Séminaires & Congrès
11, 2005, p. 29–40

ON THE CALCULATION AND ESTIMATION OF WARING NUMBER FOR FINITE FIELDS

by

Oscar Moreno & Francis N. Castro

Abstract. — In this paper we present a new method that often computes the exact value of the Waring number or estimates it. We also improve the lower bound for the Waring problem for large finite fields.

Résumé **(Sur le calcul et l'estimation du nombre de Waring pour les corps finis)**
Dans cet article, nous présentons une nouvelle méthode qui permet souvent de calculer la valeur exacte du nombre de Waring ou d'en donner une estimation. Nous améliorons également la borne inférieure relative au problème de Waring pour de grands corps finis.

1. Review of some results about the divisibility of the number of solutions of a system of polynomials over finite fields

In this section we present recent results about the divisibility of the number of solutions of a system of polynomials equation over finite fields.

Let k be a positive integer $k = a_0 + a_1p + a_2p^2 + \cdots + a_mp^m$ where $0 \leqslant a_i < p$. We define the p-weight of k by $\sigma_p(k) = \sum_{i=0}^{m} a_i$. The p-weight degree of a monomial $\boldsymbol{X}^d = X_1^{d_1} \cdots X_n^{d_n}$ is $w_p(\boldsymbol{X}^d) = \sigma_p(d_1) + \cdots + \sigma_p(d_n)$. The p-weight degree of a polynomial $F(X_1,\ldots,X_n) = \sum_d a_d\boldsymbol{X}^d$ is $w_p(F) = \max_{\boldsymbol{X}^d,\, a_d\neq 0} w_p(\boldsymbol{X}^d)$.

Let $F_1,\ldots,F_r$ be polynomials in n variables over $\mathbb{F}_q$, where $q = p^f$.

$$F_k(\boldsymbol{X}) = \sum_{i=1}^{N_k} a_{k_i}\boldsymbol{X}^{d_{ki}}.$$

2000 ***Mathematics Subject Classification***. — Primary 11T06; Secondary 11T23.
Key words and phrases. — Exponential sums, solutions of polynomial equations.

Let $|N|$ be the number of common zeros to the r polynomials. Introduce r auxiliary variables $Y_1, \ldots, Y_r$.

$$\begin{aligned} q^r|N| &= \sum_{(X_1,\ldots,X_n)\in\mathbb{F}_q} \Big(\sum_{Y_1\in\mathbb{F}_q} (Y_1F_1(X_1,\ldots,X_n))\Big)\cdots\Big(\sum_{Y_r\in\mathbb{F}_q} (Y_rF_r(X_1,\ldots,X_n))\Big) \\ &= \sum_{\boldsymbol{X}}\sum_{\boldsymbol{Y}} (Y_1F_1(\boldsymbol{X}) + \cdots + Y_rF_r(\boldsymbol{X})). \end{aligned}$$

We define L as follows

$$L = \min\Big\{\textstyle\sum_{k=1}^{r}\sum_{j=1}^{n}\sum_{i=1}^{N_k} \sigma(t_{ijk})/(p-1)\Big\} - rf, \tag{1}$$

where the minimum is taken over all t_{ijk}'s ($0 \leqslant t_{ijk} \leqslant q-1$), satisfying the following conditions

$$\begin{aligned} t_{111} + t_{221} + \cdots + t_{1N_11} &\equiv 0 \mod q-1, \\ t_{112} + t_{222} + \cdots + t_{2N_22} &\equiv 0 \mod q-1, \\ &\vdots \\ t_{11r} + t_{22r} + \cdots + t_{nN_rr} &\equiv 0 \mod q-1, \\ d_{111}t_{111} + d_{121}t_{121} + \cdots + d_{1N_rr}t_{1N_rr} &\equiv 0 \mod q-1, \\ d_{211}t_{211} + d_{221}t_{221} + \cdots + d_{2N_rr}t_{2N_rr} &\equiv 0 \mod q-1, \\ &\vdots \\ d_{n11}t_{n11} + d_{n21}t_{n21} + \cdots + d_{nN_rr}t_{nN_rr} &\equiv 0 \mod q-1. \end{aligned}$$

Now we are ready to state the main theorem of [**15**].

