On p-Adic Estimates of Weights in Abelian Codes over Galois Rings

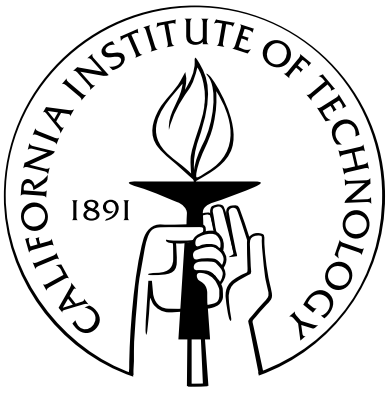
Thesis by

Daniel J. Katz

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy



California Institute of Technology

Pasadena, California

2005

(Defended May 11, 2005)

ΚΑΙ ’ΕΙΠΕΝ ΔΑΝΙΗΛ ’ΕΜΝΗΣΘΗΣ ΓΑΡ ΜΟΥ ‘Ο ΘΕΟΣ

Acknowledgements

I cannot thank Rick Wilson enough for getting me interested in this line of research and for invaluable assistance along the way. His elegant approach to mathematics is truly inspiring, and this work would never have been achieved without him first showing me how to do difficult things easily. He has always been a supportive, patient, good-humored, and fun advisor.

I also thank Bob McEliece, not only for serving as a member of my thesis committee, but also for having started this area of research in the 1960s with Gustave Solomon. Professor McEliece has been of great help in letting me know about past work, especially [18], which has greatly informed all of this research. He has also been very supportive about my work and has pointed me in fruitful directions.

I thank Dinakar Ramakrishnan and David Wales, the other members of my thesis committee, for their time and patience. Both have served at times as the graduate representative in the mathematics department, and both have helped me whenever I have asked them about anything. Thanks also go to Nick Katz for his gracious reply to a query about his work, and to Rob Calderbank for his encouragement. Many of my fellow graduate students have helped me by answering questions, discussing things, listening to my talks, and the like: Matthew Gealy, David Grynkiewicz, Tejaswi Navilarekallu, Carlos Salazar-Lazaro, Dave Whitehouse, and Bahattin Yildiz. Thanks go to Kimball Martin for answering many thesis quodlibets.

I thank the Caltech Mathematics Department for supporting me during my studies. Gary Lorden, who introduced me to the department when he was graduate representative and who sees me through now while he is department chair, deserves special mention for always being supportive and gracious. Great thanks go to the department staff for their

invaluable assistance: Kathy Carreon, Stacey Croomes, Pamela Fong, Cherie Galvez, Sara Mena, Seraj Muhammed, and Elizabeth Wood, along with Shirley Beatty of the electrical engineering department staff. I thank the graduate office staff for their assistance and the anonymous proofreader for checking the text. I also thank Steve and Rosemary Johnson for financial assistance in the form of the Scott Russell Johnson Prize.

I thank my friends, who have given me much encouragement: Roberto Aparicio Joo, Isaac Chenchiah, Francisco Godoy, Jennifer Johnson, Christopher Lee, Mihai Stoiciu, Seth Thomas, Ivan Veselič, Winnie Wang, and many others. I thank my mother and father for their unflagging support.

Abstract

Let p be a prime. We prove various analogues and generalizations of McEliece's theorem on the p-divisibility of weights of words in cyclic codes over a finite field of characteristic p. Here we consider Abelian codes over various Galois rings. We present four new theorems on p-adic valuations of weights. For simplicity of presentation here, we assume that our codes do not contain constant words.

The first result has two parts, both concerning Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$. The first part gives a lower bound on the p-adic valuations of Hamming weights. This bound is shown to be sharp: for each code, we find the maximum k such that p^k divides all Hamming weights. The second part of our result concerns the number of occurrences of a given nonzero symbol $s \in \mathbb{Z}/p^d\mathbb{Z}$ in words of our code; we call this number the *s-count*. We find a j such that p^j divides the s-counts of all words in the code. Both our bounds are stronger than previous ones for infinitely many codes.

The second result concerns Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. We give a sharp lower bound on the 2-adic valuations of Lee weights. It improves previous bounds for infinitely many codes.

The third result concerns Abelian codes over arbitrary Galois rings. We give a lower bound on the p-adic valuations of Hamming weights. When we specialize this result to finite fields, we recover the theorem of Delsarte and McEliece on the p-divisibility of weights in Abelian codes over finite fields.

The fourth result generalizes the Delsarte-McEliece theorem. We consider the number of components in which a collection $c_1, \ldots, c_t$ of words all have the zero symbol; we call this the *simultaneous zero count.* Our generalized theorem p-adically estimates simultaneous zero counts in Abelian codes over finite fields, and we can use it to prove the theorem of N. M. Katz on the p-divisibility of the cardinalities of affine algebraic sets over finite fields.

Contents

Summary of Notation and Definitions

The following tables give the basic definitions and notations that hold throughout this thesis. The section of Chapter 2 where an item first appears is given in the rightmost column.

$\mathbb{Z}$	the rational integers	2.1
$\mathbb{Z}_+$	the strictly positive rational integers	2.1
$\mathbb{N}$	the nonnegative rational integers	2.1
$\mathbb{Q}$	the rational numbers	2.1
p	a rational prime	2.1
$\mathbb{Z}_p$	the p-adic integers	2.1
$\mathbb{Q}_p$	the p-adic rationals	2.1
ζ_n	a root of unity of order n over $\mathbb{Q}_p$	2.1
$\mathbb{F}_{p^n}$	the finite field with p^n elements	2.1
$\mathbb{Z}/m\mathbb{Z}$	the rational integers modulo m	2.1
$\mathrm{GR}(p^m, n)$	the Galois ring of characteristic p^m of order p^{mn}	2.1
π_m	reduction modulo p^m on Galois rings and on $\mathbb{Z}_p[\zeta_{p^n-1}]$	2.1
π_∞	the identity map on $\mathbb{Z}_p[\zeta_{p^n-1}]$	2.1
τ_m	the Teichmüller lift to characteristic p^m on Galois rings	2.1
τ_∞	the Teichmüller lift to characteristic 0 on Galois rings	2.1
v_p	the p-adic valuation in $\mathbb{Q}_p(\zeta_{p^n-1})$ and $\mathrm{GR}(p^m, n)$	2.1
Fr	the Frobenius automorphism on $\mathbb{Q}_p(\zeta_{p^n-1})$ and $\mathrm{GR}(p^m, n)$	2.1
$\mathrm{Tr}_{n_1}^{n_2}$	the trace from $\mathbb{Q}_p(\zeta_{p^{n_2}-1})$ to $\mathbb{Q}_p(\zeta_{p^{n_1}-1})$ and the trace from $\mathrm{GR}(p^m, n_2)$ to $\mathrm{GR}(p^m, n_1)$	2.1

A	a finite Abelian group with $p \nmid \lvert A\rvert$	2.2
$R[A]$	the group algebra with scalar ring R and group A	2.2
$\cdot$	pointwise multiplication in $R[A]$	2.2
$(R[A], \cdot)$	$R[A]$ equipped with pointwise multiplication	2.2
R^A	the R-algebra of functions from a group A into a ring R	2.2
$*$	convolution in R^A	2.2
$(R^A, *)$	R^A equipped with convolution	2.2
$\langle \cdot, \cdot \rangle$	the bilinear pairing	2.2
$\delta(\cdot, \cdot)$	the Kronecker delta	2.2
FT	the Fourier transform	2.2
$\hat{f}$	the Fourier transform of f	2.2
$\tilde{f}$	the scaled Fourier transform of f	2.2
d	a positive integer; our usual Galois ring is $\mathrm{GR}(p^d, e)$	2.3
e	a positive integer; our usual Galois ring is $\mathrm{GR}(p^d, e)$	2.3
q	p^e	2.3
e'	the least positive integer such that the exponent of A divides $q^{e'} - 1$	2.3
q'	$q^{e'} = p^{ee'}$	2.3
π	π_d, reduction modulo p^d, also extended to elements of group algebras and functions into $\mathbb{Z}_p[\zeta_{q'-1}]$	2.3
τ	τ_∞, Teichmüller lift to characteristic 0, also extended to elements of group algebras and functions into $\mathrm{GR}(p^d, ee')$	2.3
$\tilde{f}^{(i)}$	the ith component in the canonical expansion of $\tilde{f}$	2.3
$f^{(i)}$	the ith component in scaled-Fourier induced breakdown of f	2.3
$\mathrm{Cl}_q(a)$	the q-class of $a \in A$	2.3
e_a	the cardinality of the q-class of $a \in A$	2.3

$\mathrm{wt}^{\mathrm{norm}}$	the normalized version of the weight function wt	2.4
zer	the zero count or simultaneous zero count function	2.4
ham	the Hamming weight function	2.4
symb_r	the r-count function	2.4
lee	the Lee weight function	2.4
$\mathbb{Z}[Y]$	the set of accounts on Y	2.5
$\mathbb{N}[Y]$	the set of multisets of elements in Y	2.5
$\lvert\mu\rvert$	the size of account μ	2.5
$\mu!$	$\prod_{y\in Y}\mu_y!$ for $\mu\in\mathbb{N}[Y]$	2.5
pr_U	the projection of account μ onto U	2.5
H	the set $\{0,1,\ldots,e-1\}$	2.5
$\Sigma\mu$	the p-weighted summation of $\mu\in\mathbb{N}[H]$	2.5
$\mathrm{Fr}^{\mu}(r)$	$\prod_{h\in H}\left(\mathrm{Fr}^h(r)\right)^{\mu_h}$ for $\mu\in\mathbb{N}[H]$	2.5
$\Pi\lambda$	the product of the account $\lambda\in\mathbb{N}[A]$, $\mathbb{N}[I\times A]$, $\mathbb{N}[H\times A]$, or $\mathbb{N}[I\times H\times A]$	2.5
$f(\lambda)$	the evaluation of f at $\lambda\in\mathbb{N}[A]$ or $\mathbb{N}[H\times A]$	2.5
$\mathrm{Co}_R(\lambda)$	the collapse of λ with respect to R	2.6
$\mathrm{Red}(\lambda)$	the reduction of λ	2.6
Fr_{A}	the Frobenius action on A, $\mathbb{Z}[A]$, $\mathbb{Z}[I\times A]$, $H\times A$, $\mathbb{Z}[H\times A]$, and $\mathbb{Z}[I\times H\times A]$	2.7
$f(\{x_j\}_{j\in J})$	a polynomial with indeterminates in $\{x_j : j\in J\}$	2.8
$R[\{x_j\}_{j\in J}]$	the R-algebra of polynomials with coefficients in the ring R and indeterminates in $\{x_j : j\in J\}$	2.8
$\mathbf{x}^{\mu}$	for $\mathbf{x}$ a listing of the indeterminates in $\{x_j : j\in J\}$ and $\mu\in\mathbb{N}[J]$, $\mathbf{x}^{\mu}=\prod_{j\in J}x_j^{\mu_j}$	2.8
$f(\{x_k=a_k\}_{k\in K})$	the polynomial or constant obtained from the polynomial f by replacing the indeterminate x_k with a_k for each $k\in K$	2.8
$\binom{x}{n}$	the nth binomial coefficient polynomial	2.8

Chapter 1

Introduction

Let p be a prime, let d and e be positive integers, and set $q = p^e$. Let $\mathbb{N}$ denote the set of nonnegative integers, and let $\mathbb{Z}_p$ denote the ring of p-adic integers. We want a class of rings that includes both finite fields and integer residue rings modulo prime powers, so we introduce the Galois rings. Let ζ_{p^e-1} denote a root of unity of order $p^e - 1$ over $\mathbb{Z}_p$. The *Galois ring* $\mathrm{GR}(p^d, e)$ is the quotient modulo p^d of $\mathbb{Z}_p[\zeta_{p^e-1}]$. $\mathrm{GR}(p^d, e)$ is a ring extension of $\mathbb{Z}/p^d\mathbb{Z}$ wherein the reduction modulo p^d of ζ_{p^e-1} is a root of unity of order $p^e - 1$. Note that $\mathrm{GR}(p^d, 1)$ is the integer residue ring $\mathbb{Z}/p^d\mathbb{Z}$, and $\mathrm{GR}(p, e)$ is the finite field $\mathbb{F}_{p^e} = \mathbb{F}_q$. Readers interested in more details on p-adic fields and Galois rings should consult Section 2.1.

We shall be interested in the group algebra $\mathrm{GR}(p^d, e)[A]$, where A is a finite Abelian group with $p \nmid |A|$. We shall write A multiplicatively with identity 1_A (or just 1 if there is no cause for confusion). By ordering the elements of the group A in some fashion, say $A = \{a_1, \ldots, a_n\}$, we can think of the element $c = \sum_{a \in A} c_a a \in \mathrm{GR}(p^d, e)[A]$ as a word of length $n = |A|$ formed of symbols from the "alphabet" $\mathrm{GR}(p^d, e)$, that is, we regard c as the word $c_{a_1} c_{a_2} \ldots c_{a_n}$. An ideal of $\mathrm{GR}(p^d, e)[A]$ is then called an *Abelian code* (*over* $\mathrm{GR}(p^d, e)$). If A is a cyclic group, then an ideal of $\mathrm{GR}(p^d, e)[A]$ is also called a *cyclic code*. Cyclic codes form a large class of error-correcting codes, which includes various subclasses (such as the Hamming codes, the Bose-Chaudhuri-Hocquenghem codes, and the punctured Reed-Muller codes), all of great importance in coding theory [32]. Abelian codes with words of length n form a subclass of the *linear codes* of length n over $\mathrm{GR}(p^d, e)$, which are the $\mathrm{GR}(p^d, e)$-submodules of $\mathrm{GR}(p^d, e)^n$. Most research on Abelian and cyclic codes concerns

codes over finite fields, but recent developments have started an interest in Abelian codes over integer residue rings and even arbitrary Galois rings.

A *weight function* is simply a function $\mathrm{wt}\colon \mathrm{GR}(p^d, e) \to \mathbb{Z}$. We can think of this function as assigning a particular weight to each symbol of our alphabet $\mathrm{GR}(p^d, e)$. We extend wt so that it also maps words into $\mathbb{Z}$; the weight of the word $c = \sum_{a \in A} c_a a \in \mathrm{GR}(p^d, e)[A]$ is simply the sum of the weights of the letters in the word, i.e., $\mathrm{wt}(c) = \sum_{a \in A} \mathrm{wt}(c_a)$. The most commonly used weight function is the *Hamming weight*, which maps 0 to 0 and all other elements of $\mathrm{GR}(p^d, e)$ to 1. We denote the Hamming weight function ham, so that if $c \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{ham}(c)$ is the number of nonzero coefficients in the sum $c = \sum_{a \in A} c_a a$. In coding theory, typical weight functions (like the Hamming weight defined above and the Lee weight defined below) give rise to metrics wherein the distance between two words is the weight of their difference; if the weight function is Hamming weight, then the associated distance, called the *Hamming distance*, simply measures the number of positions where two words disagree. It will often be more convenient for us to use a weight function, called the *zero count*, which is complementary to the Hamming weight. The zero count function maps 0 to 1 and the rest of $\mathrm{GR}(p^d, e)$ to 0. We denote the zero count function by zer, so that if $c \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{zer}(c)$ is the number of zero coefficients in the sum $c = \sum_{a \in A} c_a a$, i.e., $\mathrm{zer}(c) = |A| - \mathrm{ham}(c)$.

In this work, we are interested in p-adic estimates of weights of words in $\mathrm{GR}(p^d, e)[A]$. By a p-adic estimate of an integer n, we mean the knowledge of n modulo some power of p. One common form of p-adic estimate is knowledge of the p-adic valuation of n, i.e., the maximum k such that $p^k \mid n$. Usually we shall place lower bounds on the p-adic valuations of weights of words belonging to a code $\mathcal{C} \subseteq \mathrm{GR}(p^d, e)[A]$. That is, we shall often furnish some k such that all weights of words in $\mathcal{C}$ are divisible by p^k. Sometimes we can also assert that there is some word $c \in \mathcal{C}$ with $p^{k+1} \nmid \mathrm{wt}(c)$. If we can say this, then we refer to our bound on the p-adic valuation as *sharp*. Roughly speaking, the larger the code in $\mathrm{GR}(p^d, e)[A]$, the less likely it is that all weights of words will be divisible by some large power of p.

For the rest of this chapter, we shall always assume that $\mathcal{C}$ is a code in $\mathrm{GR}(p^d, e)[A]$.

We use the Fourier transform to characterize our codes. Since the intricacies of the Fourier transform with group algebras over Galois rings may be unfamiliar to the reader, we provide a brief overview here. Readers who want more detail can find it in Sections 2.2 and 2.3.

To define a Fourier transform for $\mathrm{GR}(p^d, e)$, we set e' to be the least integer such that $q^{e'} - 1$ is a multiple of the exponent of A, and we set $q' = q^{e'}$. Then $\mathrm{GR}(p^d, ee')$ is a ring extension of $\mathrm{GR}(p^d, e)$ and contains roots of unity whose orders include all orders of elements in A. Then we let X be the set of characters (multiplicative homomorphisms) from A into $\mathrm{GR}(p^d, ee')$. The Fourier transform $\hat{c}$ of $c \in \mathrm{GR}(p^d, e)[A]$ is a function from X to $\mathrm{GR}(p^d, ee')$ with $\hat{c}(\chi) = \sum_{a \in A} c_a \chi(a)^{-1}$. We often refer to the values $\hat{c}(\chi)$ taken by the Fourier transform at the various characters χ as the *Fourier coefficients* of c. By applying a (non-canonical) isomorphism between X and A, we shall consider the domain of $\hat{c}$ to be A rather than X. The word c is uniquely determined by its Fourier transform, and furthermore, $\hat{c}(a^q) = \mathrm{Fr}^e(\hat{c}(a))$ for all $a \in A$, where Fr is the Frobenius automorphism (which can be defined on $\mathrm{GR}(p^d, ee')$ as the automorphism induced via reduction modulo p^d from the Frobenius automorphism on $\mathbb{Z}_p[\zeta_{q'-1}]$). Since q is coprime to the order of A, the action $a \mapsto a^q$ partitions A into orbits that we shall call *q-classes*. We shall say that a subset B of A is *q-closed* if B is a union of q-classes. With this terminology, c is uniquely determined by its Fourier transform on a set R of representatives of q-classes. Indeed, the Fourier transform followed by restriction to R is an isomorphism of $\mathrm{GR}(p^d, e)$-algebras from $\mathrm{GR}(p^d, e)[A]$ to the product of rings

$$\prod_{r \in R} \mathrm{GR}(p^d, ee_r), \tag{1.1}$$

where e_r is the size of the q-class of r. Thus codes (ideals) in $\mathrm{GR}(p^d, e)[A]$ are in one-to-one correspondence with ideals in this product, which are just products of some selection of ideals in the Galois rings $\mathrm{GR}(p^d, ee_r)$. The ideals in $\mathrm{GR}(p^d, ee_r)$ are $(0) = (p^d) \subseteq (p^{d-1}) \subseteq \cdots \subseteq (p) \subseteq (1) = \mathrm{GR}(p^d, ee_r)$. Thus, the Fourier transform followed by restriction to R

maps our code $\mathcal{C}$ to an ideal of (1.1), say

$$\prod_{r\in R} p^{i_r}\,\mathrm{GR}(p^d, ee_r), \tag{1.2}$$

where $i_r \in \{0, 1, \ldots, d\}$ for each $r \in R$. Knowledge of the integers i_r characterizes $\mathcal{C}$ completely. The support S of the Fourier transform of $\mathcal{C}$ is the union of the q-classes of those r such that $i_r < d$. Thus, when $d = 1$, the support S fully characterizes $\mathcal{C}$, but when $d > 1$, there can be multiple codes whose Fourier transforms have the same support. We devise a generalization of the notion of support that will uniquely determine the code, even when $d > 1$. For each $j \in \{0, 1, \ldots, d-1\}$, let S_j be the union of the q-classes of those r such that $i_r \le j$. Then our code $\mathcal{C}$ is fully characterized by the tower $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$, which we call the *tower of supports of* $\mathcal{C}$. The largest set S_{d-1} in the tower is just S, the support of the Fourier transform of the code. Note that a code in $\mathrm{GR}(p^d, e)[A]$ is a free $\mathrm{GR}(p^d, e)$-module if and only if all the sets in its tower of supports are identical.

For the rest of this introduction, we use $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$ to denote the tower of supports of the Fourier transform of our code $\mathcal{C} \subseteq \mathrm{GR}(p^d, e)[A]$, and we let S be the support of the Fourier transform, i.e., $S = S_{d-1}$. All S_i, including $S_{d-1} = S$, are q-closed. As a simplifying assumption, we shall always assume $1_A \notin S$ in this introduction. This assumption is not necessary in these researches, but it will simplify this introductory presentation. We do without this assumption in the rest of this thesis by introducing the normalized weights in Section 2.4. Here we shall quote our own results and those of other researchers with this simplifying assumption in force; the more general results are quoted in the body of the thesis. We now have enough background to discuss the various results that predate this work.

1.1 History

The most natural and convenient Galois rings to use in coding theory are the finite fields. Thus, it is not surprising that the first p-adic estimates of weights were with Abelian codes (usually cyclic) over finite fields. We begin by recalling that Mattson and Solomon [33]

introduced the Fourier transform (also known as the Mattson-Solomon polynomial) into the study of weights in cyclic codes. Solomon continued to study weights in cyclic codes [50], and with McEliece produced some initial p-adic estimates of weights [51]. In the latter paper, Solomon and McEliece, working with cyclic codes over $\mathbb{F}_2$, expressed the digits in the base-2 expansion of the weight of a word c (with such digits regarded as elements of $\mathbb{F}_2$) as polynomial functions of the Fourier coefficients of c. They proved that if $\mathcal{C}$ is a cyclic code in $\mathbb{F}_2[A]$ such that $a \in S$ implies $a^{-1} \notin S$, then $\mathrm{ham}(c) \equiv 0 \pmod 4$ for all $c \in \mathcal{C}$. In his thesis [35], McEliece found that this is an example of a much more general phenomenon. If $\mathcal{C} \subseteq \mathbb{F}_p[A]$ with A cyclic, one should consider (nonempty, finite) unity-product sequences of elements of S, i.e., sequences of elements of S such that the product of the terms of the sequence is 1_A. Let $\omega(\mathcal{C})$ denote the minimum of the lengths of such sequences, and set $\ell(\mathcal{C}) = \left\lfloor \frac{\omega(\mathcal{C})-1}{p-1} \right\rfloor$. Then McEliece asserts that $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell(\mathcal{C})}}$, or equivalently, that $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell(\mathcal{C})}}$, for all $c \in \mathcal{C}$. This is a generalization of the earlier Solomon-McEliece result because the condition that $a \in S$ implies $a^{-1} \notin S$ is equivalent to the condition $\omega(\mathcal{C}) \geq 3$, which then implies (when $p = 2$) that $\ell(\mathcal{C}) \geq 2$, and thus $\mathrm{ham}(c) \equiv 0 \pmod 4$.

