On the Waring Problem with Multivariate Dickson Polynomials

Alina Ostafe, David Thomson, and Arne Winterhof

Abstract. We extend recent results of Gomez and Winterhof, and Ostafe and Shparlinski on the Waring problem with univariate Dickson polynomials in a finite field to the multivariate case. We give some sufficient conditions for the existence of the Waring number for multivariate Dickson polynomials, that is, the smallest number g of summands needed to express any element of the finite field as sum of g values of the Dickson polynomial. Moreover, we prove strong bounds on the Waring number using a reduction to the case of fewer variables and an approach based on recent advances in arithmetic combinatorics due to Glibichuk and Rudnev.

1. Introduction

For a finite field $\mathbb{F}_q$ of q elements and a parameter $a \in \mathbb{F}_q$, the values of the *multivariate Dickson polynomials of the first kind*, denoted $D_e^{(i)}(x_1, \ldots, x_k, a)$, $i = 1, \ldots, k$, where e is any positive integer, are defined by the functional equations

$$D_e^{(i)}(x_1, \ldots, x_k, a) = s_i(u_1^e, \ldots, u_{k+1}^e), \quad x_1, \ldots, x_k \in \mathbb{F}_q,$$

where $x_i = s_i(u_1, \ldots, u_{k+1})$, s_i is the ith symmetric function in the indeterminates $u_1, \ldots, u_{k+1}$ and

$$u_1 \cdots u_{k+1} = a,$$

see [**11**, Chapter 2.4].

During the preparation of this paper, the first author was supported in part by SNF Grant 133399 (Switzerland).

The second author was supported in part by NSERC of Canada.

Equivalently, $u_1, \ldots, u_{k+1}$ are the zeros of the polynomial

$$\begin{aligned} r(Z) &= r(Z, x_1, \ldots, x_k, a) \\ &= Z^{k+1} - x_1 Z^k + \cdots + (-1)^k x_k Z + (-1)^{k+1} a = \prod_{i=1}^{k+1} (Z - u_i) \end{aligned}$$

in the indeterminate Z and $u_1^e, \ldots, u_{k+1}^e$ are the zeros of

$$\begin{aligned} r_e(Z) &= r_e(Z, x_1, \ldots, x_k, a) \\ &= Z^{k+1} - D_e^{(1)}(x_1, \ldots, x_k, a) Z^k + \cdots \\ &\quad + (-1)^k D_e^{(k)}(x_1, \ldots, x_k, a) Z + (-1)^{k+1} a^e \\ &= \prod_{i=1}^{k+1} (Z - u_i^e). \end{aligned}$$

In particular, if the polynomial $r(Z)$ is irreducible, then the roots are the conjugates $u_i = u^{q^{i-1}}$, $i = 1, \ldots, k+1$, with a defining element u of $\mathbb{F}_{q^{k+1}} = \mathbb{F}_q(u)$, and the condition that

$$u u^q \cdots u^{q^k} = u^{(q^{k+1}-1)/(q-1)} = a.$$

In general, the u_i are in an extension field $\mathbb{F}_{q^j}$ of $\mathbb{F}_q$ with $1 \le j \le k$ if $a = 0$, and $1 \le j \le k+1$ if $a \ne 0$, respectively. Put $\ell = \operatorname{lcm}\{2, \ldots, k\}$ if $a = 0$ and $\ell = \operatorname{lcm}\{2, \ldots, k+1\}$ if $a \ne 0$. Then we have

$$(1) \qquad D_e^{(i)}(x_1, \ldots, x_k, a) = D_f^{(i)}(x_1, \ldots, x_k, a) \quad \text{if } e \equiv f \bmod q^\ell - 1.$$

In this paper we will consider the Waring problem with the first multivariate Dickson polynomials which have the values

$$D_e^{(1)}(x_1, \ldots, x_k, a) = u_1^e + \cdots + u_{k+1}^e, \quad x_i = s_i(u_1, \ldots, u_{k+1}),$$

that is, the question of the existence and estimation of the smallest positive integer $g = g_a(e, k, q)$ such that the equation

$$(2) \quad D_e^{(1)}(x_{1,1}, \ldots, x_{1,k}, a) + \cdots + D_e^{(1)}(x_{g,1}, \ldots, x_{g,k}, a) = c, \quad x_{i,j} \in \mathbb{F}_q,$$

is solvable for any $c \in \mathbb{F}_q$. We call $g_a(e, k, q)$ the *Waring number of* $D_e^{(1)}$ and put $g_a(e, k, q) = \infty$ if such g does not exist.

