frac{q-1}{m}} = (\pm 1)^{\frac{q-1}{m}} \left( \frac{a^{\frac{1}{2}}}{a^{\frac{1}{2}}} \right)^n \), while \( \theta a^{-n} = \pm \sqrt{a^n} a^{-n} \) is an \( \ell \)th power in \( U \) if and only if \( 1 = (\pm \sqrt{a^n} a^{-n})^{\frac{q+1}{2\ell}} = (\pm 1)^{\frac{q+1}{2\ell}} \left( \frac{a^{\frac{1}{2}}}{a^{\frac{1}{2}}} \right)^n \). Note also that \( a^{\frac{q+1}{2}} = 1 \) if \( a \) is a square, and \( a^{\frac{q+1}{2}} = -1 \) if \( a \) is a non-square. So, there are only two cases to be considered.

(1) \( a \) is quadratic in \( GF(q)^* \). Then \( a^{\frac{q-1}{2}} = 1 \) and so \( \theta = \sqrt{a^m} \) is an \( m \)th power in \( GF(q)^* \) and an \( \ell \)th power in \( U \). So \( \sum_{i=0}^{m-1} \lambda^{(q+1)i}(\sqrt{a^m}) = m \) and \( \sum_{i=0}^{\ell-1} \mu^{(q-1)i}(\sqrt{a^m} a^{-n}) = \ell \). From equations (3.5), (3.6) and (3.7), if \( q \) is even, we have \( |V_{D_n(x,a)}| = \frac{q-1}{2m} + \frac{q+1}{2\ell} \) (i.e., \( \delta = 0 \)), because \( k = 1 \). Assume now \( q \) odd. From the above results, \( -\sqrt{a^m} \) is an \( m \)th power in \( GF(q)^* \) if and only if \( \frac{q-1}{m} \) is even, and \( -\sqrt{a^m} a^{-n} \) is an \( \ell \)th power in \( U \) if and only if
\(q + 1\) is even. If \(t \geq r - 1\), then both \(q^{-1}/m\) and \(q + 1\) are odd and so, \(k = 1\). In this case, \(|V_{D_n(x,a)}| = q^{-1}/m + 1 = q^{-1}/m + q + 1\) (i.e., \(\delta = 0\)), from equations (3.5), (3.6) and (3.7). If \(t < r - 1\), then \(k = 2\). If \(t = 0\), then \(|V_{D_n(x,a)}| = q^{-1}/m + 2 = q^{-1}/m + q + 1\) (i.e., \(\delta = 0\)), from equations (3.5), (3.6) and (3.7). If \(1 \leq t \leq r - 2\), then one of \(q^{-1}/m\) and \(q + 1\) is even and the other is odd. In this case, we have \(|V_{D_n(x,a)}| = q^{-1}/m + 2 + 1/2\) from equations (3.5), (3.6) and (3.7).