Theorem 1.1. — *Let $\mathcal{G}$ be the following class of polynomials*

$$\mathcal{G} = \{a_{11}\boldsymbol{X}^{d_{11}} + \cdots + a_{1N_1}\boldsymbol{X}^{d_{1N_1}}, \cdots, a_{r1}\boldsymbol{X}^{d_{r1}} + \cdots, a_{rN_r}\boldsymbol{X}^{d_{rN_r}} \mid a_{ij} \in \mathbb{F}_q\}.$$

With L as above, there are polynomials $F_1, \ldots, F_r$ in $\mathcal{G}$, such that $|N|$ is divisible by p^{L-fr} but not divisible by p^{L+1-fr}.

Theorem 1.1 gives a tight bound that involves the solution of a set of modular equations which are not always easy to solve. In [**15**], we introduced several techniques in order to give concrete approximate solutions.

The following result gives a dramatics improvement to Ax-Katz's, and Moreno-Moreno's results for certain diagonal equations.

Theorem 1.2. — *Let $q = p^f$ and let d_i be a divisor of $q^{m-1} + q^{m-2} + \cdots + 1$ for $i = 1, \ldots, n$. Let $a_1X_1^{d_1} + \cdots + a_nX_n^{d_n}$ be a polynomial over $\mathbb{F}_{q^{ml}}$. Then p^μ divides $|N|$, where $\mu \geqslant (n-m)lf$.*

Let s be the smallest positive integer such that the equation $x_1^d + \cdots + x_s^d = \beta$ has at least a solution for every $\beta \in \mathbb{F}_{p^f}$. We denote this s by $g(d, p^f)$. Let $L = \{x_1^d + \cdots + x_s^d \mid x_1, \ldots, x_s \in \mathbb{F}_{q^f}\}$. $g(d, p^f)$ exists if and only if L is not a proper subfield of $\mathbb{F}_{p^f}$ (see [**19**]). We will suppose from now on that $g(d, p^f)$ exists. Without loss of generality, we are going to assume throughout the paper that d divides $p^f - 1$. Note that if d divides $p^f - 1$, then $g(d, p^f) \geqslant 2$. Hence, the minimum value of $g(d, p^f)$ in the non-trivial case is 2. In [**13**], we proved the following theorem:

Theorem 1.3. — *$g(p^j + 1, p^f) = 2$ whenever $(p^j + 1) \mid (p^f - 1)$.*

Remark 1.4. — In [**5**], Helleseth indicates that is possible to combine the Theorem of Delsarte (see [**3**]) and other results to estimate the Waring number for finite fields of characteristic 2.

2. Review of Applications of Divisibility to Covering Radius

In this section we will state the main results of [**11**] and [**12**].

In [**11**], we solved a question posed in [**2**]. The question was to give an direct proof of the computation of the covering radius for $BCH(3)$ (see [**2**]). Recall that the covering radius of a code C is the smallest r such that the spheres $B_r(c) = \{c' \in C \mid d(c, c') \leqslant r\}$ with $c \in C$ cover $\mathbb{F}_q^n$ (n is the length of the code).

If a code C has minimum distance $2e + 1$ and all the coset leaders have weight $\leqslant e + 1$ then the code is called quasi-perfect (A coset leader of a coset $\alpha + C$ is a vector of smallest weight in its coset). The covering radius is the weight of a coset leader with maximum weight (see [**10**]).

Theorem 2.1. — *Let α be a primitive root of $\mathbb{F}_{2^f}$ and let C be the code of length $n = 2^f - 1$ with zeros α, α^d over $\mathbb{F}_{2^f}$, where $d = 2^i + 1$. If $(i, f) = 1$, then C is a quasi-perfect code.*

Theorem 2.2. — *Let α be a primitive root of $\mathbb{F}_{2^f}$. The code C with zeros $\alpha, \alpha^d, \alpha^{d'}$ and minimum distance 7, where $d = 2^i + 1$, and $d' = 2^j + 1$, has covering radius 5 for $f > 8$.*

Theorem 2.2 provided an elementary proof for BCH(3), as well as the Non-BCH triple error correcting codes of section 9.11 in [**10**]. Notice that the computation of the covering radius of BCH(3) required 3 papers (see [**1**], [**4**], and [**6**]). The first paper by J.A. van der Horst and T. Berger; the second paper by E.F. Assmus and H.F. Mattson used the Delsarte's bound, and the final paper by Helleseth invokes the Weil-Carlitz-Uchiyama bound.