All the rest of the results we present here, whether previous work or our own, are analogous to this theorem of McEliece. In all cases, one must determine the "minimum size" (in some appropriate sense) of unity-product sequences of elements in the support S of the code (or sometimes in the set of pth powers of elements in S). The "larger" this "minimum size," the more powers of p divide the weights of words in the code. At times one must place some sort of condition on the sequences, and at times the notion of the "size" of the sequences must be refined beyond a simple count of how many terms occur. This leads to a few variants of the parameters $\omega(\mathcal{C})$ and $\ell(\mathcal{C})$ defined in the previous paragraph. While it would be historically informative to introduce each new variant as it appears in the literature, it would also make it difficult to take them all in at a glance. So we shall define them all here and then await the appearance of each when we resume our historical overview.

As stated above, $\omega(\mathcal{C})$ is the minimum length of a (nonempty) unity-product sequence of

elements from S when $d = e = 1$, i.e., when our Galois ring $\mathrm{GR}(p^d, e)$ is the prime field $\mathbb{F}_p$. In a general Galois ring, we define $\omega(\mathcal{C})$ as the minimum length of a (nonempty) unity-product sequence of pth powers of elements of S, i.e., a sequence of the form $a_1^{p^{j_1}}, a_2^{p^{j_2}}, \ldots, a_n^{p^{j_n}}$, with each $a_i \in S$ and $j_i \in \mathbb{N}$. Since S is p-closed when $e = 1$, this definition coincides with our original one. We then define $\ell(\mathcal{C}) = \left\lfloor \frac{\omega(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1)$. This reduces to our original definition of $\ell(\mathcal{C})$ when $d = e = 1$.

Sometimes we need to restrict our attention to the smaller class of unity-product sequences of elements of S (and their pth powers) that satisfy a certain additional condition which we call the *modular condition*. We again use sequences of the form $a_1^{p^{j_1}}, a_2^{p^{j_2}}, \ldots, a_n^{p^{j_n}}$ with each $a_i \in S$ and $j_i \in \mathbb{N}$, but consider only those in which $p^{j_1} + p^{j_2} + \cdots + p^{j_n} \equiv 0 \pmod{q-1}$. We let $\omega_{mc}(\mathcal{C})$ be the minimum length of such a sequence. If we reduce our congruence modulo $p-1$, we see that all our sequences here have length divisible by $p-1$. Indeed, if $e = 1$, then our sequences are simply sequences of elements in S, and they meet the modular condition if and only if their length is divisible by $p-1$. Thus, if $p = 2$ and $e = 1$, $\omega_{mc}(\mathcal{C}) = \omega(\mathcal{C})$. In all cases, we have $\omega_{mc}(\mathcal{C}) \geq \omega(\mathcal{C})$, and this inequality can be strict, as we shall see later. We define $\ell_{mc}(\mathcal{C}) = \left\lfloor \frac{\omega_{mc}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1)$. Thus $\ell_{mc}(\mathcal{C}) \geq \ell(\mathcal{C})$, with equality when $p = 2$ and $e = 1$, but the inequality can be strict in other situations, as we shall see in time.

Another new parameter will also be defined by considering unity-product sequences of pth powers of elements in S, but here we shall need to record the set in the tower of supports $S_0 \subseteq \cdots \subseteq S_{d-1} = S$ from which we took each term of our sequence. Thus our new parameter will be sensitive to the structure of the tower of supports of our code. This sensitivity is not unreasonable; the Fourier coefficients $\hat{c}(a)$ for $a \in S_{d-1} \setminus S_{d-2}$ vary only over the ideal (p^{d-1}) in a Galois ring of characteristic p^d, while those Fourier coefficients $\hat{c}(b)$ with $b \in S_0$ range over an entire Galois ring. Thus we should expect the latter coefficients to exert more influence on the weights of words. We shall only need to use this new parameter (about to be defined) in cases where $e = 1$, so that pth powers of elements in S_i are just elements of S_i itself (since each S_i is p-closed when $e = 1$). Note that $\mathrm{GR}(p^d, e) = \mathbb{Z}/p^d\mathbb{Z}$

when $e = 1$. We consider (nonempty) unity-product sequences of the form

$$a_1^{(0)}, \ldots, a_{n_0}^{(0)}, a_1^{(1)}, \ldots, a_{n_1}^{(1)}, \ldots, a_1^{(d-1)}, \ldots, a_{n_{d-1}}^{(d-1)},$$

where $a_j^{(i)} \in S_i$ for all i, j. Now we introduce a device that we call our *scoring system*. To our sequence above, we assign a number called the *score*, which is equal to $n_0 + pn_1 + \cdots + p^{d-1}n_{d-1}$, and we let $\omega^{ss}(\mathcal{C})$ be the minimum of the scores of such unity-product sequences. We then let $\ell^{ss}(\mathcal{C}) = \left\lfloor \frac{\omega^{ss}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor$. It is not hard to see that $\omega^{ss}(\mathcal{C}) \geq \omega(\mathcal{C})$, and thus $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$, for any code $\mathcal{C}$. If $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module, it is straightforward to show that $\omega^{ss}(\mathcal{C}) = \omega(\mathcal{C})$ and $\ell^{ss}(\mathcal{C}) = \ell(\mathcal{C})$ (see Proposition 4.22 of this thesis). Strict equality can hold in other cases, as we shall soon find out.

We also introduce a parameter (which may not have appeared before this thesis) by combining both the modular condition and the scoring system. Again, we need only use this new parameter in cases where $e = 1$, so that $\mathrm{GR}(p^d, e) = \mathbb{Z}/p^d\mathbb{Z}$ and pth powers of elements in S_i are just elements of S_i itself (since each S_i is p-closed when $e = 1$). As in the previous paragraph, we consider (nonempty) unity-product sequences of the form

$$a_1^{(0)}, \ldots, a_{n_0}^{(0)}, a_1^{(1)}, \ldots, a_{n_1}^{(1)}, \ldots, a_1^{(d-1)}, \ldots, a_{n_{d-1}}^{(d-1)},$$

where $a_j^{(i)} \in S_i$ for all i, j. We further insist that our sequences meet the modular condition, which, for $e = 1$, is equivalent to insisting that the sequences have length divisible by $p - 1$. As before, the *score* of the above sequence is $n_0 + pn_1 + \cdots + p^{d-1}n_{d-1}$, and we let $\omega_{mc}^{ss}(\mathcal{C})$ be the minimum of the scores of such unity-product sequences. We then let $\ell_{mc}^{ss}(\mathcal{C}) = \left\lfloor \frac{\omega_{mc}^{ss}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor$. It is not hard to show that $\omega_{mc}^{ss}(\mathcal{C}) \geq \omega^{ss}(\mathcal{C})$, and thus $\ell_{mc}^{ss}(\mathcal{C}) \geq \ell^{ss}(\mathcal{C})$, for any code $\mathcal{C}$, with equality when $p = 2$. It is also straightforward to show that $\omega_{mc}^{ss}(\mathcal{C}) \geq \omega_{mc}(\mathcal{C})$, and thus $\ell_{mc}^{ss}(\mathcal{C}) \geq \ell_{mc}(\mathcal{C})$, for any code $\mathcal{C}$, with equality when $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module. Strict inequality may hold in the four inequalities just mentioned, as we shall soon see.

In summary, we have four parameters, $\omega(\mathcal{C})$, $\omega_{mc}(\mathcal{C})$, $\omega^{ss}(\mathcal{C})$, and $\omega_{mc}^{ss}(\mathcal{C})$, measuring minimum "sizes" of various kinds of sequences, and four parameters, $\ell(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$,

and $\ell^{ss}_{mc}(\mathcal{C})$, where each ℓ-parameter is obtained from its corresponding ω-parameter by the formula $\ell = \left\lfloor \frac{\omega - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1)$. The more decorations the parameter has, the higher it is in general. That is, we always have $\omega(\mathcal{C}) \leq \omega_{mc}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$ and $\omega(\mathcal{C}) \leq \omega^{ss}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$, but $\omega_{mc}(\mathcal{C})$ and $\omega^{ss}(\mathcal{C})$ are not strictly comparable. Furthermore, $\omega(\mathcal{C}) = \omega_{mc}(\mathcal{C})$ and $\omega^{ss}(\mathcal{C}) = \omega^{ss}_{mc}(\mathcal{C})$ when $p = 2$ and $e = 1$. Also $\omega(\mathcal{C}) = \omega^{ss}(\mathcal{C})$ and $\omega_{mc}(\mathcal{C}) = \omega^{ss}_{mc}(\mathcal{C})$ when $e = 1$ and $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module. On the other hand, we can find an infinite sequence of cyclic codes over Galois rings where $\omega(\mathcal{C}) < \omega_{mc}(\mathcal{C}) < \omega^{ss}(\mathcal{C}) < \omega^{ss}_{mc}(\mathcal{C})$, and where all the differences between terms in this chain of inequalities simultaneously tend to infinity as $\mathcal{C}$ runs through the sequence. See Proposition 4.22 of this thesis for details.

Now let us resume the thread of our history. We had left off where McEliece showed [35] that if $\mathcal{C} \subseteq \mathbb{F}_p[A]$ with A cyclic, then $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell(\mathcal{C})}}$, or equivalently, $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell(\mathcal{C})}}$, for all $c \in \mathcal{C}$. Furthermore, McEliece showed that every nonzero symbol (element of $\mathbb{F}_p$) occurs a multiple of $p^{\ell(\mathcal{C})}$ times in any given $c \in \mathcal{C}$. Delsarte generalized this theorem from cyclic codes over $\mathbb{F}_p$ to Abelian codes over $\mathbb{F}_p$ [17], and McEliece generalized this theorem from cyclic codes over $\mathbb{F}_p$ to cyclic codes over $\mathbb{F}_q$, an arbitrary finite field of characteristic p [36].

The next major discovery is also due to McEliece [37], who introduced the modular condition to improve the above results, thus producing a sharp bound on the p-adic valuations of Hamming weights in cyclic codes over $\mathbb{F}_p$:

Theorem 1.1 (McEliece [37]). *Let $\mathcal{C}$ be a code in $\mathbb{F}_p[A]$ with A cyclic and 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then* $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$*, and there is some $c \in \mathcal{C}$ with* $\mathrm{ham}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$*. Equivalently,* $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})}}$*, and there is some $c \in \mathcal{C}$ with* $\mathrm{zer}(c) \not\equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$*.*

This is an improvement (since $\ell_{mc}(\mathcal{C})$ is sometimes greater than $\ell(\mathcal{C})$) and a sharpening of the results in McEliece's thesis. McEliece had already shown that in a cyclic code $\mathcal{C}$ over $\mathbb{F}_p$, the number of instances in each word c of any nonzero symbol is divisible by $p^{\ell(\mathcal{C})}$ [35]. In [37], he used the Theorem 1.1 to show that this is sharp. That is, for any given nonzero $r \in \mathbb{F}_p$, there is some $c \in \mathcal{C}$ such that the number of instances of r in c is not divisible by $p^{\ell(\mathcal{C})+1}$. The results of McEliece have been used in studies of weights in codes [27], [26],

[57], [6], [56]. They have also been used in the study of highly nonlinear functions and cross-correlation properties of m-sequences[1] [24], [9], [10], [11], [14], [20], [8], [12].

The definitive result for Hamming weights of words in Abelian codes in $\mathbb{F}_q[A]$ with $p \nmid |A|$ is due to Delsarte and McEliece [18]. They determined the correct generalization, for use with an arbitrary finite field, of the modular condition that was introduced for prime fields by McEliece.

Theorem 1.2 (Delsarte-McEliece [18]). *Let $\mathcal{C}$ be a code in $\mathbb{F}_q[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, and there is some $c \in \mathcal{C}$ with $\mathrm{zer}(c) \not\equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$. Equivalently, $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, and there is some $c \in \mathcal{C}$ with $\mathrm{ham}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$.*

Thus Delsarte and McEliece give a sharp bound on the p-adic valuations of Hamming weights in Abelian codes over finite fields. One particularly satisfying corollary of the Delsarte-McEliece theorem is the theorem of Ax [2] on the cardinalities of affine algebraic sets generated by low-degree polynomials over finite fields:

Theorem 1.3 (Ax [2]). *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a nonconstant polynomial of degree $\mathfrak{d}$. Let ν be the least nonnegative integer greater than or equal to $(n - \mathfrak{d})/\mathfrak{d}$. Let $V(f)$ be the set of zeroes of f in $\mathbb{F}_q^n$. Then $|V(f)|$ is divisible by q^ν.*

Delsarte and McEliece showed that their theorem implies Ax's by using a special correspondence [28] between polynomial functions on $\mathbb{F}_q^n \setminus \{(0, \ldots, 0)\}$ and elements of the group algebra $\mathbb{F}_q[A]$ with A the cyclic group of order $q^n - 1$. We should also note that the Delsarte-McEliece theorem has been further generalized by Ward, who considered group algebras $\mathbb{F}_q[G]$ for more general groups, i.e., non-Abelian groups and groups G with $|G|$ divisible by p [58], [59], [60], [61].

As the study of error-correcting codes progressed, it became clear that codes over finite rings other than fields, particularly codes over integer residue rings, were interesting. This idea had occurred to various researchers in the 1970s and 1980s, e.g., see [4], [5], [52], [53], [44], [49], [63]. Particularly significant is the result of Nechaev [41], who showed that the

[1] An m-sequence is a sequence of elements in $\mathbb{F}_q$ generated by a linear recurrence whose characteristic polynomial is the minimal polynomial (over $\mathbb{F}_q$) of a root of unity of order $q^k - 1$ for some k.

Kerdock code (a very good, but nonlinear code over $\mathbb{F}_2$) has a simple description in terms of quaternary sequences (i.e., sequences of elements in $\mathbb{Z}/4\mathbb{Z}$). Interest in codes over $\mathbb{Z}/4\mathbb{Z}$ increased spectacularly when Hammons, Kumar, Calderbank, Sloane, and Solé showed that the Kerdock code and a code equivalent to the Preparata code, when regarded as extended cyclic codes over $\mathbb{Z}/4\mathbb{Z}$, are dual to each other [23]. These researchers made much use of the weight function known as the *Lee weight*, which we shall denote $\mathrm{lee}\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}$, and which is defined by $\mathrm{lee}(0) = 0$, $\mathrm{lee}(1) = \mathrm{lee}(3) = 1$, and $\mathrm{lee}(2) = 2$. There is a map, called the *Gray map*, which is a distance-preserving bijection from $(\mathbb{Z}/4\mathbb{Z})^k$, equipped with Lee distance, to $\mathbb{F}_2^{2k}$, equipped with Hamming distance. Therefore, one can obtain binary codes with large Hamming distance between codewords if one can obtain quaternary codes with large Lee distance between codewords. Thus Lee weight is perhaps the most important weight function to consider when working with codes over $\mathbb{Z}/4\mathbb{Z}$. More generally, the Lee weight function $\mathrm{lee}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ is obtained by setting $\mathrm{lee}(r)$ to be the minimum of the absolute values of the elements in $\mathbb{Z}$ which equal r modulo p^d.

Since the class of Galois rings includes both finite fields and integer residue rings modulo prime powers, it is not unnatural for researchers to study cyclic codes over Galois rings, as indeed they have begun to do [3], [64], [42], [54], [55], [19]. One desires analogues of the theorems (such as those of Delsarte and McEliece) that have been worked out for Abelian codes over finite fields.

Most published analogues of McEliece's theorem for Abelian codes over Galois rings (aside from those for codes over finite fields, which we have already discussed) treat of codes over integer residue rings modulo prime powers, i.e., Galois rings of the form $\mathrm{GR}(p^d, 1) = \mathbb{Z}/p^d\mathbb{Z}$. The first result we discuss, due to Helleseth, Kumar, Moreno, and Shanbhag [25], is actually stated as a result for $\mathbb{Z}/4\mathbb{Z}$-linear trace codes, which are extended cyclic codes over $\mathbb{Z}/4\mathbb{Z}$, where A is a cyclic group of order $2^n - 1$ for some $n > 1$. Their result is easily translated into an equivalent result for cyclic codes over $\mathbb{Z}/4\mathbb{Z}$:

Theorem 1.4 (Helleseth-Kumar-Moreno-Shanbhag [25]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$ with A cyclic of order $2^n - 1$ for some $n > 1$, and with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then $\mathrm{lee}(c) \equiv 0 \pmod{2^{\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1}}$ for all $c \in \mathcal{C}$.*

Around the same time, Calderbank, Li, and Poonen [7] proved a theorem that is wider in scope. They demonstrated that the Lee weights of words in any cyclic code over $\mathbb{Z}/4\mathbb{Z}$ are always divisible by $2^{\lceil \omega(\mathcal{C})/2 \rceil - 1}$. This theorem is more generally applicable than that of Helleseth et al., since it does not assume that A is of order $2^n - 1$ for some n. However, when we restrict to this special case, which Helleseth et al. treat, then their theorem is stronger than that of Calderbank et al., since $\omega^{ss}(\mathcal{C}) \geq \omega(\mathcal{C})$, and sometimes this inequality is strict. For codes that are free $\mathbb{Z}/4\mathbb{Z}$-modules, one has $\omega^{ss}(\mathcal{C}) = \omega(\mathcal{C})$, so that the two results coincide in this case. The results of Helleseth et al. and of Calderbank et al. have been useful to coding theorists [48], [13].

Wilson generalized and strengthened the results of Calderbank, Li, and Poonen in an unpublished manuscript [67].

Theorem 1.5 (Wilson [67]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/2^d\mathbb{Z}[A]$ with A cyclic and 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then* $\mathrm{lee}(c)$ *is divisible by $2^{\lfloor (\omega(\mathcal{C})-2)/2^{d-1} \rfloor + 1}$ for all $c \in \mathcal{C}$.*

In the special case of cyclic codes over $\mathbb{Z}/4\mathbb{Z}$ (i.e., when $d = 2$), Wilson's theorem asserts that weights are divisible by $2^{\lfloor \omega(\mathcal{C})/2 \rfloor} = 2^{\ell(\mathcal{C})+1}$, which is stronger than the result $2^{\lceil \omega(\mathcal{C})/2 \rceil - 1}$ of Calderbank, Li, and Poonen when $\omega(\mathcal{C})$ is even. If we further restrict A to be cyclic of order $2^n - 1$ for some $n > 1$, then Wilson's result is sometimes stronger than that of Helleseth et al., for example, in the case when the codes are free $\mathbb{Z}/4\mathbb{Z}$-modules (where the results of Helleseth et al. and Calderbank et al. coincide) with $\omega(\mathcal{C})$ even. On the other hand, Wilson's result can be worse than that of Helleseth et al., because one can construct a sequence of codes (to which Theorem 1.4 applies) in which $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ increases without bound as $\mathcal{C}$ runs through the sequence (see Proposition 4.22 of this thesis). So the results of Wilson and of Helleseth et al. are not strictly comparable.

Now let us consider zero counts and Hamming weights of codes in $\mathbb{Z}/p^d\mathbb{Z}[A]$. The results here mostly occur in the same papers where one finds the results for Lee weights. Calderbank, Li, and Poonen [7] showed that Hamming weights in cyclic codes over $\mathbb{Z}/4\mathbb{Z}$ are always divisible by $\max\left\{2^{\lceil \omega(\mathcal{C})/2 \rceil - 2}, 2^{\lceil \omega(\mathcal{C})/3 \rceil - 1}\right\}$. More generally, they showed that Hamming weights in a cyclic code $\mathcal{C}$ over $\mathbb{Z}/2^d\mathbb{Z}$ are always divisible by $2^{\lceil \omega(\mathcal{C})/2^{d-1} \rceil - 2}$.

Indeed, they showed that the number of instances of each nonzero symbol is always divisible by $2^{\lceil \omega(\mathcal{C})/2^{d-1} \rceil - 2}$. If we specialize to $d = 1$, this shows that Hamming weights in cyclic codes over $\mathbb{F}_2$ are divisible by $\omega(\mathcal{C}) - 2 = \ell(\mathcal{C}) - 1$, which is a result inferior to that obtained by McEliece in his thesis [35]. Again, the results of Calderbank et al. were generalized and strengthened by Wilson. Wilson showed that for any code $\mathcal{C}$ in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with A cyclic, the Hamming weights of words are divisible by $p^{\ell(\mathcal{C})}$. More strongly, he showed the following result:

Theorem 1.6 (Wilson [65]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with A cyclic and 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then for any $c \in \mathcal{C}$ and $r \in \mathbb{Z}/p^d\mathbb{Z}$ with $r \neq 0$, the number of occurrences of the symbol r in the word c is a multiple of $p^{\ell(\mathcal{C})} = p^{\left\lfloor \frac{\omega(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor}$.*

Note that the specialization of this theorem to $p = 2$ is stronger than the result of Calderbank, Li, and Poonen. For Hamming weights in cyclic codes over $\mathbb{Z}/4\mathbb{Z}$, Wilson's result is stronger when $\omega(\mathcal{C})$ is even and greater than or equal to 6. More generally (for $d > 2$ and when counting occurrences of any nonzero symbol), Wilson's result is stronger when $\omega(\mathcal{C}) \geq 2^d$ and $2^{d-1} \mid \omega(\mathcal{C})$. We should also compare Wilson's results with those of McEliece. For $d = 1$, i.e., when $\mathcal{C}$ is a cyclic code over $\mathbb{F}_p$, Wilson's results assert that each nonzero symbol occurs a multiple of $p^{\ell(\mathcal{C})}$ times, which is the result of McEliece's thesis [35]. However, if we wish to know about the p-divisibility of Hamming weights, this is not as strong as McEliece's later result (Theorem 1.1), which states that Hamming weights are divisible by $p^{\ell_{mc}(\mathcal{C})}$ (which can be greater than $p^{\ell(\mathcal{C})}$). Thus Wilson's theorem does not reduce to the strongest result available for cyclic codes over prime fields.

1.2 New Results

We present four new results in this thesis, after laying a foundation of preliminary material (Chapter 2) and presenting our estimation method in abstract form (Chapter 3) to avoid repetitive calculations. Our first result, presented in Chapter 4, concerns zero counts, Hamming weights, and counts of nonzero symbols in words of Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$. Our second result, presented in Chapter 5, concerns Lee weights in Abelian codes over

$\mathbb{Z}/4\mathbb{Z}$. The third new result, discussed in Chapter 6, concerns zero counts and Hamming weights in Abelian codes over arbitrary Galois rings. The last result, presented in Chapter 7, generalizes the theorem of Delsarte and McEliece (Theorem 1.2) to count the number of positions where a selection of words $c_1, \ldots, c_t \in \mathbb{F}_q[A]$ simultaneously have the zero symbol. From this we derive N. M. Katz's generalization [30] of Ax's theorem (Theorem 1.3). We present each result in more detail below.