By (1) we have

$$g_a(e, k, q) = g_{a^{e/d}}(d, k, q), \quad \text{where } d = \gcd(e, q^\ell - 1).$$

More precisely, $D_e(x_1, \ldots, x_k, a)$ and $D_d(x_1, \ldots, x_k, a^{e/d})$ have the same value sets since on the one hand $u_1^e + \cdots + u_{k+1}^e = (u_1^{e/d})^d + \cdots + (u_{k+1}^{e/d})^d$ and $u_1^{e/d} \cdots u_{k+1}^{e/d} = a^{e/d}$, and on the other hand we have $d = ex + q^{\ell-1} y$ for some integers x and y, $u_i^{q^\ell - 1} = 1$, and thus $u_1^d + \cdots + u_{k+1}^d = (u_1^x)^e + \cdots + (u_{k+1}^x)^e$ with $u_1^x \cdots u_{k+1}^x = a^{ex/d} = a$. Since we focus on the case $a = 1$ (but present the results for an arbitrary a whenever it is possible), we may assume from now on that

$$e \mid q^\ell - 1, \quad e < q^\ell - 1. \tag{3}$$

Note that for $e = q^\ell - 1$ the value set of $D_e^{(1)}$ contains only the element $k+1$ and only $g(k+1)$ is representable with exactly g summands. In this case, $g_a(q^\ell - 1, k, q) = \infty$.

We note that the Waring number associated to the shifted Dickson polynomial with values

$$D_e^{(1)}(x_1, \ldots, x_k, a) + d$$

for some $d \in \mathbb{F}_q$ is equal to $g_a(e, k, q)$. Indeed, if (2) has a solution for any $c \in \mathbb{F}_q$ and fixed g, then so does

$$D_e^{(1)}(x_{1,1}, \ldots, x_{1,k}, a) + \cdots + D_e^{(1)}(x_{g,1}, \ldots, x_{g,k}, a) + dg = c', \quad x_{i,j} \in \mathbb{F}_q,$$

where $c' = c + dg$.

The existence of $g_a(e, k, q)$ is guaranteed when $q = p$ is a prime by the Cauchy-Davenport inequality

$$|A + B| \geq \min\{|A| + |B| - 1, p\} \quad \text{for any } A, B \subseteq \mathbb{F}_p$$

with B the value set of $D_e^{(1)}$ and $A = A_j$ the set of sums of j values of $D_e^{(1)}$. Since the value set of $D_e^{(1)}$ contains at least two elements by (3), we have either $|A_{j+1}| > |A_j|$ or $A_{j+1} = \mathbb{F}_p$.

For $q = p^m$ with a prime p and $m > 1$, the existence was characterized for $a = 0$ and $k = 1$ in [**1**] and for $a = k = 1$ in [**10**]. By [**1**, Theorem G] we have

$$g_0(e, 1, q) < \infty \quad \text{if and only if} \quad \frac{q-1}{p^t - 1} \nmid e \text{ for all } t \mid m \text{ with } t \neq m,$$

or equivalently the eth powers generate $\mathbb{F}_q$ over $\mathbb{F}_p$ and do not fall into a proper subfield.

Lemma 1. [**10**, Theorem 2.1] *Let $q = p^m$ for a prime p and let $m = 2^k \ell_0$, where k is a nonnegative integer and ℓ_0 is odd. Then $g_1(e, 1, q) < \infty$ if and only if at least one of the following two conditions is satisfied.*

1. $$\frac{q-1}{p^t - 1} \nmid e \text{ for all } t \mid m \text{ with } t \neq m, \qquad p^{m/2} - 1 \nmid e \text{ if } k \geq 1,$$ $$\text{and} \quad \frac{q-1}{(2, p+1)} \nmid e \text{ if } \ell_0 > 1.$$
2. $$\frac{q+1}{(2, p+1)} \nmid e, \qquad \frac{q+1}{p^t + 1} \nmid e \text{ for all } t \mid m,\ t < m,\ m/t \text{ odd}.$$

We note that there is a typo in [**10**, Theorem 2.1] where the expression reads $q+1$ instead of $q-1$ in the last line of 1. Moreover, there is a small gap in the proof which is filled in Theorem 10 of this paper, namely that $g_a(e,k,q) < \infty$ if the value set of $D_e^{(1)}$ contains a basis of $\mathbb{F}_q$.