An immediate consequence of the above theorem is the calculation of the covering radius of the Non-BCH triple correcting code of section 9.11 in [**10**].

Corollary 2.3. — *Let $f = 2t+1$ and α be a primitive root of $\mathbb{F}_{2^f}$. The code C with zeroes $\alpha, \alpha^d, \alpha^{d'}$, where $d = 2^{t-1}+1$, and $d' = 2^t+1$ has covering radius 5.*

Let d_1, d_2 be distinct natural numbers. Let $N(d_1, d_2, n, \mathbb{F}_q)$ be the number of solutions over $\mathbb{F}_q$ of the following system of polynomials equations:

$$x_1^{d_1} + x_2^{d_1} + x_3^{d_1} = \beta_1 x_4^{d_1}$$
$$x_1^{d_2} + x_2^{d_2} + x_3^{d_2} = \beta_2 x_4^{d_2}$$

Now we state a generalization of Theorem 2.1.

Theorem 2.4. — *Let α be a primitive root of $\mathbb{F}_{2^f}$ and let C be the code of length $n = 2^f - 1$ with zeros $\alpha^{d_1}, \alpha^{d_2}$ over $\mathbb{F}_{2^f}$. We assume that the minimum distance of C is 5. Then C is a quasi-perfect code whenever 4 divides $N(d_1, d_2, 4, \mathbb{F}_{2^f})$.*

Theorem 2.5. — *Let α be a primitive root of $\mathbb{F}_{2^{2t+1}}$, and let C be the code of length $n = 2^{2t+1} - 1$ with zeros $\alpha^{2^i+1}, \alpha^{2^j+1}$. If C has minimum distance 5, then C is quasi-perfect.*

Corollary 2.6. — *Let α be a primitive root of $\mathbb{F}_{2^f}$.*

(1) *Let $f = 2t+1$ and let C be the code of length $n = 2^{2t+1} - 1$ with zeros $\alpha^{2^{t-1}+1}, \alpha^{2^t+1}$ over $\mathbb{F}_{2^{2t+1}}$, then C is a quasi-perfect code.*

(2) *Let C be the code of length $n = 2^f - 1$ with zeros $\alpha, \alpha^{2^{2i}-2^i+1}$ over $\mathbb{F}_{2^f}$, then C is a quasi-perfect code whenever $(i, f) = 1$.*

Remark 2.7. — Note that the dual of the code C with zeroes α and $\alpha^{2^{2i}-2^i+1}$ over $\mathbb{F}_{2^f}$ for $f/(f,i)$ odd has three nonzero weights (Kasami code, see [**7**], [**8**]) and using a result of Delsarte (see [**10**]) gives that the covering radius is 3. For the case when $f/(f,i)$ is even, the result of Delsarte implies that the covering radius of C is at most 5.

3. On the Exact Value of Waring Number

In this section we introduce a new technique to compute the Waring number. This is a criterion to decide if the Waring number is equal to 2. We also generalize Theorem 1.3. Let p be a prime number, for any integer a, define $\mathrm{ord}_p(a)$ as follows:

$$\mathrm{ord}_p(a) = \max\{k \mid p^k \text{ divides } a\}.$$

Let $N_n(\beta)$ be the number of solutions of the equation $x_1^d + x_2^d + \cdots + x_{n-1}^d = \beta x_n^d$ over $\mathbb{F}_{p^f}^{\times}$.

Lemma 3.1. — *With the above notations. If $\sigma_p(c(p^f-1)/d) \geqslant f(p-1)/2$ for $1 \leqslant c \leqslant d-1$, then $p^{\lceil f/2 \rceil}$ divide $N_3(\beta)$ for any $\beta \neq 0$.*

Proof. — The system of modular equations associated to $x_1^d + x_2^d = \beta x_3^d$ is the following system:

$$\begin{aligned} dj_1 &\equiv 0 \mod p^f - 1 \\ dj_2 &\equiv 0 \mod p^f - 1 \\ dj_3 &\equiv 0 \mod p^f - 1 \\ j_1 + j_2 + j_3 &\equiv p^f - 1 \end{aligned} \tag{2}$$

(see [**14**, section 3] and [**15**, section IV]).