The first result (Chapter 4) consists of two theorems. One theorem concerns counts of nonzero symbols in words:

Theorem 1.7 (Theorem 4.21). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Let $r \in \mathbb{Z}/p^d\mathbb{Z}$ with $r \neq 0$, and let $c \in \mathcal{C}$. Then the number of occurrences of the symbol r in the word c is a multiple of $p^{\ell^{ss}(\mathcal{C})}$.*

This improves Wilson's result (Theorem 1.6) because $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$. Indeed, there exists a sequence of codes such that $\ell^{ss}(\mathcal{C}) - \ell(\mathcal{C})$ is unbounded (see Proposition 4.22). Since Wilson's result is stronger than the result of Calderbank, Li, and Poonen on the number of instances of nonzero symbols, our new theorem here is also stronger than the results of these researchers. Our other new theorem gives an even stronger result for zero counts and Hamming weights:

Theorem 1.8 (Theorem 4.18). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then* $\operatorname{zer}(c) \equiv |A| \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, and* $\operatorname{zer}(c) \not\equiv |A| \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$ *for some $c \in \mathcal{C}$. Equivalently,* $\operatorname{ham}(c) \equiv 0 \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, and* $\operatorname{ham}(c) \not\equiv 0 \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$ *for some $c \in \mathcal{C}$.*

Thus we have a sharp lower bound on the p-adic valuations of Hamming weights of words in Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$. This strengthens the bound for Hamming weights that can be deduced from Theorem 1.7, and so *a fortiori* improves the results of Wilson (Theorem 1.6) and of Calderbank, Li, and Poonen [7], as applied to Hamming weights. Unlike these other theorems, Theorem 1.8 reduces to Theorem 1.1 of McEliece on Hamming weights in codes over prime fields. We note in passing that Theorem 1.7 can be applied to obtain lower bounds on 2-adic valuations of Lee weights of words in Abelian codes over $\mathbb{Z}/2^d\mathbb{Z}$.

When this is done, we obtain a result not strictly comparable to Wilson's result on Lee weights (Theorem 1.5); sometimes the one is better and sometimes the other is better. Thus, by combining this new result with Wilson's result, we obtain new improved bounds on 2-divisibility of Lee weights in $\mathbb{Z}/2^d\mathbb{Z}[A]$.

The second result (Chapter 5) presented in this thesis concerns Lee weights in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$:

Theorem 1.9 (Theorem 5.12). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then we have* $\mathrm{lee}(c) \equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+1}}$ *for all $c \in \mathcal{C}$, and* $\mathrm{lee}(c) \not\equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$ *for some $c \in \mathcal{C}$.*

Thus we have a sharp lower bound on the 2-adic valuations of Lee weights of words in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. We first compare this result with the specialization to $\mathbb{Z}/4\mathbb{Z}$ of Wilson's result (Theorem 1.5). The new result is stronger for $\mathbb{Z}/4\mathbb{Z}$-codes because $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$. Indeed, there exists a sequence of codes such that $\ell^{ss}(\mathcal{C}) - \ell(\mathcal{C})$ is unbounded (see Proposition 4.22). Since Wilson's result is stronger than that of Calderbank, Li, and Poonen, this new theorem is stronger than theirs as well. We should also compare this with the result of Helleseth, Kumar, Moreno, and Shanbhag, which applies only to the special case when our Abelian group A is cyclic of order $2^n - 1$ for some $n > 1$. The new theorem states that the 2-adic valuations of weights are bounded below by $\ell^{ss}(\mathcal{C}) + 1 = \lfloor \omega^{ss}(\mathcal{C})/2 \rfloor$, while the result of Helleseth et al. gives a lower bound of $\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1$. Thus, our result is stronger when $\omega^{ss}(\mathcal{C})$ is even. In fact, if one were to take the maximum of the lower bounds of Wilson and those of Helleseth et al. for codes in $\mathbb{Z}/4\mathbb{Z}[A]$ with A cyclic of order $2^n - 1$, Theorem 1.9 would still give a stronger bound for infinitely many codes (see the discussion at the beginning of Chapter 5 for more details). It is especially satisfactory that our new theorem includes the statement that the lower bound it furnishes is sharp.

The third result (Chapter 6) is an analogue of McEliece's theorem for Abelian codes over an arbitrary Galois ring $\mathrm{GR}(p^d, e)$. To the author's knowledge, no such result has appeared in the literature at this time. We prove the following result:

Theorem 1.10 (Theorem 6.12). *Let $\mathcal{C}$ be a code in $\mathrm{GR}(p^d, e)[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then* $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, or*

equivalently, $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all* $c \in \mathcal{C}$.

If we set $d = 1$ in this theorem, we recover the Delsarte-McEliece theorem (Theorem 1.2), which is sharp. However, if we set $e = 1$ in this theorem, we only obtain a weakened version of Theorem 1.8 (since $\ell^{ss}_{mc}(\mathcal{C}) \geq \ell_{mc}(\mathcal{C})$).

The fourth result (Chapter 7) is a generalization of the Delsarte-McEliece theorem (Theorem 1.2). Our generalized version counts the number of components where a collection $c_1, \ldots, c_t$ of codewords in $\mathbb{F}_q[A]$ simultaneously have the zero symbol. We extend the definition of zer so that $\mathrm{zer}(c_1, \ldots, c_t)$ is this simultaneous zero count. To state the theorem, we need a slight generalization of the parameter $\ell_{mc}(\mathcal{C})$. We suppose that $\mathcal{C}_1, \ldots, \mathcal{C}_t$ are ideals (codes) in $\mathbb{F}_q[A]$, and we let Γ_i be the support of the Fourier transform of $\mathcal{C}_i$ for each i. We consider unity-product sequences of the form

$$a_{1,1}^{p^{k_{1,1}}}, \ldots, a_{1,n_1}^{p^{k_{1,n_1}}}, \ldots, a_{t,1}^{p^{k_{t,1}}}, \ldots, a_{t,n_t}^{p^{k_{t,n_t}}}$$

with $a_{i,j} \in \Gamma_i$ and $k_{i,j} \in \mathbb{N}$ for each i and j. We insist that $\sum_{j=1}^{n_i} p^{k_{i,j}} \equiv 0 \pmod{q-1}$ for each $i \in \{1, 2, \ldots, t\}$. Note that this modular condition forces $p-1 \mid n_i$ for all i. We consider the "size" of such a sequence to be $\sum_{i=1}^{t} \max\left\{0, \frac{n_i}{p-1} - e\right\}$, and we set $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ to be the minimum size of the sequences with these properties. It is not hard to show that when we are working with a single codeword, i.e., when $t = 1$, this $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ becomes the parameter $\ell_{mc}(\mathcal{C}_1)$ which we have already defined. Now we can state our theorem.

Theorem 1.11 (Theorem 7.14). *Let* $t \geq 1$ *and let* $\mathcal{C}_1, \ldots, \mathcal{C}_t$ *be codes in* $\mathbb{F}_q[A]$ *with* 1_A *not in the supports of their Fourier transforms. Then* $\mathrm{zer}(c_1, \ldots, c_t) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)}}$ *for all* $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. *There are some* $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$ *such that* $\mathrm{zer}(c_1, \ldots, c_t) \not\equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)+1}}$.

This theorem reduces to the Delsarte-McEliece theorem (Theorem 1.2) in the special case $t = 1$. The Delsarte-McEliece theorem implies the result of Ax (Theorem 1.3) on the p-divisibility of the cardinality of the zero set of a single polynomial over $\mathbb{F}_q$. In the same manner, our new theorem implies the generalization of Ax's theorem by N. M. Katz on the p-divisibility of the cardinality of the set of simultaneous zeros of a collection of polynomials

over $\mathbb{F}_q$.

Theorem 1.12 (N. M. Katz [30]). *Let $f_1, \dots f_t \in \mathbb{F}_q[x_1, \dots, x_n]$ be nonconstant polynomials of degrees $\mathfrak{d}_1 \le \cdots \le \mathfrak{d}_t$, respectively. Let ν be the least nonnegative integer greater than or equal to $\left(n - \sum_{i=1}^{t} \mathfrak{d}_i\right)/\mathfrak{d}_t$. Let $V(f_1, \dots, f_t)$ be the set of simultaneous zeroes of $f_1, \dots, f_t$ in $\mathbb{F}_q^n$. Then $|V(f_1, \dots, f_t)|$ is divisible by q^ν.*

We also prove that N. M. Katz's theorem is sharp in the sense that (using the notation of the theorem) there exist homogeneous polynomials $f_1, \dots, f_t$ of degrees $\mathfrak{d}_1, \dots, \mathfrak{d}_t$ such that $pq^\nu \nmid |V(f_1, \dots, f_t)|$. The proof of this form of sharpness by N. M. Katz has an easily fixed flaw, which is discussed and repaired in Section 7.6. The author has not been able prove that anyone had fixed this before he did, but notes that anyone could have.

1.3 Methods

Our point of departure is the counting polynomial method of Wilson [67], [65], which we shall review here briefly, while casting it into our own notation. Let us assume for the moment that we have an Abelian code $\mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$, and we wish to p-adically estimate the weights of words in $\mathcal{C}$. For concreteness, suppose m is a positive integer, and we want to show that all weights vanish modulo p^m. For the rest of this chapter, let π denote reduction modulo p^d. When $e = 1$, i.e., when our Galois ring $\mathrm{GR}(p^d, e)$ is $\mathbb{Z}/p^d\mathbb{Z}$, Wilson's basic idea is to devise a polynomial $f(x) \in \mathbb{Q}[x]$ that approximates modulo p^m the lift of the weight function, i.e., such that $f(r) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$. We call such a polynomial a *counting polynomial*. Then for $c \in \mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$, Wilson carefully devises a lifted word $C \in \mathbb{Z}_p[A]$ such that $\pi(C_a) = c_a$ for all $a \in A$, and such that $\hat{C}(a) = 0$ whenever $\hat{c}(a) = 0$. So $\mathrm{wt}(c) = \sum_{a \in A} \mathrm{wt}(c_a) = \sum_{a \in A} \mathrm{wt}(\pi(C_a)) \equiv \sum_{a \in A} f(C_a) \pmod{p^m}$.

Now Wilson writes C_a in terms of its Fourier coefficients (i.e., uses the inverse Fourier transform). To be consistent with the notation of this thesis (not with Wilson), we devise a bilinear pairing $\langle \cdot, \cdot \rangle$ from $A \times A$ into $\mathbb{Q}_p(\zeta_{q'-1})$, which furnishes a non-canonical isomorphism between A and the group of characters of A, namely, $\langle a, \cdot \rangle \colon A \to \mathbb{Q}_p(\zeta_{q'-1})$ is the character that we identify with the element $a \in A$. Then we write $C_a = |A|^{-1} \sum_{b \in A} \hat{C}(b) \langle b, a \rangle$.

We want to calculate $\sum_{a\in A} f(C_a)$, which approximates $\mathrm{wt}(c)$ modulo p^m. For any $k \in \mathbb{N}$, we have $C_a^k = \left(|A|^{-1} \sum_{b\in S} \hat{C}(b)\langle b, a\rangle\right)^k = |A|^{-k} \sum_{b_1,\ldots,b_k\in S} \hat{C}(b_1)\ldots\hat{C}(b_k)\langle b_1\ldots b_k, a\rangle$, and $f(C_a)$ is a linear combination of such terms with $k \le \deg(f)$. Note that we are only summing over $b \in S$ (rather than $b \in A$) since S is a support of $\hat{c}$ (and thus, by the lifting procedure, it is also a support of $\hat{C}$). When we sum over a in A, we have $\sum_{a\in A} C_a^k = |A|^{1-k} \sum_{\substack{b_1,\ldots,b_k\in S \\ b_1\ldots b_k=1_A}} \hat{C}(b_1)\ldots\hat{C}(b_k)$. Then $\sum_{a\in A} f(C_a)$ (which is congruent modulo p^m to $\mathrm{wt}(c)$) is a linear combination of such terms for $k \le \deg(f)$. If $\deg(f)$ is less than the minimum length of unity-product sequences of elements in S (i.e., if $\deg(f) \le \omega(\mathcal{C})$), then $\sum_{a\in A} f(C_a) = 0$, and so $\mathrm{wt}(c) \equiv 0 \pmod{p^m}$. In this way, Wilson obtained his results (Theorems 1.5 and 1.6) by showing that one can find polynomials of low degree that approximate lifts of the appropriate weight functions (Lee weight, Hamming weight, and weight functions that count instances of particular symbols). The degree of the polynomial increases as the desired p-adic accuracy of the approximation (measured here by m) increases. To find such polynomials, Wilson performs some nontrivial calculations using the calculus of finite differences. Indeed, the calculations we have shown here (which assume the counting polynomial has already been found) are straightforward, while the existence of sufficiently low degree counting polynomials is not obvious.

We need to modify Wilson's counting polynomial method extensively in three ways (at least) to provide what is needed to prove the new results presented here (Theorems 1.7–1.11). Note that Wilson's method gives results (Theorems 1.5 and 1.6) in terms of the parameter $\ell(\mathcal{C})$ only, never in terms of $\ell_{mc}(\mathcal{C})$, $\ell_{mc}^{ss}(\mathcal{C})$, or $\ell_{mc}^{ss}(\mathcal{C})$. Thus our first two challenges are to devise counting polynomials that respect the modular condition and the scoring system described in Section 1.1 above. Thirdly, none of Wilson's results furnish proofs of sharpness. This is done by careful combinatorial analysis of terms in our p-adic estimates of weights.

To make a counting polynomial that respects the modular condition, we introduce averaging techniques. The averaging is straightforward if $e = 1$. Roughly speaking, we replace a counting polynomial $f(x)$ with $g(x) = (p-1)^{-1} \sum_{i=0}^{p-2} f(\zeta_{p-1}^i x)$, where ζ_{p-1} is a root of unity of order $p-1$. This $g(x)$ has all exponents of x divisible by $p-1$, which is exactly

what is needed to enforce the modular condition on sequences in our calculations. In the proof of Theorem 4.12 in Section 4.2, we use a generalization of this averaging procedure to obtain a counting polynomial suitable for proving Theorem 1.8. There we have a polynomial $f(x_0, \ldots, x_{d-1})$ that respects the scoring system (more details on this below), and we replace it with $g(x_0, \ldots, x_{d-1}) = (p-1)^{-1} \sum_{i=0}^{p-2} f(\zeta_{p-1}^i x_0, \ldots, \zeta_{p-1}^i x_{d-1})$ to produce a polynomial that respects both the modular condition and the scoring system.

In the case where $e > 1$, the polynomials constructed by Wilson do not even approximate lifted weight functions. For when $e > 1$, $\mathrm{GR}(p^d, e)$ is the quotient of $\mathbb{Z}_p[\zeta_{q-1}]$ modulo p^d, so that we need a polynomial $g(x)$ with $g(r) = \mathrm{wt}(\pi(r))$ for all $r \in \mathbb{Z}_p[\zeta_{q-1}]$, but Wilson's polynomials are designed to give approximations only for $r \in \mathbb{Z}_p$. So before we even address the modular condition, we must address a new challenge: finding counting polynomials for use with Galois rings $\mathrm{GR}(p^d, e)$ with $e > 1$. To do this, we perform an averaging procedure, called *trace-averaging*, which is based on the trace $\mathrm{Tr}\colon \mathbb{Q}_p(\zeta_{q-1}) \to \mathbb{Q}_p$. The trace-averaging procedure is somewhat technical even when $d = 1$ (i.e., for finite fields), and requires a great deal of care when $d > 1$. Trace-averaging forms from Wilson's polynomial a new polynomial $g(x_0, \ldots, x_{e-1}) \in \mathbb{Q}_p(\zeta_{q-1})[x_0, \ldots, x_{e-1}]$ with the property that $g(r, \mathrm{Fr}(r), \ldots, \mathrm{Fr}^{e-1}(r)) \equiv \mathrm{zer}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_p[\zeta_{q-1}]$, where Fr is the Frobenius automorphism. It turns out that trace-averaging not only fills a void by providing counting polynomials for use with Galois rings $\mathrm{GR}(p^d, e)$ with $e > 1$, but the polynomials thus furnished also respect the modular condition. In this way, we can obtain lower bounds on p-adic valuations of weights in terms of $\ell_{mc}(\mathcal{C})$ instead of bounds based on $\ell(\mathcal{C})$.

We also need to modify Wilson's method to provide counting polynomials that respect our scoring system, which was used to define the parameters $\omega^{ss}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$, $\omega^{ss}_{mc}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C})$ introduced in Section 1.1 above. Instead of constructing a single-variable counting polynomial $f(x) \in \mathbb{Q}[x]$ with the property that $f(r) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$, we construct a multivariable polynomial $f(x_0, \ldots, x_{d-1})$ that has the property that $f(r_0, \ldots, r_{d-1}) \equiv \mathrm{wt}(\pi(r_0 + pr_1 + \cdots + p^{d-1} r_{d-1})) \pmod{p^m}$ for all $r_0, \ldots, r_{d-1} \in \mathbb{Z}_p$. The degree of our polynomial in the variable x_i will be roughly $1/p^i$ times its degree in x_0. Then we decompose our codeword $c \in \mathrm{GR}(p^d, e)[A]$ in a very specific way (this is the *scaled*

Fourier-induced breakdown introduced in Section 2.3 and taken up again in Section 4.3). The decomposition is of the form $c = c^{(0)} + pc^{(1)} + \cdots + p^{d-1}c^{(d-1)}$. Each $c^{(i)}$ is then lifted to obtain a word $C^{(i)} \in \mathbb{Z}_p[A]$, and we compute $\sum_{a \in A} f(C_a^{(0)}, \ldots, C_a^{(d-1)})$ to approximate the weight. Precise details would be lengthy to state, but this method respects the scoring system, so we can obtain new lower bounds on p-adic valuations of weights in terms of $\ell^{ss}(\mathcal{C})$. We may also use an averaging technique to make a polynomial that respects both the scoring system and the modular condition, so we can obtain strong lower bounds in terms of $\ell^{ss}_{mc}(\mathcal{C})$.

In certain cases, we want to obtain sharp bounds on the p-adic valuations of weights from the counting polynomial method. Some of our new counting polynomials are suitable for this task, but they must be employed with great care to obtain proofs of sharpness. Recall that Wilson uses a counting polynomial $f(x)$ that approximates $\mathrm{wt} \circ \pi$ modulo p^m, and for which $\sum_{a \in A} f(C_a)$ vanishes, to prove that $\mathrm{wt}(c) \equiv 0 \pmod{p^m}$. Naturally, Wilson chooses a polynomial $f(x)$ that approximates $\mathrm{wt} \circ \pi$ as closely as possible, subject to the constraint that the degree of $f(x)$ be low enough that $\sum_{a \in A} f(C_a)$ vanishes. To obtain a sharp bound we use a counting polynomial g that approximates $\mathrm{wt} \circ \pi$ a little more precisely, say modulo p^{m+1}, so that the sum $\sum_{a \in A} g(C_a)$ does not entirely vanish, but becomes a polynomial function of the lifted Fourier coefficients $\hat{C}(a)$. (We may actually be looking at an analogous, but more complicated sum if we are using some of the more exotic multivariable polynomials discussed above, but the idea remains the same.) Then a combinatorial analysis of $\sum_{a \in A} g(C_a)$, regarded as a polynomial function of the lifted Fourier coefficients, can be used to determine that, as c runs through our code $\mathcal{C}$, the lifted Fourier coefficients at some point take on values such that $\sum_{a \in A} g(C_a)$ does not vanish modulo p^{m+1}. This combinatorial analysis can be quite intricate in certain cases, e.g., see the proof of Theorem 4.18.

Finally, we combine the trace-averaging method with techniques for dealing with multiple words to obtain a polynomial for counting simultaneous zeroes. This enables us to prove Theorem 1.11. We obtain the result of N. M. Katz (Theorem 1.12) by deriving and employing a slightly refined version of the result that punctured Reed-Muller codes are

cyclic [28].

1.4 Sketch of the Contents

Chapter 2 is all preliminary material. Section 2.1 reviews p-adic fields and Galois rings, and Sections 2.2 and 2.3 review the Fourier transform. Section 2.4 introduces the various weight functions we shall consider, and introduces the notion of *normalized weight*, which is our device for dealing with codes in which 1_A is in the support of the Fourier transform (i.e., codes with constant words). Of particular note is Section 2.5, which introduces the notion of *accounts*, which are simply functions from a set Y into the integers. Accounts that take nonnegative values are regarded as multisets. This combinatorial device is indispensable for making our equations (barely) compact enough to display conveniently on the page. Any reader who wishes to understand the calculations performed here must be familiar with the notations for accounts. Sections 2.6 and 2.7 include various combinatorial devices that we employ to obtain our more precise results (such as proofs of sharpness). We recommended that the reader pass over these sections and return to them only when the tools they describe are actually employed (in parts of Chapters 4–7). Section 2.8 describes some notations we use for multivariable polynomials as well as some basic facts about polynomials that we shall need. The reader should be familiar with the notations set down there because they are often used.

Chapter 3 provides abstract theorems that will give p-adic estimates of weights if one can furnish an appropriate counting polynomial. Nothing is said about how to find counting polynomials; this will be done in each of the succeeding chapters as the need arises.

In Chapter 4, we prove Theorems 1.8 and 1.7, while laying down the foundations needed for all our counting polynomial constructions. Section 4.1 has some fundamental material on the Newton expansion, which is the mathematical device underlying all our counting polynomial constructions. We construct our counting polynomials in Section 4.2, some of which will be used in Chapters 6 and 7. We show how to employ the polynomials in Section 4.3. The techniques and results of Sections 4.1–4.3 will be reused in Chapter 5. In Sections 4.4 and 4.5, we use our counting polynomials to prove Theorems 1.8 and 1.7, and in Section

4.6 we compare these results with earlier work.

Chapter 5 is dedicated to proving Theorem 1.9. After discussing previous results and comparing our new theorem with them (relying heavily on material from Section 4.6 for the comparison), we spend the next two sections (5.1 and 5.2) specializing the notions of Sections 4.2 and 4.3 for Lee weight. Thus we obtain a counting polynomial, which we use in Section 5.3 to prove Theorem 1.9.

Chapter 6 is dedicated to proving Theorem 1.10. In Sections 6.1–6.3, we develop the trace-averaging procedure to obtain an appropriate counting polynomial. We derive Theorem 1.10 in Section 6.4 and show that we can recover some earlier results from this highly general theorem in Section 6.5.

In Chapter 7, we prove Theorem 1.11 and relate it to the theorem of N. M. Katz (Theorem 1.12). In Sections 7.1–7.3, we carry out a more specialized version (for finite fields only) of the trace-averaging procedure of Chapter 6. Then in Section 7.4, we construct our polynomial for counting simultaneous zeroes. We use this polynomial in Section 7.5 to prove Theorem 1.11. In Section 7.6, we review the theorems of Chevalley-Warning, Ax, and N. M. Katz. In Section 7.7, we show how to translate results about weights in group algebras to results about cardinalities of affine algebraic sets over finite fields. In Section 7.8, we prove the theorem of N. M. Katz and the associated statement about its sharpness.

Chapter 2

Preliminaries

In this chapter, we review the fundamental mathematics needed to state and prove our results. We also introduce definitions, notations, and combinatorial devices that allow us to describe and manipulate the objects that arise in this study. We discuss p-adic fields and Galois rings in Section 2.1. Then we introduce the Fourier transform for the group algebra $R[A]$ (with R a fairly generic ring) in Section 2.2. In Section 2.3, we give more specialized results on the Fourier transform in the case when R is a Galois ring or a ring of integers in an unramified extension of the p-adics. In Section 2.4, we review weight functions commonly used in algebraic coding theory. There we introduce the normalized weight function, a device for simplifying the presentation of our results when our code has the trivial character in the support of its Fourier transform (i.e., when our code contains constant words).

