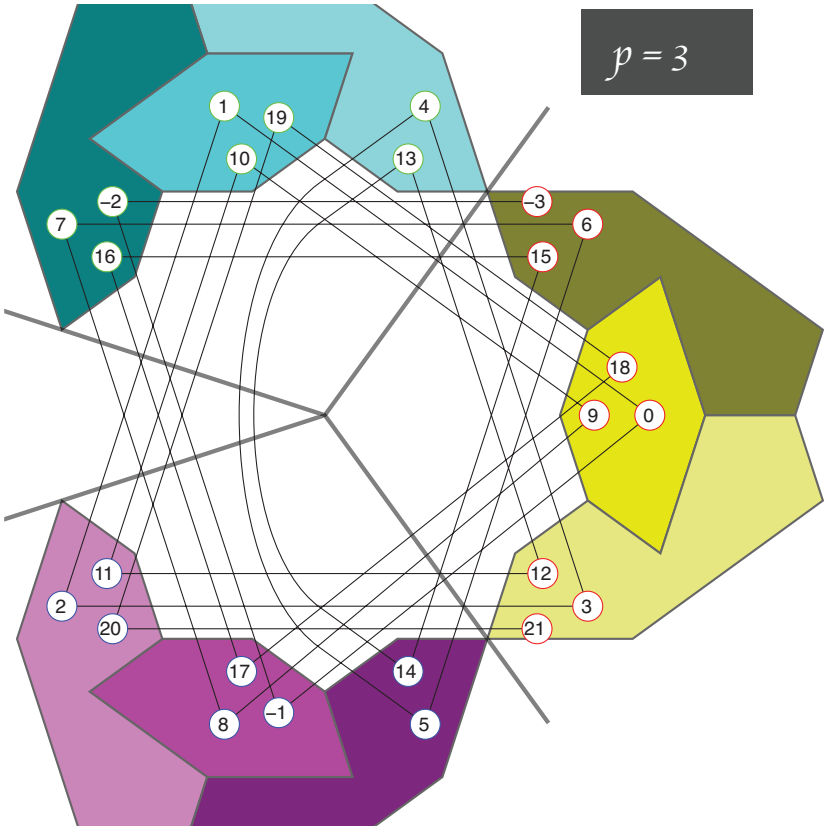
The Covering Method for Exponential Sums and Some Applications



Ivelisse M. Rubio

Introduction

Exponential sums over finite fields are an important tool for solving mathematical problems and have applications to many other areas. However, some of the methods and proofs of the results are nonelementary. The main purpose of this article is to present the covering method, an elementary and intuitive way to estimate or compute the p-divisibility of exponential sums, which is particularly convenient in the applications. The covering method allows us to determine solvability of systems of polynomial equations, improve the search for balanced Boolean functions, give better estimates for covering radius of codes, and has many other applications.

Solvability of systems of polynomial equations. One of the prominent problems in mathematics is to determine if a polynomial equation has solutions. In 1935 Artin conjectured that a homogeneous polynomial over a finite field has a nontrivial zero if the number of variables is larger than the degree. Chevalley obtained almost immediately a slightly better result changing the hypothesis of

Ivelisse M. Rubio is a professor of mathematics in the Department of Computer Sciences at the University of Puerto Rico, Río Piedras. Her email address is ivelisse.rubio@upr.edu.

Communicated by Notices *Associate Editor Emilie Purvine.*

DOI: https://doi.org/10.1090/noti2073

homogeneity to the weaker one of the polynomial having no constant term. Note that the homogeneous and the no-constant-term conditions imply that the polynomial has the trivial zero. The theorem guarantees additional zeros.

Warning improved Chevalley's result by proving that if the number of variables is larger than the sum of the degrees of a system of polynomials, then p, the characteristic of the field, divides the number of common zeros. This classical result is known as the Chevalley–Warning theorem and has an elementary proof [12, 20]. By elementary we mean that it uses only elementary results from number theory. Note that the number of zeros could be 0, but if the system has the trivial zero, Chevalley–Warning guarantees nontrivial solutions.

There are many results improving Chevalley–Warning's theorem. The results presented by Ax [2], Katz [11], Adolphson–Sperber [1], Moreno–Moreno [15], and Moreno et al. [17] have proofs that are nonelementary or semielementary. Other results presented by Moreno–Moreno [13], Wan [19], and Castro et al. [6] have entirely elementary proofs. As in the Chevalley–Warning theorem, solvability is not guaranteed; nontrivial solutions exist if the system has the trivial zero.

The covering method to study the p-divisibility of exponential sums is an elementary method introduced in [6] that lets us determine sufficient conditions to guarantee solvability and allows us to construct general families of solvable systems of polynomial equations [4, 5].

Applications to cryptography and coding theory. The divisibility of exponential sums has been used to characterize and prove properties in coding theory and cryptography [3, 7, 18]. The computation of bounds or the exact 2-divisibility of exponential sums of Boolean functions provides information on the Hamming weight of the function and can be used to obtain information on the covering radius and the weight distribution of certain codes. These properties are important for the analysis of decoding algorithms and are also related to cryptography, as they can be used to study nonlinearity and to search for balanced Boolean functions.

Exponential Sums Associated to Polynomials

We will restrict our exposition to exponential sums associated to polynomials in $\mathbb{F}_p[X_1, \dots, X_n]$, where p is a prime number and $\mathbb{F}_p$ is the finite field with p elements. The definition of these exponential sums depends on ζ, a pth root of unity over the p-adic field

$$\mathbb{Q}_p = \left\{a_r p^r + a_{r+1}p^{r+1} + \cdots \mid a_i \in \{0, \dots, p-1\}, r \in \mathbb{Z}\right\}.$$

For $a_r \neq 0$, define the **p-adic valuation of** $x = a_r p^r + a_{r+1}p^{r+1} + \cdots \in \mathbb{Q}_p$ as $v_p(x) = r$, the highest power of p dividing x, $v_p(0) = \infty$. We also call $v_p(x)$ the **p-divisibility of** x. If $v_p(x) \neq \infty$, we say that $v_p(x)$ is the **exact p-divisibility** of x.

Example 1. Consider $x = 36 = (3^2)(4) \in \mathbb{Z}$. Note that we can also represent x as $x = 3^2 + 3^3 \in \mathbb{Q}_3$. This implies that the exact 3-divisibility of 36 is 2. That is, $v_3(36) = 2$.

The set of p-adic integers is the local ring $\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\right\}$ with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. One can use this valuation to define the **p-adic absolute value of** x by $|x|_p = p^{-v_p(x)}$ if $x \neq 0$ and $|0|_p = 0$.

The p-adic field $\mathbb{Q}_p$ is a completion of the rationals $\mathbb{Q}$, and its construction is similar to the construction of the real numbers $\mathbb{R}$ from $\mathbb{Q}$ but using the p-adic absolute value. So, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|.|_p$. The p-adic numbers offer a different perspective to study problems, and these methods can be helpful to understand concepts and prove properties that may be difficult without them. For an accessible introduction to the beautiful theory of p-adic numbers we refer the reader to [9].

For a polynomial $F \in \mathbb{F}_p[\mathbf{X}]$, where $\mathbf{X} = (X_1, X_2, \dots, X_n)$, and ζ a primitive pth root of unity over $\mathbb{Q}_p$, let $\zeta^a = \zeta^{a \bmod p}$, and define the **exponential sum associated to** F as

$$S(F) = \sum_{\mathbf{x} \in (\mathbb{F}_p)^n} \zeta^{F(\mathbf{x})} \in \mathbb{Z}_p.$$

The explicit evaluation of the exponential sum of a polynomial might be a difficult task, but for many applications it is enough to have estimates for $v_p(S(F))$. For simplicity, in some of the results in this article we consider only one polynomial, but the results can be extended to systems of polynomials $F_1, F_2, \dots, F_t \in \mathbb{F}_p[\mathbf{X}]$ by adding t extra variables $Y_1, \dots, Y_t$ (one per polynomial) and constructing a new polynomial $P = Y_1F_1 + Y_2F_2 + \cdots + Y_tF_t$. The **exponential sum associated to the system of polynomials** $F_1, F_2, \dots, F_t$ is the exponential sum associated to P. The relation between the number $\mathcal{N}$ of elements $(x_1, \dots, x_n) \in \left(\mathbb{F}_p\right)^n$ that are common zeros of the system and the exponential sum associated to the system is given by the following lemma:

Lemma 1. *Let $\mathcal{N}$ be the number of common zeros of $F_1, F_2, \dots, F_t \in \mathbb{F}_p[\mathbf{X}]$. Then*

$$\mathcal{N} = p^{-t} \sum_{\mathbf{x} \in (\mathbb{F}_p)^n, \mathbf{y} \in (\mathbb{F}_p)^t} \zeta^{y_1F_1(\mathbf{x}) + y_2F_2(\mathbf{x}) + \cdots + y_tF_t(\mathbf{x})}.$$

Since $\mathcal{N} = p^{-t}S(Y_1F_1 + Y_2F_2 + \cdots + Y_tF_t) = p^{-t}S(P)$, computing the exact value of $\mathcal{N}$ depends on the computation of $S(P)$, which is not easy. However, if we can get the exact p-divisibility of $S(P)$, $v_p(\mathcal{N}) < \infty$, we know that $p^{v_p(\mathcal{N})+1} \nmid \mathcal{N}$. This implies that $\mathcal{N} \neq 0$ and the system is solvable. Therefore, being able to compute the exact p-divisibility of an exponential sum of a system of polynomials gives a criterion for solvability of the system.

2-Divisibility of Exponential Sums of Boolean Functions

Most of the applications of exponential sums to coding theory and cryptography consider Boolean functions $f : (\mathbb{F}_2)^n \longrightarrow \mathbb{F}_2$. Any Boolean function f can be identified with a unique Boolean polynomial $F = \sum_{\mathbf{e}\in \mathrm{Supp}(F)} \mathbf{X}^{\mathbf{e}}$, where $\mathrm{Supp}(F)$ is the set of exponents of the nonzero terms, $\mathbf{e} = (e_1, \dots, e_n) \in (\mathbb{F}_2)^n$, and $\mathbf{X}^{\mathbf{e}} = X_1^{e_1} X_2^{e_2} \cdots X_n^{e_n}$. This polynomial is known as the *algebraic normal form* of the Boolean function. The exponential sum of a Boolean polynomial $F \in \mathbb{F}_2[\mathbf{X}]$ is

$$S(F) = \sum_{\mathbf{x}\in(\mathbb{F}_2)^n} (-1)^{F(\mathbf{x})}.$$

The covering method for 2-divisibility. In [14], Moreno–Moreno introduced the covering method, which provides an elementary way to give a bound on the 2-divisibility of exponential sums of Boolean functions. Using this method, they gave an improvement to Ax's theorem in [2] for the binary case. However, the result does not give exact 2-divisibility and cannot be used to determine solvability or to find nonbalanced Boolean functions. Additional conditions have to be imposed to determine exact 2-divisibility. We now assume that any polynomial F is not a polynomial in some proper subset of the variables $X_1, \dots, X_n$.

Definition 1. A set C of monomials $F_{i_1}, \dots, F_{i_r}$ of a polynomial $F = F_1 + \cdots + F_m \in \mathbb{F}_2[\mathbf{X}]$ is called a **covering of** F if every variable X_i is in at least one monomial of C. The **size** of a covering C is its cardinality $|C|$. A set C is called a **minimal covering of** F if there is no other covering of F of smaller size.

Note that since, for $a \neq 0$, $X^a = X$ over $\mathbb{F}_2$, if we take the product of the monomials $F_{i_1} \cdots F_{i_r}$ in C we get $X_1 X_2 \cdots X_n$, the monomial with all the variables. This fact will be useful in the generalization of the covering to any characteristic p.

Example 2. Let $F = X_1 + X_2 + \cdots + X_8 + X_1X_2X_3X_4 + X_3X_5X_6 + X_2X_7X_8 + X_4X_7X_8 \in \mathbb{F}_2[X_1, \dots, X_8]$. Then $C_1 = \{X_1, X_2, \dots, X_8\}$, $C_2 = \{X_1X_2X_3X_4, X_3X_5X_6, X_2X_7X_8\}$, and $C_3 = \{X_1X_2X_3X_4, X_3X_5X_6, X_4X_7X_8\}$ are coverings of F, but C_2, C_3 are the only minimal coverings of F.

Moreno–Moreno used minimal coverings of a Boolean function F to obtain a bound on the 2-divisibility of the exponential sum of F.

