An Elementary Approach to Ax-Katz, McEliece's Divisibility and Applications to Quasi-Perfect Binary 2-Error Correcting Codes

Francis N. Castro
Department of Mathematics
University of Puerto Rico
Río Piedras, Puerto Rico 00931-3355
Email: fcastro@goliath.cnnet.clu.edu

Ivelisse Rubio
Department of Mathematics
University of Puerto Rico
Humacao, Puerto Rico 00791
Email: ive@mate.uprh.edu

Hugues Randriam
Ecole nationale supérieure des télécommunications
46 rue Barrault
75634 Paris Cedex 13 – France
Email: randriam@email.enst.fr

Oscar Moreno
Department of Computer Science
University of Puerto Rico
Rıio Piedras, Puerto Rico 00931-3355
Email: moreno@upr.pr

H. F. Mattson, Jr.
Electrical Engineering and Computer Science
Syracuse University CST 2-179
Syracuse, New York 13244-4100
Email: hmattson@syr.edu

***Abstract*— In this paper we present an algorithmic approach to the problem of the divisibility of the number of solutions to a system of polynomial equations. Using this method we prove that all binary cyclic codes with two zeros over $\mathbb{F}_{2^f}$ and minimum distance 5 are quasi-perfect for $f \leq 10$. We also present elementary proofs of divisibility results that, in some cases, improve previous results.**

I. Introduction

Even though the Ax-Katz, McEliece divisibility results have been used widely in coding theory (for example see [16],[10]) and cryptography (for example [3],[5]), most of the methods required advanced mathematical theory and were not algorithmic. This motivates us here to study elementary and algorithmic approaches to this problem.

In this paper we present new approaches to the problem of the divisibility of the number of solutions to a system of polynomial equations:

1) We use integer linear programming to estimate the divisibility in our generalization of McEliece's theorem [14]. In Section III, we show that this method has the advantage of being algorithmic and easy to program and, as a consequence, in Section IV we prove that all binary cyclic codes with two zeros over $\mathbb{F}_{2^f}$ and minimum distance 5 are quasi-perfect for $f \leq 10$. This new result is remarkable since it was previously thought that a double error-correcting code being quasi-perfect was a rare property.

2) We give an elementary proof of the divisibility result by Moreno-Moreno. For the prime field case we also present a new improvement to results by Adolphson-Sperber [1] and Ax-Katz [8], which solves a question raised by Ax in [2]. This proof is completely algorithmic, hence giving an elementary proof of the algorithmic treatment of the divisibility problem.

II. Generalization of McEliece's Theorem

The following is the characteristic 2 version of the well known theorem of McEliece [15] that we generalize to the multi-variable case:

Theorem 1 (McEliece [15]). *Let $\mathcal{C}$ be a binary cyclic code and let l be the smallest number such that $(l+1)$ nonzeros of $\mathcal{C}$ (with repetitions allowed) have product equal to 1. Then the weight of every codeword is divisible by 2^l and there is a codeword $\mathbf{w} \in \mathcal{C}$ such that 2^{l+1} does not divide the weight of $\mathbf{w}$.*

Let $F(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{N} a_i x_1^{e_{1i}} x_2^{e_{2i}} \cdots x_n^{e_{ni}}$ be a polynomial over a finite field $\mathbb{F}_{p^f}$. We denote by ζ a primitive p-th root of unity over $\mathbf{Q}$ and put $\theta = 1 - \zeta$, so that $pA = \theta^{p-1}A$ where $A = \mathbb{Z}[\zeta]$ is the ring of integers of $\mathbf{Q}(\zeta)$. Set $S(F) = \sum_{\mathbf{x} \in \mathbb{F}_{p^f}^n} \zeta^{Tr(F(\mathbf{x}))}$, where Tr is trace function from $\mathbb{F}_{p^f}$ to $\mathbb{F}_p$. We say that θ^l divides $S(F)$ if there exists $a \in \mathbb{Z}[\zeta]$ such that $S(F) = a\theta^l$. The divisibility of $S(F)$ gives us the divisibility of the number of solutions to a system of polynomial equations and hence the divisibility of the weights of codewords.

