Waring's Problem in Finite Fields with Dickson Polynomials

Domingo Gomez and Arne Winterhof

Abstract. We study the problem of finding or estimating the smallest number of summands needed to express each element of a fixed finite field as sum of values of a Dickson polynomial. We study the existence problem and prove several bounds using results from additive number theory and bounds on additive character sums.

1. Introduction

Let $q = p^r$ be a power of a prime p and denote by $\mathbb{F}_q$ the finite field of q elements. We recall that the family of *Dickson polynomials* $D_e(X, \alpha) \in \mathbb{F}_q[X]$ is defined by the following recurrence relation

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

with initial values

$$D_0(X,\alpha) = 2, \qquad D_1(X,\alpha) = X,$$

and $\alpha \in \mathbb{F}_q$. We refer to the monograph [**8**] for many useful properties and applications of Dickson polynomials.
Our aim is to study the following *Waring problem with Dickson polynomials in finite fields*.
We define $g_\alpha(e, q)$ as the smallest positive integer s such that every $y \in \mathbb{F}_q$ can be expressed as

$$y = D_e(u_1,\alpha) + \ldots + D_e(u_s,\alpha)$$

with $u_1, \ldots,\ u_s \in \mathbb{F}_q$.

This problem has been studied for $\alpha = 0$ by many authors, see [**1, 2, 5, 6, 11, 12, 13**] and references therein.

Here we focus on the case $\alpha = 1$ but state the results for arbitrary $\alpha \neq 0$ if possible.

If $u = \mu + \alpha\mu^{-1} \in \mathbb{F}_q^*$ with $\mu \in \mathbb{F}_{q^2}$, the property

$$D_e(\mu + \alpha\mu^{-1}, \alpha) = \mu^e + \alpha^e\mu^{-e}, \tag{1.1}$$

see [**8**], implies $D_e(u,\alpha) = D_f(u,\alpha)$ if $e \equiv f \bmod q^2 - 1$. Hence,

$$g_\alpha(e, q) = g_\alpha(\gcd(e, q^2 - 1), q)$$

1991 *Mathematics Subject Classification.* 11P05.

The first author is partially supported by the Project MTM2007-67088. He worked on the article during a pleasant research visit in Linz.

and we may restrict ourselves to the case

$$e|q^2-1.$$

In the case $r=1$ the number $g_\alpha(e,p)$ always exists. However, for $r>1$ it is possible that the value set of $D_e(X,\alpha)$ does not generate $\mathbb{F}_q$. For example, Equation (1.1) implies $g_\alpha(p^2-1,p)=p$ and $g_\alpha(q^2-1,q)$ does not exist for $r>1$.

We give necessary and sufficient conditions on the existence of $g_1(e,q)$ in Section 2. Sections 3 and 4 are devoted to bounds on $g_\alpha(e,q)$. We use results from additive number theory as well as bounds on additive character sums.

2. Existence of $g_1(e,q)$

In this section we characterize the pairs (e,q) such that $g_1(e,q)$ exists.

THEOREM 2.1. *Let $r=2^u v>1$ with an odd v. Then $g_1(e,q)$ exists if and only if one of the following two conditions holds*

1. $\dfrac{q-1}{p^d-1} \not| e$ *for all* $d|r,\ d\neq r,\quad (p^{r/2}-1)\not| e$ *if* $u\geq 1$,

   and $\dfrac{q+1}{\gcd(2,p+1)}\not| e$ *if* $v>1$.

2. $\dfrac{q+1}{(2,p+1)}\not| e$ *and* $\dfrac{q+1}{p^d+1}\not| e$ *for all* $d|r,\ d<r$, *with* r/d *odd.*

In particular, $g_1(e,q)$ *exists if* $\gcd(e,q-1)<q^{1/2}-1$ *or* $\gcd(e,q+1)<\frac{3}{4}q^{2/3}$.

PROOF. Put

$$\mathbf{D}=\{D_e(u_1,1)+\ldots+D_e(u_s,1): u_1,\ldots,\ u_s\in\mathbb{F}_q,\ s\in\mathbb{N}\}.$$

We have to characterize the conditions when $\mathbf{D}=\mathbb{F}_q$.

