PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 11, November 2011, Pages 3815–3820
S 0002-9939(2011)10843-8
Article electronically published on March 11, 2011

ON THE WARING PROBLEM WITH DICKSON POLYNOMIALS IN FINITE FIELDS

ALINA OSTAFE AND IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

Abstract. We improve recent results of D. Gomez and A. Winterhof on the Waring problem with Dickson polynomials in finite fields. Our approach is based on recent advances in arithmetic combinatorics in arbitrary finite fields due to A. Glibichuk and M. Rudnev.

1. Introduction

For a finite field $\mathbb{F}_q$ of q elements, and a parameter $a \in \mathbb{F}_q$, we define the sequence of Dickson polynomials $D_e(X, a)$, $e = 0, 1, \ldots$, recursively by

$$D_e(X, a) = XD_{e-1}(X, a) - aD_{e-2}(X, a), \qquad e = 2, 3, \ldots,$$

where $D_0(X, a) = 2$ and $D_1(X, a) = X$; see [12] for a background on Dickson polynomials.

D. Gomez and A. Winterhof [11] have considered an analogue of the Waring problem for Dickson polynomials over $\mathbb{F}_q$, that is, the question of the existence and estimation of a positive integer s such that the equation

$$D_e(u_1, a) + \cdots + D_e(u_s, a) = c, \qquad u_1, \ldots, u_s \in \mathbb{F}_q, \tag{1}$$

is solvable for any $c \in \mathbb{F}_q$; see also [3].

In particular, we denote by $g_a(e, q)$ the smallest possible value of s in (1) and put $g_a(e, q) = \infty$ if such an s does not exist.

Since for $a = 0$ we have $D_e(X, a) = X^e$, this case corresponds to the classical Waring problem in finite fields where recently quite substantial progress has been achieved; see [4, 5, 6, 14]. A survey of earlier results can also be found in [13]. So, we can restrict ourselves to the case of $a \in \mathbb{F}_q^*$.

Using the identity

$$D_e(v + av^{-1}, a) = v^e + a^e v^{-e}, \tag{2}$$

which holds for any nonzero v in the algebraic closure of $\mathbb{F}_q$ (see [11, Equation (1.1)]) and Weil-type bounds of additive character sums with rational functions, D. Gomez

Received by the editors September 12, 2010.
2010 *Mathematics Subject Classification.* Primary 11T06, 11T30.
During the preparation of this paper, the first author was supported in part by SNF Grant 121874 (Switzerland) and the second author by ARC Grant DP1092835 (Australia) and by NRF Grant CRP2-2007-03 (Singapore).

and A. Winterhof [11] have proved that for $s \geq 2$ the inequality $g_a(e,q) \leq s$ holds

- for any $a \in \mathbb{F}_q^*$ and

$$\gcd(e, q-1) \leq \frac{1}{8} q^{1/2 - 1/2(s-1)}; \tag{3}$$

- for $a = 1$ and

$$\gcd(e, q+1) \leq \frac{1}{8} q^{1/2 - 1/2(s-1)}. \tag{4}$$

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]. The question of the possibility of extending this technique to the Waring problem with Dickson polynomials has been posed in [11]. This work gives a positive answer to this. More precisely, we use a recent result of A. Glibichuk and M. Rudnev [10] to show that in fact $g_a(e,q)$ remains uniformly bounded even under much more liberal conditions than (3) and (4). We also replace the condition $a = 1$ by the weaker condition that a is a square in $\mathbb{F}_q^*$.

Theorem 1. *The inequality $g_a(e,q) \leq 16$ holds*

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

Clearly Theorem 1 gives a stronger estimate than that of [11] (that is, $g_a(e,q) \leq s$ under the conditions (3) and (4)) for

$$2^{-3/2}(q-2)^{1/2} \geq \gcd(e, q \pm 1) > \frac{1}{8} q^{7/15}.$$

Furthermore, it is easy to see that for a prime $q = p$, a result of J. Bourgain [1] (see also [2]) together with (2) immediately implies that for any fixed $\varepsilon > 0$ there exists a constant $C(\varepsilon)$ such that $g_a(e,p) \leq C(\varepsilon)$

- for any $a \in \mathbb{F}_p^*$ and $\gcd(e, p-1) \leq p^{1-\varepsilon}$;
- for any a that is a square in $\mathbb{F}_p^*$ and $\gcd(e, p+1) \leq p^{1-\varepsilon}$.