The solutions of the modular system of equations (2) determine the p-divisibility of $N_3(\beta)$, *i.e.*, if

$$\mu = \min_{\substack{(j_1,j_2,j_3) \\ \text{is a solution of (2)}}} \Big\{ \frac{\sigma_p(j_1) + \sigma_p(j_2) + \sigma_p(j_3)}{p-1} \Big\} - f,$$

then p^μ divides $N_3(\beta)$. Theorem 8 in [**14**] implies that is enough to consider $j_i \neq 0$ in the modular system (2). Note that the solutions of the first three equations are of the form:

$$j_i = \frac{c(p^f - 1)}{d} \quad \text{for } 1 \leqslant c \leqslant d, \tag{3}$$

since $dj_i = c(p^f - 1)$ where $c \leqslant d$. Note that if $c = d$, the $j_i = q - 1$, hence $\sigma_p(j_i) = f(p-1)$. Therefore we only need to consider c's satisfying $1 \leqslant c \leqslant d - 1$. We now apply the function σ_p to (3) and obtain that

$$\sigma_p(j_i) = \sigma_p\Big(\frac{c(p^f - 1)}{d}\Big) \geqslant \frac{f(p-1)}{2}.$$

Therefore $\sigma_p(j_1) + \sigma_p(j_2) + \sigma_p(j_3) \geqslant 3f(p-1)/2$. Therefore $\mu \geqslant \frac{3f}{2} - f = f/2$. Hence $p^{\lceil f/2 \rceil}$ divides $N_3(\beta)$. □

Remark 3.2. — Note that if d has p-weight 2, then d satisfies hypothesis of Lemma 3.1. But there are many d's such that $\sigma_p(d) > 2$ and $\sigma_2(c(p^f - 1)/d) \geqslant f(p-1)/2$ for $1 \leqslant c \leqslant d - 1$.

Theorem 3.3. — *Let $N(x_1^d + x_2^d)$ be the number of solutions of the equation $x_1^d + x_2^d = 0$ over $\mathbb{F}_{p^f}$. If $\sigma_p(c(p^f - 1)/d) \geqslant \frac{f(p-1)}{2}$ for $1 \leqslant c \leqslant d - 1$ and $\operatorname{ord}_p(N(x_1^d + x_2^d)) < \lceil f/2 \rceil$, then $g(d, p^f) = 2$.*

Proof. — We need to prove that the following equation has a solution:

$$x_1^d + x_2^d = \beta \tag{4}$$

for any $\beta \in \mathbb{F}_{p^f}$.

The proof consists of two steps:

Step 1. — Now we consider the homogenation of equation (4):

$$x_1^d + x_2^d = \beta x_3^d \tag{5}$$

By Lemma 3.1, the number of solutions of (5) is divisible by $p^{f/2}$.

Step 2. — We will prove that the equation (4) has solutions with $x_3 \neq 0$. If the equation (5) does not have solutions with $x_3 \neq 0$, then the equation

$$x_1^d + x_2^d = 0 \tag{6}$$

and equation (5) have the same number of solutions. But this is a contradiction since $p^{f/2}$ has to divide the number of solutions of (6) and $\mathrm{ord}_p(N(x_1^d + x_2^d)) < f/2$. Hence the equation (5) has at least one solution with $x_3 \neq 0$. Therefore the equation (4) has at least one solution for any $\beta \in \mathbb{F}_q$. Hence, we can conclude that $g(d, p^f) \leqslant 2$. We have that $g(d, p^f) \neq 1$ since d divides $p^f - 1$. □

Theorem 3.3 generalizes Theorem 1.3

Corollary 3.4

(1) *If -1 is a dth power in $\mathbb{F}_{p^f}$, $\sigma_p(c(p^f - 1)/d) \geqslant f(p-1)/2$ for $1 \leqslant c \leqslant d-1$ and* $\mathrm{ord}_p(d-1) < \lceil f/2 \rceil$*, then $g(d, p^f) = 2$. In particular, if the finite field has characteristic 2, we have $g(d, 2^f) = 2$ whenever* $\mathrm{ord}_2(d-1) < \lceil f/2 \rceil$ *and $= \sigma_p(c(p^f - 1)/d) \geqslant f(p-1)/2$ for $1 \leqslant c \leqslant d-1$.*