We consider the following vector spaces $\mathbf{A}$ and $\mathbf{B}$ over $\mathbb{F}_p$,

$$\begin{aligned}\mathbf{A} &= \{\ D_e(\mu_1+\mu_1^{-1},1)+\ldots+D_e(\mu_s+\mu_s^{-1},1):\mu_1,\ldots,\mu_s\in\mathbb{F}_q^*,\ s\in\mathbb{N}\},\\ \mathbf{B} &= \{\ D_e(\mu_1+\mu_1^{-1},1)+\ldots+D_e(\mu_s+\mu_s^{-1},1):\mu_1^{q+1}=\ldots=\mu_s^{q+1}=1,\\ &\quad\ \mu_1,\ldots,\mu_s\in\mathbb{F}_{q^2}^*,\ s\in\mathbb{N}\}.\end{aligned}$$

For $u\in\mathbb{F}_q^*$ the substitution $u=\mu+\mu^{-1}$ with $\mu\in\mathbb{F}_{q^2}^*$ implies either $\mu\in\mathbb{F}_q^*$ or $\mu^{q+1}=1$ since $u^q=\mu^q+\mu^{-q}=\mu+\mu^{-1}=u$. It is easy to see that

$$\mathbf{D}=\mathbf{A}+\mathbf{B}=\{a+b:a\in\mathbf{A},b\in\mathbf{B}\}.$$

Since

$$\begin{aligned}&D_e(\mu_1+\mu_1^{-1},1)D_e(\mu_2+\mu_2^{-1},1)=\\ &D_e(\mu_1\mu_2+(\mu_1\mu_2)^{-1},1)+D_e(\mu_1\mu_2^{-1}+\mu_1^{-1}\mu_2,1)\end{aligned}\tag{2.1}$$

by (1.1), we see that $\mathbf{A}$ and $\mathbf{B}$ are fields.

We note that $\mathbf{D}=\mathbb{F}_q$ implies $\mathbf{A}=\mathbb{F}_q$ or $\mathbf{B}=\mathbb{F}_q$.

The cardinality of $\mathbf{D}$ can be bounded by

$$|\mathbf{A}+\mathbf{B}|<|\mathbf{A}||\mathbf{B}|$$

since both fields contain $\mathbb{F}_p$. Using the fact that the cardinality of $|\mathbf{A}|=p^d$, $|\mathbf{B}|=p^{d'}$, where $d,\ d'$ are divisors of $r,\ q=p^r$, we get that $d=r$ or $d'=r$.

The problem has been reduced to prove in which cases

$$\mathbf{A}_1 = \{\ D_e(\mu+\mu^{-1},1) : \mu \in \mathbb{F}_q^*\ \} \quad \text{and}$$
$$\mathbf{B}_1 = \{\ D_e(\mu+\mu^{-1},1) : \mu \in \mathbb{F}_{q^2}^*, \mu^{q+1}=1\}$$

are both contained in a proper subfield.
If $\mathbf{A}_1 \subset \mathbb{F}_{p^d}$ for some $d|r$ with $d \neq r$, we have

$$\mu^e + \mu^{-e} = D_e(\mu+\mu^{-1},1) = D_e(\mu+\mu^{-1},1)^{p^d} = \mu^{ep^d} + \mu^{-ep^d}$$

for any $\mu \in \mathbb{F}_q^*$, in particular, for a primitive element $\mu = g$ of $\mathbb{F}_q$. This implies $g^{e(p^d-1)} = 1$ or $g^{e(p^d+1)} = 1$ and thus

$$e(p^d-1) \equiv 0 \mod q-1 \quad \text{or} \quad e(p^d+1) \equiv 0 \mod q-1. \tag{2.2}$$

If $\mathbf{B}_1 \subset \mathbb{F}_{p^{d'}}$ with $d'|r$ and $d' \neq r$ we get analogously

$$e(p^{d'}-1) \equiv 0 \bmod q+1 \quad \text{or} \quad e(p^{d'}+1) \equiv 0 \bmod q+1. \tag{2.3}$$

The number $g_1(e,q)$ does not exist if and only if (2.2) and (2.3) both hold for some proper divisors d and d' of r.