Here we use a result of A. Glibichuk and M. Rudnev [10] to get a fully explicit bound on $g_1(e,q)$ (note that the case of $a = 1$ is of principal interest in [11]) in arbitrary finite fields $\mathbb{F}_q$ provided that $\gcd(e, q^2-1) \leq q^{2-\varepsilon}$ and that at least one of the following conditions is satisfied:

$$\begin{gathered} \frac{q-1}{p^r - 1} \nmid e \text{ for all } r \neq m, \qquad p^{m/2} - 1 \nmid e \text{ if } k \geq 1, \\ \frac{q+1}{(2, p+1)} \nmid e \text{ if } \ell > 1, \end{gathered} \tag{5}$$

and

$$\frac{q+1}{(2, p+1)} \nmid e, \qquad \frac{q+1}{p^r + 1} \nmid e \text{ for all } r \mid m,\ r < m,\ m/r \text{ odd}, \tag{6}$$

where $q = p^m$ for a prime p and $m = 2^k \ell$ with a nonnegative integer k and an odd integer ℓ.

We note that by [11, Theorem 2.1] $g_1(e,d)$ exists if and only if at least one of the conditions (5) and (6) is satisfied.

Theorem 2. *For any positive $\varepsilon < 1$ and*

$$q \geq 2^{4\varepsilon^{-2}},$$

the inequality

$$g_1(e,q) \leq \begin{cases} 20 & \text{if } \varepsilon > 1/2, \\ \dfrac{5}{54} \cdot 24^n \left(1 + \left\lfloor \dfrac{\log n}{\log 2} \right\rfloor\right) & \text{if } \varepsilon \leq 1/2, \end{cases}$$

where $n = \lceil \varepsilon^{-1} + 5/6 \rceil$, holds

- **i.** *for any integer e with $\gcd(e, q-1) \leq (q-1)q^{-\varepsilon}$ for which (5) is satisfied;*
- **ii.** *for any integer e with $\gcd(e, q+1) \leq (q+1)q^{-\varepsilon}$ for which (6) is satisfied.*

In particular, it is noted in [11] that at least one of the conditions (5) and (6) is always satisfied, and thus $g_1(e,q)$ exists if $\gcd(e, q-1) < q^{1/2}$ or $\gcd(e, q+1) < 0.75q^{2/3}$. From Theorem 2 we derive an explicit uniform bound

$$g_1(e,q) \leq 92160,$$

which holds if one of these inequalities is satisfied provided q is large enough.

Finally, we note that the results and methods of arithmetic combinatorics have been used for several other additive problems; see [7, 8].

2. Preparations

2.1. **Background on Dickson polynomials.** As in [11], the identity (2) is one of our principal tools. We also need the following generalisation of [11, Equation (2.1)], which follows immediately from (2):

Lemma 3. *For any v and w in the algebraic closure of $\mathbb{F}_q$, we have*

$$D_e(v + av^{-1}, a) D_e(w + w^{-1}, 1) = D_e(vw + av^{-1}w^{-1}, a) + D_e(vw^{-1} + awv^{-1}, a).$$

For $a \in \mathbb{F}_q$ we consider the sets

$$\begin{aligned} \mathcal{D}_a &= \{D_e(v + av^{-1}, a) \ : \ v \in \mathbb{F}_q^*\}, \\ \mathcal{E} &= \{D_e(v + v^{-1}, 1) \ : \ v^{q+1} = 1, \ v \in \mathbb{F}_{q^2}\}. \end{aligned}$$

A simple remark is that $\mathcal{D}_a, \mathcal{E} \subseteq \mathbb{F}_q$. Indeed, for $\mathcal{D}_a$ it is obvious. To see this for $\mathcal{E}$ we put $u = D_e(v + v^{-1}, 1) = v^e + v^{-e}$ with $v^{q+1} = 1$ or, equivalently, $v^q = v^{-1}$. Then $u^q = v^{qe} + v^{-qe} = v^{-e} + v^e = u$, and thus $u \in \mathbb{F}_q$.

Lemma 4. *For any $a \in \mathbb{F}_q^*$, we have*

$$\#\mathcal{D}_a \geq \frac{q-1}{2\gcd(e, q-1)} \qquad \text{and} \qquad \#\mathcal{E} \geq \frac{q+1}{2\gcd(e, q+1)}.$$

Proof. To estimate $\#\mathcal{D}_a$ we remark that by the identity (2), $D_e(v + av^{-1}, a) = c$ is equivalent to $v^e = w$, where w is a root of $w + a^e w^{-1} = c$ and thus takes at most two possible values.