We associate to F the following system of modular equations:

$$\begin{array}{ccc} e_{11}t_1 + \cdots + e_{1N}t_N \equiv 0 \bmod p^f - 1 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ e_{n1}t_1 + \cdots + e_{nN}t_N \equiv 0 \bmod p^f - 1, \end{array} \tag{1}$$

where $0 \leq t_i \leq p^f - 1$. The system (1) determines the p-divisibility of $S(F)$; i.e., if

$$\mu = \min_{\substack{(t_1,\ldots,t_N) \\ is\ solution\ of (1)}} \{\sigma_p(t_1) + \cdots + \sigma_p(t_N)\}, \tag{2}$$

then p^μ divides $S(F)$, where σ_p is the p-weight function. In [14] we needed p-adic analysis and the theorem of Stickelberger to justify that $p^\mu | S(F)$; an innovation in this paper is that, in Section V, we present a completely elementary proof of this result.

The relation of McEliece's theorem and modular equations can be found in [4]. Now, using the above modular system and the properties of the p-weight function, the following generalization of McEliece's theorem [15] was proved in [14]. This also improves results by Ax-Katz [2] and Adolphson-Sperber [1].

Theorem 2. *Let $\mathcal{G}$ be the set of polynomials spanned by the monomials of F. That is,*

$$\mathcal{G} = \{a_1 x_1^{e_{11}} \cdots x_n^{e_{n1}} + \cdots + a_N x_1^{e_{1N}} \cdots x_n^{e_{nN}} \mid a_1, \ldots, a_N \in \mathbb{F}_{p^f}\}.$$

With μ as in (2), there is at least one polynomial $G \in \mathcal{G}$ such that $S(G)$ is divisible by θ^μ but not by $\theta^{\mu+1}$.

III. Divisibility Properties Reduced to a Problem in Integer Linear Programming

In this section we estimate the divisibility of the exponential sum $S(F)$ by associating it to a system of inequalities that form a problem of integer linear programming. Solving such a problem might be hard but, in many cases, we obtain good estimates using elementary methods.

The system (1) is equivalent to the following system of equations:

$$\begin{aligned} e_{11}t_1 + \cdots + e_{1N}t_N &= c_1(p^f - 1) \\ \vdots \qquad\qquad & \vdots \\ e_{n1}t_1 + \cdots + e_{nN}t_N &= c_n(p^f - 1), \end{aligned} \tag{3}$$

where $0 \le t_i \le p^f - 1$ and $c_i > 0$. Using the properties of the p-weight function σ_p, we obtain

$$\begin{aligned} \sigma_p(e_{11})\sigma_p(t_1) + \cdots + \sigma_p(e_{1N})\sigma_p(t_N) &\ge \sigma_p(c_1(p^f - 1)) \\ &\ge (p-1)f \\ \vdots \qquad\qquad & \vdots \qquad\qquad \vdots \\ \sigma_p(e_{n1})\sigma_p(t_1) + \cdots + \sigma_p(e_{nN})\sigma(t_N) &\ge \sigma_p(c_n(p^f - 1)) \\ &\ge (p-1)f. \end{aligned} \tag{4}$$

Now, our problem of finding the divisibility of $S(F)$ reduces to the integer linear programming problem of finding $\underline{\mu} = \min_{(T_1,\ldots,T_N)}\{T_1 + \cdots + T_N \mid, (T_1, \ldots, T_N)$ is a solution of system below$\}$:

$$\begin{aligned} \sigma_p(e_{11})T_1 + \cdots + \sigma_p(e_{1N})T_N &\ge (p-1)f \\ \vdots \qquad\qquad & \vdots \qquad\qquad \vdots \\ \sigma_p(e_{n1})T_1 + \cdots + \sigma_p(e_{nN})T_N &\ge (p-1)f. \end{aligned} \tag{5}$$

Note that $\underline{\mu} \le \mu$, therefore $\theta^{\underline{\mu}}$ divides $S(F)$ if θ^μ does.

IV. Quasi-perfect Cyclic Codes

In this section, we use the divisibility results and the algorithmic methods to obtain that every binary primitive cyclic code with two zeros over $\mathbb{F}_{2^f}$ and minimum distance 5 is quasi-perfect for $f \le 10$.

