p-Adic Estimates of Hamming Weights in Abelian Codes Over Galois Rings

Daniel J. Katz, *Member, IEEE*

***Abstract*—A generalization of McEliece's theorem on the p-adic valuation of Hamming weights of words in cyclic codes is proved in this paper by means of counting polynomial techniques introduced by Wilson along with a technique known as trace-averaging introduced here. The original theorem of McEliece concerned cyclic codes over prime fields. Delsarte and McEliece later extended this to Abelian codes over finite fields. Calderbank, Li, and Poonen extended McEliece's original theorem to cover cyclic codes over the rings $\mathbb{Z}_{2^d}$, Wilson strengthened their results and extended them to cyclic codes over $\mathbb{Z}_{p^d}$, and Katz strengthened Wilson's results and extended them to Abelian codes over $\mathbb{Z}_{p^d}$. It is natural to ask whether there is a single analogue of McEliece's theorem which correctly captures the behavior of codes over all finite fields and all rings of integers modulo prime powers. In this paper, this question is answered affirmatively: a single theorem for Abelian codes over Galois rings is presented. This theorem contains all previously mentioned results and more.**

***Index Terms*—Abelian codes, codes over Galois rings, counting polynomials, McEliece's theorem.**

I. Introduction

McELIECE'S theorem [1] is a powerful tool for analyzing the Hamming weights of codewords in cyclic codes over prime fields. In fact, it will be more convenient for us to handle the *zero count*, i.e., the number of times the symbol zero occurs in a codeword. Since we always assume that the length n of the codewords is known, and since the Hamming weight is n minus the zero count, all statements about zero count readily translate into equivalent statements about Hamming weight. So for any ring R, we define zer: $R \to \mathbb{Z}$ by

$$\operatorname{zer}(r) = \begin{cases} 1, & \text{if } r = 0 \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

We extend the function zer to all finite sequences of elements of R so that if $c = (c_1, \ldots, c_n) \in R^n$, then we set $\operatorname{zer}(c) = \sum_{i=1}^{n} \operatorname{zer}(c_i)$. To simplify the presentation of material in this Introduction (Section I), we shall assume that all our codes have words whose symbols sum to zero. For cyclic codes, this means that we always assume that 1 is a zero of the generator polynomial of our code.

Manuscript received September 8, 2004; revised September 21, 2005. This work was supported in part by the Scott Russell Johnson Prize for Excellence in Graduate Study in Mathematics at Caltech, given by Steve and Rosemary Johnson.

The author was with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125 USA. He is now with the Department of Mathematics, Princeton University, Princeton, NJ 08544 USA (e-mail: dankatz@math.princeton.edu).

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2005.864428

A. History

Let p be a prime and let C be a cyclic code over $\mathrm{GF}(p)$. McEliece's theorem relates the highest power of p dividing all the Hamming weights of codewords in C to the set S of zeroes of the check polynomial, also known as *nonzeroes* of the code. One should calculate the length ℓ of the shortest sequence of nonzeroes whose product is 1, subject to the constraint that the length be divisible by $p-1$ and that the sequence not be trivial (i.e., not composed entirely of 1's). We now cast this definition into mathematical notation. Using the notation X^* to denote the set of all finite-length sequences whose terms are elements of a set X, we set

$$\Lambda = \left\{ (s_1, \ldots, s_k) \in S^* \colon \exists_i s_i \neq 1, \prod_{i=1}^{k} s_i = 1, k \equiv 0 \pmod{p-1} \right\} \quad (1)$$

and then, using $|\lambda|$ to denote the length of a sequence λ, we set

$$\ell = \min_{\lambda \in \Lambda} |\lambda|. \quad (2)$$

Throughout this section, we shall assume that S contains some element other than 1, so that Λ is nonempty and ℓ is defined. Then we have McEliece's theorem.

Theorem 1.1: (McEliece [1]) Let C be a cyclic code of length n over $\mathrm{GF}(p)$ with S the set of nonzeroes of C and $1 \notin S$. For any $c \in C$, we have

$$\operatorname{zer}(c) \equiv n \left(\bmod p^{\frac{\ell}{p-1}-1} \right)$$

where Λ and ℓ are as defined in (1) and (2).

Furthermore, this congruence is sharp in the sense that there is some word $c \in C$ such that the congruence does not hold modulo $p^{\frac{\ell}{p-1}}$. In other words, there is some word whose Hamming weight is not divisible by $p^{\frac{\ell}{p-1}}$. In fact, the full version of McEliece's theorem (not presented in this Introduction) even provides an explicit formula for calculating the zero count of a codeword modulo $p^{\frac{\ell}{p-1}}$ in terms of the Fourier transform (Mattson–Solomon polynomial). The full version also considers the possibility that $1 \in S$.

Example 1.2: Consider the binary quadratic residue code C of length n for n a prime with $n \equiv \pm 1 \pmod 8$. Let ζ_n be a primitive nth root of unity over $\mathrm{GF}(2)$. Then C can be thought of as the ideal in $\mathrm{GF}(2)[x]/(x^n - 1)$ whose check polynomial has roots $\zeta_n, \zeta_n^4, \ldots, \zeta_n^{((n-1)/2)^2}$.

If $n \equiv 1 \pmod 8$, then -1 is a quadratic residue modulo n. Thus, ζ_n^{-1} and ζ_n are both nonzeroes, so that Λ contains the sequence (ζ_n, ζ_n^{-1}), and so $\ell = 2$. McEliece's theorem tells us that $\mathrm{zer}(c) \equiv n \pmod 2$ for all $c \in C$. Equivalently, all Hamming weights are even. The full version of the theorem also tells us that some Hamming weight is not divisible by 4.

On the other hand, if $n \equiv -1 \pmod 8$, then -1 is not a quadratic residue modulo n. Thus, the inverse of each nonzero is a zero of the code, hence $\ell > 2$. In fact, it ℓ is always 3, since there always exists some $k \in \{1, 2, \ldots, (n-1)/2\}$ such that ζ_n^k is a nonzero and ζ_n^{k+1} is not a nonzero. Then $\zeta_n^{-(k+1)}$ must be a nonzero and thus, $(\zeta_n, \zeta_n^k, \zeta_n^{-(k+1)}) \in \Lambda$. So McEliece's theorem tells us that all Hamming weights are divisible by 4 and that some Hamming weight is not divisible by 8. □

Delsarte and McEliece [2] later extended this result to cover Abelian codes over an arbitrary finite field $\mathrm{GF}(q)$, with $q = p^e$. Since they are no longer dealing solely with cyclic codes, the set of nonzeroes is replaced with its natural generalization: the minimal support S of the set of Fourier transforms of the codewords. For brevity, we refer to the set of Fourier transforms of words in C as the *Fourier transform of* C. As in Theorem 1.1, the highest power of p dividing all Hamming weights of codewords is related to some minimum length ℓ of sequences in a specific class of sequences. This class of sequences has a definition somewhat more complicated than that of the Λ in (1) above. We present it in a way slightly different than Delsarte and McEliece do in order to facilitate comparison with the developments of this paper. Let $E = \{0, 1, \ldots, e-1\}$, where we recall that our alphabet is $\mathrm{GF}(q)$ with $q = p^e$. Then set

$$\Lambda = \left\{ ((s_1, t_1), \ldots, (s_k, t_k)) \in (S \times E)^* : \exists_i s_i \neq 1, \prod_{i=1}^{k} s_i^{p^{t_i}} = 1, \sum_{i=1}^{k} p^{t_i} \equiv 0 \pmod{q-1} \right\} \quad (3)$$

and, as before, set

$$\ell = \min_{\lambda \in \Lambda} |\lambda|. \quad (4)$$

Note that the condition $\sum_{i=1}^{k} p^{t_i} \equiv 0 \pmod{q-1}$ reduces modulo $p-1$ to $k \equiv 0 \pmod{p-1}$, so that $p-1 \mid \ell$. When $e = 1$, the Λ defined here is in essence the same as the Λ of (1). Now we can state the generalization of Delsarte and McEliece.

Theorem 1.3: (Delsarte-McEliece [2]) Let C be an Abelian code of length n over $\mathrm{GF}(p^e)$, with S the minimal support of the Fourier transform of C and $1 \notin S$. For any $c \in C$, we have

$$\mathrm{zer}(c) \equiv n \pmod{p^{\frac{\ell}{p-1} - e}}$$

where Λ and ℓ are as defined in (3) and (4).

As before, this congruence is sharp in the sense that there is some $c \in C$ so that the congruence fails to hold modulo any higher power of p. The full theorem of Delsarte and McEliece even provides a formula which can be used to calculate the zero count modulo $p^{\frac{\ell}{p-1} - e + 1}$ in terms of the Fourier transform (see Theorem 5.5). The full version also considers the possibility that $1 \in S$. Theorem 1.3 reduces to McEliece's original theorem (Theorem 1.1) discussed above if we restrict to cyclic codes over prime fields.

Example 1.4: Let $k > 0$, let A be the cyclic group of order $4^k - 1$ generated by an element a, and let C be the code in $\mathrm{GF}(4)[A]$ whose Fourier transform is supported on the set $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. In a more conventional presentation of cyclic codes, this is the code in $\mathrm{GF}(4)[x]/(x^{4^k-1} - 1)$ whose check polynomial is one of the kth-degree irreducible factors of the cyclotomic polynomial $\Phi_{4^k-1}(x)$ in $\mathrm{GF}(4)[x]$. This code is also known as the shortened first-order Reed–Muller code of length $4^k - 1$ over $\mathrm{GF}(4)$. We want to investigate the set Λ, as defined in (3), and the parameter ℓ, as defined in (4), for this code, so that we may apply the Delsarte–McEliece theorem.

Here $p = 2$ and $e = 2$, since we are working with $\mathrm{GF}(4)$. Thus. $E = \{0, 1\}$. Furthermore, $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. The set Λ consists of certain nonempty sequences of the form

$$(a^{4^{f_1}}, g_1), (a^{4^{f_2}}, g_2), \ldots, (a^{4^{f_m}}, g_m)$$

with $f_i \in \{0, 1, \ldots, k-1\}$ and $g_i \in E$. The product condition in Λ allows us to restrict attention to sequences with

$$\sum_i 2^{g_i} 4^{f_i} \equiv 0 \pmod{4^k - 1}.$$

From this it is easy to classify minimal-length sequences in Λ. If $\lambda \in \Lambda$ has two or more instances of an element (a^{4^f}, g), then we can form a shorter sequence $\kappa \in \Lambda$ as follows: if $g = 0$, then replace the two instances of $(a^{4^f}, 0)$ with one instance of $(a^{4^f}, 1)$, but if $g = 1$, then replace the two instances of $(a^{4^f}, 1)$ with one instance of $(a^{4^{f+1}}, 0)$. In either case, all defining properties of Λ are preserved. Thus a minimum-length sequence

$$(a^{4^{f_1}}, g_1), (a^{4^{f_2}}, g_2), \ldots, (a^{4^{f_m}}, g_m)$$

in Λ has no repeated elements. But then $0 < \sum_i 2^{g_i} 4^{f_i} \leq 4^k - 1$, which forces equality in the second inequality, which in turn forces our sequence to have one instance of each element (a^{4^h}, j). Thus, the sequences of length $2k$ with exactly one instance of each element of $S \times E$ are precisely the minimum-length elements of Λ, and so $\ell = 2k$. By the same reasoning, it is not hard to show that each sequence of length $2k+1$ in Λ is obtained from a minimal-length sequence by deleting one element (a^{4^f}, g) and inserting two instances of $(a^{4^{f+k-1}}, 1)$ if $g = 0$, or two instances of $(a^{4^f}, 0)$ if $g = 1$.

Since $\ell = 2k$, the Deslarte–McEliece theorem tells us that $\mathrm{zer}(c) \equiv 4^k - 1 \pmod{2^{2k-2}}$, or equivalently, that all Hamming weights are divisible by 2^{2k-2}. Furthermore, the full version of the theorem tells us that some word has Hamming weight not divisible by 2^{2k-1}. In fact, it is not hard to show that all nonzero words have Hamming weight $2^{2k} - 2^{2k-2}$. □

Ward obtained generalizations of Theorems 1.1 and 1.3 for codes which are ideals in group algebras $\mathrm{GF}(q)[G]$ where G is non-Abelian or of order divisible by p [3]–[6]. Calderbank, Li, and Poonen [7] extended McEliece's original theorem in a different direction. They proved a version for cyclic codes with alphabet $\mathbb{Z}_{2^d}$. Their result was strengthened and extended to cyclic codes over $\mathbb{Z}_{p^d}$ by Wilson [8], [9], and his result was further

strengthened (in the case where $p \neq 2$) and extended to Abelian codes over $\mathbb{Z}_{p^d}$ by Katz [10]. As with the theorem of Delsarte and McEliece, we set S to be the minimal support of the set of Fourier transforms of the codewords, and then we set Λ and ℓ as in (1) and (2). Then we have the following theorem.

Theorem 1.5: (Katz [10]) Let C be an Abelian code of length n over $\mathbb{Z}_{p^d}$ with S the minimal support of the Fourier transform of C and $1 \notin S$. For any codeword $c \in C$, we have

$$\operatorname{zer}(c) \equiv n \left(\operatorname{mod} p^{\lfloor \frac{\ell - p^d - 1}{(p-1)p^{d-1}} \rfloor} \right)$$

where Λ and ℓ are as defined in (1) and (2).

If we set $d = 1$, we obtain a version of McEliece's theorem for Abelian codes over prime fields, which is at once a generalization of McEliece's original theorem (Theorem 1.1) and a special case of the theorem of Delsarte and McEliece (Theorem 1.3). These theorems of McEliece and Delsarte are sharp, i.e., they determine the maximum power of p that divides all Hamming weights in the code C. Thus, the congruence in Theorem 1.5 becomes sharp when $d = 1$. In the case when $p = 2$ and $d = 2$ (i.e., for Abelian codes over $\mathbb{Z}_4$), Katz [10] has shown this congruence to be sharp in the sense that there is some codeword c with Fourier transform supported on S such that the Hamming weight of c is not divisible by $p^{\lfloor \frac{\ell - p^d - 1}{(p-1)p^{d-1}} \rfloor + 1}$. This proves that Theorem 1.5 is sharp for codes which are free $\mathbb{Z}_4$-modules. A very recent result of the author [11], obtained after this paper was submitted, shows that Theorem 1.5 is sharp for all codes which are free $\mathbb{Z}_{p^d}$-modules (for all p and d), but is not sharp for infinitely many other codes. This new result includes a version of Theorem 1.5 which has been refined so as to be sharp for all Abelian codes over $\mathbb{Z}_{p^d}$. This new theorem, now only available in the author's dissertation [11], will be the subject of a future paper. The full version of Theorem 1.5 presented by Katz in [10] also provides formulas for computing the zero count of a word modulo any power of p from its Fourier transform, but these formulas rapidly become cumbersome modulo powers of p higher than $\lfloor \frac{\ell - p^d - 1}{(p-1)p^{d-1}} \rfloor$.

B. The New Result

Since we now have a version of the McEliece theorem for Abelian codes over finite fields and a version for Abelian codes over $\mathbb{Z}_{p^d}$, we should ask ourselves if these are not special cases of a more general theorem. First, we need to consider if there is a general class of rings which includes both the finite fields and the integers modulo powers of p. Fortunately, we do not need to look far, as such rings, called the *Galois rings*, have already been used extensively in researches on cyclic codes over $\mathbb{Z}_{p^d}$ [7], [10], [12]–[21]. Furthermore, codes over Galois rings, and especially cyclic and Abelian codes over Galois rings, are being studied actively at this time [22]–[32], so that it is natural to desire an analogue of McEliece's theorem for such codes. Section II-A of [10] contains, in summary format, all we shall need to know about Galois rings in this paper. For more details on such rings, see [33].

In this paper we shall use the notation GR (p^d, e) to denote the Galois ring of characteristic p^d generated by $\mathbb{Z}_{p^d}$ and a primitive root of unity of order $p^e - 1$. To construct such a ring, we start by adjoining a primitive root of unity ζ of order $p^e - 1$ to the p-adic rationals $\mathbb{Q}_p$. In this paper, we denote the ring of integers in $\mathbb{Q}_p$ by $\mathbb{Z}_{p^\infty}$ to avoid a clash of notation with the integers modulo p. Now $\mathbb{Z}_{p^\infty}[\zeta]$ is the ring of elements in $\mathbb{Q}_p(\zeta)$ that are integral over $\mathbb{Z}_{p^\infty}$, and $\mathbb{Z}_{p^\infty}[\zeta]$ is a local ring with the sole prime ideal generated by p. Then GR (p^d, e) is the quotient of $\mathbb{Z}_{p^\infty}[\zeta]$ by the ideal $p^d \mathbb{Z}_{p^\infty}[\zeta]$. It is not difficult to see that GR $(p^1, e) =$ GF (p^e) and GR $(p^d, 1) = \mathbb{Z}_{p^d}$. Thus, both finite fields and rings of integers modulo prime powers can be viewed as two different boundary cases of Galois rings.

The following is the main result of this paper.

Theorem 1.6: Let C be an Abelian code of length n over alphabet GR (p^d, e) with S the minimal support of the Fourier transform of C and $1 \notin S$. For any $c \in C$, we have

$$\operatorname{zer}(c) \equiv n \left(\operatorname{mod} p^{\lfloor \frac{\ell - p^d - 1}{(p-1)p^{d-1}} \rfloor - d(e-1)} \right)$$

where Λ and ℓ are as defined in (3) and (4).

This theorem reduces to Theorem 1.3 when $d = 1$ and to Theorem 1.5 when $e = 1$ (recall that $p - 1 \,|\, \ell$ in all cases). The full version of Theorem 1.6 also considers the possibility that $1 \notin S$ (see Corollary 5.2 to Theorem 5.1).

Example 1.7: As in Example 1.4, let $k > 0$ and let A be the cyclic group of order $4^k - 1$ generated by an element a. Here we let C be the code in GR $(4, 2)[A]$ whose Fourier transform is supported on the set $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. In a more conventional presentation of cyclic codes, this is the code in GR $(4, 2)[x]/(x^{4^k - 1} - 1)$ whose check polynomial is one of the kth-degree irreducible factors of the cyclotomic polynomial $\Phi_{4^k - 1}(x)$ in GR $(4, 2)[x]$.

Here, $p = 2, e = 2$, and $d = 2$ since we are working with GR $(4, 2)$. We can think of GR $(4, 2)$ as $\mathbb{Z}_4[\xi]$, where ξ is a root of unity of order 3. As in Example 1.4, $E = \{0, 1\}$ and $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. Therefore, Λ is exactly as in Example 1.4, and so $\ell = 2k$ here also. Thus, Theorem 1.6 tells us that $\operatorname{zer}(c) \equiv 4^k - 1 \pmod{2^{k-3}}$, or equivalently, that all Hamming weights are divisible by 2^{k-3}. □

To prove Theorem 1.6, we first set down mathematical preliminaries and examine the structure of Abelian codes over Galois rings in Section II. We shall prove a general form of our theorem in Section III, which will assume the existence of counting polynomials which we shall construct later in Section IV, using a technique called trace-averaging. This will enable us to prove Theorem 1.6 and related results in Section V.

II. Abelian Codes Over Galois Rings

Here we set down the mathematical foundations needed to present and prove our results. We are interested in understanding the structure of Abelian codes over Galois rings by means of the Fourier transform. These codes have already been studied, as remarked above, and moreover, their Fourier transform has already been presented in [30]. The familiar mathematical devices used for Abelian codes over finite fields or over $\mathbb{Z}_{p^d}$ generalize neatly to Abelian codes over Galois rings. In the Sections II-A

through II-C we provide a brief overview of these fundamentals, while casting them in a notation and terminology which will facilitate exposition of analogues of McEliece's theorem. Section II-D introduces many compact notations for dealing with objects related to the set Λ as defined in (1) or (3).

A. Preliminaries

The Galois ring GR (p^d, e) is defined in Section I-B above. As noted there, one can find in Section II-A of [10] all that we need to know about Galois rings. One also finds there what we need to know about the rings of algebraic integers in unramified extensions of the p-adic rationals. These latter rings are important because Galois rings are quotients of them and because we perform many of our calculations in p-adic fields. Throughout this paper, *integer* will mean rational integer, $\mathbb{N}$ will be the set of nonnegative integers, p will always be a prime in $\mathbb{Z}$, and d and e will be positive integers. We set $q = p^e$. The alphabet for our codes will be GR (p^d, e). As in Section I-B above, ζ is a root of unity of order $q-1$ over $\mathbb{Q}_p$, and $\mathbb{Z}_{p^\infty}$ denotes the ring of p-adic integers in $\mathbb{Q}_p$, and thus GR (p^d, e) is the quotient modulo p^d of $\mathbb{Z}_{p^\infty}[\zeta]$.

Our objects of study will be Abelian codes over GR (p^d, e). Throughout this paper, A will be a finite Abelian group with $p \nmid |A|$, and we shall write A multiplicatively with identity 1_A (or simply 1 when there is no cause for confusion). An *Abelian code over* GR (p^d, e) is an ideal in the group ring GR $(p^d, e)[A]$. We write an element $f \in$ GR $(p^d, e)[A]$ as a formal sum $\sum_{a \in A} f_a a$, and it is clear that such elements can be regarded as words of length $|A|$ over the alphabet GR (p^d, e).