To estimate $\#\mathcal{E}$, we notice that the equation $v^{q+1} = 1$ has $q+1$ solutions in $\mathbb{F}_{q^2}$. □

2.2. **Set products and sums.** We recall the following result of A. Glibichuk and M. Rudnev [10, Theorem 6]:

Lemma 5. *For any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$, with $\#A\#\mathcal{B} > 2q$ 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 say that a set $\mathcal{A} \subseteq \mathbb{F}_q$ is *special* if for some $\alpha \in \mathbb{F}_q^*$ and a proper subfield $\mathbb{F}_r \subseteq \mathbb{F}_q$, $\mathbb{F}_r \neq \mathbb{F}_q$, we have

$$\{\alpha a \ : \ a \in \mathcal{A}\} \subseteq \mathbb{F}_r.$$

Otherwise, we say that $\mathcal{A}$ is *nonspecial*.

By [9, Theorem 6] we have

Lemma 6. *For any nonspecial set $\mathcal{A} \subseteq \mathbb{F}_q$ with $\#A > q^{1/(n-\delta)}$, an arbitrary integer $n \geq 2$ and a positive $\delta < 1$, we have*

$$\left\{\sum_{j=1}^{N(n,\delta)} \prod_{\nu=1}^{2n-2} a_{j,\nu} \ : \ a_{j,\nu} \in \mathcal{A},\ j = 1, \ldots, N(n,\delta),\ \nu = 1, \ldots, 2n-2\right\} = \mathbb{F}_q,$$

where

$$N(n,\delta) = \begin{cases} 10 & \text{if } n = 2; \\ 6^{n-3} \max\left\{30\left(3 + \left\lfloor \dfrac{\log \delta^{-1}}{\log 2} \right\rfloor\right), 160\left(1 + \left\lfloor \dfrac{\log n}{\log 2} \right\rfloor\right)\right\} & \text{if } n \geq 3. \end{cases}$$

We also recall that for special types of finite fields a series of stronger versions of Lemma 6 can be found in [9].

3. Proofs

3.1. **Proof of Theorem 1.** Let $\mathcal{V}_a$ be an arbitrary set of $v \in \mathbb{F}_q^*$ of cardinality $\#\mathcal{V}_a = \#\mathcal{D}_a$ and such that $\mathcal{D}_a = \{D_e(v + av^{-1}, a) \ : \ v \in \mathcal{V}_a\}$.

By Lemma 4 we see that if $\gcd(e, q-1) \leq 2^{-3/2}(q-2)^{1/2}$, then

$$\#\mathcal{V}_a = \#\mathcal{D}_a \geq 2^{1/2} \frac{q-1}{(q-2)^{1/2}} > 2^{1/2} q^{1/2}.$$

Thus, by Lemma 5, we see that for any $c \in \mathbb{F}_q$ there are $v_1, \ldots, v_8 \in \mathcal{V}_a$ and $w_1, \ldots, w_8 \in \mathcal{V}_1$ such that

$$\sum_{j=1}^{8} D_e(v_j + av_j^{-1}, a) D_e(w_j + w_j^{-1}, 1) = c.$$

Applying Lemma 3, we obtain the first assertion.

Now, if a is a square in $\mathbb{F}_q^*$, we find $b \in \mathbb{F}_q^*$ with $b^2 = a$ and remark that by (2) we have

$$\begin{aligned} D_e(b(v + v^{-1}), a) &= D_e(bv + a(bv)^{-1}, a) = (bv)^e + a^e (bv)^{-e} \\ &= b^e \left(v^e + v^{-e}\right) = b^e D_e(v + v^{-1}, 1). \end{aligned}$$

We now notice that if $v^{q+1} = 1$, then

$$v + v^{-1} = v + v^q \in \mathbb{F}_q.$$

Furthermore, by Lemma 3, we have

$$D_e(v+v^{-1},1)D_e(w+w^{-1},1) = D_e(vw+v^{-1}w^{-1},1) + D_e(vw^{-1}+wv^{-1},1),$$

and thus the proof follows the same lines as for the first assertion.

3.2. **Proof of Theorem 2.** We show first that at least one of the sets $\mathcal{D}_1$ and $\mathcal{E}$ is nonspecial under the conditions (5) and (6), respectively.

Assume that $\alpha\mathcal{D}_1$ or $\alpha\mathcal{E}$ is contained in a proper subfield of $\mathbb{F}_q$ for some $\alpha \in \mathbb{F}_q^*$. Taking $v = 1$ we see that $2 \in \mathcal{D}_1 \cap \mathcal{E}$, so if $\alpha\mathcal{D}_1$ or $\alpha\mathcal{E}$ belong to a proper subfield $\mathbb{F}_r$ of $\mathbb{F}_q$, then $\alpha \in \mathbb{F}_r$. Thus, if $\mathcal{D}_1$ is special, then $\mathcal{D}_1 \subseteq \mathbb{F}_r$; and if $\mathcal{E}$ is special, then $\mathcal{E} \subseteq \mathbb{F}_r$. Applying [11, Theorem 2.1] we see that the set $\mathcal{D}_1$ is nonspecial whenever condition (5) is satisfied and $\mathcal{E}$ is nonspecial whenever condition (6) is satisfied.