(2) *If $\sigma_p(c(p^f - 1)/d) \geqslant f(p-1)/2$ for $1 \leqslant c \leqslant d-1$, and -1 is not a dth power in $\mathbb{F}_{p^f}$, then $g(d, p^f) = 2$.*

Proof. — In case (1) we have that $x_1^d + x_2^d = 0$ has $(q-1)d + 1$ solutions over $\mathbb{F}_{p^f}$. Applying Theorem 3.3, we obtain part (1) of Corollary 3.4. The proof of (2) is similar. □

Example 3.5. — Let $q = 7^3$. We are going to compute $g(9, q^f) = 2$. Note that $\sigma_7(\frac{7^{3f}-1}{9}) = 8f$ (this implies that 7 divide $N_3(\beta)$) and -1 is a 9th power in $\mathbb{F}_{q^f}$. Hence $\mathrm{ord}_7(N(x_1^9 + x_2^9)) = 0 < 4f - 3f = f$. Therefore $g(9, q^f) = 2$.

Corollary 3.6. — *Let $q = p^f$ and let d be a divisor of $q+1$. If* $\mathrm{ord}_p(d-1) < mf$*, then $g(d, q^{2m}) = 2$.*

Proof. — Applying Corollary 3.4 and Theorem 1.2 we obtain the result. □

Previous theorem gives the exact value of the Waring number for many unknown cases.

Example 3.7. — Let $q = 2^{10}$. We are going to compute $g(11, q^f)$. Note that $\mathrm{ord}_2(11-1) = 1$. Applying Corollary 3.6, we obtain that $g(11, q^f) = 2$. Therefore $g(11, 2^f) = 2$ if $11 \mid (2^f - 1)$ and 1 otherwise. The same argument can be applied to $d = 13, 19$ and 43. Hence $g(13, 2^{12f}) = 2$, $g(19, 2^{18f}) = 2$ and $g(43, 2^{14f}) = 2$.

In general we obtain the following theorem that gives a way to estimate the Waring number:

Theorem 3.8. — *Let $N(x_1^d+\cdots+x_{n-1}^d)$ be the number of solutions of the equation $x_1^d+\cdots+x_{n-1}^d=0$ over $\mathbb{F}_{p^f}$. Let $l=\min_{1\leqslant c\leqslant d-1}\sigma_p(c\cdot\frac{p^f-1}{d})$. We have $g(d,p^f)\leqslant n-1$ whenever*

$$\operatorname{ord}_p\big(N(x_1^d+\cdots+x_{n-1}^d)\big)<\frac{ml}{p-1}-f.$$

Proof. — The hypothesis of Theorem 3.8 implies that $p^{\frac{mt}{p-1}-f}$ divides $N_n(\beta)$. If we assume that the equation $x_1^d+\cdots+x_{n-1}^d=\beta$ does not have a solution, then $N_n(\beta)=N(x_1^d+\cdots+x_{n-1}^d)$. But this is a contradition to $\operatorname{ord}_p\big(N(x_1^d+\cdots+x_{n-1}^d)\big)<\frac{mt}{p-1}-f$. □

Example 3.9. — We are going to compute $g(73,2^{9f})$. Using the techniques introduced in [**15**], it is easy to prove that $N(x_1^{73}+x_2^{73}+x_3^{73})=2k+1$ for some natural number k. Note that $\sigma_2((2^{9f}-1)/73)=3f$. Applying Theorem 3.8, we have $g(73,2^{9f})\leqslant 3$. The same argument can be applied to $d=23$. Hence $g(23,2^{11f})\leqslant 3$.

4. Previous Estimates for Waring Number of Large Finite Fields

I. Kaplansky made the following "outrageous conjecture" (according to C. Small in [**17**]): for each fixed positive integer d, every element of every sufficiently large finite field is a sum of two dth powers. In [**17**], C. Small showed that every finite field with more than $(d-1)^4$ elements is sufficiently large. Now we state C. Small's theorem:

Theorem 4.1. — *Let d be a positive integer, let $\mathbb{F}_{p^f}$ be a finite field, and put $l=(p^f-1,d)$. Assume $l>(d-1)^4$. Then*

$$g(d,p^f)\leqslant 2.$$

In particular the conclusion holds if $p^f>(d-1)^4$, since $d\geqslant l$.