Since we wish to calculate weights of codewords, or equivalently, to count zeroes, we would like to perform computations in rings of characteristic zero, since we cannot be sure in advance how high our counts will become. Thus, it is more advantageous to perform calculations in a ring like $\mathbb{Z}_{p^\infty}[\zeta]$ than to perform them in our alphabet GR (p^d, e), which is the quotient of $\mathbb{Z}_{p^\infty}[\zeta]$ modulo p^d. Furthermore, Theorem 2 of [34] tells us that we can define a Fourier transform if and only if we have a ring with roots of unity whose orders include all orders of elements in A. Therefore, we let ε be the least positive integer such that $q^\varepsilon - 1$ is a multiple of the order of every element in A, and we let η be a root of unity of order $q^\varepsilon - 1$ over $\mathbb{Q}_p$, such that $\zeta = \eta^{\frac{q^\varepsilon - 1}{q-1}}$. Then $\mathbb{Z}_{p^\infty}[\eta]$ and its quotient GR $(p^d, e\varepsilon)$ contain sufficient roots of unity to allow for a Fourier analysis with the finite Abelian group A, and, for the purposes of counting, $\mathbb{Z}_{p^\infty}[\eta]$ is of characteristic 0 (so it contains $\mathbb{Z}$).

B. Quotients, Lifts, and Automorphisms

We shall use π: $\mathbb{Z}_{p^\infty}[\eta] \to$ GR $(p^d, e\varepsilon)$ to denote the quotient map modulo p^d. Note that π restricted to $\mathbb{Z}_{p^\infty}[\zeta]$ is the quotient modulo p^d onto GR (p^d, e), and π restricted to $\mathbb{Z}_{p^\infty}$ is the quotient modulo p^d onto $\mathbb{Z}_{p^d}$. Note that $\pi(\eta)$ and $\pi(\zeta)$ are roots of unity or orders $q^\varepsilon - 1$ and $q-1$, respectively, in GR $(p^d, e\varepsilon)$ and GR (p^d, e).

We also define a right-inverse τ of π, which we call the *standard lift*. Any element $r \in$ GR $(p^d, e\varepsilon)$ can be written uniquely as $r = \sum_{i=0}^{d-1} r^{(i)} p^i$, where each $r^{(i)}$ is either zero or some power of $\pi(\eta)$. Any element $R \in \mathbb{Z}_{p^\infty}[\eta]$ can be written uniquely as $R = \sum_{i=0}^{\infty} R^{(i)} p^i$, where each $R^{(i)}$ is either zero or some power of η. We call these the *canonical expansions* of elements in GR $(p^d, e\varepsilon)$ and $\mathbb{Z}_{p^\infty}[\eta]$. The standard lift of r above is $\tau(r) = \sum_{i=0}^{d-1} R^{(i)} p^i$ where $R^{(i)} = 0$ when $r^{(i)} = 0$ and $R^{(i)} = \eta^j$ when $r^{(i)} = \pi(\eta)^j$. Note that $\tau(r) = 0$ if and only if $r = 0$. This property is called *preservation of support* because a function f from a set S into GR $(p^d, e\varepsilon)$ will vanish on precisely those points in S where the lifted function $\tau \circ f$ vanishes.

The Galois group of $\mathbb{Q}_p(\eta)$ over $\mathbb{Q}_p$ is cyclic of order $e\varepsilon$ and is generated by the automorphism σ, which fixes $\mathbb{Q}_p$ pointwise and maps η to η^p (and hence ζ to ζ^p). The Galois group of $\mathbb{Q}_p(\eta)$ over $\mathbb{Q}_p(\zeta)$ is cyclic of order ε and is generated by σ^e, which takes η to η^q. The restriction of σ to $\mathbb{Q}_p(\zeta)$ generates the Galois group of order e of $\mathbb{Q}_p(\zeta)$ over $\mathbb{Q}_p$. Since σ maps p to itself and units to units in the ring $\mathbb{Z}_{p^\infty}[\eta]$, it does not change the p-adic valuation of any element. Thus, it induces an automorphism on GR $(p^d, e\varepsilon)$ which fixes $\mathbb{Z}_{p^d}$ pointwise and maps $\pi(\eta)$ to $\pi(\eta)^p$. This automorphism of GR $(p^d, e\varepsilon)$ will also be called σ by abuse of notation, and it, in turn, restricts to an automorphism of the subring GR (p^d, e) which fixes $\mathbb{Z}_{p^d}$ pointwise and maps $\pi(\zeta)$ to $\pi(\zeta)^p$. All of these versions of σ, which take roots of unity to their pth power, will be called the *Frobenius automorphism*. Note that $\pi \circ \sigma = \sigma \circ \pi$ and $\sigma \circ \tau = \tau \circ \sigma$, where the version of σ appearing on the left-hand sides of these equations is σ on $\mathbb{Q}_p(\eta)$, and the version of σ appearing on the right-hand sides of these equations is σ on GR $(p^d, e\varepsilon)$. Thus, we may say that the Frobenius automorphism commutes with the quotient map and the standard lift.

Finally, we will employ the *trace*, the map Tr: $\mathbb{Q}_p(\zeta) \to \mathbb{Q}_p$ given by

$$\mathrm{Tr}(a) = \sum_{i=0}^{e-1} \sigma^i(a)$$

which is familiar from the theory of fields. Since Tr is $\mathbb{Z}_{p^\infty}$-linear, we have $\mathrm{Tr}(p^d a) = p^d \mathrm{Tr}(a)$, so that trace induces another map from GR (p^d, e) to $\mathbb{Z}_{p^d}$. This map is also called *trace* and is also denoted Tr. Note that Tr commutes with π and τ as a consequence of commutativity of these maps with the Frobenius automorphism.

C. Fourier Transform

The Fourier transform for Abelian codes over finite fields was introduced by MacWilliams [35] as a generalization of the Mattson–Solomon polynomial [36] for cyclic codes over finite fields. The basic theorems on the Fourier transform for Abelian codes over Galois rings are presented in [30], often without explicit proof, since the methods used for Abelian codes over finite fields and over $\mathbb{Z}_{p^d}$ generalize neatly. This section summarizes the results we shall need. We shall try to stay close to the style of Delsarte and McEliece [2] to facilitate comparison with their results. Nevertheless, we differ from them in writing the group operation of A multiplicatively and in other small points of notation.

Following Delsarte and McEliece [2], we introduce the bilinear pairing of [37], which establishes an isomorphism between A and the group of characters of A. This provides a con-

venient mode of presentation, inasmuch as the Fourier transform becomes a function whose domain is the group A rather than the set of characters of A. Fix elements $a_1, a_2, \ldots, a_t \in A$ of orders $n_1, n_2, \ldots, n_t$ so that every element of A may be written uniquely as $a_1^{e_1} a_2^{e_2} \cdots a_t^{e_t}$, with $0 \leq e_i < n_i$ for each i. Set $\eta_i = \eta^{\frac{q^e-1}{n_i}}$ for each i, so that η_i is a root of unity of order n_i. If $a = a_1^{e_1} a_2^{e_2} \cdots a_t^{e_t}$ and $b = a_1^{f_1} a_2^{f_2} \cdots a_t^{f_t}$ are in A, define

$$\langle a, b \rangle = \prod_{i=1}^{t} \eta_i^{e_i f_i}.$$

We have defined a function $\langle \cdot, \cdot \rangle \colon A \times A \to \mathbb{Z}_{p^\infty}[\eta]$, whose basic properties we now state. We use the convention that $\delta_{x,y} = 1$ if $x = y$ and is zero otherwise.

Lemma 2.1: For any $a, b, c \in A$ and $n \in \mathbb{Z}$

$$\begin{aligned} \langle a, b \rangle &= \langle b, a \rangle \\ \langle a, bc \rangle &= \langle a, b \rangle \langle a, c \rangle \\ \langle a, b^n \rangle &= \langle a, b \rangle^n \\ \sum_{b \in A} \langle a, b \rangle &= |A| \delta_{a, 1_A} \end{aligned}$$

and $\langle a, b \rangle = 1$ for all $b \in A$ if and only if $a = 1_A$.

Proof: These can be verified easily. □

For $f \in \mathbb{Z}_{p^\infty}[\eta][A]$, we define the *Fourier transform of* f, which we denote by $\hat{f}$, as the function from A to $\mathbb{Z}_{p^\infty}[\eta]$ given by

$$\hat{f}_a = \sum_{b \in A} f_b \langle b^{-1}, a \rangle$$

where we write $\hat{f}_a$ rather than $\hat{f}(a)$ for the value of $\hat{f}$ at the point a. The Fourier transform maps $\mathbb{Z}_{p^\infty}[\eta][A]$ to $\mathbb{Z}_{p^\infty}[\eta]^A$, and is in fact a bijection with inverse

$$f_a = \frac{1}{|A|} \sum_{b \in A} \hat{f}_b \langle b, a \rangle.$$

Furthermore, the Fourier transform clearly preserves addition and $\mathbb{Z}_{p^\infty}[\eta]$-scalar multiplication. It also takes multiplication in the group ring $\mathbb{Z}_{p^\infty}[\eta][A]$ to pointwise multiplication in $\mathbb{Z}_{p^\infty}[\eta]^A$. Thus, the Fourier transform is a $\mathbb{Z}_{p^\infty}[\eta]$-algebra isomorphism. The Fourier transform and its inverse establish a bijection between $p^d \mathbb{Z}_{p^\infty}[\eta][A]$ and $p^d \mathbb{Z}_{p^\infty}[\eta]^A$, so that they induce a Fourier transform and inverse Fourier transform on $\mathrm{GR}\,(p^d, e\varepsilon)[A]$ and $\mathrm{GR}\,(p^d, e\varepsilon)^A$. For convenience in presenting our results, it will be useful to introduce a version of the Fourier transform which has been scaled by $\frac{1}{|A|}$, so we set $\tilde{f} = \frac{1}{|A|} \hat{f}$ and call it the *scaled Fourier transform*. Since $p \nmid |A|$, $\frac{1}{|A|}$ exists in $\mathbb{Z}_{p^\infty}[\eta]$ and $\mathrm{GR}\,(p^d, e\varepsilon)$. Then the inversion formula becomes $f_a = \sum_{b \in A} \tilde{f}_b \langle b, a \rangle$.

Since our codes are ideals in $\mathbb{Z}_{p^\infty}[\zeta][A]$, a proper subring of $\mathbb{Z}_{p^\infty}[\eta][A]$, it will be useful to see which elements of $\mathbb{Z}_{p^\infty}[\eta]^A$ are actually Fourier transforms of elements in $\mathbb{Z}_{p^\infty}[\zeta][A]$.

Proposition 2.2: (cf. [30, eq. (4)]): Let $f \in \mathbb{Z}_{p^\infty}[\eta][A]$ (resp., $\mathrm{GR}\,(p^d, e\varepsilon)[A]$). Then the word f is in $\mathbb{Z}_{p^\infty}[\zeta][A]$ (resp., $\mathrm{GR}\,(p^d, e)[A]$) if and only if $\hat{f}_{a^q} = \sigma^e(\hat{f}_a)$ for all $a \in A$. Equivalently, f is in $\mathbb{Z}_{p^\infty}[\zeta][A]$ (resp., $\mathrm{GR}\,(p^d, e)[A]$) if and only if $\tilde{f}_{a^q} = \sigma^e(\tilde{f}_a)$ for all $a \in A$. The Fourier transform is thus an isomorphism of $\mathrm{GR}\,(p^d, e)$-algebras from $\mathrm{GR}\,(p^d, e)[A]$ to the $\mathrm{GR}\,(p^d, e)$-algebra $\mathcal{A}$ consisting of the elements $g \in \mathrm{GR}\,(p^d, e\varepsilon)^A$ that meet the condition $g_{a^q} = \sigma^e(g_a)$.

Proof: The proof is much the same as that of [2, eq. (2.10)], [19, Theorem 3], and [10, Proposition 2.1]. □

The following corollary, needed for our proof, shows that the scaled Fourier transform and the standard lift are in some respect compatible.

Corollary 2.3: Let $f \in \mathrm{GR}\,(p^d, e)[A]$ and let F be the unique element of $\mathbb{Z}_{p^\infty}[\eta][A]$ so that $\tilde{F} = \tau \circ \tilde{f}$. Then F is in $\mathbb{Z}_{p^\infty}[\zeta][A]$ with $\pi \circ F = f$.

Proof: This proof is much the same as that of Corollary 2.2 in [10]. □

If $f \in \mathrm{GR}\,(p^d, e)[A]$, then the proposition shows that $\hat{f}_a, \hat{f}_{a^q}, \hat{f}_{a^{q^2}}, \ldots$ are all determined by the value of $\hat{f}_a$. Following Delsarte and McEliece (in [2, Section 1]), we define two elements $a, b \in A$ to be *q-equivalent* if $a = b^{q^j}$ for some $j \in \mathbb{Z}$ (treating exponents as integers modulo $|A|$). This is an equivalence relation partitioning A into *q-classes* (also called *cyclotomic classes*), and so the proposition says that if $f \in \mathrm{GR}\,(p^d, e)[A]$, then $\hat{f}$ is determined entirely by its values on a set of representatives of q-classes. The following proposition makes this observation more precise.

Proposition 2.4: (cf. [30, pp. 2244–2245]): Let R be a set of q-class representatives of A, and for each $r \in R$, set ε_r equal to the cardinality of the q-class of r. Then $\varepsilon_r \,|\, \varepsilon$ for each r. Let $\mathcal{A}$ be the $\mathrm{GR}\,(p^d, e)$-subalgebra of $\mathrm{GR}\,(p^d, e\varepsilon)^A$ as defined in Proposition 2.2. Then restriction of domains from A to R is a $\mathrm{GR}\,(p^d, e)$-algebra isomorphism from $\mathcal{A}$ to $\bigoplus_{r \in R} \mathrm{GR}\,(p^d, e\varepsilon_r)$.

Proof: The proof is much the same as that of [19, Theorem 4] or [10, Proposition 2.4]. □

Combining Propositions 2.2 and 2.4, we obtain the basic structure theorem for Abelian codes over Galois rings.

Theorem 2.5 (cf. [30, pp. 2245–2246]): Let R be a set of q-class representatives of A, and for each $r \in R$, set ε_r equal to the cardinality of the q-class of r. Then the $\mathrm{GR}\,(p^d, e)$-algebra $\mathrm{GR}\,(p^d, e)[A]$ is isomorphic (*via* Fourier transform followed by restriction of domains to R) to

$$\mathcal{B} = \bigoplus_{r \in R} \mathrm{GR}\,(p^d, e\varepsilon_r).$$

This establishes a bijective correspondence between ideals (codes) in the group ring $\mathrm{GR}\,(p^d, e)[A]$ and ideals in the direct sum $\mathcal{B}$, which are of the form $\bigoplus_{r \in R} p^{i_r} \mathrm{GR}\,(p^d, e\varepsilon_r)$ with $0 \leq i_r \leq d$.

Proof: This is just the combination of Propositions 2.2 and 2.4 and the observation that all ideals in a Galois ring are generated by powers of p. □

For any function f from A into a ring, we define a *support* of f to be a subset S of A such that $f_a = 0$ for $a \notin S$. If our function f takes values in $\mathrm{GR}\,(p^d, e\varepsilon)$, then a *$p^k$-support* of f is a subset S of A such that $f_a \equiv 0 \,(\mathrm{mod}\, p^k)$ for $a \notin S$. By

minimal supports or p^k-supports we mean minimal ones under the inclusion relation $\subseteq$. If $f\colon A \to \mathrm{GR}(p^d, e\varepsilon)$ and S_k is the minimal p^k-support of f for $1 \le k \le d$, then $S_1 \subseteq \cdots \subseteq S_d$ is called the *tower of supports* of f.

If $\mathcal{F}$ is a set of functions, then a *support* (resp., p^k-*support*) of $\mathcal{F}$ is a set which is simultaneously a support (resp., p^k-support) of all $f \in \mathcal{F}$. If the functions in $\mathcal{F}$ have $\mathrm{GR}(p^d, e\varepsilon)$ as their target space, then $\mathcal{F}$ has a tower supports formed of its minimal p^k-supports. This terminology of supports now enables us to draw out the consequences of Theorem 2.5 for the structure of Abelian codes over Galois rings.

Corollary 2.6: (cf. [30, p. 2246]): For each ideal (code) C in $\mathrm{GR}(p^d, e)[A]$, let $T(C)$ be the tower of supports of the set $\hat{C}$ of Fourier transforms of the elements of C. Then T is a bijection between the set of codes in $\mathrm{GR}(p^d, e)[A]$ and the set of towers $S_1 \subseteq \cdots \subseteq S_d$ of q-closed subsets of A.

Proof: The proof is much the same as that of Corollary 2.6 in [10]. □

This shows that an Abelian code over $\mathrm{GR}(p^d, e)$ is uniquely determined by the tower of supports of its Fourier transform. The sets in the tower are called *defining sets* in [25], where they are shown to determine uniquely cyclic codes over Galois rings. Equivalently, in [30] the collection of sets

$$\{S_1, S_2 \setminus S_1, \ldots, S_d \setminus S_{d-1}, A \setminus S_d\}$$

called the *defining partition*, is shown to determine uniquely Abelian codes over Galois rings. In the case when $d = 1$, $\mathrm{GR}(p^d, e) = \mathrm{GF}(q)$, and the tower is simply S_1, the support of the Fourier transform modulo p^1. In the finite field $\mathrm{GF}(q)$, we have $p = 0$, so S_1 is the support of the Fourier transform, i.e., the spectrum of the code. This prompts us to call the tower of supports of the Fourier transform of a code in $\mathrm{GR}(p^d, e)[A]$ the *spectral tower* of the code.

D. Accounts and Compact Notations

Here we introduce some notation which is intended to make constructions like that of Λ in (3) easier to handle. One can observe that if a sequence λ is in the set Λ in (3), then so is any permutation of λ; the order of the sequences does not play any role in the determination of the key parameter ℓ in (4). This became apparent in Example 1.4, where, in considering sequences in Λ, it was often useful to avoid specifying the order of the terms. For this reason, we shall be more interested in multisets of elements than in sequences. In fact, it will be convenient to have a generalization of multisets which allows us to have a negative count of any given element. Thus, given any finite set X, we define an *account of* X to be a function from X into $\mathbb{Z}$. If f is an account of X, we shall use f_x to denote the value of f at $x \in X$. The set of accounts of X is just the free Abelian group on X under addition and is denoted $\mathbb{Z}[X]$. We can write the account f in additive form $f = \sum_{x \in X} f_x x$ or, if there is danger of confusion of the integer coefficients f_x with the elements $x \in X$, we shall enclose the elements of X in square brackets, so $f = \sum_{x \in X} f_x[x]$. If $X \subseteq Y$, we may consider $f \in \mathbb{Z}[X]$ to be an element of $\mathbb{Z}[Y]$ by considering $f_y = 0$ for $y \in Y \setminus X$.

Accounts of X which take only nonnegative values are identified with multisets of elements of X in the obvious way and accounts which take only values in $\{0, 1\}$ are similarly identified with subsets of X. We let $\mathbb{N}[X]$ denote the set of all multisets of elements of X, and from now on we shall simply say *multisets of* X to mean multisets of elements of X. If Y is a subset of X, we use the notation $f \Subset Y$ to mean that f is a multiset supported on Y, i.e., $f_x = 0$ for $x \notin Y$ and $f_x \ge 0$ for all x.

The *size* of an account f on X is $\sum_{x \in X} f_x$ and is denoted by $|f|$. Note that $|\cdot|\colon \mathbb{Z}[X] \to \mathbb{Z}$ is a homomorphism of additive groups. If f is a multiset, then size is the same as cardinality.

Now we can formulate an equivalent definition of ℓ in (4) using our new notation for accounts and multisets. For the rest of this paper, we shall use E to denote the set $\{0, 1, \ldots, e-1\}$, as in Section I-A. With S a subset of A, we let

$$\Lambda' = \left\{ \lambda \in \mathbb{N}[S \times E]\colon \lambda \notin \{1\} \times E, \prod_{(s,t) \in S \times E} (s^{p^t})^{\lambda_{s,t}} = 1, \sum_{(s,t) \in S \times E} \lambda_{s,t} p^t \equiv 0 \,(\mathrm{mod}\, q-1) \right\}. \quad (5)$$

A careful comparison shows that a multiset λ is in Λ' if and only if it is the multiset of terms of some sequence in the set Λ defined in (3). Thus, we could define

$$\ell = \min_{\lambda \in \Lambda'} |\lambda|$$

and this would be equivalent to the definition in (4).

Example 2.7: As in Examples 1.4 and 1.7, let $k > 0$ and let A be the cyclic group of order $4^k - 1$ generated by an element a. In both examples, we let C be a code over some ring R (i.e., we let C be an ideal in $R[A]$) whose Fourier transform is supported on the set $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. We had $R = \mathrm{GF}(4)$ in Example 1.4 and $R = \mathrm{GR}(4, 2)$ in Example 1.7. In both examples, $E = \{0, 1\}$, so that Λ and ℓ were the same.