The second half of this chapter deals more with notations and devices that make it easier for us to state and prove our theorems. Section 2.5 is especially critical in this regard. There we introduce the notion of an *account* (which is a generalization of a multiset) and tools for manipulation of accounts. These accounts are ubiquitous in this thesis, so the reader must be familiar with them, with their notation, and with the basic operations that can be performed upon them. Section 2.6 introduces the procedures called *collapse* and *reduction* of accounts. These devices are needed in our proofs of sharpness of lower bounds on p-adic valuations of weights. The reader should probably skip this section until collapse and reduction are actually used (beginning in Section 4.4). Section 2.7 introduces the *Frobenius action* on accounts. This device is used to prove that certain quantities in our p-adic

estimates, which we already know to be elements of $\mathbb{Z}_p[\zeta_{q-1}]$, are in fact elements of $\mathbb{Z}_p$. It would be a good idea for readers to skip this section, and return to it only if they want to understand the use of the Frobenius action in the proofs of Theorems 4.18, 5.12, 6.13, and 7.14. Section 2.8 includes notations we use with multivariable polynomials. There we also include a basic fact about polynomials, which we use to prove that certain of our bounds on p-adic valuations of weights are sharp.

2.1 Number Systems

Before we discuss p-adic fields and Galois rings, we fix certain conventions and notations once and for all. We use *integer* to mean a rational integer unless further qualified. We let $\mathbb{Z}$ denote the set integers, $\mathbb{Z}_+$ the set of strictly positive integers, $\mathbb{N}$ the set of nonnegative integers, and $\mathbb{Q}$ the rational numbers. We always use p to denote a prime in $\mathbb{N}$. We represent the ring of integers modulo m as $\mathbb{Z}/m\mathbb{Z}$. We use $\mathbb{Z}_p$ to denote the p-adic integers and $\mathbb{Q}_p$ to denote the p-adic rationals, which are described in Chapter II of [46]. We use ζ_n to denote a root of unity of order n over $\mathbb{Q}_p$. We record the facts we need to know about $\mathbb{Z}_p$ and $\mathbb{Q}_p$ here:

Proposition 2.1 (p-Adic Integers and Rationals). *$\mathbb{Z}_p$ is a discrete valuation ring of characteristic 0 with the unique nonzero prime ideal generated by p, and $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. Thus each nonzero element of $\mathbb{Q}_p$ can be written uniquely as $p^m u$ with $m \in \mathbb{Z}$ and u a unit in $\mathbb{Z}_p$, where the nonzero elements of $\mathbb{Z}_p$ are precisely such elements with $m \geq 0$, and the units in $\mathbb{Z}_p$ are precisely such elements with $m = 0$. $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are complete in the topology defined by this valuation. $\mathbb{Z}_p$ contains ζ_{p-1}. The set consisting of zero and the powers of ζ_{p-1} is a set of representatives of the equivalence classes modulo p in $\mathbb{Z}_p$. The quotient modulo p of $\mathbb{Z}_p$ is the prime field $\mathbb{F}_p$, whose cyclic group of units is generated by the reduction modulo p of ζ_{p-1}. The quotient modulo p^m of $\mathbb{Z}_p$ is the integer residue ring $\mathbb{Z}/p^m\mathbb{Z}$. Each element of $a \in \mathbb{Z}_p$ has a unique representation as $\sum_{i=0}^{\infty} a_i p^i$, where each a_i is either zero or a power of ζ_{p-1}.*

Proof. These are all either explicitly mentioned in, or readily apparent from, the discussion in Chapter II of [46]. □

We consider certain algebraic extensions of $\mathbb{Q}_p$ whose behavior is similar.

Proposition 2.2 (Unramified Extensions of the p-Adics). *$\mathbb{Q}_p(\zeta_{p^n-1})$ is a degree n Galois extension of $\mathbb{Q}_p$, and the Galois group of $\mathbb{Q}_p(\zeta_{p^n-1})$ over $\mathbb{Q}_p$ is the cyclic group of order n generated by the automorphism* Fr *which takes ζ_{p^n-1} to $\zeta_{p^n-1}^p$. The elements of $\mathbb{Q}_p(\zeta_{p^n-1})$ that are integral over $\mathbb{Z}_p$ form the ring $\mathbb{Z}_p[\zeta_{p^n-1}]$. $\mathbb{Z}_p[\zeta_{p^n-1}]$ is a discrete valuation ring of characteristic 0 with the unique nonzero prime ideal generated by p, and $\mathbb{Q}_p(\zeta_{p^n-1})$ is the field of fractions of $\mathbb{Z}_p[\zeta_{p^n-1}]$. Thus each nonzero element of $\mathbb{Q}_p(\zeta_{p^n-1})$ can be written uniquely as $p^m u$ with $m \in \mathbb{Z}$ and u a unit in $\mathbb{Z}_p[\zeta_{p^n-1}]$, where the nonzero elements of $\mathbb{Z}_p[\zeta_{p^n-1}]$ are precisely such elements with $m \geq 0$, and the units in $\mathbb{Z}_p[\zeta_{p^n-1}]$ are precisely such elements with $m = 0$. $\mathbb{Q}_p(\zeta_{p^n-1})$ and $\mathbb{Z}_p[\zeta_{p^n-1}]$ are complete in the topology defined by this valuation. The set consisting of zero and the powers of ζ_{p^n-1} is a set of representatives of the equivalence classes modulo p in $\mathbb{Z}_p[\zeta_{p^n-1}]$. The quotient modulo p of $\mathbb{Z}_p[\zeta_{p^n-1}]$ is the finite field $\mathbb{F}_{p^n}$, whose cyclic group of units is generated by the reduction modulo p of ζ_{p^n-1}. The automorphism* Fr *on $\mathbb{Q}_p[\zeta_{p^n-1}]$ induces an automorphism (which we shall also call* Fr*) on $\mathbb{F}_{p^n}$; this induced automorphism takes each element to its pth power and it generates the Galois group of order n of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Furthermore, $\mathbb{Q}_p(\zeta_{p^{n_1}-1}) \cap \mathbb{Q}_p(\zeta_{p^{n_2}-1}) = \mathbb{Q}_p(\zeta_{p^{\gcd(n_1,n_2)}-1})$ and $\mathbb{Z}_p[\zeta_{p^{n_1}-1}] \cap \mathbb{Z}_p[\zeta_{p^{n_2}-1}] = \mathbb{Z}_p[\zeta_{p^{\gcd(n_1,n_2)}-1}]$. Thus, $\mathbb{Q}_p(\zeta_{p^{n_1}-1}) \subseteq \mathbb{Q}_p(\zeta_{p^{n_2}-1})$ if and only if $n_1 \mid n_2$, and $\mathbb{Z}_p[\zeta_{p^{n_1}-1}] \subseteq \mathbb{Z}_p[\zeta_{p^{n_2}-1}]$ if and only if $n_1 \mid n_2$.*

Proof. This follows from Proposition 16 (along with Corollary 1) in Chapter IV of [47], assuming the theory developed in that book up until that point, most particularly Propositions 3 and 8 of Chapter II. □

Let us examine in more detail the valuation mentioned in Propositions 2.1 and 2.2 above. For a nonzero element $a \in \mathbb{Q}_p(\zeta_{p^n-1})$, the unique integer m such that $a = p^m u$ for some unit $u \in \mathbb{Z}_p[\zeta_{p^n-1}]$ is called the *p-adic valuation* of a. If a also lies in $\mathbb{Q}_p(\zeta_{p^{n'}-1})$, then it is not hard to show that the p-adic valuation of a in this other field is precisely the same as its p-adic valuation in the $\mathbb{Q}_p(\zeta_{p^n-1})$. Thus no reference to the field containing a is necessary, and the p-adic valuation of a is simply denoted $v_p(a)$. We define $v_p(0) = \infty$, and we consider ∞ strictly greater than any integer and set anything plus ∞ to ∞. We say that

two elements a and b are *congruent modulo* p^m to mean that $v_p(a-b) \geq m$. Thus the notion of equivalence of elements modulo powers of p is independent of which unramified extension of $\mathbb{Q}_p$ we regard as the ambient field. With these conventions, we have the following easily verified properties of the p-adic valuation:

Lemma 2.3 (Properties of v_p). *For any $a, b \in \mathbb{Q}_p(\zeta_{p^n-1})$, we have the following:*

(i) $v_p(a) = \infty$ *if and only if* $a = 0$.

(ii) $v_p(ab) = v_p(a) + v_p(b)$.

(iii) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$, *with equality when* $v_p(a) \neq v_p(b)$.

For $a \in \mathbb{Q}_p(\zeta_{p^n-1})$, we also define the *p-adic absolute value* of a, denoted $|a|_p$, to be $p^{-v_p(a)}$, where $p^{-\infty}$ is considered to be 0. The properties of v_p translate into properties of $|\cdot|_p$ as follows:

Lemma 2.4 (Properties of $|\cdot|_p$). *For any $a, b \in \mathbb{Q}_p(\zeta_{p^n-1})$, we have the following:*

(i) $|a|_p = 0$ *if and only if* $a = 0$.

(ii) $|ab|_p = |a|_p |b|_p$.

(iii) $|a+b|_p \leq \max\{|a|_p, |b|_p\}$, *with equality when* $|a|_p \neq |b|_p$.

Thus the p-adic absolute value provides a metric on $\mathbb{Q}_p(\zeta_{p^n-1})$, where the distance between a and b is $|a-b|_p$. This metric defines a topology on $\mathbb{Q}_p(\zeta_{p^n-1})$ that we call the *p-adic topology*. It is this topology that is discussed in Propositions 2.1 and 2.2 above.

In Proposition 2.2, we saw that the finite fields of characteristic p can be obtained as quotients modulo p of rings of algebraic integers in unramified extensions of $\mathbb{Q}_p$. We shall also be interested in the quotients of these rings modulo powers of p. The *Galois ring of characteristic p^m and order p^{mn}*, denoted $\mathrm{GR}(p^m, n)$ is the quotient modulo p^m of $\mathbb{Z}_p[\zeta_{p^n-1}]$. Note that $\mathrm{GR}(p, n)$ is the finite field $\mathbb{F}_{p^n}$ of order p^n. Also note that $\mathrm{GR}(p^m, 1)$ is the integer residue ring $\mathbb{Z}/p^m\mathbb{Z}$. The ring $\mathrm{GR}(p^m, n)$ contains $\mathbb{Z}/p^m\mathbb{Z}$ as a subring and can be thought of as an extension of $\mathbb{Z}/p^m\mathbb{Z}$ obtained by adjoining a root of unity of order p^n-1. Furthermore, the statements regarding intersections and containments of extensions of $\mathbb{Q}_p$

and $\mathbb{Z}_p$ in Proposition 2.2 imply that $\mathrm{GR}(p^m, n_1) \cap \mathrm{GR}(p^m, n_2) = \mathrm{GR}(p^m, \gcd(n_1, n_2))$, and therefore $\mathrm{GR}(p^m, n_1) \subseteq \mathrm{GR}(p^m, n_2)$ if and only if $n_1 \mid n_2$. In this case, $\mathrm{GR}(p^m, n_2)$ is a free $\mathrm{GR}(p^m, n_1)$-module. Note that $\mathrm{GR}(p^m, n)$ is a principal ideal ring with $m+1$ ideals, namely $p^j \mathrm{GR}(p^m, n_2)$ for $j = 0, 1, \ldots, m$. Here $p^0 \mathrm{GR}(p^m, n_2)$ is the entire ring and $p^m \mathrm{GR}(p^m, n_2)$ is the zero ideal. For more information on Galois rings, the reader should consult the book of McDonald [34].

It does not make sense to consider the ring $\mathrm{GR}(p^{m_1}, n)$ as a subring of $\mathrm{GR}(p^{m_2}, n)$ when $m_1 < m_2$, since the two rings have different characteristics. However, we do have a way of relating elements of the one ring to elements of the other. Since $m_1 < m_2$, reduction modulo p^{m_1} furnishes an epimorphism from $\mathrm{GR}(p^{m_2}, n)$ to $\mathrm{GR}(p^{m_1}, n)$. Thus for $m_1 \leq m_2$, if $a \in \mathrm{GR}(p^{m_2}, n)$, we define $\pi_{m_1}(a) \in \mathrm{GR}(p^{m_1}, n)$ to be the reduction modulo p^{m_1} of a. Also, if $a \in \mathbb{Z}_p[\zeta_{p^n-1}]$, we define $\pi_{m_1}(a) \in \mathrm{GR}(p^{m_1}, n)$ to be the reduction modulo p^{m_1} of a. Since ζ_{p^n-1} is a root of unity of order $p^n - 1$ over $\mathbb{Q}_p$ and since $\pi_1(\zeta_{p^n-1})$ is a root of unity of order $p^n - 1$ in $\mathbb{F}_{p^n}$ (see Proposition 2.2 above), we know that $\pi_m(\zeta_{p^n-1})$ is a root of unity of order $p^n - 1$ in $\mathrm{GR}(p^m, n)$ for every positive integer m. As a convention, we define π_∞ to be the identity map on $\mathbb{Z}_p[\zeta_{p^n-1}]$.

Now we wish to define a map from $\mathrm{GR}(p^{m_1}, n)$ to $\mathrm{GR}(p^{m_2}, n)$ when $m_1 < m_2$. Proposition 2.2 tells us that each element $a \in \mathbb{Z}_p[\zeta_{p^n-1}]$ can be written uniquely as $\sum_{i=0}^{\infty} a_i p^i$, where each a_i is either zero or a power of ζ_{p^n-1}. We call this the *canonical expansion* of $a \in \mathbb{Z}_p[\zeta_{p^n-1}]$. This implies that when m is a positive integer, each element a of $\mathrm{GR}(p^m, n)$ can be written uniquely as $\sum_{i=0}^{m-1} a_i p^i$, where each a_i is either zero or a power of $\pi_m(\zeta_{p^n-1})$. We likewise call this the *canonical expansion* of $a \in \mathrm{GR}(p^m, n)$. For $m_1 \leq m_2$ and $a \in \mathrm{GR}(p^{m_1}, n)$, with canonical expansion $a = \sum_{i=0}^{m_1-1} a_i p^i$, we define $\tau_{m_2}(a)$ to be an element $b \in \mathrm{GR}(p^{m_2}, n)$ with canonical expansion $b = \sum_{i=0}^{m_1-1} b_i p^i$, where $b_i = 0$ whenever $a_i = 0$ and $b_i = \pi_{m_2}(\zeta_{p^n-1})^j$ whenever $a_i = \pi_{m_1}(\zeta_{p^n-1})^j$. We also define $\tau_\infty(a) = \sum_{i=0}^{m_1-1} c_i p^i$, where $c_i = 0$ whenever $a_i = 0$ and $c_i = \zeta_{p^n-1}^j$ whenever $a_i = \pi_{m_1}(\zeta_{p^n-1})^j$. For each positive integer m, we call π_m the *Teichmüller lift to characteristic* p^m and call τ_∞ the *Teichmüller lift to characteristic* 0.

For $m_1 \leq m_2$ in $\mathbb{Z}_+ \cup \{\infty\}$, we have $\pi_{m_1} \circ \pi_{m_2} = \pi_{m_1}$ and $\tau_{m_2} \circ \tau_{m_1} = \tau_{m_2}$. Furthermore,

if $a \in \mathrm{GR}(p^{m_1}, n)$, $\pi_{m_1}(\tau_{m_2}(a)) = a$, but if $a \in \mathrm{GR}(p^{m_2}, n)$, then it is not always true that $\tau_{m_2}(\pi_{m_1}(a)) = a$.

To summarize the relationships between the various unramified extensions of $\mathbb{Q}_p$ and the various Galois rings, we have the following commutative diagrams, where unmarked arrows are inclusion maps:

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xrightarrow{\pi_m} & \mathrm{GR}(p^m, n) & \xrightarrow{\pi_1} & \mathbb{F}_{p^n} \\
\uparrow & & \uparrow & & \uparrow & & \uparrow \\
\mathbb{Q}_p & \longleftarrow & \mathbb{Z}_p & \xrightarrow{\pi_m} & \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\pi_1} & \mathbb{F}_p
\end{array}$$

and

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xleftarrow{\tau_\infty} & \mathrm{GR}(p^m, n) & \xleftarrow{\tau_m} & \mathbb{F}_{p^n} \\
\uparrow & & \uparrow & & \uparrow & & \uparrow \\
\mathbb{Q}_p & \longleftarrow & \mathbb{Z}_p & \xleftarrow{\tau_\infty} & \mathbb{Z}/p^m\mathbb{Z} & \xleftarrow{\tau_m} & \mathbb{F}_p.
\end{array}$$

In each diagram, the two rows coincide when $n = 1$, and the last two columns coincide when $m = 1$.

We transplant the notion of p-adic valuation from the unramified extensions of $\mathbb{Q}_p$ to the Galois rings. The *p-adic valuation* of a nonzero element $a \in \mathrm{GR}(p^m, n)$, denoted $v_p(a)$, is defined to be the greatest k such that $a \in p^k \mathrm{GR}(p^m, n)$. We define $v_p(0) = \infty$ in $\mathrm{GR}(p^m, n)$. Thus we have defined $v_p\colon \mathrm{GR}(p^m, n) \to \{0, 1, \ldots, m-1, \infty\}$. Note that for any $m_1 \in \mathbb{Z}$, $m_2 \in \mathbb{Z}_+ \cup \{\infty\}$ with $m_1 \le m_2$, and $a \in \mathrm{GR}(p^{m_1}, a)$, we have $v_p(\tau_{m_2}(a)) = v_p(a)$. On the other hand, if $m_1 \le m_2$ are positive integers and $a \in \mathrm{GR}(p^{m_2}, n)$, then $v_p(\pi_{m_1}(a)) = v_p(a)$ if $v_p(a) < m_1$ or $v_p(a) = \infty$, but $v_p(\pi_{m_1}(a)) = \infty$ when $m_1 \le v_p(a) < \infty$. Likewise, if $a \in \mathbb{Z}_p[\zeta_{p^n-1}]$ and m_1 is a positive integer, then $v_p(\pi_{m_1}(a)) = v_p(a)$ if $v_p(a) < m_1$ or $v_p(a) = \infty$, but $v_p(\pi_{m_1}(a)) = \infty$ when $m_1 \le v_p(a) < \infty$.

In Proposition 2.2, we used Fr to denote the field automorphism of $\mathbb{Q}_p(\zeta_{p^n-1})$ that fixes $\mathbb{Q}_p$ pointwise and takes ζ_{p^n-1} to $\zeta_{p^n-1}^p$. Note that Fr restricted to $\mathbb{Z}_p[\zeta_{p^n-1}]$ is an automorphism of rings. We also used Fr to denote the field automorphism it induces on $\mathbb{F}_{p^n}$ through reduction modulo p; this automorphism takes every element to its pth power. Because the automorphism Fr of the field $\mathbb{Q}_p(\zeta_{p^n-1})$ takes p^m to p^m, it permutes the ideal $p^m\mathbb{Z}_p[\zeta_{p^n-1}]$ of the ring $\mathbb{Z}_p[\zeta_{p^n-1}]$, and thus induces an automorphism of the ring $\mathrm{GR}(p^m, n)$

for each positive m through reduction modulo p^m. This automorphism fixes pointwise the subring $\mathrm{GR}(p^m,1)=\mathbb{Z}/p^m\mathbb{Z}$ of $\mathrm{GR}(p^m,n)$ and maps the element $\pi_m(\zeta_{p^n-1})$ to $\pi_m(\zeta_{p^n-1})^p$. Throughout the thesis we call all of these automorphisms the *Frobenius automorphism* and denote them all by Fr.

It is not difficult to show that Fr commutes with π_m and τ_m for all $m\in\mathbb{Z}_+\cup\{\infty\}$. That is, we have the commutative diagrams

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xrightarrow{\pi_m} & \mathrm{GR}(p^m,n) & \xrightarrow{\pi_1} & \mathbb{F}_{p^n} \\
\mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow \\
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xrightarrow{\pi_m} & \mathrm{GR}(p^m,n) & \xrightarrow{\pi_1} & \mathbb{F}_{p^n}
\end{array}$$

and

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xleftarrow{\tau_\infty} & \mathrm{GR}(p^m,n) & \xleftarrow{\tau_m} & \mathbb{F}_{p^n} \\
\mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow & & \mathrm{Fr}\downarrow \\
\mathbb{Q}_p(\zeta_{p^n-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^n-1}] & \xleftarrow{\tau_\infty} & \mathrm{GR}(p^m,n) & \xleftarrow{\tau_m} & \mathbb{F}_{p^n},
\end{array}$$

where unlabeled arrows are inclusion maps.

Recall that $\mathbb{Q}_p(\zeta_{p^{n_1}-1})\subseteq\mathbb{Q}_p(\zeta_{p^{n_2}-1})$ if and only if $n_1\mid n_2$, and recall that $\mathrm{GR}(p^{n_1},m)\subseteq\mathrm{GR}(p^{n_2},m)$ if and only if $n_1\mid n_2$. Suppose $n_1\mid n_2$. Since Fr generates the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_2}-1})/\mathbb{Q}_p)$ of order n_2 and the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_1}-1})/\mathbb{Q}_p)$ of order n_1, we see that Fr^{n_1} generates the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_2}-1})/\mathbb{Q}_p(\zeta_{p^{n_1}-1}))$ of order n_2/n_1. Thus an element of $\mathbb{Q}_p(\zeta_{p^{n_2}-1})$ is in $\mathbb{Q}_p(\zeta_{p^{n_1}-1})$ if and only if it is fixed by Fr^{n_1}. Likewise, for any positive integer m, an element of $\mathrm{GR}(p^m,n_2)$ is in $\mathrm{GR}(p^m,n_1)$ if and only if it is fixed by Fr^{n_1}. This can be checked by writing the canonical expansion of an arbitrary element of $\mathrm{GR}(p^m,n_2)$ and applying Fr^{n_1}. If any coefficient is neither zero nor a power of $\pi_m(\zeta_{p^{n_1}-1})$, the element will not be fixed by Fr^{n_1}; otherwise the element will be fixed.