Finally, we simplify the conditions (2.2) and (2.3).
The first condition in (2.2) is $\frac{q-1}{p^d-1}|e$.
If r/d is odd, we have $\gcd(q-1,p^d+1) = \gcd(2,p^d+1) = \gcd(2,p+1)$ since $q-1 \equiv (p^d)^{r/d}-1 \equiv -2 \bmod p^d+1$ and thus the second condition in (2.2) is $\frac{q+1}{\gcd(2,p+1)}|e$.
If r is even and $d = r/2$, the second condition in (2.2) is $(p^{r/2}-1)|e$.
If r/d is even and $d < r/2$, the second condition is covered by $\frac{q-1}{p^{2d}-1}|e$.
Since $\gcd(p^{d'}-1,q+1) = \gcd(2,p+1)$ the first condition in (2.3) is $\frac{q+1}{\gcd(2,p+1)}|e$.
If r/d' is odd, the second condition in (2.3) is $\frac{q+1}{p^{d'}+1}|e$.
If r/d' is even, the second condition in (2.3) is $\frac{q+1}{\gcd(2,p+1)}|e$ which is already covered by the first condition in (2.3). □

For arbitrary α a result of the same flavor cannot be obtained since $\mathbf{A}$ and $\mathbf{B}$ are not fields in general.

3. Bounds based on addition theorems

3.1. A consequence of the Cauchy-Davenport theorem. In this subsection we prove the following bound on $g_\alpha(e,p)$ based on the Cauchy-Davenport theorem.

THEOREM 3.1. *We have*

$$g_\alpha(e,p) \leq 3\min\{\gcd(e,p-1),\gcd(e,p+1)\}, \quad p \geq 3.$$

PROOF. For $s \geq 1$ put

$$\mathbf{D}_s = \{D_e(u_1,\alpha)+\ldots+D_e(u_s,\alpha) : u_1,\ldots,u_s \in \mathbb{F}_p\}.$$

By the Cauchy-Davenport theorem we have

$$|\mathbf{D}_s| \geq \min\{|\mathbf{D}_{s-1}|+|\mathbf{D}_1|-1,p\}, \quad s \geq 2,$$

and get by induction

$$|\mathbf{D}_s| \geq \min\{s(|\mathbf{D}_1|-1)+1,p\}, \quad s \geq 1.$$

By the formula of [**3**] for the cardinality of $\mathbf{D}_1$ we get

$$\begin{aligned}|\mathbf{D}_1| &\geq \frac{p-1}{2\gcd(e,p-1)}+\frac{p+1}{2\gcd(e,p+1)}\\ &\geq \max\left\{\frac{p-1}{2\gcd(e,p-1)},\frac{p+1}{2\gcd(e,p+1)}\right\}+\frac{1}{2}.\end{aligned}$$

If $\gcd(e,p-1)\geq(p-1)/2$, we get trivially $g_\alpha(e,p)\leq p\leq 3\gcd(e,p-1)$.
If $\gcd(e,p-1)\leq(p-1)/3$, we get $\mathbf{D}_s=\mathbb{F}_p$ if

$$s\geq 2\gcd(e,p-1)\geq\frac{p-1}{(p-1)/2\gcd(e,p-1)-1/2}.$$

If $\gcd(e,p+1)\geq(p+1)/3$, we get $g_\alpha(e,p)\leq p\leq 3\gcd(e,p+1)$.
If $\gcd(e,p+1)\leq(p+1)/4$, we get $\mathbf{D}_s=\mathbb{F}_p$ if

$$s\geq 3\gcd(e,p+1)\geq\frac{p-1}{(p+1)/2\gcd(e,p+1)-1/2}$$

and the result follows. □

Note that the Cauchy-Davenport theorem is not valid in general for arbitrary finite fields.

For the case of prime fields and $\alpha=0$, sum-product techniques (see [**5**] and references therein) can be applied to derive very strong bounds on $g_0(e,p)$. It would be interesting to study this approach for $\alpha\neq 0$ as well.

3.2. Extension to arbitrary finite fields. In the case $\alpha=1$ we can reduce the problem of estimating $g_1(e,q)$ to the corresponding problem for prime fields.

THEOREM 3.2. *Let $q=p^r$. If $g_1(e,q)$ exists, then we have*

$$g_1(e,q)\leq 2r\max\{g_1(d,p),g_1(f,p)\},$$

where

$$d=\frac{d_1d_2}{\gcd(d_1,d_2)}$$

with

$$d_1=\frac{p-1}{\gcd\left(\frac{(q-1)}{\gcd(e,q-1)},p-1\right)}\quad\textit{and}\quad d_2=\frac{p+1}{\gcd\left(\frac{(q-1)}{\gcd(e,q-1)},p+1\right)}$$

and

$$f=\frac{f_1f_2}{\gcd(f_1,f_2)}$$

with

$$f_1=\frac{p-1}{\gcd\left(\frac{(q+1)}{\gcd(e,q+1)},p-1\right)}\quad\textit{and}\quad f_2=\frac{p+1}{\gcd\left(\frac{(q+1)}{\gcd(e,q+1)},p+1\right)}.$$