In Example 1.4, we determined that the minimum-length sequences in Λ were all sequences in which each element of $S \times E$ occurred exactly once. Thus, we determined that $\ell = 2k$. Recall that a sequence is in Λ if and only if the multiset of its terms is in Λ'. Thus, Λ' is more convenient to use than Λ because it contains a unique multiset $\lambda_{\min}$ of minimum cardinality: the multiset with one instance of each element of $S \times E$, which we can denote as the formal sum

$$\lambda_{\min} = (a, 0) + (a, 1) + \cdots + (a^{4^{k-1}}, 0) + (a^{4^{k-1}}, 1).$$

Of course $|\lambda_{\min}| = 2k$.

In Example 1.4, we also discussed the sequences of length $2k + 1$ in Λ, which were obtained from the minimum-length sequences by deleting an element (a^{4^f}, g) and inserting two instances of $(a^{4^f}, 0)$ if $g = 1$ or two instances of $(a^{4^{f+k-1}}, 1)$ if $g = 0$. Again, it is easier to handle Λ', wherein there are precisely $2k$ multisets of cardinality $2k + 1$, which have the form $\lambda_{\min} - (a^{4^j}, 1) + 2(a^{4^j}, 0)$ for $j = 0, 1, \ldots, k-1$ or $\lambda_{\min} - (a^{4^j}, 0) + 2(a^{4^{j+k-1}}, 1)$ for $j = 0, 1, \ldots, k-1$. □

Since we can think of multisets as sequences without order, it is useful to provide a terminology and notation which will help

in counting the number of sequences which can be formed from a multiset. If $f \in \mathbb{N}[X]$, we use $f!$ as a shorthand for $\prod_{x\in X} f_x!$. Thus, the number of distinct sequences which can be formed by placing the elements of the multiset f in various orders is $|f|!/f!$.

The definition of Λ' in (5), like that of Λ in (3), is still quite cumbersome, and we shall attempt to make it more manageable. Note that the multisets in Λ' are composed of elements of $S \times E \subseteq A \times E$. An account $\lambda \in \mathbb{Z}[A \times E]$ is called *trivial* if it is supported on $\{1_A\} \times E$, i.e., if $\lambda_{a,b} = 0$ whenever $a \neq 1_A$. Note that the first condition in the definition of Λ' in (5) says that λ is nontrivial.

Now consider the second condition in the definition of Λ'. If $\lambda \in \mathbb{Z}[A \times E]$, then we define the *product* of λ, denoted $\Pi\lambda$, to be

$$\Pi\lambda = \prod_{(a,b)\in A\times E} \left(a^{p^b}\right)^{\lambda_{a,b}}.$$

Note that Π is a homomorphism from the additive group of $\mathbb{Z}[A \times E]$ into the group A. An account $\lambda \in \mathbb{Z}[A \times E]$ is called *unity-product* if $\Pi\lambda = 1_A$. Note that the trivial elements of $\mathbb{Z}[A \times E]$ are always unity-product (indeed, in a trivial way) and that the empty set is trivial. The second condition in the definition of Λ' in (5) can now be written in a more compact notation

$$\Lambda' = \left\{ \lambda \in \mathbb{N}[S \times E] \colon \lambda \notin \{1\} \times E, \Pi\lambda = 1, \sum_{(s,t)\in S\times E} \lambda_{s,t} p^t \equiv 0 \,(\mathrm{mod}\, q-1) \right\}. \quad (6)$$

This is more convenient, but the third condition is still lengthy to state.

We shall condense the third condition in the definition of Λ' by considering accounts of E. If $\gamma = (a,b) \in A \times E$, then we define the *exponent of* γ, denoted $\exp(\gamma)$, to be b. If $\lambda \in \mathbb{Z}[A \times E]$, then define $\exp(\lambda)$ to be the account of exponents in λ, i.e., $\exp(\lambda)$ is the account $\mu \in \mathbb{Z}[E]$ with $\mu_b = \sum_{a\in A} \lambda_{a,b}$ for all $b \in E$. Note that exp is a homomorphism of additive groups from $\mathbb{Z}[A \times E]$ to $\mathbb{Z}[E]$. With this notation, we can rewrite the last condition in the definition of Λ' in (6) as

$$\sum_{t\in E} (\exp(\lambda))_t p^t \equiv 0 \pmod{q-1}.$$

If μ is an account of E, we define the *sum* of μ, denoted $\Sigma\mu$, to be

$$\Sigma\mu = \sum_{t\in E} \mu_t p^t \pmod{q-1}.$$

Note that Σ is a homomorphism of groups from $\mathbb{Z}[E]$ to the group of integers modulo $q-1$ under addition. Now we can further condense our notation for the last condition in the definition of Λ' to obtain

$$\Lambda' = \{\lambda \in \mathbb{N}[S \times E] \colon \lambda \notin \{1\} \times E, \Pi\lambda = 1, \Sigma \exp(\lambda) = 0\}.$$

We shall name and more carefully analyze this last condition.

An account μ on E will be called *Delsarte–McEliece* (or *D-M* for short) if $\Sigma\mu = 0$. An account $\lambda \in \mathbb{Z}[A \times E]$ is said to be *Delsarte–McEliece* (or *D–M* for short) if $\exp(\lambda)$ is a D-M account of E. So the third condition in the definition of Λ' states that λ must be D-M.

Example 2.8: We return to the same situation as in Examples 1.4, 1.7, and 2.7: $k > 0, A$ is the cyclic group of order $4^k - 1$ generated by $a, S = \{a, a^4, \ldots, a^{4^{k-1}}\}$, $E = \{0,1\}, p = 2, e = 2$, and $q = p^e = 4$. Then it was shown in Example 2.7 that Λ' contains a unique multiset of minimal cardinality

$$\lambda_{\min} = (a,0) + (a,1) + \cdots + (a^{4^{k-1}},0) + (a^{4^{k-1}},1)$$

with $|\lambda_{\min}| = 2k$. We also saw that Λ' contains precisely $2k$ multisets of cardinality $2k+1$, which have the form $\lambda_{\min} - (a^{4^j},1) + 2(a^{4^j},0)$ for $j = 0,1,\ldots,k-1$ or $\lambda_{\min} - (a^{4^j},0) + 2(a^{4^{j+k-1}},1)$ for $j = 0,1,\ldots,k-1$.

Note that $\exp(\lambda_{\min}) = k[0] + k[1]$, so that

$$\sum \exp(\lambda_{\min}) = k \cdot 1 + k \cdot 2 = 0 \pmod 3.$$

Likewise, note that

$$\exp\left(\lambda_{\min} - (a^{4^j},0) + 2(a^{4^{j+k-1}},1)\right) = (k-1)[0] + (k+2)[1]$$

so that

$$\sum \exp\left(\lambda_{\min} - (a^{4^j},0) + 2(a^{4^{j+k-1}},1)\right) = (k-1)\cdot 1 + (k+2)\cdot 2$$

which is zero, since $\sum$ maps into the integers modulo 3. □

Here we state and prove some important basic results about D-M accounts of E. The first lemma is essentially the same as a result proved by Ward [6] in a study of p-divisibility of weights in codes, so we omit the proof.

Lemma 2.9: (cf. [6, Lemma 2.1]): All D-M accounts of E have cardinality divisible by $p-1$. The unique smallest nonempty D-M multiset of E is $\sum_{i\in E}(p-1)[i]$, which has cardinality $e(p-1)$.

This implies corresponding facts about D-M accounts of $A \times E$.

Corollary 2.10: A D-M account of $A \times E$ has cardinality divisible by $p-1$, and if it is a nonempty multiset, it has cardinality at least $e(p-1)$.

Proof: This follows immediately from Lemma 2.9 and the fact that $|\lambda| = |\exp(\lambda)|$ for any $\lambda \in \mathbb{Z}[A \times E]$. □

Here are some facts about D-M unity-product elements of $\mathbb{N}[A \times E]$ that we shall need to know in Section V.

Lemma 2.11: If S is a subset of A and there is some $s \in S$ with $s \neq 1_A$, then there exists a nontrivial D-M unity-product element of $\mathbb{N}[S \times E]$.

Proof: Let n be the order of s in the group A and consider the multiset $n(q-1)(s,0)$. Note that this multiset is nontrivial, D-M, unity-product, and supported on $S \times E$. □

Lemma 2.12: Suppose that S is q-closed. Suppose that $\lambda \in \mathbb{N}[S \times E]$ is a nontrivial D-M unity-product multiset of minimal cardinality subject to these conditions. Then λ will have no more than $p-1$ instances of any given element, and so $\lambda!$ will be an integer not divisible by p.

Proof: Suppose that κ is a nontrivial D-M unity-product multiset supported on $S \times E$ with $\kappa_{a,b} \geq p$ for some $(a,b) \in S \times E$. We shall construct another nontrivial D-M unity-product multiset supported on $S \times E$ of smaller cardinality. If $b < e-1$, let $\nu = -p(a,b)+(a,b+1)$, and if $b = e-1$, let $\nu = -p(a,b)+(a^q,0)$. In each case, one can see that ν is D-M, unity-product, and supported on $S \times E$. Thus, $\kappa + \nu$ is D-M, unity-product, and supported on $S \times E$. Furthermore, since $\kappa_{a,b} \geq p$, this new account is in fact a multiset. Note that $|\kappa+\nu| = |\kappa|+|\nu| = |\kappa|-(p-1)$. It remains to show that $\kappa+\nu$ is nontrivial. If $a = 1_A$, then ν is trivial, and since κ is nontrivial, this means that $\kappa+\nu$ must be nontrivial. So henceforth assume $a \neq 1_A$. Then $a^q \neq 1_A$ since $|A|$ is coprime to q. Thus, $\kappa+\nu$ is clearly nontrivial since $(\kappa+\nu)_{(a,b+1)} > 0$ if $b < e-1$ or $(\kappa+\nu)_{(a^q,0)} > 0$ if $b = e-1$.

So it is clear that if κ is a nontrivial D-M unity-product multiset supported on $S \times E$ of minimal cardinality, then $\kappa_{a,b} < p$ for all $(a,b) \in S \times E$. Thus, $\kappa! = \prod_{(a,b) \in S \times E} \kappa_{a,b}!$ is clearly not divisible by p. □

We have developed enough notation to express compactly some notions of previous works. Now we give some notational conventions whose usefulness will be seen later in this paper. We shall often use polynomials in the e indeterminates $x_0, x_1, \ldots, x_{e-1}$. The boldface letter $\boldsymbol{x}$ will always stand for the list $(x_0, x_1, \ldots, x_{e-1})$. We can consider an element $\mu \in \mathbb{N}[E]$ as a list of exponents for these indeterminates by means of the convention $\boldsymbol{x}^\mu = x_0^{\mu_0} x_1^{\mu_1} \cdots x_{e-1}^{\mu_{e-1}}$. If $r \in \mathbb{Q}_p(\eta)$ or $\mathrm{GR}\,(p^d, e\varepsilon)$, then we define

$$r^\mu = \prod_{i \in E} (\sigma^i(r))^{\mu_i}.$$

Note that with this definition we have $(rs)^\mu = r^\mu s^\mu$. If F is a function from A to $\mathbb{Q}_p(\eta)$ or from A to $\mathrm{GR}\,(p^d, e\varepsilon)$ and $\lambda \in \mathbb{N}[A \times E]$, we shall use the notation F_λ to denote

$$\prod_{(a,b) \in A \times E} (\sigma^b(F_a))^{\lambda_{a,b}}.$$

If κ is another element of $\mathbb{N}[A \times E]$, note that $F_{\kappa+\lambda} = F_\kappa F_\lambda$.

III. The Form of the Theorem

We now prove a generic version of our analogue of McEliece's theorem. It presupposes the existence of polynomials having certain properties; these will be constructed in Section IV. Although we are interested mainly in p-adic estimates of the Hamming weights (or equivalently, the zero counts) of codewords, we can work in a more general context, where we have a function wt: $\mathrm{GR}\,(p^d, e) \to \mathbb{Z}$, which we call a *weight function*, in place of zer. This function assigns an integer weight $\mathrm{wt}(r)$ to each letter r of the alphabet $\mathrm{GR}\,(p^d, e)$. If $c \in \mathrm{GR}\,(p^d, e)[A]$ is a codeword, the weight of the codeword is, of course, the sum of the weights of the letters occurring in it, i.e., $\sum_{a \in A} \mathrm{wt}(c_a)$, which we denote by $\mathrm{wt}(c)$. The statement of our theorem uses extensively the compact notations introduced in Section II-D.

Theorem 3.1: Let $h(\boldsymbol{x}) = \sum_{\mu \in \mathbb{N}[E]} h_\mu \boldsymbol{x}^\mu$ be a polynomial in $\mathbb{Q}_p(\zeta)[\boldsymbol{x}]$ with the property that

$$h(r, \sigma(r), \ldots, \sigma^{e-1}(r)) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}$$

for all $r \in \mathbb{Z}_{p^\infty}[\zeta]$. Suppose that $f \in \mathrm{GR}\,(p^d, e)[A]$ with S a support of $\hat{f}$. Let $\tilde{F} = \tau \circ \tilde{f}$. Then

$$\mathrm{wt}(f) \equiv |A| \mathrm{wt}\left(\tilde{f}_{1_A}\right) + |A| \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where B_μ is the set of nontrivial unity-product $\lambda \in \mathbb{N}[S \times E]$ with $\exp(\lambda) = \mu$.

Proof: The symbol $\equiv$ will always denote congruence modulo p^m in this proof.

Let us start by considering an arbitrary word g in the group ring $\mathrm{GR}\,(p^d, e)[A]$. Set G to be the element of $\mathbb{Z}_{p^\infty}[\eta][A]$ such that $\tilde{G} = \tau \circ \tilde{g}$. Then by Corollary 2.3, we have $\pi \circ G = g$, so that

$$\begin{aligned} \mathrm{wt}(g) &= \mathrm{wt}(\pi \circ G) \\ &= \sum_{a \in A} \mathrm{wt}(\pi(G_a)). \end{aligned}$$

Corollary 2.3 further tells us that $G_a \in \mathbb{Z}_{p^\infty}[\zeta]$ for all a, so that we may employ the given property of the polynomial h to obtain

$$\begin{aligned} \mathrm{wt}(g) &\equiv \sum_{a \in A} h(G_a, \sigma(G_a), \ldots, \sigma^{e-1}(G_a)) \\ &\equiv \sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} h_\mu G_a^\mu. \end{aligned}$$

Now we write G_a using the inverse Fourier transform to obtain

$$\mathrm{wt}(g) \equiv \sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} h_\mu \left(\sum_{b \in A} \tilde{G}_b \langle b, a \rangle \right)^\mu.$$

We use the distributive law and some combinatorics to manipulate the final term. Then $\mathrm{wt}(g)$ is congruent modulo p^m to

$$\sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} h_\mu \sum_{\substack{\lambda \in \mathbb{N}[A \times E], \\ \exp(\lambda) = \mu}} \frac{\mu!}{\lambda!} \prod_{(b,t) \in A \times E} (\sigma^t(\tilde{G}_b \langle b, a \rangle))^{\lambda_{b,t}}$$

which, using our compact notation, equals

$$\sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\substack{\lambda \in \mathbb{N}[A \times E], \\ \exp(\lambda) = \mu}} \frac{\tilde{G}_\lambda}{\lambda!} \prod_{(b,t) \in A \times E} (\sigma^t(\langle b, a \rangle))^{\lambda_{b,t}}.$$

Since $\langle b, a \rangle$ is always a root of unity, σ maps it to its pth power, so that

$$\mathrm{wt}(g) \equiv \sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\substack{\lambda \in \mathbb{N}[A \times E], \\ \exp(\lambda) = \mu}} \frac{\tilde{G}_\lambda}{\lambda!} \prod_{(b,t) \in A \times E} \langle b, a \rangle^{p^t \lambda_{b,t}}.$$

Now Lemma 2.1 tells us that

$$\begin{aligned} \prod_{(b,t) \in A \times E} \langle b, a \rangle^{p^t \lambda_{b,t}} &= \left\langle \prod_{(b,t) \in A \times E} b^{p^t \lambda_{b,t}}, a \right\rangle \\ &= \langle \Pi\lambda, a \rangle, \end{aligned}$$

so that

$$\mathrm{wt}(g) \equiv \sum_{a \in A} \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\substack{\lambda \in \mathbb{N}[A \times E], \\ \exp(\lambda) = \mu}} \frac{\tilde{G}_\lambda}{\lambda!} \langle \Pi\lambda, a \rangle.$$

Now we exchange the order of summation and apply Lemma 2.1 to get

$$\begin{aligned}\mathrm{wt}(g) &\equiv \sum_{\mu\in\mathbb{N}[E]} \mu! h_\mu \sum_{\substack{\lambda\in\mathbb{N}[A\times E],\\ \exp(\lambda)=\mu}} \frac{\tilde{G}_\lambda}{\lambda!} \sum_{a\in A}\langle \Pi\lambda, a\rangle \\ &\equiv |A| \sum_{\mu\in\mathbb{N}[E]} \mu! h_\mu \sum_{\substack{\lambda\in\mathbb{N}[A\times E],\\ \exp(\lambda)=\mu,\\ \Pi\lambda=1}} \frac{\tilde{G}_\lambda}{\lambda!}.\end{aligned}$$

We may regard the last expression as a polynomial function with coefficients in $\mathbb{Q}_p(\zeta)$ and variables in the set $\{\sigma^t(\tilde{G}_a)\colon a\in A, t\in E\}$. If we segregate all terms that only have variables in $\{\sigma^t(\tilde{G}_{1_A})\colon t\in E\}$, we obtain

$$\begin{aligned}\mathrm{wt}(g) \equiv \rho\left(\tilde{G}_{1_A}, \sigma(\tilde{G}_{1_A}), \ldots, \sigma^{e-1}(\tilde{G}_{1_A})\right) \\ + |A| \sum_{\mu\in\mathbb{N}[E]} \mu! h_\mu \sum_{\lambda\in\Gamma_\mu} \frac{\tilde{G}_\lambda}{\lambda!} \quad (7)\end{aligned}$$

where $\rho(\boldsymbol{x})$ is some polynomial in $\mathbb{Q}_p(\zeta)[\boldsymbol{x}]$ and Γ_μ is the set of all nontrivial unity-product $\lambda\in\mathbb{N}[A\times E]$ with $\exp(\lambda)=\mu$.

Now vary g over all words in $\mathrm{GR}\,(p^d,e)[A]$ such that $\tilde{g}$ is supported on $\{1_A\}$, i.e., over all constant words. By preservation of support by τ (see Section II-B), $\tilde{G}$ is also supported on $\{1_A\}$. So for these words, the second term on the right-hand side of (7) vanishes. Such words have $g_a=\tilde{g}_{1_A}$ for all a. Thus, $\mathrm{wt}(g)=|A|\mathrm{wt}(\tilde{g}_{1_A})$ for such words. So

$$\rho\left(\tilde{G}_{1_A}, \sigma(\tilde{G}_{1_A}), \ldots, \sigma^{e-1}(\tilde{G}_{1_A})\right) \equiv |A|\mathrm{wt}\,(\tilde{g}_{1_A})$$

for all g whose Fourier transform is supported on $\{1_A\}$. For such words, $\tilde{g}_{1_A}$ varies over all of $\mathrm{GR}\,(p^d,e)$. So

$$\rho(\tau(r), \sigma(\tau(r)), \ldots, \sigma^{e-1}(\tau(r))) \equiv |A|\mathrm{wt}(r)$$

for all $r\in\mathrm{GR}\,(p^d,e)$.

Now it should be observed that any word at all in $\mathrm{GR}\,(p^d,e)[A]$ has $\tilde{g}_{1_A}\in\mathrm{GR}\,(p^d,e)$, so that $\tilde{G}_{1_A}$ will always be the standard lift of the element $\tilde{g}_{1_A}\in\mathrm{GR}\,(p^d,e)$. Thus, we may replace the first term on the right-hand side of (7) with $|A|\mathrm{wt}(\tilde{g}_{1_A})$, to obtain

$$\mathrm{wt}(g) \equiv |A|\mathrm{wt}\,(\tilde{g}_{1_A}) + |A| \sum_{\mu\in\mathbb{N}[E]} \mu! h_\mu \sum_{\lambda\in\Gamma_\mu} \frac{\tilde{G}_\lambda}{\lambda!}. \quad (8)$$

Suppose now that $\hat{g}$ (and, hence, $\tilde{g}$) is supported on the subset S of A. Then, by preservation of support by the standard lift (see Section II-B), $\tilde{G}$ is also supported on S. Furthermore, suppose that there is some $\mu\in\mathbb{N}[E]$ and some $\lambda\in\Gamma_\mu$ with $\lambda\notin\mathbb{N}[S\times E]$. Then we have $\lambda_{a,t}>0$ for some $a\in A\setminus S$ and some $t\in E$. In this case, note that $\tilde{G}_\lambda=\sigma^t(\tilde{G}_a)\tilde{G}_{\lambda-(a,t)}=0$. Thus, we can replace the set Γ_μ in (8) with B_μ as defined in the statement of this theorem. □

We pause to show some examples of the use of this theorem. In each example, we furnish a particular polynomial $h(\boldsymbol{x})$ which allows us to use the theorem in our specific application without giving a detailed account of how such a polynomial is obtained. The procedure for constructing these polynomials is the subject of the next section. The main result of this paper, Theorem 1.6, follows from Theorem 3.1 applied with a family of polynomials whose existence is proved in Theorem 4.10 of the next section. Thus, in the most typical application of Theorem 3.1, we shall not need to construct explicitly or even write out the polynomial $h(\boldsymbol{x})$ with which the theorem is being applied. Nevertheless, we write out explicit polynomials in our examples that follow to give the reader a notion of the objects used in the inner workings of Theorem 3.1. The first two examples show the usual scenario in which knowledge of the existence and degree of the polynomial $h(\boldsymbol{x})$ alone is sufficient to obtain useful results from Theorem 3.1. This is the usual situation. The third example shows how one can sometimes obtain more information by an explicit calculation with $h(\boldsymbol{x})$.