Theorem 1 ([14]). *Let C be a minimal covering of $F \in \mathbb{F}_2[\mathbf{X}]$. Then*

$$v_2(S(F)) \geq |C|.$$

One can use Theorem 1 and Lemma 1 to give a bound on the 2-divisibility of the number of solutions $\mathcal{N}$ of F. However, a bound does not guarantee that $\mathcal{N} \neq 0$. To determine solvability one needs to obtain exact 2-divisibility. Theorem 1 is general and tight in the sense that there are polynomials that attain the bound and have exact 2-divisibility $|C|$. This implies that to determine if a polynomial has exact 2-divisibility or to improve the bound, we need to impose additional conditions. The next theorem has simple conditions that are sufficient to obtain exact 2-divisibility.

Theorem 2 ([7]). *Let $F \in \mathbb{F}_2[\mathbf{X}]$, and let $C_1, \dots, C_c$ be all the minimal coverings of F. If, for each $1 \leq i \leq c$, each monomial in C_i has at least two variables that are not present in the other monomials of C_i, then $v_2(S(F)) = |C_i|$ if c is odd, and otherwise $v_2(S(F)) \geq |C_i| + 1$, where $|C_i|$ is the size of a minimal covering.*

With the given conditions, the above theorem refines Moreno–Moreno's Theorem 1.

Example 3. The polynomial in Example 2 has exactly two minimal coverings. Moreno–Moreno's Theorem 1 implies that $v_2(F) \geq 3$, but Theorem 2 guarantees that $v_2(F) \geq 4$. This might seem a small improvement, but in the applications even small improvements are important.

The next example shows that even though different Boolean functions might have the same unique minimal covering, and hence the same 2-divisibility, there is an ample spectrum for the exact value of $S(F)$.

Example 4. Consider $F = X_1X_2X_3X_4 + X_4X_5X_6X_7 + X_7X_8X_9$ and $F' = X_1X_2X_3X_4 + X_4X_5X_6X_7 + X_7X_8X_9 + X_1 + X_2 + \cdots + X_9$ in $\mathbb{F}_2[X_1, \dots, X_9]$. It can be verified that $S(F) = 8 \cdot 3 \cdot 13$ and $S(F') = 8$.

Although, in general, it is not an easy task to find all the minimal coverings of a given polynomial, one can easily construct polynomials for which one knows all the minimal coverings and hence knows the exact 2-divisibility. For example, to obtain unique minimal coverings it is enough to construct systems of polynomials with lead monomials of degree at least 2 and of disjoint support that cover all the variables.

Example 5. Consider the following system of polynomials in 13 variables, where $(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{F}_2)^3$:

$$F_1 + G_1 = X_1X_2X_3X_4X_5 + \sum_i X_i - \alpha_1,$$

$$F_2 + G_2 = X_6X_7X_8X_9 + \sum_{i<j} X_iX_j - \alpha_2,$$

$$F_3 + G_3 = X_{10}X_{11}X_{12}X_{13} + \sum_{i<j<k} X_iX_jX_k - \alpha_3,$$

where $F_1 = X_1X_2X_3X_4X_5$, $F_2 = X_6X_7X_8X_9$, and $F_3 = X_{10}X_{11}X_{12}X_{13}$. Note that $C = \{Y_1F_1, Y_2F_2, Y_3F_3\}$ is the unique minimal covering of the associated polynomial

$P = Y_1(F_1 + G_1) + Y_2(F_2 + G_2) + Y_3(F_3 + G_3)$. This implies that $S(P)$ has exact 2-divisibility $v_2(S(P)) = 3$.

Note that any system $F_1' + G_1', \dots, F_t' + G_t'$, where $F_1', \dots, F_t'$ have disjoint support and $\deg(G_i') < \min_i\{\deg(F_i')\}$, will also have an associated polynomial P with unique minimal covering, and hence $S(P)$ will have exact 2-divisibility $v_p(S(P)) = t$. One can determine other conditions so that families of "deformations" $F + G_i$ of a polynomial F have the same minimal coverings as F. This provides a way to obtain the 2-divisibility of exponential sums of polynomial deformations $F + G_i$ from the 2-divisibility of the exponential sum of the polynomial F.

Theorem 3 ([7]). *Let $F, G \in \mathbb{F}_2[\mathbf{X}]$. Suppose that the minimal coverings of F are the minimal coverings of $F+G$ and each monomial in each minimal covering C_F has at least two variables that are not present in the other monomials of C_F. Then $S(F+G) \equiv S(F) \pmod{2^{|C_F|+1}}$. Moreover, if the number of minimal coverings is odd, then $v_2(S(F+G)) = v_2(S(F)) = |C_F|$.*

Example 6. Consider $F = X_1X_2X_3 + X_4X_5X_6 \in \mathbb{F}_2[X_1, \dots, X_6]$ and let $F + G$ be any polynomial in $\mathbb{F}_2[X_1, \dots, X_6]$ with $\deg(G) \le 2$. Then $C = \{X_1X_2X_3, X_4X_5X_6\}$ is the unique minimal covering of F and $F + G$, and each monomial in C has three variables that are not present in the other monomial. This implies that $S(F)$ and $S(F + G)$ have exact 2-divisibility $v_2(S(F + G)) = v_2(S(F)) = |C| = 2$.

Example 7. Consider $F = X_1X_2X_3 + X_4X_5X_6 + X_1X_4X_5 + X_2X_4X_6 + X_3X_5X_6 \in \mathbb{F}_2[X_1, \dots, X_6]$ and let $F + G$ be any polynomial in $\mathbb{F}_2[X_1, \dots, X_6]$ where $\deg(G) \le 2$. Again, $C = \{X_1X_2X_3, X_4X_5X_6\}$ is the unique minimal covering of F and $F + G$ and $v_2(S(F + G)) = v_2(S(F)) = 2$.

Examples 6 and 7 provide families of polynomials whose exponential sums have exact 2-divisibility. The intuitive and simple condition of $F + G$ and F having the same minimal coverings allows us to easily construct families of deformations with exact 2-divisibility. We will see later that this has useful applications to the determination of nonbalanced Boolean functions.

Solvability. As mentioned above, one of the main applications of p-divisibility of exponential sums is to obtain information about the number of solutions of systems of equations. Lemma 1 gives the relation between exponential sums and the number of solutions $\mathcal{N}$ of a system of polynomial equations $F_1 = \cdots = F_t = 0$. Using Theorem 2 one could determine if $\mathcal{N}$ has exact 2-divisibility $v_2(\mathcal{N})$. If this happens, $2^{v_2(\mathcal{N})+1}$ does not divide $\mathcal{N}$, $\mathcal{N} \neq 0$, and the system is solvable.