If $n_1\mid n_2$, we define the trace map $\mathrm{Tr}_{n_1}^{n_2}\colon\mathbb{Q}_p(\zeta_{p^{n_2}-1})\to\mathbb{Q}_p(\zeta_{p^{n_1}-1})$ by $\mathrm{Tr}_{n_1}^{n_2}(a)=\sum_{j=0}^{(n_2/n_1)-1}\mathrm{Fr}^{n_1 j}(a)$. Since Fr commutes with π_m for all positive integers m, it induces a trace map on the Galois rings, which we express with the same notation, i.e., we write $\mathrm{Tr}_{n_1}^{n_2}\colon\mathrm{GR}(p^m,n_2)\to\mathrm{GR}(p^m,n_1)$. That this trace map is a surjective $\mathrm{GR}(p^m,n_1)$-linear map follows from the fact that $\mathrm{Tr}_{n_1}^{n_2}\colon\mathbb{Q}_p(\zeta_{p^{n_2}-1})\to\mathbb{Q}_p(\zeta_{p^{n_1}-1})$ is a surjective $\mathbb{Q}_p(\zeta_{p^{n_1}-1})$-linear map. Of course $\mathrm{Tr}_{n_1}^{n_2}\colon\mathrm{GR}(p,n_2)\to\mathrm{GR}(p,n_1)$ is just the usual trace from $\mathbb{F}_{p^{n_2}}$ to

$\mathbb{F}_{p^{n_1}}$. Since Fr commutes with the maps π_m and τ_m for all $m \in \mathbb{Z}_+ \cup \{\infty\}$, we also know that $\mathrm{Tr}_{n_1}^{n_2}$ commutes with π_m and τ_m for all $n_1, n_2 \in \mathbb{Z}_+$ and $m \in \mathbb{Z}_+ \cup \{\infty\}$. In terms of commutative diagrams, we have

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^{n_2}-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^{n_2}-1}] & \xrightarrow{\pi_m} & \mathrm{GR}(p^m, n_2) & \xrightarrow{\pi_1} & \mathbb{F}_{p^{n_2}} \\
\mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow \\
\mathbb{Q}_p(\zeta_{p^{n_1}-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^{n_1}-1}] & \xrightarrow{\pi_m} & \mathrm{GR}(p^m, n_1) & \xrightarrow{\pi_1} & \mathbb{F}_{p^{n_1}}
\end{array}$$

and

$$\begin{array}{ccccccc}
\mathbb{Q}_p(\zeta_{p^{n_2}-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^{n_2}-1}] & \xleftarrow{\tau_\infty} & \mathrm{GR}(p^m, n_2) & \xleftarrow{\tau_m} & \mathbb{F}_{p^{n_2}} \\
\mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow & & \mathrm{Tr}_{n_1}^{n_2}\downarrow \\
\mathbb{Q}_p(\zeta_{p^{n_1}-1}) & \longleftarrow & \mathbb{Z}_p[\zeta_{p^{n_1}-1}] & \xleftarrow{\tau_\infty} & \mathrm{GR}(p^m, n_1) & \xleftarrow{\tau_m} & \mathbb{F}_{p^{n_1}},
\end{array}$$

where unlabeled arrows are inclusion maps.

2.2 Group Algebras and the Fourier Transform

We now define the group algebra $R[A]$, which is our basic object of study. Recall from the last section that we always use p to denote a positive rational prime. We shall always use A to denote a finite Abelian group with $p \nmid |A|$. We write A multiplicatively with identity 1_A (or just 1 if there is no cause for confusion). Throughout this section, let R be a commutative ring with multiplicative identity 1_R (or just 1 if there is no cause for confusion). We assume that the characteristic of R is 0 or a power of p and that $|A|$ has a multiplicative inverse in R.

An element $f \in R[A]$ is written as a formal sum $f = \sum_{a \in A} f_a a$, with each coefficient f_a in R. We use the notation f_a and $f(a)$ interchangeably for the coefficient of a in f, as we find it convenient. If $f, g \in R[A]$ and $c \in R$, then the addition operation of $R[A]$ is given by $(f+g)_a = f_a + g_a$, i.e., pointwise addition, and the R-scalar multiplication of $R[A]$ is given by $(cf)_a = cf_a$. The ring multiplication, called *convolution*, is given by $(fg)_a = \sum_{a \in A} f_b g_{b^{-1}a}$. $R[A]$ contains an isomorphic copy of R, namely $\{r1_A : r \in R\}$, which includes $1_R 1_A$, the multiplicative identity of $R[A]$. An ideal of $R[A]$ is called an *Abelian code* (or just *code*) *in* $R[A]$, and elements of $R[A]$ are often called *codewords* or just *words*. The *constant words* are precisely those words $f \in R[A]$ for which there exists an $r \in R$ such that $f_a = r$ for all

$a \in A$.

Another algebra of interest to us is R^A, which consists of all functions from A to R, with pointwise addition and multiplication of functions, i.e., $(f+g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$. We also have R-scalar multiplication $(rf)(a) = rf(a)$ for $r \in R$ and $a \in A$. We use the notation $f(a)$ and f_a interchangeably for the value of f at a, as we find it convenient. The multiplicative identity is the constant function equal to 1 everywhere.

Sometimes we shall combine elements of $R[A]$ by means of pointwise multiplication or combine elements of R^A by convolution. Since these are not the proper multiplications in these rings, we write $f \cdot g$ for the pointwise product of $f, g \in R[A]$ and $f * g$ for the convolution product of $f, g \in R^A$. If we wish to equip $R[A]$ with pointwise multiplication as its multiplicative operation, we shall write $(R[A], \cdot)$, and if we wish to equip R^A with convolution, we shall write $\left(R^A, *\right)$ to make these unusual circumstances apparent.

We analyze elements and ideals of group rings by means of the Fourier transform. In order to have a satisfactory Fourier transform, $|A|$ should be a unit in our ring of scalars R, and R should contain roots of unity of order equal to the exponent of A (see Theorem 18 of [21]). The first condition is fulfilled by one of our initial assumptions about R. We also assume that the second condition is fulfilled for the rest of this section.

We define a *character of A into R* to be a homomorphism from A into the group of units of R. These characters, regarded as functions with pointwise multiplication, form an Abelian group X, which we shall show to be isomorphic to A. Let $a_1, \ldots, a_k$ be elements of A of orders $n_1, \ldots, n_k$, such that each element of A can be written uniquely as $a_1^{i_1} \ldots a_k^{i_k}$ with $0 \leq i_h < n_h$ for each h. A character from A to R is uniquely determined by its values on $a_1, \ldots, a_k$. Let θ_h be a root of unity of order n_h in R for each h. A character must take a_h to some power of θ_h; if $a = a_1^{i_1} \ldots a_k^{i_k}$, we define χ_a to be the character that takes a_h to $\theta_h^{i_h}$ for all h. Then we note that if $a, b \in A$, then $\chi_{ab} = \chi_a \chi_b$, so that $a \mapsto \chi_a$ is in fact an isomorphism from A to our group X of characters. To make this isomorphism easier to employ, we follow Delsarte [16] and introduce the pairing $\langle \cdot, \cdot \rangle \colon A \times A \to R$, defined so that $\left\langle a_1^{i_1} \ldots a_k^{i_k}, a_1^{j_1} \ldots a_k^{j_k} \right\rangle = \theta_1^{i_1 j_1} \ldots \theta_k^{i_k j_k}$. Then $\chi_a(b) = \langle a, b \rangle$, i.e., for each $a \in A$, the character χ_a is the function $\langle a, \cdot \rangle \colon A \to R$. We now examine the basic properties of $\langle \cdot, \cdot \rangle$.

In the following lemma, and for the rest of this thesis, we use the Kronecker delta $\delta(x, y)$, which equals 1 when $x = y$, and equals 0 otherwise.

Lemma 2.5 (Properties of $\langle \cdot, \cdot \rangle$). *For any $a, b, c \in A$ and $n \in \mathbb{Z}$, we have the following:*

(i) $\langle a, b \rangle = \langle b, a \rangle$.

(ii) $\langle a, bc \rangle = \langle a, b \rangle \langle a, c \rangle$.

(iii) $\langle a, b^n \rangle = \langle a, b \rangle^n$.

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

(v) $\sum_{b \in A} \langle a, b \rangle = |A| \delta_{a, 1_A}$.

Proof. These are easy to verify. □

Thus our pairing is symmetric and bilinear and establishes a (non-canonical) isomorphism from A to X. Now we are ready to introduce the Fourier transform in terms of our pairing.

The Fourier transform of a function $f \in R[A]$ is usually defined to be the function $g \colon X \to R$ so that $g(\chi) = \sum_{b \in A} f_b \chi(b)^{-1}$. Using the isomorphism from A to X given by $a \mapsto \chi_a$, we can consider the Fourier transform to have domain A instead of X, i.e., we consider the Fourier transform of f to be the function $h \colon A \to R$ with $h(a) = g(\chi_a)$. We take this as our standard definition for the Fourier transform; our bilinear pairing makes this definition easy to state.

Let $f \in R[A]$. Then the *Fourier transform of* f, denoted $\mathrm{FT}(f)$ or $\hat{f}$, is the element of R^A with $\hat{f}(a) = \sum_{b \in A} f_b \langle b^{-1}, a \rangle$ for all $a \in A$. The *scaled Fourier transform of* f, denoted $\tilde{f}$, is the element of R^A with $\tilde{f}(a) = |A|^{-1} \hat{f}(a)$ for all $a \in A$. We often call the values $\hat{f}(a)$ for $a \in A$ the *Fourier coefficients* of f and the values $\tilde{f}(a)$ the *scaled Fourier coefficients* of f.

The first thing we should note is that the Fourier transform is an R-algebra isomorphism.

Proposition 2.6 (Fourier Transform is an Isomorphism). *The Fourier transform is an isomorphism of R-algebras from $R[A]$ to R^A with inverse given by*

$$f(a) = |A|^{-1} \sum_{b \in A} \hat{f}(b)\langle b, a\rangle.$$

For $f, g \in R[A]$, the Fourier transform of $f \cdot g$ is $|A|^{-1}\hat{f} * \hat{g}$.

The scaled Fourier transform is an R-module isomorphism from $R[A]$ to R^A with inverse given by

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

For $f, g \in R[A]$, the scaled Fourier transform of fg is $|A|\tilde{f}\tilde{g}$, and the scaled Fourier transform of $f \cdot g$ is $\tilde{f} * \tilde{g}$.

Proof. It is well-known that the Fourier transform is an isomorphism of R-algebras that takes convolution to pointwise multiplication. The facts about the scaled Fourier transform follow easily by keeping track of the scale factors. □

We also note that constant words have a very simple description via the scaled Fourier transform.

Lemma 2.7 (Constant Words). *The word $f \in R[A]$ is the constant word with $f(a) = r$ for all $a \in A$ if and only if $\tilde{f}(1_A) = r$ and $\tilde{f}(a) = 0$ for all $a \neq 1_A$.*

Proof. If $\tilde{f}(1_A) = r$ and $\tilde{f}(a) = 0$ for $a \neq 1_A$, then by the inversion formula $f_b = \sum_{a \in A} \tilde{f}(a)\langle a, b\rangle = r\langle 1_A, b\rangle = r$ for all $b \in B$. The scaled Fourier transform is a bijection, so the "only if" part follows immediately. □

2.3 Group Algebras over $\mathrm{GR}(p^d, e)$ and $\mathbb{Z}_p[\zeta_{q-1}]$

Now we introduce the rings and group algebras that are of special interest to us. Throughout this thesis, we let d and e denote positive integers, and we define $q = p^e$. We shall be concerned mostly with the group algebra $\mathrm{GR}(p^d, e)[A]$ and its ideals (codes). For many

counting calculations, it will be advantageous to perform computations in a ring of characteristic zero that resembles $\mathrm{GR}(p^d, e)$ as much as possible. For this reason, we employ the ring $\mathbb{Z}_p[\zeta_{q-1}]$, whose quotient modulo p^d is $\mathrm{GR}(p^d, e)$, and we also use the group algebra $\mathbb{Z}_p[\zeta_{q-1}][A]$, whose quotient modulo p^d is $\mathrm{GR}(p^d, e)[A]$. In this section, we shall describe the structure of $\mathrm{GR}(p^d, e)[A]$ and $\mathbb{Z}_p[\zeta_{q-1}][A]$ via the Fourier transform. Note that since $p \nmid |A|$, $|A|$ is a unit in $\mathrm{GR}(p^d, e)$ and $\mathbb{Z}_p[\zeta_{q-1}]$. However, these rings may not contain roots of unity of order equal to the exponent of A. Therefore, we extend our rings by adjoining roots of unity. We choose e' to be the least positive integer such that the exponent of A divides $q^{e'} - 1$, and let $q' = q^{e'} = p^{ee'}$. Then we consider the ring $\mathbb{Z}_p[\zeta_{q'-1}]$ and its quotient modulo p^d, which is $\mathrm{GR}(p^d, ee')$. These rings contain the roots of unity of order $q^{e'} - 1$, hence they have the roots of unity whose order is the exponent of A. Furthermore, since ee' is a multiple of e, we have $\mathbb{Z}_p[\zeta_{q-1}] \subseteq \mathbb{Z}_p[\zeta_{q'-1}]$ and $\mathrm{GR}(p^d, e) \subseteq \mathrm{GR}(p^d, ee')$. So we may consider $\mathrm{GR}(p^d, e)[A] \subseteq \mathrm{GR}(p^d, ee')[A]$ and $\mathbb{Z}_p[\zeta_{q-1}][A] \subseteq \mathbb{Z}_p[\zeta_{q'-1}][A]$, and carry out Fourier analysis within $\mathrm{GR}(p^d, ee')[A]$ and $\mathbb{Z}_p[\zeta_{q'-1}][A]$.

The Fourier transform was applied to cyclic codes over $\mathbb{F}_2$ by Mattson and Solomon [33] and, more generally, to Abelian codes over $\mathbb{F}_2$ by MacWilliams [31]. Working with an arbitrary finite field is no more difficult than working with $\mathbb{F}_2$, and the results generalize naturally when fields are replaced with integer residue rings [43] or Galois rings [3], [54]. We are presenting the Fourier transform in a manner close to that of Delsarte and McEliece [18] to facilitate comparison of our results with theirs. However, there are minor differences in notation, and we write our group A multiplicatively, while they write theirs additively.

For the rest of the thesis, we use π without a subscript for π_d, which is reduction modulo p^d. We shall use τ without a subscript for τ_∞, which is the Teichmüller lift to characteristic 0. In the definition of the pairing $\langle \cdot, \cdot \rangle$ given in the previous section, i.e.,

$$\left\langle a_1^{i_1} \dots a_k^{i_k}, a_1^{j_1} \dots a_k^{j_k} \right\rangle = \prod_{h=1}^{k} \theta_h^{i_h j_h}$$

we shall use $\theta_h = \zeta_{n_h}$ if our ring is $\mathbb{Z}_p[\zeta_{q'-1}]$, and we shall use $\theta_h = \pi(\zeta_{n_h})$ if our ring is $\mathrm{GR}(p^d, ee')$. With these choices, the Fourier transform commutes with reduction modulo p^d. To notate this fact, for $f = \sum_{a \in A} f_a a$ in $\mathbb{Z}_p[\zeta_{q'-1}][A]$, we let $\pi(f)$ denote the element

$\sum_{a\in A}\pi(f_a)a \in \mathrm{GR}(p^d, ee')[A]$, and for $g \in \mathbb{Z}_p[\zeta_{q'-1}]^A$, we let $\pi(g)$ denote the function $\pi \circ g \in \mathrm{GR}(p^d, ee')^A$. Then the diagrams

$$\begin{array}{ccc} \mathbb{Z}_p[\zeta_{q'-1}][A] & \xrightarrow{\mathrm{FT}} & \mathbb{Z}_p[\zeta_{q'-1}]^A \\ \pi\downarrow & & \pi\downarrow \\ \mathrm{GR}(p^d, ee')[A] & \xrightarrow{\mathrm{FT}} & \mathrm{GR}(p^d, ee')^A \end{array} \tag{2.1}$$

and

$$\begin{array}{ccc} \mathbb{Z}_p[\zeta_{q'-1}][A] & \xleftarrow{\mathrm{FT}^{-1}} & \mathbb{Z}_p[\zeta_{q'-1}]^A \\ \pi\downarrow & & \pi\downarrow \\ \mathrm{GR}(p^d, ee')[A] & \xleftarrow{\mathrm{FT}^{-1}} & \mathrm{GR}(p^d, ee')^A \end{array}$$

commute.

Although we introduced the algebras $\mathrm{GR}(p^d, ee')[A]$ and $\mathbb{Z}_p[\zeta_{q'-1}][A]$ to obtain a Fourier transform, our real interest is in the elements of the smaller algebras $\mathrm{GR}(p^d, e)[A]$ and $\mathbb{Z}_p[\zeta_{q-1}][A]$. Thus we would like to characterize $\mathrm{FT}(\mathrm{GR}(p^d, e)[A])$ and $\mathrm{FT}(\mathbb{Z}_p[\zeta_{q-1}][A])$ as subsets of $\mathrm{GR}(p^d, ee')^A$ and $\mathbb{Z}_p[\zeta_{q'-1}]^A$, respectively. We shall obtain several characterizations in Proposition 2.8 below, but first we need to make some definitions that will be used there and which are critical to the techniques used in Chapters 4 and 5.

Recall from Section 2.1 the canonical expansion of elements in $\mathrm{GR}(p^d, e)$ and $\mathbb{Z}_p[\zeta_{q-1}]$. If $f \in \mathrm{GR}(p^d, ee')[A]$, for each $a \in A$ we can write the canonical expansion $\tilde{f}(a) = \sum_{i=0}^{d-1}(\tilde{f}(a))^{(i)}p^i$, where $(\tilde{f}(a))^{(i)}$ is always 0 or a power of $\pi(\zeta_{q'-1})$. We define $f^{(i)} \in \mathrm{GR}(p^d, ee')[A]$ so that $\tilde{f}^{(i)}(a) = (\tilde{f}(a))^{(i)}$ for all $a \in A$. Thus we have $\tilde{f}^{(0)}, \ldots, \tilde{f}^{(d-1)} \colon A \to \{0, 1, \pi(\zeta_{q'-1}), \ldots, \pi(\zeta_{q'-1})^{q'-2}\}$ and $\tilde{f} = \sum_{i=0}^{d-1} p^i\tilde{f}^{(i)}$. Note that the uniqueness of canonical expansions ensures that $\tilde{f} = \tilde{g}$ if and only $\tilde{f}^{(i)} = \tilde{g}^{(i)}$ for all $i \in \{0, 1, \ldots, d-1\}$. Since $\tilde{f} = \sum_{i=0}^{d-1} p^i\tilde{f}^{(i)}$, by the inverse scaled Fourier transform, we have $f = \sum_{i=0}^{d-1} p^i f^{(i)}$. Furthermore, by the bijectivity of the scaled Fourier transform, $f = g$ if and only if $f^{(i)} = g^{(i)}$ for all $i \in \{0, 1, \ldots, d-1\}$.

Likewise, if $f \in \mathbb{Z}_p[\zeta_{q'-1}][A]$, for each $a \in A$ we can write the canonical expansion $\tilde{f}(a) = \sum_{i=0}^{\infty}(\tilde{f}(a))^{(i)}p^i$, where $(\tilde{f}(a))^{(i)}$ is always 0 or a power of $\zeta_{q'-1}$. As before, we define $f^{(i)} \in \mathbb{Z}_p[\zeta_{q'-1}][A]$ so that $\tilde{f}^{(i)}(a) = (\tilde{f}(a))^{(i)}$ for all $a \in A$. Thus we have each $\tilde{f}^{(i)} \colon A \to \{0, 1, \zeta_{q'-1}, \ldots, \zeta_{q'-1}^{q'-2}\}$ and $\tilde{f} = \sum_{i=0}^{\infty} p^i\tilde{f}^{(i)}$. Now uniqueness of canonical expansions ensures

that $\tilde{f} = \tilde{g}$ if and only $\tilde{f}^{(i)} = \tilde{g}^{(i)}$ for all $i \in \mathbb{N}$. Since $\tilde{f} = \sum_{i=0}^{\infty} p^i \tilde{f}^{(i)}$, the inverse scaled Fourier transform gives us $f = \sum_{i=0}^{\infty} p^i f^{(i)}$. The bijectivity of the scaled Fourier transform tells us that $f = g$ if and only if $f^{(i)} = g^{(i)}$ for all $i \in \mathbb{N}$.

Now we give names to the functions we have defined in the previous two paragraphs. Whether $f \in \mathrm{GR}(p^d, ee')[A]$ or $\mathbb{Z}_p[\zeta_{q'-1}][A]$, we call the sum $\tilde{f} = \sum_i p^i \tilde{f}^{(i)}$ the *canonical expansion of* $\tilde{f}$, and we call $\tilde{f}^{(i)}$ the *ith component of the canonical expansion of* $\tilde{f}$. Whether $f \in \mathrm{GR}(p^d, ee')[A]$ or $\mathbb{Z}_p[\zeta_{q'-1}][A]$, we call the sum $f = \sum_i p^i f^{(i)}$ the *scaled Fourier-induced breakdown of* f, and we call $f^{(i)}$ the *ith component of the scaled Fourier-induced breakdown of* f. Note that if $f \in \mathrm{GR}(p^d, e)[A]$ and if we set $F \in \mathbb{Z}_p[\zeta_{q'-1}][A]$ to have $\tilde{F} = \tau \circ \tilde{f}$, then $\tilde{F}^{(i)} = \tau \circ \tilde{f}^{(i)}$ and $\tilde{f}^{(i)} = \pi \circ \tilde{F}^{(i)}$ for all $i \in \{0, 1, \ldots, d-1\}$. Of course $\tilde{F}^{(i)}(a) = 0$ for all $a \in A$ when $i \geq d$.

Now we are ready to characterize the image under FT of $\mathrm{GR}(p^d, e)[A]$ in $\mathrm{GR}(p^d, ee')[A]$ and the image under FT of $\mathbb{Z}_p[\zeta_{q-1}][A]$ in $\mathbb{Z}_p[\zeta_{q'-1}][A]$.

Proposition 2.8. *For $f \in \mathrm{GR}(p^d, ee')[A]$, the following are equivalent:*

(i) $f \in \mathrm{GR}(p^d, e)[A]$.

(ii) $\hat{f}(a^q) = \mathrm{Fr}^e(\hat{f}(a))$ *for all* $a \in A$.

(iii) $\tilde{f}(a^q) = \mathrm{Fr}^e(\tilde{f}(a))$ *for all* $a \in A$.

(iv) $\tilde{f}^{(i)}(a^q) = \left(\tilde{f}^{(i)}(a)\right)^q$ *for all* $i \in \{0, 1, \ldots, d-1\}$ *and* $a \in A$.

(v) $f^{(i)} \in \mathrm{GR}(p^d, e)[A]$ *for all* $i \in \{0, 1, \ldots, d-1\}$.

Thus FT *is an isomorphism of* $\mathrm{GR}(p^d, e)$*-algebras from* $\mathrm{GR}(p^d, e)[A]$ *to the set of elements* $g \in \mathrm{GR}(p^d, ee')^A$ *that satisfy* $g(a^q) = \mathrm{Fr}^e(g(a))$.

For $f \in \mathbb{Z}_p[\zeta_{q'-1}][A]$, the following are equivalent:

(i) $f \in \mathbb{Z}_p[\zeta_{q-1}][A]$.

(ii) $\hat{f}(a^q) = \mathrm{Fr}^e(\hat{f}(a))$ *for all* $a \in A$.

(iii) $\tilde{f}(a^q) = \mathrm{Fr}^e(\tilde{f}(a))$ *for all* $a \in A$.

(iv) $\tilde{f}^{(i)}(a^q) = \left(\tilde{f}^{(i)}(a)\right)^q$ *for all* $i \in \mathbb{N}$ *and* $a \in A$.