In our first example, we consider a code over a finite field to show how our method can be used to recover the results of Delsarte and McEliece (Theorem 1.3).

Example 3.2: Let A be the cyclic group of order 15 generated by an element a and let C be the code in $\mathrm{GR}\,(2,2)[A]=\mathrm{GF}\,(4)[A]$ whose Fourier transform is supported on the set $S=\{a,a^4\}$. In a more conventional presentation of cyclic codes, this is the code in $\mathrm{GF}\,(4)[x]/(x^{15}-1)$ whose check polynomial is one of the quadratic irreducible factors of the cyclotomic polynomial

$$\Phi_{15}(x)=\frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)}$$

in $\mathrm{GF}\,(4)[x]$. This code is also known as the shortened first-order Reed–Muller code of length 15 over $\mathrm{GF}\,(4)$. We have already investigated codes of this form in Example 1.4.

Here $p=2, d=1, e=2$, and ζ is a root of unity of order 3 over $\mathbb{Q}_2$. The map π is reduction modulo 2. We claim that the polynomial $h(x_0,x_1)=1+x_0x_1-x_0^3-x_1^3$ has the property that for any $r\in\mathbb{Z}_{2^\infty}[\zeta]$ we have

$$h(r,\sigma(r)) \equiv \begin{cases} 1 \pmod 4, & \text{if } r\equiv 0 \pmod 2 \\ 0 \pmod 4, & \text{otherwise.}\end{cases}$$

That is, $h(r,\sigma(r))\equiv \mathrm{zer}(\pi(r))\,(\mathrm{mod}\,4)$. We verify this. It suffices to evaluate the polynomial on a set of representatives modulo 4 in $\mathbb{Z}_{2^\infty}[\zeta]$, for example, on the elements $u+v\zeta$ with $0\le u,v<4$. If we set $r=u+v\zeta$, then $\sigma(r)=u+v\zeta^2$. Since the minimal polynomial of ζ is x^2+x+1, we obtain

$$h(r,\sigma(r))=1-uv+u^2+v^2+3uv(u+v)-2(u^3+v^3).$$

If u and v are both even, then clearly $h(r,\sigma(r))\equiv 1\,(\mathrm{mod}\,4)$. If u and v are both odd, then $h(r,\sigma(r))\equiv(1-u)(v-1)\equiv 0\,(\mathrm{mod}\,4)$. If u is odd and v is even, then $h(r,\sigma(r))\equiv(1-u)(v+2)\equiv 0\,(\mathrm{mod}\,4)$. If u is even and v is odd, then $h(r,\sigma(r))\equiv 0\,(\mathrm{mod}\,4)$ in the same manner. See Example 4.11 for an account of how this polynomial was constructed.

Let f be any codeword of C; note that $\tilde{f}_{1_A}=0$ since 1_A is not in the support of the Fourier transform of C. Then Theorem 3.1 tells us that

$$\mathrm{zer}(f) \equiv 15 + 15 \sum_{\mu\in\mathbb{N}[E]} \mu! h_\mu \sum_{\lambda\in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod 4. \quad (9)$$

Now $E=\{0,1\}$, so that $\mathbb{N}[E]=\mathbb{N}[\{0,1\}]$ is the set of all multisets of zeroes and ones. Since $h(x0,x1)=1+x_0x_1+3x_0^3+3x_1^3$, the only μ such that $h_\mu\neq 0$ are $\emptyset$, the set $\{0,1\}$ (also denoted $1[0]+1[1]$), the multiset with three instances of the element zero (which we denote $3[0]$), and the multiset $3[1]$. Note

that all these multisets are Delsarte–McEliece (see Section II-D for the definition of a D-M multiset).

For each such multiset $\mu \in \mathbb{N}[E]$, the set B_μ consists of those multisets $\lambda \in \mathbb{N}[S \times E]$ that are nontrivial, unity-product, and have $\exp(\lambda) = \mu$. The reader should consult Section II-D to be familiar with these conditions. We are concerned with B_μ only when μ is a D-M multiset. In this case, we can think of B_μ in terms of the set Λ' defined in Section II-D: B_μ is the set of $\lambda \in \Lambda'$ with $\exp(\lambda) = \mu$. From Example 2.7, we know that the minimum cardinality of elements of Λ' is 4. Thus, no $\lambda \in \Lambda'$ can have $\exp(\lambda) = \mu$ for $\mu = \emptyset, \{0,1\}, 3[0]$, or $3[1]$. So the double sum in (9) is empty, and so $\mathrm{zer}(f) \equiv -1 \pmod 4$. From Example 1.4, we know that this is precisely what the Delsarte–McEliece theorem predicts. In fact, it is not hard to show that any nonzero word in this code has three zeroes. □

For examples of the application of this theorem to a $\mathbb{Z}_4$-code see Examples 3.2 and 3.3 in [10]. Now we work with a code over a Galois ring which is neither a finite field nor an integer residue ring.

Example 3.3: Let A be the cyclic group of order 1023 generated by an element a, and let C be the code in $\mathrm{GR}(4,2)[A]$ whose Fourier transform is supported on the set $S = \{a, a^4, a^{16}, a^{64}, a^{256}\}$. In a more conventional presentation of cyclic codes, this is the code in $\mathrm{GR}(4,2)[x]/(x^{1023}-1)$ whose check polynomial is one of the quintic irreducible factors of cyclotomic polynomial $\Phi_{1023}(x)$ in $\mathrm{GR}(4,2)[x]$.

Here $d = 2, e = 2$, and ζ is a root of unity of order 3 over $\mathbb{Q}_2$. The map π is reduction modulo 4. We claim that the polynomial

$$\begin{aligned} h(x_0,x_1) = 1 &+ 2x_0x_1 - \frac{11+3\zeta}{8}x_0^3 + \frac{-8+3\zeta}{8}x_1^3 \\ &- \frac{25}{16}x_0^2x_1^2 + \frac{28-51\zeta}{32}x_0^4x_1 + \frac{-49+51\zeta}{32}x_0x_1^4 \\ &+ \frac{13}{16}x_0^6 - \frac{3}{2}x_0^3x_1^3 + \frac{13}{16}x_1^6 + \frac{17-9\zeta}{16}x_0^5x_1^2 \\ &+ \frac{26+9\zeta}{16}x_0^2x_1^5 + 2x_0^7x_1 + \frac{7}{16}x_0^4x_1^4 + 2x_0x_1^7 \\ &- \frac{9+49\zeta}{32}x_0^9 + \frac{8+5\zeta}{8}x_0^6x_1^3 \\ &+ \frac{3-5\zeta}{8}x_0^3x_1^6 + \frac{40+49\zeta}{32}x_1^9 \end{aligned}$$

has the property that for any $r \in \mathbb{Z}_{2^\infty}[\zeta]$, we have

$$h(r,\sigma(r)) \equiv \begin{cases} 1 \pmod 4, & \text{if } r \equiv 0 \pmod 4 \\ 0 \pmod 4, & \text{otherwise.} \end{cases}$$

That is, $h(r,\sigma(r)) \equiv \mathrm{zer}(\pi(r)) \pmod 4$. We do not verify this here, but it suffices to check the values for $r = u + v\zeta$ with $0 \le u, v < 128$. For if $r \equiv r' \pmod{128}$, then $h(r,\sigma(r)) \equiv h(r',\sigma(r')) \pmod 4$ since the denominators of the coefficients of $h(x_0,x_1)$ are divisors of 32. Such a calculation can be done with standard mathematical software [38]. See Example 4.12 for an account of how this polynomial was constructed.

Let f be any codeword of C; note that $\tilde{f}_{1_A} = 0$ since 1_A is not in the support of the Fourier transform of C. Then Theorem 3.1 tells us that

$$\mathrm{zer}(f) \equiv 1023 + 1023 \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod 4. \quad (10)$$

Now $E = \{0,1\}$, so that $\mathbb{N}[E] = \mathbb{N}[\{0,1\}]$ is the set of all multisets of zeroes and ones. One can check that $h(x_0,x_1)$ has total degree 9, and the coefficient h_μ of the monomial $\boldsymbol{x}^\mu$ in $h(\boldsymbol{x})$ is nonzero only if μ is a D-M multiset in $\mathbb{N}[E]$. Thus, we need only consider μ with $|\mu| \le 9$ and μ Delsarte–McEliece.

As in the previous example, for any such μ, the set B_μ consists of $\lambda \in \Lambda'$ such that $\exp(\lambda) = \mu$, where Λ' and exp are as defined in Section II-D. From Example 2.7, we know that Λ' contains no multiset with fewer than 10 elements, thus, $\exp(\lambda)$ cannot be equal to any μ such that $h_\mu \neq 0$. So the double sum in (10) is empty, and so $\mathrm{zer}(f) \equiv -1 \pmod 4$. Equivalently, all Hamming weights are divisible by 4. In Example 1.7, we learn that this is precisely what Theorem 1.6 predicts about 2-divisibility of Hamming weights in this code. In fact, direct computations with mathematical software [38] can be done to show that the weight enumerator of this code is $1 + 1023x^{768} + 556512x^{948} + 491040x^{972}$. □

The two examples above show that if the parameter ℓ of the code exceeds the degree of a polynomial $h(\boldsymbol{x})$ which estimates zero count modulo p^m, then one instantly knows that $\mathrm{zer}(f) \equiv |A|\mathrm{zer}(\tilde{f}_{1_A}) \pmod{p^m}$ without any difficult calculations. This is the usual way in which Theorem 3.1 is applied. The following example shows a situation in which an actual calculation with $h(\boldsymbol{x})$ yields an interesting weight congruence which goes beyond the predictions of p-divisibility contained in Theorem 1.6.

Example 3.4: Let A be the cyclic group of order 255 generated by an element a and let C be the code in $\mathrm{GR}(4,2)[A]$ whose Fourier transform is supported on the set $S = \{a, a^4, a^{16}, a^{64}\}$. In a more conventional presentation of cyclic codes, this is the code in $\mathrm{GR}(4,2)[x]/(x^{255}-1)$, whose check polynomial is one of the quartic irreducible factors of cyclotomic polynomial $\Phi_{255}(x)$ in $\mathrm{GR}(4,2)[x]$.

Here $d = 2, e = 2$, and ζ is a root of unity of order 3 over $\mathbb{Q}_2$. The map π is reduction modulo 4. We use the same polynomial $h(x0,x1)$ which was introduced in the previous example and which has the property that $h(r,\sigma(r)) \equiv \mathrm{zer}(\pi(r)) \pmod 4$ for any $r \in \mathbb{Z}_{2^\infty}[\zeta]$.

Let f be any codeword of C; note that $\tilde{f}_{1_A} = 0$ since 1_A is not in the support of the Fourier transform of C. Then Theorem 3.1 tells us that

$$\mathrm{zer}(f) \equiv 255 + 255 \sum_{\mu \in \mathbb{N}[E]} \mu! h_\mu \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod 4. \quad (11)$$

As in the previous example, $E = \{0,1\}$, so that $\mathbb{N}[E] = \mathbb{N}[\{0,1\}]$, and for the purposes of computing the sum in (11), we need only consider μ with $|\mu| \le 9$ and μ Delsarte–McEliece. Again, for each of these relevant μ, the set B_μ consists of $\lambda \in \Lambda'$ such that $\exp(\lambda) = \mu$, where Λ' and exp are as defined in Section II-D. From Example 2.7, we know that Λ' contains no multisets of cardinality less than 8, and that there is a unique multiset of cardinality 8, namely,

$$\lambda_{\min} = (a,0) + (a,1) + \cdots + (a^{64},0) + (a^{64},1).$$

Thus, in the notation of Sections II-D and the Introduction, we have $\ell = 8$ for this code. So Theorem 1.6 predicts that $\mathrm{zer}(f) \equiv -1 \pmod 2$ in this case. In fact, a detailed calculation based

on Theorem 3.1 with our polynomial $h(x_0, x_1)$ will show that $\mathrm{zer}(f) \equiv -1 \pmod 4$ for all $f \in C$.

To resume, $\lambda_{\min}$ is the unique minimal-cardinality multiset in Λ'. From Example 2.7, we also know that Λ' contains precisely eight multisets of cardinality 9, which have the form

$$\kappa_j = \lambda_{\min} - (a^{4^j}, 1) + 2(a^{4^j}, 0), \qquad \text{for } j = 0, 1, 2, 3$$

or

$$\nu_j = \lambda_{\min} - (a^{4^j}, 0) + 2(a^{4^{j+3}}, 1), \qquad \text{for } j = 0, 1, 2, 3.$$

Note that all these multisets are Delsarte–McEliece, with $\exp(\lambda_{\min}) = 4[0] + 4[1], \exp(\kappa_j) = 6[0] + 3[1]$, and $\exp(\nu_j) = 3[0] + 6[1]$. These are the only relevant μ in the first sum in (11). Note that if $\mu = \exp(\lambda_{\min}) = 4[0] + 4[1]$, then $h_\mu = 7/16, \mu! = 4!4! = 576$ and $\lambda_{\min}! = 1$, so that $(\mu! h_\mu)/\lambda_{\min}! = 252$. Computing the rest of the coefficients of (11) in this fashion, we obtain

$$\mathrm{zer}(f) \equiv 255 + 255 \cdot 252 \tilde{F}_{\lambda_{\min}} + 255(720 + 450\zeta) \sum_{i=0}^{3} \tilde{F}_{\kappa_i} + 255(270 - 450\zeta) \sum_{j=0}^{3} \tilde{F}_{\nu_j} \pmod 4.$$

Note that $\tilde{F}_\theta \in \mathbb{Z}_{2^\infty}[\eta]$ for any $\theta \in \mathbb{N}[S \times E]$, so we can reduce the coefficients modulo 4 to obtain

$$\mathrm{zer}(f) \equiv -1 + 2\zeta \sum_{i=0}^{3} \tilde{F}_{\kappa_i} + (2 + 2\zeta) \sum_{j=0}^{3} \tilde{F}_{\nu_j} \pmod 4.$$

Write each lifted scaled Fourier coefficient in its canonical expansion (see Section II-B) as $\tilde{F}_b = \tilde{F}_b^{(0)} + 2\tilde{F}_b^{(1)}$. Then note that $\tilde{F}_{\kappa_i} \equiv \tilde{F}_{\kappa_i}^{(0)} \pmod 2$, so that

$$\mathrm{zer}(f) \equiv -1 + 2\zeta \sum_{i=0}^{3} \tilde{F}_{\kappa_i}^{(0)} + (2 + 2\zeta) \sum_{j=0}^{3} \tilde{F}_{\nu_j}^{(0)} \pmod 4. \tag{12}$$

Note that Proposition 2.2 shows us that $\tilde{F}_{b^4} = \sigma^2(\tilde{F}_b)$ for all $b \in A$, and therefore, $\tilde{F}_{b^4}^{(0)} = \sigma^2(\tilde{F}_b^{(0)})$ as well. Furthermore, since $\tilde{F}_b^{(0)}$ is always zero or a power of η, this means that $\tilde{F}_{b^4}^{(0)} = (\tilde{F}_b^{(0)})^4$. From this it is possible to show that $\tilde{F}_{\kappa_i}^{(0)} = (\tilde{F}_a^{(0)})^{255}$ for all i and $\tilde{F}_{\nu_j}^{(0)} = (\tilde{F}_a^{(0)})^{255}$ for all j. Since $\tilde{F}_a^{(0)}$ is 0 or a power of the primitive 255th root of unity known as η, all terms of the sums in (12) are either simultaneously 0 or simultaneously 1, and so

$$\mathrm{zer}(f) \equiv -1 \pmod 4$$

which is a stronger statement than that given by Theorem 1.6 alone. Indeed, computations with mathematical software [38] show that the weight enumerator of our code C is $1 + 255x^{192} + 10200x^{228} + 48960x^{240} + 6120x^{252}$. □

These examples have shown us that in order to use Theorem 3.1, we need to furnish the polynomial $h(\boldsymbol{x})$ as described in the hypothesis, although sometimes it suffices merely to know that there exists such a polynomial of a certain (preferably low) degree. We devote the next section to constructing the polynomials we need in the case where wt is zer, the function which counts the number of zeroes appearing in the codeword.

IV. Trace-Averaged Counting Polynomials

In this section, we shall devise an adaptation of counting polynomial methods (see [8]–[10], [39]) to the problem of p-adic estimates of weights in codes over Galois rings. We make use of one fact, which has been proved in [10]; all but the last statement had been proved previously in [9], [39].

Theorem 4.1 ([10, Corollary 4.9]): For any $\delta, m \geq 1$, there exists a polynomial $h_{\delta,m}(x) \in \mathbb{Q}_p[x]$ of degree $\lceil m(p-1) + 1 \rceil p^{\delta-1} - 1$ such that for any $r \in \mathbb{Z}_{p^\infty}$

$$h_{\delta,m}(r) \equiv \begin{cases} 1 \pmod{p^m}, & \text{if } r \equiv 0 \pmod{p^\delta} \\ 0 \pmod{p^m}, & \text{otherwise.} \end{cases}$$

No polynomial of lower degree has this property. If we write

$$h_{\delta,m}(x) = \sum_{i=0}^{\deg(h_{\delta,m})} h_{\delta,m}^{(i)} x^i$$

then

$$\deg(h_{\delta,m})! h_{\delta,m}^{(\deg(h_{\delta,m}))} \equiv (-p)^{m-1} \pmod{p^m}.$$

Furthermore, we can always choose $h_{\delta,m}(x)$ so that $h_{\delta,m}^{(i)} = 0$ when $p - 1 \nmid i$.

The theorem says that the polynomial approximates modulo p^m the characteristic function of the ideal $p^\delta \mathbb{Z}_{p^\infty}$ in $\mathbb{Z}_{p^\infty}$.

Example 4.2: We claim that the polynomial $h(x) = 1 + 2x + 3x^2 + 2x^3$ has the property that for any $r \in \mathbb{Z}_{2^\infty}$

$$h(r) \equiv \begin{cases} 1 \pmod 8, & \text{if } r \equiv 0 \pmod 2 \\ 0 \pmod 8, & \text{otherwise.} \end{cases}$$

To verify this, it suffices to check that this congruence holds for $r = 0, 1, \ldots, 7$. Note that Theorem 4.1 tells us that no lower degree polynomial satisfies the congruence, and furthermore, that any cubic polynomial $g(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3$ satisfying the congruence has $6g_3 \equiv 4 \pmod 8$, as is the case for $h(x)$. □

The construction of polynomials such as these is described in detail in [10, Section IV]. See especially Example 4.10.

Theorem 4.1 was used to prove analogues of McEliece's theorem for Abelian codes over $\mathbb{Z}_{p^d}$ in [8]–[10] by lifting codewords from alphabet $\mathbb{Z}_{p^d}$ to alphabet $\mathbb{Z}_{p^\infty}$. For if $R \in \mathbb{Z}_{p^\infty}$ is a lift of a symbol $r \in \mathbb{Z}_{p^d}$, then $h_{d,m}(R) \equiv \mathrm{zer}(r) \pmod{p^m}$; equivalently, $h_{d,m}$ approximates $\mathrm{zer} \circ \pi$ modulo p^m. Here we can mimic these efforts by lifting our codes from alphabet $\mathrm{GR}(p^d, e)$ to alphabet $\mathbb{Z}_{p^\infty}[\zeta]$. Unfortunately, we typically cannot use the polynomials of Theorem 4.1, which approximate $\mathrm{zer} \circ \pi$ on $\mathbb{Z}_{p^\infty}$, to approximate $\mathrm{zer} \circ \pi$ on $\mathbb{Z}_{p^\infty}[\zeta]$.

Example 4.3: Consider the polynomial $h(x) = 1 + 2x + 3x^2 + 2x$ from Example 4.2, which approximates $\mathrm{zer} \circ \pi$ modulo 8 on $\mathbb{Z}_{2^\infty}$, where π is reduction modulo 2 and zer is the zero-count weight function on $\mathrm{GF}(2) = \mathrm{GR}(2, 1)$. Now suppose that we want to approximate zero counts in codes over $\mathrm{GF}(4) = \mathrm{GR}(2, 2)$. Then we extend zer to be the zero-count weight function on $\mathrm{GF}(4)$ and we extend π to be reduction modulo 2 on $\mathbb{Z}_{2^\infty}[\zeta_3]$, where ζ_3 is a primitive third root of unity over $\mathbb{Z}_{2^\infty}$. Thus, $\mathrm{GF}(4)$ is the image of $\mathbb{Z}_{2^\infty}[\zeta_3]$ under π. Unfortunately, although we saw in Example 4.2 that $h(r) \equiv \mathrm{zer}(\pi(r)) \pmod 8$ for all $r \in \mathbb{Z}_{2^\infty}$, it is not the case that $h(r) \equiv \mathrm{zer}(\pi(r)) \pmod 8$

for all $r \in \mathbb{Z}_{2^\infty}[\zeta_3]$. Indeed, h does not even approximate $\mathrm{zer} \circ \pi$ modulo 2 on $\mathbb{Z}_{2^\infty}[\zeta_3]$, because $h(\zeta_3) = -\zeta_3 \not\equiv 0 \pmod 2$. (To perform the computation, use the minimal polynomial $\zeta_3^2 + \zeta_3 + 1 = 0$.) □

Thus, the polynomials of Theorem 4.1 developed in [39], [9], [10] do not provide p-adic approximations of zero count or Hamming weight for use with Galois rings that are not quotients of $\mathbb{Z}$. The modification of the polynomials of Theorem 4.1 to overcome this obstacle is the subject of this section.