Example 8. Consider the system

$$X_1X_2X_3X_4X_5 + \sum_i X_i = \alpha_1,$$
$$X_6X_7X_8X_9 + \sum_{i<j} X_iX_j = \alpha_2,$$
$$X_{10}X_{11}X_{12}X_{13} + \sum_{i<j<k} X_iX_jX_k = \alpha_3.$$

The solutions of this system are the zeros of the system of polynomials $F_1 + G_1, F_2 + G_2, F_3 + G_3$ in Example 5. Since $v_2(S(P)) = 3$, $v_2(\mathcal{N}) = 0$ and $2 \nmid \mathcal{N}$. This implies that $\mathcal{N} \neq 0$ and the system is solvable for any $(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{F}_2)^3$.

Other applications. Other important applications of exponential sums are to coding theory and cryptography. Error-correcting codes are used to protect digital information from accidental errors that might occur during transmission or storage; the aim is for the receiver to be able to detect and correct errors that were introduced accidentally and retrieve the original message that was sent. On the other hand, cryptography is used to hide information from intruders; the information transmitted should be understood only by its intended receiver. Coding theory and cryptography serve different purposes, but they both share some theoretical concepts and methods.

In the coding process an **encoder** adds redundancy to a block of symbols of length k that represents the **message m** to transform it into a **codeword c** of block length n so that when received, the **decoder** can detect and correct errors. The **code** $\mathcal{C}$ is the set of all codewords. One can identify the messages with k-tuples of symbols from a finite field $\mathbb{F}_q$ and give the code the structure of a vector space of dimension k over $\mathbb{F}_q$. The encoder is then a one-to-one linear map $\mathcal{E}_{\mathcal{C}} : (\mathbb{F}_q)^k \longrightarrow (\mathbb{F}_q)^n$, and the linear code $\mathcal{C} = \mathrm{Im}(\mathcal{E}_{\mathcal{C}})$.

At first one might think that the decoder could just be the inverse of the encoding function. But the problem is that after the codeword $\mathbf{c} = \mathcal{E}_{\mathcal{C}}(\mathbf{m})$ is transmitted, the received word is $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{e}$ is an error vector. So, $\mathcal{E}_{\mathcal{C}}^{-1}(\mathbf{r}) \neq \mathbf{c}$ if $\mathbf{e} \neq 0$. Hence we need "good" codes, coding and decoding algorithms that allow us to detect and correct errors. The main problem in coding theory is to find codes with large rate $\frac{k}{n}$ of information symbols k per total number of symbols n that can correct "enough" errors, where "large" and "enough" will depend on the transmission channel for which the code is designed.

From now on we will consider **binary linear codes**, that is, linear codes over $\mathbb{F}_2$. The **Hamming weight of a vector x**, $w_H(\mathbf{x})$, is the number of entries of $\mathbf{x}$ that are nonzero. The **Hamming distance between two vectors x, y**, $d_H(\mathbf{x}, \mathbf{y})$ defines a metric and is the number of places on which the vectors disagree; this is equivalent to the Hamming weight of $\mathbf{x} + \mathbf{y}$. The **minimum distance d of a code** $\mathcal{C}$ is the minimum (Hamming) distance

between any two codewords, $d = \min\{d_H(\mathbf{x},\mathbf{y}) \mid \mathbf{x},\mathbf{y} \in \mathcal{C}\}$, and, since we are considering linear codes, this is equal to the minimum of the Hamming weight of the codewords $d = \min\{w_H(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}\}$.

Let $d \geq 2t+1$ be the minimum distance of a code $\mathcal{C}$ and suppose that a codeword $\mathbf{c}$ has been transmitted and $\mathbf{r} = \mathbf{c} + \mathbf{e}$ has been received, where $\mathbf{e}$ is an error vector with $w_H(\mathbf{e}) \leq t$. Then, $\mathbf{c}$ is the only codeword with distance from $\mathbf{r}$ less than or equal to t. Hence a possible decoding algorithm for a received word $\mathbf{r}$ is to look for the codeword that is closest in Hamming distance to $\mathbf{r}$. In practice this would be too inefficient but guarantees that if t or fewer errors occur, we can always correct them. This is why a linear block code with minimum distance $d \geq 2t+1$, block length n, and dimension k is called a **t-error-correcting code** with parameters (n,k,t). The goal of research in coding theory is to construct codes that have large d for the given rate $\frac{k}{n}$ and to design efficient algorithms to encode and decode them.

A **cryptographic system** is a set of transformations of the set of all messages into another space with certain properties. The message is **enciphered** into the **ciphertext** using a particular key that defines an injective mapping. Two important principles in the design of cryptographic systems are *confusion* and *diffusion*. The principle of diffusion makes different messages equally likely to occur; one way to measure diffusion is to determine if the function used to cipher is *balanced*. The principle of confusion measures the complexity of the decryption process; the *nonlinearity* of the functions used in the system gives a measure for confusion. Functions that are balanced and have large nonlinearity are desired.

Reed–Muller codes are some of the oldest and most-studied codes; nevertheless, there are still many open problems related to them that are important in both coding and cryptographic applications. To define a Reed–Muller code of size 2^n, given a fixed ordering of $(\mathbb{F}_2)^n$, one associates a Boolean polynomial $F \in \mathbb{F}_2[X_1,\ldots,X_n]$ with the vector of size 2^n consisting of all the values of $F(\mathbf{x})$ as $\mathbf{x}$ varies according to the ordering. This is also called the **truth table** of F. For example, if $(F_2)^3$ is ordered in lexicographic order with $X_1 > X_2 > X_3$, the truth table for $F(X_1,X_2,X_3) = X_1 + X_2X_3$ is $(0,0,0,1,1,1,1,0) \in (\mathbb{F}_2)^8$. When convenient, we will work with this representation of F in $(\mathbb{F}_2)^n$ instead of its polynomial representation; we will also alternate between calling F a function or a polynomial. The **kth order Reed–Muller code of length 2^n**, $R(k,n)$, is the set of truth tables of all the Boolean polynomials in n variables and degree less than or equal to k. That is, $R(k,n)$ can be identified with the set of Boolean polynomials in n variables and degree less than or equal to k.

The Reed–Muller code of order 1, $R(1,n)$, is the set of Boolean polynomials in n variables with degree less than or equal to 1. The *nonlinearity* of a Boolean function F is the Hamming distance from F to $R(1,n)$.