PROOF. As in the proof of Theorem 2.1 we see that either $\mathbf{A}=\mathbb{F}_q$ or $\mathbf{B}=\mathbb{F}_q$. Thus, we can select $\{\beta_1,\ldots,\beta_r\}$ a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ that either $\{\beta_1,\ldots,\beta_r\}\subset\mathbf{A}_1$ or $\{\beta_1,\ldots,\beta_r\}\subset\mathbf{B}_1$.
Each element of $\mathbb{F}_q$ is a linear combination of $\{\beta_1,\ldots,\beta_r\}$ and Equation (2.1) states that the products of elements of $\mathbf{A}_1$ or $\mathbf{B}_1$ can be expressed as a sum of elements of $\mathbf{A}_1$ or $\mathbf{B}_1$, respectively. So we are going to investigate how many summands of elements of $\mathbf{A}_1$ and $\mathbf{B}_1$ are necessary to generate $\mathbb{F}_p$.

First we suppose that $\{\beta_1, \ldots, \beta_r\} \subset \mathbf{A}_1$. For $\mu \in \mathbb{F}_q^*$ we have

$$D_e(\mu + \mu^{-1}, 1) = \mu^e + \mu^{-e} \in \mathbb{F}_p$$

if $\mu^e \in \mathbb{F}_p^*$ or $\mu^{e(p+1)} = 1$ with $\mu \in \mathbb{F}_{p^2}^*$. The eth powers in $\mathbb{F}_q^*$ are the $(q-1)/(e, q-1)$th roots of unity and the elements of $\mathbb{F}_p^*$ are the $(p-1)$th roots of unity in $\mathbb{F}_q^*$. Hence, the elements $\mu^e \in \mathbb{F}_p^*$ with $\mu \in \mathbb{F}_q^*$ are the $((q-1)/\gcd(e, q-1), p-1))$th roots of unity or the $d_1 = (p-1)/((q-1)/\gcd(e, q-1), p-1)$th powers in $\mathbb{F}_p^*$. Similarly, we see that the eth powers $\mu^e \in \mathbb{F}_q^*$ with $\mu^{e(p+1)} = 1$ are the $d_2 = (p+1)/((q-1)/\gcd(e, q-1), p+1)$th powers of elements $\mu \in \mathbb{F}_p^*$ with $\mu^{p+1} = 1$. Put $d = d_1 d_2/(d_1, d_2)$. Hence, the values $D_e(u, 1) \in \mathbb{F}_p$ with $u \in \mathbb{F}_q$ coincide with the values $D_d(u, 1)$ with $u \in \mathbb{F}_p$. Now every element of $\mathbb{F}_p$ is sum of at most $g_1(d, p)$ summands. By (2.1) all elements $u\beta_i,\ u \in \mathbb{F}_p,\ i = 1, \ldots, r$, are sums of $2g_1(d, p)$ elements and we get the bound

$$g_1(e, q) \leq 2rg_1(d, p).$$

If we assume $\{\beta_1, \ldots, \beta_r\} \subset \mathbf{B}_1$, we obtain

$$g_1(e, q) \leq 2rg_1(f, p)$$

analogously. □

4. Bounds derived by additive character sums

Theorems 3.1 and 3.2 give general bounds for arbitrary finite fields which are up to a constant best possible since $g(p^2-1, p) = p$. However, these results can be improved using bounds on additive character sums if $\min\{\gcd(e, q-1), \gcd(e, q+1)\}$ is small. Note that in this case $g_\alpha(e, q)$ always exists.

THEOREM 4.1. *We have*

$$g_\alpha(e, q) \leq s \quad \textit{if} \quad \gcd(e, q-1) \leq \frac{1}{8} q^{1/2 - 1/2(s-1)}, \quad s \geq 2.$$

For $\alpha = 1$ we have additionally

$$g_1(e, q) \leq s \quad \textit{if} \quad \gcd(e, q+1) \leq \frac{1}{2} q^{1/2 - 1/2(s-1)}, \quad s \geq 2.$$

PROOF. Without loss of generality we restrict ourselves to the cases when $s \geq 2$ and $e = \gcd(e, q-1)$ or $e = \gcd(e, q+1)$. First we consider the case $e = \gcd(e, q-1)$. In this case our technique works for all α whereas in the second case we need $\alpha = 1$.