A. Trace and p-adic Valuation

The essential insight of this paper is to use the trace to map the elements of $\mathbb{Z}_{p^\infty}[\zeta]$ to $\mathbb{Z}_{p^\infty}$, so that the polynomial $h_{d,m}(x)$ of Theorem 4.1 may then be applied. This is not straightforward, since there can be elements of $\mathbb{Z}_{p^\infty}[\zeta]$ which themselves are nonzero modulo p^d but whose traces vanish modulo p^d. That is, if we take $h_{d,m}(x)$ from Theorem 4.1 and simply consider the function

$$H(x) = h_{d,m}(\mathrm{Tr}(x))$$

then $H(s)$ can equal 1 modulo p^m even in cases where $s \in \mathbb{Z}_{p^\infty}[\zeta]$ does not vanish modulo p^d. So the essential problem is that trace does not preserve p-adic valuation. Trace does respect p-adic valuation in a weaker sense, namely, it never decreases p-adic valuation, because trace is $\mathbb{Z}_{p^\infty}$-linear and so

$$\mathrm{Tr}(p^j a) = p^j \mathrm{Tr}(a).$$

The key idea is to consider

$$H'(x) = \sum_{r \in R} h_{d,m}(\mathrm{Tr}(rx)),$$

where R is a set of representatives of equivalence classes modulo p^d in $\mathbb{Z}_{p^\infty}[\zeta]^\times$. Then, as r ranges over R, the quantity rx will range over a family of elements which are uniformly distributed among those equivalence classes modulo p^d which have the same p-adic valuation as x. Recall that trace commutes with π, so that the distribution of values of $\mathrm{Tr}(rx)$ modulo p^d will depend only upon $v_p(x)$. We guess that $\mathrm{Tr}(rx)$ will vanish modulo p^d for more values of $r \in R$ as $v_p(x)$ increases. Thus, $H'(x)$ will depend only upon $v_p(x)$ and we expect it to vary somewhat as $v_p(x)$ varies.

In order to perform this procedure, which we call *trace-averaging*, we need to make precise the notions in the previous paragraph. For now we shall find it convenient to work with trace on the ring $\mathrm{GR}(p^\delta, e)$ with δ some positive integer. We need a notion of p-adic valuation in this finite ring. Quite naturally, for $a \in \mathrm{GR}(p^\delta, e)$ with $a \neq 0$, we define

$$v_p(a) = \max\{n \in \{0, 1, \ldots, d-1\} \colon p^n \mid a\}$$

and we set $v_p(0) = \infty$. In order to perform the trace-averaging procedure sketched out in the previous paragraph, we must compute what fraction of the elements in $\mathrm{GR}(p^\delta, e)$ with a given valuation are taken by trace to 0. So for $j \in \{0, 1, \ldots, \delta - 1, \infty\}$, we define

$$\theta_j^\delta = \frac{|\{a \in \mathrm{GR}(p^\delta, e) \colon v_p(a) = j, \mathrm{Tr}(a) = 0\}|}{|\{a \in \mathrm{GR}(p^\delta, e) : v_p(a) = j\}|} \tag{13}$$

and our goal will be to compute these values. The answer is given in Proposition 4.5 later, and the rest of this section is devoted to proving it.

Recall the definition of trace; for $a \in \mathrm{GR}(p^\delta, e)$, we have

$$\mathrm{Tr}(a) = \sum_{i=0}^{e-1} \sigma^i(a).$$

Note that trace is a $\mathbb{Z}_{p^\delta}$-linear map from $\mathrm{GR}(p^\delta, e)$ to $\mathrm{GR}(p^\delta, 1) = \mathbb{Z}_{p^\delta}$. Trace is also surjective. This can be demonstrated by recalling from elementary field theory that the trace from $\mathrm{GF}(q) = \mathrm{GR}(p, e)$ to $\mathrm{GF}(p) = \mathrm{GR}(p, 1)$ is surjective and by employing the commutativity of trace with reduction modulo p. Together, these facts show us that there is some element in $\mathrm{GR}(p^\delta, e)$ whose trace in $\mathbb{Z}_{p^\delta}$ is 1 modulo p. Then $\mathbb{Z}_{p^\delta}$-linearity of trace implies that the image of trace is all of $\mathbb{Z}_{p^\delta}$. Our first step in proving Proposition 4.5 uses the surjectivity of trace.

Lemma 4.4: Given $a \in \mathrm{GR}(p^\delta, e)$, there exists $b \in \mathrm{GR}(p^\delta, e)$ with $a \equiv b \pmod p$ and with

$$\mathrm{Tr}(b) \in \{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}_{p^\delta}.$$

Proof: Pick $\alpha \in \{0, 1, \ldots, p-1\}$ such that $\mathrm{Tr}(a) \equiv \alpha \pmod p$. Then choose $\gamma \in \mathbb{Z}_{p^\delta}$ so that $p\gamma = \mathrm{Tr}(a) - \alpha$. Choose $c \in \mathrm{GR}(p^\delta, e)$ with $\mathrm{Tr}(c) = \gamma$ (using surjectivity). Then set $b = a - pc$. Then

$$\mathrm{Tr}(b) = \mathrm{Tr}(a) - p\mathrm{Tr}(c) = \mathrm{Tr}(a) - p\gamma = \alpha. \qquad \square$$

This lemma enables us to pick a set U of representatives of the equivalence classes modulo p in $\mathrm{GR}(p^\delta, e)$ with the special property that for any $u \in U$, we have $\mathrm{Tr}(u) \in \{0, 1, \ldots, p-1\}$. We insist that 0 lie in U, which is acceptable since 0 has trace 0. We define $V = \{u \in U \colon \mathrm{Tr}(u) = 0\}$ and note that $0 \in V$ since $\mathrm{Tr}(0) = 0$. The cardinality of U is q, and we would like to know the cardinality of V. By the commutativity of the trace with reduction modulo p, this is the size of the kernel of the trace map from $\mathrm{GF}(q)$ to $\mathrm{GF}(p)$. Thus, $|V| = q/p$. Since U is a class of representatives modulo p in $\mathrm{GR}(p^\delta, e)$, every element of $\mathrm{GR}(p^\delta, e)$ can be written uniquely as $\sum_{i=0}^{\delta-1} u_i p^i$ with each $u_i \in U$. Now we can prove our proposition.

Proposition 4.5: For $0 \leq j < \delta$, we have

$$|\{a \in \mathrm{GR}(p^\delta, e) \colon v_p(a) = j\}| = (q-1)q^{\delta-1-j}$$

and

$$|\{a \in \mathrm{GR}(p^\delta, e) : v_p(a) = j, \mathrm{Tr}(a) = 0\}| = \left(\frac{q}{p} - 1\right)\left(\frac{q}{p}\right)^{\delta-1-j}$$

so that

$$\theta_j^\delta = \frac{q-p}{q-1} p^{j-\delta}$$

where θ_j^δ is defined in (13) above. We also have $\theta_\infty^\delta = 1$.

Proof: Since 0 is the only element of infinite valuation and $\mathrm{Tr}(0) = 0$, we have $\theta_\infty^\delta = 1$. So henceforth suppose that $0 \leq j < \delta$, and we shall calculate θ_j^δ. We now use the fact that we can represent elements of $\mathrm{GR}(p^\delta, e)$ using the set U as noted above. The elements $a \in \mathrm{GR}(p^\delta, e)$ with valuation j are just those which are represented as $a = \sum_{i=0}^{\delta-1} u_i p^i$ where $u_i = 0$

for $i < j, u_j \in U\backslash\{0\}$, and $u_i \in U$ for $i > j$. Since $|U| = q$, we obtain the desired formula for $|\{a \in \mathrm{GR}(p^\delta, e)\colon v_p(a) = j\}|$. For our element $a \in \mathrm{GR}(p^\delta, e)$ represented as $\sum_{i=0}^{\delta-1} u_i p^i$ with $u_i \in U$, we have

$$\mathrm{Tr}(a) = \sum_{i=0}^{\delta-1} \mathrm{Tr}(u_i) p^i.$$

We know that $\mathrm{Tr}(u) \in \{0, 1, \ldots, p-1\}$ for all $u \in U$, so we know that $\mathrm{Tr}(a) = 0$ if and only if $\mathrm{Tr}(u_i) = 0$ for all i, i.e., if and only if $u_i \in V$ for all i. Thus, the elements $a \in \mathrm{GR}(p^\delta, e)$ with valuation j and trace 0 are those with $u_i = 0$ for $i < j, u_j \in V \setminus \{0\}$, and $u_i \in V$ for $i > j$. Recall that $|V| = q/p$ so that we obtain the desired formula for

$$|\{a \in \mathrm{GR}(p^\delta, e) : v_p(a) = j, \mathrm{Tr}(a) = 0\}|.$$

Now we can calculate θ_j^δ by dividing the cardinalities we have calculated. □

This proposition makes precise the intuition that although trace does not preserve the p-adic valuation of elements in $\mathrm{GR}(p^\delta, e)$, nevertheless the fraction of elements of a given valuation j which lie in the kernel of trace does increase as j increases.

B. Trace-Averaging Functions

Now we are ready to apply the trace-averaging procedure to functions. It will simplify matters if we first observe the effects of trace-averaging on the exact characteristic function of the ideal $p^\delta \mathbb{Z}_{p^\infty}$ in $\mathbb{Z}_{p^\infty}$ (which only takes values 0 and 1) rather than on the polynomial approximations of this characteristic function furnished by Theorem 4.1.

Lemma 4.6: For $\delta \geq 1$, let $F_\delta\colon \mathbb{Z}_{p^\infty} \to \mathbb{Z}$ be the function defined by

$$F_\delta(s) = \begin{cases} 1, & \text{if } s \equiv 0 \pmod{p^\delta} \\ 0, & \text{otherwise.} \end{cases}$$

Let R be any set of representatives of the equivalence classes modulo p^δ in $\mathbb{Z}_{p^\infty}[\zeta]^\times$. Let $\mathfrak{F}_\delta\colon \mathbb{Z}_{p^\infty}[\zeta] \to \mathbb{Z}$ be defined by

$$\mathfrak{F}_\delta(s) = \sum_{r \in R} F_\delta(\mathrm{Tr}(rs)).$$

Then

$$\mathfrak{F}_\delta(s) = \begin{cases} p^{v_p(s)} \left(\frac{q}{p} - 1\right) \left(\frac{q}{p}\right)^{\delta-1}, & \text{if } v_p(s) < \delta \\ (q-1)q^{\delta-1}, & \text{if } v_p(s) \geq \delta. \end{cases}$$

Thus, $\mathfrak{F}_\delta$ is independent of the choice of representatives in R.

Proof: Let $s \in \mathbb{Z}_{p^\infty}[\zeta]$ with $j = v_p(s)$. First, let us suppose that $j \geq \delta$. Then, for any $r \in R$, we have $v_p(rs) = j \geq \delta$ and so $v_p(\mathrm{Tr}(rs)) \geq \delta$. Thus, $F_\delta(\mathrm{Tr}(rs)) = 1$ for all $r \in R$, so $\mathfrak{F}_\delta(s) = |R|$, which equals $(q-1)q^{\delta-1}$ by Proposition 4.5.

Now let us suppose that $v_p(s) = j < \delta$. Then as r ranges over R, the quantity rs takes values in $\mathbb{Z}_{p^\infty}[\zeta]$ with valuation equal to j. Let $\psi\colon \mathbb{Z}_{p^\infty}[\zeta] \to \mathrm{GR}(p^\delta, e)$ be the quotient map modulo p^δ. Then $\psi(r)$ ranges over the set of units in $\mathrm{GR}(p^\delta, e)$, taking each value once, and so $\psi(rs)$ ranges over $\{a \in \mathrm{GR}(p^\delta, e)\colon v_p(a) = j\}$, taking each value an equal number of times. Thus, $\psi(\mathrm{Tr}(rs)) = \mathrm{Tr}(\psi(rs))$ takes the value 0 precisely $|R|\theta_j^\delta$ times, where θ_j^δ is as defined in (13). Proposition 4.5 tells us that $|R| = (q-1)q^{\delta-1}$ and $\theta_j^\delta = \frac{q-p}{q-1} p^{j-\delta}$, which completes the proof. □

This lemma furnishes us with a function which is sensitive only to the p-adic valuation of its argument and which takes different values for different p-adic valuations. Now we shall make linear combinations of $\mathfrak{F}_\delta$ for $1 \leq \delta \leq d$ to obtain the characteristic function of the ideal generated by p^d in $\mathbb{Z}_{p^\infty}[\zeta]$.

Lemma 4.7: With $\mathfrak{F}_\delta$ as defined in Lemma 4.6, let

$$\mathfrak{F}(x) = \frac{p}{(p-1)q^d} \left[\mathfrak{F}_d(x) - \left(\frac{q}{p} - 1\right) \left(1 + \sum_{i=1}^{d-1} \mathfrak{F}_i(x)\right) \right].$$

Then

$$\mathfrak{F}(s) = \begin{cases} 0, & \text{if } v_p(s) < d \\ 1, & \text{if } v_p(s) \geq d \end{cases}$$

for all $s \in \mathbb{Z}_{p^\infty}[\zeta]$.

Proof: For an element s of a given valuation, plug in the values of $\mathfrak{F}_i(s)$ given in Lemma 4.6 and perform a routine calculation involving telescoping sums. □

We could make a polynomial approximation to the function $\mathfrak{F}$ defined in Lemma 4.7 above by replacing the $\mathfrak{F}_i$ which appear in its definition with trace-averaged polynomials. For $\mathfrak{F}_i$, as defined in Lemma 4.6, is just a trace-averaged version of F_i, which is approximated by the polynomials in Theorem 4.1. Suppose that we proceed in this way and desire to construct a polynomial which approximates $\mathfrak{F}$ modulo p^m. Looking at the definition of $\mathfrak{F}$, we would want to have a polynomial which approximates $\frac{p}{(p-1)q^d}\mathfrak{F}_d$ modulo p^m, or equivalently, a polynomial which approximates $\mathfrak{F}_d$ modulo p^{m-1+de}. Thus, we should trace-average the polynomial $h_{d,m-1+de}(x)$ of Theorem 4.1, which approximates F_d modulo p^{m-1+de}. All the other F_i would also need to be approximated modulo p^{m-1+de}, since all the coefficients of the functions $\mathfrak{F}_i$ in the expression for $\mathfrak{F}$ have the same p-adic valuation.

If we trace-average more carefully, we can reduce the size of the set R of units over which we sum and then we shall not need to divide by so many powers of p to get our trace-averaged function. This will allow us to use less precise (and hence lower degree) polynomial approximations. We proceed to make a more selective set of units. For $\delta \geq 1$, let $\mathrm{GR}(p^\delta, e)^\times$ denote the multiplicative group of units in $\mathrm{GR}(p^\delta, e)$ and let $\mathrm{GR}(p^\delta, e)^{\equiv 1}$ denote the subgroup of $\mathrm{GR}(p^\delta, e)^\times$ consisting of elements congruent to 1 modulo p. Note that $\mathrm{GR}(p^\delta, 1)^{\equiv 1} = \mathbb{Z}_{p^\delta}^{\equiv 1}$ is a subgroup of $\mathrm{GR}(p^\delta, e)^{\equiv 1}$. Let $\mathrm{GR}(p^\delta, e)^\sharp$ be a set of representatives of equivalence classes in the quotient of $\mathrm{GR}(p^\delta, e)^{\equiv 1}$ modulo $\mathbb{Z}_{p^\delta}^{\equiv 1}$. If $\delta = 1$, then $\mathrm{GR}(p^\delta, e)^{\equiv 1} = \mathrm{GF}(q)^{\equiv 1} = \{1\}$ and $\mathbb{Z}_{p^\delta}^{\equiv 1} = \mathrm{GF}(p)^{\equiv 1} = \{1\}$, and so $\mathrm{GR}(p^\delta, e)^\sharp = \{1\}$. If $e = 1$, then $\mathrm{GR}(p^\delta, e)^{\equiv 1} = \mathrm{GR}(p^\delta, 1)^{\equiv 1} = \mathbb{Z}_{p^\delta}^{\equiv 1}$, and we shall insist that $\mathrm{GR}(p^\delta, e)^\sharp = \{1\}$ in this case. Now each element in $\mathrm{GR}(p^\delta, e)^{\equiv 1}$ can be represented uniquely as vw where $v \in \mathrm{GR}(p^\delta, e)^\sharp$ and $w \in \mathbb{Z}_{p^\delta}^{\equiv 1}$. An element of $\mathrm{GR}(p^\delta, e)$ is a unit if and only if it is nonzero modulo p, and the powers of $\pi(\zeta)$ form a set of representatives of the nonzero congruence classes modulo p. Thus, each element in $\mathrm{GR}(p^\delta, e)^\times$ can be represented

uniquely as $\pi(\zeta)^i vw$ where $0 \le i < q-1, v \in \mathrm{GR}\,(p^\delta, e)^\sharp$, and $w \in \mathbb{Z}_{p^\delta}^{\equiv 1}$.

Now we lift the sets we just defined to $\mathbb{Z}_{p^\infty}[\zeta]^\times$ *via* the standard lift τ, which takes units in $\mathrm{GR}\,(p^\delta, e)$ to units in $\mathbb{Z}_{p^\infty}[\zeta]$. Let $V_\delta = \tau(\mathrm{GR}\,(p^\delta, e)^\sharp)$ and $W_\delta = \tau(\mathbb{Z}_{p^\delta}^{\equiv 1})$. Note that the standard lift lifts elements of $\mathbb{Z}_{p^\delta} = \mathrm{GR}\,(p^\delta, 1)$ into $\mathbb{Z}_{p^\infty}$ and so $W_\delta \subseteq \mathbb{Z}_{p^\infty}^\times$. Furthermore, note that τ lifts $1 \in \mathrm{GR}\,(p^\delta, e)$ to $1 \in \mathbb{Z}_{p^\infty}[\zeta]$, so that we have $V_\delta = \{1\}$ when $d = 1$ or $e = 1$. Let

$$U_\delta = \{\zeta^i vw \colon 0 \le i < q-1, v \in V_\delta, w \in W_\delta\}.$$

Then U_δ is a set of representatives modulo p^δ for $\mathbb{Z}_{p^\infty}[\zeta]^\times$, i.e., U_δ is a lift (perhaps not the standard lift) of $\mathrm{GR}\,(p^\delta, e)^\times$. Now we shall trace-average more efficiently in the following lemma:

Lemma 4.8: Let F_δ and $\mathfrak{F}_\delta$ be as defined in Lemma 4.6. Let V_δ be the set defined in the text above. Let $\mathfrak{G}_\delta \colon \mathbb{Z}_{p^\infty}[\zeta] \to \mathbb{Z}$ be defined by

$$\mathfrak{G}_\delta(s) = \sum_{i=0}^{q-2} \sum_{v \in V_\delta} F_\delta(\mathrm{Tr}(\zeta^i vs)).$$

Then $\mathfrak{G}_\delta = p^{1-\delta}\mathfrak{F}_\delta$.

Proof: Let W_δ and U_δ be the sets defined in the text preceding this lemma. Note that for any $s \in \mathbb{Z}_{p^\infty}[\zeta]$ and $w \in W_\delta$

$$\begin{aligned}\mathfrak{G}_\delta(ws) &= \sum_{i=0}^{q-2} \sum_{v \in V_\delta} F_\delta(\mathrm{Tr}(\zeta^i vws)) \\ &= \sum_{i=0}^{q-2} \sum_{v \in V_\delta} F_\delta(w\mathrm{Tr}(\zeta^i vs)) \\ &= \sum_{i=0}^{q-2} \sum_{v \in V_\delta} F_\delta(\mathrm{Tr}(\zeta^i vs)) \\ &= \mathfrak{G}_\delta(s)\end{aligned}$$

where the second equality uses the $\mathbb{Z}_{p^\infty}$-linearity of trace along with the fact that $w \in W_\delta \subseteq \mathbb{Z}_{p^\infty}^\times$, and where the third equality uses the fact that w is a unit in $\mathbb{Z}_{p^\infty}$, and so the p-adic valuation of $w\mathrm{Tr}(\zeta^i vs)$ is the same as that of $\mathrm{Tr}(\zeta^i vs)$. Thus,

$$\sum_{w \in W_\delta} \mathfrak{G}_\delta(ws) = |W_\delta| \mathfrak{G}_\delta(s).$$

On the other hand

$$\begin{aligned}\sum_{w \in W_\delta} \mathfrak{G}_\delta(ws) &= \sum_{w \in W_\delta} \sum_{i=0}^{q-2} \sum_{v \in V_\delta} F(\mathrm{Tr}(\zeta^i vws)) \\ &= \sum_{u \in U_\delta} F(\mathrm{Tr}(us)) \\ &= \mathfrak{F}_\delta(s)\end{aligned}$$

where the final equality uses U_δ in the role of R in Lemma 4.6. Thus, we conclude that

$$\mathfrak{G}_\delta(s) = \frac{1}{|W_\delta|}\mathfrak{F}_\delta(s).$$

Observing that $|W_\delta| = |\mathbb{Z}_{p^\delta}^{\equiv 1}| = p^{\delta-1}$, we finish the proof. □

Now we can obtain a new version of the result in Lemma 4.7 by using these new trace-averaged functions $\mathfrak{G}_\delta$ instead of the functions $\mathfrak{F}_\delta$.