In the univariate case for $a = 0$ we have $D_e(X, a) = X^e$, which corresponds to the classical Waring problem in finite fields where recently quite substantial progress has been achieved, see [**3, 4, 5, 6, 15**]. A survey of earlier results can also be found in [**14**].

However, recently it has become apparent that the methods of arithmetic combinatorics provide a very powerful tool for the Waring problem and lead to results which are not accessible by other methods, see [**4, 5**]. In particular, we have, by [**4**, Corollary 7],

$$g_0(e, 1, q) \le 8 \quad \text{if } e < q^{1/2}.$$

In a recent work, Ostafe and Shparlinski [**13**] used a result of Glibichuk and Rudnev [**9**] to show that, in the univariate case for $a \ne 0$, the following inequality holds:

Lemma 2.

$$g_a(e, 1, q) \le 16$$

holds for

1. *any* $a \in \mathbb{F}_q^*$ *and* $\gcd(e, q-1) \le 2^{-3/2}(q-2)^{1/2}$;
2. a *that is a square in* $\mathbb{F}_q^*$ *and* $\gcd(e, q+1) \le 2^{-3/2}(q-2)^{1/2}$.

Throughout this paper we use the following notation. Let m be a positive integer, let p be a prime and let $q = p^m$. The values $u_1, \dots, u_{k+1}$ are in the algebraic closure of $\mathbb{F}_q$ (precisely, $u_1, \dots, u_{k+1}$ are in the splitting field of the polynomial $r(Z)$), and

$$\begin{aligned} x_i &= s_i(u_1, \dots, u_k, u_{k+1}), \quad u_{k+1} = a(u_1 \cdots u_k)^{-1}, \\ y_i &= s_i(v_1, \dots, v_k, v_{k+1}), \quad v_{k+1} = (v_1 \cdots v_k)^{-1}. \end{aligned} \tag{4}$$

Furthermore, for any $j \in \mathbb{N}$ we denote by

$$\mathrm{Nm}_j(u) = u u^q \cdots u^{q^{j-1}} = u^{\frac{q^j - 1}{q-1}}$$

the $\mathbb{F}_{q^j}$ norm over $\mathbb{F}_q$ and by

$$\mathrm{Tr}_j(u) = u + u^q + \cdots + u^{q^{j-1}}$$

the $\mathbb{F}_{q^j}$ trace over $\mathbb{F}_q$.

In this paper we study the existence problem for $g_1(e, k, q)$, and get bounds on $g_a(e, k, q)$ by reducing the case of $k \ge 2$ variables to the case of fewer variables. We also use the same techniques of additive combinatorics as in [**13**] to prove bounds on $g_a(e,k,q)$ and extend the range of nontrivial results. Our results become stronger with increasing k.

2. Preparations

Results on the value set. We consider the set

$$\mathcal{E} = \Big\{ D_e^{(1)}(x_1,\dots,x_k,1) \ : \ u_{i+1} = u_1^{q^i}, \ i=0,\dots,k, \qquad \mathrm{Nm}_{k+1}(u_1) = u_1^{(q^{k+1}-1)/(q-1)} = 1, \ u_1 \in \mathbb{F}_{q^{k+1}}^* \Big\},$$

where the x_i are defined by (4).

A simple remark is that $\mathcal{E} \subseteq \mathbb{F}_q$. Indeed, we have

$$D_e^{(1)}(x_1,\dots,x_k,1) = u_1^e + u_1^{eq} + \dots + u_1^{eq^{k-1}} + u_1^{eq^k} = \mathrm{Tr}_{k+1}(u_1^e) \in \mathbb{F}_q. \tag{5}$$

LEMMA 3. *Let $\mathcal{E}$ be defined as above. Then,*

$$\#\mathcal{E} \geq \frac{(q^{k+1}-1)}{dd_0(q-1)},$$

where $d = q^{k-1} + (q^k-1)/(q-1)$ and $d_0 = \gcd(e,(q^{k+1}-1)/(q-1))$.

