International Journal of Pure and Applied Mathematics

Volume 19 No. 2 2005, 255-263

IMPROVEMENT OF AX-KATZ'S AND MORENO-MORENO'S RESULTS AND APPLICATIONS

Oscar Moreno[1], Francis N. Castro[2] §

[1]Department of Computer Sciences
University of Puerto Rico
Rio Piedras, P.O. Box 23355 SJ, 00931-3355, PUERTO RICO
[1]e-mail: moreno@uprr.pr

[2]Department of Mathematics
University of Puerto Rico
Rio Piedras, P.O. Box 23355 SJ, 00931-3355, PUERTO RICO
[2]e-mail: fcastro@goliath.cnnet.clu.edu

Abstract: In this paper we introduce the p^m-weight degree of a polynomial and using techniques of Ax-Katz, Moreno-Moreno and Adolphson-Sperber, we improve results of Ax-Katz, Moreno-Moreno and Adolphson-Sperber. Finally, we apply divisibility results to the Waring's problem and to the calculation of the covering radius of primitive codes with three zeros.

AMS Subject Classification: 11T06, 11T23
Key Words: Ax-Katz Theorem, Moreno-Moreno Theorem, Adolphson-Sperber Theorem, p^m-weight degree of a polynom

1. Results of Ax-Katz and Moreno-Moreno

The following notations will be used throughout the paper. Let p be a prime number and let $\mathbb{F}_p$ be the finite field of p elements. Let $\mathbb{F}$ be a finite field with p^f elements and let $\mathbb{F}'$ be subfield of $\mathbb{F}$ with p^m elements. $Tr_{\mathbb{F}/\mathbb{F}'}$ denotes the trace map from the finite field $\mathbb{F}$ to the finite field $\mathbb{F}'$.

Received: February 8, 2005

§Correspondence author

Let n be a positive integer $n = a_0 + a_1 p^m + a_2 p^{2m} + \cdots + a_l p^{ml}$, where $0 \leq a_i < p^m$ we define the p^m-weight of n by $\sigma_{p^m}(n) = \sum_{i=0}^{l} a_i$. The p^m-weight degree of a monomial $X^d = X_1^{d_1} \cdots X_n^{d_n}$ is $w_{p^m}(X^d) = \sigma_{p^m}(d_1) + \cdots + \sigma_{p^m}(d_n)$. The p^m-weight degree of a polynomial $F(X_1, \ldots, X_n) = \sum_d a_d X^d$ is $w_{p^m}(F) = \max_{X^d,\, a_d \neq 0} w_{p^m}(X^d)$.

Let $F_1, \ldots, F_t$ be polynomials in n variables with coefficients in $\mathbb{F}$ of total degrees $d_1, \ldots, d_t$, respectively, and $|N|$ be the number of simultaneous solutions of $F_1 = 0, \ldots, F_t = 0$. If μ is the least integer that satisfies $\mu \geq \frac{n - \sum_{i=1}^{t} d_i}{\max_i d_i}$, then $(p^f)^\mu$ divides $|N|$ (Ax-Katz's Theorem [3]). Also if μ is the smallest integer such that $\mu \geq f\left(\frac{n - \sum_{i=1}^{t} w_p(F_i)}{\max_i w_p(F_i)}\right)$, then p^μ divides $|N|$(Moreno-Moreno's Theorem [7]).

2. Improvement to Ax-Katz's and Moreno-Moreno's Results

In this section following [7], we will combine the reduction to the intermediate field method and the Ax-Katz's result to give an improvement to the Ax-Katz's and Moreno-Moreno's results.

We now explain how the reduction to the intermediate field method works. Given a monomial $X_1^{d_1} \cdots X_n^{d_n}$ over $\mathbb{F}$, we can choose a $\mathbb{F}'$-basis $\alpha_1, \ldots, \alpha_s$ of $\mathbb{F}$ such that $X_j = \sum_{i=1}^{s} x_{ji} \alpha_i$ for $j = 1, \ldots, n$. Note that since $|\mathbb{F}| = p^f$ and $|\mathbb{F}'| = p^m$, therefore $f = ms$. Then we use a similar procedure to that of [7], but with $X_j = \sum_{i=1}^{s} x_{ji} \alpha_i$, and we obtain a polynomial over $\mathbb{F}'$ of degree less than or equal to its p^m-weight degree.