Remark 4.2. — $g(d,p^f)=1\Longleftrightarrow 1=(p^f-1,d)$

The following theorem is an improvement to Theorem 4.1 (see [**9**, Example 6.38]).

Theorem 4.3. — *With above notations, we have that*

$$g(d,p^f)\leqslant 2\quad\textit{whenever } p^f>\frac{1}{4}\Big((d-1)(d-2)+\sqrt{d(d-1)(d^2-5d+8)}\Big)^2.$$

Theorems 4.1 and 4.3 give how large has to be $\mathbb{F}_{p^f}$ to guarantee $g(d,p^f)\leqslant 2$.

Let $\overline{N}_n$ be the number of solutions of the equation $x_1^d+x_2^d+\cdots+x_{n-1}^d=\beta x_n^d$ over $\mathbb{P}^{n-1}(\mathbb{F}_{p^f})$. The following theorems provide estimates for $\overline{N}_n$.

Theorem 4.4 **(Serre Improvement of Weil's Theorem)**

$$|\overline{N}_3 - (p^f + 1)| \leqslant \frac{(d-1)(d-2)}{2}\,[2\,p^{f/2}].$$

Theorem 4.5 **(Deligne)**

$$|\overline{N}_n - (p^{(n-2)f} + \cdots + p^f + 1)| \leqslant \frac{1}{d}((d-1)^n + (-1)^n(d-1))p^{(n-2)f/2}.$$

5. Calculation of Waring Number for Large Finite Fields

In [**17**], C. Small said that it would be interesting to know if the bound $(l-1)^4$ given in Theorem 4.1 is anywhere near the best possible. Motivated by this, we obtain an improvement to the Small's theorem.We also improved equation (1) in [**19**].

Remark 5.1. — Serre improvement of Weil's theorem implies that $g(d, p^f) = 2$ whenever $p^f > (d-1)(\frac{(d-2)}{2}[2\,p^{f/2}] + 1)$. This gives a modest improvement to Theorem 4.3 (see Table 1).

$g(d, p^{2t+1}) = 2$	Thm. 4.3	Remk. 5.1
$g(3, p^{2t+1}) = 2$	for $p^{2t+1} > 7$	for $p^{2t+1} > 8$
$g(4, p^{2t+1}) = 2$	for $p^{2t+1} > 41$	for $p^{2t+1} > 39$
$g(5, p^{2t+1}) = 2$	for $p^{2t+1} > 151$	for $p^{2t+1} > 142$
$g(6, p^{2t+1}) = 2$	for $p^{2t+1} > 409$	for $p^{2t+1} > 405$
$g(7, p^{2t+1}) = 2$	for $p^{2t+1} > 911$	for $p^{2t+1} > 906$
$g(8, p^{2t+1}) = 2$	for $p^{2t+1} > 1777$	for $p^{2t+1} > 1750$
$g(9, p^{2t+1}) = 2$	for $p^{2t+1} > 3151$	for $p^{2t+1} > 3116$
$g(10, p^{2t+1})$=2	for $p^{2t+1} > 5201$	for $p^{2t+1} > 5193$
$g(11, p^{2t+1}) = 2$	for $p^{2t+1} > 8119$	for $p^{2t+1} > 8110$
$g(12, p^{2t+1}) = 2$	for $p^{2t+1} > 12121$	for $p^{2t+1} > 12056$

TABLE 1

In [**17, 18, 16**], C. Small considered finding the largest prime field requiring three dth powers for $d = 3, 4$ and 5. Following this idea we want to find the largest prime field such $g(d, p) > 2$ for $d = 3, \ldots, 9$. Applying Remark 5.1 and the hypothesis that d divides $p - 1$ we obtain Table 2

Now using the computer we calculated the largest prime field requiring at least three dth powers to express its elements (see Table 3). We want to point out that in [**18**], the cardinality of some of these prime fields can be found.

$g(3,p)=2,\ p>7$	$g(7,p)=2,\ p>883$
$g(4,p)=2,\ p>37$	$g(8,p)=2,\ p>1721$
$g(5,p)=2,\ p>131$	$g(9,p)=2,\ p^f>3079$
$g(6,p)=2,\ p>397$	$g(10,p)=2,\ p>5171$

Table 2

$g(3,7)>2$
$g(4,29)>2$
$g(5,61)>2$
$g(6,223)>2$
$g(7,127)>2$
$g(8,761)>2$
$g(9,307)>2$

Table 3. Largest Prime Fields Requiring at Least Three dth Powers

Remark 5.2. — Note that cases $g(6,223)>2$, $g(8,761)>2$ imply that the lower bound on p^f cannot be improved to $(d-1)^3$, since $223>(6-1)^3=125$, $761>(8-1)^3>716$.