Exponential sums, Hamming weights, and nonlinearity. The **Hamming weight associated to a Boolean function** F, $w_H(F)$, is the Hamming weight of its truth table. This is the number of $\mathbf{x} \in (\mathbb{F}_2)^n$ such that $F(\mathbf{x}) = 1$. If $w_0(F)$ is the number of $\mathbf{x} \in (\mathbb{F}_2)^n$ such that $F(\mathbf{x}) = 0$, then $2^n = w_H(F) + w_0(F)$. Also, $S(F) = \sum_{\mathbf{x}\in(\mathbb{F}_2)^n}(-1)^{F(\mathbf{x})} = w_0(F)(-1)^0 + w_H(F)(-1)^1 = w_0(F) - w_H(F)$. This implies that $w_H(F) = 2^{n-1} - \frac{1}{2}S(F)$ and gives a correspondence between results on exponential sums and Hamming weights of Boolean functions. Hence, any result for exponential sums of a Boolean function also gives a corresponding result about the Hamming weight of the function.

Defining the Hamming distance of a Boolean function F to a vector $\mathbf{x}$ as the Hamming weight of the sum of $\mathbf{x}$ with the truth table of F, one can define the Hamming distance from F to a code $\mathcal{C}$ as $\min_{\mathbf{c}\in\mathcal{C}}\{w_H(F+\mathbf{c})\}$. This lets us define a measure for the principle of confusion in the cryptographic system, a sense of "how far is a Boolean function F from being linear." The **nonlinearity** of F is $Nl(F) = w_H(F + R(1,n))$, that is, the minimum Hamming distance between F and all the codewords in $R(1,n)$. This can be defined in terms of the exponential sums of cosets of $R(1,n)$,

$$Nl(F) = \min_{\mathbf{c}\in R(1,n)}\left\{2^{n-1} - \frac{1}{2}S(F+\mathbf{c})\right\},$$

and we can use results on exponential sums of deformations of Boolean functions to study the nonlinearity of a Boolean function F.

Covering radius of a code. The **covering radius** $\rho(\mathcal{C})$ is another important parameter of a code $\mathcal{C}$:

$$\rho(\mathcal{C}) = \max_{\mathbf{x}\in(\mathbb{F}_2)^n}\left\{\min_{\mathbf{c}\in\mathcal{C}}\{w_H(\mathbf{x}+\mathbf{c})\}\right\}.$$

This measure gives the maximum weight of a correctable error and can be used for the design of decoding algorithms. A code of minimum distance $2t+1$ is called **perfect** if $\rho(\mathcal{C}) = t$ and **quasi-perfect** if $\rho(\mathcal{C}) = t+1$.

The covering radius of the Reed–Muller code of order 1, $\rho(R(1,n))$, is the maximum Hamming distance of all n-variate Boolean polynomials to $R(1,n)$. We then have $Nl(F) \leq \rho(R(1,n))$. The covering radius of $R(1,n)$ gives a point of comparison for the nonlinearity of a Boolean polynomial and hence a sense of "how good" the function could be for cryptographic applications.

Results on the 2-divisibility of exponential sums have been used in several papers [16] to give elementary direct proofs of the covering radius of certain cyclic codes and to prove that families of cyclic codes are quasi-perfect.

Weight distribution. The weight distribution of a code $\mathcal{C}$ counts how many codewords of each weight there are. Much work has been done studying the weight distribution of Reed–Muller codes, but (as mentioned earlier) many problems remain open. Many of the properties of a Boolean function F that are important to cryptography can be related to the weight distribution of the coset $F+R(1,n)$ and can be studied using exponential sums. Canteaut [3] obtained a result that is a refinement of the Hamming weight version of Katz's theorem for the Boolean case and used it to study the weight distribution of cosets of first-order Reed–Muller codes. Her result is tight for the Boolean case and can be improved only by imposing additional conditions. The additional conditions to the covering method in Theorem 3 allowed us to obtain an improvement of her results [7].

Balanced functions. A Boolean function F is said to be **balanced** if the function is equal to 1 in half of the values of $\mathbf{x} \in (\mathbb{F}_2)^n$. Equivalently, an n-variate Boolean function F is balanced if the Hamming weight of its truth table, $w_H(F)$, is 2^{n-1}. This property is important in cryptographic applications because it follows the principle of diffusion: the function has no bias towards a value. The search for balanced Boolean functions and the development of new methods for constructing them are active areas of research.

It is easy to see that a Boolean function F is balanced if and only if $S(F) = 0$. If $S(F)$ has exact 2-divisibility, then $p^{v_p(S(F))+1} \nmid S(F)$, $S(F) \neq 0$, and F is not balanced. Hence, if one can describe families of Boolean functions with exact 2-divisibility, one is describing families of Boolean functions that are not balanced, and this can reduce the search for balanced Boolean functions.

In [10] Hou used the action of the group $\mathrm{GL}(n,2)$ on quotients of Reed–Muller codes $R(k,n)/R(k-1,n)$ to count the number of balanced polynomials in the cosets of $R(k-1,n)$. Note that the number of balanced polynomials in a coset of $R(k-1,n)$ is included in the weight distribution of the coset. Cosets of $R(k-1,n)$ belonging to the same orbit under this action have the same weight distribution and hence the same number of balanced polynomials. This implies that to know the number of balanced polynomials of all the cosets in an orbit, it is enough to study a coset representative for the orbit. Cosets of Reed–Muller codes $F+R(k-1,n)$ are sets of deformations of the polynomial F, and one can use Theorem 3 to determine nonbalanced polynomials a priori and improve the search for balanced functions.

Example 9. Consider the cosets of $R(3,6)/R(2,6)$, $X_1X_2X_3+X_4X_5X_6+R(2,6)$, and $X_1X_2X_3+X_4X_5X_6+X_1X_4X_5+X_2X_4X_6+X_3X_5X_6+R(2,6)$. The polynomials in these cosets satisfy the conditions in Examples 6 and 7 and hence have exact 2-divisibility. Therefore all the polynomials in these cosets are nonbalanced.

Hou presented representatives for each of the different orbits in $R(k,n)/R(k-1,n)$ for $k=3, n=6,7,8$. Example 9 shows two of the six cosets of $R(3,6)/R(2,6)$. Cusick and Cheon noticed in [8] the uneven distribution of the balanced functions in the table of balanced functions in the cosets of $R(3,6)/R(2,6)$. Two of the six cosets, the two cosets of Examples 6, 7, and 9, have zero balanced functions compared to more than 1.5 million in each of the other four cosets. The covering method gives a simple explanation for this phenomenon: as was seen in the examples, for any $G \in R(2,6)$, F and $F+G$ have the same unique minimal covering $\{X_1X_2X_3, X_4X_5X_6\}$, where each monomial has three variables not contained in the other monomial, and hence $F+G$ is not balanced.