Let χ be a nontrivial additive character of $\mathbb{F}_q$. By

$$\sum_{u \in \mathbb{F}_q} \chi(au) = \begin{cases} 0 & a \neq 0, \\ q & a = 0, \end{cases} \tag{4.1}$$

the number N_s of solutions of the equation

$$y = D_e(\mu_1 + \alpha\mu_1^{-1}, \alpha) + \ldots + D_e(\mu_s + \alpha\mu_s^{-1}, \alpha), \quad \mu_1, \ldots, \mu_s \in \mathbb{F}_q^*,$$

is

$$\begin{aligned} N_s &= \frac{1}{q}\sum_{u\in\mathbb{F}_q}\sum_{\mu_1,\ldots,\mu_s\in\mathbb{F}_q^*}\chi\left(u\left(\sum_{i=1}^s D_e(\mu_i+\alpha\mu_i^{-1},\alpha)-y\right)\right)\\ &= \frac{(q-1)^s}{q}+\frac{1}{q}\sum_{u\in\mathbb{F}_q^*}\sum_{\mu_1,\ldots,\mu_s\in\mathbb{F}_q^*}\chi\left(\sum_{i=1}^s uD_e(\mu_i+\alpha\mu_i^{-1},\alpha)\right)\\ &= \frac{(q-1)^s}{q}+\frac{1}{q}\sum_{u\in\mathbb{F}_q^*}\left|\sum_{\mu\in\mathbb{F}_q^*}\chi\left(uD_e(\mu+\alpha\mu^{-1},\alpha)\right)\right|^s. \end{aligned}$$

Since $e|q^2-1$ it is not divisible by p and by [**10**, Lemma 2] we see that the rational function $X^e+\alpha^eX^{-e}$ is not of the form A^p-A. Hence, we can apply the character sum bound of Moreno and Moreno [**9**, Theorem 2] which implies

$$\left(\max_{u\in\mathbb{F}_q^*}\left|\sum_{\mu\in\mathbb{F}_q^*}\chi\left(uD_e(\mu+\alpha\mu^{-1},\alpha)\right)\right|\right)^{s-2}\leq(2eq^{1/2})^{s-2}.$$

This implies that

$$\left|N_s-\frac{(q-1)^s}{q}\right| < \frac{(2eq^{1/2})^{s-2}}{q}\sum_{u\in\mathbb{F}_q}\left|\sum_{\mu\in\mathbb{F}_q^*}\chi\left(uD_e(\mu+\alpha\mu^{-1},\alpha)\right)\right|^2. \tag{4.2}$$

Expanding the inner sum, we get

$$\sum_{\mu_1,\ \mu_2\in\mathbb{F}_q^*}\sum_{u\in\mathbb{F}_q}\chi\left(u\left(D_e(\mu_1+\alpha\mu_1^{-1},\alpha)-D_e(\mu_2+\alpha\mu_2^{-1},\alpha)\right)\right).$$

By (4.1), we get that the inner sum is zero, except if

$$D_e(\mu_1+\alpha\mu_1^{-1},\alpha)-D_e(\mu_2+\alpha\mu_2^{-1},\alpha)=0.$$

For each μ_1 there exist at most $2e$ choices of μ_2 such that this equation holds. So, this sum is at most $2eq^2$. Substituting in (4.2), we get

$$\left|N_s-\frac{(q-1)^s}{q}\right|<(2eq^{1/2})^{s-1}q^{1/2}.$$

The number N_s is positive for all $y\in\mathbb{F}_q$ if

$$e\leq\frac{q^{1/2}}{8q^{1/2(s-1)}}$$

and thus $g_\alpha(e,q)\leq s$ under this condition.

Now we assume $e=\gcd(e,q+1)$ and $\alpha=1$, and denote by N_s the number of solutions of

$$y=D_e(\mu_1+\mu_1^{-1},1)+\ldots+D_e(\mu_s+\mu_s^{-1},1),\quad \mu_1^{q+1}=\ldots=\mu_s^{q+1}=1,$$

where we need bounds on

$$\max_{u\in\mathbb{F}_q^*}\left|\sum_{\substack{\mu\in\mathbb{F}_{q^2}^*,\\ \mu^{q+1}=1}}\chi\left(uD_e(\mu+\mu^{-1},1)\right)\right|.$$