Lemma 4.9: With $\mathfrak{G}_\delta$ as defined in Lemma 4.8, define $\mathfrak{G}(x)$ to be

$$\frac{p^d}{(p-1)q^d}\left[\mathfrak{G}_d(x) - \left(\frac{q}{p} - 1\right)\left(p^{1-d} + \sum_{i=1}^{d-1} p^{i-d}\mathfrak{G}_i(x)\right)\right].$$

Then

$$\mathfrak{G}(s) = \begin{cases} 0, & \text{if } v_p(s) < d \\ 1, & \text{if } v_p(s) \ge d \end{cases}$$

for all $s \in \mathbb{Z}_{p^\infty}[\zeta]$.

Proof: Use Lemma 4.8 to substitute the functions $\mathfrak{F}_i$ for $\mathfrak{G}_i$, and then Lemma 4.7 completes the proof. □

This lemma serves as the model for the trace-averaging techniques we shall apply to polynomials. In the next subsection, we shall replace the $\mathfrak{G}_\delta$ by trace-averaged polynomial approximations to obtain the polynomials we need to prove Theorem 1.6 from Theorem 3.1.

C. Trace-Averaging Polynomials

Now we shall apply our trace-averaging techniques to polynomials, especially those furnished by Theorem 4.1. We shall continue to use the sets V_δ for $\delta \ge 1$ as defined in Section IV-B in the text preceding Lemma 4.8. Given any polynomial $h(x) \in \mathbb{Q}_p[x]$ and $\delta \ge 1$, we define

$$\mathfrak{T}_\delta h(\boldsymbol{x}) = \sum_{i=0}^{q-2} \sum_{v \in V_\delta} h\left(\sum_{j \in E} \sigma^j(\zeta^i v) x_j\right).$$

Given any $s \in \mathbb{Z}_{p^\infty}[\zeta]$, we have

$$\mathfrak{T}_\delta h(s, \sigma(s), \ldots, \sigma^{e-1}(s)) = \sum_{i=0}^{q-2} \sum_{v \in V_\delta} h(\mathrm{Tr}(\zeta^i vs)) \qquad (14)$$

which is essentially the trace-averaging technique used in Lemma 4.8. From this we can now make a polynomial approximation of the function $\mathfrak{G}$ in Lemma 4.9.

Theorem 4.10: For each $\delta, m \ge 1$, let $h_{\delta,m}(x) \in \mathbb{Q}_p[x]$ be the polynomial as described in Theorem 4.1. For each δ with $1 \le \delta \le d$ and each $m \ge 1$, let

$$H_{\delta,m}(\boldsymbol{x}) = \mathfrak{T}_\delta h_{\delta, m+ed-\delta}(\boldsymbol{x}).$$

Let

$$H(\boldsymbol{x}) = \frac{p^d}{(p-1)q^d}\left[H_{d,m}(\boldsymbol{x}) - \left(\frac{q}{p} - 1\right)\left(p^{1-d} + \sum_{i=1}^{d-1} p^{i-d} H_{i,m}(\boldsymbol{x})\right)\right].$$

Then for any $s \in \mathbb{Z}_{p^\infty}[\zeta]$

$$H(s, \sigma(s), \ldots, \sigma^{e-1}(s)) \equiv \begin{cases} 0 \pmod{p^m}, & \text{if } v_p(s) < d \\ 1 \pmod{p^m}, & \text{if } v_p(s) \ge d. \end{cases}$$

We can write

$$H(\boldsymbol{x}) = \sum_{\mu \in D} H_\mu \boldsymbol{x}^\mu$$

where D is the set of D-M multisets of E having cardinality less than or equal to $[(m+d(e-1))(p-1)+1]p^{d-1}-1$ and where each H_μ is an element of $\mathbb{Q}_p(\zeta)$.

Proof: Theorem 4.1 says that $h_{\delta,m+ed-\delta}$ approximates modulo $p^{m+ed-\delta}$ the function F_δ defined in Lemma 4.6. Then (14) shows us that for any $s \in \mathbb{Z}_{p^\infty}[\zeta]$

$$\begin{aligned} H_{\delta,m}(s,\ldots,\sigma^{e-1}(s)) &= \sum_{i=0}^{q-2} \sum_{v \in V_\delta} h_{\delta,m+de-\delta}(\mathrm{Tr}(\zeta^i v s)) \\ &\equiv \mathfrak{G}_\delta(s) \pmod{p^{m+ed-\delta}} \end{aligned}$$

where $\mathfrak{G}_\delta$ is defined in Lemma 4.8. Thus,

$$\begin{aligned} &\frac{p^d}{(p-1)q^d} H_{d,m}(s,\sigma(s),\ldots,\sigma^{e-1}(s)) \\ &\qquad \equiv \frac{p^d}{(p-1)q^d} \mathfrak{G}_d(s) \pmod{p^m} \end{aligned}$$

and for $1 \le i < d$, we have

$$\begin{aligned} &-\frac{p^d}{(p-1)q^d}\left(\frac{q}{p}-1\right) p^{i-d} H_{i,m}(s,\sigma(s),\ldots,\sigma^{e-1}(s)) \\ &\qquad \equiv -\frac{p^d}{(p-1)q^d}\left(\frac{q}{p}-1\right) p^{i-d} \mathfrak{G}_i(s) \pmod{p^m}. \end{aligned}$$

Now adding these together along with a constant, we have

$$H(s,\sigma(s),\ldots,\sigma^{e-1}(s)) \equiv \mathfrak{G}(s) \pmod{p^m}$$

for all $s \in \mathbb{Z}_{p^\infty}[\zeta]$, where $\mathfrak{G}$ is as defined in Lemma 4.9. Now Lemma 4.9 completes the proof of our congruence for $H(\boldsymbol{x})$.

By Lemma 4.13 below, we can write each $H_{\delta,m}(\boldsymbol{x})$ as a polynomial with coefficients in $\mathbb{Q}_p(\zeta)$ and monomials of the form $\boldsymbol{x}^\mu$, where μ must be a D-M multiset of E. Thus, we can write

$$H(\boldsymbol{x}) = \sum_{\mu \in \Delta} H_\mu \boldsymbol{x}^\mu$$

where Δ is the set of all D-M multisets and the coefficients H_μ lie in $\mathbb{Q}_p(\zeta)$. Then Lemma 4.14 shows that the degree of $H(\boldsymbol{x})$ does not exceed $[(m+d(e-1))(p-1)+1]p^{d-1}-1$. Since the degree of $\boldsymbol{x}^\mu$ is $|\mu|$, we may restrict the index set of our sum from Δ to the set D as defined in the statement of this theorem. □

This establishes the existence of a polynomial which can be used in Theorem 3.1 to prove Theorem 1.6. We provide two examples of the computations which would be involved in the trace-averaging procedure. They explain the origin of the polynomials used in Examples 3.2, 3.3, and 3.4. In typical applications of Theorem 3.1, such as those use to prove Theorem 1.6, we shall not need to make specific computations such as these; the existence of the polynomials we need will be guaranteed by Theorem 4.10 above, and their degrees are shown to be sufficiently low in Lemma 4.14 below. So the following examples show calculations that would not normally need to be performed; nonetheless, they illustrate the algebraic workings of the trace-averaging procedure.

Example 4.11: Let us consider the case when $p=2, d=1$, and $e=2$, so that $\mathrm{GR}(p^d,e) = \mathrm{GR}(2,2) = \mathrm{GF}(4)$. Then $\mathrm{GF}(4)$ is the reduction modulo 2 of $\mathbb{Z}_{2^\infty}[\zeta]$, where ζ is a primitive third root of unity over $\mathbb{Z}_{2^\infty}$. Suppose that we are interested in a polynomial $H(x_0,x_1)$ with the property that for any $s \in \mathbb{Z}_{2^\infty}[\zeta]$

$$H(s,\sigma(s)) \equiv \begin{cases} 0 \pmod 4, & \text{if } s \equiv 0 \pmod 2 \\ 1 \pmod 4, & \text{otherwise.} \end{cases}$$

Then Theorem 4.10 tells us that we should use $H(\boldsymbol{x}) = \frac{1}{2}(H_{1,2}(\boldsymbol{x})-1)$, where $H_{1,2}(\boldsymbol{x}) = \mathfrak{T}_1 h_{1,3}(\boldsymbol{x})$ with $h_{1,3}(x)$ the polynomial furnished by Theorem 4.1. In Example 4.2, we saw that we could set $h_{1,3}(x) = 1+2x+3x^2+2x^3$. Then we compute $H_{1,1}(\boldsymbol{x})$ by applying the trace-averaging operator for polynomials, which was defined at the beginning of this subsection. Note that $q = p^e = 4, V_1 = \{1\}$ since we are working with a finite field, and $E = \{0,1\}$ since $e=2$. Thus,

$$H_{1,2}(x_0,x_1) = \sum_{i=0}^{2} h_{1,3}\left(\sum_{j=0}^{1} \sigma^j(\zeta^i) x_j\right).$$

Recalling that the minimal polynomial for ζ is $\zeta^2+\zeta+1=0$ and that $\sigma(\zeta)=\zeta^2$, we compute $H_{1,2}(x_0,x_1) = 3+18x_0x_1+6x_0^3+6x_1^3$. Thus, Theorem 4.10 tells us that the polynomial $H(x_0,x_1) = 1+9x_0x_1+3x_0^3+3x_1^3$ has the property we want. Since x_0 and x_1 are always set to be elements of $\mathbb{Z}_{2^\infty}[\zeta]$ and since we are interested in the output of $H(x_0,x_1)$ modulo 4, we could equally well use the polynomial $1+x_0x_1-x_0^3-x_1^3$. Recall that this polynomial was used in Example 3.2 to compute zero counts modulo 4 in codewords of a code over $\mathrm{GF}(4)$. □

Example 4.12: Let us consider the case when $p=2, d=2$, and $e=2$, so that $\mathrm{GR}(p^d,e) = \mathrm{GR}(4,2)$. Then $\mathrm{GR}(4,2)$ is the reduction modulo 4 of $\mathbb{Z}_{2^\infty}[\zeta]$, where ζ is a primitive third root of unity over $\mathbb{Z}_{2^\infty}$. Here π is reduction modulo 4 and zer is the zero count weight function on $\mathrm{GR}(4,2)$. Suppose that we are interested in a polynomial $H(x_0,x_1)$ with the property that for any $s \in \mathbb{Z}_{2^\infty}[\zeta]$

$$H(s,\sigma(s)) \equiv \mathrm{zer}(\pi(s)) \pmod 4.$$

Then Theorem 4.10 tells us that we should use

$$H(\boldsymbol{x}) = \frac{1}{4}\left(H_{2,2}(\boldsymbol{x}) - \frac{1}{2} - \frac{1}{2}H_{1,2}(\boldsymbol{x})\right)$$

where $H_{i,2}(\boldsymbol{x}) = \mathfrak{T}_i h_{i,6-i}(\boldsymbol{x})$ with $h_{i,j}(x)$ the polynomial furnished by Theorem 4.1.

So we need polynomials $h_{2,4}(x)$ and $h_{1,5}(x)$ guaranteed to exist by Theorem 4.1. The construction of such polynomials is described in [10, Sec. IV]. See especially Example 4.10 of that paper, which describes the construction of $1-h_{2,3}(x)$. By

such methods and with the aid of mathematical software [38] to perform the computations, one can construct polynomials

$$h_{2,4}(x) = 1 - 6x^2 + \frac{11}{4}x^3 + \frac{15}{16}x^4 + \frac{117}{16}x^5 - \frac{43}{8}x^6 - \frac{43}{8}x^7 + \frac{23}{16}x^8 + \frac{53}{16}x^9$$

and

$$h_{1,5}(x) = 1 - 8x^2 + 14x^3 - 9x^4 + 2x^5.$$

One can verify that $h_{2,4}(x)$ takes the appropriate values modulo 16 on all of $\mathbb{Z}_{2^\infty}$ by checking it at the points $0, 1, \ldots, 255$, for clearly $h(r) \equiv h(r') \pmod{16}$ when $r \equiv r' \pmod{256}$, since all denominators of coefficients are divisors of 16. Similarly, one can verify that $h_{1,5}(x)$ takes appropriate values modulo 32 on $\mathbb{Z}_{2^\infty}$ by checking its values at $0, 1, \ldots, 31$.

Now we compute $H_{2,2}(\boldsymbol{x}) = \mathfrak{T}_2 h_{2,4}(\boldsymbol{x})$ by applying to our polynomials the trace-averaging operator defined at the beginning of this section. Note that $q = p^e = 4$ and $E = \{0, 1\}$ since $e = 2$. We must determine the set V_2 used in trace-averaging; it is defined in Section IV-B as a set of representatives in the quotient of

$$\mathrm{GR}\,(4,2)^{\equiv 1} = \{1, -1, 1 + 2\pi(\zeta), -1 - 2\pi(\zeta)\}$$

modulo $\mathrm{GR}\,(4,1)^{\equiv 1} = \{1, -1\}$. So we may set $V_2 = \{1, 1 + 2\pi(\zeta)\}$. Then

$$H_{2,2}(\boldsymbol{x}) = \sum_{i=0}^{2} \sum_{v \in V_2} h_{2,4}\left(\sum_{j=0}^{1} \sigma^j(v\zeta^i)x_j\right).$$

Recalling that the minimal polynomial for ζ is $\zeta^2 + \zeta + 1 = 0$ and that $\sigma(\zeta) = \zeta^2$, one can use mathematical software [38] to compute

$$\begin{aligned} H_{2,2}(x_0, x_1) &= 6 - 144x_0x_1 - \frac{33 + 99\zeta}{2}x_0^3 + \frac{66 + 99\zeta}{2}x_1^3 \\ &\quad + \frac{675}{4}x_0^2x_1^2 - \frac{7020 + 15795\zeta}{32}x_0^4x_1 \\ &\quad + \frac{8775 + 15795\zeta}{8}x_0x_1^4 + \frac{1677}{4}x_0^6 - 9030x_0^3x_1^3 + \frac{1677}{4}x_1^6 \\ &\quad + \frac{35217 + 73143\zeta}{4}x_0^5x_1^2 - \frac{37926 + 73143\zeta}{4}x_0^2x_1^5 \\ &\quad - 2760x_0^7x_1 + \frac{99015}{4}x_0^4x_1^4 - 2760x_0x_1^7 \\ &\quad + \frac{6519 + 12879\zeta}{8}x_0^9 - \frac{133560 + 270459\zeta}{2}x_0^6x_1^3 \\ &\quad + \frac{136899 + 270459\zeta}{8}x_0^3x_1^6 + \frac{6360 - 12879\zeta}{8}x_1^9. \end{aligned}$$

The computation $H_{1,2}(\boldsymbol{x}) = \mathfrak{T}_1 h_{1,5}(\boldsymbol{x})$ is similar to the calculation done in the previous example, since $V_1 = \{1\}$. We obtain

$$\begin{aligned} H_{1,2}(x_0, x_1) = 3 &- 48x_0x_1 + 42x_0^3 + 42x_1^3 \\ &- 162x_0^2x_1^2 + 30x_0^4x_1 + 30x_0x_1^4. \end{aligned}$$

From these, we can compute

$$H(x_0, x_1) = \frac{1}{4}H_{2,2}(x_0, x_1) - \frac{1}{8}H_{1,2}(x_0, x_1) - \frac{1}{8}$$

which is a polynomial in $\mathbb{Q}[\zeta][x_0, x_1]$ which approximates $\mathrm{zer} \circ \pi$ modulo 4 in the manner desired. If one adds integer multiples of 4 to the rational coefficients of $H(x_0, x_1)$ in such a way as to make each rational coefficient as small in magnitude as possible, one obtains the polynomial used in Examples 3.3 and 3.4. □

We finish this section by stating and proving the lemmas which were used to bound the degree and describe structure of the polynomials of Theorem 4.10. The first of our propositions uses some of the compact notations from Section II-D in its statement and proof, so it might be helpful for readers to review these.

Lemma 4.13: Suppose that $\delta \geq 1$ and $h(x) \in \mathbb{Q}_p[x]$ with $n = \deg(h)$ and $h(x) = \sum_{i=0}^{n} h_i x^i$. Then

$$\mathfrak{T}_\delta h(\boldsymbol{x}) = (q-1)\sum_{i=0}^{n} i! h_i \sum_{\mu \in D_i} \frac{1}{\mu!}\rho_{\delta,\mu}\boldsymbol{x}^\mu$$

where D_i is the set of D-M multisets of E of cardinality i and $\rho_{\delta,\mu} = \sum_{v \in V_\delta} v^\mu \in \mathbb{Z}_{p^\infty}[\zeta]$. If $\delta = 1$ or $e = 1$, then $\rho_{\delta,\mu} = 1$.

Proof: First note that $\mathfrak{T}_\delta$ is $\mathbb{Q}_p$-linear. Therefore, it will suffice to prove the theorem for the monomial $h(x) = x^\ell$. Then

$$\begin{aligned} \mathfrak{T}_\delta h(\boldsymbol{x}) &= \sum_{i=0}^{q-2}\sum_{v \in V_\delta}\left(\sum_{j \in E}\sigma^j(\zeta^i v)x_j\right)^\ell \\ &= \sum_{i=0}^{q-2}\sum_{v \in V_\delta}\left(\sum_{j_1 \in E}\cdots\sum_{j_\ell \in E}\prod_{k=1}^{\ell}\sigma^{j_k}(\zeta^i v)x_{j_k}\right) \\ &= \sum_{i=0}^{q-2}\sum_{v \in V_\delta}\sum_{\substack{\mu \in \mathbb{N}[E],\\ |\mu| = \ell}}\frac{|\mu|!}{\mu!}\prod_{k \in E}(\sigma^k(\zeta^i v)x_k)^{\mu_k} \\ &= \sum_{i=0}^{q-2}\sum_{v \in V_\delta}\sum_{\substack{\mu \in \mathbb{N}[E],\\ |\mu| = \ell}}\frac{\ell!}{\mu!}(\zeta^i)^\mu v^\mu \boldsymbol{x}^\mu \\ &= \ell!\sum_{\substack{\mu \in \mathbb{N}[E],\\ |\mu| = \ell}}\frac{1}{\mu!}\boldsymbol{x}^\mu \sum_{v \in V_\delta} v^\mu \sum_{i=0}^{q-2}(\zeta^i)^\mu \\ &= \ell!\sum_{\substack{\mu \in \mathbb{N}[E],\\ |\mu| = \ell}}\frac{1}{\mu!}\rho_{\delta,\mu}\boldsymbol{x}^\mu \sum_{i=0}^{q-2}(\zeta^i)^\mu \end{aligned}$$

where $\rho_{\delta,\mu}$ in the last expression is as defined in the statement of this lemma. Note that $V_\delta \subseteq \mathbb{Z}_{p^\infty}[\zeta]$, so that $\rho_{\delta,\mu} \in \mathbb{Z}_{p^\infty}[\zeta]$. Now let us consider the term

$$\begin{aligned} \sum_{i=0}^{q-2}(\zeta^i)^\mu &= \sum_{i=0}^{q-2}\prod_{j \in E}(\sigma^j(\zeta^i))^{\mu_j} \\ &= \sum_{i=0}^{q-2}\prod_{j \in E}\zeta^{ip^j\mu_j} \\ &= \sum_{i=0}^{q-2}\zeta^{i\sum_{j \in E}\mu_j p^j} \\ &= \sum_{i=0}^{q-2}\zeta^{i\Sigma\mu} \end{aligned}$$

where in the last step it is permissible to think of $\Sigma\mu$, an integer modulo $q-1$, as an exponent because ζ has order $q-1$. Thus,

$$\sum_{i=0}^{q-2}(\zeta^i)^\mu = \begin{cases} q-1, & \text{if } \Sigma\mu = 0 \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

Equivalently, our term is $q-1$ when μ is Delsarte–McEliece and vanishes otherwise. Thus,

$$\mathfrak{T}_\delta h(\boldsymbol{x}) = (q-1)\ell! \sum_{\mu\in D_\ell} \frac{1}{\mu!}\rho_{\delta,\mu}\boldsymbol{x}^\mu$$

as we were to show.

It remains to show that if $\delta = 1$ or $e = 1$, then $\rho_{\delta,\mu} = 1$. When $\delta = 1$ or $e = 1$, then $V_\delta = \{1\}$ according to the definition in Section IV-B preceding Lemma 4.8, so this is immediate. □

Now we shall prove a result about the degree of the polynomial $H(\boldsymbol{x})$ of Theorem 4.10. Note that Lemma 4.13 shows that if $h(x)$ is of degree n, then $\mathfrak{T}_\delta h(\boldsymbol{x})$ is of degree at most n, since $\boldsymbol{x}^\mu$ is a monomial of degree $|\mu|$. We must be careful to note that trace-averaging may strictly decrease the degree of a polynomial, for the set D_i of Lemma 4.13 may be empty for a given value of i.