It is not difficult to find sufficient conditions that can be used to determine a priori cosets of Reed–Muller codes that do not contain any balanced function, saving computational time. For example, we can use the covering method to identify by inspection 15 coset representatives (out of 32) in $R(3,8)/R(2,8)$ for which at least half of the functions in each coset are not balanced and provide constructions for these nonbalanced functions [7, 10]. This can be used to determine a priori types of polynomials to avoid in the search for balanced functions.

p-Divisibility of Exponential Sums

As mentioned above, the proof of most of the improvements and extensions of the Chevalley–Warning theorem are nonelementary. Ax and Katz used estimates on the p-divisibility of exponential sums to improve the Chevalley–Warning theorem. Katz [11] obtained that $\mathcal{N}$, the number of common zeros of polynomials $F_1,\dots,F_t$ in $\mathbb{F}_q[X_1,\dots,X_n]$ of degree $d_1,\dots,d_t$, is divisible by q^μ, where μ is the smallest nonnegative integer $\mu \geq \mu_0$:

$$\mu_0 = \frac{n - \sum_{i=1}^{t} d_i}{\max\{d_i\}}.$$

Note that the theorem gives information on the p-divisibility of $\mathcal{N}$ only if there are "enough variables" n; if $n < \sum_{i=1}^{t} d_i$, $\mu = 0$, the conclusion is that $1|\mathcal{N}$, and the theorem does not give any information. Adolphson–Sperber [1] improved Katz's result using a Newton polyhedra approach, and Moreno–Moreno gave an improvement by using the p-weight degree of the polynomials instead of their regular degree. The **p-weight degree** of a polynomial F, $w_p(F)$ is the maximal p-weight degree of its monomials. The p-weight degree of the monomial $\mathbf{X}^{\mathbf{e}} = X_1^{e_1}\cdots X_n^{e_n}$ is

$$w_p(\mathbf{X}^{\mathbf{e}}) = \sigma_p(e_1) + \cdots + \sigma_p(e_n),$$

where for $a = a_0 + a_1 p + \cdots + a_r p^r$, $\sigma_p(a) = \sum_{i=0}^{r} a_i$. For $q = p^f$, Moreno–Moreno [13] found that $\mathcal{N}$ is divisible by

p^μ, where μ is the smallest nonnegative integer $\mu \geq \mu_0$,

$$\mu_0 = f\frac{n - \sum_{i=1}^{t} w_p(F_i)}{\max\{w_p(F_i)\}}.$$

Again, note that the theorem gives information on the p-divisibility of $\mathcal{N}$ only if there are "enough variables"; if the number of variables is less than or equal to the sum of the p-weight degree of the polynomials, $\mu = 0$ and the theorem does not give any information. A tight bound for the p-divisibility of exponential sums was given by Moreno et al. in [17]. That and Adolphson–Sperber's results use the exponents $\mathbf{e}_1, \ldots, \mathbf{e}_m$ of all the monomials in the polynomial $F(\mathbf{X}) = \sum_{i=1}^{m} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$ in contrast to the Chevalley–Warning, Ax–Katz, and Moreno–Moreno results that use only the degree or the p-weight degree of the polynomial. In this sense the result in [17] resembles the covering method for Boolean polynomials. None of these results can be used to determine if the exponential sum has exact p-divisibility, and solvability cannot be determined.

The covering method for p-divisibility. In [6], Castro et al. introduced a generalization to any prime field of the covering method introduced in [14] for characteristic 2. With it they proved the prime field case of the theorem on the p-divisibility of exponential sums presented in [17]. The new proof was entirely elementary, and, as a consequence, elementary proofs and improvements of previous results on the p-divisibility of exponential sums were obtained.

For the case $q = p$, the tight bound in [17] relies on finding a minimal solution $(s_1, \ldots, s_m)$ to a system of n modular equations $e_{j1}s_1 + e_{j2}s_2 + \cdots + e_{jm}s_m \equiv 0 \pmod{p-1}$, associated to the exponents of each variable in the polynomial $F(\mathbf{X}) = \sum_{i=1}^{m} a_i X_1^{e_{1i}} \cdots X_n^{e_{ni}}$. That is, one needs to find solutions to a system

$$\begin{cases} e_{11}s_1 + e_{12}s_2 + \cdots + e_{1m}s_m & = \lambda_1(p-1) \\ \qquad\vdots & \qquad\vdots \\ e_{n1}s_1 + e_{n2}s_2 + \cdots + e_{nm}s_m & = \lambda_n(p-1), \end{cases}$$

$\lambda_i \in \mathbb{N}$, where each column corresponds to a term and each row to a variable, that are minimal in terms of $L = \sum_{i=1}^{m} s_i$. In this case, $v_p(S(F)) \geq \frac{L}{p-1}$.

If the system is rewritten as

$$\begin{pmatrix} e_{11} \\ e_{21} \\ \vdots \\ e_{n1} \end{pmatrix} s_1 + \cdots + \begin{pmatrix} e_{1m} \\ e_{2m} \\ \vdots \\ e_{nm} \end{pmatrix} s_m = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} (p-1), \qquad (1)$$

one sees that the solutions that one is looking for are exponents s_i for the monomials $F_i = X_1^{e_{1i}} \cdots X_n^{e_{ni}}$ in F such that

$$F_1^{s_1} F_2^{s_2} \cdots F_m^{s_m} = X_1^{\lambda_1(p-1)} \cdots X_n^{\lambda_n(p-1)},$$

for $\lambda_1, \ldots, \lambda_n \geq 1$, and such that $s_1 + \cdots + s_m$ is as small as possible [4]. If $p = 2$, then $C = \{F_1^{s_1}, F_2^{s_2}, \ldots, F_m^{s_m}\}$ is a covering for F, as some of the s_i could be zero. This is the motivation for the definition of a minimal $(p-1)$-covering below. Note that the solutions do not depend on the coefficients of the polynomial F.

Definition 2. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_mF_m$. A set $C = \{F_1^{s_1}, \ldots, F_m^{s_m}\}$ of powers of the monomials in F is a **minimal $(p-1)$-covering of** F if $F_1^{s_1} \cdots F_m^{s_m} = X_1^{\lambda_1(p-1)} \cdots X_n^{\lambda_n(p-1)}$ with $\lambda_i \geq 1$ and its **size**, $\sum_{i=1}^{m} s_i$, is minimal.

A $(p-1)$-covering need not use all the F_i's, and therefore some of the s_i's could be equal to 0.