Note that for μ with $\mu^{q+1}=\mathrm{Nm}_{\mathrm{q^2/q}}(\mu)=1$ we have $D_e(\mu+\mu^{-1},1)=\mu^e+\mu^{-e}=\mu^e+\mu^{eq}=\mathrm{Tr}_{\mathrm{q^2/q}}(\mu^e)$.
Let ψ be a multiplicative character of $\mathbb{F}_{q^2}$ of order e. Then we have

$$\frac{1}{e}\sum_{j=0}^{e-1}\psi^j(\xi)=\begin{cases}1, & \xi=\mu^e \text{ for some } \mu\in\mathbb{F}_{q^2}^*,\\ 0, & \text{otherwise,}\end{cases}\quad \xi\in\mathbb{F}_{q^2}^*.$$

Hence,

$$\sum_{\substack{\mu\in\mathbb{F}_{q^2}^*,\\ \mu^{q+1}=1}}\chi\left(uD_e(\mu+\mu^{-1},1)\right)=\sum_{j=0}^{e-1}\sum_{\substack{\xi\in\mathbb{F}_{q^2}^*,\\ \mathrm{Nm}_{\mathrm{q^2/q}}(\xi)=1}}\psi^j(\xi)\chi(\mathrm{Tr}_{\mathrm{q^2/q}}(\xi)).$$

(Note that each ξ which is an eth power equals μ^e for e different μ.) By [**7**, Theorem 2] the absolute value of the sum over ξ can be bounded by $2q^{1/2}$ and we get

$$\left|N_s-\frac{(q+1)^s}{q}\right|<(2eq^{1/2})^{s-2}\sum_{u\in\mathbb{F}_q}\left|\sum_{\substack{\mu\in\mathbb{F}_{q^2}^*,\\ \mu^{q+1}=1}}\chi\left(uD_e(\mu+\mu^{-1},1)\right)\right|^2.$$

Following a similar reasoning as in the previous case, $g_1(e,q)\le s$ if

$$e\le\frac{q^{1/2}}{2q^{1/2(s-1)}}.$$

This finishes the proof. □

Note that from [**4**, Theorem 10]

$$g_\alpha(e,q)\le s \text{ if } \gcd(e,q-1)+\gcd(e,q+1)\le\frac{q^{1/2}}{(q-1)^{1/s}}.$$

References

[1] Francis N. Castro, Ivelisse Rubio, Puhua Guan, and Raúl Figueroa. On systems of linear and diagonal equation of degree p^i+1 over finite fields of characteristic p. *Finite Fields Appl.*, 14(3):648–657, 2008.

[2] Francis N. Castro, Ivelisse Rubio, and José M. Vega. Divisibility of exponential sums and solvability of certain equations over finite fields. *Q. J. Math.*, 60(2):169–181, 2009.

[3] Wun Seng Chou, Javier Gomez-Calderon, and Gary L. Mullen. Value sets of Dickson polynomials over finite fields. *Journal of Number Theory*, 30:334–344, 1988.

[4] Wun Seng Chou, Gary L. Mullen, and Bertram Wassermann. On the number of solutions of equations of Dickson polynomials over finite fields. *Taiwanese J. Math.*, 12(4):917–931, 2008.

[5] Todd Cochrane and Christopher Pinner. Sum-product estimates applied to Waring's problem mod p. *Integers*, 8:A46, 18, 2008.

[6] S. V. Konyagin. Estimates for Gaussian sums and Waring's problem modulo a prime. *Trudy Mat. Inst. Steklov.*, 198:111–124, 1992.

[7] Wen-Ching Winnie Li. Character sums over norm groups. *Finite Fields Appl.*, 12(1):1–15, 2006.

[8] Rudolf Lidl, Gary L. Mullen, and Gerhard Turnwald. *Dickson Polynomials*. Longman, London-Harlow-Essex, 1993.

[9] Carlos Moreno and Oscar Moreno. Exponential sums and Goppa codes. *Proceedings of the American Mathematical Monthly*, 111:523–531, 1991.

[10] Harald Niederreiter and Arne Winterhof. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. *Acta Arith.*, 93(4):387–399, 2000.

[11] Christian van de Woestijne and Arne Winterhof. Exact solutions to waring's problem for finite fields. *Acta Arith.*, to appear.

[12] Arne Winterhof. On Waring's problem in finite fields. *Acta Arith.*, 87(2):171–177, 1998.

[13] Arne Winterhof. A note on Waring's problem in finite fields. *Acta Arith.*, 96(4):365–368, 2001.

Faculty of Sciences, University of Cantabria, Avd. Los Castros, Santander, Spain.
E-mail address: domingo.gomez@unican.es

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