\((2)\) \(a\) is a non-square in \(GF(q)^*\). Then \(q\) is odd and \(a^{q^{-1}/m} = -1\). Moreover, \(\theta = \pm \sqrt{a^n} = S\) if and only if \(n\) is even. So, if \(n\) is odd, then \(|S| = 0 = k\) and so \(|V_{D_n(x,a)}| = q^{-1}/m + a^{-1/2}\) from equations (3.5), (3.6) and (3.7). From now on, let \(n\) be even. Then \(S = \{\pm \sqrt{a^n}\}\). From the above results, \(\theta = \pm \sqrt{a^n}\) is an \(m\)th power in \(GF(q)^*\) if and only if \(1 = (\pm 1)^{q^{-1}/m}(-1)^{\frac{m}{4}}\), while \(\theta a^{-n} = \pm \sqrt{a^n} \alpha^{-n} - n\) is an \(\ell\)th power in \(U\) if and only if \(1 = (\pm 1)^{q^{-1}/m}(-1)^{\frac{\ell}{2}}\). If \(t = 1\), then both \(n/m\) and \(a^{-1/2}\) are odd and exactly one of \(q^{-1}/m + n/m\) and \(q^{-1}/m + n/m\) is odd. In this case, \(k = 1\) and, from equations (3.5), (3.6) and (3.7), \(|V_{D_n(x,a)}| = q^{-1}/m + q^{-1}/m + 1/2\). If \(2 \leq t \leq r - 2\), then exactly one of \(n/m\) and \(a^{-1/2}\) is odd and both \(q^{-1}/m + n/m\) and \(q^{-1}/m + a^{-1/2}\) are odd. So, we also have \(k = 1\) and \(|V_{D_n(x,a)}| = q^{-1}/m + q^{-1}/m + 1/2\) in this case. If \(t = r - 1\), then exactly one of \(n/m\) and \(a^{-1/2}\) is even, exactly one of \(n/m\) and \(n/m + q^{-1}/m\) is even, and exactly one of \(a^{-1/2}\) and \(n/m + q^{-1}/m\) is even. In this case, we have \(k = 2\) and, from equations (3.5), (3.6) and (3.7), \(|V_{D_n(x,a)}| = q^{-1}/m + q^{-1}/m + 1\). Finally, if \(t \geq r\), then both \(n/m\) and \(a^{-1/2}\) are even and both \(q^{-1}/m + n/m\) and \(q^{-1}/m + a^{-1/2}\) are odd. So, we have that \(k = 1\) and, from equations (3.5), (3.6) and (3.7), \(|V_{D_n(x,a)}| = q^{-1}/m + q^{-1}/m + 1/2\) in this case. This completes the proof.

4. An Equation Involving Dickson Polynomials

In this section, let \(k, n_1, \ldots, n_k \geq 2\) be fixed positive integers, \(c_1, \ldots, c_k \in GF(q)^*\), and \(a_1, \ldots, a_k, c \in GF(q)\). We are going to estimate the number \(N_k\) of solutions in \(GF(q)\) of the equation (1.1); namely, the number of solutions in \(GF(q)\) of the equation \(c_1D_{n_1}(x_1, a_1) + c_2D_{n_2}(x_2, a_2) + \cdots + c_kD_{n_k}(x_k, a_k) = c\), where each \(D_{n_i}(x, a_i)\) is a Dickson polynomial of degree \(n_i\) with parameter \(a_i\). For this purpose, we need the following two lemmas.

**Lemma 8.** (Theorem 10, Chapter 6, [2]) Let \(\chi\) be a non-trivial additive character of \(GF(q)\). Suppose either \(\lambda\) is a non-trivial multiplicative character of \(GF(q)^*\) or \(b, c \in GF(q)\) are not equal to zero simultaneously. Then

\[
\left| \sum_{\theta \in GF(q)^*} \chi(b\theta + c) \lambda(\theta) \right| \leq 2\sqrt{q}.
\]
In the following lemma, let $U$ be the subset of $GF(q^2)$ defined at the beginning of Section 2. That is, every element of $U$ has multiplicative order dividing $q + 1$. So, $U$ is the set of elements in $GF(q^2)$ which have norm 1 in $GF(q)$.

**Lemma 9.** (Corollary 8, Chapter 6, [2]) For either $\chi$ a non-trivial additive character of $GF(q^2)$ or $\lambda$ a non-trivial multiplicative character of $GF(q^2)$ of order dividing $q + 1$, one has

$$\left| \sum_{\theta \in U} \chi(\theta)\lambda(\theta) \right| \leq 2\sqrt{q}.$$ 

We now estimate $N_k$. It is easy to see that

$$N_k = \sum_{u_1 \in GF(q)} \cdots \sum_{u_k \in GF(q)} \frac{1}{q} \sum_{\chi} \chi(c_1D_{n_1}(u_1, a_1) + \cdots + c_kD_{n_k}(u_k, a_k) - c)$$

$$= \frac{1}{q} \sum_{\chi} \chi(c)^{-1} \sum_{u_1 \in GF(q)} \chi(c_1D_{n_1}(u_1, a_1)) \cdots \sum_{u_k \in GF(q)} \chi(c_kD_{n_k}(u_k, a_k)),$$

where $\chi$ runs over all the additive characters. Let $\chi_0$ be the trivial additive character over $GF(q)$. Then the last equation becomes

$$N_k - q^{k-1} = \frac{1}{q} \sum_{\chi \neq \chi_0} \chi(c)^{-1}$$

(4.8)

$$\sum_{u_1 \in GF(q)} \chi(c_1D_{n_1}(u_1, a_1)) \cdots \sum_{u_k \in GF(q)} \chi(c_kD_{n_k}(u_k, a_k)).$$