Example 10. Let $F(\mathbf{X}) = X_1^2X_2^3 + X_1^2 + X_2^3 \in \mathbb{F}_7[X_1, X_2]$. Then $C_1 = \left\{\left(X_1^2X_2^3\right)^6\right\}, C_2 = \left\{\left(X_1^2\right)^3, \left(X_2^3\right)^2\right\}$, and $C_3 = \left\{\left(X_1^2X_2^3\right)^2, \left(X_1^2\right)^1\right\}$ are 6-coverings of F, and C_3 is the unique minimal 6-covering of F (of size 3).

A minimal $(p-1)$-covering of a polynomial F might not be unique, and the concept is independent of the coefficients of F. However, the exact p-divisibility of $S(F)$ and the solvability of equations involving F depend on both the minimal $(p-1)$-coverings and the relation among the coefficients. Also, if there are powers of the monomials in F that cover some (but not all) of the variables and are minimal in some sense, it is very hard to determine the exact p-divisibility. In Theorem 4 we avoid polynomials with this type of *minimal partial $(p-1)$-covering*.

Definition 3. Let $F(\mathbf{X}) = a_1F_1 + a_2F_2 + \cdots + a_mF_m$. A set $C = \{F_1^{s_1}, \ldots, F_m^{s_m}\}$ of powers of the monomials in F is a **partial $(p-1)$-covering of** F if $F_1^{s_1} \cdots F_m^{s_m} = X_1^{\lambda_1(p-1)} \cdots X_n^{\lambda_n(p-1)}$ with $\lambda_i \geq 0$. The set C is a **minimal partial $(p-1)$-covering of** F if its size $\sum_{i=1}^{m} s_i + s(p-1)$, where s is the number of variables missing, is the size of a minimal $(p-1)$-covering of F.

Note that instead of requiring each exponent $\lambda_i(p-1)$ of X_i to be a positive multiple of $p-1$, in the definition of a partial $(p-1)$-covering, λ_i could be equal to 0, and therefore some variables could be missing. If $s = 0$, there are no variables missing, and we have the previous definition of the $(p-1)$-covering.

Example 11. Let $F(\mathbf{X}) = X_1^2X_2^3 + X_1^2 + X_2^3 \in \mathbb{F}_7[X_1, X_2]$ be the polynomial of Example 10. Then $C_4 = \left\{\left(X_2^3\right)^2\right\}$ is a partial 6-covering of F of size $2 + 6 = 8$. In Example 10 we saw that the minimal 6-coverings have size 3, and therefore C_4 is not a minimal partial 6-covering of F.

By avoiding minimal partial $(p-1)$-coverings we can improve previous results by computing exact p-divisibility of exponential sums or improving previous bounds. The

next result [4] is a generalization of Theorem 2 to any characteristic.

Theorem 4. *Let $C_1, \dots, C_c$ be all the minimal $(p-1)$-coverings of size L of a polynomial $F = a_1F_1 + \cdots + a_mF_m$, $C_i = \{F_1^{s_{i1}}, \dots, F_m^{s_{im}}\}$, and suppose that any minimal partial $(p-1)$-covering is one of the C_i's. Then, $v_p(S(F)) = \frac{L}{p-1}$ if $\sum_{i=1}^{c} \frac{a_1^{s_{i1}} \cdots a_m^{s_{im}}}{s_{i1}! \cdots s_{im}!} \not\equiv 0 \pmod{p}$, and otherwise $v_p(S(F)) \geq \frac{L}{p-1} + 1$.*

The condition $\sum_{i=1}^{c} \frac{a_1^{s_{i1}} \cdots a_m^{s_{im}}}{s_{i1}! \cdots s_{im}!} \not\equiv 0 \pmod{p}$ is the generalization of the number c of minimal coverings being odd in the case of $p = 2$. The condition of the minimal partial $(p-1)$-coverings being one of the C_i's implies that any minimal partial $(p-1)$-covering does not have a missing variable. Similarly to the case where $p = 2$, a sufficient condition for not having minimal partial $(p-1)$-coverings with missing variables is to require that for each of the minimal $(p-1)$-coverings C_i, each monomial in C_i has at least two variables that are not present in the other monomials of C_i. This simple condition provides families of polynomials for which the "greater than or equal to" relation obtained in the classical results on p-divisibility is replaced by either equality or strict inequality.

Theorem 4, when applied to the number of solutions of systems of polynomial equations, gives refinements to the prime field case of many of the known results by giving precise conditions for when the system is solvable or the bound on the p-divisibility of the number of solutions $\mathcal{N}$ is improved. Moreover, it can also give information on the solvability or p-divisibility of $\mathcal{N}$ for cases that are not covered by previous theorems.

Example 12. Let $p \neq 2$ and consider the system

$$X_1^2X_2^4 + X_3^6X_4^2 + X_1 + X_2 + X_6 + X_7 = \alpha,$$
$$X_5^2X_6^2 + X_7^6X_8^2 + X_3 + X_5 + X_8 = \beta$$

over $\mathbb{F}_p^*$. Note that the system has 8 variables and the sum of the degree of the polynomials is 16; hence Ax–Katz's theorem does not give any information on solvability nor p-divisibility of $\mathcal{N}$. For $p = 3, 5$ and $p > 5$ the sum of the p-weight degree of the polynomials is $8, 10$, and 16, respectively; hence Moreno–Moreno's theorem does not give any information either.

To use the covering method, we first compute the polynomial associated to this system:

$$P = Y_1\left(X_1^2X_2^4 + X_3^6X_4^2 + X_1 + X_2 + X_6 + X_7 - \alpha\right)$$
$$+ Y_2\left(X_5^2X_6^2 + X_7^6X_8^2 + X_3 + X_5 + X_8 - \beta\right).$$

It is easy to see that the unique minimal $(p-1)$-covering for P is

$$C = \left\{\left(Y_1X_1^2X_2^4\right)^{\frac{p-1}{2}}, \left(Y_1X_3^6X_4^2\right)^{\frac{p-1}{2}}, \right.$$
$$\left. \left(Y_2X_5^2X_6^2\right)^{\frac{p-1}{2}}, \left(Y_2X_7^6X_8^2\right)^{\frac{p-1}{2}}\right\},$$

there are no minimal partial $(p-1)$-coverings with missing variables, and $\frac{a_1^{s_1} \cdots a_4^{s_4}}{s_1! \cdots s_4!} \not\equiv 0 \pmod{p}$. This implies that the exact p-divisibility of $\mathcal{N}$ is $v_p(\mathcal{N}) = 4\left(\frac{p-1}{2}\right)/(p-1) - 2 = 0$. Therefore, $p \nmid \mathcal{N}$, $\mathcal{N} \neq 0$, and the system is solvable for any $\alpha, \beta \in \mathbb{F}_p^*$.