Let $\overline{N}_{4,0}$ be the number of solutions of the equation $x_1^d+x_2^d+x_3^d=\beta x_4^d$ with $x_4=0$ over $\mathbb{P}(\mathbb{F}_{p^f})$ and $\overline{N}_{4,1}$ be the number of solutions of the equation $x_1^d+x_2^d+x_3^d=\beta x_4^d$ with $x_4\neq 0$ over $\mathbb{P}(\mathbb{F}_{p^f})$. Now we estimate how large has to be $\mathbb{F}_{p^f}$ to obtain that $g(d,p^f)\leqslant 3$.

Theorem 5.3. — *$g(d,p^f)\leqslant 3$ whenever $p^{2f}>\frac{(d-1)(d-2)}{2}[2p^{f/2}]+\frac{1}{d}((d-1)^4+(d-1))p^f$.*

Proof. — We need to prove that the following equation has a solution:

$$x_1^d+x_2^d+x_3^d=\beta \tag{7}$$

for any $\beta\in\mathbb{F}_{p^f}$. Now consider the homogeneous of the equation (7):

$$x_1^d+x_2^d+x_3^d=\beta x_4^d \tag{8}$$

The proof consists of two steps:

Step 1. — By Theorem 4.5, we have that $\overline{N}_4$ satisfies

$$|\overline{N}_4-(p^{2f}+p^f+1)|\leqslant\frac{1}{d}((d-1)^4+(d-1))p^f. \tag{9}$$

Step 2. — We will prove that the equation (7) has a solution with $x_4 \neq 0$ for

$$p^{2f} - \frac{(d-1)(d-2)}{2}[2p^{f/2}] - \frac{1}{d}((d-1)^4 + (d-1))p^f > 0.$$

We have that

$$\overline{N}_4 \geqslant p^{2f} + p^f + 1 - \frac{1}{d}((d-1)^4 + (d-1))p^f.$$

Therefore

$$\overline{N}_{4,1} \geqslant p^{2f} + p^f + 1 - \overline{N}_{4,0} - \frac{1}{d}((d-1)^4 + (d-1))p^f. \tag{10}$$

We can conclude that

$$\begin{aligned} p^{2f} + p^f + 1 - \overline{N}_{4,0} - \frac{1}{d}((d-1)^4 + (d-1))p^f \\ \geqslant p^{2f} - \frac{(d-1)(d-2)}{2}[2p^{f/2}] - \frac{1}{d}((d-1)^4 + (d-1))p^f, \end{aligned}$$

since $\overline{N}_{4,0} \leqslant p^f + 1 + \frac{(d-1)(d-2)}{2}[2p^{f/2}]$. This completes the proof. □

Remark 5.4. — In Table 3, we computed the smallest prime field with $g(d,p) > 2$ for $i = 3, \ldots, 9$. Using Theorem 5.3, we have that $g(d,p) \leqslant 3$ for $(3,7)$, $(4,29)$, $(5,61)$, $(6,223)$, $(8,761)$. Hence we can compute the smallest prime field requiring three d-powers (see Table 4).

$g(3,7) = 3$
$g(4,29) = 3$
$g(5,61) = 3$
$g(6,223) = 3$
$g(8,761) = 3$

TABLE 4. Smallest Prime Fields Requiring Three dth Powers

Theorem 5.3 can be generalized to the following theorem.