Theorem 1. *Let $\mathbb{F}$ be a finite field with p^f elements and $\mathbb{F}'$ be a subfield of $\mathbb{F}$ with p^m elements. We let $F_1, \ldots, F_t$ be polynomials in n-variables over $\mathbb{F}$ and we use the above notations and if μ_m is the smallest integer such that*

$$\mu_m \geq s\left(\frac{n - \sum_{i=1}^{t} w_{p^m}(F_i)}{\max_i w_{p^m}(F_i)}\right),$$

then $(p^m)^{\mu_m}$ divides $|N|$.

Proof. Let $|N|$ be the number of solutions of the following system of polynomials equations $F_1(X_1, \ldots, X_n) = 0, \ldots, F_t(X_1, \ldots, X_n) = 0$ over $\mathbb{F}$.

We apply the reduction to the intermediate field method to $F_i(X_1, \ldots, X_n)$ for $i = 1, \ldots, t$ and obtain

$$F_i(X_1, \ldots, X_n) = \sum_{j=1}^{s} F'_{ij}(x_{11}, \ldots, x_{ns}) \alpha_j.$$

Note that the degree of $F'_{ij} \leq w_{p^m}(F_i)$ for $j = 1, \ldots, s$ and F'_{ij} is polynomial over $\mathbb{F}'$. We obtain

$$|N| = |N(F'_{11}, \ldots, F'_{ts})|,$$

where $|N(F'_{11}, \ldots, F'_{ts})|$ is the number of simultaneous solutions of $F'_{11}, \ldots, F'_{ts}$ over $\mathbb{F}'$. Now we consider the following system of polynomials equations over $\mathbb{F}'$: $F'_{11} = 0, F'_{12} = 0, \ldots, F'_{ts} = 0$. Now applying Ax-Katz's Theorem to the last system of polynomials equations we obtain the theorem. □

We now obtain the following corollary that improves Ax-Katz's, Moreno-Moreno's results and Theorem 1.

Corollary 2. *With the above notations. Let r be defined by*

$$r = \max_{\substack{\mathbb{F}' \text{ is a subfield} \\ \text{of } \mathbb{F}}} \left\{ |\mathbb{F}'|^{\mu_m} \ : \ \text{where } \mu_m \text{ is as defined in Theorem 1} \right\},$$

then r divides $|N|$.

Remark 1. Note that Corollary 2 generalizes Ax-Katz and Moreno-Moreno's Theorems in the following manner: when $\mathbb{F}' = \mathbb{F}$ we obtain Ax-Katz's result and when $\mathbb{F}' = \mathbb{F}_p$ we obtain Moreno-Moreno's result. Consequently, Corollary 2 is an improvement to both theorems.

Remark 2. Note if $w_p(F) = w_{p^m}(F)$, Theorem 1 improves Moreno-Moreno's Theorem whenever $w_{p^m}(F)$ does not divide sn.

Example 1. Let $q = p^f$ and $i_j \,|\, s$ for $j = 1, 2, 3$. Let $F(X_1, X_2, X_3) = a_1 X_1^{q^{i_1}+1} + a_2 X_2^{q^{i_2}+1} + a_3 X_3^{q^{i_3}+1} + \sum_{j,k} b_{jk} X_j X_k + \sum_m c_m X_m$ over $\mathbb{F}_{q^s}$. We have that $w_q(F) = 2$, hence $q^{\lceil \frac{s}{2} \rceil}$ divides the number of zeros of F. Note that the Ax-Katz's theorem does not provide any information about the zeros of F and Moreno-Moreno's Theorem implies that $p^{\lceil \frac{sf}{2} \rceil}$ divides the zeros of F. In particular, if $q = 2^{13}$ and $s = 3$, our theorem implies that 2^{26} divides the number of zeros of F and Moreno-Moreno's Theorem implies that 2^{20} divides the number of zeros of F.

3. Improvement to Theorem 1

Adolphson and Sperber in [1] gave a lower bound for the p-divisibility of exponential sums. They used the theory of Newton polyhedra in the proof of their theorem.

In this section, we will combine the reduction to the intermediate field method and the Newton polyhedra method of Adolphson and Sperber to give an improvement to Theorem 1.