Let $N_{\beta_1,\beta_2}(d_1, d_2)$ be the number of solutions over $\mathbb{F}_{2^f}$ of the following system of polynomial equations:

$$\begin{aligned} x_1^{d_1} + x_2^{d_1} + x_3^{d_1} &= \beta_1 x_4^{d_1} \\ x_1^{d_2} + x_2^{d_2} + x_3^{d_2} &= \beta_2 x_4^{d_2}. \end{aligned} \tag{6}$$

Now consider the code $\mathcal{C}$ with zeros α^{d_1} and α^{d_2} over $\mathbb{F}_{2^f}$, where α is a primitive root of $\mathbb{F}_{2^f}$. $\mathcal{C}$ being quasi-perfect depends on the covering radius and the minimum distance of $\mathcal{C}$. Double error-correcting codes with two zeros over $\mathbb{F}_{2^f}$ are known for $f \le 25$ (for example, see [4]). The covering radius of $\mathcal{C}$ is 3 if and only if system (6) has a solution with $x_1 x_2 x_3 x_4 \ne 0$. The existence of this type of solutions to the system and hence quasi-perfection is given by the following theorem proved in [11].

Theorem 3. *Let α be a primitive root of $\mathbb{F}_{2^f}$ and let $\mathcal{C}$ be the code with zeros $\alpha^{d_1}, \alpha^{d_2}$ over $\mathbb{F}_{2^f}$, and minimum distance 5. Then $\mathcal{C}$ is a quasi-perfect code whenever 4 divides $N_{\beta_1,\beta_2}(d_1, d_2)$.*

Several infinite families of quasi-perfect codes with two zeros are known ([7], [5], [10]). Theorem 3 gives a way to get quasi-perfect codes, but, to apply it, we would need to give a theoretical proof that 4 divides $N_{\beta_1,\beta_2}(d_1, d_2)$ for all $(\beta_1, \beta_2) \ne (0, 0)$ and this can be very difficult. However, if we follow the techniques of Section III, we can determine divisibility with a computer program. For this, as in [14], consider the following modular system associated to (6):

$$\begin{aligned} d_1 t_1 + d_2 t_2 &\equiv 0 \bmod 2^f - 1 \\ &\cdots\vdots \\ d_1 t_7 + d_2 t_8 &\equiv 0 \bmod 2^f - 1 \\ t_1 + t_3 + t_5 + t_7 &\equiv 0 \bmod 2^f - 1 \\ t_2 + t_4 + t_6 + t_8 &\equiv 0 \bmod 2^f - 1. \end{aligned} \tag{7}$$

Now, we need to prove that $\mu > 2f + 1$, where μ is as defined in (2). Note that the computation of μ is not a difficult one. In the cases we computed, we only need to compute the minimum μ_p of just one modular equation,i.e.,

$$\mu_p = \min\{\sigma_2(u) + \sigma_2(v) \mid d_1 u + d_2 v \equiv 0 \bmod 2^f - 1\},$$

and this is simple. This is true since $\mu \ge 4\mu_p - 2f$.

Using the above procedure, we verified that $\mu > 2f + 1$ for $f \le 10$ and obtained the following result:

Theorem 4. *Let $\mathcal{C}$ be a binary primitive cyclic code with two zeros over $\mathbb{F}_{2^f}$ and minimum distance 5. If $f \le 10$, then $\mathcal{C}$ is a quasi-perfect code.*

Formerly, finding primitive quasi-perfect codes with minimum distance 5 and two zeros was considered difficult, but, as we mentioned, there are infinite families of such

codes. Now Theorem 4 suggests that it is difficult to find codes with minimum distance 5 that are not quasi-perfect.

Problem: Prove that all the binary primitive cyclic codes with two zeros and minimum distance 5 are quasi-perfect or find the smallest binary primitive cyclic code with two zeros and minimum distance 5 that it is not quasi-perfect.

V. Elementary Approach to the Divisibility of the Number of Solutions to Systems of Equations

There are several results on the divisibility of the number of solutions to systems of equations; some examples are the results by Ax-Katz ([2], [8]), Moreno-Moreno [12] and Adolphson-Sperber [1]. These results have been widely used in applications to coding theory (for example see [16],[10]) and cryptography (for example [3],[5]). However, the methods used to obtain these and other related results required advanced mathematics techniques such as p-adic analysis, the theorem of Stickelberger and Newton Polyhedra.

On [9] we presented an elementary proof of the Moreno-Moreno result for characteristic 2 that uses the covering method introduced in [13]. In the present paper we estimate the divisibility of exponential sums, for arbitrary characteristic, using a generalization of the covering method. This new generalization allows us to give a completely elementary proof of Moreno-Moreno's result [12] for any characteristic and improvements to Ax-Katz and Adolphson-Sperber's results over the prime field.