Now, using the notation of Lemma 6, we take

$$(n,\delta) = \begin{cases} (2, \min\{1/2, 2-2\varepsilon^{-1}\}) & \text{if } \varepsilon > 1/2; \\ \left(\left\lceil \varepsilon^{-1} + 5/6 \right\rceil, 1/2\right) & \text{if } \varepsilon \le 1/2. \end{cases}$$

We note that for $\varepsilon > 1/2$ we have

$$0.5q^{\varepsilon} > q^{\varepsilon/2} \ge q^{1/(n-\delta)}$$

for

$$q \ge 2^{4\varepsilon^{-2}} > 2^{2\varepsilon^{-1}}.$$

If $\varepsilon \le 1/2$, then $n - \delta > \varepsilon^{-1} + 1/3$; thus again we have

$$0.5q^{\varepsilon} > q^{1/(n-\delta)}$$

for

$$q \ge 2^{4\varepsilon^{-2}} \ge 2^{3\varepsilon^{-2}+\varepsilon^{-1}}.$$

Now, proceeding exactly as in the proof of Theorem 1 but applying Lemma 6 instead of Lemma 5 with $\mathcal{A} = \mathcal{D}_1$ in the case **i** and with $\mathcal{A} = \mathcal{E}$ in the case **ii**, we derive

$$g_1(e,q) \le 2^{2n-3} N(n,\delta),$$

and after simple calculations we obtain the desired result.

Acknowledgement

The authors are grateful to Arne Winterhof for valuable discussions and a careful reading of the original version of the paper.

References

[1] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.*, **18** (2005), 477–499. MR2137982 (2006b:11099)

[2] J. Bourgain, 'Some arithmetical applications of the sum-product theorems in finite fields', *Geometric aspects of functional analysis*, Lecture Notes in Math., vol. 1910, Springer, Berlin, 2007, 99–116. MR2347043 (2008j:11098)

[3] W.-S. Chou, G. L. Mullen and B. Wassermann, 'On the number of solutions of equations of Dickson polynomials over finite fields', *Taiwanese J. Math.*, **12** (2008), 917–931. MR2426536 (2009f:11148)

[4] J. Cipra, 'Waring's number in a finite field', *Integers*, **9** (2009), 435–440. MR2592521

[5] J. Cipra, T. Cochrane and C. Pinner, 'Heilbronn's conjecture on Waring's number (mod p)', *J. Number Theory*, **125** (2007), 289–297. MR2332590 (2008d:11116)

[6] T. Cochrane and C. Pinner, 'Sum-product estimates applied to Waring's problem mod p', *Integers*, **8** (2008), A46, 1–18. MR2472064 (2009m:11163)

[7] V. C. Garcia, 'On the distribution of sparse sequences in prime fields and applications', preprint, 2010 (available from `http://arxiv.org/abs/1008.4180`).

[8] V. C. Garcia, F. Luca and V. J. Mejia, 'On sums of Fibonacci numbers modulo p', *Bull. Aust. Math. Soc.* (to appear).
[9] A. Glibichuk, 'Sums of powers of subsets of arbitrary finite fields', *Izv. Ross. Akad. Nauk Ser. Mat.* (transl. as *Izvestiya. Mathematics)*, to appear (in Russian).
[10] A. Glibichuk and M. Rudnev, 'On additive properties of product sets in an arbitrary finite field', *J. d'Analyse Math.*, **108** (2009), 159–170. MR2544757 (2010i:11018)
[11] D. Gomez and A. Winterhof, 'Waring's problem in finite fields with Dickson polynomials', *Finite fields: Theory and applications*, Contemp. Math., vol. 477, Amer. Math. Soc., 2010, 185–192.
[12] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London-Harlow-Essex, 1993. MR1237403 (94i:11097)
[13] A. Winterhof, 'On Waring's problem in finite fields', *Acta Arith.*, **87** (1998), 171–177. MR1665204 (99k:11154)
[14] A. Winterhof and C. van de Woestijne, 'Exact solutions to Waring's problem in finite fields', *Acta Arith.*, **141** (2010), 171–190. MR2579843

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, CH-8057, Zürich, Switzerland
E-mail address: alina.ostafe@math.uzh.ch

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