Let $F(X) = F(X_1, \ldots, X_n)$ be a polynomial over $\mathbb{F}_{q^s}$ and let D be the set of all the integral vectors d corresponding to the monomials $a(d)X^d = a_{d_1,\ldots,d_n}X^{d_1}\cdots X_n^{d_n}$ of F. The Newton polyhedron $\Delta(F)$ is defined to be convex hull in $\mathbf{R}^n$ of the set $D\bigcup\{(0,\ldots,0)\}$. Let $\omega(F)$ be the smallest positive rational number such that $\omega(F)\Delta(F)$ contains at least one point with positive integral coordinates. Now, we state without proof (see [1]) the Adolphson and Sperber's Theorem.

Theorem 3. *With the above notations and assumptions, we have*

$$\mathrm{ord}_{q^s}(S(F)) \geq \omega(F),$$

where ψ is an additive character of $\mathbb{F}_q$ and

$$S(F) = \sum_{X_1,\ldots,X_n\in\mathbb{F}_q} \psi(F(X_1,\ldots,X_n)).$$

Now we combine Theorem 3 and the reduction to the intermediate field method to obtain the following result.

Theorem 4. *Let $F_1, \ldots, F_t$ be polynomials in n variables with coefficients in $\mathbb{F}_{q^s}$, a finite field. Let $w_q(F_i)$ be the q-weight degree of F_i. Let $\sum_{j=1}^{s} F'_{ij}\alpha_j$ be the polynomial corresponding to F_i after we apply the reduction method over $\mathbb{F}_q$ to it. Then*

$$ord_q(N(F_1,\ldots,F_t)) \geq \omega(\sum_{j=1}^{s}\sum_{i=1}^{t} y_{ij}F'_{ij}) - ts.$$

Now, we prove that Theorem 4 is an improvement to Theorem 1.

Theorem 5. *With the notations of previous theorem:*

$$\omega(\sum_{j=1}^{s}\sum_{i=1}^{t} y_{ij}F'_{ij}) - ts \geq s\left(\frac{n-\sum_{i=1}^{t} w_q(F_i)}{\max_i w_q(F_i)}\right).$$

Remark 3. Denote $\omega(\sum_{j=1}^{s}\sum_{i=1}^{t} y_{ij}F'_{ij})$ is the smallest positive rational number such that

$$\omega(\sum_{j=1}^{s}\sum_{i=1}^{t} y_{ij}F'_{ij})\Delta(\sum_{j=1}^{s}\sum_{i=1}^{t} y_{ij}F'_{ij})$$

contains at least one point with positive integral coordinates.

Proof. Adolphson and Sperber proved in [1] that Theorem 3 is an improvement to the Ax-Katz's Theorem. By applying Theorem 3 to the new system of polynomial equations obtained in the proof of Theorem 1 we obtain the desired result. □

4. Application to Waring's Problem

In this section, we compute the Waring's number when the powers are of the form $p^j + 1$. We refer to [9] for recent results and an excellent survey.

Let $g(d, p^f)$ be the smallest s such that the equation $X_1^d + \cdots + X_s^d = \beta$ has a solution for every $\beta \in \mathbb{F}_{p^f}$. We assume that $g(d, p^f)$ exists. Without loss of generality we can assume that d divides $p^f - 1$.

Theorem 6. *$g(p^j + 1, p^f) = 2$ whenever $(p^j + 1) \,|\, (p^f - 1)$.*

Proof. Note that $j \leq f/2$ since $(p^j + 1) \,|\, (p^f - 1)$. If $j = f/2$ then $g(p^j + 1, \mathbb{F}_{p^f})$ does not exist, therefore we can assume that $j < f/2$. What we need to prove is that the equation: $X_1^{p^j+1} + X_2^{p^j+1} = \beta$ has a solution for all $\beta \in \mathbb{F}_q$.