(v) $f^{(i)} \in \mathbb{Z}_p[\zeta_{q-1}][A]$ *for all* $i \in \mathbb{N}$.

Thus FT *is an isomorphism of* $\mathbb{Z}_p[\zeta_{q-1}]$*-algebras from* $\mathbb{Z}_p[\zeta_{q-1}][A]$ *to the set of elements* $g \in \mathbb{Z}_p[\zeta_{q'-1}]^A$ *that satisfy* $g(a^q) = \mathrm{Fr}^e(g(a))$.

Proof. To prove the first set of equivalences, let $R = \mathrm{GR}(p^d, e)$, $R' = \mathrm{GR}(p^d, ee')$, and $I = \{0, 1, \ldots, d-1\}$. To prove the second set of equivalences, let $R = \mathbb{Z}_p[\zeta_{q-1}]$, $R' = \mathbb{Z}_p[\zeta_{q'-1}]$, and $I = \mathbb{N}$. Then the rest of this proof works in either case.

Since $\mathrm{Fr}(|A|) = |A|$, it is clear that (ii) and (iii) are equivalent. Note that Fr^e fixes 0 and p and takes $\zeta_{q'-1}$ and $\pi(\zeta_{q'-1})$ to their qth powers. So $\mathrm{Fr}^e(\tilde{f}(a)) = \mathrm{Fr}^e\left(\sum_{i\in I} \tilde{f}^{(i)}(a)p^i\right) = \sum_{i\in I}\left(\tilde{f}^{(i)}(a)\right)^q p^i$. This, along with uniqueness of canonical expansions, shows that (iii) and (iv) are equivalent.

Now we show that (i) and (iii) are equivalent. Note that $\langle a, b\rangle$ is a power of $\pi(\zeta_{q'-1})$ or $\zeta_{q'-1}$ for all $a, b \in A$. Note also that Fr^e takes such elements to their qth powers. In particular, Fr^e fixes an element $r \in R'$ if and only if $r \in R$. Since $p \nmid |A|$, a^q runs through A as a runs through A. Thus

$$\begin{aligned} f_a &= \sum_{b\in A} \tilde{f}(b)\langle b, a\rangle \\ &= \sum_{b\in A} \tilde{f}(b^q)\langle b^q, a\rangle \\ &= \sum_{b\in A} \tilde{f}(b^q)\langle b, a\rangle^q, \end{aligned}$$

so that

$$\mathrm{Fr}^{-e}(f_a) = \sum_{b\in A} \mathrm{Fr}^{-e}(\tilde{f}(b^q))\langle b, a\rangle. \tag{2.2}$$

If $f \in R[A]$, then $\mathrm{Fr}^e(f_a) = f_a$ for all $a \in A$, so that (2.2) becomes

$$f_a = \sum_{b\in A} \mathrm{Fr}^{-e}(\tilde{f}(b^q))\langle b, a\rangle.$$

Then the bijectivity of the scaled Fourier transform tells us that $\tilde{f}(b) = \mathrm{Fr}^{-e}(\tilde{f}(b^q))$ for all

$b \in A$. Conversely, if $\tilde{f}(a^q) = \mathrm{Fr}^e(\tilde{f}(a))$ for all $a \in A$, then (2.2) becomes

$$\mathrm{Fr}^{-e}(f_a) = \sum_{b \in A} \tilde{f}(b)\langle b, a\rangle,$$

i.e., $\mathrm{Fr}^{-e}(f_a) = f_a$ for all $a \in A$. This is equivalent to $f_a \in R$ for all $a \in A$.

Finally, since $f = \sum_{i \in I} p^i f^{(i)}$, it is clear that (v) implies (i). On the other hand, if we assume (iv), then for each $i \in I$ and $a \in A$, we have $\tilde{f}^{(i)}(a^q) = \left(\tilde{f}^{(i)}(a)\right)^q = \mathrm{Fr}^e(\tilde{f}^{(i)}(a))$. Since we have already proved the equivalence of (i) and (iii), we may apply it to see that $f^{(i)} \in R[A]$ for all $i \in I$, i.e., that (v) holds. □

We also investigate how the Fourier transform interacts with Teichmüller lifting. For $f = \sum_{a \in A} f_a a$ in $\mathrm{GR}(p^d, ee')[A]$, we let $\tau(f)$ denote the element $\sum_{a \in A} \tau(f_a)a \in \mathbb{Z}_p[\zeta_{q'-1}][A]$, and for $g \in \mathrm{GR}(p^d, ee')^A$, we let $\tau(g)$ denote the function $\tau \circ g \in \mathbb{Z}_p[\zeta_{q'-1}]^A$.

Lemma 2.9. *Let $f \in \mathrm{GR}(p^d, e)[A]$ and let F be the unique element in $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{F} = \tau \circ \tilde{f}$. Then $F \in \mathbb{Z}_p[\zeta_{q-1}][A]$ and $\pi(F) = f$. For each $i \in \mathbb{N}$, we have $F^{(i)} \in \mathbb{Z}_p[\zeta_{q-1}][A]$, and $\pi(F^{(i)}) = f^{(i)}$ for $i \in \{0, 1, \ldots, d-1\}$, while $F^{(i)} = 0$ for $i \geq d$.*

Proof. By Proposition 2.8, we have $\tilde{f}(a^q) = \mathrm{Fr}^e(\tilde{f}(a))$ for all $a \in A$. Applying τ to both sides, and recalling that τ commutes with Fr, we have $\tau(\tilde{f}(a^q)) = \mathrm{Fr}^e(\tau(\tilde{f}(a)))$ for all $a \in A$, i.e., $\tilde{F}(a^q) = \mathrm{Fr}^e(\tilde{F}(a))$ for all $a \in A$. Then Proposition 2.8 tells us that $F \in \mathbb{Z}_p[\zeta_{q-1}][A]$.

Since $\tilde{F} = \tau(\tilde{f})$, we have $\mathrm{FT}(|A|^{-1}F) = \tau(\tilde{f})$. Apply π to both sides of this equation, commute π with FT by diagram (2.1), and recognize that $\pi \circ \tau$ is the identity to obtain $\mathrm{FT}(\pi(|A|^{-1}F)) = \tilde{f}$. Thus $\pi(|A|^{-1})\,\mathrm{FT}(\pi(F)) = \tilde{f}$. Since the scaled Fourier transform is a bijection, we have $\pi(F) = f$.

Since $f \in \mathrm{GR}(p^d, e)[A]$ and $F \in \mathbb{Z}_p[\zeta_{q-1}][A]$, we have $f^{(i)} \in \mathrm{GR}(p^d, e)[A]$ for all $i \in \{0, 1, \ldots, d-1\}$ and $F^{(i)} \in \mathbb{Z}_p[\zeta_{q-1}][A]$ for all $i \in \mathbb{N}$ by Proposition 2.8. Furthermore, we have already noted (before Proposition 2.8) that $\tilde{F}^{(i)} = 0$ for $i \geq d$; this is a simple consequence of the definition of the Teichmüller lift. Thus $F^{(i)} = 0$ for $i \geq d$. Just before this, we noted that $\tilde{F}^{(i)} = \tau \circ \tilde{f}^{(i)}$ for all $i \in \{0, 1, \ldots, d-1\}$. Thus, by the first part of the theorem, applied with $f^{(i)}$ in place of f, we have $\pi(F^{(i)}) = f^{(i)}$. □

Proposition 2.8 above tells us that if $f \in \mathrm{GR}(p^d, e)[A]$ or $\mathbb{Z}_p[\zeta_{q-1}][A]$, then $\hat{f}(a)$, $\hat{f}(a^q)$, $\hat{f}(a^{q^2})$, ... are all determined by the value of $\hat{f}(a)$. We say that two elements $a, b \in A$ are *q-equivalent* if $a = b^{q^i}$ for some $i \in \mathbb{Z}$, where powers of q here are construed as integers modulo $|A|$. This defines an equivalence relation on A, called *q-equivalence*, which partitions A into *q-classes*. We denote the q-class of $a \in A$ by $\mathrm{Cl}_q(a)$ and denote $|\mathrm{Cl}_q(a)|$ by e_a, so that $\mathrm{Cl}_q(a) = \{a, a^q, \ldots, a^{q^{e_a-1}}\}$ and $a^{q^k} = a$ if and only if $k \mid e_a$. This leads to the following simple but important observation:

Lemma 2.10 (Sizes of q-Classes). *For each $a \in A$, $e_a \mid e'$.*

Proof. We chose e' so that the exponent of A divides $q^{e'} - 1$. Thus $a^{q^{e'}} = a$, and so $e_a \mid e'$. □

A subset of A is said to be *q-closed* if it is a union of q-classes. With our q-equivalence terminology, Proposition 2.8 says that if $f \in \mathrm{GR}(p^d, e)[A]$ or $\mathbb{Z}_p[\zeta_{q-1}][A]$, then $\hat{f}$ (or $\tilde{f}$) is uniquely determined by its values on a set of q-class representatives. We make this notion more precise in the following proposition:

Proposition 2.11. *Fix R a set of q-class representatives for A. Then the restriction of domains to R is an $\mathrm{GR}(p^d, e)$-algebra isomorphism from $\mathrm{FT}(\mathrm{GR}(p^d, e)[A])$ to $U = \prod_{r \in R} \mathrm{GR}(p^d, ee_r)$. Thus the Fourier transform followed by restriction of domains to R is a $\mathrm{GR}(p^d, e)$-algebra isomorphism from $\mathrm{GR}(p^d, e)[A]$ to U, and so induces a one-to-one correspondence between the ideals (codes) in $\mathrm{GR}(p^d, e)[A]$ and the ideals in U. The latter ideals can all be written uniquely as $\prod_{r \in R} p^{i_r} \mathrm{GR}(p^d, ee_r)$ where each $i_r \in \{0, 1, \ldots, d\}$. Thus $\mathrm{GR}(p^d, e)[A]$ has $(d+1)^{|R|}$ ideals, and every ideal of $\mathrm{GR}(p^d, e)[A]$ is principal. The ideals in U that are free $\mathrm{GR}(p^d, e)$-modules are those with all $i_r \in \{0, d\}$.*

Proof. First we prove that restriction of domains to R maps $\mathrm{FT}(\mathrm{GR}(p^d, e)[A])$ into U, i.e., we shall show that for each $f \in \mathrm{GR}(p^d, e)[A]$ and each $r \in R$, $\hat{f}(r) \in \mathrm{GR}(p^d, ee_r)$. Of course $\hat{f}(r)$ is in $\mathrm{GR}(p^d, ee')$. By Proposition 2.8, we know that $\hat{f}(r^{q^{e_r}}) = \mathrm{Fr}^{ee_r}(\hat{f}(r))$. But $r^{q^{e_r}} = r$, so that $\hat{f}(r)$ is fixed by Fr^{ee_r}. Thus $\hat{f}(r)$ is in $\mathrm{GR}(p^d, ee_r)$.

We also know that restriction of domains to R is injective on $\mathrm{FT}(\mathrm{GR}(p^d, e)[A])$ since the Fourier transform of a function $f \in \mathrm{GR}(p^d, e)[A]$ is uniquely determined by its val-

ues on a set of q-class representatives by Proposition 2.8. Furthermore, note that $|U| = \prod_{r\in R}\left|\mathrm{GR}(p^d, ee_r)\right| = \prod_{r\in R} p^{dee_r} = p^{de\sum_{r\in R} e_r} = p^{de|A|} = \left|\mathrm{GR}(p^d, e)\right|^{|A|}$, so that $|U| = \left|\mathrm{GR}(p^d, e)[A]\right| = \left|\mathrm{FT}\left(\mathrm{GR}(p^d, e)[A]\right)\right|$. Thus restriction of domains is also surjective. Clearly restriction of domains preserves $\mathrm{GR}(p^d, e)$-scalar multiplication and pointwise addition and multiplication. So it is a $\mathrm{GR}(p^d, e)$-algebra isomorphism from $\mathrm{FT}(\mathrm{GR}(p^d, e)[A])$ to U. The statements about correspondence of ideals, the form of ideals, and the number of ideals are clear. In a free $\mathrm{GR}(p^d, e)$-module, for each element u that is annihilated by p^{d-1}, there is some element v with $u = pv$. This will clearly be violated in the ideal $\prod_{r\in R} p^{i_r}\,\mathrm{GR}(p^d, ee_r)$ of U if we have any $i_r \notin \{0, d\}$. But if $i_r \in \{0, d\}$ for all $r \in R$, then our ideal is a product of extensions of $\mathrm{GR}(p^d, e)$, each of which is a free $\mathrm{GR}(p^d, e)$-module. This proves the statement about which ideals are free $\mathrm{GR}(p^d, e)$-modules. □

Suppose that f is a function from A into a Galois ring or an unramified extension of the p-adic field, and suppose that $\mathcal{G}$ is a set of such functions. For example, f might be the Fourier transform of an element of $\mathrm{GR}(p^d, e)[A]$ or $\mathbb{Z}_p[\zeta_{q-1}][A]$, and $\mathcal{G}$ might be the set of Fourier transforms of words in an Abelian code. A *support* of f is a subset S of A such that $f(a) = 0$ for all $a \notin S$. For $k \in \mathbb{N}$, a *support modulo* p^k of f is a subset S of A such that $f(a) \equiv 0 \pmod{p^k}$ for all $a \notin S$. We also call a support modulo p^k a *p^k-support*. A *support* (resp., *support modulo* p^k) of $\mathcal{G}$ is a subset S of A that is a support (resp., support modulo p^k) of each $g \in \mathcal{G}$. A support (resp., support modulo p^k) S of a function or set of functions is said to be *minimal* if there is no support (resp., support modulo p^k) properly contained in S. For example if f is a function, then its minimal support is $\{a \in A : f(a) \neq 0\}$ and its minimal p^k-support is $\{a \in A : f(a) \not\equiv 0 \pmod{p^k}\}$. If we use the definite article with the word "support", i.e., if we say "the support" or "the p^k-support" in any circumstance, we mean the minimal one.

Now suppose that the range of f is $\mathrm{GR}(p^d, ee')$. For example, f might be the Fourier transform of some element of $\mathrm{GR}(p^d, e)[A]$. For each $k \in \{0, 1, \ldots, d-1\}$, define S_k to be the minimal p^{k+1}-support of f. Then $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$ is called the *tower of supports of* f. Each S_k is the same as the support of $p^{d-k-1}f$, so that S_{d-1} is the support of f. Indeed, $S_k = \{a \in A : v_p\left(f(a)\right) \leq k\}$.

Similarly, suppose that $\mathrm{GR}(p^d, ee')$ is the range of the functions in $\mathcal{G}$. For example, $\mathcal{G}$ might be the Fourier transform of some code in $\mathrm{GR}(p^d, e)[A]$. For each $k \in \{0, 1, \ldots, d-1\}$, define S_k to be the minimal p^{k+1}-support of $\mathcal{G}$ and then define the *tower of supports of* $\mathcal{G}$ to be $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$. Each S_k is the same as the support of $\{p^{d-1-k}g : g \in \mathcal{G}\}$, so that S_{d-1} is the support of $\mathcal{G}$. Indeed S_k is the set of $a \in A$ such that there exists a $g \in \mathcal{G}$ with $v_p(g(a)) \leq k$.

Note that the Frobenius automorphism preserves the p-adic valuations of elements in $\mathrm{GR}(p^d, ee')$. Therefore, Proposition 2.8 shows us that if $f \in \mathrm{GR}(p^d, e)[A]$, then $v_p(\hat{f}(a))$ is constant as a varies over a q-class. Thus, the sets in the tower of supports of $\hat{f}$ are q-closed. Similarly, if $\mathcal{G}$ is the Fourier transform of a set of elements of $\mathrm{GR}(p^d, e)[A]$, then the sets in the tower of supports of $\mathcal{G}$ are q-closed. With this insight, we may rephrase the essential content of Proposition 2.11 as follows:

Proposition 2.12. *For each ideal (code)* $\mathcal{C}$ *in the group algebra* $\mathrm{GR}(p^d, e)[A]$*, let* $T(\mathcal{C})$ *be the tower of supports of* $\mathrm{FT}(\mathcal{C})$*. Then* T *is a bijection between the set of ideals in* $\mathrm{GR}(p^d, e)[A]$ *and the set of towers of height* d *consisting of* q*-closed subsets of* A*.*

Proof. First of all, T maps the ideals in $\mathrm{GR}(p^d, e)[A]$ to towers of q-closed sets by the comments preceding this proposition. Suppose we are given a tower of $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$ of q-closed subsets. For convenience, define $S_{-1} = \emptyset$ and $S_d = A$. Then define h to be the function from A to $\mathrm{GR}(p^d, ee')$ such that $h(a) = p^j$ for all $j \in \{0, 1, \ldots, d\}$ and $a \in S_j \setminus S_{j-1}$. Then h is the Fourier transform of some $g \in \mathrm{GR}(p^d, e)[A]$ by Proposition 2.8. If we set $\mathcal{C}$ to be the ideal generated by g, then $\mathrm{FT}(\mathcal{C})$ is generated by h, and it is easy to see that $T(\mathcal{C}) = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$. So T is surjective.

To see that T is bijective, we show that the number of ideals in $\mathrm{GR}(p^d, e)[A]$ equals the number of towers of height d consisting of q-closed subsets of A. Proposition 2.11 tells us that the latter number is $(d+1)^n$, where n is the number of q-classes of A. To calculate the number of towers, note that

$$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1} \mapsto S_0, S_1 \setminus S_0, \ldots, S_{d-1} \setminus S_{d-2}, A \setminus S_{d-1}$$

establishes a bijective correspondence from the set of towers of height d consisting of q-closed subsets of A to the set of $(d+1)$-tuples of pairwise disjoint q-closed subsets of A that cover A. The number of these latter objects is $(d+1)^n$. □

We finish this section with two more technical lemmas on how the scaled Fourier coefficients parameterize an Abelian code over a Galois ring.

Lemma 2.13. *Let $\mathcal{C}$ be an ideal (code) in $\mathrm{GR}(p^d, e)[A]$ with tower of supports $S_0 \subseteq \cdots \subseteq S_{d-1}$, and set $S_{-1} = \emptyset$. Let R be a set of q-class representatives of A, and set $R_i = R \cap S_i$ for each $i \in \{-1, 0, 1, \ldots, d-1\}$. Then each word $c \in \mathcal{C}$ is uniquely determined by the values of $\{\tilde{c}(r) : r \in R_{d-1}\}$. These values are in $\prod_{i=0}^{d-1} \prod_{r \in R_i \setminus R_{i-1}} p^i \,\mathrm{GR}(p^d, ee_r)$, and as they run through this product of ideals, the word c runs through $\mathcal{C}$. Furthermore, $|\mathcal{C}| = q^{\sum_{i=0}^{d-1} |S_i|}$. $\mathcal{C}$ is a free $\mathrm{GR}(p^d, e)$-module if and only if $S_0 = S_1 = \cdots = S_{d-1}$.*

Proof. By Proposition 2.11, c is uniquely determined by the values in $\{\hat{c}(r) : r \in R\}$, hence c is uniquely determined by the values in $\{\tilde{c}(r) : r \in R\}$. If $r \notin R_{d-1}$, then the q-class of r is not in the q-closed set S_{d-1}, so that $\tilde{c}(r) \equiv 0 \pmod{p^d}$, i.e., $\tilde{c}(r) = 0$, for all $c \in \mathcal{C}$. So c is uniquely determined by the values in $\{\tilde{c}(r) : r \in R_{d-1}\}$.

Furthermore, we know that as c runs through $\mathcal{C}$, the values $\{\tilde{c}(r) : r \in R_{d-1}\}$ run through some ideal of the ring $\prod_{r \in R_{d-1}} \mathrm{GR}(p^d, ee_r)$. If $i \in \{0, 1, \ldots, d-1\}$ and $r \in R_i \setminus R_{i-1}$, then $\tilde{c}(r) \equiv 0 \pmod{p^i}$ for all $c \in \mathcal{C}$, but $\tilde{c}(r) \not\equiv 0 \pmod{p^{i+1}}$ for some $c \in \mathcal{C}$. So $\tilde{c}(r)$ must run through the ideal $p^i \,\mathrm{GR}(p^d, ee_r)$. Thus

$$\begin{aligned}
|\mathcal{C}| &= \prod_{i=0}^{d-1} \prod_{r \in R_i \setminus R_{i-1}} \left| p^i \,\mathrm{GR}(p^d, ee_r) \right| \\
&= \prod_{i=0}^{d-1} \prod_{r \in R_i \setminus R_{i-1}} p^{(d-i)ee_r} \\
&= p^{e \sum_{i=0}^{d-1} (d-i) \sum_{r \in R_i \setminus R_{i-1}} e_r} \\
&= p^{e \sum_{i=0}^{d-1} (d-i) |S_i \setminus S_{i-1}|} \\
&= p^{e \sum_{i=0}^{d-1} |S_i|} \\
&= q^{\sum_{i=0}^{d-1} |S_i|}.
\end{aligned}$$

Again, if $i \in \{0, 1, \ldots, d-1\}$ and $r \in R_i \setminus R_{i-1}$, then $\tilde{c}(r)$ runs through the ideal $p^i \operatorname{GR}(p^d, ee_r)$. So, by the characterization of which ideals in $\prod_{r \in R} \operatorname{GR}(p^d, ee_r)$ are free $\operatorname{GR}(p^d, e)$-modules in Proposition 2.11, our ideal $\mathcal{C}$ is a free $\operatorname{GR}(p^d, e)$-module if and only if $R_i \setminus R_{i-1} = \emptyset$ for $i = 1, \ldots, d-1$. This is equivalent to saying that $R_0 = R_1 = \cdots = R_{d-1}$. But each R_i is a set of q-class representatives of the q-closed set S_i, so this last condition is equivalent to $S_0 = \cdots = S_{d-1}$. □

Lemma 2.14. *Let $\mathcal{C}$ be an ideal (code) in $\operatorname{GR}(p^d, e)[A]$ with tower of supports $S_0 \subseteq \cdots \subseteq S_{d-1}$. Let R be a set of q-class representatives of A and let $R_i = S_i \cap R$ for $i = 0, 1, \ldots, d-1$. For each $c \in \mathcal{C}$, let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \pi \circ \tilde{c}$. Then $\tilde{c}^{(i)}$ and $\tilde{C}^{(i)}$ are supported on S_i for each $c \in \mathcal{C}$. Also, c is uniquely determined by the values of $\{\tilde{c}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$. As the word c runs through $\mathcal{C}$, these values run through $\prod_{i=0}^{d-1} \prod_{r \in R_i} U_{i,r}$, where $U_{i,r}$ is the set containing 0 and all powers of $\pi(\zeta_{q^{e_r}-1})$. Equivalently, c is uniquely determined by the values of $\{\tilde{C}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$. As the word c runs through $\mathcal{C}$, these values run through $\prod_{i=0}^{d-1} \prod_{r \in R_i} V_{i,r}$, where $V_{i,r}$ is the set containing 0 and all powers of $\zeta_{q^{e_r}-1}$.*

Proof. Suppose $\tilde{c}^{(i)}(a) \neq 0$. Then $\tilde{c}(a) = \sum_{i=0}^{d-1} \tilde{c}^{(i)}(a) p^i$ is not divisible by p^{i+1}. So $a \in S_i$ by the definition of the tower of supports. So $\tilde{c}^{(i)}$ is supported on S_i. Since $\tilde{C}^{(i)} = \tau \circ \tilde{c}^{(i)}$ and $\tau(0) = 0$, $\tilde{C}^{(i)}$ is also supported on S_i.