Let $\chi$ be any non-trivial additive character and take any $1 \leq j \leq k$. Let $\chi_{c_j}$ be the additive character satisfying $\chi_{c_j}(u) = \chi(cju)$ for all $u \in GF(q)$. Then

$$\sum_{u_j \in GF(q)} \chi(c_jD_{n_j}(u_j, a_j)) = \sum_{u_j \in GF(q)} \chi_{c_j}(D_{n_j}(u_j, a_j))$$

(4.9)

$$= \sum_{u \in GF(q)} \chi_{c_j}(u)N(D_{n_j}(x_j, a_j) = u).$$

Let $m_j = \gcd(n_j, q - 1)$ and $\ell_j = \gcd(n_j, q + 1)$. Assume that $\lambda_j$ and $\mu_j$ are multiplicative characters on $GF(q^2)$ of orders $m_j(q + 1)$ and $\ell_j(q - 1)$, respectively.

At first, we consider all $a_j \neq 0$. Write $u = \theta + \frac{a_j}{\theta}$ with $\theta \in GF(q)^* \cup M(a_j^{\mu_j})$ and take a fixed $\alpha_j \in M(a_j)$. Then from Theorem 4, the equation (4.9) becomes

$$\sum_{u_j \in GF(q)} \chi(c_jD_{n_j}(u_j, a_j))$$
\[= \sum_{u \in GF(q)} \chi_{c_j}(u) N_q(D_{n_j}(x_j, a_j) = u)\]
\[= \frac{1}{2} \sum_{\theta \in GF(q)^* \cup M(a_j^{n_j})} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \left( \frac{1}{q + 1} \sum_{i=0}^{m_j(q+1)-1} \lambda_j^i(\theta) + \frac{1}{q-1} \sum_{i=0}^{\ell_j(q-1)-1} \mu_j^i(\theta a_j^{-n_j}) \right) \]

Since each \( \theta \in GF(q) \) is a \((q + 1)\)th power of some element in \( GF(q^2) \) and each \( \theta a_j^{-n_j} \) with \( \theta \in M(a_j^{n_j}) \) is a \((q - 1)\)th power of some element in \( GF(q^2) \), we may consider \( \lambda \) to be of order \( m_j \) and \( \mu \) to be of order \( \ell_j \). Then the last equation can be rewritten as

\[= \frac{1}{2} \sum_{i=0}^{m_j-1} \sum_{\theta \in GF(q)^*} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \lambda_j^i(\theta) + \frac{1}{2} \sum_{i=0}^{\ell_j-1} \sum_{\theta \in M(a_j^{n_j})} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \mu_j^i(\theta a_j^{-n_j}). \]  

(4.10)

In the equation (4.10), the sum \( \sum_{\theta \in GF(q)^*} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \lambda_j^i(\theta) \) is a twisted Kloosterman sum. From Lemma 8, we have

\[\left| \sum_{\theta \in GF(q)^*} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \lambda_j^i(\theta) \right| \leq 2\sqrt{q}. \]  

(4.11)

For estimating the sum \( \sum_{\theta \in M(a_j^{n_j})} \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) \mu_j^i(\theta a_j^{-n_j}) \) in the equation (4.10), we have to modify some notation. Let \( \chi_j' = \chi_{c_j} \circ Tr_{q^2/q} \), where \( Tr_{q^2/q} \) is the trace function from \( GF(q^2) \) onto \( GF(q) \). Then \( \chi_j' \) is a non-trivial additive character of \( GF(q^2) \). For any \( \theta \in M(a_j^{n_j}) \), we have \( \theta^{q+1} = a_j^{n_j} \) and thus \( \theta + \frac{a_j^{n_j}}{\theta} = Tr_{q^2/q}(\theta) \). This implies \( \chi_{c_j}(\theta + \frac{a_j^{n_j}}{\theta}) = \chi_j'(\theta) \). Furthermore, let \( \chi_{a_j^{n_j}}'(u) = \chi_j'(a_j^{n_j}u) \) for all \( u \) in \( GF(q^2) \). Then \( \chi_{a_j^{n_j}}' \) is a non-trivial additive character of \( GF(q^2) \) and \( \chi_{a_j^{n_j}}'(\theta a_j^{-n_j}) = \chi_j'(\theta) \). Notice that \( \theta a_j^{-n_j} \in U \) from the definition of \( U \). By Lemma 9,
Equations of Dickson Polynomials 929