Let $|\mathcal{C}_\beta|$ and $|\mathcal{C}_0|$ be respective number of solutions of $X_1^{p^j+1} + X_2^{p^j+1} = \beta X_3^{p^j+1}$ and of $X_1^{p^j+1} + X_2^{p^j+1} = 0$ over $\mathbb{F}_{p^f}$. Applying Corollary 2, we obtain that $p^{f/2}$ divides $|\mathcal{C}_\beta|$. We will prove that the set $\mathcal{C}_\beta$ has an element (x_1, x_2, x_3) such that $x_3 \neq 0$. Otherwise $|\mathcal{C}_0| = |\mathcal{C}_\beta|$. Suppose now that the set $\mathcal{C}_\beta$ does not have an element with $x_3 \neq 0$. We have that $|\mathcal{C}_0|$ is equal to $p^j(p^f + p^{f-j} - 1)$ or 1 since $(p^j + 1) \,|\, (p^f - 1)$. But this is a contradiction since $p^{f/2}$ has to divide $|\mathcal{C}_0|$, i.e., $p^{f/2}$ divides $p^j(p^f + p^{f-j} + 1)$ or 1. Hence, the system has at least one solution with $x_3 \neq 0$ and the first equation has at least one solution for any $\beta \in \mathbb{F}_q$. Hence, we can conclude that $g(p^j + 1, p^f) = 2$. □

Note that in Theorem 6 we obtain the exact value of the Waring number, in other words, $g(p^j + 1, \mathbb{F}_{p^f}) = 2$. This is a nice result since there are few values of k, where the exact value for the Waring number is known. Actually, in the past, the results for Waring number were for any k: gives the best possible bound on $g(d, \mathbb{F}_{p^f})$, for example our Theorem 6 was known only for $f/4 > j$ (see [9]).

Remark 4. Applying Theorem 6 to coding theory, we obtain the following result:

Let α be a primitive root of $\mathbb{F}_{2^f}$. The code with zero α^{2^j+1} has minimum distance 2 and covering radius 2 whenever $(2^j+1) \mid (2^f-1)$ and $j < f/2$.

For more details about codes with a zero α^d (see [2]).

5. Applications to Coding Theory

The calculation of covering radius is important in coding theory and our method of this paper are applicable for this problem. In particular, we apply Corollary 2 to compute the covering radius of the primitive codes with zeros $\alpha, \alpha^{2^i+1}, \alpha^{2^{3i}+1}$ over $\mathbb{F}_{2^{2s+1}}$ (see [5]). Let $N_{d_1,d_2,d_3}(\beta_1,\beta_2,\beta_3)$ be the number solutions of the following system polynomial equations:

$$\begin{aligned} X_1^{d_1} + \cdots + X_5^{d_1} &= \beta_1 X_6^{d_1}, \\ X_1^{d_2} + \cdots + X_5^{d_2} &= \beta_2 X_6^{d_2}, \\ X_1^{d_3} + \cdots + X_5^{d_3} &= \beta_3 X_6^{d_3}. \end{aligned}$$

The following theorem gives a way to compute the covering radius.

Theorem 7. *Let α be a primitive root of $\mathbb{F}_{2^f}$. The code C with zeros $\alpha^{d_1}, \alpha^{d_2}, \alpha^{d_3}$ and minimum distance 7 has covering radius 5 whenever 32 divides $N_{d_1,d_2,d_3}(\beta_1,\beta_2,\beta_3)$ for every $(\beta_1,\beta_2,\beta_3)$.*

Proof. We need to prove that C has covering radius 5. Equivalently, we need to prove that the following system of equations has a solution

$$\begin{aligned} X_1^{d_1} + \cdots + X_5^{d_1} &= \beta_1, \\ X_1^{d_2} + \cdots + X_5^{d_2} &= \beta_2, \\ X_1^{d_3} + \cdots + X_5^{d_3} &= \beta_3, \end{aligned} \tag{1}$$

for any $(\beta_1,\beta_2,\beta_3) \in \mathbb{F}_{2^f}^3$. The proof consists of three steps:

Step 1. By hypothesis, we obtain that the number of solutions of the following system of polynomial equations

$$\begin{aligned} X_1^{d_1} + \cdots + X_5^{d_1} &= \beta_1 X_6^{d_1}, \\ X_1^{d_2} + \cdots + X_5^{d_2} &= \beta_2 X_6^{d_2}, \\ X_1^{d_3} + \cdots + X_5^{d_3} &= \beta_3 X_6^{d_3} \end{aligned} \tag{2}$$

is divisible by 32, i.e., 32 divides $N_{d_1,d_2,d_3}(\beta_1,\beta_2,\beta_3)$.