The word $c \in \mathcal{C}$ is uniquely determined by $\{\tilde{c}(r) : r \in R_{d-1}\}$ by Lemma 2.13. Now $\tilde{c} = \sum_{i=0}^{d-1} p^i \tilde{c}^{(i)}$, so c is uniquely determined by $\{\tilde{c}^{(i)}(r) : 0 \leq i < d, r \in R_{d-1}\}$. But we have seen that $\tilde{c}^{(i)}$ is supported on S_i, so $\tilde{c}^{(i)}(r) = 0$ if $r \in R \setminus S_i = R \setminus R_i$. So c is uniquely determined by $\{\tilde{c}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$. For each $r \in R$, we know that $\tilde{c}(r) \in \operatorname{GR}(p^d, ee_r)$ by Proposition 2.11. So $\tilde{c}^{(i)}(r)$ is zero or a power of $\pi(\zeta_{q^{e_r}-1})$ for all $r \in R$ and $i \in \{0, 1, \ldots, d-1\}$, i.e., $\tilde{c}^{(i)}(r) \in U_{i,r}$. So the collection of $\{\tilde{c}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$ runs through some subset of $\prod_{i=0}^{d-1} \prod_{r \in R_i} U_{i,r}$ as c runs through $\mathcal{C}$. Note that the cardinality of this product is $\prod_{i=0}^{d-1} \prod_{r \in R_i} q^{e_r} = q^{\sum_{i=0}^{d-1} \sum_{r \in R_i} e_r} = q^{\sum_{i=0}^{d-1} |S_i|}$, which is the cardinality of $\mathcal{C}$ by Lemma 2.13. Therefore the values of $\{\tilde{c}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$ run through all of $\prod_{i=0}^{d-1} \prod_{r \in R_i} U_{i,r}$, and each distinct assignment of values corresponds to a different element of $\mathcal{C}$.

Since $\tilde{C}^{(i)} = \tau(\tilde{c}^{(i)})$ and $\tilde{c}^{(i)} = \pi(\tilde{C}^{(i)})$ for each $i \in \{0, 1, \ldots, d-1\}$, we see that the elements$\{\tilde{C}^{(i)}(r) : 0 \leq i < d, r \in R_i\}$ also uniquely determine c, and we see that these values run through $\prod_{i=0}^{d-1} \prod_{r \in R_i} V_{i,r}$ as c runs through $\mathcal{C}$. □

2.4 Weight Functions

We consider elements of $\mathrm{GR}(p^d, e)[A]$ as words by regarding elements of $\mathrm{GR}(p^d, e)$ as symbols and by fixing some ordering of the group A. Thus if we order the elements of A as $a_1, \ldots, a_n$, we consider $c \in \mathrm{GR}(p^d, e)[A]$ to be the word $c_{a_1} c_{a_2} \ldots c_{a_n}$. In this scheme, the *symbol at position* a in the word $c \in A$ is simply c_a.

There are many ways of reckoning weights of words in Abelian codes. For t a positive integer, we define a *t-wise weight function* to be a function from $\mathrm{wt}\colon \mathrm{GR}(p^d, e)^t \to \mathbb{Z}$. Often we omit reference to t and just call wt a *weight function*. If $r_1, \ldots, r_t \in \mathrm{GR}(p^d, e)$, then we call $\mathrm{wt}(r_1, \ldots, r_t)$ the *weight of* $(r_1, \ldots, r_t)$.

If we are given a t-wise weight function $\mathrm{wt}\colon \mathrm{GR}(p^d, e)^t \to \mathbb{Z}$, and a collection of words $c_1, \ldots, c_t \in \mathrm{GR}(p^d, e)[A]$, we define the *weight of* $(c_1, \ldots, c_t)$ to be

$$\sum_{a \in A} \mathrm{wt}(c_1(a), \ldots, c_t(a)).$$

Indeed, we make the convention that the domain of wt is automatically extended to include $\mathrm{GR}(p^d, e)[A]^t$, and we set $\mathrm{wt}(c_1, \ldots, c_t)$ to be the weight of $(c_1, \ldots, c_t)$ for each $(c_1, \ldots, c_t) \in \mathrm{GR}(p^d, e)[A]^t$.

For a given t-wise weight function $\mathrm{wt}\colon \mathrm{GR}(p^d, e)^t \to \mathbb{Z}$, we also introduce the corresponding *normalized weight function*, $\mathrm{wt}^{\mathrm{norm}}\colon \mathrm{GR}(p^d, e)[A]^t \to \mathbb{Z}$, which is defined as

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \ldots, c_t) = \mathrm{wt}(c_1, \ldots, c_t) - |A| \, \mathrm{wt}(\tilde{c}_1(1_A), \ldots, \tilde{c}_t(1_A))$$

for each $(c_1, \ldots, c_t) \in \mathrm{GR}(p^d, e)[A]^t$. Note that the normalized weight function is used only for words, not single symbols. The normalized weight function is a device for simplifying the presentation and proof of our results when our codes are allowed to have 1_A in the supports of their Fourier transforms.

We introduce some of the basic weight functions that will be of interest to us. The *t-wise zero count function* is the weight function $\mathrm{zer}\colon \mathrm{GR}(p^d, e)^t \to \mathbb{Z}$ that has the values

$$\mathrm{zer}(r_1, \ldots, r_t) = \begin{cases} 1 & \text{if } r_1 = \cdots = r_t = 0, \\ 0 & \text{otherwise.} \end{cases}$$

The 1-wise zero count function is simply known as the *zero count function*, and if $c \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{zer}(c)$ is called the *zero count of* c. This is just the number of instances of the zero symbol in the word. For arbitrary t, a t-wise zero count function is called a *simultaneous zero count function*, and if $c_1, \ldots, c_t \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{zer}(c_1, \ldots, c_t)$ is called the *simultaneous zero count of* $c_1, \ldots, c_t$. This is just the number of positions where the words all simultaneously have the zero symbol.

Closely related to the zero count is the *Hamming weight function* $\mathrm{ham}\colon \mathrm{GR}(p^d, e) \to \mathbb{Z}$, which has values

$$\mathrm{ham}(r) = \begin{cases} 0 & \text{if } r = 0, \\ 1 & \text{otherwise.} \end{cases}$$

If $c \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{ham}(c)$ is called the *Hamming weight of* c. This is just the number of nonzero symbols in the word. Note that $\mathrm{ham}(r) = 1 - \mathrm{zer}(r)$ for $r \in \mathrm{GR}(p^d, e)$, and that $\mathrm{ham}(c) = |A| - \mathrm{zer}(c)$ for $c \in \mathrm{GR}(p^d, e)[A]$. Thus

$$\begin{aligned} \mathrm{ham}^{\mathrm{norm}}(c) &= \mathrm{ham}(c) - |A| \,\mathrm{ham}(\tilde{c}(1_A)) \\ &= |A| - \mathrm{zer}(c) - |A| \,[1 - \mathrm{zer}(\tilde{c}(1_A))] \\ &= -\mathrm{zer}(c) + |A| \,\mathrm{zer}(\tilde{c}(1_A)) \\ &= -\mathrm{zer}^{\mathrm{norm}}(c). \end{aligned}$$

For each $r \in \mathrm{GR}(p^d, e)$, there is the weight function $\mathrm{symb}_r\colon \mathrm{GR}(p^d, e) \to \mathbb{Z}$, called the

r-count function, which is given by

$$\mathrm{symb}_r(s) = \begin{cases} 1 & \text{if } s = r, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the (1-wise) zero count function zer is the same as symb_0. If $c \in \mathrm{GR}(p^d, e)[A]$, then $\mathrm{symb}_r(c)$ is called the *r-count of c*. This is the number of instances of the symbol r in the word c.

If $e = 1$, there is the Lee weight function $\mathrm{lee}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$, given by

$$\mathrm{lee}(r) = \min\{|k| : k \in \mathbb{Z}, \pi(k) = r\}$$

for all $r \in \mathbb{Z}/p^d\mathbb{Z}$. That is, $\mathrm{lee}(\pi(k)) = k$ for $k = 0, 1, \ldots, \lfloor p^d/2 \rfloor$ and $\mathrm{lee}(\pi(k)) = p^d - k$ for $k = \lceil p^d/2 \rceil, \ldots, p^d - 1$.

2.5 Accounts and Compact Notations

In this section, we introduce a class of objects known as *accounts*, which will simplify the expression and proof of our results. If Y is a set, we define an *account on* Y to be a function from Y into $\mathbb{Z}$. If μ is an account on Y and $y \in Y$, we use the notation μ_y for the value of μ at y. We say μ *has* k *instances of* y to mean $\mu_y = k$. The set of accounts on Y, when equipped with addition, forms an Abelian group that we denote by $\mathbb{Z}[Y]$, and we sometimes write and manipulate an account μ as if it were the formal sum $\sum_{y \in Y} \mu_y y$. The multisets with elements from Y are regarded in a natural way as the accounts on Y that take only nonnegative values. The subsets of Y are regarded as the accounts on Y that take only values 0 and 1. The set of multisets with elements from Y is denoted $\mathbb{N}[Y]$.

Suppose that $Y_1 \subseteq Y_2$. Then we regard $\mathbb{Z}[Y_1]$ as a subset of $\mathbb{Z}[Y_2]$ by regarding each $\mu\colon Y_1 \to \mathbb{Z}$ as the function from Y_2 to $\mathbb{Z}$ that vanishes on $Y_2 \setminus Y_1$ and extends the original function μ. In this way, we also have $\mathbb{N}[Y_1] \subseteq \mathbb{N}[Y_2]$. Conversely, if $\mu \in \mathbb{Z}[Y_2]$ is supported on Y_1, then we can regard μ as an element of $\mathbb{Z}[Y_1]$ via restriction of domain. Indeed, we often indicate that $\mu \in \mathbb{Z}[Y_2]$ is supported on Y_1 by writing $\mu \in \mathbb{Z}[Y_1]$.

The *size* of an account μ on Y is $\sum_{y\in Y}\mu_y$ and is denoted $|\mu|$. This is just the cardinality of the account if the account is a set or a multiset. If μ is a multiset, we use the notation $\mu!$ as a shorthand for $\prod_{y\in Y}\mu_y!$. Thus there are $|\mu|!/\mu!$ distinct ways of arranging the $|\mu|$ elements of the multiset μ into an ordered $|\mu|$-tuple. Multisets will be easier to use than the sequences that are employed in the definitions of the parameters $\ell(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C})$ that appear in Section 1.1 of the Introduction. Multisets are more natural than sequences since the order of terms in these sequences is irrelevant.

Since we shall often be dealing with accounts on finite Cartesian products of sets, we establish some conventions for dealing with accounts of k-tuples. If k is a positive integer, and $\mu\in\mathbb{Z}[B_1\times\cdots\times B_k]$, then we write $\mu_{b_1,\ldots,b_k}$ instead of $\mu_{(b_1,\ldots,b_k)}$ for the value of μ at $(b_1,b_2,\ldots,b_k)\in B_1\times B_2\times\cdots\times B_k$. If $1\le j_1<j_2<\cdots<j_s\le k$, then we define the *projection of μ to $B_{j_1}\times\cdots\times B_{j_s}$*, denoted $\mathrm{pr}_{B_{j_1}\times\cdots\times B_{j_s}}\mu$, to be the account on $B_{j_1}\times\cdots\times B_{j_s}$ with

$$\left(\mathrm{pr}_{B_{j_1}\times\cdots\times B_{j_s}}\mu\right)_{b_{j_1},\ldots,b_{j_s}}=\sum_{\substack{(c_1,\ldots,c_k)\in B_1\times\cdots\times B_k\\ c_{j_1}=b_{j_1},\ldots,c_{j_s}=b_{j_s}}}\mu_{c_1,\ldots,c_k}$$

for each $b_{j_1},\ldots,b_{j_s}\in B_{j_1}\times\cdots\times B_{j_s}$. Note that

$$\mathrm{pr}_{B_{j_1}\times\cdots\times B_{j_s}}(\mu_1+\mu_2)=\mathrm{pr}_{B_{j_1}\times\cdots\times B_{j_s}}\mu_1+\mathrm{pr}_{B_{j_1}\times\cdots\times B_{j_s}}\mu_2.$$

For example, if $\mu\in\mathbb{Z}[V\times W]$, then $\mathrm{pr}_W\mu\in\mathbb{Z}[W]$ with $(\mathrm{pr}_W\mu)_w=\sum_{v\in V}\mu_{v,w}$ for all $w\in W$.

Suppose that $k\in\mathbb{N}$, $j\in\{1,2,\ldots,k-1\}$, $\mu\in\mathbb{Z}[B_1\times\cdots\times B_k]$, and $b_1\in B_1,\ldots,b_j\in B_j$. Then we define $\mu_{b_1,\ldots,b_j}$ to be the account in $\mathbb{Z}[B_{j+1}\times\cdots\times B_k]$ with $(\mu_{b_1,\ldots,b_j})_{b_{j+1},\ldots,b_k}=\mu_{b_1,\ldots,b_j,b_{j+1},\ldots,b_k}$ for all $b_{j+1}\in B_{j+1},\ldots,b_k\in B_k$. For example, if $\mu\in\mathbb{Z}[V\times W]$ and $v\in V$, then $\mu_v\in\mathbb{Z}[W]$ with $(\mu_v)_w=\mu_{v,w}$ for all $w\in W$.

Throughout this thesis, we let $H=\{0,1,\ldots,e-1\}$. If $\mu\in\mathbb{Z}[H]$, we define the *p-weighted summation of μ*, denoted $\Sigma\mu$, by

$$\Sigma\mu=\sum_{h\in H}\mu_h p^h\pmod{q-1}. \tag{2.3}$$

Note that Σ is a homomorphism from $\mathbb{Z}[H]$ into the group $\mathbb{Z}/(q-1)\mathbb{Z}$ under addition. If $\mu \in \mathbb{Z}[H]$ with $\Sigma\mu = 0$, we call μ a *Delsarte-McEliece* account; the Delsarte-McEliece accounts form a subgroup of $\mathbb{Z}[H]$. Recall the modular condition used in the definition of the parameter $\omega_{mc}(\mathcal{C})$ in Section 1.1 of the Introduction. There we wanted to find the minimum length of unity-product sequences of the form $a_1^{p^{j_1}}, a_2^{p^{j_2}}, \ldots, a_n^{p^{j_n}}$, where each a_i is in some q-closed subset S of A and each $j_i \in \mathbb{N}$, subject to the condition $p^{j_1} + p^{j_2} + \cdots + p^{j_n} \equiv 0 \pmod{q-1}$. It harms nothing to further stipulate that each j_i lie in H, for S is q-closed and the congruence is modulo $q-1$. Then the modular condition is equivalent to saying that the multiset $\mu \in \mathbb{N}[H]$ with elements $j_1, \ldots, j_n$ is Delsarte-McEliece. This modular condition was discovered by Delsarte and McEliece [18], hence we attach their names to accounts in $\mathbb{Z}[H]$ that correspond to it. The following fact is very useful and not difficult to prove:

Lemma 2.15. *A Delsarte-McEliece account in $\mathbb{Z}[H]$ has size divisible by $p-1$. The unique nonempty Delsarte-McEliece multiset in $\mathbb{N}[H]$ of minimal cardinality has $p-1$ instances of each element of H, and thus has a cardinality of $e(p-1)$.*

Proof. A very similar thing is proved in Lemma 2.1 of [61]. If $\mu \in \mathbb{Z}[H]$ is a Delsarte-McEliece account, reduce (2.3) modulo $p-1$ to obtain $0 \equiv \sum_{h\in H} \mu_h \pmod{p-1}$. If we assume that μ is a nonempty Delsarte-McEliece multiset of minimal cardinality, then we claim that $\mu_h < p$ for all $h \in H$. Otherwise, we could make a smaller nonempty Delsarte-McEliece multiset μ' by removing p copies of an element h and adding one copy of the element $h+1$ (where we treat $h+1$ as 0 if $h = e-1$). So $0 \le \mu_h \le p-1$ for all $h \in H$ and not all μ_h are zero. If we had $\mu_h < p-1$ for any h, then $0 < \sum_{h\in H} \mu_h p^h < q-1$, contradicting the fact that μ is Delsarte-McEliece. So $\mu_h = p-1$ for all $h \in H$. □

If $\mu \in \mathbb{N}[H]$ and $r \in \mathbb{Z}_p[\zeta_{q'-1}]$ or $\mathrm{GR}(p^d, ee')$, we define $\mathrm{Fr}^\mu(r) = \prod_{h\in H} \left(\mathrm{Fr}^h(r)\right)^{\mu_h}$. Note that $\mathrm{Fr}^\mu(rs) = \mathrm{Fr}^\mu(r)\mathrm{Fr}^\mu(s)$ and that $\mathrm{Fr}^{\mu_1+\mu_2}(r) = \mathrm{Fr}^{\mu_1}(r)\mathrm{Fr}^{\mu_2}(r)$.

We shall often work with accounts of elements in A. We use multisets in $\mathbb{N}[A]$ instead of the sequences of elements of A used to define the parameters $\omega(\mathcal{C})$ and $\ell(\mathcal{C})$ in Section 1.1 of the Introduction. This is more natural, since the order of the sequences was irrelevant

there. If $\lambda \in \mathbb{Z}[A]$, then we define the *product* of λ, denoted $\Pi\lambda$, to be

$$\Pi\lambda = \prod_{a \in A} a^{\lambda_a}.$$

Note that Π is a homomorphism from $\mathbb{Z}[A]$ (under addition) into the group A. If $\Pi\lambda = 1_A$, we say that λ is a *unity-product* account. If $\lambda \subseteq \mathbb{Z}[\{1_A\}]$, then it is trivially unity-product, and we say that λ is *all-unity*; otherwise λ is *not all-unity*. If f is a function from A into $\mathrm{GR}(p^d, ee')$ or $\mathbb{Z}_p[\zeta_{q'-1}]$ (for example, f might be the Fourier transform of an element of $\mathrm{GR}(p^d, e)[A]$ or $\mathbb{Z}_p[\zeta_{q-1}][A]$), then we define the *evaluation of f at λ*, denoted $f(\lambda)$, by

$$f(\lambda) = \Pi_{a \in A} f(a)^{\lambda_a}.$$

Note that if $F\colon A \to \mathbb{Z}_p[\zeta_{q'-1}]$ and $f = \pi \circ F$, then $\pi(F(\lambda)) = f(\lambda)$ for all $\lambda \in \mathbb{Z}[A]$. Also note that $f(\lambda_1 + \lambda_2) = f(\lambda_1) f(\lambda_2)$.

Suppose for the rest of this section that I is a finite set. We shall often need to work with accounts on sets like $I \times H$, $I \times A$, and $I \times H \times A$. Multisets in $\mathbb{N}[I \times A]$ will replace the sequences used to define the parameters $\omega^{ss}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$, $\omega^{ss}_{mc}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C})$ in Section 1.1 of the Introduction. If $\lambda \in \mathbb{Z}[I \times A]$, then we define the *product* of λ, denoted $\Pi\lambda$, to be

$$\Pi\lambda = \prod_{(i,a) \in I \times A} a^{\lambda_{i,a}}.$$

Note that Π is a homomorphism from $\mathbb{Z}[I \times A]$ (under addition) into the group A. If $\Pi\lambda = 1_A$, we say that λ is a *unity-product* account. If $\lambda \subseteq \mathbb{Z}[I \times \{1_A\}]$, or, equivalently, if $\mathrm{pr}_A \lambda \in \mathbb{N}[\{1_A\}]$, then λ is trivially unity-product, and we say that λ is *all-unity*; otherwise λ is *not all-unity*.

We also shall work with accounts of elements in $H \times A$. When $e > 1$, multisets in $\mathbb{N}[H \times A]$ will replace the sequences used to define the parameters $\omega_{mc}(\mathcal{C})$ and $\ell_{mc}(\mathcal{C})$ in Section 1.1 of the Introduction. If $\lambda \in \mathbb{Z}[H \times A]$, then we define the *product* of λ, denoted $\Pi\lambda$, to be

$$\Pi\lambda = \prod_{(h,a) \in H \times A} a^{p^h \lambda_{h,a}}.$$

Note that Π is a homomorphism from $\mathbb{Z}[H \times A]$ (under addition) into the group A. If $\Pi\lambda = 1_A$, we say that λ is a *unity-product* account. If $\lambda \subseteq \mathbb{Z}[H \times \{1_A\}]$, or, equivalently, if $\mathrm{pr}_A \lambda \in \mathbb{Z}[\{1_A\}]$, then λ is trivially unity-product, and we say that λ is *all-unity*; otherwise λ is *not all-unity*. If f is a function from A into $\mathrm{GR}(p^d, ee')$ or $\mathbb{Z}_p[\zeta_{q'-1}]$ (for example, f might be the Fourier transform of an element of $\mathrm{GR}(p^d, e)[A]$ or $\mathbb{Z}_p[\zeta_{q-1}][A]$), then we define the *evaluation of f at λ*, denoted $f(\lambda)$, by

$$f(\lambda) = \Pi_{(h,a)\in H\times A}\mathrm{Fr}^h(f(a))^{\lambda_{h,a}}.$$

Note that if $F\colon A \to \mathbb{Z}_p[\zeta_{q'-1}]$ and $f = \pi \circ F$, then $\pi(F(\lambda)) = f(\lambda)$ for all $\lambda \in \mathbb{Z}[A]$, because π commutes with Fr. Also note that $f(\lambda_1 + \lambda_2) = f(\lambda_1)f(\lambda_2)$. If $\lambda \in \mathbb{Z}[H \times A]$, then $\mathrm{pr}_H \lambda \in \mathbb{Z}[H]$. We say that λ is *Delsarte-McEliece* if and only if $\mathrm{pr}_H \lambda$ is a Delsarte-McEliece account in $\mathbb{Z}[H]$, as defined above. Recall the modular condition used in the definition of the parameter $\omega_{mc}(\mathcal{C})$ in Section 1.1 of the Introduction. Suppose λ is a multiset in $\mathbb{N}[H \times A]$ and suppose that its elements are $(h_1, a_1), (h_2, a_2), \ldots, (h_n, a_n)$, listed with multiplicity (but order is unimportant). Suppose we form the sequence $a_1^{p^{h_1}}, a_2^{p^{h_2}}, \ldots, a_n^{p^{h_n}}$. Then this sequence meets the modular condition $p^{h_1} + p^{h_2} + \cdots + p^{h_n} \equiv 0 \pmod{q-1}$ of Section 1.1 if and only if $\Sigma\,\mathrm{pr}_H \lambda = 0$, i.e., if and only if λ is Delsarte-McEliece. Concerning the possible sizes of Delsarte-McEliece accounts in $\mathbb{Z}[H \times A]$, Lemma 2.15 implies the following:

Lemma 2.16. *A Delsarte-McEliece account in $\mathbb{Z}[H \times A]$ has size divisible by $p-1$. A nonempty Delsarte-McEliece multiset in $\mathbb{N}[H \times A]$ has cardinality at least $e(p-1)$.*

Proof. If $\lambda \in \mathbb{Z}[H \times A]$ is Delsarte-McEliece, then $\mathrm{pr}_H \lambda \in \mathbb{N}[H]$ is Delsarte-McEliece and has the same size. Then apply Lemma 2.15. □

We shall need to consider accounts of elements in sets of the form $I \times H \times A$. Multisets in $\mathbb{N}[I \times H \times A]$ will replace the sequences used to define the parameters $\omega_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ and $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ in Section 1.1 of the Introduction. If $\lambda \in \mathbb{Z}[I \times H \times A]$, then we define

the *product* of λ, denoted $\Pi\lambda$, to be

$$\Pi\lambda = \prod_{(i,h,a)\in I\times H\times A} a^{p^h \lambda_{i,h,a}}.$$

Note that Π is a homomorphism from $\mathbb{Z}[I \times H \times A]$ (under addition) into the group A. If $\Pi\lambda = 1_A$, we say that λ is a *unity-product* account. If $\lambda \subseteq \mathbb{Z}[I \times H \times \{1_A\}]$, or, equivalently, if $\mathrm{pr}_A\, \lambda \in \mathbb{Z}[\{1_A\}]$, then λ is trivially unity-product, and we say that λ is *all-unity*; otherwise λ is *not all-unity*.