Lemma 4.14: The total degree of the polynomial $H(\boldsymbol{x})$ defined in Theorem 4.10 above is less than or equal to $[(m+d(e-1))(p-1)+1]p^{d-1}-1$.

Proof: The polynomial $H(\boldsymbol{x})$ is a constant plus a linear combination of the polynomials $H_{\delta,m}$ for $1 \le \delta \le d$, which are also defined in Theorem 4.10. By the remark preceding this lemma, we know that the degree of $H_{\delta,m}$ is less than or equal to the degree of $h_{\delta,m+ed-\delta}$, which is described in Theorem 4.1 and used in Theorem 4.10 to define $H_{\delta,m}$. We also know that $h_{\delta,m+ed-\delta}$ has degree

$$[(m+ed-\delta)(p-1)+1]p^{\delta-1}-1$$

as given in Theorem 4.1. Thus,

$$\deg(H) \le \max_{1\le\delta\le d}[(m+ed-\delta)(p-1)+1]p^{\delta-1}-1.$$

We shall show that $f(\delta) = [(m+ed-\delta)(p-1)+1]p^{\delta-1}-1$ is a strictly increasing function of δ for $1 \le \delta \le d$, which will complete our proof. If we assume that $1 \le \delta < d$, then it is not hard to show that

$$f(\delta+1) - f(\delta) = (m+ed-\delta-1)(p-1)^2p^{\delta-1}.$$

But this last expression is at least $(m+d(e-1))(p-1)^2p^{\delta-1}$, which is a positive integer. □

This finishes the development of what we need to know about our trace-averaged counting polynomials in order to prove Theorem 1.6 from Theorem 3.1. The next section is devoted to this proof and its ramifications.

V. Analogues of McEliece's Theorem

Here we prove the main result of the paper (Theorem 1.6) and show that various generalizations and analogues of McEliece's theorem extant in the literature are specializations of our theorem. We will see the power and scope of the counting polynomial method in its ability to unify existing results and obtain new ones.

A. Abelian Codes Over Galois Rings

To prove Theorem 1.6, we simply combine Theorem 3.1 with the trace-averaged counting polynomials developed in Section IV-C. We start with a somewhat more general theorem, of which Theorem 1.6 will be a corollary.

Theorem 5.1: Let $m \ge 1$ be given. Let $f \in \mathrm{GR}(p^d, e)[A]$ and suppose that $\hat{f}$ is supported on S. Let $\tilde{F} = \tau \circ \tilde{f}$. Let $H(\boldsymbol{x})$ be the polynomial defined in Theorem 4.10, written

$$H(\boldsymbol{x}) = \sum_{\mu\in D} H_\mu \boldsymbol{x}^\mu$$

where D denotes the set of all D-M multisets of E of cardinality at most $[(m+d(e-1))(p-1)+1]p^{d-1}-1$. Then

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}\left(\tilde{f}_{1_A}\right) + |A|\sum_{\mu\in D}\mu!H_\mu \sum_{\lambda\in B_\mu}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where B_μ is the set of nontrivial unity-product $\lambda \in \mathbb{N}[S\times E]$ with $\exp(\lambda) = \mu$.

Proof: This is the application of Theorem 3.1 using the polynomial $H(\boldsymbol{x})$, whose relevant properties are proved in Theorem 4.10. □

Now we shall prove Theorem 1.6 as a corollary. We rewrite the assumptions in the notation and terminology which has been developed for this paper. See Section II-D for the correspondence between the notation used in Section I-B in the statement of Theorem 1.6 and the notation used here. Note also that this version of Theorem 1.6 does not require the assumption that the Fourier transforms of codewords vanish at 1_A.

Corollary 5.2: Let $f \in \mathrm{GR}(p^d, e)[A]$ and suppose that $\hat{f}$ is supported on the set S with $S \not\subseteq \{1_A\}$. Let ℓ be the cardinality of the smallest nontrivial unity-product D-M multiset in $\mathbb{N}[S\times E]$ (which exists by Lemma 2.11). Then

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}\left(\tilde{f}_{1_A}\right) \quad \left(\mathrm{mod}\, p^{\lfloor\frac{\ell-p^{d-1}}{(p-1)p^{d-1}}\rfloor - d(e-1)}\right)$$

with $\mathrm{zer}(\tilde{f}_{1_A}) = \mathrm{zer}(\sum_{a\in A} f_a)$.

Proof: Let $\tilde{F} = \tau\circ\tilde{f}$. Set $m = \lfloor\frac{\ell-p^{d-1}}{(p-1)p^{d-1}}\rfloor - d(e-1)$. If $m < 1$, then the result is trivial, so assume $m \ge 1$ henceforth. Then $m + d(e-1) = \lfloor\frac{\ell-p^{d-1}}{(p-1)p^{d-1}}\rfloor$, and so

$$\ell - p^{d-1} \ge (m+d(e-1))(p-1)p^{d-1}$$

so that

$$\ell > [(m+d(e-1))(p-1)+1]p^{d-1}-1. \tag{15}$$

Now apply our theorem with this value of m to obtain

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}\left(\tilde{f}_{1_A}\right) + |A|\sum_{\mu\in D}\mu!H_\mu\sum_{\lambda\in B_\mu}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

and note that B_μ is empty if μ is a D-M multiset of cardinality less than ℓ. But all $\mu \in D$ are D-M multisets with cardinality less than ℓ by the definition of D in the theorem and by (15). This gives the congruence we were to prove. Now $\tilde{f}_{1_A} = \frac{1}{|A|}\hat{f}_{1_A}$, so that $\tilde{f}_{1_A} = 0$ if and only if $\hat{f}_{1_A} = 0$, i.e., if and only if $\sum_{a\in A} f_a = 0$. □

We pause to present some examples illustrating the use of Corollary 5.2.

Example 5.3: Let $k > 0$ and let A be the cyclic group of order $4^k - 1$ generated by an element a. Here we let C_k be the code in GR $(4,2)[A]$ whose Fourier transform is supported on the set $S = \{a, a^4, \ldots, a^{4^{k-1}}\}$. In a more conventional presentation of cyclic codes, this is the code in GR $(4,2)[x]/(x^{4^k-1}-1)$ whose check polynomial is one of the kth-degree irreducible factors of the cyclotomic polynomial $\Phi_{4^k-1}(x)$ in GR $(4,2)[x]$. The family of codes C_k for $k > 0$ was investigated in Example 1.7. It was determined that $\ell = 2k$ for this code, and thus Corollary 5.2 (known before as Theorem 1.6) tells us that for any word $c \in C_k$, we have $\operatorname{zer}(c) \equiv -1 \pmod{2^{k-3}}$. Equivalently, our theorem shows that the Hamming weights are divisible by 2^{k-3}. Example 3.3 shows that when $k = 5$, this result is sharp: the words of C_5 have Hamming weights divisible by 4, and the weight enumerator is $1 + 1023x^{768} + 556512x^{948} + 491040x^{972}$, so some words do not have Hamming weights divisible by 8. On the other hand, Example 3.4 shows that our theorem is not sharp for $k = 4$: the theorem merely predicts that Hamming weights are divisible by 2, where in fact the weight enumerator is $1 + 255x^{192} + 10200x^{228} + 48960x^{240} + 6120x^{252}$. Thus, all Hamming weights are divisible by 4 (but not all by 8). Recall that in Example 3.4, a calculation using Theorem 3.1 and detailed knowledge of the polynomial used to estimate weights was used to demonstrate that all Hamming weights in this code are divisible by 4. Thus, it can happen that the estimates which give rise to Theorem 5.1 and Corollary 5.2 are not as sharp as possible, but stronger estimates can be recovered from the general theorem (Theorem 3.1). □

The following example shows how Corollary 5.2 can also be applied to relatives of cyclic codes. We consider a family of codes which are used in constructing the Kerdock codes over Galois fields of characteristic 2 (see [22] for details).

Example 5.4: For each positive integer j, let C_j be the code described in the previous example. Let $\bar{C}_j$ be the code generated by adding constant words to elements of C_j, i.e., the minimal support of the Fourier transform of $\bar{C}_j$ is $\{1, a, a^4, \ldots, a^{4^{j-1}}\}$. Let K_j be the code obtained by appending one extra letter to each word of $\bar{C}_j$ in such a way that the letters in each word sum to zero.

In Example 2.7, we investigated the set Λ' (as defined in Section II-D) for the codes C_j. A similar analysis shows that Λ' for $\bar{C}_j$ is quite similar: it contains no multiset of cardinality less than $2j$, and it contains a unique multiset of cardinality $2j$, which is precisely the same as the one in Λ' for C_j. Thus, $\ell = 2j$ for $\bar{C}_j$, and so Corollary 5.2 tells us that

$$\operatorname{zer}(f) \equiv -\operatorname{zer}(\tilde{f}_1) \pmod{2^{j-3}} \tag{16}$$

for all $f \in \bar{C}_j$.

Now let us consider what this implies for the code K_j. Any word $g \in K_j$ is obtained by taking a word $f \in \bar{C}_j$ and appending the symbol $-\sum_{a \in A} f_a$ to make a word whose letters sum to zero. Thus,

$$\operatorname{zer}(g) = \operatorname{zer}(f) + \operatorname{zer}(-\hat{f}_1) = \operatorname{zer}(f) + \operatorname{zer}(\tilde{f}_1).$$

Thus, in view of (16), $\operatorname{zer}(g) \equiv 0 \pmod{2^{j-3}}$. Since words in K_j have length 2^{2j}, this means all zero counts and Hamming weights are divisible by 2^{j-3}.

When j is odd and $j \geq 3$, the results of Nechaev and Kuzmin [22] show that our claim that zero counts and weights are divisible by 2^{j-3} is sharp, i.e., there exists some word in K_j with zero count and Hamming weight not divisible by 2^{j-2}. Specifically, they prove that the zero counts which occur are $0, 2^{2j}, 2^{2j-2}, 2^{2j-4} \pm 2^{j-3}$, and $2^{2j-4} \pm 3 \cdot 2^{j-3}$.

When j is even and $j \geq 4$, our claim that zero counts and weights are divisible by 2^{j-3} is not sharp. For Kuzmin and Nechaev [22] show that the zero counts that occur are $0, 2^{2j}, 2^{2j-2}, 2^{2j-4}, 2^{2j-4} \pm 2^{j-2}$, and $2^{2j-4} \pm 3 \cdot 2^{j-2}$. Thus, all zero counts and weights are divisible by 2^{j-2}. □

Note that one can also use Theorem 5.1 and Corollary 5.2 to count the number of instances in a codeword of a particular symbol other than 0. If $r \in$ GR (p^d, e), then counting the number of instances of r in $f \in$ GR $(p^d, e)[A]$ is equivalent to counting the number of zeroes in the word g where $g_a = f_a - r$ for all $a \in A$. So we apply our theorem to g, noting that $\tilde{g}_a = \tilde{f}_a$ for all $a \neq 1_A$ and $\tilde{g}_{1_A} = \tilde{f}_{1_A} - r$.

Now we shall show how various results already in the literature are special cases of our theorem. We obtain a theorem for finite fields by setting $d = 1$ and a theorem for the rings $\mathbb{Z}_{p^d}$ by setting $e = 1$.

B. Abelian Codes Over Finite Fields

Throughout this section, we fix $d = 1$ so that GR $(p^d, e) =$ GF $(p^e) =$ GF (q), a finite field. We shall show that in this case, Theorem 5.1 implies the generalization of McEliece's original theorem due to Delsarte and McEliece [2]. Theorem 5.1 also includes sharper versions of the Delsarte–McEliece theorem, which can be obtained by increasing the parameter m, which controls the p-adic precision of the weight congruence. The main point of the theorem of Delsarte and McEliece is given as Theorem 1.3, but we shall prove their full theorem, which is somewhat more precise. The following is equivalent to the Delsarte–McEliece theorem.

Theorem 5.5: (Delsarte–McEliece [2]): Let $f \in$ GF $(q)[A]$ and suppose that $\hat{f}$ is supported on the q-closed subset S with $S \not\subseteq \{1_A\}$. Let $\tilde{F} = \tau \circ \tilde{f}$. Let ℓ be the cardinality of the smallest nontrivial unity-product D-M multiset in $\mathbb{N}[S \times E]$ (which exists by Lemma 2.11). Let $m = \frac{\ell}{p-1} - e + 1$. Then

$$\frac{1}{|A|}\operatorname{zer}(f) \equiv \operatorname{zer}\left(\tilde{f}_{1_A}\right) + (-1)^{m+e} p^{m-1} \sum_{\kappa \in B} \frac{\tilde{F}_\kappa}{\kappa!} \pmod{p^m}$$

where B is the set of nontrivial unity-product D-M multisets $\kappa \in \mathbb{N}[S \times E]$ with $|\kappa| = \ell$. The sum over B is a p-adic integer so that

$$\operatorname{zer}(f) \equiv |A| \operatorname{zer}\left(\tilde{f}_{1_A}\right) \pmod{p^{m-1}}$$

and if f is varied over all codewords whose Fourier transforms are supported on S, then there is some f such that

$$\operatorname{zer}(f) \not\equiv |A| \operatorname{zer}\left(\tilde{f}_{1_A}\right) \pmod{p^m}.$$

Proof: We apply Theorem 5.1 with $d = 1$ and m as given in the statement of this theorem to obtain

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\mu \in D} \mu! H_\mu \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where D is the set of D-M multisets of E having cardinality less than or equal to $(m+e-1)(p-1) = \ell$, H_μ is the coefficient of $\boldsymbol{x}^\mu$ in the polynomial $H(\boldsymbol{x})$ employed in Theorem 5.1, and B_μ is the set of nontrivial unity-product $\lambda \in \mathbb{N}[S \times E]$ with $\exp(\lambda) = \mu$. By our given assumption, B_μ will be empty for all D-M multisets μ with $|\mu| < \ell$, since $\exp(\lambda) = \mu$ implies $|\lambda| = |\mu|$. Thus, we have

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\mu \in D'} \mu! H_\mu \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where D' is the set of all D-M multisets of E having cardinality equal to ℓ.

We set $d = 1$ in Theorem 4.10, where $H(\boldsymbol{x})$ is defined, to see that

$$H(\boldsymbol{x}) = \frac{p}{(p-1)q}\mathfrak{T}_1 h_{1,m+e-1}(\boldsymbol{x}) - \frac{q-p}{(p-1)q}$$

where $h_{1,m+e-1}(x) \in \mathbb{Q}_p[x]$ is as defined in Theorem 4.1. Note that the polynomial $h_{1,m+e-1}(x)$ has degree $(m+e-1)(p-1) = \ell$ and then write it as $\sum_{i=0}^{\ell} h_i x^i$. By Lemma 4.13, if $\mu \in D'$, then the coefficient $\boldsymbol{x}^\mu$ in $\mathfrak{T}_1 h_{1,m+e-1}(\boldsymbol{x})$ will be

$$(q-1)\ell! h_\ell \frac{1}{\mu!}$$

so that

$$H_\mu = \frac{p(q-1)}{(p-1)q}\ell! h_\ell \frac{1}{\mu!}.$$

Thus,

$$\begin{aligned}\frac{1}{|A|}\mathrm{zer}(f) &\equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \frac{p(q-1)}{(p-1)q}\ell! h_\ell \sum_{\mu \in D'} \sum_{\lambda \in B_\mu} \frac{\tilde{F}_\lambda}{\lambda!} \\ &\equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \frac{p(q-1)}{(p-1)q}\ell! h_\ell \sum_{\kappa \in B} \frac{\tilde{F}_\kappa}{\kappa!} \pmod{p^m}\end{aligned}$$

where B is as defined in the statement of this theorem. Now by Lemma 2.12, $\kappa! \in \mathbb{N}$ is not divisible by p for any $\kappa \in B$. So $\frac{1}{\kappa!}$ is a p-adic integer. Furthermore, $\sigma^j(\tilde{F}_a)$ is p-adically integral for all $j \in E$ and $a \in A$, so that $\tilde{F}_\kappa$ is p-adically integral for all $\kappa \in B$. Therefore, the sum over B in the last expression is p-adically integral. Thus, to prove the first congruence asserted by this theorem, it suffices to show that

$$\frac{p(q-1)}{(p-1)q}\ell! h_\ell \equiv (-1)^{m+e} p^{m-1} \pmod{p^m}.$$

Now $\ell! h_\ell \equiv (-p)^{m+e-2} \pmod{p^{m+e-1}}$ by Theorem 4.1. Thus,

$$\frac{p(q-1)}{(p-1)q}\ell! h_\ell \equiv \frac{p(q-1)}{(p-1)q}(-p)^{m+e-2} \pmod{p^m}$$

and so

$$\begin{aligned}\frac{p(q-1)}{(p-1)q}\ell! h_\ell &\equiv \frac{q-1}{p-1}(-1)^{m+e} p^{m-1} \\ &\equiv (-1)^{m+e} p^{m-1} \pmod{p^m}.\end{aligned}$$

Thus the first congruence asserted by this theorem is true.

This congruence is the same, allowing for different notational conventions, as a congruence in the proof of Delsarte and McEliece [2, eq. (4.29)], which, as those authors note, is equivalent to their theorem. In particular, knowing that the sum over B is a p-adic integer immediately gives us

$$\mathrm{zer}(f) \equiv |A| \mathrm{zer}\left(\tilde{f}_{1_A}\right) \pmod{p^{m-1}}.$$

To prove the sharpness result, it will suffice to show that

$$\sum_{\kappa \in B} \frac{\tilde{F}_\kappa}{\kappa!} \not\equiv 0 \pmod{p}$$

or equivalently

$$\pi\left(\sum_{\kappa \in B} \frac{\tilde{F}_\kappa}{\kappa!}\right) \neq 0$$

for some f with $\hat{f}$ supported on S. From Lemma 2.12, we know that $\kappa!$ is an integer not divisible by p for all $\kappa \in B$. Thus, $\kappa!$ has a multiplicative inverse in $\mathrm{GF}(p)$, which we can also write as $\frac{1}{\kappa!}$ without confusion. Since π is a homomorphism of rings, it suffices to show

$$\sum_{\kappa \in B} \frac{1}{\kappa!}\pi(\tilde{F}_\kappa) \neq 0$$

for some f with $\hat{f}$ supported in S. Now, using the fact that π commutes with σ, it is straightforward to show that $\pi(\tilde{F}_\kappa) = (\pi \circ \tilde{F})_\kappa$, and note that $\pi \circ \tilde{F} = \pi \circ \tau \circ \tilde{f} = \tilde{f}$, so that $\pi(\tilde{F}_\kappa) = \tilde{f}_\kappa$. Thus, it suffices to show

$$\sum_{\kappa \in B} \frac{\tilde{f}_\kappa}{\kappa!} \neq 0 \tag{17}$$

for some f with $\hat{f}$ supported in S.

Let R be a set of q-class representatives for A. For each $r \in R$, denote the q-class of r by $\mathrm{Cl}(r)$. Let $T = R \cap S$ so that T is a set of q-class representatives for S. Thus, S is the disjoint union $\bigcup_{t \in T} \mathrm{Cl}(t)$. Set $\varepsilon_r = |\mathrm{Cl}(r)|$ for each $r \in R$. Then $\mathrm{Cl}(r) = \{r, r^q, \ldots, r^{q^{\varepsilon_r - 1}}\}$. For any $\kappa \in B$, we have

$$\kappa = \sum_{t \in T} \sum_{i=0}^{\varepsilon_t - 1} \sum_{j \in E} \kappa_{(t^{q^i}, j)} (t^{q^i}, j)$$

so that

$$\begin{aligned}\tilde{f}_\kappa &= \prod_{t \in T} \prod_{i=0}^{\varepsilon_t - 1} \prod_{j \in E} \left(\sigma^j(\tilde{f}_{t^{q^i}})\right)^{\kappa_{(t^{q^i}, j)}} \\ &= \prod_{t \in T} \prod_{i=0}^{\varepsilon_t - 1} \prod_{j \in E} \left(\sigma^{j+ie}(\tilde{f}_t)\right)^{\kappa_{(t^{q^i}, j)}} \\ &= \prod_{t \in T} \prod_{i=0}^{\varepsilon_t - 1} \prod_{j \in E} (\tilde{f}_t)^{\kappa_{(t^{q^i}, j)} p^{ie+j}}\end{aligned}$$

where the second equality is from Proposition 2.2 and the third equality uses that fact that σ takes any element in a finite field to its pth power. So we have

$$\tilde{f}_\kappa = \prod_{t \in T} (\tilde{f}_t)^{\sum_{i=0}^{\varepsilon_t - 1} \sum_{j=0}^{e-1} \kappa_{(t^{q^i}, j)} p^{ie+j}}. \tag{18}$$

Thus, $\tilde{f}_\kappa$ can be viewed as a monomial in the variables $\{\tilde{f}_t : t \in T\}$.

We claim that if $\kappa, \kappa' \in B$ are distinct, then $\tilde{f}_\kappa$ and $\tilde{f}_{\kappa'}$ give rise to different monomials in (18). Note that for any $\kappa \in B$, we have $0 \le \kappa_{(t^{q^i},j)} \le p-1$ for all t, i, j by Lemma 2.12. Thus, we see that for any $t \in T$, the exponent $\sum_{i=0}^{\varepsilon_t - 1} \sum_{j=0}^{e-1} \kappa_{(t^{q^i},j)} p^{ie+j}$ is the p-ary expansion of an integer n with $0 \le n < q^{\varepsilon_t}$, where $\kappa_{(t^{q^i},j)}$ is the digit for the p^{ie+j}-place. Since each such number has a unique p-ary expansion, this means that if $\kappa, \kappa' \in B$, then the exponents of $\tilde{f}_t$ we get when we apply (18) to $\tilde{f}_\kappa$ and $\tilde{f}_{\kappa'}$ will coincide if and only if $\kappa_{(t^{q^i},j)} = \kappa'_{(t^{q^i},j)}$ for $0 \le i < \varepsilon_t$ and $j \in E$. Thus, the monomials we get by applying (18) to $\tilde{f}_\kappa$ and $\tilde{f}_{\kappa'}$ will coincide if and only if κ and κ' take equal values at all points (t^{q^i}, j) with $t \in T, 0 \le i < \varepsilon_t$, and $j \in E$, i.e., if and only if $\kappa = \kappa'$. This proves that for each $\kappa \in B$, $\tilde{f}_\kappa$ is equal to a monomial in the variables $\{\tilde{f}_t \colon t \in T\}$ where the exponent of $\tilde{f}_t$ is strictly less than q^{ε_t} and different $\kappa \in B$ give rise to different monomials. Now note that B is nonempty since it contains the smallest nontrivial unity-product D-M multisets supported on $S \times E$. Furthermore, recall that $\kappa!$ is an integer not divisible by p for all $\kappa \in B$, so that $\sum_{\kappa \in B} \frac{\tilde{f}_\kappa}{\kappa!}$ is equal to a nonzero polynomial with coefficients in $\mathrm{GF}(p)$ and variables in $\{\tilde{f}_t \colon t \in T\}$, where $\tilde{f}_t$ never occurs with exponent q^{ε_t} or higher. We need to prove that this polynomial does not vanish for some choice of f where $\hat{f}$ is supported on S.

We are varying f over all codewords with $\hat{f}$ supported on S, or equivalently, by Proposition 2.2, for all codewords with $\hat{f}|_R$ supported on T. Thus, by Theorem 2.5, $\hat{f}|_T$ can vary over all of $\bigoplus_{t \in T} \mathrm{GF}(q^{\varepsilon_t})$. Since $\tilde{f} = \frac{1}{|A|}\hat{f}$ and $|A|$ is a unit in fields of characteristic p, $\tilde{f}|_T$ varies over the same set as $\hat{f}|_T$. So we have $\sum_{\kappa \in B} \frac{\tilde{f}_\kappa}{\kappa!}$ equal to a nonzero polynomial with coefficients in $\mathrm{GF}(p)$ and variables $\{\tilde{f}_t \colon t \in T\}$ where the degree in each $\tilde{f}_t$ is less than q^{ε_t} and each $\tilde{f}_t$ is varied independently of the others over the field $\mathrm{GF}(q^{\varepsilon_t})$. A basic result in the theory of polynomials over finite fields (given in [2, Lemma 3.10]) says that since the size of the set over which each $\tilde{f}_t$ is varied exceeds the degree of $\tilde{f}_t$ in the polynomial, there will be an assignment of values for the variables $\tilde{f}_t$ where the polynomial does not vanish. So we have proved (17) for some f with $\hat{f}$ supported on S, thus completing the proof of this theorem. □

We have now shown that the theorem of Delsarte and McEliece is one specific case of Theorem 5.1 when $d = 1$ and when we set the p-adic precision (governed by the size of m in Theorem 5.1) to be just sufficient to show that $\mathrm{zer}(f)$ is not always identical to $|A|\mathrm{zer}(\tilde{f}_{1_A})$. Raising m provides sharper versions of the Delsarte–McEliece theorem, which are correspondingly more complex.

It might also be possible to obtain congruences of increased accuracy (and increased complexity) by expanding upon the approach of Delsarte and McEliece [2]. Their relation (4.10) for the zero count in terms of the Fourier transform is an exact expansion, which is then truncated in (4.14) to obtain a congruence whose p-adic accuracy governs the precision of their theorem. If more terms were preserved and if the coefficients L_m in the expansion could be estimated with increased accuracy, it might be possible to obtain congruences like those furnished by Theorem 5.1. Determining the coefficients L_m with greater accuracy would amount to obtaining more accurate versions of the Stickelberger relation [40]. We leave such matters for future work, and we now investigate a different specialization of Theorem 5.1 which recapitulates some recent results.

C. Abelian Codes Over Integer Residue Rings $\mathbb{Z}_{p^d}$

Throughout this subsection we fix $e = 1$, while d can be any positive integer. Thus, we are working in the case when the alphabet of our code is $\mathrm{GR}(p^d, e) = \mathrm{GR}(p^d, 1) = \mathbb{Z}_{p^d}$, the integers modulo p^d. We prove the following result of Katz (of which Theorem 1.5 above is a part) by setting $e = 1$ in Theorem 5.1.

Theorem 5.6: ([10, Theorem 5.1 and Corollary 5.2]): Let $m \ge 1$ be given and set $d_m = [m(p-1)+1]p^{d-1} - 1$. Let $f \in \mathbb{Z}_{p^d}[A]$ and suppose that $\hat{f}$ is supported on S. Let $\tilde{F} = \tau \circ \tilde{f}$. Let

$$h(x) = \sum_{\substack{0 \le j \le d_m, \\ p-1 \,|\, j}} h_j x^j$$

be the polynomial $h_{d,m}(x)$ defined in Theorem 4.1. Then

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\substack{1 < j \le d_m, \\ p-1 \,|\, j}} j! h_j \sum_{\lambda \in B_j} \frac{1}{\lambda!} \prod_{s \in S} \tilde{F}_s^{\lambda_s} \pmod{p^m} \quad (19)$$

where B_j is the set of all $\lambda \in \mathbb{N}[S]$ with $|\lambda| = j, \prod_{s \in S} s^{\lambda_s} = 1_A$, and $\lambda \notin \{1_A\}$. If S contains some element which is not 1_A, then some B_j with $p-1 \,|\, j$ is nonempty. Let ℓ be the least multiple of $p-1$ such that $B_\ell \ne \emptyset$. Then

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}\left(\tilde{f}_{1_A}\right) \pmod{p^{\left\lfloor \frac{\ell - p^d + 1}{(p-1)p^{d-1}} \right\rfloor}}.$$

Proof: The symbol $\equiv$ will always denote congruence modulo p^m in this proof.

We apply Theorem 5.1 with $e = 1$ to obtain

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\mu \in D} \mu! H_\mu \sum_{\kappa \in C_\mu} \frac{\tilde{F}_\kappa}{\kappa!}$$

where D is the set of D-M multisets of E having cardinality less than or equal to d_m, H_μ is the coefficient of $\boldsymbol{x}^\mu$ in the polynomial $H(\boldsymbol{x})$ employed in Theorem 5.1, and C_μ is the set of nontrivial unity-product $\kappa \in \mathbb{N}[S \times E]$ with $\exp(\kappa) = \mu$. Since $e = 1$, we have $E = \{0\}$. Thus, all multisets of E are of the form $\mu = n[0]$ with $n \in \mathbb{N}$, and then $\mu! = n!$. Furthermore, since $q = p^e = p$, the D-M multisets of E are precisely those $n[0]$ with $p - 1 \,|\, n$. Thus, we have

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\substack{0 \le j \le d_m, \\ p-1 \,|\, j}} j! H_{j[0]} \sum_{\kappa \in C_{j[0]}} \frac{\tilde{F}_\kappa}{\kappa!}.$$

Since $e = 1, \boldsymbol{x}$ stands for the single indeterminate x_0. Looking at the definition of $H(\boldsymbol{x})$ in Theorem 4.10 and recalling that $e = 1$ and $q = p$, we have

$$H(\boldsymbol{x}) = \frac{1}{p-1}\mathfrak{T}_d h_{d,m}(\boldsymbol{x}) = \frac{1}{p-1}\sum_{i=0}^{p-2} \sum_{v \in V_d} h_{d,m}(\zeta^i v x_0).$$

Recall from the discussion preceding Lemma 4.8 that $V_d = \{1\}$ when $e = 1$, so that

$$H(\boldsymbol{x}) = \frac{1}{p-1}\sum_{i=0}^{p-2} h_{d,m}(\zeta^i x_0).$$

Using the notation for $h_{d,m}(x)$ given in the statement of this theorem, we have

$$\begin{aligned} H(\boldsymbol{x}) &= \frac{1}{p-1}\sum_{i=0}^{p-2}\sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} h_j \zeta^{ij} x_0^j \\ &= \frac{1}{p-1}\sum_{i=0}^{p-2}\sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} h_j x_0^j \\ &= \sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} h_j x_0^j \\ &= h(x_0) \end{aligned}$$

where the second equality uses the fact that ζ is a root of unity of order $p-1$. Thus, for $0 \le j \le d_m$ with $p-1 \,|\, j$, $H_{j[0]} = h_j$, and we have

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + \sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} j! h_j \sum_{\kappa\in C_{j[0]}} \frac{\tilde{F}_\kappa}{\kappa!}.$$

$C_{j[0]}$ is the set of nontrivial unity-product $\kappa \in \mathbb{N}[S\times E]$ with $\exp(\kappa) = j[0]$. Since $E = \{0\}$, this means that $C_{j[0]}$ is the set of $\kappa \in \mathbb{N}[S\times\{0\}]$ with $\kappa \notin \{(1_A,0)\}$, $\prod_{s\in S} s^{\kappa(s,0)} = 1_A$, and $|\kappa| = j$. For any account in $\mathbb{Z}[S]$, say $\lambda = \sum_{s\in S}\lambda_s s$, we define $\Phi(\lambda) \in \mathbb{Z}[S\times\{0\}]$ by setting $(\Phi(\lambda))_{(s,0)} = \lambda_s$. Note that Φ is an group isomorphism from $\mathbb{Z}[S]$ to $\mathbb{Z}[S\times\{0\}]$. Then $C_{j[0]} = \{\Phi(\lambda)\colon \lambda \in B_j\}$, where B_j is as defined in the statement of this theorem. So

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + \sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} j! h_j \sum_{\lambda\in B_j} \frac{\tilde{F}_{\Phi(\lambda)}}{\lambda!},$$

where we have used the observation that $\Phi(\lambda)! = \lambda!$. Since $E = \{0\}$, we have

$$\begin{aligned} \tilde{F}_{\Phi(\lambda)} &= \prod_{(s,j)\in S\times\{0\}} (\sigma^j(\tilde{F}_s))^{(\Phi(\lambda))_{(s,j)}} \\ &= \prod_{s\in S} (\tilde{F}_s)^{(\Phi(\lambda))_{(s,0)}} \\ &= \prod_{s\in S} \tilde{F}_s^{\lambda_s} \end{aligned}$$

so that

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}\left(\tilde{f}_{1_A}\right) + \sum_{\substack{0\le j\le d_m,\\ p-1\,|\,j}} j! h_j \sum_{\lambda\in B_j} \frac{1}{\lambda!}\prod_{s\in S}\tilde{F}_s^{\lambda_s}.$$

We note that the only unity-product multisets of S of cardinality less than two are $\emptyset$ and $\{1_A\}$, and these are supported on $\{1_A\}$. Thus, B_0 and B_1 are empty and we can omit the $j = 0$ and $j = 1$ terms from the sum to obtain congruence (19), which we were to prove.

Now suppose further that S contains some element s other than 1_A. If n is the order of s, then the multiset $n(p-1)[s]$ is an element of $B_{n(p-1)}$. This proves the existence of a nonempty B_j with j a multiple of $p-1$. Let ℓ be as defined in the statement of this theorem. Then set $m = \lfloor \frac{\ell - p^{d-1}}{(p-1)p^{d-1}} \rfloor$ and consider congruence (19). We have $\ell > [m(p-1)+1]p^{d-1} - 1 = d_m$, so that $B_j = \emptyset$ for $j \le d_m$. Therefore, congruence (19) becomes

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}\left(\tilde{f}_{1_A}\right)$$

which is what we were to show. □

The preceding theorem is a strengthening and generalization of a result of Wilson [8], [9], which in turn is a strengthening and generalization of a result of Calderbank, Li, and Poonen [7]. As noted in Section I-A, the congruence

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}(\tilde{f}_{1_A}) \left(\mathrm{mod}\, p^{\left\lfloor \frac{\ell - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}\right)$$

in this theorem is sharp for codes which are free $\mathbb{Z}_{p^d}$-modules, but is not sharp for infinitely many other Abelian codes over $\mathbb{Z}_{p^d}$ [11]. In particular, it is always sharp when $d = 1$ (since all vector spaces are free modules). There one recovers the results of McEliece and Delsarte for Abelian codes over prime fields.

VI. Conclusion

A single analogue of McEliece's theorem for p-adically estimating the zero counts of words in Abelian codes over Galois rings contains within itself the results of Delsarte and McEliece for Abelian codes over finite fields and the more recent results of Katz [10] (improving those of Calderbank, Li, and Poonen [7] and of Wilson [8], [9]) for Abelian codes over $\mathbb{Z}_{p^d}$. This shows that the counting polynomial methods first employed by Wilson, when applied with appropriate further insights, are powerful enough to recover all these analogues of McEliece's theorem, which were originally proved using a variety of techniques.

Besides unifying existing results, the theorem proved here tells us new things and opens new directions for research. In one direction, it can provide us with strengthened versions of the theorem of Delsarte and McEliece in [2]. These stronger versions, like the original theorem, express the approximate zero count of a codeword in terms of the word's Fourier transform. They are stronger in that one may obtain the approximate zero counts with any desired p-adic precision, keeping in mind that increasingly precise versions will be correspondingly more complex. The original theorem of McEliece [1] not only gave the integer m such that all codewords $c = (c_1, \ldots, c_n)$ in a specified cyclic code over GF(p) have $\mathrm{zer}(c) \equiv n\mathrm{zer}(c_1 + \cdots + c_n) \,(\mathrm{mod}\, p^m)$, but also provided a formula for $\mathrm{zer}(c)$ modulo p^{m+1} in terms of the Fourier transform of c. This was used in the calculation of weight enumerators of cyclic codes in [41]. It is now possible to obtain generalizations which give approximations modulo p^{m+2} or modulo even higher powers of p. We note that it has already been shown that analogues of McEliece's theorem of arbitrary p-adic precision can be devised for Abelian codes

over $\mathbb{Z}_{p^d}$. For example, see [10, Theorem 5.1], which appears as Theorem 5.6 in this paper. Our unified theorem tells us that arbitrary accuracy can be also be obtained in the same fashion for Abelian codes over finite fields.

In another direction, our theorem tells us something about the p-adic valuation of Hamming weights in Abelian codes whose alphabets are Galois rings GR (p^d, e) with $d, e \neq 1$. Such Galois rings are neither fields nor quotients of $\mathbb{Z}$, but have some properties of both. Many researchers recently have undertaken the study of Abelian codes over Galois rings and their relatives [22], [24], [25], [27]–[32]. It is hoped that this analogue of McEliece's theorem will be helpful in their studies.

ACKNOWLEDGMENT

The author wishes to thank R. M. Wilson and R. J. McEliece for their interest and support. He also thanks the Associate Editor and anonymous referees for helpful suggestions which improved this paper.

REFERENCES

[1] R. J. McEliece, "Weight congruences for p-ary cyclic codes," *Discr. Math.*, vol. 3, pp. 177–192, 1972.

[2] P. Delsarte and R. J. McEliece, "Zeros of functions in finite Abelian group algebras," *Amer. J. Math.*, vol. 98, pp. 197–224, 1976.

[3] H. N. Ward, "Combinatorial polarization," *Discr. Math.*, vol. 26, pp. 185–197, 1979.

[4] ——, "Multilinear forms and divisors of codeword weights," *Quart. J. Math. Oxford Ser. (2)*, vol. 34, pp. 115–128, 1983.

[5] ——, "Weight polarization and divisibility," *Discr. Math.*, vol. 83, pp. 315–326, 1990.

[6] ——, "Divisors of codes of Reed-Muller type," *Discr. Math.*, vol. 131, pp. 311–323, 1994.

[7] A. R. Calderbank, W.-C. W. Li, and B. Poonen, "A 2-adic approach to the analysis of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 977–986, May 1997.

[8] R. M. Wilson, "A Version for the Lee Metric of a Theorem of McEliece and Weights of Codewords in Cyclic Codes," unpublished manuscript, Feb. 1995.

[9] ——, "A lemma on polynomials modulo p^m and applications to coding theory," *Discr. Math.*, to be published.

[10] D. J. Katz, "p-Adic valuation of weights in Abelian codes over $\mathbb{Z}_{p^d}$," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 281–305, Jan. 2005.

[11] ——, "On p-Adic estimates of weights in Abelian codes over Galois rings," Ph.D. dissertation, Calif. Inst. Technol., Pasadena, CA, 2005.

[12] E. Spiegel, "Codes over $\mathbb{Z}_m$," *Inf. Contr.*, vol. 35, pp. 48–52, 1977.

[13] ——, "Codes over $\mathbb{Z}_m$, revisited," *Inf. Contr.*, vol. 37, pp. 100–104, 1978.

[14] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 4, pp. 480–483, Jul. 1979.

[15] A. A. Nechaev, "Kerdock's code in cyclic form" (in , 1991), *Diskret. Mat.*, pp. 123–139, 1989. English translation in *Discr. Math. Appl.*, vol.. 1, pp. 365–384.

[16] A. S. Kuz'min and A. A. Nechaev, "Construction of noise-stable codes using linear recurrent sequences over Galois rings," *Usp. Mat. Nauk*, vol. 47, pp. 183–184, 1992. English translation in *Russ. Math. Sur.*.

[17] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[18] A. S. Kuz'min and A. A. Nechaev, "Linearly representable codes and the Kerdock code over an arbitrary Galois field of characteristic 2," *Usp. Mat. Nauk*, vol. 49, pp. 165–166, 1994. English translation in *Russ. Math. Surv.*.

[19] B. S. Rajan and M. U. Siddiqi, "A generalized DFT for Abelian codes over $\mathbb{Z}_n$," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2082–2090, Nov. 1994.

[20] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic cyclic codes," *Des., Codes Cryptogr.*, vol. 6, pp. 21–35, 1995.

[21] A. A. Nechaev and A. S. Kuzmin, *Formal Duality of Linearly Presentable Codes Over a Galois Field (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1255, pp. 263–276.

[22] ——, *Trace-function on a Galois ring in coding theory (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1255, pp. 277–290.

[23] A. Ashikhmin, "On generalized Hamming weights for Galois ring linear codes," *Des., Codes Cryptogr.*, vol. 14, pp. 107–126, 1998.

[24] A. Kuz'min and A. Nechaev, "Complete weight functions of the generalized Kerdock code and of linear recursive codes over Galois rings of characteristic 4," in *Mathematical Methods and Applications*. Moscow, U.S.S.R., 1998, pp. 99–103.

[25] J. T. Blackford and D. K. Ray-Chaudhuri, "A transform approach to permutation groups of cyclic codes over Galois rings," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2350–2358, Nov. 2000.

[26] N. S. Babu and K.-H. Zimmermann, "Decoding of linear codes over Galois rings," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1599–1603, May 2001.

[27] A. Kuzmin and A. Nechaev, "Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring," *Discr. Appl. Math.*, vol. 111, pp. 117–137, 2001.

[28] W. Willems, "A note on self-dual group codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3107–3109, Dec. 2002.

[29] J. Pei, J. Cui, and S. Liu, "Cyclic codes over GR(4^m) which are also cyclic over $\mathbb{Z}_4$," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 749–758, Mar. 2003.

[30] Kiran. T and B. S. Rajan, "Abelian codes over Galois rings closed under certain permutations," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2242–2253, Sep. 2003.

[31] ——, "Consta-Abelian codes over Galois rings," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 367–380, Feb. 2004.

[32] B. K. Dey and B. S. Rajan, "Affine invariant extended cyclic codes over Galois rings," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 691–698, Apr. 2004.

[33] B. R. McDonald, *Finite Rings with Identity*. New York: Marcel Dekker, 1974.

[34] E. Dubois and A. N. Venetsanopoulos, "The discrete Fourier transform over finite rings with applications to fast convolution," *IEEE Trans. Comput.*, vol. C-27, no. 7, Jul. 1978.

[35] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an Abelian group," *Bell Syst. Tech. J.*, vol. 49, pp. 987–1011, 1970.

[36] M. F. Mattson and G. Solomon, "A new treatment of Bose-Chaudhuri codes," *J. SIAM*, vol. 9, pp. 654–669, Dec. 1961.

[37] P. Delsarte, "Automorphisms of Abelian codes," *Phillips Res. Repts*, vol. 25, pp. 389–403, 1970.

[38] "Mathematica, Version 5.2," Wolfram Research, Inc., Champaign, IL, 2005.

[39] R. M. Wilson, "A Remark on the Number of Codewords of Weight Congruent to j Modulo p^e and the MacWilliams Transform," unpublished manuscript, Apr. 1995.

[40] L. Stickelberger, "Ueber eine verallgemeinerung der kreistheilung," *Math. Ann.*, vol. 37, pp. 321–367, 1890.

[41] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes," *Inf. Control*, vol. 18, pp. 369–394, 1971.