PROOF. To estimate $\#\mathcal{E}$, we notice that

$$D_e^{(1)}(x_1,\dots,x_k,1) = u_1^e + u_1^{eq} + \dots + u_1^{eq^{k-1}} + u_1^{-e(q^k-1)/(q-1)}$$

has degree $d = q^{k-1} + (q^k-1)/(q-1)$ as a rational function in u_1^e. Moreover, u_1^e takes any value at most $d_0 = \gcd(e,(q^{k+1}-1)/(q-1))$ times. Hence, $D_e^{(1)}$ takes any value at most dd_0 times. Since there are $(q^{k+1}-1)/(q-1)$ different u_1 with $\mathrm{Nm}_{k+1}(u_1) = 1$, the result follows. □

Moreover, the value sets of different Dickson polynomials can coincide.

LEMMA 4. *If ab^{-1} is a $(k+1)$th power in $\mathbb{F}_q$, the value sets of $D_e^{(1)}(X_1,\dots,X_k,a)$ and $D_e^{(1)}(X_1,\dots,X_k,b)$ are the same and thus we have*

$$g_a(e,k,q) = g_b(e,k,q).$$

PROOF. If $ab^{-1} = c^{k+1}$, we have

$$\begin{aligned} D_e^{(1)}(x_1,\dots,x_k,a) &= u_1^e + \dots + u_{k+1}^e \\ &= c^e((c^{-1}u_1)^e + \dots + (c^{-1}u_{k+1})^e) \\ &= c^e D_e(y_1,\dots,y_k,b) \end{aligned}$$

for some $y_1,\dots,y_k \in \mathbb{F}_q$ since $c^{-(k+1)}u_1\cdots u_{k+1} = c^{-(k+1)}a = b$. □

Reduction from k variables to fewer variables.

THEOREM 5. *For $1 \le k_0 < k$ put $\ell_{k_0} = \mathrm{lcm}(2, \ldots, k_0+1)$ if $a \ne 0$, $\ell_{k_0} = \mathrm{lcm}(2, \ldots, k_0)$ if $a = 0$ and $e_{k_0} = \gcd(e, q^{\ell_{k_0}} - 1)$. Then we have*

$$g_0(e,k,q) \le \left\lceil \frac{g_0(e_{k_0}, k_0, q)}{\lfloor k/k_0 \rfloor} \right\rceil,$$

$$g_a(e,k,q) = g_1(e,k,q) \le \left\lceil \frac{g_1(e_{k_0}, k_0, q)}{\lfloor (k+1)/(k_0+1) \rfloor} \right\rceil \quad \text{if } a = b^{k+1}$$

for some $b \in \mathbb{F}_q$, and otherwise

$$g_a(e,k,q) \le \left\lceil \frac{g_1(e_{k_0}, k_0, q)}{\lfloor k/(k_0+1) \rfloor} \right\rceil.$$

PROOF. We start with the case $a = 0$, where

$$D_e^{(1)}(x_1, \ldots, x_k, 0) = u_1^e + \cdots + u_k^e.$$

Since $k_0 < k$, we consider only those values with $u_i = 0$ for $i = k_0\lfloor k/k_0 \rfloor + 1, \ldots, k+1$ and see that $g_0(e,k,q)$ is not larger than the smallest g such that

$$g\lfloor k/k_0 \rfloor \ge g_0(e, k_0, q) = g_0(e_{k_0}, k_0, q) \quad \text{with } 1 \le k_0 < k,$$

which implies the first result.

By Lemma 4 we have $g_a(e,k,q) = g_1(e,k,q)$ if $a = b^{k+1}$ for some $b \in \mathbb{F}_q$.

For $a = 1$, we have $D_e^{(1)}(x_1, \ldots, x_k, a) = u_1^e + \cdots + u_{k+1}^e$ with $u_1 \cdots u_{k+1} = 1$. We consider only those u_i with

$$u_{(k_0+1)i+1} \cdots u_{(k_0+1)i+k_0+1} = 1$$

for $i = 0, \ldots, \lfloor (k+1)/(k_0+1) \rfloor$ and $u_{(k_0+1)\lfloor (k+1)/(k_0+1) \rfloor + 1} = \cdots = u_{k+1} = 1$. Hence, $g_1(e,k,q)$ is not larger than the smallest g with $g\lfloor (k+1)/(k_0+1) \rfloor \ge g_1(e_{k_0}, k_0, q)$ and the second result follows.