We have two different elementary proofs for this result [6]; the one that we sketch here is algorithmic for the prime field $\mathbb{F}_p$, providing then a completely elementary treatment of the algorithmic solution to the divisibility problem.

To generalize the covering method, let $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_N\}$ be a set of n-tuples, $\mathbf{e}_i = (e_{i1}, \ldots, e_{in})$, where each e_{ij} is a non-negative integer. Let $U = (\nu_i)_{1 \le i \le N}$ be an N-tuple of non-negative integers. If m is a positive integer, we say that U is an m-covering when the vector sum $\mathbf{f} = \nu_1\mathbf{e}_1 + \cdots + \nu_N\mathbf{e}_N$ has all its entries nonzero and divisible by m, or equivalently, when there exist positive integers $\lambda_1, \ldots, \lambda_n$ such that

$$\begin{array}{c} \nu_1 e_{11} + \cdots + \nu_N e_{N1} = m\lambda_1 \\ \cdots \\ \nu_1 e_{1n} + \cdots + \nu_N e_{Nn} = m\lambda_n. \end{array} \tag{8}$$

We define $\kappa_m(E)$, the m-th covering number of E, as the smallest cardinality of any such m-covering, that is the minimal value of $\nu_1 + \cdots + \nu_N$ for which the preceding system holds. One clearly has $\kappa_m(E) \le mn$.

Let now ζ be a primitive p-th root of unity over $\mathbf{Q}$ and put $\theta = 1 - \zeta$, so that $pA = \theta^{p-1}A$, where A is the ring of integers of $\mathbf{Q}(\zeta)$. Also let $F \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a polynomial in n variables with coefficients in the finite field $\mathbb{F}_p$ with p elements, and such that E is the set of exponent n-tuples of monomials that appear in F with non-zero coefficient, that is

$$F(\mathbf{x}) = \sum_{i=1}^{N} c_i \mathbf{x}^{\mathbf{e}_i} \tag{9}$$

with $c_i \in {\mathbb{F}_p}^{\times}$.

Consider $S = \{0, 1\}$ if $p = 2$, and, for $p \ge 3$ and g a generator of the group of units of $\mathbb{Z}_{p^n}$, $S = \{0\} \cup \left\{g^{ip^{n-1}} \mid 0 \le i \le p-2\right\}$. This implies that S is a complete residue system modulo p.

We put

$$\mathcal{S}(F) = \sum_{\mathbf{x} \in (\mathbb{F}_p)^n} \zeta^{F(\mathbf{x})} \in A. \tag{10}$$

By abuse of notation we will also write F for the polynomial with integral coefficients obtained by lifting $\mathbb{F}_p$ to S. Since ζ^m depends only on m modulo p, the preceding can also be written as

$$\mathcal{S}(F) = \sum_{\mathbf{s} \in S^n} \zeta^{F(\mathbf{s})}. \tag{11}$$

Now, if we write

$$\mathcal{S}(F) = \sum_{\mathbf{s} \in S^n} \prod_{i=1}^{N} (1-\theta)^{c_i \mathbf{s}^{\mathbf{e}_i}}, \tag{12}$$

and use the binomial theorem to expand

$$(1-\theta)^{c_i \mathbf{s}^{\mathbf{e}_i}} = \sum_{\nu \ge 0} \binom{c_i \mathbf{s}^{\mathbf{e}_i}}{\nu} (-\theta)^{\nu}, \tag{13}$$

we can obtain

Proposition 5. *With these notations, if $\mathcal{S}(F)$ is a rational integer, then it is divisible by $p^{\lceil \kappa_{p-1}(F)/(p-1) \rceil}$.*

With the above proposition we obtain the following new result, which gives an improvement of the main theorem of Adolphson-Sperber [1] for the finite field $\mathbb{F}_p$. The result of Adolphson-Sperber is an improvement to Ax-Katz's theorem ([2], [8]).

Theorem 6. *With the above notations, $\kappa_{p-1}(F) \ge \omega(F)$, where $\omega(F)$ is as defined in [1].*

Also note that $\kappa_{p-1}(E)$ coincides with μ of (2) when the finite field is $\mathbb{F}_p$, and we then obtain an elementary proof of the algorithmic treatment in Section III.