\[ | \sum_{\theta \in M(a_{nj})} \chi_{c_j}(\theta + \frac{a_{nj}}{\theta}) \mu_j^c(\theta a_{nj}^{-1}) | = | \sum_{\theta \in U} \chi'_{a_{nj}}(\theta) \mu_j^c(\theta) | \leq 2 \sqrt{q}. \]

Substituting both inequalities (4.11) and (4.12) into (4.10) and simplifying, we have

\[ | \sum_{u_j \in GF(q)} \chi(c_j D_{n_j}(u_j, a_j)) | \leq (m_j + \ell_j) \sqrt{q}. \]

Suppose that \( a_j = 0 \). Then the equation (4.9) becomes

\[ \sum_{u_j \in GF(q)} \chi(c_j D_{n_j}(u_j, a_j)) = \sum_{u \in GF(q)} \chi(c_j u^{n_j}). \]

From Theorem 5.30, [4], the last equation becomes

\[ \sum_{u_j \in GF(q)} \chi(c_j D_{n_j}(u_j, a_j)) = \sum_{i=1}^{m_j-1} \lambda_j^{-1}(c_j) G(\chi, \lambda_j^i), \]

where \( G(\chi, \lambda_j^i) = \sum_{u \in GF(q)^*} \chi(u) \lambda_j^i(u) \) is a Gauss sum. Since \( |G(\chi, \lambda_j^i)| = \sqrt{q} \) (Theorem 5.11, [4]), we have

\[ | \sum_{u_j \in GF(q)} \chi(c_j D_{n_j}(u_j, a_j)) | \leq (m_j - 1) \sqrt{q}. \]

Suppose now that there exists \( 0 \leq t \leq k \) such that \( a_1 = \cdots = a_t = 0 \) (\( t = 0 \) means that no such \( t \) exists) and \( a_j \neq 0 \) for all \( t < j \leq k \) (\( t = k \) means the equation (1.1) is a diagonal equation). Substituting both bounds (4.13) and (4.14) into (4.8) and simplifying, we have

\[ |N_k - q^{k-1}| \leq q^{k-2} (q - 1) \prod_{j=1}^t (m_j - 1) \prod_{j=t+1}^k (m_j + \ell_j). \]

We summarize all of these results above in the following

**Theorem 10.** Let \( k, n_1, \ldots, n_k \geq 2 \) be fixed positive integers, \( c_1, \ldots, c_k \in GF(q)^* \), and \( a_1, \ldots, a_k, c \in GF(q) \). Moreover, suppose that there exists \( 0 \leq t \leq k \) such that \( a_1 = \cdots = a_t = 0 \) and \( a_j \neq 0 \) for all \( t < j \leq k \). Let \( N_k \) be the number of solutions in \( GF(q) \) of the equation

\[ c_1 D_{n_1}(x_1, a_1) + c_2 D_{n_2}(x_2, a_2) + \cdots + c_k D_{n_k}(x_k, a_k) = c. \]
Then
\[ |N_k - q^{k-1}| \leq q^{k-2} (q - 1) \prod_{j=1}^{t} (m_j - 1) \prod_{j=t+1}^{k} (m_j + \ell_j), \]
where \( m_j = \gcd(n_j, q - 1) \) and \( \ell_j = \gcd(n_j, q + 1) \) for \( 1 \leq j \leq k \).