The third result follows if we take $u_{k+1} = a$, split the remaining u_i in groups of $k_0 + 1$ elements with product 1 and put the remaining $u_i = 1$. □

Setting $k_0 = 1$ in Theorem 5, together with the first condition of Lemma 2, gives the following consequence.

COROLLARY 6. *Suppose $a \in \mathbb{F}_q^*$ and $\gcd(e, q-1) < 2^{-3/2}(q-2)^{1/2}$ or $\gcd(e, q+1) < 2^{-3/2}(q-2)^{1/2}$. Then,*

$$g_a(e,k,q) \le \left\lceil \frac{16}{\lfloor (k+1)/2 \rfloor} \right\rceil \quad \text{if } a = b^{k+1},\ k \ge 1,$$

and

$$g_a(e,k,q) \le \left\lceil \frac{16}{\lfloor k/2 \rfloor} \right\rceil \quad \text{if } a \ne b^{k+1},\ k \ge 2.$$

Set products and sums. We recall the following result of A. Glibichuk and M. Rudnev [**9**, Theorem 6].

LEMMA 7. *For any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$, with $\#\mathcal{A}\#\mathcal{B} > 2q$ we have*

$$\left\{ \sum_{j=1}^{8} a_j b_j \ :\ a_j \in \mathcal{A},\ b_j \in \mathcal{B},\ j = 1, \ldots, 8 \right\} = \mathbb{F}_q.$$

We will need the following extension of the Cauchy-Davenport inequality.

LEMMA 8. [**12**] *Let $\mathcal{B}$ be a finite non-empty subset of an Abelian group G. Then the following conditions are equivalent:*

1. *For every finite non-empty subset $\mathcal{A}$ of G, $|\mathcal{A}+\mathcal{B}| \ge \min(|\mathcal{A}| + |\mathcal{B}| - 1, |G|)$.*
2. *For every finite subgroup H of G, $|H+\mathcal{B}| \ge \min(|H| + |\mathcal{B}| - 1, |G|)$.*

LEMMA 9. *For $q = p^m$, let $\mathcal{B}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For any subgroup H of $\mathbb{F}_q$, $|H+\mathcal{B}| \ge \min(|H| + |\mathcal{B}| - 1, q)$.*

PROOF. We may restrict ourselves to the case $\{0\} \ne H \ne \mathbb{F}_q$. Put $|H| = p^j$ with $1 \le j < m$. Then at least $m-j$ elements of $\mathcal{B}$ are not in H and $H+\mathcal{B}$ contains at least $m-j+1$ different cosets $H+b$ with $b \in \mathcal{B}$. Hence,

$$\begin{aligned} |H+\mathcal{B}| &\ge (m-j+1)p^j \ge p^j + (m-j) + p^j - 1 \\ &\ge p^j + m - j + j - 1 = |H| + |\mathcal{B}| - 1, \end{aligned}$$

which completes the proof. $\square$

3. Existence of $g_1(e,k,q)$

In this section we give conditions on the existence of $g_1(e,k,q)$.

THEOREM 10. *For $k_0 = 1, \ldots, k+1$ put $\ell_{k_0} = \mathrm{lcm}(2, \ldots, k_0+1)$ and $e_{k_0} = \gcd(e, q^{\ell_{k_0}} - 1)$. We have $g_1(e,k,q) < \infty$ if either $e_1 \ne q^2 - 1$ and one of the two conditions of Lemma 1 with e_1 instead of e is satisfied or there exists $2 \le k_0 \le k+1$ such that $e_{k_0} \ne q^{\ell_{k_0}} - 1$ and*

$$\frac{q^{k_0} - 1}{p^t - 1} \nmid \gcd(e(q-1), q^{k_0} - 1) \quad \text{for all } t \mid k_0 m \text{ with } t < k_0 m.$$

PROOF. By Theorem 5 we have $g_1(e,k,q) < \infty$ if $g_1(e_{k_0}, k_0, q) < \infty$ for some $1 \le k_0 \le k+1$. Taking $k_0 = 1$, the first part of the theorem follows directly from Lemma 1. For the second part it is enough to consider the case $k_0 = k+1$. Let $u_j = u^{q^{j-1}}$, $j = 1, 2, \ldots, k+1$, where $\mathbb{F}_{q^{k+1}} = \mathbb{F}_q(u)$. This corresponds to the case that $r(Z)$ is irreducible. We have $\mathrm{Nm}_{k+1}(u) = u^{(q^{k+1}-1)/(q-1)} = 1$, that is, u is a $(q-1)$th power of an element of $\mathbb{F}_{q^{k+1}}$. Now, we get $D_e(x_1, \ldots, x_k, 1) = \mathrm{Tr}_{k+1}(u^e)$. Note that the eth powers u^e of elements in $\mathbb{F}_{q^{k+1}}$ of norm 1 are exactly the $(q-1)e$th powers in $\mathbb{F}_{q^{k+1}}$ and generate $\mathbb{F}_{q^{k+1}}$ over $\mathbb{F}_p$ if and only if

