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 $k = a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m$ 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: