p-Adic Valuation of Weights in Abelian Codes Over $\mathbb{Z}_{p^d}$

Daniel J. Katz

***Abstract*—Counting polynomial techniques introduced by Wilson are used to provide analogs of a theorem of McEliece. McEliece's original theorem relates the greatest power of p dividing the Hamming weights of words in cyclic codes over GF (p) to the length of the smallest unity-product sequence of nonzeroes of the code. Calderbank, Li, and Poonen presented analogs for cyclic codes over $\mathbb{Z}_{2^d}$ using various weight functions (Hamming, Lee, and Euclidean weight as well as count of occurrences of a particular symbol). Some of these results were strengthened by Wilson, who also considered the alphabet $\mathbb{Z}_{p^d}$ for p an arbitrary prime. These previous results, new strengthened versions, and generalizations are proved here in a unified and comprehensive fashion for the larger class of Abelian codes over $\mathbb{Z}_{p^d}$ with p any prime. For Abelian codes over $\mathbb{Z}_4$, combinatorial methods for use with counting polynomials are developed. These show that the analogs of McEliece's theorem obtained by Wilson (for Hamming weight, Lee weight, and symbol counts) and the analog obtained here for Euclidean weight are sharp in the sense that they give the maximum power of 2 that divides the weights of all the codewords whose Fourier transforms have a specified support.**

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

I. Introduction

INVESTIGATIONS into cyclic codes over $\mathbb{Z}_4$ have shed new light on problems in algebraic coding theory [1]. This has stimulated the already existing study of cyclic and Abelian codes whose alphabets are $\mathbb{Z}_m$, in an attempt to obtain theorems like those already available when the alphabet is a finite field [2]–[10]. It is common to consider alphabets $\mathbb{Z}_{p^d}$ with p a prime, since codes over arbitrary $\mathbb{Z}_m$ are isomorphic to direct sums of codes over various $\mathbb{Z}_{p^d}$ *via* the Chinese Remainder Theorem.

In this paper, we generalize a theorem of McEliece [11] on cyclic codes over GF(p) to Abelian codes over $\mathbb{Z}_{p^d}$. McEliece's original theorem provides p-adic estimates (i.e., estimates modulo powers of p) of the Hamming weight or the number of occurrences of a given symbol in codewords of a cyclic code over GF (p). These estimates are given in terms of the set of nonzeroes, i.e., roots of the check polynomial, of the code. More precisely, one must determine the length ℓ of the shortest unity-product sequence of nonzeroes, i.e., the shortest sequence $\theta_1, \theta_2, \ldots, \theta_\ell$ of nonzeroes with $\theta_1\theta_2 \ldots \theta_\ell = 1$. (In this Introduction, we will assume that 1 is not a nonzero of our code in order to simplify the discussion.) One must also determine the length ℓ' of the shortest unity-product sequence of nonzeroes with length divisible by $p-1$. Then McEliece's theorem shows that the number of occurrences of a given nonzero symbol $s \in$ GF (p) in each codeword is divisible by $p^{\lceil \frac{\ell}{p-1} \rceil - 1}$ but some word has a number of occurrences of s not divisible by $p^{\lceil \frac{\ell}{p-1} \rceil}$. McEliece's Theorem also shows that the Hamming weight of each codeword is divisible by $p^{\frac{\ell'}{p-1}-1}$ and says that some word has Hamming weight not divisible by $p^{\frac{\ell'}{p-1}}$. For $p = 2$, $\ell = \ell'$, but for p odd, we can have $\ell' > \ell$, as shown in Example 1 of [11, Sec. 3]. McEliece's theorem has found use beyond the obvious applications to cyclic codes over GF (p). The $p = 2$ case has been used to derive results on the divisibility of Lee weights and on the minimum Lee distance in $\mathbb{Z}_4$-linear trace codes [12]. McEliece's theorem has also been used in calculations of the cross correlation of pseudorandom sequences [13], [14].

Later, Delsarte and McEliece [15] generalized their argument to give an analog of the theorem for Abelian codes over arbitrary finite fields GF (p^k). In doing this, the set of nonzeroes of the code is very naturally replaced by the support of the Fourier transform of the code and new and intricate combinatorial arguments are necessary to handle alphabets that are finite fields not of prime order.

Generalizations of McEliece's theorem to cyclic codes over $\mathbb{Z}_{2^d}$ were obtained by Calderbank, Li, and Poonen and are stated in [10, Corollary 3.6 and Theorem 3.7]. In particular, they show that the number of occurrences of a nonzero symbol $s \in \mathbb{Z}_{2^d}$ in a codeword of such a code is divisible by $2^{\lceil \frac{\ell}{2^{d-1}} \rceil - 2}$. With regard to cyclic codes over $\mathbb{Z}_4$, they show that the Hamming, Lee, and Euclidean weights of a word must be divisible by $2^{\max\{\lceil \frac{\ell}{2} \rceil - 2, \lceil \frac{\ell}{3} \rceil - 1\}}$, $2^{\lceil \frac{\ell}{2} \rceil - 1}$, and $2^{\lceil \frac{\ell}{2} \rceil}$, respectively. They obtain these results by use of the 2-adic numbers and algebraic extensions thereof along with Galois rings, which are quotients of rings of algebraic integers in unramified algebraic extensions of the 2-adic numbers.

Improvements to the results of Calderbank, Li, and Poonen for Hamming weight, Lee weight, and symbol counts were obtained by Wilson [16], [17], whose counting polynomial method is the starting point for this research. In particular, Wilson showed that for cyclic codes over $\mathbb{Z}_{2^d}$, the number of occurrences of a nonzero symbol $s \in \mathbb{Z}_{2^d}$ is divisible by $2^{\lfloor \frac{\ell}{2^{d-1}} \rfloor - 1}$ and the Lee weight is divisible by $2^{\lfloor \frac{\ell-2}{2^{d-1}} \rfloor + 1}$ ([16, Theorems 3 and 2], respectively). When applied to cyclic codes

Manuscript received April 27, 2004; revised September 24, 2004. 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 is with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125 USA (email: katz@caltech.edu).

Communicated by R. J. McEliece, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.839495

over $\mathbb{Z}_4$, this shows that Hamming and Lee weights are all divisible by $2^{\lfloor \frac{\ell}{2} \rfloor - 1}$ and $2^{\lfloor \frac{\ell}{2} \rfloor}$, respectively. Wilson also provided a generalization to codes over $\mathbb{Z}_{p^d}$ for p an arbitrary prime; in [17, Theorem 9] he showed that the number of occurrences of any nonzero symbol (and hence the Hamming weight) is divisible by $p^{\left\lfloor \frac{\ell - p^d + 1}{(p-1)p^d - 1} \right\rfloor}$.

Our setting will be Abelian codes with alphabet $\mathbb{Z}_{p^d}$, where the underlying Abelian group has order coprime to p. We consider Hamming, Lee, and Euclidean weights, as well as the weight function that counts instances of a particular symbol. In Section II, we shall investigate the structure of such codes while developing the mathematics necessary for the statements and proofs of our theorems. Then, in Section III, we shall prove the Main Theorem of which our specific analogs of McEliece's theorem are applications. Since this Main Theorem will not provide good analogs of McEliece's theorem without carefully constructed counting polynomials, we dedicate Section IV to proofs of the existence and properties of such polynomials. Then we derive our analogs of McEliece's theorem in Section V. We show how our results imply those of McEliece in [11] as well as Wilson's improvements [16], [17] of the results of Calderbank, Li, and Poonen [10]. We also improve Wilson's analog for Hamming weights and derive a new analog for Euclidean weights of Abelian codes over $\mathbb{Z}_{p^d}$ which, when specialized to codes over $\mathbb{Z}_4$, is stronger than the version of Calderbank, Li, and Poonen. Finally, for codes with alphabet $\mathbb{Z}_4$, we shall develop further combinatorial ideas which will provide even more explicit and refined analogs of McEliece's theorem than any developed so far for these codes and, in the process, we prove that these analogs are sharp in a certain sense.

II. Structure of Abelian Codes Over $\mathbb{Z}_{p^d}$

In this section, we develop the mathematical background necessary for the presentation and proof of our results. Most of this material focuses on understanding the structure of Abelian codes over $\mathbb{Z}_{p^d}$ through their Fourier transforms.

A. Abelian Codes and Number Systems

In this paper, the word *integer* will always mean a rational integer, while *p-adic integer* is used for algebraic integers in the p-adics or extensions thereof. $\mathbb{N}$ denotes the set of nonnegative integers. We shall be interested in codes whose alphabet is $\mathbb{Z}_{p^d}$, where p always denotes a prime in $\mathbb{Z}$ and d a positive integer. A denotes a finite Abelian group with $p \nmid |A|$. We shall write the group operation of A multiplicatively and shall denote the identity of A by 1_A or simply by 1 where there is no occasion for confusion. By an *Abelian code over* $\mathbb{Z}_{p^d}$ or a *$\mathbb{Z}_{p^d}$-Abelian code* we mean a $\mathbb{Z}_{p^d}$-algebra ideal of the group ring $\mathbb{Z}_{p^d}[A]$. An element f of $\mathbb{Z}_{p^d}[A]$ is written as a sum $f = \sum_{a \in A} f_a a$ and is often regarded as a function from A into $\mathbb{Z}_{p^d}$. If $g = \sum_{a \in A} g_a a$ is another such element and $r \in \mathbb{Z}_{p^d}$, then the addition, scalar multiplication, and ring multiplication in $\mathbb{Z}_{p^d}[A]$ are given by $(f+g)_a = f_a + g_a$, $(rf)_a = r f_a$, and $(fg)_a = \sum_{b \in A} f_b g_{b^{-1}a}$. This ring multiplication is sometimes called *convolution*. If A is given an ordering, then it is clear that the elements of $\mathbb{Z}_{p^d}[A]$ can be regarded as words of length $|A|$ with symbols in the alphabet $\mathbb{Z}_{p^d}$.

Note that we assume that the order of the group A is coprime to the characteristic p^d of the alphabet. We do this because we intend to make extensive use of the Fourier transform and inverse Fourier transform in an algebra $R[A]$, where R is a ring extension of our alphabet $\mathbb{Z}_{p^d}$. For the usual Fourier transform and its inverse to exist, it is necessary that $|A|$ have a multiplicative inverse in R (see [18, Theorem 3]). Since R is an extension of $\mathbb{Z}_{p^d}$, it is also of characteristic p^d, and so $|A|$ will be invertible in it if and only if $p \nmid |A|$. It is possible in some situations (e.g., in certain repeated-residue cyclic codes) to apply counting polynomial techniques without this restriction on $|A|$, but the methods presented in this paper would need to be modified significantly in such cases.

We will not be content to perform our calculations of codeword weights in the alphabet $\mathbb{Z}_{p^d}$ of our code, since the weights we encounter may exceed p^d. We would like to compute weights in a ring as much like $\mathbb{Z}_{p^d}$ as possible, so we shall use a larger ring that has $\mathbb{Z}_{p^d}$ as one of its quotients. It would seem that $\mathbb{Z}$ is the natural choice for such a ring, but in fact, p-adic numbers have been found to be most suitable for these studies [10], [11]. To this end, we introduce the field of p-adic rational numbers, denoted $\mathbb{Q}_p$, which has characteristic zero. See [19, Ch. II] for a construction of the p-adics and an exposition of their basic properties, some of which we recall here. Also see [9] and [10] for an overview of the p-adics and their uses in the study of cyclic codes over $\mathbb{Z}_{p^d}$. We denote the set p-adic integers in $\mathbb{Q}_p$ by $\mathbb{Z}_{p^\infty}$, a useful if unconventional notation employed in [9]. This prevents a clash with the notation $\mathbb{Z}_p$ for the integers modulo p. $\mathbb{Z}_{p^\infty}$ is a ring of characteristic 0 and contains the rational integers $\mathbb{Z}$, so it is suitable for counting and calculating weights. $\mathbb{Z}_{p^\infty}$ is a local ring with unique nonzero prime ideal $p\mathbb{Z}_{p^\infty}$. All other ideals (except (0)) are powers of this ideal. Furthermore, $\mathbb{Z}_{p^d}$ is the quotient of $\mathbb{Z}_{p^\infty}$ by the ideal $p^d\mathbb{Z}_{p^\infty}$. We define the *p-adic valuation* $v_p \colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ in the usual way, namely, that

$$v_p(r) = \sup\{k \in \mathbb{Z} : r \in p^k \mathbb{Z}_{p^\infty}\}.$$

Then $\mathbb{Z}_{p^\infty}$ is seen to be the set of elements of $\mathbb{Q}_p$ with nonnegative valuation and the units in $\mathbb{Z}_{p^\infty}$ (i.e., elements in $\mathbb{Z}_{p^\infty}$ with a multiplicative inverse in $\mathbb{Z}_{p^\infty}$) are precisely those elements of zero valuation. We also use the p-adic absolute value $|\cdot|_p$ which has $|0|_p = 0$ and $|r|_p = p^{-v_p(r)}$ for $r \neq 0$. This provides a metric on $\mathbb{Q}_p$ which makes it into a metric space with a topology which we call the *p-adic topology*. We shall also make use of the fact that $\mathbb{Z}_{p^\infty}$ contains primitive roots of unity of order $p-1$.

Since McEliece's theorem relates the weights of codewords to their Fourier transforms, we must introduce the Fourier transform to state our analogs. We must first define a ring extension of $\mathbb{Z}_{p^d}$ containing sufficiently many roots of unity to allow for a Fourier transform (cf. [18, Theorem 3] and [8, Theorem 1]). However, just as we do not wish to calculate weights in $\mathbb{Z}_{p^d}$, so we do not want to do so in any ring extension thereof, for such an extension would have characteristic p^d. Therefore, in addition to finding an extension R of $\mathbb{Z}_{p^d}$ with sufficient roots of

unity for the Fourier transform, we would like to find an extension S of $\mathbb{Z}_{p^\infty}$ that has R as its quotient. In fact, we shall start by extending the p-adics. We shall first define an algebraic extension E of $\mathbb{Q}_p$, then obtain our extension S of $\mathbb{Z}_{p^\infty}$ as the ring of elements in E that are integral over $\mathbb{Z}_{p^\infty}$, and finally obtain our extension R of $\mathbb{Z}_{p^d}$ by passing to a quotient of S.

Our idea is to adjoin a root of unity of order $p^\epsilon - 1$ to the field $\mathbb{Q}_p$ and to the ring $\mathbb{Z}_{p^\infty}$, where ϵ is chosen to be large enough that the extended ring and its quotient by the ideal (p^d) will both contain all the roots of unity necessary for Fourier analysis with the group A. The quotient of the extension of $\mathbb{Z}_{p^\infty}$ is called a Galois ring and is an extension of the ring $\mathbb{Z}_{p^d}$. See [20] for properties of Galois rings in general and [6], [8], and [10] for their uses in the study of cyclic codes over $\mathbb{Z}_{p^d}$. See also [21, Sec. I.B] for a brief account of the relationship between p-adic fields and Galois rings, which are used in that paper to construct sequences of low correlation. Although we choose a particular value of ϵ suitable for our purposes, varying ϵ over the positive integers in the discussion below would produce all Galois rings with characteristic p^d. To determine the value of ϵ we need, we choose elements $a_1, a_2, \ldots, a_t$ of A having orders $n_1, n_2, \ldots, n_t$, respectively, so that $n_1 \mid n_2 \mid \cdots \mid n_t$ and so that any element of A has a unique representation as $a_1^{e_1} a_2^{e_2} \cdots a_t^{e_t}$ with $0 \leq e_i < n_i$ for all i. Then let ϵ be the least positive integer so that $p^\epsilon \equiv 1 \pmod{n_t}$.

Let ζ be a root of unity of order $p^\epsilon - 1$ over $\mathbb{Q}_p$. Then $\mathbb{Q}_p(\zeta)$ is a degree ϵ Galois extension of $\mathbb{Q}_p$. See [22, Ch. IV, Proposition 16] for this and many of the properties mentioned below. The group of automorphisms of $\mathbb{Q}_p(\zeta)$ that pointwise fix $\mathbb{Q}_p$ is the cyclic group of order ϵ generated by the automorphism σ which takes ζ to ζ^p. $\mathbb{Z}_{p^\infty}[\zeta]$ is the ring of elements in the field $\mathbb{Q}_p(\zeta)$ that are integral over $\mathbb{Z}_{p^\infty}$. $\mathbb{Z}_{p^\infty}[\zeta]$ has a unique nonzero prime ideal generated by p. All other ideals (except (0)) are powers of this prime ideal. We can extend the domain of the p-adic valuation v_p from $\mathbb{Q}_p$ to $\mathbb{Q}_p(\zeta)$ so that

$$v_p(r) = \sup\{k \in \mathbb{Z} : r \in p^k \mathbb{Z}_{p^\infty}[\zeta]\}.$$

Then $\mathbb{Z}_{p^\infty}[\zeta]$ is seen to be the set of elements in $\mathbb{Q}_p(\zeta)$ with nonnegative valuation and the units of $\mathbb{Z}_{p^\infty}[\zeta]$ (i.e., elements of $\mathbb{Z}_{p^\infty}[\zeta]$ whose multiplicative inverse is in $\mathbb{Z}_{p^\infty}[\zeta]$) are the elements of zero valuation. In this paper, the congruence $a \equiv b \pmod{p^m}$ is equivalent to $v_p(a-b) \geq m$, so that congruences modulo powers of p between elements of $\mathbb{Q}_p(\zeta)$ are meaningful.

Now we define the Galois ring $\mathrm{GR}(p^d, \epsilon)$ to be the quotient of $\mathbb{Z}_{p^\infty}[\zeta]$ by the ideal $p^d \mathbb{Z}_{p^\infty}[\zeta]$. We shall always use π to denote the quotient map from $\mathbb{Z}_{p^\infty}[\zeta]$ to $\mathrm{GR}(p^d, \epsilon)$. The restriction of π to $\mathbb{Z}_{p^\infty}$ is the quotient map from $\mathbb{Z}_{p^\infty}$ to $\mathbb{Z}_{p^d}$. $\mathrm{GR}(p^d, \epsilon)$ is our extension of the ring $\mathbb{Z}_{p^d}$. In fact, $\mathrm{GR}(p^d, \epsilon) = \mathbb{Z}_{p^d}[\pi(\zeta)]$ and $\pi(\zeta)$ is a root of unity of order $p^\epsilon - 1$. Thus, both $\mathbb{Z}_{p^\infty}[\zeta]$ and $\mathrm{GR}(p^d, \epsilon)$ contain primitive roots of unity of order n_i for $0 \leq i \leq t$. Since the automorphism σ of $\mathbb{Z}_{p^\infty}[\zeta]$ maps the ideal $p^d \mathbb{Z}_{p^\infty}[\zeta]$ onto itself, $\mathrm{GR}(p^d, \epsilon)$ has an automorphism induced by σ which fixes the points in $\mathbb{Z}_{p^d}$ and maps $\pi(\zeta)$ to $\pi(\zeta)^p$. By abuse of notation, we denote this automorphism by σ also. We shall call both versions of σ the *Frobenius automorphism*. Then $\pi \circ \sigma = \sigma \circ \pi$, with the former σ being the automorphism on $\mathbb{Z}_{p^\infty}[\zeta]$ and the latter σ being the automorphism on $\mathrm{GR}(p^d, \epsilon)$. We refer to this property as *commutativity of the quotient map with the Frobenius automorphism*. The ideals of $\mathrm{GR}(p^d, \epsilon)$ are generated by p^k with $0 \leq k \leq d$, where we note that $p^d = 0$. Note that if $d = 1$, then $\mathrm{GR}(p^d, \epsilon) = \mathbb{Z}_p[\pi(\zeta)]$ is actually the finite field $\mathrm{GF}(p^\epsilon)$.

We shall analyze the weights of codewords with alphabet $\mathbb{Z}_{p^d} \subseteq \mathrm{GR}(p^d, \epsilon)$, but wish to perform calculations in $\mathbb{Z}_{p^\infty}[\zeta]$, so we shall choose a right-inverse τ of the quotient map π, which we call the *standard lift*. Any element $r \in \mathrm{GR}(p^d, \epsilon)$ can be written uniquely as

$$r = \sum_{i=0}^{d-1} r^{(i)} p^i$$

where each $r^{(i)}$ lies in the set

$$\{\pi(0), \pi(1), \pi(\zeta), \pi(\zeta)^2, \ldots, \pi(\zeta)^{p^\epsilon - 2}\}.$$

Any element $R \in \mathbb{Z}_{p^\infty}[\zeta]$ can be written uniquely as $R = \sum_{i=0}^{\infty} R^{(i)} p^i$ where each $R^{(i)}$ lies in $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^\epsilon - 2}\}$. We call these representations the *canonical expansions* of elements in $\mathrm{GR}(p^d, \epsilon)$ and $\mathbb{Z}_{p^\infty}[\zeta]$. Then the standard lift of r above is the element

$$\tau(r) = \sum_{i=0}^{d-1} R^{(i)} p^i$$

where $R^{(i)} = \zeta^n$ if $r^{(i)} = \pi(\zeta)^n$ and $R^{(i)} = 0$ if $r^{(i)} = \pi(0)$. Note that $\sigma \circ \tau = \tau \circ \sigma$, with the former σ being the automorphism on $\mathbb{Z}_{p^\infty}[\zeta]$ and the latter σ being the automorphism on $\mathrm{GR}(p^d, \epsilon)$. We refer to this property as *commutativity of the standard lift with the Frobenius automorphism*. Another property of τ is that $\tau(r) = 0$ if and only if $r = 0$, so that a function f from some set S to $\mathrm{GR}(p^d, \epsilon)$ has zeroes precisely where $\tau \circ f$ has zeroes. We call this property *preservation of support*, a name which is natural in the light of definitions to be made in Section II-C.

B. Fourier Transform

The Fourier transform for Abelian codes over $\mathbb{Z}_{p^d}$ is presented by Rajan and Siddiqi [8], but we shall try to stay close to the treatment of Delsarte and McEliece [15], who present the Fourier transform for Abelian codes over finite fields. This will help us to compare our analogs of McEliece's theorem with the results of Delsarte and McEliece. The reader should note that in order to ease the presentation of our results, we write our group operation multiplicatively rather than additively and we use a notation slightly different from that of either of the two accounts just cited.

Since we are not working solely with cyclic codes, we cannot use a Fourier transform like that of Mattson and Solomon (i.e., the Mattson–Solomon polynomial in [23]), but must use a version of the more general Fourier transform introduced for Abelian codes by MacWilliams [24]. In this setting, the Fourier transform becomes a function whose domain is the set of characters of the Abelian group A, i.e., the set of group homomorphisms from A into the multiplicative group of an appropriate field. Characters of finite Abelian groups are themselves important in information theory; see [25] for a brief

introduction to complex-valued characters and their use in producing sequences with good correlation properties. The set of characters of A is itself a group isomorphic to A, which is most easily seen by employing the bilinear pairing introduced by Delsarte [26] and used by Delsarte and McEliece [15] in their generalization of McEliece's original theorem. In this way, the Fourier transform becomes a function defined on A rather than on the set of characters of A. We continue to write elements of A in the form $a_1^{e_1}a_2^{e_2}\cdots a_t^{e_t}$ as in Section II-A above. Let $\zeta_i = \zeta^{(p^\epsilon-1)/n_i}$ for $1 \le i \le t$ so that ζ_i is a root of unity of order n_i in $\mathbb{Z}_{p^\infty}[\zeta]$. 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, then define

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

This defines a function $\langle\cdot,\cdot\rangle : A \times A \to \mathbb{Z}_{p^\infty}[\zeta]$. For $a, b, c \in A$ and $n \in \mathbb{Z}$, we have

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

where $\delta_{u,v} = 1$ if $u = v$ and $\delta_{u,v} = 0$, otherwise. Also,

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

These properties are straightforward to verify.

For $f \in \mathbb{Z}_{p^\infty}[\zeta][A]$, we define the Fourier transform of f, written $\hat{f}$, as the function from A to $\mathbb{Z}_{p^\infty}[\zeta]$ with

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

where we are writing the value of the function $\hat{f}$ at the point a as $\hat{f}_a$ rather than in the more usual notation $\hat{f}(a)$. Thus, the Fourier transform maps $\mathbb{Z}_{p^\infty}[\zeta][A]$ into the set $\mathbb{Z}_{p^\infty}[\zeta]^A$ of functions from A to $\mathbb{Z}_{p^\infty}[\zeta]$. It is straightforward to show that the Fourier transform is a bijection from $\mathbb{Z}_{p^\infty}[\zeta][A]$ to $\mathbb{Z}_{p^\infty}[\zeta]^A$ with inverse given by

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

If we consider $\mathbb{Z}_{p^\infty}[\zeta]^A$ as a $\mathbb{Z}_{p^\infty}[\zeta]$-algebra with pointwise addition and multiplication of functions as the ring operations, then the Fourier transform and its inverse are in fact $\mathbb{Z}_{p^\infty}[\zeta]$-algebra isomorphisms from $\mathbb{Z}_{p^\infty}[\zeta][A]$ to $\mathbb{Z}_{p^\infty}[\zeta]^A$ (cf. [8, Theorem 2] and [15, eq. (2.9)]).

Since $f \in p^d\mathbb{Z}_{p^\infty}[\zeta][A]$ if and only if $\hat{f} \in p^d\mathbb{Z}_{p^\infty}[\zeta]^A$, the Fourier transform and its inverse on $\mathbb{Z}_{p^\infty}[\zeta][A]$ and $\mathbb{Z}_{p^\infty}[\zeta]^A$ induce a Fourier transform and inverse Fourier transform on $\mathrm{GR}(p^d,\epsilon)[A]$ and $\mathrm{GR}(p^d,\epsilon)^A$. These transforms could have been constructed directly by replacing ζ_i with $\pi(\zeta_i)$ in the definition of our pairing $\langle\cdot,\cdot\rangle$.

If F is a set of functions, we use $\hat{F}$ to denote $\{\hat{f} : f \in F\}$. It will also be useful in the presentation of our results to introduce a scaled version of the Fourier transform. If $f \in \mathbb{Z}_{p^\infty}[\zeta][A]$ (resp., $\mathrm{GR}(p^d,\epsilon)[A]$), then the *scaled Fourier transform* of f, written $\tilde{f}$, is $\frac{1}{|A|}\hat{f}$. The inversion formula for the scaled Fourier transform is just

$$f_a = \sum_{b\in A} \tilde{f}_b \langle b, a\rangle .$$

Note that $|A|$ is a unit in $\mathbb{Z}_{p^\infty}[\zeta]$ and in $\mathrm{GR}(p^d,\epsilon)$.

We have presented the Fourier transform as a map defined on $\mathrm{GR}(p^d,\epsilon)[A]$, but recall that our codewords are elements $\mathbb{Z}_{p^d}[A]$. We need a characterization of the Fourier transforms of elements of $\mathbb{Z}_{p^d}[A]$ and of $\mathbb{Z}_{p^\infty}[A]$ to shed light on the structure of our Abelian codes and to aid in our proofs of analogs of McEliece's theorem.

Proposition 2.1: (cf. [8, Theorem 3], [15, eq. (2.10)]) Let $f \in \mathbb{Z}_{p^\infty}[\zeta][A]$ (resp., $\mathrm{GR}(p^d,\epsilon)[A]$). Then $f \in \mathbb{Z}_{p^\infty}[A]$ (resp., $\mathbb{Z}_{p^d}[A]$) if and only if $\hat{f}_{a^p} = \sigma(\hat{f}_a)$ for all $a \in A$. Equivalently, $f \in \mathbb{Z}_{p^\infty}[A]$ (resp., $\mathbb{Z}_{p^d}[A]$) if and only if $\tilde{f}_{a^p} = \sigma(\tilde{f}_a)$ for all $a \in A$. Thus, the Fourier transform is an isomorphism of $\mathbb{Z}_{p^d}$-algebras from $\mathbb{Z}_{p^d}[A]$ to the $\mathbb{Z}_{p^d}$-algebra $\mathcal{A}$ consisting of the elements $g \in \mathrm{GR}(p^d,\epsilon)^A$ that meet the condition $g_{a^p} = \sigma(g_a)$.

Proof: The "only if" part of our proposition with $f \in \mathrm{GR}(p^d,\epsilon)[A]$ is Theorem 3 of [8] and the "if" part can be proved in a similar fashion (for the "if and only if" statement see the beginning of [8, Sec. III]). The proof of the version with $f \in \mathbb{Z}_{p^\infty}[\zeta][A]$ is analogous. Since $\sigma(|A|^{-1}) = |A|^{-1}$ both in $\mathrm{GR}(p^d,\epsilon)$ and in $\mathbb{Z}_{p^\infty}[\zeta]$, the version of the proposition with scaled Fourier transforms follows immediately from the version with the usual Fourier transforms. □

Here we record a corollary of this proposition which will be crucial in proving our main result.

Corollary 2.2: Let $f \in \mathbb{Z}_{p^d}[A]$ and let F be the unique element of $\mathbb{Z}_{p^\infty}[\zeta][A]$ so that $\tilde{F} = \tau\circ\tilde{f}$. Then F is in $\mathbb{Z}_{p^\infty}[A]$ with $\pi\circ F = f$.

Proof: By the proposition, we have $\tilde{f}_{a^p} = \sigma(\tilde{f}_a)$ for all $a \in A$. Applying τ to both sides, we have $\tilde{F}_{a^p} = \tau(\sigma(\tilde{f}_a))$ for all $a \in A$. By commutativity of the standard lift with the Frobenius automorphism (see Section II-A), we have $\tilde{F}_{a^p} = \sigma(\tau(\tilde{f}_a))$, i.e., $\tilde{F}_{a^p} = \sigma(\tilde{F}_a)$, for all $a \in A$. Then the proposition shows that $F \in \mathbb{Z}_{p^\infty}[A]$.

If we let $g = |A|^{-1}f$, we have $\tilde{f} = \hat{g}$, and so $\tilde{F} = \tau\circ\hat{g}$. We shall apply the inverse Fourier transform to both sides of this equation and then compose on the left with the quotient map π. Considering the definition of the inverse Fourier transform from $\mathrm{GR}(p^d,\epsilon)^A$ to $\mathrm{GR}(p^d,\epsilon)[A]$ as the map induced by the inverse Fourier transform from $\mathbb{Z}_{p^\infty}[\zeta]^A$ to $\mathbb{Z}_{p^\infty}[\zeta][A]$ *via* reduction modulo p^d, we see that if we apply the inverse Fourier transform to $\tau\circ\hat{g}$ and then compose on the left with π, we get g. If we do the same to $\tilde{F}$, then we get $\pi\circ(|A|^{-1}F) = |A|^{-1}\pi\circ F$. Thus, $|A|^{-1}\pi\circ F = g = |A|^{-1}f$, so that $\pi\circ F = f$. □

We also need another corollary for some of our results on Abelian codes over $\mathbb{Z}_4$.

Corollary 2.3: Let $f \in \mathbb{Z}_{p^d}[A]$ and let F be the unique element of $\mathbb{Z}_{p^\infty}[\zeta][A]$ so that $\tilde{F} = \tau \circ \tilde{f}$. If we write the canonical expansion

$$\tilde{F}_a = \sum_{i=0}^{d-1} \tilde{F}_a^{(i)} p^i$$

for each $a \in A$, then $\tilde{F}_{a^p}^{(i)} = (\tilde{F}_a^{(i)})^p$ for all $a \in A$ and $0 \le i < d$.

Proof: Since $F \in \mathbb{Z}_{p^\infty}[A]$ by the previous corollary, we have $\tilde{F}_{a^p} = \sigma(\tilde{F}_a)$ for all $a \in A$ by the proposition. Taking canonical expansions, we get

$$\sum_{i=0}^{d-1} \tilde{F}_{a^p}^{(i)} p^i = \sum_{i=0}^{d-1} \sigma(\tilde{F}_a^{(i)}) p^i.$$

Since all coefficients in canonical expansions are roots of unity or zero, σ takes them to their pth power, and so

$$\sum_{i=0}^{d-1} \tilde{F}_{a^p}^{(i)} p^i = \sum_{i=0}^{d-1} (\tilde{F}_a^{(i)})^p p^i$$

for all $a \in A$. Uniqueness of canonical expansions finishes the proof. □

Our proposition tells us that if $f \in \mathbb{Z}_{p^d}[A]$, then $\hat{f}_a, \hat{f}_{a^p}, \hat{f}_{a^{p^2}}, \ldots$ are all determined by the value of $\hat{f}_a$. This leads us to define two elements a and b of A to be p *-equivalent* if $a = b^{p^j}$ for some $j \in \mathbb{Z}$, where powers of p are construed to be integers modulo $|A|$. This defines an equivalence relation which partitions A into p*-classes*, and a subset S of A is p *-closed* if it is a union of p-classes (cf. [8, Definition 5] and [15, Sec. 1]). With this terminology, our proposition tells us that for $f \in \mathbb{Z}_{p^d}[A]$, $\hat{f}$ is uniquely determined by its values on a set of p-class representatives. This notion can be elaborated further.

Proposition 2.4: (cf. [8, Theorem 4]) Let R be a set of p-class representatives in A and for each $r \in R$, let ϵ_r be the cardinality of the p-class of r. Then $\epsilon_r \mid \epsilon$ for each r. Let $\mathcal{A}$ be the $\mathbb{Z}_{p^d}$-subalgebra of $\mathrm{GR}(p^d, \epsilon)^A$ as defined in Proposition 2.1. Then restriction of domain from A to R is an isomorphism of $\mathbb{Z}_{p^d}$-algebras from $\mathcal{A}$ to

$$\bigoplus_{r \in R} \mathbb{Z}_{p^d}[\pi(\zeta)^{(p^\epsilon - 1)/(p^{\epsilon_r} - 1)}] = \bigoplus_{r \in R} \mathrm{GR}(p^d, \epsilon_r).$$

Proof: Since the p-class of r has ϵ_r elements, ϵ_r is the minimum positive integer so that $r^{p^{\epsilon_r} - 1} = 1_A$. On the other hand, $p^\epsilon - 1$ is divisible by n_t and all elements in A have order a divisor of n_t, so $r^{p^\epsilon - 1} = 1_A$. So

$$1_A = r^{\gcd(p^{\epsilon_r} - 1, p^\epsilon - 1)} = r^{p^{\gcd(\epsilon_r, \epsilon)} - 1}.$$

By the minimality of ϵ_r, we must have $\epsilon_r \le \gcd(\epsilon_r, \epsilon)$, or equivalently, $\epsilon_r \mid \epsilon$. For the second claim, see [8, Theorem 4]. □

Our two propositions can be combined to give a characterization of the convolution ideals (i.e., codes) in $\mathbb{Z}_{p^d}[A]$.

Theorem 2.5: If R is a set of p-class representatives of A and ϵ_r is the cardinality of the p-class of $r \in R$, then the $\mathbb{Z}_{p^d}$-algebra $\mathbb{Z}_{p^d}[A]$ is isomorphic (*via* Fourier transform followed by restriction of domains to R) to

$$\mathcal{B} = \bigoplus_{r \in R} \mathbb{Z}_{p^d}[\pi(\zeta)^{(p^\epsilon - 1)/(p^{\epsilon_r} - 1)}] = \bigoplus_{r \in R} \mathrm{GR}(p^d, \epsilon_r).$$

This establishes a bijective correspondence between convolution ideals (codes) in $\mathbb{Z}_{p^d}[A]$ and (pointwise) ideals in $\mathcal{B}$, which are of the form $\bigoplus_{r \in R} p^{i_r} \mathrm{GR}(p^d, \epsilon_r)$ with $0 \le i_r \le d$.

Proof: The isomorphism is proved by Propositions 2.1 and 2.4. Recall that ideals in a Galois ring are generated by p^k for $0 \le k \le d$. □

Since pointwise ideals in a direct sum are simple to identify and manipulate, this theorem tells us a great deal about the codes in $\mathbb{Z}_{p^d}[A]$. For instance, all codes in $\mathbb{Z}_{p^d}[A]$ have a single generator and the number of codes is precisely $(d+1)^n$, where n is the the number of p-classes in A. In the next subsection, we shall introduce the notion of *support*, which will provide an economical way of summarizing the content of our theorem.

C. Supports and Accounts

Suppose we have a function f with domain A, e.g., the Fourier transform of a codeword. A *support* of f is any subset S of A so that $f_a = 0$ for $a \notin S$. If our function f takes values in the ring $\mathrm{GR}(p^d, \epsilon)$, then a *support of f modulo p^k* or a p^k*-support* of f is a set S so that $f_a \equiv 0 \pmod{p^k}$ for $a \notin S$. Since $p^d = 0$ in $\mathrm{GR}(p^d, \epsilon)$, a p^d-support is identical to a support. By *minimal* supports or p^k-supports we mean minimal ones under the inclusion relation $\subseteq$. If S_k is a minimal p^k-support of f for $0 \le k \le d$, then the sequence

$$\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$$

is called the *tower of supports* of f.

For $\mathcal{F}$ a set of functions, a *support (resp., p^k -support)* of $\mathcal{F}$ is a set that is simultaneously a support (resp., p^k-support) of all the elements of $\mathcal{F}$. If $\mathcal{F}$ consists of functions mapping into $\mathrm{GR}(p^d, \epsilon)$, it also has a tower of supports formed from its minimal p^k-supports. With this terminology, we may now state the essential content of Theorem 2.5 succinctly in the following corollary.

Corollary 2.6: For each convolution ideal (i.e., code) C in the $\mathbb{Z}_{p^d}$-algebra $\mathbb{Z}_{p^d}[A]$, let $T(C)$ be the tower of supports of $\hat{C}$. Then T is a bijection between the set of codes in $\mathbb{Z}_{p^d}[A]$ and the set of towers $\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$ of p-closed subsets of A.

Proof: Suppose that C is a code. Given any $f \in C$, Proposition 2.1 tells us that $\hat{f}_{a^{p^i}} = \sigma^i(\hat{f}_a)$ for any $a \in A$, $i \in \mathbb{Z}$. Note that for any $r \in \mathrm{GR}(p^d, \epsilon)$, $\sigma(r) \equiv 0 \pmod{p^k}$ if and only if $r \equiv 0 \pmod{p^k}$. So the minimal p^k-support of $\hat{f}$ is p-closed. Thus, the minimal p^k-support of $\hat{C}$ is p-closed and so all the sets in the tower $T(C)$ are p-closed.

On the other hand, given any tower

$$\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$$

of p-closed subsets of A, construct the function γ with domain A so that $\gamma_a = p^k$ if $a \in S_{k+1} \setminus S_k$ for $0 \le k < d$ and $\gamma_a = 0$ if $a \notin S_d$. Thus, γ has $\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$ as

its tower of supports. By Proposition 2.1, this $\gamma = \hat{g}$ for some $g \in \mathbb{Z}_{p^d}[A]$. Let C be the code generated by g in $\mathbb{Z}_{p^d}[A]$. Then an arbitrary element $h = fg$ of C has $\hat{h}_a = \hat{f}_a \gamma_a$ for all $a \in A$, so that the minimal p^k-supports of $\hat{h}$ are no larger than those of γ. Yet $\gamma = \hat{g}$ is in $\hat{C}$, so that the minimal p^k-supports of $\hat{C}$ are those of γ, namely, the tower $\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$.

Finally, fix R a set of p-class representatives of A and suppose that C is a code in $\mathbb{Z}_{p^d}[A]$ with $\emptyset = S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_d$ the tower of supports $T(C)$ of $\hat{C}$. Then let $R_k = R \cap (S_{k+1} \setminus S_k)$ for $0 \leq k < d$ and $R_d = R \setminus S_d$ so that $R_0, R_1, \ldots, R_d$ form a partition of R. Restriction of domains from A to R maps $\hat{C}$ to a pointwise ideal of $\bigoplus_{r \in R} \mathrm{GR}(p^d, \epsilon_r)$ which is of the form $\bigoplus_{r \in R} p^{i_r} \mathrm{GR}(p^d, \epsilon_r)$ with $0 \leq i_r \leq d$.

Now suppose that $r \in R_k$ for $0 \leq k < d$. Then, $r \in S_{k+1}$, so that $\hat{C}$ has some element $\hat{g}$ with $\hat{g}_r \not\equiv 0 \pmod{p^{k+1}}$. Thus $i_r < k+1$. On the other hand $\hat{f}_r \equiv 0 \pmod{p^k}$ for all $f \in C$ since $r \notin S_k$. Thus, $i_r \geq k$ and so $i_r = k$.

Suppose that $r \in R_d$. Then $r \notin S_d$ so that $\hat{f}_r = 0$ for all $f \in C$. So $i_r = d$.

So for any k, we have $i_r = k$ for $r \in R_k$. Thus, the pointwise ideal of $\bigoplus_{r \in R} \mathrm{GR}(p^d, \epsilon_r)$ to which $\hat{C}$ is mapped by restriction of domains is entirely determined by $R_0, R_1, \ldots, R_d$ and these are entirely determined by $T(C)$. Thus, the bijective correspondence of Theorem 2.5 tells us that no two codes in $\mathbb{Z}_{p^d}[A]$ can have the same tower of supports for their Fourier transforms. □

From this corollary we see that Abelian codes over $\mathbb{Z}_{p^d}$ have a greater richness than Abelian codes over the prime field $\mathbb{Z}_p$ in that their Fourier transforms characterize them through a tower of supports rather than a single support set. The single support set which characterizes a code over a finite field is called the *spectrum* in [15].

We have already encountered many subsets of A and functions with domain A in these preliminary investigations into the structure of Abelian codes over $\mathbb{Z}_{p^d}$. To help state and prove combinatorial facts, we define an *account* to be a function from A to $\mathbb{Z}$. If λ is an account, we shall write the value of λ at a as λ_a rather than $\lambda(a)$ and write the accounts as if they are elements of the group ring $\mathbb{Z}[A]$ so that $\lambda = \sum_{a \in A} \lambda_a a$ and so that $c_1 a_1 + c_2 a_2 + \cdots + c_n a_n$ with distinct $a_i \in A$ is the account μ with $\mu_{a_i} = c_i$ for $1 \leq i \leq n$ and $\mu_a = 0$ if $a \notin \{a_1, a_2, \ldots, a_n\}$. Accounts that take only nonnegative values are identified with multisets of A in the obvious way. If $S \subseteq A$, we write $\lambda \Subset S$ to mean that λ is a multiset supported on S. Accounts that take only the values 0 and 1 are identified with subsets of A.

If λ is an account, then define the *size* of λ, denoted $|\lambda|$, to be $\sum_{a \in A} \lambda_a$. If λ is a set or multiset, then $|\lambda|$ is the cardinality. For λ an account, we define the *product* of the account, denoted $\Pi\lambda$, to be $\prod_{a \in A} a^{\lambda_a}$. An account λ with $\Pi\lambda = 1_A$ is said to be a *unity-product* account.

For λ a multiset, $\lambda!$ is a shorthand for $\prod_{a \in A} \lambda_a!$. Thus, there are $\frac{|\lambda|!}{\lambda!}$ ways of ordering the elements of λ. For $f \in \mathbb{Z}_{p^\infty}[\zeta]^A$ and λ a multiset, f_λ is a shorthand for $\prod_{a \in A} f_a^{\lambda_a}$. An account λ supported on $\{1_A\}$ is said to be *all-unity*, otherwise λ is *not all-unity*. We denote the set of all-unity multisets, i.e., $\{k1_A : k \in \mathbb{N}\}$, by 1^*.

D. Weight Functions

In studying codes with alphabet $\mathbb{Z}_{p^d}$, there are many ways of reckoning weights of codewords besides the ubiquitous Hamming weight which assigns all nonzero symbols a weight of 1. For us, a *weight function* is simply a function from our alphabet $\mathbb{Z}_{p^d}$ to $\mathbb{Z}$. For each symbol $s \in \mathbb{Z}_{p^d}$, there is a weight function symb_s which maps s to 1 and all other symbols to 0. We give the special name zer to symb_0 and note that the Hamming weight function ham for symbols is just $1 - \mathrm{zer}$. We also have the Lee weight function lee which takes $s \in \mathbb{Z}_{p^d}$ to $\min_{t \in s} |t|$, where s in the last expression is being regarded as a coset of the ideal $p^d\mathbb{Z}$ in the ring $\mathbb{Z}$. Finally, we have the Euclidean weight function euc, for which $\mathrm{euc}(s) = \mathrm{lee}(s)^2$.

We do not want to compute the weights of letters alone, but rather of codewords. If wt is a weight function and $f \in \mathbb{Z}_{p^d}[A]$, then the *weight* of the codeword f is simply $\sum_{a \in A} \mathrm{wt}(f_a)$, and this will be denoted $\mathrm{wt}(f)$. Then $\mathrm{symb}_s(f)$ is the number of occurrences of the symbol s in the codeword f, $\mathrm{zer}(f)$ is the number of zeroes, and $\mathrm{ham}(f)$, $\mathrm{lee}(f)$, and $\mathrm{euc}(f)$ are, respectively, the Hamming, Lee, and Euclidean weights of f. In this work, our goal is to find the highest power of p dividing the weights of all codewords in a code.

III. The Main Theorem

We are now ready to state the general theorem which can be used to produce our analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_{p^d}$. The proof is a general form of the argument used by Wilson [16], [17].

Theorem 3.1: Let $\mathrm{wt}: \mathbb{Z}_{p^d} \to \mathbb{Z}$ be a weight function. Let $m \geq 1$ be given and suppose that $h(x) = \sum_{j \geq 0} h_j x^j$ is a polynomial in $\mathbb{Q}_p[x]$ with the property that

$$h(s) \equiv \mathrm{wt}(\pi(s)) \pmod{p^m}$$

for all $s \in \mathbb{Z}_{p^\infty}$. Suppose that $f \in \mathbb{Z}_{p^d}[A]$ with S a support of $\hat{f}$. Let F be the unique element of $\mathbb{Z}_{p^\infty}[\zeta][A]$ with $\tilde{F} = \tau \circ \tilde{f}$. Then

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_{1_A}) + \sum_{j>1} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where B_j is the set of all multisets λ supported on S with $|\lambda| = j$, $\Pi\lambda = 1_A$, and λ not all-unity.

Proof: Let us consider an arbitrary codeword $g \in \mathbb{Z}_{p^d}[A]$ and let G be the unique element of $\mathbb{Z}_{p^\infty}[\zeta][A]$ such that $\tilde{G} = \tau \circ \tilde{g}$. Then by Corollary 2.2

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

Another application of Corollary 2.2 shows that $G_a \in \mathbb{Z}_{p^\infty}$ for all $a \in A$, so that our polynomial $h(x)$ can be used on it to approximate $\mathrm{wt} \circ \pi$. Thus,

$$\begin{aligned}\mathrm{wt}(g) &\equiv \sum_{a \in A} h(G_a) \\ &\equiv \sum_{j \geq 0} \sum_{a \in A} h_j (G_a)^j \pmod{p^m}.\end{aligned}$$

Now we write G_a using the inversion formula for the scaled Fourier transform to get

$$\begin{aligned}\mathrm{wt}(g) &\equiv \sum_{j\geq 0}\sum_{a\in A} h_j \left(\sum_{b\in A}\tilde{G}_b\langle b,a\rangle\right)^j \\ &\equiv \sum_{j\geq 0}\sum_{a\in A} h_j \sum_{\substack{\lambda\Subset A\\ |\lambda|=j}} \frac{|\lambda|!}{\lambda!}\prod_{b\in A}\left(\tilde{G}_b\langle b,a\rangle\right)^{\lambda_b} \\ &\equiv \sum_{j\geq 0}\sum_{a\in A} h_j \sum_{\substack{\lambda\Subset A\\ |\lambda|=j}} \frac{|\lambda|!}{\lambda!}\tilde{G}_\lambda\langle \Pi\lambda,a\rangle \\ &\equiv \sum_{j\geq 0} j!h_j \sum_{\substack{\lambda\Subset A\\ |\lambda|=j}} \frac{\tilde{G}_\lambda}{\lambda!}\sum_{a\in A}\langle \Pi\lambda,a\rangle \\ &\equiv |A|\sum_{j\geq 0} j!h_j \sum_{\substack{\lambda\Subset A,|\lambda|=j\\ \Pi\lambda=1}}\frac{\tilde{G}_\lambda}{\lambda!} \pmod{p^m}.\end{aligned}$$

Now regard the last expression as a polynomial with coefficients in $\mathbb{Q}_p$ and variables in $\{\tilde{G}_a : a\in A\}$. If we segregate all terms that only have the variable $\tilde{G}_{1_A}$, we get

$$\mathrm{wt}(g)\equiv \rho(\tilde{G}_{1_A}) + |A|\sum_{j>1} j!h_j \sum_{\substack{\lambda\Subset A,|\lambda|=j\\ \Pi\lambda=1,\lambda\not\in 1^*}}\frac{\tilde{G}_\lambda}{\lambda!} \pmod{p^m} \tag{1}$$

where $\rho(x)$ is some polynomial in $\mathbb{Q}_p[x]$ and we begin the sum in j at $j=2$ because any unity-product multiset with less than two elements must be all-unity.

Now vary g over all words for which $\hat{g}$ is supported on $\{1_A\}$. By the preservation of support by τ (see Section II-A), $\tilde{G}=\tau\circ\tilde{g}$ will be supported on $\{1_A\}$ for all such words. So the second term of the right-hand side of (1) vanishes for these words. Such words have $g_a=\tilde{g}_{1_A}$ for all a and so have $\mathrm{wt}(g)=|A|\mathrm{wt}(\tilde{g}_{1_A})$. Thus, we have

$$|A|\mathrm{wt}(\tilde{g}_{1_A})\equiv\rho(\tilde{G}_{1_A}) \pmod{p^m}$$

for all words with Fourier transform supported on $\{1_A\}$. But for these words, $\tilde{g}_{1_A}$ varies over all of $\mathbb{Z}_{p^d}$. So

$$|A|\mathrm{wt}(r)\equiv\rho(\tau(r)) \pmod{p^m},\qquad \text{for all } r\in\mathbb{Z}_{p^d}.$$

Now recognize that any word $g\in\mathbb{Z}_{p^d}[A]$, regardless of the support of its Fourier transform, will have $\tilde{g}_{1_A}\in\mathbb{Z}_{p^d}$. Since $\tilde{G}_{1_A}=\tau(\tilde{g}_{1_A})$, we can replace the first term on the right-hand side of congruence (1) with $|A|\mathrm{wt}(\tilde{g}_{1_A})$ to obtain

$$\frac{1}{|A|}\mathrm{wt}(g)\equiv\mathrm{wt}(\tilde{g}_{1_A})+\sum_{j>1} j!h_j\sum_{\substack{\lambda\Subset A,|\lambda|=j\\ \Pi\lambda=1,\lambda\not\in 1^*}}\frac{\tilde{G}_\lambda}{\lambda!} \pmod{p^m}.$$

Now let us suppose that $\hat{g}$ is supported on a subset S of A and that $a\in A$ but $a\not\in S$. Then $\hat{g}_a=0$, so that $\tilde{g}_a=0$ and so $\tilde{G}_a=0$ by preservation of support by τ. So if $\lambda\Subset A$ with $\lambda_a\neq 0$, then $\tilde{G}_\lambda=0$. Thus, the previous congruence becomes

$$\frac{1}{|A|}\mathrm{wt}(g)\equiv\mathrm{wt}(\tilde{g}_{1_A})+\sum_{j>1} j!h_j\sum_{\substack{\lambda\Subset S,|\lambda|=j\\ \Pi\lambda=1,\lambda\not\in 1^*}}\frac{\tilde{G}_\lambda}{\lambda!} \pmod{p^m},$$

which is what we were to prove. □

To use this theorem at all, we need to find a polynomial $h(x)$ in $\mathbb{Q}_p[x]$ with the property that $h(s)\equiv\mathrm{wt}(\pi(s)) \pmod{p^m}$ for all $s\in\mathbb{Z}_{p^\infty}$. To use this theorem to the greatest effect, we would like the degree of h to be as low as possible so that fewer nonzero terms appear in the approximation of $\mathrm{wt}(f)$. Therefore, we dedicate the next section to finding such polynomials. We close this section with some examples to show how this Main Theoremcan be used to calculate 2-adic estimates of weights of codewords in cyclic codes over $\mathbb{Z}_4$.

Example 3.2: Let A be the cyclic group of order 7 generated by an element a and let C be the code in $\mathbb{Z}_4[A]$ consisting of all words whose Fourier transforms are supported on $S=\{a,a^2,a^4\}$. In a more conventional presentation of cyclic codes, this is a code in $\mathbb{Z}_4[x]/(x^7-1)$ whose check polynomial is one of the irreducible factors of $\frac{x^7-1}{x-1}$ of degree 3, either $u(x)=x^3-x^2+2x-1$ or $v(x)=x^3+2x^2+x-1$. Equivalently, it is the code generated either by $(x-1)v(x)$ or by $(x-1)u(x)$. We are interested in the Euclidean weights of words.

We note that the polynomial $h(x)=x^2$ has the property that

$$h(u+4v)\equiv u^2 \pmod 8,\qquad \text{for all } u,v\in\mathbb{Z}_{2^\infty}.$$

Thus,

$$h(s)\equiv\mathrm{euc}(\pi(s)) \pmod 8,\qquad \text{for all } s\in\mathbb{Z}_{2^\infty}.$$

Later, in Example 4.24, we will see the motivation for choosing x^2 to approximate Euclidean weight. Let f be any codeword in C and set F so that $\tilde{F}=\tau\circ\tilde{f}$. Then the Main Theorem tells us that

$$\frac{1}{7}\mathrm{euc}(f)\equiv\mathrm{euc}(\tilde{f}_{1_A})+2!\sum_{\lambda\in B_2}\frac{\tilde{F}_\lambda}{\lambda!} \pmod 8$$

where B_2 is the set of all multisets λ supported on S with $|\lambda|=2$, $\Pi\lambda=1_A$, and λ not all-unity. Note that (a,a^2,a^4) is a sequence of three elements in S with product unity and also note that there is no sequence of two elements in S with product unity. Thus, $B_2=\emptyset$ and the minimum length of a unity-product and not all-unity sequence of elements in S is $\ell=3$. Furthermore, 1_A is not an element of S, so $\tilde{f}_{1_A}=0$. Thus, $\frac{1}{7}\mathrm{euc}(f)\equiv 0 \pmod 8$, so that all words in C have Euclidean weight divisible by 8. Note that this specific calculation gives us more information than we would get from [10, Corollary 3.6], which tells us that Euclidean weights of words in C are divisible by $2^{\lceil\frac{\ell}{2}\rceil}=4$. □

Example 3.3: Let the group A generated by a, the subset S of A, and the code C be as described in the previous example. Now we are interested in Lee weights.

Consider the polynomial $h(x)=\frac{1}{3}(x+3x^2-x^3)$. We claim that

$$h(s)\equiv\mathrm{lee}(\pi(s)) \pmod 4,\qquad \text{for all } s\in\mathbb{Z}_{2^\infty}.$$

The origin of this polynomial will be made clear later in Example 4.17, when we have a theory of counting polynomials. For now, we will prove the claim we made. Note that $h(0)=0$, $h(1)=1$, $h(2)=2$, and $h(3)=1$, so that $h(s)=\mathrm{lee}(\pi(s))$ for $s\in\{0,1,2,3\}$. Since we have proved that $h(x)$ takes the appropriate values on a set of representatives of the equivalence classes modulo 4 in $\mathbb{Z}_{2^\infty}$, it suffices to show that $h(u')\equiv h(u)$

$(\mathrm{mod}\ 4)$ whenever $u', u \in \mathbb{Z}_{2^\infty}$ with $u' \equiv u \pmod 4$. One can calculate that $h(u+4v) - h(u)$ equals

$$\frac{4}{3}(v + 6uv + 12v^2 - 3u^2v - 12uv^2 - 16v^3).$$

Since $\frac{1}{3}$ is a 2-adic integer, the right-hand side always vanishes modulo 4 if $u, v \in \mathbb{Z}_{2^\infty}$. Thus, we have proved that $h(x)$ approximates $\mathrm{lee} \circ \pi$ modulo 4 on all of $\mathbb{Z}_{2^\infty}$.

Write our polynomial as $h(x) = \sum_{j=0}^{3} h_j x^j$. Let f be any codeword in C and set F so that $\tilde{F} = \tau \circ \tilde{f}$. Then the Main Theorem tells us that

$$\frac{1}{7}\mathrm{lee}(f) \equiv \mathrm{lee}(\tilde{f}_{1_A}) + \sum_{j=2}^{3} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod 4$$

where B_j is the set of all multisets λ supported on S with $|\lambda| = j$, $\Pi\lambda = 1_A$, and λ not all-unity. In the previous example, we saw that $B_2 = \emptyset$. Note that the set S itself, which can be written in account form as $S = a + a^2 + a^4$, is an element of B_3. It is not hard to prove that this is the only element of B_3. So

$$\frac{1}{7}\mathrm{lee}(f) \equiv \mathrm{lee}(\tilde{f}_{1_A}) + 3! h_3 \frac{\tilde{F}_S}{S!} \pmod 4.$$

Note that 1_A is not an element of S, so $\tilde{f}_{1_A} = 0$. Also, $h_3 = -\frac{1}{3}$ and $S! = 1$, so we obtain

$$\frac{1}{7}\mathrm{lee}(f) \equiv -2\tilde{F}_S \pmod 4,$$

and so

$$\mathrm{lee}(f) \equiv -14\tilde{F}_a \tilde{F}_{a^2} \tilde{F}_{a^4} \pmod 4.$$

Since the 2-class of a is the set $S = \{a, a^2, a^4\}$ of cardinality 3, the scaled Fourier coefficient $\tilde{f}_a$ parameterizes the code as it ranges over $\mathrm{GR}(4,3)$ (see Theorem 2.5). The coefficients $\tilde{F}_{a^{2^j}} = \tau(\tilde{f}_{a^{2^j}})$ are therefore elements of the ring $\mathbb{Z}_{2^\infty}[\zeta]$, where ζ is a root of unity of order $2^3 - 1 = 7$. Write canonical expansions $\tilde{F}_{a^{2^j}} = \tilde{F}^{(0)}_{a^{2^j}} + 2\tilde{F}^{(1)}_{a^{2^j}}$ and note that each $\tilde{F}^{(i)}_{a^{2^j}}$ ranges over the set $\{0, 1, \zeta, \zeta^2, \ldots, \zeta^6\}$, so that $\tilde{F}_{a^{2^j}}$ takes 64 different values for the 64 different codewords. Using these expansions in our congruence and reducing modulo 4, we obtain

$$\mathrm{lee}(f) \equiv 2\tilde{F}^{(0)}_a \tilde{F}^{(0)}_{a^2} \tilde{F}^{(0)}_{a^4} \pmod 4.$$

Now apply Corollary 2.3 to get

$$\mathrm{lee}(f) \equiv 2\left(\tilde{F}^{(0)}_a\right)^7 \pmod 4.$$

So

$$\mathrm{lee}(f) \equiv 0 \pmod 4, \qquad \text{if } \tilde{F}^{(0)}_a = 0$$

and

$$\mathrm{lee}(f) \equiv 2 \pmod 4, \qquad \text{if } \tilde{F}^{(0)}_a \in \{1, \zeta, \ldots, \zeta^6\}.$$

Note that the Lee weight modulo 4 is independent of $\tilde{F}^{(1)}_a \in \{0, 1, \zeta, \ldots, \zeta^6\}$. Thus, there are eight words with Lee weight divisible by 4 and 56 words with Lee weight congruent to 2 modulo 4. Since the minimum length of a unity-product and not all-unity sequence of elements in S is $\ell = 3$, both Corollary 3.6 of [10] and Theorem 2 of [16] (quoted in the Introduction) predict that codewords have even Lee weights. This calculation goes beyond these theorems by showing that they are sharp (that is, some words do not have weight divisible by 4). Our calculation even tells us how many codewords do not have weights divisible by 4. □

These examples show how one can employ our Main Theorem when given appropriate counting polynomials, but they do not explain how these polynomials are found. The discovery of such polynomials is undertaken in the next section.

IV. Polynomial Approximations of Lifted Weight Functions

If $\mathrm{wt} : \mathbb{Z}_{p^d} \to \mathbb{Z}$ is a weight function, then we call

$$\mathrm{wt} \circ \pi : \mathbb{Z}_{p^\infty} \to \mathbb{Z}$$

a lifted weight function. A polynomial $h(x) \in \mathbb{Q}_p[x]$ is said to *approximate* $\mathrm{wt} \circ \pi$ *(uniformly) modulo* p^m if $h(r) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_{p^\infty}$. Here we determine minimum degree approximating polynomials for typical lifted weight functions. Many of these forthcoming results on Lee weight functions (for $\mathbb{Z}_{2^d}$) and symbol-counting weight functions (for all $\mathbb{Z}_{p^d}$) have been obtained by Wilson [16], [17], [27], using calculations in quotients of polynomial rings. The following presentation also considers Lee weight functions for $\mathbb{Z}_{p^d}$ when p is odd and Euclidean weight functions. We also sharpen some of Wilson's existing results in areas critical for our use of the Main Theorem and shall obtain both the old and new results by a method which is different from that of Wilson and interesting in its own right.

A. Newton Expansions

In order to study polynomials that are used to p-adically approximate lifted weight functions, we introduce the Newton expansion of a function from $\mathbb{N}$ to $\mathbb{Z}_{p^\infty}$. This is an expansion of the function as an infinite series in terms of the polynomials

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}, \qquad \text{for } n \in \mathbb{N}.$$

The following proposition summarizes the most fundamental properties of the Newton expansion.

Proposition 4.1: For any sequence $(c_i)_{i \in \mathbb{N}}$ of elements of $\mathbb{Z}_{p^\infty}$, the infinite series

$$c(x) = \sum_{i \in \mathbb{N}} c_i \binom{x}{i}$$

defines a function from $\mathbb{N}$ to $\mathbb{Z}_{p^\infty}$. Given any function $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$, there exists a unique sequence $(f_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}_{p^\infty}$ such that

$$f(n) = \sum_{i \in \mathbb{N}} f_i \binom{n}{i} \tag{2}$$

for all $n \in \mathbb{N}$. The truncation

$$\sum_{i=0}^{m} f_i \binom{n}{i}$$

is the unique polynomial in n of degree less than or equal to m that agrees with f on the set $\{0, 1, \ldots, m\}$.

We call the infinite series (2) the *Newton expansion* of the function f and the coefficients f_i are called the *Newton coefficients*. If f is a function whose domain contains $\mathbb{N}$ we may speak of the Newton expansion of $f\,|_{\mathbb{N}}$, which we shall simply call the Newton expansion of f. The proof of this proposition is routine, depending almost entirely on the fact that $\binom{n}{n} = 1$ and $\binom{n}{i} = 0$ when $i > n$. This proves that the Newton expansion, when evaluated at a nonnegative integer, has only finitely many nonzero terms. It also means that if we are trying to determine the coefficients of the expansion of some function f, they can be computed recursively by setting $f_i = f(i) - \sum_{j=0}^{i-1} f_j \binom{i}{j}$ for all $i \geq 0$. The following corollary to our proposition is also easy to prove.

Corollary 4.2: Let $m \geq 1$ and $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$. Then f is a function that vanishes modulo p^m on all of $\mathbb{N}$ if and only if all its Newton coefficients vanish modulo p^m.

Given a weight function $\mathrm{wt} : \mathbb{Z}_{p^d} \to \mathbb{Z}$, our approach to finding a low-degree polynomial approximating $\mathrm{wt} \circ \pi$ modulo p^m will be to consider the Newton expansion of $\mathrm{wt} \circ \pi$ and then to truncate the infinite series so that every coefficient in the tail removed vanishes modulo p^m. If this can be done, then Corollary 4.2 tells us that we shall have an approximation of $\mathrm{wt} \circ \pi|_{\mathbb{N}}$ modulo p^m. The following Proposition shows that the approximation holds good on the larger domain $\mathbb{Z}_{p^\infty}$ and tells us more about all possible polynomial approximations.

Proposition 4.3: Let $f : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^\infty}$ be a p-adically continuous function and let

$$\sum_{i \in \mathbb{N}} f_i \binom{x}{i}$$

be the Newton expansion of f. Suppose that there is some $i_0 \in \mathbb{N}$ such that $v_p(f_{i_0}) < m$ and $v_p(f_i) \geq m$ for all $i > i_0$. Then there exists a polynomial $h(x) \in \mathbb{Q}_p[x]$ of degree i_0 such that

$$h(r) \equiv f(r) \pmod{p^m} \tag{3}$$

for all $r \in \mathbb{Z}_{p^\infty}$. One such polynomial is given by the truncation

$$g(x) = \sum_{i=0}^{i_0} f_i \binom{x}{i}.$$

No polynomial of degree less than i_0 can satisfy (3) for all $r \in \mathbb{Z}_{p^\infty}$. Any polynomial $h(x) = \sum_{i=0}^{i_0} h_i x^i$ of minimal degree satisfying (3) has $i_0! h_{i_0} \equiv f_{i_0} \pmod{p^m}$ and if $p \neq 2$ or if i_0 is odd, then it also has

$$(i_0 - 1)! h_{i_0 - 1} \equiv -\frac{i_0 - 1}{2} f_{i_0} + f_{i_0 - 1} \pmod{p^m}.$$

Proof: By Corollary 4.2, $g(x)$ and $f(x)$ agree modulo p^m on the set $\mathbb{N}$. Since g (being a polynomial) and f are both p-adically continuous, since they agree modulo p^m on the set $\mathbb{N}$ which is dense in $\mathbb{Z}_{p^\infty}$, and since the ideal (p^m) in $\mathbb{Z}_{p^\infty}$ is closed, we must have $f(r) \equiv g(r) \pmod{p^m}$ for all $r \in \mathbb{Z}_{p^\infty}$.

Suppose that $h(x)$ is a polynomial satisfying (3) for all $r \in \mathbb{Z}_{p^\infty}$. Then we can write the Newton expansion

$$h(x) = \sum_{i \in \mathbb{N}} c_i \binom{x}{i}$$

which is in actuality a finite sum. By Corollary 4.2, we must have $c_{i_0} \equiv f_{i_0} \pmod{p^m}$ so that $c_{i_0} \not\equiv 0 \pmod{p^m}$ and so $\deg(h) \geq i_0$. Now suppose further that $h(x)$ is of degree i_0. Then matching coefficients in

$$\sum_{i=0}^{i_0} h_i x^i = h(x) = \sum_{i=0}^{i_0} c_i \binom{x}{i}$$

we obtain

$$h_{i_0} = \frac{c_{i_0}}{i_0!}$$

and

$$\begin{aligned} h_{i_0 - 1} &= \frac{c_{i_0 - 1}}{(i_0 - 1)!} + \frac{c_{i_0}}{i_0!} \sum_{j=0}^{i_0 - 1} (-j) \\ &= \frac{c_{i_0 - 1}}{(i_0 - 1)!} - \frac{c_{i_0}}{(i_0 - 1)!} \cdot \frac{i_0 - 1}{2}. \end{aligned}$$

So $i_0! h_{i_0} = c_{i_0}$ and

$$(i_0 - 1)! h_{i_0 - 1} = c_{i_0 - 1} - \frac{i_0 - 1}{2} c_{i_0}.$$

By Corollary 4.2, $c_i \equiv f_i \pmod{p^m}$ for all i. This proves that $i_0! h_{i_0} \equiv f_{i_0} \pmod{p^m}$. It also proves that

$$(i_0 - 1)! h_{i_0 - 1} \equiv f_{i_0 - 1} - \frac{i_0 - 1}{2} f_{i_0} \pmod{p^m}$$

provided that $\frac{i_0 - 1}{2} \in \mathbb{Z}_{p^\infty}$. This condition is certainly fulfilled if $p \neq 2$ or if i_0 is odd. □

If $\mathrm{wt} : \mathbb{Z}_{p^d} \to \mathbb{Z}$ is a weight function then $\mathrm{wt} \circ \pi$ will be periodic with period p^d, since π is reduction modulo p^d. This prompts us to study the effect of translation on the Newton expansion, which is summarized in the next proposition. We use the convention that $\binom{x}{i} = 0$ if $i < 0$ in the rest of this paper.

Proposition 4.4: Let $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$ have Newton expansion $f(x) = \sum_{i \in \mathbb{N}} f_i \binom{x}{i}$. For $\ell \in \mathbb{N}$, the translated function $f(x + \ell)$ has Newton expansion

$$f(x + \ell) = \sum_{i \in \mathbb{N}} \left(\sum_{j=0}^{\ell} \binom{\ell}{j} f_{i+j} \right) \binom{x}{i}.$$

Proof: This follows from Pascal's identity

$$\binom{x+1}{i} = \binom{x}{i} + \binom{x}{i-1}$$

iterated ℓ times to produce

$$\binom{x + \ell}{i} = \sum_{j=0}^{\ell} \binom{\ell}{j} \binom{x}{i - j}.$$

The proposition follows from plugging this in for $\binom{x+\ell}{i}$ in the expansion

$$f(x + \ell) = \sum_{i \in \mathbb{N}} f_i \binom{x + \ell}{i}$$

and rearranging the sum to collect all terms involving $\binom{x}{i}$ with a particular value of i. Because we are dealing with functions on

$\mathbb{N}$, all series involved are actually finite sums when evaluated at a point, so this rearrangement is possible. □

We now introduce the finite difference operators Δ_j. If f is a function whose domain is $\mathbb{N}$ or $\mathbb{Z}_{p^\infty}$, then $(\Delta_j f)(x) = f(x+j) - f(x)$. We also introduce the operator Σ_j, for which $(\Sigma_j f)(x) = f(x+j) + f(x)$. The Newton expansion is apt for problems involving such operators, particularly Δ_1, as the following proposition shows.