Note that the main term \( q^{k-1} \) in the last theorem is reasonable. For instance, if some \( n_j \) is relatively prime to \( q^2 - 1 \), then the equation (1.1) has exactly \( q^{k-1} \) solutions in \( GF(q) \) because \( D_{n_j}(x_j, a_j) \) is a permutation polynomial on \( GF(q) \) and so, for each \( u_i \in GF(q), 1 \leq i \leq k \) and \( i \neq j \), \( c_jD_{n_j}(x_j, a_j) = c - c_1D_1(u_1, a_1) - \cdots - c_{j-1}D_{j-1}(u_{j-1}, a_{j-1}) - c_j + 1D_{j+1}(u_{j+1}, a_{j+1}) - \cdots - c_kD_k(u_k, a_k) \) has exactly one solution in \( GF(q) \).

From the last theorem, we have the following existence result for \( k \geq 3 \).

**Theorem 11.** Let \( k, n_1, \ldots, n_k \geq 2 \) be fixed positive integers, \( c_1, \ldots, c_k \in GF(q)^*, \) and \( a_1, \ldots, a_k, c \in GF(q) \). Moreover, suppose that there exists \( 0 \leq t \leq k \) such that \( a_1 = \cdots = a_t = 0 \) and \( a_j \neq 0 \) for all \( t < j \leq k \). If \( k \geq 3 \) and \( q > (\prod_{j=1}^{k} (n_j + 2))^{\frac{2}{k-2}} \), then \( N_k > 0 \).

**Proof.** From Theorem 10, we have
\[
(4.16) \quad N_k \geq q^{k-1} - q^{k-2} (q - 1) \prod_{j=1}^{t} (m_j - 1) \prod_{j=t+1}^{k} (m_j + \ell_j).
\]
For any \( 1 \leq j \leq k \), both \( m_j - 1 \leq n_j + 2 \) and \( m_j + \ell_j \leq n_j + 2 \) hold. Since \( q > (\prod_{j=1}^{k} (n_j + 2))^{\frac{2}{k-2}} \), the right hand side of the inequality (4.16) is positive and so \( N_k > 0 \).

Note that the last theorem cannot hold for \( k = 1 \) or 2. When \( k = 1 \), it is easy to see that no matter how large the prime power \( q \) is, \( N_k \) may be zero from Theorem 7. For \( k = 2 \), we give an example as following:

**Example.** Let \( n_1, n_2 \geq 2 \) be relatively prime odd integers. Take any prime number \( q \) of the form \( q = 8n_1n_2s + (4n_1n_2 + 1) \). We now consider the equation
\[
(4.17) \quad D_{4n_1}(x_1, 1) + D_{4n_2}(x_2, 1) = 0.
\]
Take any \( c \in GF(q) \). Suppose that \( \rho \) is a root of \( x^2 - cx + 1 = 0 \). Then \( -\rho \) is a root of \( x^2 + cx + 1 = 0 \). If \( D_{4n_1}(x_1, 1) = c \) has a solution in \( GF(q) \), then \( \rho \in GF(q) \) is a \( 4n_1 \)th power in \( GF(q) \) and so \( -\rho \in GF(q) \) is only a square but not a 4th power. Hence \( D_{4n_1}(x_2, 1) = -c \) has no solution in this case. On the other hand, if \( D_{4n_1}(x_1, 1) = c \) has a solution in \( U = \{ u \in GF(q^2) | u^{q+1} = 1 \} \), then \( \rho \in U \) is a
square in $U$ and so $-\rho \in U$ is a non-square. This implies that $D_{4n^2}(x_2, 1) = -c$ has no solution in this case. Combining all the arguments together, the equation (4.17) has no solution in $GF(q)$.

REFERENCES


Wun-Seng Chou  
Institute of Mathematics,  
Academia Sinica,  
Nankang, Taipei 115  
Taiwan, R.O.C.  
E-mail: macws@math.sinica.edu.tw

Gary L. Mullen  
Department of Mathematics,  
The Pennsylvania State University,  
University Park, PA 16802,  
U.S.A.  
E-mail: mullen@math.psu.edu

Bertram Wassermann  
Department of Mathematics,  
The Pennsylvania State University,  
University Park, PA 16802,  
U.S.A.