$$\frac{q^{k+1}-1}{p^t-1} \nmid \gcd(e(q-1), q^{k+1}-1) \quad \text{for all } t \mid (k+1)m \text{ with } t < (k+1)m.$$

Under this condition, there is a basis $\{u_1^e, \ldots, u_{(k+1)m}^e\}$ of $\mathbb{F}_{q^{k+1}}$ over $\mathbb{F}_p$ with $\mathrm{Nm}_{k+1}(u_1) = \cdots = \mathrm{Nm}_{k+1}(u_{(k+1)m}) = 1$. Hence,

$$\{\mathrm{Tr}_{k+1}(u_i^e) : i = 1, \ldots, (k+1)m\}$$

must contain a basis $\mathcal{B}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ since the trace is linear and surjective, and the existence follows by Lemmas 8 and 9. $\square$

4. Estimates for $g_a(e,k,q)$

We prove the following estimates which follow from Theorem 5 and the same argument as in [**13**, Theorem 1] using Lemma 7. We also improve Corollary 6 in some cases.

THEOREM 11. *Let $1 \le k_0 \le k$ be minimal such that*

$$\gcd\left(e, (q^{k_0+1}-1)/(q-1)\right) \le \frac{3}{8\sqrt{2}} q^{1/2}.$$

If a is a $(k+1)$th power in $\mathbb{F}_q^*$, then

$$g_a(e,k,q) \le \left\lceil \frac{8(k_0+1)}{\lfloor (k+1)/(k_0+1) \rfloor} \right\rceil$$

and otherwise if $k > k_0 + 1$,

$$g_a(e,k,q) \le \left\lceil \frac{8(k_0+1)}{\lfloor k/(k_0+1) \rfloor} \right\rceil.$$

PROOF. If $a = b^{k+1}$, by Theorem 5 we may assume $a = 1$.
By Lemma 3 we see that

$$\gcd(e, (q^{k_0+1}-1)/(q-1)) \le \frac{3}{8\sqrt{2}} q^{1/2}$$

implies

$$\#\mathcal{E} > 2^{1/2} q^{1/2}$$

since

$$\frac{3}{8\sqrt{2}}q^{1/2} < 2^{-1/2}\frac{q^{k_0+1}-1}{(2q^{k_0}-q^{k_0-1}-1)q^{1/2}}.$$

Thus, by Lemma 7 applied with the sets $\mathcal{A} = \mathcal{B} = \mathcal{E}$, we see that for any $c \in \mathbb{F}_q$ there are $u_j, v_j \in \mathbb{F}_{q^{k_0+1}}$ with $\mathrm{Nm}_{k_0+1}(u_j) = \mathrm{Nm}_{k_0+1}(v_j) = 1$, $j = 1, \dots, 8$ such that

$$\sum_{j=1}^{8} \mathrm{Tr}(u_j^e)Tr(v_j^e) = c,$$

by (5). Since

$$\mathrm{Tr}_{k_0+1}(u_j^e)\mathrm{Tr}_{k_0+1}(v_j^e) = \sum_{i=0}^{k_0} \mathrm{Tr}_{k_0+1}(u_j^e v_j^{eq^i})$$

again by (5), we get

$$g_1(e, k_0, q) \le 8(k_0+1)$$

if $\gcd(e, (q^{k_0+1}-1)/(q-1)) \le \frac{3}{8\sqrt{2}}q^{1/2}$. Theorem 5 completes the proof. Note that we get the strongest bound if k_0 is minimal. □

5. Final remarks

We remark that, using [**8**, Theorem 6], [**13**, Theorem 2] and Theorem 5, one can obtain easily a generalisation of [**13**, Theorem 2] for multivariate Dickson polynomials $D_e^{(1)}$, which we do not present here. We note, however, if $\gcd(e, q-1) < 0.75q^{2/3}$, from [**13**] we get

$$g_1(e, k, q) \le \left\lceil \frac{92160}{\lfloor (k+1)/2 \rfloor} \right\rceil.$$

For $a = 0$ a similar result as [**13**, Theorem 2] immediately follows from the character sum bound of Chang and Bourgain. More precisely, from [**3**, Theorem 1] it follows that for any $\varepsilon > 0$, if $e \le q^{1-\varepsilon}$ and $g_0(e, 1, q)$ exists, there is a constant $c(\varepsilon)$ such that $g_0(e, k, q) \le c(\varepsilon)$.