Proposition 4.5: If $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$ has Newton expansion $\sum_{i\in\mathbb{N}} f_i\binom{x}{i}$, then $\Delta_1 f$ has Newton expansion $\sum_{i\in\mathbb{N}} f_{i+1}\binom{x}{i}$. If $\Delta_1 f$ has Newton expansion $\sum_{i\in\mathbb{N}} g_i\binom{x}{i}$, then f has Newton expansion $f(0) + \sum_{i\geq 1} g_{i-1}\binom{x}{i}$.

Proof: The first statement comes from calculating $f(x+1) - f(x)$ using Proposition 4.4. The second statement comes from setting

$$h(x) = f(0) + \sum_{i\geq 1} g_{i-1}\binom{x}{i}$$

and noting that $\Delta_1 h = \Delta_1 f$ and $h(0) = f(0)$, so that $h = f$. □

B. Periodic Functions

We wish to approximate functions of the form $\mathrm{wt}\circ\pi$ where $\mathrm{wt} : \mathbb{Z}_{p^d} \to \mathbb{Z}$ is a weight function. Such functions will of course be periodic with period p^d, i.e., constant on cosets of the ideal (p^d) in $\mathbb{Z}_{p^\infty}$. Since these cosets are open in the p-adic topology, $\mathrm{wt}\circ\pi$ will always be p-adically continuous. It will be worthwhile to see what properties all p^d-periodic functions have in common with regard to their Newton expansions. The following theorem tells us how quickly the coefficients of the Newton expansion must diminish in p-adic magnitude (equivalently, how quickly they must increase in p-adic valuation). Furthermore, it tells us more about the Newton expansions of characteristic functions of cosets of the ideal (p^d) in $\mathbb{Z}_{p^\infty}$, from which functions we can form any function of period p^d by linear combination.

Theorem 4.6: (cf. Wilson [17, Lemma 1]) Let $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$ be periodic with period p^d. Suppose that $\sum_{i\in\mathbb{N}} f_i\binom{n}{i}$ is the Newton expansion of f. Then for any $m \geq 0$, and $i \geq [m(p-1)+1]p^{d-1}$, we have $v_p(f_i) \geq m$. Suppose further that f is the restriction to $\mathbb{N}$ of the characteristic function of some coset of the ideal (p^d) in $\mathbb{Z}_{p^\infty}$. Then for any $m \geq 1$ and $i = [m(p-1)+1]p^{d-1} - 1$, we have $f_i \equiv (-p)^{m-1} \pmod{p^m}$.

In order to prove this theorem, we first investigate a recursion which must hold for the coefficients in the Newton expansion of any function with period p^d.

Proposition 4.7: Let $f : \mathbb{N} \to \mathbb{Z}_{p^\infty}$ be periodic with period p^d and with Newton expansion $f(n) = \sum_{i\in\mathbb{N}} f_i\binom{n}{i}$. Then

$$f_i = -\sum_{j=i-p^d+1}^{i-1} f_j \binom{p^d}{i-j}$$

for all $i \geq p^d$.

Proof: By periodicity, $f(n+p^d) - f(n) = 0$ for all n. Applying Proposition 4.4, we obtain

$$\begin{aligned} 0 &= \sum_{i\in\mathbb{N}} \left(\sum_{j=0}^{p^d} f_{i+j}\binom{p^d}{j}\binom{n}{i} \right) - \sum_{i\in\mathbb{N}} f_i\binom{n}{i} \\ &= \sum_{i\in\mathbb{N}} \sum_{j=1}^{p^d} f_{i+j}\binom{p^d}{j}\binom{n}{i} \end{aligned}$$

for all $n \in \mathbb{N}$. By the uniqueness of Newton expansions (Proposition 4.1), we conclude that

$$\sum_{j=1}^{p^d} f_{i+j}\binom{p^d}{j} = 0$$

for all $i \in \mathbb{N}$. From this we obtain the recursion which we were to show. □

Knowing this recursion will enable us to estimate p-adic valuations of the coefficients in the Newton expansion of periodic functions. However, to do this we need to have some idea of the p-adic valuations of the numbers $\binom{p^d}{j}$ for $0 < j < p^d$. The following lemma provides what we need in this area.

Lemma 4.8: For any integer j with $0 < j < p^d$ and $v_p(j) \leq d-2$, we have

$$\binom{p^d}{j} \equiv 0 \pmod{p^2}.$$

For any integer k with $0 < k < p$, we have

$$\binom{p^d}{kp^{d-1}} \equiv \binom{p}{k} \not\equiv 0 \pmod{p^2}$$

but $\binom{p}{k} \equiv 0 \pmod{p}$. Furthermore,

$$\binom{p^d-1}{\ell} \equiv (-1)^\ell \pmod{p}, \qquad \text{if } 0 \leq \ell \leq p^d - 1.$$

Proof: It is a well-known fact that $\binom{p}{k} \equiv 0 \pmod{p}$ for $0 < k < p$. This is equivalent to $(x+1)^p \equiv x^p + 1 \pmod{p}$. That $\binom{p}{k} \not\equiv 0 \pmod{p^2}$ for $0 < k < p$ is evident from the fact that $p^2 \nmid p!$.

If we can show that

$$(x+1)^{p^n} \equiv (x^{p^{n-1}} + 1)^p \pmod{p^2}, \qquad \text{for all } n \geq 1$$

then setting $n = d$ and comparing coefficients on either side, we see that we shall have proved both statements about $\binom{p^d}{i}$ for $0 < i < p^d$. We proceed by induction on n. For $n = 1$, the result is immediate. Suppose now that $n > 1$ and we know that $(x+1)^{p^{n-1}} \equiv (x^{p^{n-2}} + 1)^p \pmod{p^2}$. Then

$$\begin{aligned} (x+1)^{p^n} &\equiv (x^{p^{n-2}} + 1)^{p^2} \\ &\equiv (x^{p^{n-1}} + 1 + pg(x))^p \pmod{p^2} \end{aligned}$$

for some $g(x) \in \mathbb{Z}[x]$. Then

$$(x+1)^{p^n} \equiv \sum_{i=0}^{p} \binom{p}{i} (x^{p^{n-1}} + 1)^{p-i} (pg(x))^i \pmod{p^2}$$

and note that all terms but the $i = 0$ term vanish modulo p^2, giving the result we need to complete the induction.

To prove the statements about $\binom{p^d-1}{\ell}$, we shall show that

$$(x-1)^{p^d-1} \equiv \sum_{i=0}^{p^d-1} x^i \pmod{p}. \tag{4}$$

We know that

$$(x-1)^{p^d} \equiv x^{p^d} - 1 \pmod{p}$$

and note that $x-1$ divides the polynomials on both sides of this congruence. p and $x-1$ are distinct irreducible elements in the unique factorization domain $\mathbb{Z}[x]$, so we can divide through by $x-1$ to obtain (4). □

Now we are ready to prove the theorem with which we began this section.

Proof of Theorem 4.6: For now assume only that f has period p^d. We shall prove the lower bound on $v_p(c_i)$ by induction on i. Of course, $v_p(f_i) \geq 0$ for all i since the f_i are p-adic integers by Proposition 4.1. So let $i \geq p^d$ and assume that the lower bound on $v_p(f_j)$ holds for coefficients f_j with $j < i$. Let m be the positive integer so that

$$[m(p-1)+1]\,p^{d-1} \leq i < [(m+1)(p-1)+1]\,p^{d-1}.$$

Then, by Proposition 4.7, we have

$$f_i = -\sum_{j=i-p^d+1}^{i-1} f_j \binom{p^d}{i-j}. \tag{5}$$

Let us examine the terms of the sum for various values of j. For all j in the sum, we have

$$j > i-p^d \geq [m(p-1)+1]\,p^{d-1} - p^d \geq [(m-2)(p-1)+1]\,p^{d-1}.$$

Suppose $j < [(m-1)(p-1)+1]\,p^{d-1}$. Then we have $v_p(f_j) \geq m-2$ by induction (unless $m = 1$, in which case this conclusion is true anyway because all f_j are p-adic integers). Note that $(p-1)p^{d-1} < i - j < p^d$, so that $v_p(i-j) \leq d-2$ and so $v_p\binom{p^d}{i-j} \geq 2$ by Lemma 4.8. Thus, all terms $f_j\binom{p^d}{i-j}$ of (5) indexed by these values of j vanish modulo p^m.

If $j \geq [(m-1)(p-1)+1]p^{d-1}$, then we have $v_p(f_j) \geq m-1$ by induction. Note that $v_p\binom{p^d}{i-j} \geq 1$ for all of the j in our sum by Lemma 4.8. So all terms $f_j\binom{p^d}{i-j}$ of (5) indexed by these values of j vanish modulo p^m.

Therefore, all terms in the sum in (5) vanish modulo p^m and so $v_p(f_i) \geq m$. This completes our inductive proof.

Now let us suppose further that f is the characteristic function of some coset of the ideal (p^d) in $\mathbb{Z}_{p^\infty}$. Write the coset as $n_0 + (p^d)$ for some $n_0 \in \mathbb{Z}$ with $0 \leq n_0 < p^d$. We shall prove the additional claim made for the coefficient $f_{[m(p-1)+1]p^{d-1}-1}$ by induction on m. First consider $m = 1$. If we consider the sum

$$\sum_{i=0}^{p^d-1} f_i \binom{x}{i}$$

of the first p^d terms of the Newton expansion of f, then Proposition 4.1 tells us that this is the polynomial of degree less than or equal to p^d-1 which vanishes on every point of $\{0, 1, \ldots, p^d-1\}$ except n_0, where it has value 1. So it must be the polynomial

$$\prod_{\substack{0 \leq i < p^d \\ i \neq n_0}} \frac{x-i}{n_0-i}$$

which has leading coefficient

$$\frac{(-1)^{p^d-n_0-1}}{n_0!(p^d-n_0-1)!}.$$

Thus, we can deduce that $f_{p^d-1} = (-1)^{p^d-n_0-1}\binom{p^d-1}{n_0}$. Then, by Lemma 4.8, we have $f_{p^d-1} \equiv (-1)^{p^d-1} \equiv 1 \pmod{p}$. Now suppose $m > 1$ and that the claim holds for all pertinent f_j with $j < [m(p-1)+1]p^{d-1}-1$. Now apply (5) specifically to $i = [m(p-1)+1]p^{d-1}-1$. The terms with

$$j > i-(p-1)p^{d-1} = [(m-1)(p-1)+1]p^{d-1} - 1$$

have $v_p(f_j) \geq m-1$ by the first half of this theorem. Also, $v_p\binom{p^d}{i-j} \geq 1$ for all j in the sum (Lemma 4.8), so that the terms $f_j\binom{p^d}{i-j}$ of (5) indexed by $j > i-(p-1)p^{d-1}$ vanish modulo p^m. The terms with $i-p^d < j < i-(p-1)p^{d-1}$ have $v_p(f_j) \geq m-2$ by the first half of this theorem. Also, $v_p\binom{p^d}{i-j} \geq 2$ for such j by Lemma 4.8, so that the terms $f_j\binom{p^d}{i-j}$ of (5) indexed by such j vanish modulo p^m. So the only term in (5) that might not vanish modulo p^m is the one where $j = i-(p-1)p^d$. Thus,

$$f_i \equiv -\binom{p^d}{(p-1)p^d} f_{i-(p-1)p^{d-1}} \pmod{p^m}.$$

Now

$$f_{i-(p-1)p^{d-1}} \equiv (-p)^{m-2} \pmod{p^{m-1}}$$

by the induction hypothesis while

$$\binom{p^d}{(p-1)p^d} \equiv \binom{p}{p-1} \equiv p \pmod{p^2}$$

by Lemma 4.8. Thus, $f_i \equiv (-p)^{m-1} \pmod{p^m}$ and our proof is complete. □

Combining Theorem 4.6 with Proposition 4.3 yields the following corollary, which will enable us to use our Main Theorem 3.1 effectively.

Corollary 4.9: (cf. Lemma 1 and Theorem 10 of Wilson [17]) Let $\mathrm{wt} : \mathbb{Z}_{p^d} \to \mathbb{Z}$ be zer, ham, or symb_{n_0} for some $n_0 \in \mathbb{Z}_{p^d}$. For any $m \geq 1$, there exists a polynomial $h(x) \in \mathbb{Q}_p[x]$ of degree $[m(p-1)+1]p^{d-1}-1$ so that

$$h(r) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}, \qquad \text{for all } r \in \mathbb{Z}_{p^\infty}.$$

No polynomial of lesser degree has this property. If we write $h(x) = \sum_{i=0}^{\deg(h)} h_i x^i$, then

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

if $\mathrm{wt} = \mathrm{zer}$ or symb_{n_0}, while

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

if $\mathrm{wt} = \mathrm{ham}$. Furthermore, if $\mathrm{wt} = \mathrm{zer}$ or ham, then we can choose $h(x)$ so that $h_i = 0$ whenever $p-1 \nmid i$.

Proof: Since the functions $\mathrm{symb}_{n_0} \circ \pi$, including $\mathrm{zer} \circ \pi = \mathrm{symb}_{\pi(0)} \circ \pi$, are precisely the characteristic functions of cosets of the ideal (p^d) in $\mathbb{Z}_{p^\infty}$ and since $\mathrm{ham} = 1 - \mathrm{zer}$, all statements other than the last follow from Proposition 4.3 and Theorem 4.6.

To prove the last statement, let $\xi \in \mathbb{Z}_{p^\infty}$ be a primitive root of unity of order $p-1$. Then since ξ is a unit in $\mathbb{Z}_{p^\infty}$, we have $v_p(\xi r) = v_p(r)$ for all $r \in \mathbb{Z}_{p^\infty}$. Thus, $\mathrm{zer}(\pi(\xi r)) = \mathrm{zer}(\pi(r))$ for all $r \in \mathbb{Z}_{p^\infty}$. So for any $r \in \mathbb{Z}_{p^\infty}$, we have

$$\begin{aligned}
\mathrm{zer}(\pi(r)) &= \frac{1}{p-1}\sum_{i=0}^{p-2} \mathrm{zer}(\pi(\xi^i r)) \\
&\equiv \frac{1}{p-1}\sum_{i=0}^{p-2} h(\xi^i r) \\
&\equiv \frac{1}{p-1}\sum_{i=0}^{p-2}\sum_{j=0}^{\deg(h)} h_j \xi^{ij} r^j \\
&\equiv \sum_{j=0}^{\deg(h)} h_j r^j \frac{1}{p-1}\sum_{i=0}^{p-2} \xi^{ij} \\
&\equiv \sum_{\substack{0 \le j \le \deg(h) \\ p-1 \mid j}} h_j r^j \pmod{p^m}.
\end{aligned}$$

This proves our final claim for $\mathrm{wt} = \mathrm{zer}$ and for ham since $\mathrm{ham} = 1 - \mathrm{zer}$. □

We pause for an example of how our theory may be used to construct a specific counting polynomial.

Example 4.10: Let $p = 2$ and $d = 2$, so that our code alphabet is $\mathbb{Z}_4$. Suppose that we want to calculate Hamming weights modulo 8. Then Corollary 4.9 asserts that there is a polynomial $h(x)$ of degree 7 (and no polynomial of lower degree) such that $h(s) \equiv \mathrm{ham}(\pi(s)) \pmod 8$ for all $s \in \mathbb{Z}_{2^\infty}$. By Proposition 4.3, one such polynomial is the degree 7 truncation of the Newton expansion $\sum_{i \in \mathbb{N}} f_i \binom{x}{i}$ of $\mathrm{ham} \circ \pi$. We can calculate

$$\begin{aligned}
f_0 &= \mathrm{ham}(\pi(0)) = 0 \\
f_1 &= \mathrm{ham}(\pi(1)) - f_0\binom{1}{0} = 1 \\
f_2 &= \mathrm{ham}(\pi(2)) - f_0\binom{2}{0} - f_1\binom{2}{1} = -1 \quad \text{and} \\
f_3 &= \mathrm{ham}(\pi(3)) - f_0\binom{3}{0} - f_1\binom{3}{1} - f_2\binom{3}{2} = 1
\end{aligned}$$

by hand and then use the recursion

$$f_i = -(4f_{i-3} + 6f_{i-2} + 4f_{i-1})$$

furnished by Proposition 4.7 to compute $f_4 = -2$, $f_5 = 6$, $f_6 = -16$, and $f_7 = 36$. Thus, the polynomial we seek is

$$\binom{x}{1} - \binom{x}{2} + \binom{x}{3} - 2\binom{x}{4} + 6\binom{x}{5} - 16\binom{x}{6} + 36\binom{x}{7}.$$

It is not difficult to calculate from the recursion that all f_i with $i \ge 8$ vanish modulo 8, and thus the rest of the Newton expansion is dropped in our approximation. We can write out the polynomial we found as

$$\frac{1}{1260}(9x^7 - 217x^6 + 2058x^5 - 9730x^4 + 23961x^3 - 29113x^2 + 14292x).$$

If we reduce the coefficients modulo 8 (using the notion of congruence modulo powers of p in $\mathbb{Q}_p$ described in Section II-A), we obtain the polynomial

$$\frac{1}{4}(11x^7 + 5x^6 - 2x^5 - 6x^4 - 5x^3 + 5x^2 - 4x),$$

which also approximates $\mathrm{ham} \circ \pi$ modulo 8. □

C. Polynomials Approximating Lee Weight

Now we shall examine polynomials that approximate the Lee weight. The results for $p = 2$ differ somewhat from those with p odd, so we deal with these two cases separately. First we explore the case when p is an odd prime.

Proposition 4.11: Suppose that p is odd. Let $\sum_{i \in \mathbb{N}} c_i \binom{x}{i}$ be the Newton expansion of $\mathrm{lee} \circ \pi$. Then for any $m \ge 0$ and $i \ge [m(p-1)+1]p^{d-1}$, we have $v_p(c_i) \ge m$. For any $m \ge 1$ and $i = [m(p-1)+1]p^{d-1} - 1$, we have $c_i \equiv -\frac{1}{4}(-p)^{m-1} \pmod{p^m}$.

Proof: Note that

$$\mathrm{lee} = \sum_{j=1}^{(p^d-1)/2} j(\mathrm{symb}_{\pi(j)} + \mathrm{symb}_{\pi(p^d-j)})$$

and Theorem 4.6 provides adequate information about the Newton coefficients of the functions $\mathrm{symb}_{\pi(j)} \circ \pi$. □

Combined with Proposition 4.3, this proposition shows that when p is odd, the polynomials approximating Lee weight modulo p^m are no less in degree than those approximating Hamming weight or symbol counts. This is recorded in the following corollary to our proposition.

Corollary 4.12: Suppose that p is odd. For any $m \ge 1$, there exists a polynomial $h(x) \in \mathbb{Q}_p[x]$ of degree $[m(p-1)+1]p^{d-1} - 1$ so that $h(r) \equiv \mathrm{lee}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_{p^\infty}$. No polynomial of lesser degree has this property. Furthermore, $h(x) = \sum_{i=0}^{\deg(h)} h_i x^i$ has

$$\deg(h)! h_{\deg(h)} \equiv -\frac{1}{4}(-p)^{m-1} \pmod{p^m}.$$

The situation is more favorable for approximating Lee weight with polynomials when $p = 2$ and $d \ge 2$. When $p = 2$ and $d = 1$, Lee weight coincides with Hamming weight. To see the properties of Lee weight modulo powers of 2 will require some calculation, starting from the following observation, whose proof is a straightforward calculation.

Lemma 4.13: Let $p = 2$. Then $\Sigma_{2^{d-1}} \Delta_1^2(\mathrm{lee} \circ \pi) = 0$.

This enables us to determine a recursion satisfied by the Newton coefficients of $\mathrm{lee} \circ \pi$ when $p = 2$. We do this in the following lemma.

Lemma 4.14: Let $p = 2$ and let $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ be the Newton expansion of $\mathrm{lee}\circ\pi$. Then

$$c_i = -2c_{i-2^{d-1}} - \sum_{j=i-2^{d-1}+1}^{i-1} c_j\binom{2^{d-1}}{i-j}.$$

for $i \geq 2 + 2^{d-1}$.

Proof: This is similar in spirit to the proof of Proposition 4.7. Use Lemma 4.13 along with two applications of Proposition 4.5 followed by an application of Proposition 4.4 to obtain a Newton expansion for the zero function in terms of the coefficients c_i. □

Knowing this recursion allows us to set a bound on the 2-adic valuations of the Newton coefficients of $\mathrm{lee}\circ\pi$. We do this in the following proposition.

Proposition 4.15: Let $p = 2$ and let $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ be the Newton expansion of $\mathrm{lee}\circ\pi$. Then for $m \geq 1$, we have $v_2(c_i) \geq m$ for all $i \geq (m-1)2^{d-1} + 2$ and

$$c_{(m-1)2^{d-1}+1} \equiv 2^{m-1} \pmod{2^m}.$$

Proof: This is similar in spirit to the proof of Theorem 4.6. Calculate c_0 and c_1 by hand and then proceed by induction, using the recursion of Lemma 4.14 along with Lemma 4.8. □

Combined with Proposition 4.3, this proposition shows that the polynomials approximating Lee weight modulo 2^d (for $d \geq 2$) have a lower degree than those approximating Hamming weight. This is recorded in the following corollary to our proposition.

Corollary 4.16: (cf. Wilson [16, Lemma 5]) Suppose that $p = 2$. For any $m \geq 1$, there exists a polynomial $h(x) \in \mathbb{Q}_2[x]$ of degree $(m-1)2^{d-1} + 1$ so that $h(r) \equiv \mathrm{lee}(\pi(r)) \pmod{2^m}$ for all $r \in \mathbb{Z}_{2^\infty}$. No polynomial of lesser degree has this property. Furthermore, $h(x) = \sum_{i=0}^{\deg(h)} h_i x^i$ has

$$\deg(h)!h_{\deg(h)} \equiv 2^{m-1} \pmod{2^m}.$$

We pause for a brief example which should make clear the hitherto mysterious choice of counting polynomial in Example 3.3.

Example 4.17: Let $p = 2$ and $d = 2$, so that our code alphabet is $\mathbb{Z}_4$. Suppose we are interested in reckoning the Lee weight of codewords modulo 4. This is precisely the situation in Example 3.3, where we employed the polynomial $\frac{1}{3}(x + 3x^2 - x^3)$ without explaining where we got it. Corollary 4.16 asserts that there is a polynomial $h(x)$ of degree 3 (and no polynomial of lower degree) such that $h(s) \equiv \mathrm{lee}(\pi(s)) \pmod 4$ for all $s \in \mathbb{Z}_{2^\infty}$. By Proposition 4.3, one such polynomial is the degree 3 truncation of the Newton expansion $\sum_{i\in\mathbb{N}} f_i\binom{x}{i}$ of $\mathrm{lee}\circ\pi$. We can calculate

$$\begin{aligned}
f_0 &= \mathrm{lee}(\pi(0)) = 0\\
f_1 &= \mathrm{lee}(\pi(1)) - f_0\binom{1}{0} = 1\\
f_2 &= \mathrm{lee}(\pi(2)) - f_0\binom{2}{0} - f_1\binom{2}{1} = 0 \quad \text{and}\\
f_3 &= \mathrm{lee}(\pi(3)) - f_0\binom{3}{0} - f_1\binom{3}{1} - f_2\binom{3}{2} = -2.
\end{aligned}$$

Thus, the polynomial we seek is

$$\binom{x}{1} - 2\binom{x}{3} = \frac{1}{3}(x + 3x^2 - x^3)$$

which is precisely the polynomial used in Example 3.3. It is not hard to see from the recursion

$$f_i = -2(f_{i-2} + f_{i-1})$$

furnished by Lemma 4.14 that f_i vanishes modulo 4 for $i \geq 4$, and thus the rest of the Newton expansion is dropped in our approximation. □

D. Polynomials Approximating Euclidean Weight

We shall find that polynomials approximating Euclidean weight can often be of considerably lower degree than their counterparts for Hamming or Lee weight, both in the case when $p = 2$ and when p is odd. There are differences between the results for $p = 2$ and p odd, so we handle each case separately, starting with the latter. Our investigation begins with the following observation, which is a straightforward calculation.

Lemma 4.18: Suppose that p is odd. Then

$$\Delta_1^2(\mathrm{euc}\circ\pi) = 2 - p^d\left(\mathrm{symb}_{\pi(\frac{p^d-3}{2})}\circ\pi + \mathrm{symb}_{\pi(\frac{p^d-1}{2})}\circ\pi\right).$$

From this we may estimate the Newton coefficients of $\mathrm{euc}\circ\pi$. We do so in the following proposition.

Proposition 4.19: Suppose that p is odd. Let $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ be the Newton expansion of $\mathrm{euc}\circ\pi$. Then $c_0 = 0$, $c_1 = 1$, and $c_2 \equiv 2 \pmod{p^d}$ so that $v_p(c_2) = 0$. For $i \geq 3$, we have $v_p(c_i) \geq d$. For any $m \geq d$ and $i \geq [(m-d)(p-1)+1]p^{d-1}+2$, we have $v_p(c_i) \geq m$. For any $m \geq d+1$ and $i = [(m-d)(p-1)+1]p^{d-1}+1$, we have $c_i \equiv 2(-1)^{m-d}p^{m-1} \pmod{p^m}$.

Proof: Calculate c_0 and c_1 by hand and use Lemma 4.18 with two applications of Proposition 4.5 to express c_i for $i \geq 2$ in terms of the Newton coefficients of

$$\mathrm{symb}_{\pi(\frac{p^d-3}{2})}\circ\pi \quad \text{and} \quad \mathrm{symb}_{\pi(\frac{p^d-1}{2})}\circ\pi$$

concerning which Theorem 4.6 supplies adequate information. □

As usual, such a proposition combined with Proposition 4.3 tells us about the polynomial approximations to $\mathrm{euc}\circ\pi$ when p is odd. We record our results as a corollary.

Corollary 4.20: Suppose that p is odd. For any $m \geq 1$, there exists a polynomial $h(x) \in \mathbb{Q}_p[x]$ so that $h(r) \equiv \mathrm{euc}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_{p^\infty}$. The minimum degree of polynomials having this property is a function of m as follows: If $1 \leq m \leq d$, then the minimum degree is 2 and one such polynomial is x^2. If $m \geq d+1$, then the minimum degree is $[(m-d)(p-1)+1]p^{d-1}+1$. Furthermore, suppose that $h(x)$ is one of these minimal degree polynomials and write

$$h(x) = \sum_{i=0}^{\deg(h)} h_i x^i.$$

Then $\deg(h)!h_{\deg(h)} \equiv 2 \pmod{p^m}$ if $1 \leq m \leq d$ and $\deg(h)!h_{\deg(h)} \equiv 2(-1)^{m-d}p^{m-1} \pmod{p^m}$ if $m \geq d+1$.

Proof: This is done as usual. Note that the Newton coefficients for $\mathrm{euc}\circ\pi$ modulo p^d are all zero except $c_1 = 1$, $c_2 \equiv 2 \pmod{p^d}$, and that $\binom{x}{1} + 2\binom{x}{2} = x^2$. □

Polynomial approximation is even more favorable for Euclidean weights modulo 2^d. We shall begin our investigation into this case with the following observation, which is a routine calculation.

Lemma 4.21: Let $p = 2$. Then

$$\Delta_1^2(\mathrm{euc} \circ \pi) = 2 - 2^{d+1}\mathrm{symb}_{\pi(2^{d-1}-1)} \circ \pi.$$

From this we may estimate the Newton coefficients of $\mathrm{euc}\circ\pi$. We do so in the following proposition.

Proposition 4.22: Suppose that $p = 2$. Let $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ be the Newton expansion of $\mathrm{euc} \circ \pi$. Then $c_0 = 0$, $c_1 = 1$, and $c_2 \equiv 2 \pmod{2^{d+1}}$ so that $v_p(c_2) = 1$. For $i \geq 3$, we have $v_p(c_i) \geq d+1$. For any $m \geq d+1$ and $i \geq (m-d)2^{d-1}+2$, we have $v_p(c_i) \geq m$. For any $m \geq d+2$ and $i = (m-d)2^{d-1}+1$, we have $c_i \equiv 2^{m-1} \pmod{2^m}$.

Proof: Calculate c_0 and c_1 by hand and use Lemma 4.21 with two applications of Proposition 4.5 to express c_i for $i \geq 2$ in terms of the Newton coefficients of $\mathrm{symb}_{\pi(2^{d-1}-1)} \circ \pi$, concerning which Theorem 4.6 supplies adequate information. □

From this proposition, combined with Proposition 4.3, we obtain information about polynomials approximating $\mathrm{euc}\circ\pi$ when $p = 2$. We record this as a corollary.

Corollary 4.23: Suppose that $p = 2$. For any $m \geq 1$, there exists a polynomial $h(x) \in \mathbb{Q}_2[x]$ so that $h(r) \equiv \mathrm{euc}(\pi(r)) \pmod{2^m}$ for all $r \in \mathbb{Z}_{2^\infty}$. The minimum degree of polynomials having this property is a function of m as follows: For $m = 1$, the minimum degree is 1 and x is such a polynomial. If $2 \leq m \leq d+1$, then the minimum degree is 2 and x^2 is such a polynomial. If $m \geq d+2$, then the minimum degree is $(m-d)2^{d-1}+1$. Furthermore, suppose that $h(x)$ is one of these minimal degree polynomials and write

$$h(x) = \sum_{i=0}^{\deg(h)} h_i x^i.$$

Then $\deg(h)!h_{\deg(h)} \equiv 1 \pmod 2$ if $m = 1$, $\deg(h)!h_{\deg(h)} \equiv 2 \pmod{2^m}$ if $2 \leq m \leq d+1$, and $\deg(h)!h_{\deg(h)} \equiv 2^{m-1} \pmod{2^m}$ if $m \geq d+2$.

We pause to note that we have used a polynomial furnished by this corollary in a previous example.

Example 4.24: In Example 3.2, we wanted to calculate Euclidean weights modulo 8 with the alphabet $\mathbb{Z}_4$. We used the polynomial x^2, which is precisely the polynomial suggested by Corollary 4.23 for this application. □

E. Polynomials Approximating Weights for Codes Over $\mathbb{Z}_4$

In this subsection, we shall assume that $p = 2$ and $d = 2$, so that we are working with weight functions on the alphabet $\mathbb{Z}_4$. We shall calculate explicitly the Newton coefficients for $\mathrm{zer} \circ \pi = \mathrm{symb}_{\pi(0)}\circ\pi$, and from these, use Proposition 4.4 to deduce the coefficients for $\mathrm{symb}_{\pi(n)} \circ \pi$ with $n = 1, 2, 3$. We shall be able to calculate the Newton coefficients of $\mathrm{ham} \circ \pi$, $\mathrm{lee} \circ \pi$, and $\mathrm{euc}\circ\pi$, since these are linear combinations of the functions $\mathrm{symb}_{\pi(n)} \circ \pi$. We begin with a lemma on zer.

Lemma 4.25: Let $p = 2$ and $d = 2$ and suppose that $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ is the Newton expansion of $\mathrm{zer} \circ \pi$. Then $c_0 = 1$ and if $i \geq 1$, then $c_i = (-1)^i(2^{\lfloor (i-1)/2\rfloor} + \tau_i)2^{\lfloor (i-2)/2\rfloor}$, where

$$\tau_i = \begin{cases} -1, & \text{if } i \equiv 3, 4, 5 \\ 1, & \text{if } i \equiv 0, 1, 7 \\ 0, & \text{if } i \equiv 2, 6 \pmod 8. \end{cases}$$

Proof: We can calculate $c_0 = 1$, $c_1 = -1$, $c_2 = 1$, and $c_3 = -1$ by hand. The rest of the c_i can be determined by the recursion $c_n = -(4c_{n-1} + 6c_{n-2} + 4c_{n-3})$ for $n \geq 4$ given in Proposition 4.7. One can check that the values proposed above match these first four values and satisfy the recursion. □

Proposition 4.26: Let $p = 2$, $d = 2$, and $\mathrm{wt} = \mathrm{symb}_{\pi(n)}$ for $n = 0, 1, 2$, or 3 or $\mathrm{wt} = \mathrm{ham}$, lee, or euc. Let $\sum_{i\in\mathbb{N}} c_i\binom{x}{i}$ be the Newton expansion for $\mathrm{wt} \circ \pi$. If $\mathrm{wt} = \mathrm{zer}$, then $c_0 = 1$, otherwise, $c_0 = 0$. For $i \geq 1$, $c_i = (-1)^i 2^{\lfloor (i-2)/2\rfloor}\gamma_i$, where γ_i is given in the following arrays as a function of wt and of i taken modulo 8:

$i \pmod 8$	zer	$\mathrm{symb}_{\pi(1)}$
0	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}$
1	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}-1$
2	$2^{\lfloor (i-1)/2\rfloor}$	$-2^{\lfloor (i-1)/2\rfloor}-1$
3	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}-1$
4	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}$
5	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}+1$
6	$2^{\lfloor (i-1)/2\rfloor}$	$-2^{\lfloor (i-1)/2\rfloor}+1$
7	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}+1$

$i \pmod 8$	$\mathrm{symb}_{\pi(2)}$	$\mathrm{symb}_{\pi(3)}$
0	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}$
1	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}+1$
2	$2^{\lfloor (i-1)/2\rfloor}$	$-2^{\lfloor (i-1)/2\rfloor}+1$
3	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}+1$
4	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}$
5	$2^{\lfloor (i-1)/2\rfloor}+1$	$-2^{\lfloor (i-1)/2\rfloor}-1$
6	$2^{\lfloor (i-1)/2\rfloor}$	$-2^{\lfloor (i-1)/2\rfloor}-1$
7	$2^{\lfloor (i-1)/2\rfloor}-1$	$-2^{\lfloor (i-1)/2\rfloor}-1$

$i \pmod 8$	ham	lee	euc
0	$-2^{\lfloor (i-1)/2\rfloor}-1$	-2	$4(2^{\lfloor (i-3)/2\rfloor}-1)$
1	$-2^{\lfloor (i-1)/2\rfloor}-1$	-2	$4(2^{\lfloor (i-3)/2\rfloor}-1)$
2	$-2^{\lfloor (i-1)/2\rfloor}$	0	$4(2^{\lfloor (i-3)/2\rfloor})$
3	$-2^{\lfloor (i-1)/2\rfloor}+1$	2	$4(2^{\lfloor (i-3)/2\rfloor}+1)$.
4	$-2^{\lfloor (i-1)/2\rfloor}+1$	2	$4(2^{\lfloor (i-3)/2\rfloor}+1)$
5	$-2^{\lfloor (i-1)/2\rfloor}+1$	2	$4(2^{\lfloor (i-3)/2\rfloor}+1)$
6	$-2^{\lfloor (i-1)/2\rfloor}$	0	$4(2^{\lfloor (i-3)/2\rfloor})$
7	$-2^{\lfloor (i-1)/2\rfloor}-1$	-2	$4(2^{\lfloor (i-3)/2\rfloor}-1)$

Proof: The Newton coefficients for $\mathrm{zer} \circ \pi$ are from Lemma 4.25. Since $(\mathrm{symb}_{\pi(3)} \circ \pi)(n) = (\mathrm{zer} \circ \pi)(n+1)$ for $n \in \mathbb{N}$, Proposition 4.4 tells us how to compute the Newton coefficients of $\mathrm{symb}_{\pi(3)} \circ \pi$ from those of $\mathrm{zer} \circ \pi$. In a similar way, we may compute the Newton coefficients of $\mathrm{symb}_{\pi(2)}$ and $\mathrm{symb}_{\pi(1)}$ by translation. For the other weight functions, we can compute the Newton coefficients using the identities $\mathrm{ham} = 1 - \mathrm{zer}$, $\mathrm{lee} = \mathrm{symb}_{\pi(1)} + 2\mathrm{symb}_{\pi(2)} + \mathrm{symb}_{\pi(3)}$, and $\mathrm{euc} = \mathrm{symb}_{\pi(1)} + 4\mathrm{symb}_{\pi(2)} + \mathrm{symb}_{\pi(3)}$. □

These calculations in conjunction with Proposition 4.3 allow us to determine the minimum degree polynomials approxi-

mating the various weight functions. We record these results as corollaries.

Corollary 4.27: Suppose that $p = 2$, $d = 2$, and $\mathrm{wt} = \mathrm{zer}, \mathrm{symb}_{\pi(1)}, \mathrm{symb}_{\pi(2)}, \mathrm{symb}_{\pi(3)}$, or ham. For $m \geq 1$, there exists a polynomial $h(x) \in \mathbb{Q}_2[x]$ of degree $2m+1$ so that $h(r) \equiv \mathrm{wt}(\pi(r)) \pmod{2^m}$ for all $r \in \mathbb{Z}_{2^\infty}$. No polynomial of lesser degree has this property. If we write

$$h(x) = \sum_{i=0}^{2m+1} h_i x^i$$

then

$$(2m+1)!h_{2m+1} \equiv 2^{m-1} \pmod{2^m}.$$

If $m > 1$ and $\mathrm{wt} \in \{\mathrm{zer}, \mathrm{symb}_{\pi(2)}, \mathrm{ham}\}$ or if $m = 1$ and $\mathrm{wt} \in \{\mathrm{symb}_{\pi(1)}, \mathrm{symb}_{\pi(3)}\}$, then $(2m)!\pi_{2m} \equiv 2^{m-1} \pmod{2^m}$. If $m > 1$ and $\mathrm{wt} \in \{\mathrm{symb}_{\pi(1)}, \mathrm{symb}_{\pi(3)}\}$ or if $m = 1$ and $\mathrm{wt} \in \{\mathrm{zer}, \mathrm{symb}_{\pi(2)}, \mathrm{ham}\}$, then $(2m)!\pi_{2m} \equiv 0 \pmod{2^m}$.

Proof: If we write the Newton expansion of $\mathrm{wt} \circ \pi$ as $\sum_{n=0}^{\infty} c_i \binom{x}{n}$, then Proposition 4.26 tells us that $v_p(c_{2m+1}) = m-1$ and $v_p(c_i) \geq m$ for $i > 2m+1$. Thus, Proposition 4.3 establishes the existence and minimal degree of polynomials approximating $\mathrm{wt} \circ \pi$ modulo 2^m. Furthermore, this proposition tells us that for any such polynomial $h(x) = \sum_{i=0}^{2m+1} h_i x^i$ of minimal degree, we have

$$(2m+1)!h_{2m+1} \equiv c_{2m+1} \pmod{2^m}$$

and

$$(2m)!h_{2m} \equiv -mc_{2m+1} + c_{2m} \pmod{2^m}.$$

Thus, using the values of c_{2m+1} and c_{2m} computed in Proposition 4.26, we can compute the estimates of $j!h_j$ (for $j = 2m, 2m+1$) given above. □

Corollary 4.28: Suppose that $p = 2$ and $d = 2$. For any $m \geq 1$ there exists a polynomial $h(x) \in \mathbb{Q}_2[x]$ of degree $2m-1$ so that

$$h(r) \equiv \mathrm{lee}(\pi(r)) \pmod{2^m}, \qquad \text{for all } r \in \mathbb{Z}_{2^\infty}.$$

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

$$h(x) = \sum_{i=0}^{2m-1} h_i x^i$$

then

$$(2m-1)!h_{2m-1} \equiv (2m-2)!h_{2m-2} \equiv 2^{m-1} \pmod{2^m}.$$

Proof: This is similar to the proof of Corollary 4.27. □

Corollary 4.29: Suppose that $p = 2$ and $d = 2$. For any $r \in \mathbb{Z}_{2^\infty}$

$$\mathrm{euc}(\pi(r)) \equiv r \pmod{2}$$

and

$$\mathrm{euc}(\pi(r)) \equiv r^2 \pmod{8}.$$

For any $m \geq 4$ there exists a polynomial $h(x) \in \mathbb{Q}_2[x]$ of degree $2m-3$ so that

$$h(r) \equiv \mathrm{euc}(\pi(r)) \pmod{2^m}, \qquad \text{for all } r \in \mathbb{Z}_{2^\infty}.$$

No lower degree polynomials exist with these properties. For $m \geq 4$, if we write

$$h(x) = \sum_{i=0}^{2m-3} h_i x^i$$

then

$$(2m-3)!h_{2m-3} \equiv 2^{m-1} \pmod{2^m}.$$

Also, $(2m-4)!h_{2m-4} \equiv 2^{m-1} \pmod{2^m}$ when $m \geq 5$. When $m = 4$, we can use

$$h(x) = -\frac{1}{5}x^5 + \frac{8}{3}x^4 - \frac{37}{3}x^3 + \frac{67}{3}x^2 - \frac{172}{15}x$$

so that $5!h_5 = -24$, $4!h_4 = 64$. and $3!h_3 = -74$.

Proof: This is similar to the proof of Corollary 4.27. For the $m \leq 4$ cases, the polynomials proposed above are truncations $\sum_{i=0}^{k} c_i \binom{x}{i}$ of the Newton expansion of $\mathrm{euc} \circ \pi$, whose coefficients c_i are given in Proposition 4.26. □

V. Analogs of McEliece's Theorem for Abelian Codes Over $\mathbb{Z}_{p^d}$

Now we are ready to obtain analogs of McEliece's theorem by combining our Main Theorem (Theorem 3.1) with the results we have just obtained concerning polynomials approximating weight functions. Throughout this section, we shall have a codeword $f \in \mathbb{Z}_{p^d}[A]$ with S, a support of $\hat{f}$. We let $F \in \mathbb{Z}_{p^\infty}[\zeta][A]$ be the word with $\tilde{F} = \tau \circ \tilde{f}$. We let B be the set of all unity-product, not all-unity multisets supported on S. In some of our results, we shall need to know that B is nonempty. If S contains any $s \neq 1_A$, then the multiset ns, with n the order of s, is an element of B. If $S = \emptyset$ or $S = \{1_A\}$, then $B = \emptyset$. If $S = \emptyset$, then f is the all-zero word. If $S = \{1_A\}$, then f is a constant word (i.e., all letters in f are the same symbol). In either of these degenerate cases, we have $\mathrm{wt}(f) = |A|\mathrm{wt}(\tilde{f}_1)$, so analysis of weights is transparent.

For $j \in \mathbb{N}$, we let $B_j = \{\lambda \in B : |\lambda| = j\}$. Note that $B_0 = B_1 = \emptyset$ since a unity-product multiset of 0 or 1 elements must be all-unity. If $B \neq \emptyset$, we let $\ell = \min\{j \in \mathbb{N} : B_j \neq \emptyset\}$ and $\ell' = \min\{j \in \mathbb{N} : B_j \neq \emptyset, p-1 \mid j\}$. We can be sure that ℓ' exists if $B \neq \emptyset$ since $(p-1)\lambda \in B$ if $\lambda \in B$. Note that $\ell = \ell'$ if $p = 2$, but in general for p odd we may have $\ell' > \ell$ (see [11, Sec. 3, Example 1]). When we use ℓ or ℓ', we are tacitly assuming that $B \neq \emptyset$, or equivalently, that S contains some $s \neq 1_A$.

A. Analogs for General p and d

1) Hamming Weight and Number of Occurrences of a Symbol: A generalization of McEliece's theorem that can be used to count zeroes or to compute Hamming weights of words in Abelian codes over $\mathbb{Z}_{p^d}$ comes immediately from enlisting the polynomials of Corollary 4.9 for use in Theorem 3.1. We record it without proof.

Theorem 5.1: For any $m \geq 1$, let $d_m = [m(p-1)+1]p^{d-1} - 1$. Then

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + \sum_{\substack{1 < j \leq d_m \\ p-1 \mid j}} j!h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m},$$

where

$$h(x) = \sum_{\substack{0 \le j \le d_m \\ p-1 \mid j}} h_j x^j \in \mathbb{Q}_p[x]$$

is a polynomial approximating $\mathrm{zer} \circ \pi$ modulo p^m on $\mathbb{Z}_{p^\infty}$ as described in Corollary 4.9. Equivalently, we have

$$\frac{1}{|A|}\mathrm{ham}(f) \equiv \mathrm{ham}(\tilde{f}_1) - \sum_{\substack{1 < j \le d_m \\ p-1 \mid j}} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}.$$

We can see that the expression for $\mathrm{zer}(f)$ in our theorem is especially easy to calculate when many the of the sets B_j with $p-1 \mid j$ are empty. This occurs when the support S of $\hat{f}$ is such that there are no unity-product multisets of elements in S having small cardinalities divisible by $p-1$. (Note that we are excluding all-unity multisets from consideration.) In graph-theoretic terms, this corresponds to there being no circuits of short lengths divisible by $p-1$ in the Cayley graph generated by the elements of S (other than perhaps circuits that correspond to all-unity multisets, i.e., circuits visiting only one vertex). We make our notions more formal in the following corollary to our theorem which closely resembles the original results of McEliece [11].

Corollary 5.2: We have

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}(\tilde{f}_1) \pmod{p^{\left\lfloor \frac{\ell' - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}}$$

and, equivalently

$$\mathrm{ham}(f) \equiv |A|\mathrm{ham}(\tilde{f}_1) \pmod{p^{\left\lfloor \frac{\ell' - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}}.$$

Proof: Set

$$m = \left\lfloor \frac{\ell' - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor$$

and apply our theorem. All B_j in the sum are empty by hypothesis. □

Note that this is an improvement of Wilson's theorem [17, Theorem 9] applied to Hamming weights, since we have replaced ℓ by ℓ', which is sometimes larger than ℓ.

If one is interested in counting the number of occurrences of some nonzero symbol r in our word f, one may take one of two approaches. In the first approach, Corollary 4.9 provides minimum-degree polynomials approximating $\mathrm{symb}_r \circ \pi$ for all $r \in \mathbb{Z}_{p^d}$, so that the following analog of McEliece's theorem for counting any particular symbol can be formulated from the Main Theorem in conjunction with these polynomials.

Proposition 5.3: (Wilson [17, Theorem 9], generalized) Let r be a symbol in the alphabet $\mathbb{Z}_{p^d}$ of the code. For any $m \ge 1$, let $d_m = [m(p-1)+1]p^{d-1} - 1$. Then

$$\frac{1}{|A|}\mathrm{symb}_r(f) \equiv \mathrm{symb}_r(\tilde{f}_1) + \sum_{j=2}^{d_m} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where

$$h(x) = \sum_{j=0}^{d_m} h_j x^j \in \mathbb{Q}_p[x]$$

is a polynomial approximating $\mathrm{symb}_r \circ \pi$ modulo p^m on $\mathbb{Z}_{p^\infty}$ as described in Corollary 4.9. Furthermore

$$\mathrm{symb}_r(f) \equiv |A|\mathrm{symb}_r(\tilde{f}_1) \pmod{p^{\left\lfloor \frac{\ell - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}}.$$

Note that when $p = 2$ and $\hat{f}_1 = 0$, this proposition tells us that the number of occurrences of the symbol r is divisible by $2^{\left\lfloor \frac{\ell}{2^{d-1}} \right\rfloor - 1}$. This was proved for cyclic codes in Wilson [16], [17]. This is stronger than the result presented by Calderbank, Li, and Poonen in [10, Theorem 3.7], which claims that the number of occurrences of r is divisible by $2^{\left\lceil \frac{\ell}{2^{d-1}} \right\rceil - 2}$ (also assuming A is cyclic). In particular, the proposition presented here gives an additional power of 2 when ℓ is a multiple of 2^{d-1} (otherwise, the results match). Consider the case when our alphabet is $\mathbb{Z}_8$ (so $d = 3$) and our group A is the cyclic group generated by an element a of order 255. Suppose that our code consists of all words whose Fourier transforms are supported on $S = \{a, a^2, a^4, \ldots, a^{128}\}$. Here $\ell = 8$, so that Proposition 5.3 tells us that the number of occurrences of each symbol is even, while Theorem 3.7 of Calderbank, Li, and Poonen gives no information.

A second approach to counting the number of occurrences of an arbitrary nonzero symbol r is to use Theorem 5.1 to count zeroes in the word γ that has $\gamma_a = f_a - r$ for all $a \in A$ (and hence $\tilde{\gamma}_a = \tilde{f}_a$ for $a \ne 1$ while $\tilde{\gamma}_1 = \tilde{f}_1 - r$). We note that this approach only requires us to determine B_j for $p-1 \mid j$, as a result of the special property of polynomials approximating $\mathrm{zer} \circ \pi$. However, the subtraction of r from all positions of the codeword will yield $\tilde{\gamma}_1 \ne 0$ unless we originally had $\tilde{f}_1 = r$. The presence of 1_A in the support of the Fourier transform will mean that a unity-product multiset of cardinality divisible by $p-1$ can always be obtained by adding extra unity elements to a unity-product multiset of arbitrary cardinality. Hence, we should expect this technique to lend no great facility to computation except when $\tilde{f}_1 = r$.

2) Lee Weight: Now consider Lee weight, for which we shall need two theorems, depending on whether $p = 2$ or not. For p odd, Corollary 4.12 and our Main Theorem combine immediately to yield the following result, recorded as a proposition without proof.

Proposition 5.4: Suppose that p is odd. For any $m \ge 1$, let $d_m = [m(p-1)+1]p^{d-1} - 1$. Then

$$\frac{1}{|A|}\mathrm{lee}(f) \equiv \mathrm{lee}(\tilde{f}_1) + \sum_{j=2}^{d_m} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where

$$h(x) = \sum_{j=0}^{d_m} h_j x^j \in \mathbb{Q}_p[x]$$

is a polynomial approximating $\mathrm{lee} \circ \pi$ modulo p^m on $\mathbb{Z}_{p^\infty}$ as described in Corollary 4.12. Furthermore

$$\mathrm{lee}(f) \equiv |A|\mathrm{lee}(\tilde{f}_1) \pmod{p^{\left\lfloor \frac{\ell - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}}.$$

For $p = 2$ and $d > 1$, our polynomials approximating $\mathrm{lee} \circ \pi$ modulo 2^m are of lower degree than those approximating $\mathrm{zer} \circ \pi$

or $\mathrm{ham} \circ \pi$ modulo 2^m (compare Corollary 4.16 with Corollary 4.9 and note that Hamming and Lee weight coincide when $d = 1$). Therefore, in this milieu, we expect to obtain stronger divisibility properties for Lee weight than for Hamming weight, as can be seen from the immediate application of Corollary 4.16 with the Main Theorem which follows.

Theorem 5.5: (Wilson [16, Theorem 2], generalized) Suppose that $p = 2$. For any $m \geq 1$, let $d_m = (m-1)2^{d-1} + 1$. Then

$$\frac{1}{|A|}\mathrm{lee}(f) \equiv \mathrm{lee}(\tilde{f}_1) + \sum_{j=2}^{d_m} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}$$

where

$$h(x) = \sum_{j=0}^{d_m} h_j x^j \in \mathbb{Q}_2[x]$$

is a polynomial approximating $\mathrm{lee} \circ \pi$ modulo 2^m on $\mathbb{Z}_{2^\infty}$ as described in Corollary 4.16. Furthermore

$$\mathrm{lee}(f) \equiv |A|\mathrm{lee}(\tilde{f}_1) \pmod{2^{\left\lfloor \frac{\ell-2}{2^{d-1}} \right\rfloor + 1}}.$$

Wilson proved this theorem in the case where A is cyclic.

3) Euclidean Weight: We now turn to Euclidean weight. As with Lee weight, it is necessary to distinguish cases where p is odd from those where $p = 2$. In both cases, the approximating polynomials can be of significantly lower degree than those for any other weight function. For p odd, we combine the results of Corollary 4.20 with our Main Theorem to obtain an analog to McEliece's theorem for Euclidean weight.

Proposition 5.6: Suppose that p is odd. Then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2 \sum_{\lambda \in B_2} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^d}.$$

For any $m > d$, let $d_m = [(m-d)(p-1)+1]p^{d-1} + 1$. Then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + \sum_{j=2}^{d_m} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m},$$

where

$$h(x) = \sum_{j=0}^{d_m} h_j x^j \in \mathbb{Q}_p[x]$$

is a polynomial approximating $\mathrm{euc} \circ \pi$ modulo p^m on $\mathbb{Z}_{p^\infty}$ as described in Corollary 4.20. Furthermore, if $2 < \ell \leq p^d + 1$, then

$$\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{p^d}.$$

If $\ell > p^d + 1$, then

$$\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{p^{d + \left\lfloor \frac{\ell - p^{d-1} - 2}{(p-1)p^{d-1}} \right\rfloor}}.$$

For $p = 2$, the approximating polynomials can be of exceptionally low degree, as perusal of Corollary 4.23 shows. These results, combined with the Main Theorem, yield the following strong analog of McEliece's theorem.

Theorem 5.7: Suppose that $p = 2$. Then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) \pmod{2}$$

and

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2 \sum_{\lambda \in B_2} \tilde{F}_\lambda \pmod{2^{d+1}}.$$

For any $m > d+1$, let $d_m = (m-d)2^{d-1} + 1$. Then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + \sum_{j=2}^{d_m} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}$$

where

$$h(x) = \sum_{j=0}^{d_m} h_j x^j \in \mathbb{Q}_2[x]$$

is a polynomial approximating $\mathrm{euc} \circ \pi$ modulo 2^m on $\mathbb{Z}_{2^\infty}$ as described in Corollary 4.23. Furthermore, if $2 < \ell \leq 2^d + 1$, then

$$\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{2^{d+1}}.$$

If $\ell > 2^d + 1$, then

$$\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{2^{d + \left\lfloor \frac{\ell-2}{2^{d-1}} \right\rfloor}}.$$

Proof: Most of these results follow immediately from use of Corollary 4.23 with the Main Theorem. Note that we have omitted the factor of $(\lambda!)^{-1}$ in the first congruence modulo 2^{d+1} because B_2 can only contain accounts of the form $a + a^{-1}$ with $a \neq a^{-1}$ since the order of A is coprime to 2. Thus, $\lambda! = 1$ for all $\lambda \in B_2$. □

We have obtained analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_{p^d}$ which give p-adic estimates of the number of occurrences of symbols and of Hamming, Lee, and Euclidean weights. McEliece's original theorem [11] includes a statement of sharpness. For the code $\mathcal{C}$ consisting of words f with $\hat{f}$ supported on S, it gives an integer m so that

$$\mathrm{ham}(f) \equiv |A|\mathrm{ham}(\tilde{f}_1) \pmod{p^m}, \qquad \text{for all } f \in \mathcal{C}$$

like the analogs in this paper. But it also states that

$$\mathrm{ham}(f) \not\equiv |A|\mathrm{ham}(\tilde{f}_1) \pmod{p^{m+1}}, \qquad \text{for some } f \in \mathcal{C}.$$

Our theorems above do not include analogs of this second part; such statements of sharpness can be difficult to prove. The remainder of this paper shows that we can obtain such statements of sharpness in certain situations. In the next subsection, we shall show that our estimates are sharp when $d = 1$, thus giving a well-known generalization of the McEliece theorem for cyclic codes over prime fields. The last portion of the paper will show that our estimates are also sharp in the same way when $p = 2$ and $d = 2$, i.e., when the alphabet is $\mathbb{Z}_4$.

B. The Delsarte–McEliece Theorem for Abelian Codes Over Prime Fields ($d = 1$)

Here we shall show that the special case of Theorem 5.1 with $d = 1$ can be used to obtain a generalization of the original theorem of McEliece [11] for counting the number of zeroes in cyclic codes over prime fields. This specialization of Theorem 5.1 is at the same time a special case of the theorem of Delsarte and McEliece [15] for counting the number of zeroes in Abelian codes over finite fields. Our presentation will include a proof of sharpness (in the sense described at the conclusion of Section V-A), which will require tools which will be needed again in the proofs of sharpness for our theorems on codes over $\mathbb{Z}_4$ in Section V-E.

Theorem 5.8: (cf. McEliece [11, Theorem 1], Delsarte and McEliece [15, Theorem 1.1]) Suppose that $d = 1$, so that $\mathbb{Z}_{p^d} = \mathbb{Z}_p$, a prime field. Assume that S is p-closed. Let $\mathcal{C}$ be the code consisting of all codewords in $\mathbb{Z}_{p^d}[A]$ with Fourier transform supported on S. Set $m = \frac{\ell'}{p-1}$. Then we have

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + (-p)^{m-1} \sum_{\lambda \in B_{\ell'}} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}.$$

Furthermore, all factors $(\lambda!)^{-1}$ appearing here are p-adic integers so that

$$\mathrm{zer}(f) \equiv |A|\mathrm{zer}(\tilde{f}_1) \pmod{p^{m-1}}.$$

There is some particular choice of $f \in \mathcal{C}$ that makes

$$\mathrm{zer}(f) \not\equiv |A|\mathrm{zer}(\tilde{f}_1) \pmod{p^m}.$$

Proof: Apply Theorem 5.1 with $d = 1$ to obtain

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + \sum_{\substack{1<j\le \ell' \\ p-1|j}} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}$$

where

$$h(x) = \sum_{\substack{0\le j\le \ell' \\ p-1|j}} h_j x^j \in \mathbb{Q}_p[x]$$

is a polynomial approximating $\mathrm{zer} \circ \pi$ modulo p^m on $\mathbb{Z}_{p^\infty}$ as described in Corollary 4.9. Then all B_j in our congruence are empty, save $B_{\ell'}$, so

$$\frac{1}{|A|}\mathrm{zer}(f) \equiv \mathrm{zer}(\tilde{f}_1) + \ell'! h_{\ell'} \sum_{\lambda \in B_{\ell'}} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{p^m}. \quad (6)$$

Now we prove that the terms $\lambda!$ appearing in the sum are in fact nonzero modulo p. Recall that $\lambda! = \prod_{a\in S} \lambda_a!$, and so it suffices to prove that $\lambda_a < p$ for all $a \in S$. If λ_a were greater than $p-1$ for some a, then consider the multiset $\mu = \lambda - pa + a^p$, which is a unity-product (but not all-unity) multiset supported on S (since S is p-closed). Furthermore, $|\mu| = \ell' - (p-1)$, which is divisible by $p-1$, thus contradicting the minimality of ℓ'. Thus, both $\lambda!$ and $(\lambda!)^{-1}$ are p-adic integers with valuation 0. Hence, the sum in (6) is itself a p-adic integer in $\mathbb{Z}_{p^\infty}[\zeta]$. Also, note that $\ell'! h_{\ell'} \equiv (-p)^{m-1} \pmod{p^m}$ by Corollary 4.9, so we obtain the desired congruence. It remains to show that there is some choice of codeword f that makes the sum $\sum_{\lambda\in B_{\ell'}} \frac{\tilde{F}_\lambda}{\lambda!}$ nonvanishing modulo p. We write the canonical expansion $\tilde{F}_a = \sum_{i=0}^{\infty} \tilde{F}_a^{(i)} p^i$ for each $a \in S$ and then note that $\tilde{F}_a^{(i)} = 0$ for $i > 0$ since $\tilde{F}$ is obtained from $\tilde{f}$ by the standard lift. So our sum is

$$\sum_{\lambda \in B_{\ell'}} \frac{1}{\lambda!} \prod_{a\in S} \left(\tilde{F}_a^{(0)}\right)^{\lambda_a}.$$

The fact that this sum is nonvanishing modulo p for some choice of $f \in \mathcal{C}$ follows immediately from Proposition 5.9 below, since we have proved that every λ appearing in the sum has $\lambda_a < p$ for all $a \in S$ and $(\lambda!)^{-1}$ a unit in $\mathbb{Z}_{p^\infty}$. □

We now supply the result which was used to prove the sharpness of our theorem. It will be useful again when we prove the sharpness of our analogs for codes over $\mathbb{Z}_4$.

Proposition 5.9: Suppose that S is p-closed. Let $\mathcal{C}$ be the code consisting of all codewords whose Fourier transform is supported on S. Write canonical expansions $\tilde{F}_a = \sum_{i=0}^{d-1} \tilde{F}_a^{(i)} p^i$ for all $a \in A$. Let h be a polynomial with coefficients in $\mathbb{Z}_{p^\infty}$ and indeterminates in $\{x_{a,i} : a \in S, 0 \le i < d\}$, where no indeterminate occurs with an exponent greater than $p-1$ and where the minimum of the p-adic valuations of the coefficients is $k \in \mathbb{N}$. Then our polynomial h evaluated with $x_{a,i} = \tilde{F}_a^{(i)}$ yields a number that has p-adic valuation at least k, and there is some $f \in \mathcal{C}$ so that the number yielded has p-adic valuation precisely k.

Proof: We reduce to the case $k = 0$ by dividing the polynomial by p^k. Then the statement that h with $x_{a,i} = \tilde{F}_a^{(i)}$ always has p-adic valuation at least 0 is immediate from the fact that the coefficients of h and the numbers $\tilde{F}_a^{(i)}$ are p-adic integers.

Now we need to prove that there is some particular f as described above for which h with $x_{a,i} = \tilde{F}_a^{(i)}$ yields a number that is nonzero modulo p. From Corollary 2.3, we know that

$$\tilde{F}^{(i)}_{a^{p^j}} = \left(\tilde{F}_a^{(i)}\right)^{p^j}.$$

Thus, for the purposes of evaluating our polynomial at the points of interest, we can replace the indeterminate $x_{a^{p^j},i}$ with $x_{a,i}^{p^j}$. To do this in an orderly fashion, fix a set R of p-class representatives of A and let ϵ_r be the cardinality of the p-class represented by each $r \in R$. Then for each $r \in S \cap R$ representing p-class $\{r, r^p, r^{p^2}, \ldots, r^{p^{\epsilon_r - 1}}\}$, we modify the polynomial h by replacing each instance of the indeterminate $x_{r^{p^j},i}$ with $x_{r,i}^{p^j}$ for $1 \le j < \epsilon_r$. The resulting polynomial, which we call g, has indeterminates in $\{x_{r,i} : r \in S \cap R, 0 \le i < d\}$ and an exponent of the indeterminate $x_{r,i}$ can never exceed

$$(p-1) + (p-1)p + \cdots + (p-1)p^{\epsilon_r - 1} = p^{\epsilon_r} - 1.$$

Furthermore, the only way to obtain a monomial in which $x_{r,i}$ appears with exponent $\gamma_0 + \gamma_1 p + \cdots + \gamma_{\epsilon_r - 1} p^{\epsilon_r - 1}$ (where $0 \le \gamma_j < p$ for all j) is to start with a monomial having $x_{r^{p^j},i}$ appearing with exponent γ_j for each j. Thus, monomials in h with different exponents give rise to monomials in g with different exponents. Thus, distinct monomials in h give rise to distinct monomials in g and so g, like h, has some coefficient that does not vanish modulo p.

Let $\rho : \mathbb{Z}_{p^\infty}[\zeta] \to \mathrm{GF}(p^\epsilon)$ denote reduction modulo p, which we extend in the usual way to polynomial rings over $\mathbb{Z}_{p^\infty}[\zeta]$. We want to prove that there is some f among the codewords with $\hat{f}$ supported on S so that $\rho(g)$ evaluated with $x_{r,i} = \rho(\tilde{F}_r^{(i)})$ yields a nonzero value. Note that $\rho(g)$ is a nonzero polynomial with coefficients in $\mathrm{GF}(p^\epsilon)$ and the same restrictions on powers of the indeterminates as are stated for g above.

From Theorem 2.5, we know that $\hat{f}|_R$ (and hence $\tilde{f}|_R$) ranges over the pointwise ideal I in the ring

$$\bigoplus_{r\in R} \mathbb{Z}_{p^d}[\pi(\zeta)^{(p^\epsilon-1)/(p^{\epsilon_r}-1)}]$$

consisting of the elements that vanish at all points not in $S\cap R$. That is, $\tilde{f}|_{S\cap R}$ ranges over the ring

$$\bigoplus_{r\in S\cap R} \mathbb{Z}_{p^d}[\pi(\zeta)^{(p^\epsilon-1)/(p^{\epsilon_r}-1)}].$$

Thus, each $\tilde{F}_r^{(i)}$ with $r \in S\cap R$ and $0 \le i < d$ may be varied independently of the others over the set consisting of zero and the $(p^{\epsilon_r}-1)$th roots of unity. Thus, each $\rho(\tilde{F}_r^{(i)})$ with $r \in S\cap R$ and $0 \le i < d$ may be varied independently over GF(p^{ϵ_r}) and note that $\epsilon_r \mid \epsilon$ for each r by Proposition 2.4, so that GF$(p^{\epsilon_r}) \subseteq$ GF(p^ϵ). Thus, each indeterminate $x_{r,i}$ in $\rho(g)$ will be varied over some subset of GF(p^ϵ) of cardinality greater than any exponent which $x_{r,i}$ has in $\rho(g)$. Then Lemma 3.10 of [15], an elementary lemma on zeroes of polynomials over finite fields, shows that some assignment of values makes $\rho(g)$ nonvanishing. □

C. Combinatorial Analysis of Accounts

In this subsection, which is preliminary to our analysis of Abelian codes over $\mathbb{Z}_4$, we always assume $p = 2$ and that S is a 2-closed subset of A with $S \neq \emptyset$ and $S \neq \{1_A\}$, so that $B \neq \emptyset$. We shall be interested in unity-product but not all-unity multisets supported on S because such multisets play an important role in our Main Theorem (Theorem 3.1) and its ramifications. In particular, we shall investigate instances of such multisets having minimal or close-to-minimal cardinality, namely, the multisets in B_ℓ, $B_{\ell+1}$, and $B_{\ell+2}$.

We introduce some notation which we shall use in this and the following sections. We shall often write terms like $a^{n/2^k}$ where $a \in A$, $n \in \mathbb{Z}$, and $k \in \mathbb{N}$. This simply means a^{nm} where m is a multiplicative inverse modulo $|A|$ in $\mathbb{Z}$ of 2^k. We shall use the notation Γ_j to denote the set of all elements of B_j that are true sets, i.e., have only 0 and 1 as coefficients. Then set $\Gamma = \bigcup_{j\in\mathbb{N}} \Gamma_j$. For $\lambda \in \Gamma$ we also introduce the following associated sets of accounts:

$$E_{\lambda,1} = \{\lambda - a + 2a^{1/2} : a \in \lambda\},$$
$$E_{\lambda,2} = \{\lambda - (a+b) + 2(a^{1/2} + b^{1/2}) : a + b \subseteq \lambda\},$$

and

$$E_{\lambda,2'} = \{\lambda - a + a^{1/2} + 2a^{1/4} : a \in \lambda, a^{1/2} \notin \lambda\}.$$

Note that all the elements of these sets are unity-product, not all-unity multisets which are not sets. Furthermore, these multisets consist of elements in S since S is 2-closed. Any $\mu \in E_{\lambda,1}$ has $|\mu| = |\lambda| + 1$ and any $\mu \in E_{\lambda,2}$ or $E_{\lambda,2'}$ has $|\mu| = |\lambda| + 2$. Ultimately, we shall be able to classify elements of B_j for $j \le \ell + 2$ using the sets $\lambda \in \Gamma$ and such modified versions of λ as appear in the collections $E_{\lambda,x}$ described above. Our first step in this classification is to establish that our collections of the form $E_{\lambda,x}$ are disjoint.

Lemma 5.10: Suppose that λ, μ are unity-product, not all-unity subsets of S. Then for $x, y \in \{1, 2, 2'\}$, the sets $E_{\lambda,x}$ and $E_{\mu,y}$ are disjoint unless $\lambda = \mu$ and $x = y$.

Proof: Consider sets of the form $E_{\kappa,z}$ with κ a unity-product and not all-unity subset of S and $z \in \{1, 2, 2'\}$. If $z = 1$, then each $\nu \in E_{\kappa,1}$ has precisely one value of $a \in S$ such that $\nu_a \ge 2$ and for this a, we have $\nu_{a^2} \neq 1$ ($\nu_{a^2} = 0$ if $a \neq 1_A$ or $\nu_{a^2} = 2$ if $a = 1_A$). On the other hand, if $z = 2'$, then each $\nu \in E_{\kappa,2'}$ has precisely one value of $a \in S$ such that $\nu_a \ge 2$ and for this a, we have $\nu_{a^2} = 1$. Finally, if $z = 2$, then each $\nu \in E_{\kappa,2}$ has precisely two values of a such that $\nu_a \ge 2$. Thus, there is no overlap between sets of the form $E_{\kappa,z}$ if their second indices differ.

Now suppose that $E_{\lambda,x}$ and $E_{\mu,y}$ are not disjoint. From the previous paragraph, we must conclude that $x = y$. If $x = y = 1$, there is some $\nu = \lambda - a + 2a^{1/2} = \mu - b + 2b^{1/2}$ for some $a \in \lambda, b \in \mu$. So $a^{1/2}$ and $b^{1/2}$ both must be the unique element of S where ν takes a value two or greater. So $a = b$ and then $\lambda = \mu$. The proofs for $x = y = 2$ and $x = y = 2'$ are similar. □

We now provide the our classification of elements of B_j for sufficiently small j in the following proposition.

Proposition 5.11: Suppose that $m \le \ell$. Then

$$B_m = \Gamma_m \tag{7}$$

and every $\lambda \in B_m$ has $1_A \notin \lambda$. Also,

$$B_{m+1} = \Gamma_{m+1} \cup \left(\bigcup_{\lambda\in\Gamma_m} E_{\lambda,1} \right) \tag{8}$$

where all the unions are disjoint. Finally

$$B_{m+2} = \Gamma_{m+2} \cup \left(\bigcup_{\lambda\in\Gamma_{m+1}} E_{\lambda,1} \right) \cup \left(\bigcup_{\lambda\in\Gamma_m} E_{\lambda,2} \right) \cup \left(\bigcup_{\lambda\in\Gamma_m} E_{\lambda,2'} \right) \tag{9}$$

where all the unions are disjoint.

Proof: Note that the discussion before Lemma 5.10 proves that the right-hand sides of (7)–(9) are included in B_m, B_{m+1}, and B_{m+2}, respectively. We shall prove the other inclusions later. The unions are disjoint by Lemma 5.10 and because the sets Γ_j contain sets while the sets $E_{\lambda,x}$ contain multisets that are not sets. We shall occupy ourselves with proving the case $m = \ell$. Once we finish this, we shall show that the others follow almost immediately.

The proof of our claims above relies mainly on the following construction: Suppose that λ is a unity-product and not all-unity multiset supported on S with $\lambda_a \ge 2$ for some $a \in S$ (i.e., λ is a multiset but not a set). Then $\mu = \lambda - 2a + a^2$ is a unity-product and not all-unity multiset with $|\mu| = |\lambda| - 1$ and is supported on S because S is 2-closed. Thus, to prove (7) for $m = \ell$, note that if $B_\ell - \Gamma_\ell$ contained some element λ, then $B_{\ell-1}$ would contain the element μ constructed above from λ, violating the minimality of ℓ. If $\lambda \in B_\ell$ with $\lambda_{1_A} > 0$, then $\nu = \lambda - 1_A$ would be in $B_{\ell-1}$, contradicting the minimality of ℓ.

To prove (8) for $m = \ell$, let $\lambda \in B_{\ell+1} - \Gamma_{\ell+1}$ with $\lambda_a \ge 2$ and form μ as above. Then $\mu \in B_\ell = \Gamma_\ell$ and if we set $b = a^2$, then we have $\lambda = \mu - b + 2b^{1/2}$ with $b \in \mu$, i.e., $\lambda \in E_{\mu,1}$.

To prove (9) for $m = \ell$, let $\lambda \in B_{\ell+2} - \Gamma_{\ell+2}$ with $\lambda_a \ge 2$ and form μ as described in the first paragraph of this proof. Set $g = a^2$ and note that $g \in \mu$ and $\lambda = \mu - g + 2g^{1/2}$. Now $\mu \in B_{\ell+1}$ and we use (8) to classify μ. If $\mu \in \Gamma_{\ell+1}$, then we

see that $\lambda \in E_{\mu,1}$. So henceforth assume that $\mu = \nu - h + 2h^{1/2}$ for some $\nu \in \Gamma_\ell, h \in \nu$. Then $\lambda = \nu - (g+h) + 2(g^{1/2} + h^{1/2})$. If $g + h \subseteq \nu$, then we have $\lambda \in E_{\nu,2}$. So henceforth suppose that $g+h$ is not a subset of ν. So either $g = h$ (i.e., $g+h$ is not a set) or $g \notin \nu$. We claim that $g = h$ is impossible. If $g = h$, then $\nu - (g+h)$ has a negative value at $g = h$ since ν is a set. Then g is $g^{1/2} = h^{1/2}$ since $\lambda = \mu - (g+h) + 2(g^{1/2} + h^{1/2})$ is a multiset, but this implies $g = h = 1_A$. But then $1_A = h \in \nu \in B_\ell$, contradicting a previous part of this proposition. So $g \notin \nu$. But then $\nu - (g+h)$ has a negative value at g. Then g is either $g^{1/2}$ or $h^{1/2}$ since $\lambda = \mu - (g+h) + 2(g^{1/2} + h^{1/2})$ is a multiset. So $g = 1_A$ or $g = h^{1/2}$. In the former case, $\lambda = \nu + 1_A - h + 2h^{1/2}$ and note that $\nu + 1_A \in \Gamma_{\ell+1}$ (since $\nu \in B_\ell$, we must have $1_A \notin \nu$ by a previous part of this proposition) and we have $h \in \nu + 1_A$ and so $\lambda \in E_{\nu+1_A,1}$. In the latter case, we have $\lambda = \nu - h + h^{1/2} + 2h^{1/4}$ with $h \in \nu$ and $h^{1/2} = g \notin \nu$. Thus, $\lambda \in E_{\nu,2^r}$.

Now note that the cases where $m < \ell$ follow easily from what we have proved in the case $m = \ell$. Specifically, for $m < \ell$, $B_m = \Gamma_m = \emptyset$ so (7) is obvious. For $m = \ell - 1$, (8) becomes

$$B_\ell = \Gamma_\ell \cup \left(\bigcup_{\lambda \in \emptyset} E_{\lambda,1} \right)$$

which is just (7) when we had $m = \ell$. For $m < \ell - 1$, both sides of (8) are empty, so it is clearly true. The proofs of (9) for $m < \ell$ are similar. □

In the next subsection, we shall use this combinatorial classification of elements of B_j for sufficiently small j to compute 2-adic approximations of terms arising in our Main Theorem (Theorem 3.1) in the case where the alphabet is $\mathbb{Z}_4$. These calculations will be critical to proving the sharpness (in the sense described at the conclusion of Section V-A) of our analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_4$.

D. Polynomials Associated to Accounts

In our Main Theorem, we encounter terms of the form $\frac{\tilde{F}_\lambda}{\lambda!}$ where $F \in \mathbb{Z}_{p^\infty}[\zeta][A]$ is defined so that $\tilde{F} = \tau \circ \tilde{f}$ for some codeword $f \in \mathbb{Z}_{p^d}[A]$ and where λ is a unity-product but not all-unity multiset supported on some support S of $\hat{f}$. Such terms will naturally arise in our analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_4$. In order to prove the sharpness (in the sense described at the conclusion of Section V-A) of such analogs, we shall approximate 2-adically (i.e., modulo powers of 2) such terms as arise in our explorations.

In the remainder of this paper, all our theorems and lesser results will assume that $f \in \mathbb{Z}_4[A]$ is a codeword with $\hat{f}$ supported on a 2-closed set S and that $F \in \mathbb{Z}_{2^\infty}[\zeta][A]$ is the word with $\tilde{F} = \tau \circ \tilde{f}$. In stating and proving these results, and in employing them in the next section, we make use of the canonical expansions of Section II-A to write $\tilde{F}_a = \tilde{F}_a^{(0)} + 2\tilde{F}_a^{(1)}$. Note that only two terms appear in the canonical expansion since $\tilde{F}$ is obtained from $\tilde{f}$ by the standard lift. In this way, we define functions

$$\tilde{F}^{(i)} : A \to \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^\epsilon - 2}\}, \qquad \text{for } i = 0, 1.$$

We begin with our 2-adic approximations of $\frac{\tilde{F}_\lambda}{\lambda!}$ in the case where λ is a set.

Proposition 5.12: Let λ be a subset of S. Then

$$\frac{\tilde{F}_\lambda}{\lambda!} \equiv \tilde{F}_\lambda^{(0)} + 2\sum_{a \in \lambda} \tilde{F}_{\lambda - a}^{(0)} \tilde{F}_a^{(1)} + 4 \sum_{a+b \subseteq \lambda} \tilde{F}_{\lambda - a - b}^{(0)} \tilde{F}_{a+b}^{(1)} \pmod 8.$$

Proof: Since λ is a set, $\lambda_a = 0$ or 1 for all $a \in A$, and so $\lambda! = 1$. So

$$\frac{\tilde{F}_\lambda}{\lambda!} = \prod_{a \in \lambda} \left(\tilde{F}_a^{(0)} + 2\tilde{F}_a^{(1)} \right).$$

Expanding this product out and omitting terms whose coefficients vanish modulo 8 finishes the proof. □

Now we approximate terms associated to multisets μ which are not sets but which are in $E_{\lambda,1}$ for λ a set.

Proposition 5.13: Let λ be a subset of S. Then

$$\sum_{\mu \in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} \equiv \left(N_\lambda - \frac{|\lambda|}{2} \right) \tilde{F}_\lambda^{(0)} + (|\lambda| + 1) \sum_{a \in \lambda} \tilde{F}_{\lambda - a}^{(0)} \tilde{F}_a^{(1)} \pmod 2$$

where N_λ is the number of $a \in \lambda$ with $a = 1_A$ or $a^{1/2} \notin \lambda$. Thus, $\sum_{\mu \in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!}$ has 2-adic valuation at least -1 and is a 2-adic integer if $|\lambda|$ is even.

Proof: For each $a \in A$, let e_a be the account $-a + 2a^{1/2}$, so each $\mu \in E_{\lambda,1}$ is of the form $\mu = \lambda + e_a$ for some $a \in \lambda$. Then

$$\begin{aligned} \tilde{F}_{\lambda + e_a} &\equiv \left(\tilde{F}_{a^{1/2}}^{(0)} + 2\tilde{F}_{a^{1/2}}^{(1)} \right)^2 \prod_{b \in \lambda - a} \left(\tilde{F}_b^{(0)} + 2\tilde{F}_b^{(1)} \right) \\ &\equiv \left(\tilde{F}_{a^{1/2}}^{(0)} \right)^2 \left(\tilde{F}_{\lambda - a}^{(0)} + 2 \sum_{b \in \lambda - a} \tilde{F}_{\lambda - a - b}^{(0)} \tilde{F}_b^{(1)} \right) \\ &\equiv \tilde{F}_a^{(0)} \left(\tilde{F}_{\lambda - a}^{(0)} + 2 \sum_{b \in \lambda - a} \tilde{F}_{\lambda - a - b}^{(0)} \tilde{F}_b^{(1)} \right) \\ &\equiv \tilde{F}_\lambda^{(0)} + 2 \sum_{b \in \lambda - a} \tilde{F}_{\lambda - b}^{(0)} \tilde{F}_b^{(1)} \pmod 4 \end{aligned}$$

where we have used Corollary 2.3 in the first terms on either side the third congruence. Now if $\mu = \lambda + e_a$, we have $\mu_b = 0$ or 1 if $b \neq a^{1/2}$, so $\mu! = \mu_{a^{1/2}}!$. If $a = 1_A$, then $\mu_{a^{1/2}} = 2$, so $\mu! = 2$. If $a^{1/2} \notin \lambda$, then $\mu_{a^{1/2}} = 2$, so $\mu! = 2$. Otherwise, $a^{1/2} \in \lambda$ and $a^{1/2} \neq a$, so that $\mu_{a^{1/2}} = 3$ and $\mu! = 6$. So there are N_λ multisets μ in $E_{\lambda,1}$ with $\mu! = 2$ and the rest have $\mu! = 6$. Now

$$\sum_{\mu \in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} \equiv \sum_{\substack{a \in \lambda \\ (\lambda + e_a)! = 2}} \left(\frac{1}{2} \tilde{F}_\lambda^{(0)} + \sum_{b \in \lambda - a} \tilde{F}_{\lambda - b}^{(0)} \tilde{F}_b^{(1)} \right) + \sum_{\substack{a \in \lambda \\ (\lambda + e_a)! = 6}} \left(\frac{1}{6} \tilde{F}_\lambda^{(0)} + \frac{1}{3} \sum_{b \in \lambda - a} \tilde{F}_{\lambda - b}^{(0)} \tilde{F}_b^{(1)} \right) \pmod 2$$

and we know that the outer sums on the right-hand side index over sets of size N_λ and $|\lambda| - N_\lambda$, respectively, so that

$$\sum_{\mu\in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} \equiv \frac{|\lambda|+2N_\lambda}{6}\tilde{F}_\lambda^{(0)} + \sum_{\substack{a\in\lambda \\ (\lambda+e_a)!=2}} \sum_{b\in\lambda-a} \tilde{F}_{\lambda-b}^{(0)}\tilde{F}_b^{(1)} + \frac{1}{3}\sum_{\substack{a\in\lambda \\ (\lambda+e_a)!=6}} \sum_{b\in\lambda-a} \tilde{F}_{\lambda-b}^{(0)}\tilde{F}_b^{(1)} \pmod 2.$$

All the $\tilde{F}_a^{(k)}$ are 2-adic integers, and $\frac{1}{3} \equiv 1 \pmod 2$ and $\frac{1}{6} \equiv \frac{-1}{2} \pmod 2$, so we obtain

$$\sum_{\mu\in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} \equiv \left(N_\lambda - \frac{|\lambda|}{2}\right)\tilde{F}_\lambda^{(0)} + \sum_{a\in\lambda}\sum_{b\in\lambda-a} \tilde{F}_{\lambda-b}^{(0)}\tilde{F}_b^{(1)} \pmod 2.$$

We can simplify the double sum to a single sum to obtain

$$\sum_{\mu\in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} \equiv \left(N_\lambda - \frac{|\lambda|}{2}\right)\tilde{F}_\lambda^{(0)} + (|\lambda|-1)\sum_{a\in\lambda} \tilde{F}_{\lambda-a}^{(0)}\tilde{F}_a^{(1)} \pmod 2$$

and $-1 \equiv 1 \pmod 2$, thus finishing the proof. □

Corollary 5.14: For any $j \le \ell + 1$

$$\sum_{\lambda\in B_j} \frac{\tilde{F}_\lambda}{\lambda!}$$

has 2-adic valuation at least -1. If $j \le \ell$ or j is odd, then the sum is a 2-adic integer.

Proof: Since $j \le \ell + 1$, Proposition 5.11 shows that our sum is

$$\sum_{\lambda\in\Gamma_j} \frac{\tilde{F}_\lambda}{\lambda!} + \sum_{\lambda\in\Gamma_{j-1}}\sum_{\mu\in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!}.$$

Now all the terms of the first sum are 2-adic integers by Proposition 5.12 and all of the sums over $E_{\lambda,1}$ have 2-adic valuation at least -1 by Proposition 5.13. If $j \le \ell$, then Γ_{j-1} is empty and so the double sum vanishes. If j is odd, then our proposition tells us that the sums over $E_{\lambda,1}$ are 2-adic integers, since $j-1$ is even. □

We conclude with two lemmas which will be necessary for proving sharpness in a particular unusual case of our analog of McEliece's theorem for Euclidean weight in Abelian codes over $\mathbb{Z}_4$. This is the case when $B_2 = \emptyset$ but $B_3 \neq \emptyset$, and it is the only situation in which we must examine elements of B that have cardinality two more than the minimal cardinality. Both lemmas assert that we can approximate certain terms associated to such elements of B with polynomial functions of the $\tilde{F}_a^{(k)}$'s having the following property.

Property 5.15: The polynomial has coefficients in $\mathbb{Q}$, variables in the set $\{\tilde{F}_a^{(k)} : 0 \le k \le 1, a \in S\}$, no variable appears with exponent greater than one, and each monomial contains at most one variable in the set $\{\tilde{F}_a^{(1)} : a \in S\}$.

Now we state and prove our two lemmas.

Lemma 5.16: Suppose that $\ell = 3$ and let $\lambda \in B_3$. Then $\sum_{\mu\in E_{\lambda,2}} \frac{\tilde{F}_\mu}{\mu!}$ is congruent modulo 2 to a polynomial with Property 5.15.

Proof: Note that a sum of polynomials with Property 5.15 is a polynomial with Property 5.15. Thus, we shall prove the claim by showing that each term $\frac{\tilde{F}_\mu}{\mu!}$ in the sum is congruent modulo 2 to a polynomial with Property 5.15. Pick an arbitrary $\mu \in E_{\lambda,2}$ and write $\lambda = a + b + c$ and $\mu = 2a^{1/2} + 2b^{1/2} + c$ where a, b, and c are distinct elements of S. Here we have used the fact that $B_3 = \Gamma_3$ from Proposition 5.11, so that λ is a set. Then $\mu! = 4$ if $c \notin \{a^{1/2}, b^{1/2}\}$, otherwise, $\mu! = 12$. In either case, to show that $\frac{\tilde{F}_\mu}{\mu!}$ is congruent modulo 2 to a polynomial with Property 5.15, it suffices to show that $\tilde{F}_\mu$ is congruent modulo 8 to a polynomial with Property 5.15. Now

$$\tilde{F}_\mu = \left(\tilde{F}_c^{(0)} + 2\tilde{F}_c^{(1)}\right)\prod_{g\in\{a,b\}}\left(\tilde{F}_{g^{1/2}}^{(0)} + 2\tilde{F}_{g^{1/2}}^{(1)}\right)^2. \quad (10)$$

Note that

$$\left(\tilde{F}_{g^{1/2}}^{(0)} + 2\tilde{F}_{g^{1/2}}^{(1)}\right)^2 = \left(\tilde{F}_{g^{1/2}}^{(0)}\right)^2 + 4\tilde{F}_{g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)} + 4\left(\tilde{F}_{g^{1/2}}^{(1)}\right)^2$$

and applying Corollary 2.3, we obtain

$$\left(\tilde{F}_{g^{1/2}}^{(0)} + 2\tilde{F}_{g^{1/2}}^{(1)}\right)^2 = \tilde{F}_g^{(0)} + 4\tilde{F}_{g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)} + 4\tilde{F}_g^{(1)}.$$

Now substituting this into (10), we obtain

$$\tilde{F}_\mu = \left(\tilde{F}_c^{(0)} + 2\tilde{F}_c^{(1)}\right)\prod_{g\in\{a,b\}}\left(\tilde{F}_g^{(0)} + 4\tilde{F}_{g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)} + 4\tilde{F}_g^{(1)}\right).$$

Expanding the product out, we obtain

$$\tilde{F}_\mu \equiv \tilde{F}_\lambda^{(0)} + 2\tilde{F}_{\lambda-c}^{(0)}\tilde{F}_c^{(1)} + 4\tilde{F}_{\lambda-b}^{(0)}\tilde{F}_b^{(1)} + 4\tilde{F}_{\lambda-a}^{(0)}\tilde{F}_a^{(1)} + 4\tilde{F}_{\lambda-a+a^{1/2}}^{(0)}\tilde{F}_{a^{1/2}}^{(1)} + 4\tilde{F}_{\lambda-b+b^{1/2}}^{(0)}\tilde{F}_{b^{1/2}}^{(1)} \pmod 8.$$

Now all the terms on the right-hand side surely have Property 5.15 except possibly the terms $4\tilde{F}_{\lambda-g+g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)}$ for $g \in \{a, b\}$. Such a term will not have all exponents less than or equal to one if $\lambda - g + g^{1/2}$ is not a set. In such a case, we shall show that $\tilde{F}_{\lambda-g+g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)}$ can be replaced with a polynomial with Property 5.15. Since $\lambda - g + g^{1/2}$ is assumed not to be a set, we have $g^{1/2} \in \lambda - g$. Then $\lambda - g + g^{1/2} = 2g^{1/2} + h$ where h is the unique element of $\lambda - g - g^{1/2}$. Then λ is the set $g + g^{1/2} + h$ and

$$\begin{aligned}\tilde{F}_{\lambda-g+g^{1/2}}^{(0)}\tilde{F}_{g^{1/2}}^{(1)} &= \left(\tilde{F}_{g^{1/2}}^{(0)}\right)^2\tilde{F}_h^{(0)}\tilde{F}_{g^{1/2}}^{(1)} \\ &= \tilde{F}_g^{(0)}\tilde{F}_h^{(0)}\tilde{F}_{g^{1/2}}^{(1)}\end{aligned}$$

where we have used Corollary 2.3 in the last equality. But this last polynomial has Property 5.15. □

Our second lemma deals with terms associated with elements of $E_{\lambda,2'}$ just as the previous one dealt with terms associated with elements of $E_{\lambda,2}$.

Lemma 5.17: Suppose that $\ell = 3$ and let $\lambda \in B_3$. Then $\sum_{\mu \in E_{\lambda,2'}} \frac{\tilde{F}_\mu}{\mu!}$ is congruent modulo 2 to a polynomial with Property 5.15.

Proof: Note that a sum of polynomials with Property 5.15 is a polynomial with Property 5.15. Thus, we shall prove the claim by showing that each term $\frac{\tilde{F}_\mu}{\mu!}$ in the sum is congruent modulo 2 to a polynomial with Property 5.15. Pick an arbitrary $\mu \in E_{\lambda,2'}$ and write $\lambda = a+b+c$ and $\mu = 2a^{1/4}+a^{1/2}+b+c$, where a, b, and c are distinct elements of S. Here we have used the fact that $B_3 = \Gamma_3$ from Proposition 5.11, so that λ is a set. Then note that $a^{1/2} \notin \{b,c\}$ by the definition of $E_{\lambda,2'}$. Thus, $\mu! = 2$ if $a^{1/4} \notin \{a^{1/2}, b, c\}$, otherwise, $\mu! = 6$. In either case, to show that $\frac{\tilde{F}_\mu}{\mu!}$ is congruent modulo 2 to a polynomial with Property 5.15, it suffices to show that $\tilde{F}_\mu$ is congruent modulo 4 to a polynomial with Property 5.15. Now

$$\tilde{F}_\mu = \left(\tilde{F}^{(0)}_{a^{1/4}} + 2\tilde{F}^{(1)}_{a^{1/4}}\right)^2 \prod_{g \in \{a^{1/2},b,c\}} \left(\tilde{F}^{(0)}_g + 2\tilde{F}^{(1)}_g\right).$$

So

$$\begin{aligned}\tilde{F}_\mu &\equiv \left(\tilde{F}^{(0)}_{a^{1/4}}\right)^2 \prod_{g \in \{a^{1/2},b,c\}} \left(\tilde{F}^{(0)}_g + 2\tilde{F}^{(1)}_g\right) \\ &\equiv \tilde{F}^{(0)}_{a^{1/2}} \prod_{g \in \{a^{1/2},b,c\}} \left(\tilde{F}^{(0)}_g + 2\tilde{F}^{(1)}_g\right) \pmod 4\end{aligned}$$

where the last congruence uses Corollary 2.3. Thus,

$$\tilde{F}_\mu \equiv \left[\left(\tilde{F}^{(0)}_{a^{1/2}}\right)^2 + 2\tilde{F}^{(0)}_{a^{1/2}}\tilde{F}^{(1)}_{a^{1/2}}\right] \prod_{g \in \{b,c\}} \left(\tilde{F}^{(0)}_g + 2\tilde{F}^{(1)}_g\right) \pmod 4$$

and another application of Corollary 2.3 gives

$$\tilde{F}_\mu \equiv \left(\tilde{F}^{(0)}_a + 2\tilde{F}^{(0)}_{a^{1/2}}\tilde{F}^{(1)}_{a^{1/2}}\right) \prod_{g \in \{b,c\}} \left(\tilde{F}^{(0)}_g + 2\tilde{F}^{(1)}_g\right) \pmod 4.$$

Thus,

$$\tilde{F}_\mu \equiv \tilde{F}^{(0)}_\lambda + 2\tilde{F}^{(0)}_{\lambda-b}\tilde{F}^{(1)}_b + 2\tilde{F}^{(0)}_{\lambda-c}\tilde{F}^{(1)}_c + 2\tilde{F}^{(0)}_{\lambda-a+a^{1/2}}\tilde{F}^{(1)}_{a^{1/2}} \pmod 4.$$

Now all the terms on the right-hand side have Property 5.15 once we establish that $\lambda - a + a^{1/2}$ is a set. But

$$\lambda - a + a^{1/2} = b + c + a^{1/2} \quad \text{and} \quad a^{1/2} \notin \{b,c\}$$

by the definition of $E_{\lambda,2'}$, so we are done. □

Now armed with sufficient knowledge of unity-product, not all-unity accounts $\lambda \in B$, and the terms $\frac{\tilde{F}_\lambda}{\lambda!}$ associated to them, we are ready to prove sharp analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_4$.

E. Analogs of McEliece's Theorem for Abelian Codes Over $\mathbb{Z}_4$

Here we present sharp analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_4$, where our notion of "sharpness" is essentially as described at the conclusion of Section V-A. To be more precise, we shall describe the common assumptions for the theorems in this subsection and examine more carefully what we mean by sharpness. We assume that S is 2-closed and we always consider the code $\mathcal{C}$ consisting of all words whose Fourier transform is supported on S. Note that in doing this for all 2-closed subsets S of A, we are not examining all Abelian codes over $\mathbb{Z}_4$, as different codes can have the same minimal support for their Fourier transform. As we saw in Corollary 2.6, only the tower of supports of the Fourier transform, i.e., the minimal support of the Fourier transform along with the minimal support of the Fourier transform modulo 2, fully characterizes an Abelian code over $\mathbb{Z}_4$. Our sharp analogs of McEliece's theorem can be summarized as follows: For a given weight function wt of interest, we prove that there is some m so that $\mathrm{wt}(f) - |A|\mathrm{wt}(\tilde{f}_1)$ is divisible by 2^m for all $f \in \mathcal{C}$. This m depends on wt and S. The results are sharp in the sense that there is some word $f \in \mathcal{C}$ such that $\mathrm{wt}(f) - |A|\mathrm{wt}(\tilde{f}_1)$ is not divisible by 2^{m+1}.

1) Hamming Weight and Number of Occurrences of a Symbol: First we present the analogs to McEliece's theorem where the weight function is one that counts symbols:

Theorem 5.18: Set $m = \left\lfloor \frac{\ell}{2} \right\rfloor$ so that $2m \le \ell \le 2m+1$. Then for $m = 1$ and $\mathrm{wt} \in \{\mathrm{symb}_1, \mathrm{symb}_3\}$ or for $m > 1$ and $\mathrm{wt} \in \{\mathrm{zer}, \mathrm{symb}_2, \mathrm{ham}\}$, we have

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + 2^{m-1} \sum_{j=2m}^{2m+1} \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}. \tag{11}$$

For $m = 1$ and $\mathrm{wt} \in \{\mathrm{zer}, \mathrm{symb}_2, \mathrm{ham}\}$ or for $m > 1$ and $\mathrm{wt} \in \{\mathrm{symb}_1, \mathrm{symb}_3\}$, we have

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + 2^{m-1} \sum_{\lambda \in B_{2m+1}} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}. \tag{12}$$

The sums over B_j in the above congruences are 2-adic integers, so that $\mathrm{wt}(f) \equiv |A|\mathrm{wt}(\tilde{f}_1) \pmod{2^{m-1}}$. If we vary f over all codewords with $\tilde{f}$ supported on S, then $\mathrm{wt}(f) \not\equiv |A|\mathrm{wt}(\tilde{f}_1) \pmod{2^m}$ for some codeword.

Proof: By combining the Main Theorem (Theorem 3.1) with Corollary 4.27, we obtain

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + \sum_{j=2}^{2m+1} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}$$

where $h(x) = \sum_{j=0}^{2m+1} h_j x^j$ is the polynomial of degree $2m+1$ described in Corollary 4.27 which approximates $\mathrm{wt} \circ \pi$ uniformly modulo 2^m. Since $B_j = \emptyset$ for $j < 2m$, we have

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + \sum_{j=2m}^{2m+1} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}.$$

Now Corollary 5.14 shows that the sums over B_j are all 2-adic integers. We use the information about the coefficients of h given in Corollary 4.27 to obtain

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + 2^{m-1} \sum_{j=2m}^{2m+1} \gamma_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}$$

where $\gamma_{2m+1} = 1$ and $\gamma_{2m} \in \{0, 1\}$ has a value which depends on the weight function wt and m, thus giving (11) or (12) in the appropriate cases.

Now we use Proposition 5.11 to obtain

$$\frac{1}{|A|}\mathrm{wt}(f) \equiv \mathrm{wt}(\tilde{f}_1) + 2^{m-1}\sum_{j=2m}^{2m+1}\gamma_j \sum_{\lambda\in\Gamma_j}\frac{\tilde{F}_\lambda}{\lambda!} + 2^{m-1}\sum_{\lambda\in\Gamma_{2m}}\sum_{\mu\in E_{\lambda,1}}\frac{\tilde{F}_\mu}{\mu!} \pmod{2^m}.$$

Then we use Propositions 5.12 and 5.13 to obtain

$$\begin{aligned}\frac{1}{|A|}\mathrm{wt}(f) \equiv{}& \mathrm{wt}(\tilde{f}_1) + 2^{m-1}\sum_{j=2m}^{2m+1}\gamma_j\sum_{\lambda\in\Gamma_j}\tilde{F}^{(0)}_\lambda \\ &+ 2^{m-1}\sum_{\lambda\in\Gamma_{2m}}(N_\lambda - m)\tilde{F}^{(0)}_\lambda \\ &+ 2^{m-1}\sum_{\lambda\in\Gamma_{2m}}\sum_{a\in\lambda}\tilde{F}^{(0)}_{\lambda-a}\tilde{F}^{(1)}_a \pmod{2^m}\end{aligned}$$

where N_λ is as defined in Proposition 5.13. Thus,

$$\begin{aligned}&\frac{1}{|A|}\mathrm{wt}(f) - \mathrm{wt}(\tilde{f}_1) \\ &\equiv 2^{m-1}\sum_{\lambda\in\Gamma_{2m}}(\gamma_{2m} + N_\lambda + m)\tilde{F}^{(0)}_\lambda \\ &\quad + 2^{m-1}\sum_{\lambda\in\Gamma_{2m+1}}\tilde{F}^{(0)}_\lambda \\ &\quad + 2^{m-1}\sum_{\lambda\in\Gamma_{2m}}\sum_{a\in\lambda}\tilde{F}^{(0)}_{\lambda-a}\tilde{F}^{(1)}_a \pmod{2^m}.\end{aligned}$$

Now we regard the right-hand side as a polynomial with variables in $\{\tilde{F}^{(k)}_a : 0 \le k \le 1, a \in S\}$. Note that no variable appears with exponent greater than one. The monomials in each of the sums are distinct, since those in the second sum have higher total degree than the others and those in the last sum have variables of the form $\tilde{F}^{(1)}_a$ which do not appear in the others. Finally, at least one of the latter two sums is nonempty, since $B_\ell \neq \emptyset$ by choice of ℓ, $\Gamma_\ell = B_\ell$ by Proposition 5.11, and $\ell = 2m$ or $2m+1$ by choice of m. Therefore, we know that some monomial has coefficient with 2-adic valuation precisely $m-1$ and clearly all monomials have coefficients with 2-adic valuation at least $m-1$. Thus, we may apply Proposition 5.9 to prove that $\frac{1}{|A|}\mathrm{wt}(f) - \mathrm{wt}(\tilde{f}_1)$ always vanishes modulo 2^{m-1} but does not vanish modulo 2^m for some codeword $f \in \mathbb{Z}_4[A]$ with $\hat{f}$ supported on S. □

This proves Wilson's strengthening ([16, Theorem 3], [17, Theorem 9]) of the results of Calderbank, Li, and Poonen ([10, Corollary 3.6]) and, in addition, shows that it is sharp. It also generalizes Wilson's result to Abelian codes. The improved result states that when $\hat{f}_1 = 0$, the Hamming weight is divisible by $2^{\lfloor \frac{\ell}{2}\rfloor - 1}$, while the result of Calderbank *et al.* states that the Hamming weight is divisible by $2^{\max\{\lceil \frac{\ell}{2}\rceil - 2, \lceil \frac{\ell}{3}\rceil - 1\}}$ (also assuming that A is cyclic). The theorem here is stronger by an additional power of 2 when ℓ is even and greater than or equal to 6. Otherwise, the results match. For example, if A is the cyclic group of order 63 generated by the element a and we consider codewords whose Fourier transforms are supported on $S = \{a, a^2, a^4, a^8, a^{16}, a^{32}\}$, then $\ell = 6$ and the strengthened theorem tells us that Hamming weights are divisible by 4, while Corollary 3.6 of Calderbank *et al.* tells us only that Hamming weights are even.

2) Lee Weight: Now we examine Lee weight for Abelian codes over $\mathbb{Z}_4$. The theorem and its proof are quite similar to the one for symbol counts and Hamming weights above.

Theorem 5.19: Set $m = \lfloor \frac{\ell}{2}\rfloor + 1$ so that $2m - 2 \le \ell \le 2m - 1$. Then we have

$$\frac{1}{|A|}\mathrm{lee}(f) \equiv \mathrm{lee}(\tilde{f}_1) + 2^{m-1}\sum_{j=2m-2}^{2m-1}\sum_{\lambda\in B_j}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}.$$

The sums over B_j here are 2-adic integers, so that

$$\mathrm{lee}(f) \equiv |A|\mathrm{lee}(\tilde{f}_1) \pmod{2^{m-1}}.$$

If we vary f over all codewords with $\hat{f}$ supported on S, then $\mathrm{lee}(f) \not\equiv |A|\mathrm{lee}(\tilde{f}_1) \pmod{2^m}$ for some codeword.

Proof: The proof is similar to that of Theorem 5.18. □

This proves Wilson's strengthening ([16, Theorem 2]) of the results of Calderbank, Li, and Poonen ([10, Corollary 3.6]) and, in addition, shows that it is sharp. It also generalizes Wilson's result to Abelian codes. Calderbank *et al.* state that when $\hat{f}_1 = 0$, the Lee weights are divisible by $2^{\lceil \frac{\ell}{2}\rceil - 1}$ (in the case where A is cyclic). The improved result states that the Lee weights are divisible by $2^{\lfloor \frac{\ell}{2}\rfloor}$ when $\hat{f}_1 = 0$. This strengthened version is stronger by an additional power of 2 for ℓ even. Otherwise the results match.

3) Euclidean Weight: In our last theorem, we examine Euclidean weight for Abelian codes over $\mathbb{Z}_4$. The spirit of the proof is the same as that of the proof of Theorem 5.18, and the analysis of most cases closely parallels the analysis found in that proof, but the cases when ℓ is small are somewhat idiosyncratic because of the peculiar efficacy of polynomials in approximating $\mathrm{euc} \circ \pi$ modulo small powers of 2. Thus, the statement and proof of the theorem are somewhat more intricate.

Theorem 5.20: If $\ell = 2$, we have

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2\sum_{\lambda\in B_2}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{8}$$

and $\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{2}$ for all codewords f with $\hat{f}$ supported on S, but $\mathrm{euc}(f) \not\equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{4}$ for some such codeword. If $\ell = 3$, then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 6\sum_{\lambda\in B_3}\frac{\tilde{F}_\lambda}{\lambda!} - 24\sum_{\lambda\in B_5}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{16} \tag{13}$$

and $\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{8}$ for all codewords f with $\hat{f}$ supported on S, but $\mathrm{euc}(f) \not\equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{16}$ for some such codeword. If $\ell = 4$ or 5, then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 8\sum_{\lambda\in B_5}\frac{\tilde{F}_\lambda}{\lambda!} \pmod{16}$$

and $\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{8}$ for all codewords f with $\hat{f}$ supported on S, but $\mathrm{euc}(f) \not\equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{16}$ for

some such codeword. If $\ell > 5$, set $m = \lfloor \frac{\ell}{2} \rfloor + 2$ so that $2m-4 \leq \ell \leq 2m-3$. Then

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2^{m-1} \sum_{j=2m-4}^{2m-3} \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{2^m}.$$

The sums over B_j here are 2-adic integers, so that $\mathrm{euc}(f) \equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{2^{m-1}}$. If we vary f over all codewords with $\hat{f}$ supported on S, then $\mathrm{euc}(f) \not\equiv |A|\mathrm{euc}(\tilde{f}_1) \pmod{2^m}$ for some codeword.

Proof: First suppose that $\ell = 2$. By combining the Main Theorem (Theorem 3.1) with Corollary 4.29, we obtain

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2 \sum_{\lambda \in B_2} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{8}$$

since x^2 is a polynomial which approximates $\mathrm{euc} \circ \pi$ uniformly modulo 8. By Corollary 5.14, the sum in our congruence is a 2-adic integer and by using Proposition 5.11, we have

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + 2 \sum_{\lambda \in \Gamma_2} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{8}.$$

Thus, by Proposition 5.12, we have

$$\frac{1}{|A|}\mathrm{euc}(f) - \mathrm{euc}(\tilde{f}_1) \equiv 2 \sum_{\lambda \in \Gamma_2} \tilde{F}_\lambda^{(0)} + 4 \sum_{\lambda \in \Gamma_2} \sum_{a \in \lambda} \tilde{F}_{\lambda-a}^{(0)} \tilde{F}_a^{(1)} \pmod{8}.$$

Now we regard the right hand side as a polynomial with variables in $\{\tilde{F}_a^{(k)} : 0 \leq k \leq 1, a \in S\}$. Note that no variable appears with exponent greater than one. The monomials in each of the sums are distinct, since those in the second sum have variables of the form $\tilde{F}_a^{(1)}$ which do not appear in the others. The minimal 2-adic valuations of the coefficients is 1. Thus, we may apply Proposition 5.9 to prove that $\frac{1}{|A|}\mathrm{euc}(f) - \mathrm{euc}(\tilde{f}_1)$ always vanishes modulo 2 but does not vanish modulo 4 for some codeword $f \in \mathbb{Z}_4[A]$ with $\hat{f}$ supported on S.

Now suppose that $\ell = 3$. By combining the Main Theorem with Corollary 4.29, we obtain

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + \sum_{j=2}^{5} j! h_j \sum_{\lambda \in B_j} \frac{\tilde{F}_\lambda}{\lambda!} \pmod{16}$$

where

$$h(x) = \sum_{j=0}^{5} h_j x^j = -\frac{1}{5}x^5 + \frac{8}{3}x^4 - \frac{37}{3}x^3 + \frac{67}{3}x^2 - \frac{172}{15}x$$

so that $5!h_5 = -24$, $4!h_4 = 64$, and $3!h_3 = -74$. First note that Corollary 5.14 shows that the 2-adic valuation of $\sum_{\lambda \in B_4} \frac{\tilde{F}_\lambda}{\lambda!}$ is at least -1. Thus, the 2-adic valuation of

$$4!h_4 \sum_{\lambda \in B_4} \frac{\tilde{F}_\lambda^{(0)}}{\lambda!}$$

is at least 5 and so vanishes modulo 16. So the $j = 4$ term drops out of the sum. Now Corollary 5.14 shows us that the sum over B_3 is a 2-adic integer, so we may replace $3!h_3 = -74$ with 6 in our congruence to obtain (13).

We use Proposition 5.11 to obtain

$$\begin{aligned}\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) &+ 6 \sum_{\lambda \in \Gamma_3} \frac{\tilde{F}_\lambda}{\lambda!} - 24 \sum_{\lambda \in \Gamma_5} \frac{\tilde{F}_\lambda}{\lambda!} \\ &- 24 \sum_{\lambda \in \Gamma_4} \sum_{\mu \in E_{\lambda,1}} \frac{\tilde{F}_\mu}{\mu!} - 24 \sum_{\lambda \in \Gamma_3} \sum_{\mu \in E_{\lambda,2}} \frac{\tilde{F}_\mu}{\mu!} \\ &- 24 \sum_{\lambda \in \Gamma_3} \sum_{\mu \in E_{\lambda,2'}} \frac{\tilde{F}_\mu}{\mu!} \pmod{16}. \qquad (14)\end{aligned}$$

Now we claim that $\frac{1}{|A|}\mathrm{euc}(f) - \mathrm{euc}(\tilde{f}_1)$ can be approximated modulo 16 as a polynomial in variables $\{\tilde{F}_a^{(k)} : 0 \leq k \leq 1, a \in S\}$ having rational coefficients, where the maximum exponent of any given variable is one and where the minimum 2-adic valuation of the coefficients is 3. We begin the proof of this by replacing the summands of the first sum over Γ_3 on the right-hand side of (14) with their approximations modulo 8 from Proposition 5.12. We also replace the summands of the first sum over Γ_5 with their approximations modulo 2 from Proposition 5.12. Then replace the sums over $E_{\lambda,1}$ (resp., $E_{\lambda,2}$, $E_{\lambda,2'}$) with their approximations modulo 2 in Proposition 5.13 (resp., Lemma 5.16, Lemma 5.17). This will give

$$\frac{1}{|A|}\mathrm{euc}(f) \equiv \mathrm{euc}(\tilde{f}_1) + g \pmod{16}$$

where g is a polynomial with rational coefficients and variables in the set we specified and no variable appears with exponent greater than one. Furthermore, the polynomials which arise from the application of Proposition 5.13 and Lemmas 5.16 and 5.17 have Property 5.15. On the other hand, the polynomial arising from the two applications of Proposition 5.12 is

$$\begin{aligned}6 \sum_{\lambda \in \Gamma_3} \tilde{F}_\lambda^{(0)} &+ 12 \sum_{\lambda \in \Gamma_3} \sum_{a \in \lambda} \tilde{F}_{\lambda-a}^{(0)} \tilde{F}_a^{(1)} \\ &+ 24 \sum_{\lambda \in \Gamma_3} \sum_{a+b \subseteq \lambda} \tilde{F}_{\lambda-a-b}^{(0)} \tilde{F}_{a+b}^{(1)} + 24 \sum_{\lambda \in \Gamma_5} \tilde{F}_\lambda^{(0)}\end{aligned}$$

which has the monomial $24\tilde{F}_a^{(0)}\tilde{F}_b^{(1)}\tilde{F}_c^{(1)}$ where $\lambda = a + b + c$ is some element of Γ_3. Because the other polynomials have Property 5.15, they do not have this monomial. Thus, g has some monomial whose coefficient has a 2-adic valuation of 3. We claim that g has no monomials with 2-adic valuation less than 3. For if this were the case, then we could use Proposition 5.9 to prove that there is a codeword f with $\hat{f}$ supported on S and with

$$\frac{1}{|A|}\mathrm{euc}(f) - \mathrm{euc}(\tilde{f}_1) \not\equiv 0 \pmod{8}.$$

But this would contradict the latter part of Theorem 5.7 (applied with $d = 2$). Thus, we have proved our claim about our polynomial g. So we may apply Proposition 5.9 to prove that $\frac{1}{|A|}\mathrm{euc}(f) - \mathrm{euc}(\tilde{f}_1)$ always vanishes modulo 8 but does not vanish modulo 16 for some codeword $f \in \mathbb{Z}_4[A]$ with $\hat{f}$ supported on S.

The cases $4 \leq \ell \leq 5$ and $\ell > 5$ have proofs similar to that of Theorem 5.18. □

This slightly strengthens the results of Calderbank, Li, and Poonen [10] and proves that the strengthening is sharp in our usual sense. Their Corollary 3.6 states that when $\hat{f}_1 = 0$, the Euclidean weights are divisible by $2^{\lceil \frac{\ell}{2} \rceil}$ (in the case where A is cyclic). Our theorem states that the Euclidean weights are always even, divisible by 8 if $\ell > 2$, and divisible by $2^{\lfloor \frac{\ell}{2} \rfloor + 1}$ when $\ell \geq 6$. Our theorem is stronger by an additional power of 2 when $\ell = 3$ or is an even number greater than or equal to 4. Otherwise the results match.

VI. Conclusion

Counting polynomial techniques have been used here to prove some new analogs of McEliece's theorem for Abelian codes over $\mathbb{Z}_{p^d}$. It is hoped that the theorems proved here will be useful to coding theorists analyzing cyclic and Abelian codes over $\mathbb{Z}_4$. Such counting polynomial techniques show great promise for attacking further problems in coding theory and combinatorics, some of which is intimated in [17]. We intend to deal with the application to codes whose alphabets are arbitrary finite fields and Galois rings in another paper.

Acknowledgment

The author would like to thank R. M. Wilson for introducing him to this area of research and for much advice and support. The author also wishes to thank R. J. McEliece for his interest, support, and for drawing his attention to [15], which greatly informed and influenced these researches. Finally, the author thanks an anonymous referee for a careful reading of the manuscript and for the useful suggestion that guiding examples on counting polynomials and the Main Theorem be included.

References

[1] 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.

[2] I. F. Blake, "Codes over certain rings," *Inf. Contr.*, vol. 20, pp. 396–404, 1972.

[3] ——, "Codes over integer residue rings," *Inf. Contr.*, vol. 29, pp. 295–300, 1975.

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

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

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

[7] S. K. Wasan, "On codes over $\mathbb{Z}_m$," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 1, pp. 117–120, Jan. 1982.

[8] 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.

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

[10] 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.

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

[12] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, "Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$-linear trace codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 4, pp. 1212–1216, Jul. 1996.

[13] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.

[14] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, "Ternary m-sequences with three-valued cross-correlation: New decimations of Welch and Niho type," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1473–1481, May 2001.

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

[16] R. M. Wilson, "A version for the Lee metric of a theorem of McEliece and weights of codewords in cyclic codes," unpublished paper, Feb. 1995.

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

[18] E. Dubois and A. N. Venetsanopoulos, "The discrete Fourier transform over finite rings with application to fast convolution," *IEEE Trans. Comput.*, vol. C-27, no. 7, pp. 586–593, Jul. 1978.

[19] J.-P. Serre, *A Course in Arithmetic*. New York: Springer-Verlag, 1973.

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

[21] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 456–468, Mar. 1995.

[22] J.-P. Serre, *Local Fields*. New York: Springer-Verlag, 1979.

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

[24] 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.

[25] R. A. Scholtz and L. R. Welch, "Group characters: Sequences with good correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 537–545, Sep. 1978.

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

[27] 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.