Step 2. We will prove that system (2) has solutions with $X_6 \neq 0$. If the system (2) does not have solutions with $X_6 \neq 0$, then

$$\begin{aligned} X_1^{d_1} + \cdots + X_5^{d_1} &= 0 \\ X_1^{d_2} + \cdots + X_5^{d_2} &= 0 \\ X_1^{d_3} + \cdots + X_5^{d_3} &= 0 \end{aligned} \tag{3}$$

and system (2) have the same number of solutions.

We say that a solution $(x_1, x_2, x_3, x_4, x_5)$ of (3) is non-trivial if all the x_i's are distinct. The system (3) does not have nontrivial solutions since the minimum distance of C is 7, i.e,. $x_{i_1} = 0, x_{i_2} = x_{i_3}, x_{i_4} = x_{i_5}$. Now we are going to compute the number of solutions of (3). Let $N = \{(x_1, \ldots, x_5) \,|\, (x_1, \ldots, x_5) \text{ is a solution of (3)}\}$ and $A_i = \{(x_1, \ldots, x_5) \in N \,|\, x_i = 0\}$. We have that $|N| = |A_1 \cup \cdots \cup A_5|$. Using the principle of inclusion-exclusion, we have that

$$\begin{aligned} |N| &= \sum_{i=1}^{5} |A_i| - \sum_{i_1<i_2} |A_{i_1} \cap A_{i_2}| + \sum_{i_1<i_2<i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &\quad - \sum_{i_1<i_2<i_3<i_4} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| + |A_1 \cap \cdots \cap A_5|. \end{aligned}$$

Therefore $|A_i| = 3q^2 - 2q$, $|A_{i_1} \cap A_{i_2}| = 3q - 2$, $|A_{i_1} \cap A_{i_2} \cap A_{i_3}| = q$, and $|A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| = 1 = |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5|$. Hence

$$|N| = 15q(q-2) + 16.$$

But this is a contradiction, since 32 has to divide $|N|$. Hence, we have that covering radius of C is 5. □

Theorem 7 generalizes Theorem 9 in [6], where we compute the covering radius of the $BCH(3)$ code.

An immediate consequence of the above theorem is the following corollary.

Corollary 8. *Let α be a primitive root of $\mathbb{F}_{2^f}$. The code C with zeros $\alpha, \alpha^{2^i+1}, \alpha^{2^{3i}+1}$ has covering radius 5 for $f > 7$ whenever $(f, i) = 1$ and f odd.*

Remark 5. In Corollary 8, we obtain the covering radius of the code of Theorem 17 in [4]. This has never been observed.

Conclusion

The results of Chevalley-Warning and Ax-Katz are classical in the theory of equations over finite fields. In recent times Moreno-Moreno and Adolphson-Sperber have improvements. In this paper we show that still further improvements are possible.

Acknowledgments

We would like to thank Dr. Arne Winterhof for his valuable suggestions.

References

[1] Adolphson, Sperber, p-adic estimates for exponential sums and the of Chevalley-Warning, *Ann. Sci. Ec. Norm. Super.*, **20**, No. 4 (1987), 545-556 (1987).

[2] T. Helleseth, On the covering radius of cyclic linear codes and arithmetic, *Disvrete Applied Mathematics*, **11** (1985), 157-173.

[3] N.M. Katz, On a theorem of Ax, *Amer. J. Math.*, **93** (1971), 485-499.

[4] J.H. van Lint, R.M. Wilson, On the minimum distance of cyclic codes, *IEEE Trans. on Inform Theory*, **32**, No.1 (1986), 23-40.

[5] F.J. MacWilliams, N.J.A. Sloane, *Theory of Error-Correcting Codes*, North-Holland Publ. Comp. (1977).

[6] O. Moreno, F.N. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* , **49**, No. 12 (2003), 3299-3303.

[7] O. Moreno, C.J. Moreno, Improvement of the Chevalley-Warning and the Ax-Katz Theorems, *Amer. J. Math.*, **117**, No. 1 (1995), 241-244.

[8] O. Moreno, K. Shum, F.N. Castro, P.V. Kumar, Tight bounds for Chevalley-Warning-Ax type estimates, with improved applications, *Proc. of the London Mathematical Society*, **88** (2004), 545-564.

[9] A. Winterhof, On Waring's problem in finite fields, *Acta Arithmetica* **LXXXVII**, No. 2 (1998), 171-177.