Furthermore, for $a = 0$ we easily get

$$g_0(e, k, q) \le \left\lceil \frac{8k_0}{\lfloor k/k_0 \rfloor} \right\rceil$$

if

$$\gcd(e, q^{k_0}-1) < q^{1/2}$$

for some $1 \le k_0 \le k$.

Moreover, we mention that

$$D_e^{(k)}(x_1, \dots, x_k, a) = (u_1^{-1}a)^e + \cdots + (u_{k+1}^{-1}a)^e = D_e^{(1)}(y_1, \dots, y_k, a^k)$$

for some $y_1, \dots, y_k$ and thus the corresponding value sets and Waring numbers are the same.

Finally, we mention that for very large e better results than ours can be obtained using the Cauchy-Davenport theorem. For very small e and k character sums are superior. See [**2, 7, 10**] for more details in the case $k = 1$.

Acknowledgement. The authors would like to sincerely thank the anonymous referee as well as D. Gomez and I. Shparlinski for their generous comments regarding a previous draft of this work.

References

[1] M. Bhaskaran, 'Sums of mth powers in algebraic and Abelian number fields', *Arch. Math.*, **17** (1966), 497–504.

[2] A. Bodin, P. Dèbes and S. Najib, 'Irreducibility of hypersurfaces', *Commun. Algebra*, **37** (2009), 1884-1900.

[3] J. Bourgain and M.-C. Chang, 'A Gauss sum estimate in arbitrary finite fields', *C. R. Math. Acad. Sci. Paris*, **342** (2006), 643–646.

[4] J. Cipra, 'Waring's number in a finite field', *Integers*, **9** (2009), 435–440.

[5] J. Cipra, T. Cochrane and C. G. Pinner, 'Heilbronn's conjecture on Waring's number mod p', *J. Number Theory*, **125** (2007), 289–297.

[6] T. Cochrane and C. Pinner, 'Sum-product estimates applied to Waring's problem mod p', *Integers*, **8** (2008), A46, 1–18.

[7] P. Deligne, 'La conjecture de Weil I', *Publ. Math. IHES*, **43** (1974), 273-307.

[8] A. Glibichuk, 'Sums of powers of subsets of arbitrary finite fields', *Izv. Ross. Akad. Nauk Ser. Mat.* (in Russian), **75** (2011), 35–68; translation in *Izvestiya. Mathematics*, **75**, 253–285.

[9] A. Glibichuk and M. Rudnev, 'On additive properties of product sets in an arbitrary finite field', *J. d'Analyse Math.*, **108** (2009), 159–170.

[10] D. Gomez and A. Winterhof, 'Waring's problem in finite fields with Dickson polynomials', *Finite Fields: Theory and applications*, Contemp. Math., v.477, Amer. Math. Soc., 2010, 185–192.

[11] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London-Harlow-Essex, 1993.

[12] H.B. Mann, 'An addition theorem for sets of elements of an abelian group', Proc. Am. Math. Soc., **4** (1953), 423.

[13] A. Ostafe and I. E. Shparlinski, 'On the Waring problem with Dickson polynomials in finite fields', *Proc. Amer. Math. Soc.*, **139** (2011), 3815–3820.

[14] A. Winterhof, 'On Waring's problem in finite fields', *Acta Arith.*, **87** (1998), 171–177.

[15] A. Winterhof and C. van de Woestijne, 'Exact solutions to Waring's problem in finite fields', *Acta Arith.*, **141** (2010), 171–190.

Department of Computing, Macquarie University, Sydney NSW 2109, Australia
E-mail address: alina.ostafe@mq.edu.au

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa ON, Canada, K1S 5B6
E-mail address: dthomson@math.carleton.ca

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, A-4040 Linz, Austria
E-mail address: arne.winterhof@oeaw.ac.at