Combining the generalization of the covering method with a generalization of the reduction to the prime field method [12] we can obtain an elementary proof of the following result by Moreno-Moreno for an arbitrary finite field.

Theorem 7. *Let F_i be a polynomial over $\mathbb{F}_{p^f}$ with p-weight degree l_i, where $i = 1, \ldots, t$. Then the number simultaneous solutions of $F_1, \ldots, F_t$ over $\mathbb{F}_{p^f}$ is divisible by p^{μ}, where $\mu = \lceil \frac{f(n - \sum_{i=1}^{t} l_i)}{\max_i l_i} \rceil$.*

Acknowledgments

The authors want to thank Carlos Corrada, UPR-RP, for the calculation of the covering radius of the codes on Section IV that led to Theorem 4. They also appreciate the comments made by the referees and the remark that all primitive double error-correcting cyclic codes with two zeros over $\mathbb{F}_{2^f}$ are known for $f \le 25$. The work of Ivelisse Rubio was supported by Program URMAA, NSA Grant H98230-04-C-0486.

REFERENCES

[1] A. Adolphson and S. Sperber, "p-adic estimates for exponential sums and the theorem of Chevalley-Warning", *Ann. Scient. E. N. Superior* 4th. series **20** (1987), 545-556.

[2] J. Ax, "Zeros of polynomials over finite fields", *Amer. J. math.* **86** (1964),255-261.

[3] A. Canteaut, P. Charpin, H. Dobbertin, "Binary m-Sequences with Three-Valued Crosscorrelation: A Proof of Welch's Conjecture", *IEEE Trans. Inform. Theory*, **46**, pp. 4-8, 2000.

[4] A. Canteaut, P. Charpin, H. Dobbertin, Weight "Divisibility of Cyclic Codes, Highly Nonlinear Functions on F_{2^m}, and Crosscorrelation of Maximum Length Sequences", *SIAM J. DISCRETE MATH.* Vol. 13, No. 1, pp. 105-138, 2000.

[5] H. Dobbertin, T. Helleseth, P.V. Kumar and H. Martinsen, "Ternary m-Sequences with Three-Valued Cross-Correlation Function: New Decimations of Welch and Niho Type",*IEEE Trans. Inform. Theory*, **47**, pp. 1473-1481, 2001.

[6] H. Randriam, F. N. Castro, O. Moreno, I. Rubio and H. F. Mattson, Jr., "Generalization of the Covering Method for Arbitrary Characteristic and the Divisibility Properties of Exponential Sums", draft.

[7] T. Kasami, "Weight Distribution of Bose-Chaudhuri-Hocquenghen Codes", *Combinatorial Math. and its Applications* Univ. of North Carolina Press, Chapel Hill, NC 1969.

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

[9] O. Moreno, F. N. Castro, and H. F. Mattson, jr., Correction to "Divisibility properties for covering radius of certain cyclic codes". To appear, *IEEE Trans. Inform. Theory*

[10] O. Moreno and F. N. Castro, "Divisibility Properties for Covering Radius of Certain Cyclic Codes", *IEEE Trans. Inform. Theory* , **49**:12(2003), pp. 3299-3303.

[11] O. Moreno and F. N. Castro, "On the Covering Radius of Certain Cyclic Codes",*Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp.129-138, Springer.

[12] O. Moreno and C.J. Moreno, "Improvement of the Chevalley-Warning and the Ax-Katz theorems", *Amer. J. Math.* **117:**1 (1995), pp. 241-244.

[13] O. Moreno and C. J. Moreno, "The MacWilliams-Sloane Conjecture on the Tightness of the Carlitz-Uchiyama Bound and the Weights of Duals of BCH Codes", *IEEE Trans. Inform. Theory* **40**:6 (1994), pp. 1894-1907.

[14] O. Moreno, K. Shum, F. N. Castro & P.V. Kumar, "Tight Bounds for Chevalley-Warning-Ax Type Estimates, with Improved Applications", *Proc. London Math. Soc.* **88**, pp. 545-564, 2004.

[15] R. McEliece, "Weight congruences for p-ary cyclic codes", *Discrete Math.*, **3**(1972), pp. 177-192.

[16] H. N. Ward, "Weight Polarization and Divisibility", *Discrete Math.*, **83**, pp. 315-226, 1990.