Theorem 5.5. — *We have that*

$$g(d,p^f) \leqslant n-1$$

whenever

$$dp^{(n-1)f/2} - ((d-1)^n + (-1)^n(d-1))p^{f/2} - ((d-1)^{n-1} + (-1)^{n-1}(d-1)) > 0. \tag{11}$$

Remark 5.6. — Equation (14) in [**19**] gives the following estimate for $g(d,p^f) \leqslant n-1$ whenever $p^f > (d-1)^{2(n-1)/(n-2)}$. Theorem 5.5 gives an improvement of it. Let $u = p^{f/2}$, then equation (11) becomes

$$du^{n-1} - ((d-1)^n + (-1)^n(d-1))u - ((d-1)^{n-1} + (-1)^{n-1}(d-1) > 0.$$

If we evaluate this equation at $u = (d-1)^{(n-1)/(n-2)}$, then

$$\begin{aligned} d(d-1)^{(n-1)^2/(n-2)} &- ((d-1)^n + (-1)^n(d-1))(d-1)^{(n-1)/(n-2)} \\ &- ((d-1)^{n-1} + (-1)^{n-1}(d-1) \\ = (d-1)^{(n-1)^2/(n-2)} &- (-1)^n(d-1)^{(2n-3)/(n-2)} - (d-1)^{n-1} - (-1)^{n-1}(d-1) > 0 \end{aligned}$$

for $d > 4$.

References

[1] E.F. Assmus, Jr. & H.F. Mattson, Jr. – Some 3-error correcting BCH codes have covering radius 5, *IEEE Trans. Inform. Theory* **22** (1976), p. 348–349.

[2] G. Cohen, L. Honkala, S. Litsyn & A. Lobstein – *Covering radius*, North-Holland mathematical library, vol. 54, North-Holland, Amsterdam, 1997.

[3] P. Delsarte – Four fundamental parameter of a code and their combinational significance, *Inform. and Control* **23** (1973), p. 407–438.

[4] T. Helleseth – All binary 3-error correcting BCH codes of length 2^m-1 have covering radius 5, *IEEE Trans. Inform. Theory* **24** (1978), p. 257–258.

[5] ______, On the covering radius of cyclic Linear codes and arithmetic codes, *Discrete Appl. Math.* **11** (1985), p. 157–173.

[6] J. van der Horst & T. Berger – Complete decoding of triple-error-correcting binary BCH codes, *IEEE Trans. Inform. Theory* **22** (1977), p. 138–147.

[7] T. Kasami – Weight distribution of Bose-Chaudhuri-Hocquenghen codes, in *Combinatorial math. and its applications* (R.C. Bose & T.A. Dowling, eds.), Univ. of North Carolina Press, Chapel Hill, NC, 1969.

[8] ______, Weight enumerators of several classes of subcodes of the and order binary Reed-Muller codes, *Inform. and Control* **18** (1971), p. 369–394.

[9] R. Lidl & H. Niederreiter – *Finite fields*, Encyclopedia of mathematics and its applications, vol. 20, Addison-Wesley, Reading, Mass., 1983.

[10] F.J. MacWilliams & N.J.A. Sloane – *Theory of error-correcting codes*, North-Holland Publ. Comp., Amsterdam, 1977.

[11] O. Moreno & F.N. Castro – Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* **49** (2003), p. 3299–3303.

[12] ______, On the covering radius of certain cyclic codes, in *Proceedings of AAECC-15*, LNCS, vol. 2643, Springer, 2003.

[13] ______, Improvement of Ax-Katz's and Moreno-Moreno's results on the number of zeros of polynomials over finite fields and applications, *Internat. J. Pure and Appl. Math.* (accepted).

[14] O. Moreno & C.J. Moreno – The MacWilliams-Sloane conjecture on the tightness of the weight of duals of BCH codes, *IEEE Trans. Inform. Theory* **40** (1994), p. 1894–1907.

[15] O. Moreno, K. Shum, F.C. Castro & P.J. Kumar – Tight b for Chevalley-Warning-Ax Type estimates, with improved applications, *Proc. London Math. Soc.* **88** (2004), p. 545–564.

[16] C. Small – Solution of Waring's problem mod n, *Amer. Math. Monthly* **84** (1977), p. 356–359.

[17] ______, Sums of powers in large fields, *Proc. Amer. Math. Soc.* **65** (1977), p. 35–35.

[18] ______, Waring's problem mod n, *Amer. Math. Monthly* **84** (1977), p. 12–25.

[19] A. Winterhof – On Waring's problem in finite fields, *Acta Arith.* **LXXXVII** (1998), no. 2, p. 171–177.

O. Moreno, Department of Computer Science, University of Puerto Rico, Rio Piedras
E-mail : `moreno@uprr.pr`

F.N. Castro, Department of Mathematics, University of Puerto Rico, Rio Piedras
E-mail : `fcastro@goliath.cnnet.clu.edu`