By imposing conditions on polynomials G so that $F+G$ and F have the same minimal $(p-1)$-coverings, one can extend known results on the p-divisibility of $S(F)$ to results on $S(F+G)$ for deformations of F.

Example 13. Let $\mathcal{N}$ be the number of solutions of the system

$$aX_1^{p-1} + \cdots + aX_p^{p-1} + G = 0,$$
$$b_1X_1 + \cdots + b_pX_p + \alpha = 0, \tag{2}$$

where $a, b_i \in \mathbb{F}_p{}^*, \alpha \in \mathbb{F}_p$, $G \in \mathbb{F}_p[\mathbf{X}]$, and deg $G < p-1$.

This system has p variables, and sum of the degree and of the p-weight degree of the polynomials is also p. Hence Ax–Katz and Moreno–Moreno's theorems do not give any information on solvability or the p-divisibility of $\mathcal{N}$. There are p different minimal $(p-1)$-coverings with form

$$\left\{Y_1X_{i_1}^{p-1}, \dots, Y_1X_{i_{p-1}}^{p-1}, \left(Y_2X_{i_p}\right)^{p-1}\right\}$$

and size $L = 2(p-1)$. Since $\sum_{i=1}^{p} \frac{a^{p-1}b_i^{p-1}}{(p-1)!} = \frac{p}{(p-1)!}$, we have $v_p(\mathcal{N}) = -2 + v_p(S(P)) > -2 + \frac{2(p-1)}{p-1} = 0$. The result does not give information about solvability but gives some information about the p-divisibility of $\mathcal{N}$.

Conclusions

The covering method is an elementary method to obtain information about the p-divisibility of exponential sums. It provides an intuitive approach to the computation of exact p-divisibility that can be exploited in applications. It also gives a simple way to construct families of systems of polynomial equations that are solvable, determine p-divisibility of the number of solutions of systems for cases where previous results do not give information, and can be applied to answer questions in coding theory and cryptography.

ACKNOWLEDGMENTS. The author dedicates this work to the memory of her friend and collaborator, Francis Castro. The author appreciates the careful review, corrections, and comments made by the associate editor, the referees, Ricardo Cortez, H. F. Mattson Jr., Herbert Medina, and Luis Medina, which helped to improve the article.

References

[1] Alan Adolphson and Steven Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci. École Norm. Sup. (4) **20** (1987), no. 4, 545–556. MR932797

[2] James Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261, DOI 10.2307/2373163. MR160775

[3] Anne Canteaut, *On the weight distributions of optimal cosets of the first-order Reed-Muller codes*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 407–413, DOI 10.1109/18.904547. MR1820387

[4] Francis N. Castro and Ivelisse M. Rubio, *Construction of systems of polynomial equations with exact p-divisibility via the covering method*, J. Algebra Appl. **13** (2014), no. 6, 1450013, 15, DOI 10.1142/S0219498814500133. MR3195170

[5] Francis Castro and Ivelisse M. Rubio, *Exact p-divisibility of exponential sums via the covering method*, Proc. Amer. Math. Soc. **143** (2015), no. 3, 1043–1056, DOI 10.1090/S0002-9939-2014-12315-X. MR3293721

[6] Francis N. Castro, Hugues Randriam, Ivelisse Rubio, and H. F. Mattson Jr., *Divisibility of exponential sums via elementary methods*, J. Number Theory **130** (2010), no. 7, 1520–1536, DOI 10.1016/j.jnt.2010.03.004. MR2645235

[7] Francis N. Castro, Luis A. Medina, and Ivelisse M. Rubio, *Exact 2-divisibility of exponential sums associated to boolean functions*, Cryptogr. Commun. **10** (2018), no. 4, 655–666, DOI 10.1007/s12095-017-0252-7. MR3770919

[8] Thomas W. Cusick and Younhwan Cheon, *Counting balanced Boolean functions in n variables with bounded degree*, Experiment. Math. **16** (2007), no. 1, 101–105. MR2312980

[9] Fernando Q. Gouvêa, *p-adic numbers: An introduction*, 2nd ed., Universitext, Springer-Verlag, Berlin, 1997. MR1488696

[10] X. Hou, GL$(m,2)$ *acting on* $R(r,m)/R(r-1,m)$, Discrete Math. **149** (1996), no. 1-3, 99–122, DOI 10.1016/0012-365X(94)00342-G. MR1375102

[11] Nicholas M. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499, DOI 10.2307/2373389. MR288099

[12] Rudolf Lidl and Harald Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn. MR1429394

[13] O. Moreno and C. J. Moreno, *An elementary proof of a partial improvement to the Ax-Katz theorem*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 257–268, DOI 10.1007/3-540-56686-4_48. MR1251983

[14] Oscar Moreno and Carlos 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** (1994), no. 6, 1894–1907, DOI 10.1109/18.340464. MR1322391

[15] O. Moreno and C. J. Moreno, *Improvements of the Chevalley-Warning and the Ax-Katz theorems*, Amer. J. Math. **117** (1995), no. 1, 241–244, DOI 10.2307/2375042. MR1314464

[16] Oscar Moreno and Francis N. Castro, *Divisibility properties for covering radius of certain cyclic codes*, IEEE Trans. Inform. Theory **49** (2003), no. 12, 3299–3303, DOI 10.1109/TIT.2003.820033. MR2045808

[17] Oscar Moreno, Kenneth W. Shum, Francis N. Castro, and P. Vijay Kumar, *Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications*, Proc. London Math. Soc. (3) **88** (2004), no. 3, 545–564, DOI 10.1112/S002461150301462X. MR2044049

[18] Gary L. Mullen and David Panario (eds.), *Handbook of finite fields*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2013. MR3087321

[19] Da Qing Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. **111** (1989), no. 1, 1–8, DOI 10.2307/2374476. MR980296

[20] Da Qing Wan, *A Chevalley-Warning approach to p-adic estimates of character sums*, Proc. Amer. Math. Soc. **123** (1995), no. 1, 45–54, DOI 10.2307/2160608. MR1215208

Ivelisse M. Rubio

Credits

The opening image is courtesy of Incnis Mrsi [CC BY-SA 3.0, (`https://commons.wikimedia.org/w/index.php?`)] via Wikimedia Commons.

Photo of the author is courtesy of the author.