2.6 Collapse and Reduction

The combinatorial devices in this section are used in the proofs of sharpness of some of our lower bounds on the p-adic valuations of weights in codes. The reader should probably skip this section until the concepts it describes are actually deployed (beginning in Section 4.4). The proofs in this section are routine and often repetitious, for we need a few variants of the same idea. Nonetheless, everything is done quite explicitly for the record.

We shall often have a multiset λ in $\mathbb{N}[A]$ or $\mathbb{N}[H \times A]$ and some element $C \in \mathbb{Z}_p[\zeta_{q'-1}][A]$ such that we want to calculate $\tilde{C}(\lambda)$. Recall from Proposition 2.8 that $\tilde{C}(a^q) = \mathrm{Fr}^e(\tilde{C}(a))$ for all $a \in A$. Therefore it is quite possible that some multisets $\lambda' \neq \lambda$ could have $\tilde{C}(\lambda') = \tilde{C}(\lambda)$. We sketch a brief example. Suppose $d = e = 1$, $c \in \mathbb{F}_p[A]$, and $C \in \mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then each scaled Fourier coefficient $\tilde{c}(a)$ lies in $\mathbb{F}_{q'}$, and thus each $\tilde{C}(a)$ is zero or a power of $\zeta_{q'-1}$. Now suppose $\lambda \in \mathbb{N}[A]$ with $\lambda \neq \emptyset$, and choose $a \in A$ with $\lambda_a \neq 0$. Since $p \nmid |A|$, there is some $b \in A$ with $b^p = a$. Set $\lambda' = \lambda - a + pb$. Then $\tilde{C}(a) = \mathrm{Fr}(\tilde{C}(b)) = \tilde{C}(b)^p$, where the second equality comes about because $\tilde{C}(b)$ is zero or a power of $\zeta_{q'-1}$. So $\tilde{C}(a) = 0$ if and only if $\tilde{C}(b) = 0$. If these coefficients are both zero, then $\tilde{C}(\lambda) = 0 = \tilde{C}(\lambda')$. Otherwise, $\tilde{C}(\lambda') = \tilde{C}(\lambda)\tilde{C}(a)^{-1}\tilde{C}(b)^q$, so again $\tilde{C}(\lambda') = \tilde{C}(\lambda)$.

We devise a mechanism to help us determine when two multisets, λ and λ', might have $\tilde{C}(\lambda) = \tilde{C}(\lambda')$. If $e = 1$ (i.e., if $q = p$), if $\lambda \in \mathbb{N}[A]$, and if R is a set of p-class representatives of A, we define the *collapse of λ with respect to R*, denoted $\mathrm{Co}_R(\lambda)$, to be the multiset κ in $\mathbb{N}[R]$ with each κ_r determined as follows: we set κ_r to be a number in $\{0, 1, \ldots, p^{e_r} - 1\}$

congruent modulo $p^{e_r}-1$ to $\sum_{i=0}^{e_r-1} p^i \lambda_{r^{p^i}}$, with $\kappa_r = 0$ if and only if $\lambda_{r^{p^i}} = 0$ for all i. We say λ *collapses to* κ *with respect to* R to mean $\kappa = \mathrm{Co}_R(\lambda)$. We make the following simple observation:

Lemma 2.17. *Suppose that $e = 1$, S is a p-closed subset of A, and $\lambda \in \mathbb{N}[S]$. Suppose R is a set of p-class representatives of A. Then $\mathrm{Co}_R(\lambda) \in \mathbb{N}[R \cap S]$.*

Proof. If $r \in R \setminus S$, then $\lambda_a = 0$ for all $a \in \mathrm{Cl}_p(r)$, since $r \notin S$, S is p-closed, and $\lambda \in \mathbb{N}[S]$. Thus $\sum_{i=0}^{e_r-1} \lambda_{r^{p^i}} p^i = 0$, so that $(\mathrm{Co}_R(\lambda))_r = 0$ by the definition of Co_R. □

Now we can prove that in certain restricted circumstances, $\tilde{C}$ evaluated at λ is the same as $\tilde{C}$ evaluated at the collapse of λ.

Lemma 2.18. *Suppose that $e = 1$, $\lambda \in \mathbb{N}[A]$, and R is a set of p-class representatives of A. Suppose that $c \in \mathbb{Z}/p^d\mathbb{Z}[A]$ such that $\tilde{c}(a)$ is zero or a power of $\pi(\zeta_{q'-1})$ for all $a \in A$. Let C be the element in $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Co}_R(\lambda))$ and $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Co}_R(\lambda))$.*

Proof. Since $\tilde{c} = \pi \circ \tilde{C}$, $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Co}_R(\lambda))$ will follow from $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Co}_R(\lambda))$. To prove the latter, start with

$$\tilde{C}(\mathrm{Co}_R(\lambda)) = \prod_{r \in R} \tilde{C}(r)^{(\mathrm{Co}_R(\lambda))_r}.$$

Note that $\tilde{C}(r)$ is zero or a power of $\zeta_{q'-1}$ (since $\tilde{c}(r)$ is zero or a power of $\pi(\zeta_{q'-1})$), and $\tilde{C}(r)$ is also the Teichmüller lift of an element of $\mathrm{GR}(p^d, e_r)$ by Proposition 2.11. This means that $\tilde{C}(r)$ is zero or a power of $\zeta_{p^{e_r}-1}$, so that $\tilde{C}(r)^{p^{e_r}} - \tilde{C}(r) = 0$. So if the exponent $(\mathrm{Co}_R(\lambda))_r$ of $\tilde{C}(r)$ is nonzero, we may replace it with any other positive integer in the same congruence class modulo $p^{e_r}-1$. Thus, checking the definition of $\mathrm{Co}_R(\lambda)$, we have $\tilde{C}(\mathrm{Co}_R(\lambda)) = \prod_{r \in R} \tilde{C}(r)^{\sum_{i=0}^{e_r-1} p^i \lambda_{r^{p^i}}} = \prod_{r \in R} \prod_{i=0}^{e_r-1} \mathrm{Fr}^i \left(\tilde{C}(r)\right)^{\lambda_{r^{p^i}}} = \prod_{r \in R} \prod_{i=0}^{e_r-1} \tilde{C}(r^{p^i})^{\lambda_{r^{p^i}}} = \prod_{a \in A} \tilde{C}(a)^{\lambda_a} = \tilde{C}(\lambda)$, where the second equality uses the fact that $\tilde{C}(a)$ is zero or a power of $\zeta_{q'-1}$ for all $a \in A$, and the third equality uses Lemma 2.9 (to show that $C \in \mathbb{Z}_p[A]$) and Proposition 2.8 (to show that $\tilde{C}(r^{p^i}) = \mathrm{Fr}^i\left(\tilde{C}(r)\right)$). □

For any $e \geq 1$, we define a similar notion of collapse for multisets in $\mathbb{N}[H \times A]$. If $\lambda \in \mathbb{N}[H \times A]$, and if R is a set of q-class representatives of A, we define the *collapse of* λ

with respect to R, denoted $\mathrm{Co}_R(\lambda)$, to be the multiset $\kappa \in \mathbb{N}[R]$ with each κ_r determined as follows: we set κ_r to be a number in $\{0, 1, \ldots, q^{e_r} - 1\}$ congruent modulo $q^{e_r} - 1$ to $\sum_{i=0}^{e_r-1} \sum_{h \in H} q^i p^h \lambda_{h,r^{q^i}}$, with $\kappa_r = 0$ if and only if $\lambda_{h,r^{q^i}} = 0$ for all i and h. As before, we say λ *collapses to* κ *with respect to* R to mean $\kappa = \mathrm{Co}_R(\lambda)$. We now prove two basic facts about this form of collapse, which are analogous to Lemmas 2.17 and 2.18.

Lemma 2.19. *Suppose that S is a q-closed subset of A, and $\lambda \in \mathbb{N}[H \times S]$. Suppose that R is a set of q-class representatives of A. Then $\mathrm{Co}_R(\lambda) \in \mathbb{N}[R \cap S]$.*

Proof. If $r \in R \smallsetminus S$, then $\lambda_{h,a} = 0$ for all $a \in \mathrm{Cl}_q(r)$ and $h \in H$, since $r \notin S$, S is q-closed, and $\lambda \in \mathbb{N}[H \times S]$. Thus $\sum_{i=0}^{e_r-1} \sum_{h \in H} q^i p^h \lambda_{h,r^{q^i}} = 0$, so that $(\mathrm{Co}_R(\lambda))_r = 0$, by the definition of Co_R. □

Lemma 2.20. *Suppose that $\lambda \in \mathbb{N}[H \times A]$ and R is a set of q-class representatives of A. Suppose that $c \in \mathrm{GR}(p^d, e)[A]$ such that $\tilde{c}(a)$ is zero or a power of $\pi(\zeta_{q'-1})$ for all $a \in A$. Let C be the element in $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Co}_R(\lambda))$ and $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Co}_R(\lambda))$.*

Proof. Since $\tilde{c} = \pi \circ \tilde{C}$, $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Co}_R(\lambda))$ will follow from $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Co}_R(\lambda))$. To prove the latter, we start with

$$\tilde{C}(\mathrm{Co}_R(\lambda)) = \prod_{r \in R} \tilde{C}(r)^{(\mathrm{Co}_R(\lambda))_r}.$$

Note that $\tilde{C}(r)$ is zero or a power of $\zeta_{q'-1}$ (since $\tilde{c}(r)$ is zero or a power of $\pi(\zeta_{q'-1})$), and $\tilde{C}(r)$ is also the Teichmüller lift of an element of $\mathrm{GR}(p^d, ee_r)$ by Proposition 2.11. This means that $\tilde{C}(r)$ is zero or a power of $\zeta_{q^{e_r}-1}$, so that $\tilde{C}(r)^{q^{e_r}} - \tilde{C}(r) = 0$. So if the exponent $(\mathrm{Co}_R(\lambda))_r$ of $\tilde{C}(r)$ is nonzero, we may replace it with any other positive integer in the same congruence class modulo $q^{e_r} - 1$. Thus, checking the definition of $\mathrm{Co}_R(\lambda)$, we have $\tilde{C}(\mathrm{Co}_R(\lambda)) = \prod_{r \in R} \tilde{C}(r)^{\sum_{i=0}^{e_r-1} \sum_{h \in H} q^i p^h \lambda_{h,r^{q^i}}} = \prod_{r \in R} \prod_{i=0}^{e_r-1} \prod_{h \in H} \mathrm{Fr}^{ei+h}\left(\tilde{C}(r)\right)^{\lambda_{h,r^{q^i}}} = \prod_{r \in R} \prod_{i=0}^{e_r-1} \prod_{h \in H} \mathrm{Fr}^h\left(\tilde{C}(r^{q^i})\right)^{\lambda_{h,r^{q^i}}} = \prod_{a \in A} \prod_{h \in H} \mathrm{Fr}^h\left(\tilde{C}(a)\right)^{\lambda_{h,a}} = \tilde{C}(\lambda)$, where the second equality uses the fact that $\tilde{C}(a)$ is zero or a power of $\zeta_{q'-1}$ for all $a \in A$, and the third equality uses Lemma 2.9 (to show that $C \in \mathbb{Z}_p[\zeta_{q-1}][A]$) and Proposition 2.8 (to show that $\tilde{C}(r^{q^i}) = \mathrm{Fr}^{ei}\left(\tilde{C}(r)\right)$). □

Given any multiset λ in $\mathbb{N}[A]$, $\mathbb{N}[I \times A]$, $\mathbb{N}[H \times A]$, or $\mathbb{N}[I \times H \times A]$, we say that λ is *reduced* if λ has no more than $p-1$ instances of any particular element. That is, for $\lambda \in \mathbb{N}[Y]$, λ is reduced if $\lambda_y < p$ for all $y \in Y$. Reduced multisets will be especially easy to work with. The next lemma shows that for each $\mu \in \mathbb{N}[A]$, there is a unique reduced multiset in $\mathbb{N}[A]$ that has the same collapse as μ.

Lemma 2.21 (Reduction Algorithm for $\mathbb{N}[A]$). *Suppose $e = 1$. Let R be a set of p-class representatives of A. Let S be a p-closed subset of A and suppose that $\lambda \in \mathbb{N}[S]$. Then there exists a unique reduced element $\kappa \in \mathbb{N}[A]$ with $\mathrm{Co}_R(\kappa) = \mathrm{Co}_R(\lambda)$. This κ is independent of the choice of R. Furthermore, $\kappa \in \mathbb{N}[S]$, $\Pi\kappa = \Pi\lambda$, κ is all-unity if and only if λ is all-unity, $\kappa = \emptyset$ if and only if $\lambda = \emptyset$, and $|\kappa| = |\lambda| - k(p-1)$ for some positive integer k if λ is not reduced.*

Proof. If $\lambda = \emptyset$ it is already reduced. It is not hard to see that $\mathrm{Co}_R(\emptyset) = \emptyset$ and that no other set collapses to the empty set.

Henceforth, we assume that $\lambda \neq \emptyset$. We shall form a finite sequence of nonempty multisets $\lambda^{(0)}, \ldots, \lambda^{(m)}$. Let $\lambda^{(0)} = \lambda$. If $\lambda^{(i)}$ is not reduced, then let $a \in A$ be such that $(\lambda^{(i)})_a \geq p$, and set $\lambda^{(i+1)} = \lambda^{(i)} - pa + a^p$. Of course, $\lambda^{(i+1)} \neq \emptyset$. Since S is p-closed, note that $\lambda^{(i+1)} \in \mathbb{N}[S]$. Also note that $\Pi\lambda^{(i+1)} = \Pi\lambda^{(i)}$ and that $\lambda^{(i+1)}$ is all-unity if and only if $\lambda^{(i)}$ is all-unity (since there are no elements of order p in A). We claim that $\mathrm{Co}_R(\lambda^{(i+1)}) = \mathrm{Co}_R(\lambda^{(i)})$. If $r \in R$ is not in the same p-class as a, it is clear that $\left(\mathrm{Co}_R(\lambda^{(i+1)})\right)_r = \left(\mathrm{Co}_R(\lambda^{(i)})\right)_r$. So let $s \in R$ be the representative of the p-class of a. Then choose $j \in \{0, 1, \ldots, e_s - 1\}$ so that $a = s^{p^j}$. If $j < e_s - 1$, then it is easy to show that $\sum_{k=0}^{e_s-1} p^k \lambda^{(i+1)}_{s^{p^k}} = \sum_{k=0}^{e_s-1} p^k \lambda^{(i)}_{s^{p^k}}$, so clearly $\left(\mathrm{Co}_R(\lambda^{(i+1)})\right)_s = \left(\mathrm{Co}_R(\lambda^{(i)})\right)_s$. If $j = e_s - 1$, then it is easy to show that $\sum_{k=0}^{e_s-1} p^k \lambda^{(i+1)}_{s^{p^k}} = \left(\sum_{k=0}^{e_s-1} p^k \lambda^{(i)}_{s^{p^k}}\right) - p^{e_s} + 1$, so that $\sum_{k=0}^{e_s-1} p^k \lambda^{(i+1)}_{s^{p^k}} \equiv \sum_{k=0}^{e_s-1} p^k \lambda^{(i)}_{s^{p^k}} \pmod{p^{e_s} - 1}$, and the sums on both sides are strictly positive (since both $\lambda^{(i+1)}$ and $\lambda^{(i)}$ have elements in the p-class of a). Thus, by the definition of Co_R, we have $\left(\mathrm{Co}_R(\lambda^{(i+1)})\right)_s = \left(\mathrm{Co}_R(\lambda^{(i)})\right)_s$ in this case also. So we have shown $\mathrm{Co}_R(\lambda^{(i+1)}) = \mathrm{Co}_R(\lambda^{(i)})$.

Note that $\left|\lambda^{(i+1)}\right| = \left|\lambda^{(i)}\right| - (p-1)$, so that this procedure must eventually terminate. Let $\lambda^{(m)}$ be the last term; it must be reduced. Furthermore, $\lambda^{(m)}$ has all the properties that the lemma claims for κ.

Now we shall show that there is only one reduced $\mu \in \mathbb{N}[A]$ such that $\mathrm{Co}_R(\mu) = \mathrm{Co}_R(\lambda)$. This will follow if we show that no two reduced elements of $\mathbb{N}[A]$ collapse to the same element of $\mathbb{N}[R]$. So suppose that $\mu, \nu \in \mathbb{N}[A]$ are reduced multisets with $\mathrm{Co}_R(\mu) = \mathrm{Co}_R(\nu)$, and we shall show that $\mu = \nu$. Let $r \in R$ be given. Since μ is reduced, we have $0 \leq \sum_{i=0}^{e_r-1} p^i \mu_{r^{p^i}} \leq p^{e_r} - 1$, so that $(\mathrm{Co}_R(\mu))_r = \sum_{i=0}^{e_r-1} p^i \mu_{r^{p^i}}$. Likewise, $(\mathrm{Co}_R(\nu))_r = \sum_{i=0}^{e_r-1} p^i \nu_{r^{p^i}}$. So $\sum_{i=0}^{e_r-1} p^i \mu_{r^{p^i}} = \sum_{i=0}^{e_r-1} p^i \nu_{r^{p^i}}$, and since $0 \leq \mu_{r^{p^i}}, \nu_{r^{p^i}} < p$ for all i, we must have $\mu_{r^{p^i}} = \nu_{r^{p^i}}$ for all i. That is, $\mu_a = \nu_a$ for all $a \in \mathrm{Cl}_p(r)$, but $r \in R$ was arbitrary, so $\mu = \nu$.

Although there might be many ways to construct the sequence $\lambda^{(0)}, \ldots, \lambda^{(m)}$ in our procedure above, this uniqueness property shows that the final term is always the same. Note that we never used R in the definition of this sequence $\lambda^{(0)}, \ldots, \lambda^{(m)}$, so the final multiset in the sequence is independent of R. □

This lemma shows us that if $\lambda \in \mathbb{N}[A]$, then there is a unique reduced $\kappa \in \mathbb{N}[A]$ such that $\mathrm{Co}_R(\kappa) = \mathrm{Co}_R(\lambda)$ for any set R of p-class representatives of A. This κ is called the *reduction of* λ and is denoted $\mathrm{Red}(\lambda)$. With this new terminology, we have the following immediate consequence of the above lemma:

Corollary 2.22. *Suppose that $e = 1$, that $\lambda_1, \lambda_2 \in \mathbb{N}[A]$, and that R is a set of p-class representatives of A. Then $\mathrm{Red}(\lambda_1) = \mathrm{Red}(\lambda_2)$ if and only if $\mathrm{Co}_R(\lambda_1) = \mathrm{Co}_R(\lambda_2)$.*

In view of Lemma 2.18, we also have the following:

Corollary 2.23. *Suppose that $e = 1$, that $\lambda \in \mathbb{N}[A]$, and that R is a set of p-class representatives of A. Suppose that $c \in \mathbb{Z}/p^d\mathbb{Z}[A]$ such that $\tilde{c}(a)$ is zero or a power of $\pi(\zeta_{q'-1})$ for all $a \in A$. Let C be the element in $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Red}(\lambda))$ and $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Red}(\lambda))$.*

We transport the notion of reduction to elements of $\mathbb{N}[I \times A]$, where I is some finite set. The *reduction* of $\lambda \in \mathbb{N}[I \times A]$ is the element $\kappa \in \mathbb{N}[I \times A]$ with $\kappa_i = \mathrm{Red}(\lambda_i)$ for all $i \in I$. Then the following is an easy consequence of Lemma 2.21:

Corollary 2.24. *Suppose $e = 1$. Let I be a finite set. For each $i \in I$, let S_i be a p-closed subset of A, and suppose that $\lambda \in \mathbb{N}[I \times A]$ with $\lambda_i \in \mathbb{N}[S_i]$ for each $i \in I$. Then*

$(\mathrm{Red}(\lambda))_i \in \mathbb{N}[S_i]$ *for all* $i \in I$, $\Pi\,\mathrm{Red}(\lambda) = \Pi\lambda$, *and* $\mathrm{Red}(\lambda)$ *is all-unity if and only if* λ *is all-unity. Furthermore, for each* $i \in I$, $(\mathrm{Red}(\lambda))_i = \emptyset$ *if and only if* $\lambda_i = \emptyset$, *and* $|(\mathrm{Red}(\lambda))_i| = |\lambda_i| - k_i(p-1)$ *for some nonnegative integer* k_i. *If* λ *is not reduced, at least one of these* k_i *is strictly positive. If* R *is a set of* p*-class representatives of* A, *then* $\mathrm{Red}(\lambda)$ *has* $\mathrm{Co}_R([\mathrm{Red}(\lambda)]_i) = \mathrm{Co}_R(\lambda_i)$ *for each* $i \in I$.

We also have a reduction algorithm for multisets in $\mathbb{N}[H \times A]$ when e is an arbitrary positive integer. It is only slightly more complicated than the algorithm of Lemma 2.21 for multisets in $\mathbb{N}[A]$.

Lemma 2.25 (Reduction Algorithm for $\mathbb{N}[H \times A]$). *Let* R *be a set of* q*-class representatives of* A. *Let* S *be a* q*-closed subset of* A *and suppose that* $\lambda \in \mathbb{N}[H \times S]$. *Then there exists a unique reduced element* $\kappa \in \mathbb{N}[H \times A]$, *with* $\mathrm{Co}_R(\kappa) = \mathrm{Co}_R(\lambda)$. *This* κ *is independent of the choice of* R. *Furthermore,* $\kappa \in \mathbb{N}[H \times S]$ *and* $\Sigma\,\mathrm{pr}_H\,\kappa = \Sigma\,\mathrm{pr}_H\,\lambda$, *so that* κ *is Delsarte-McEliece if and only if* λ *is Delsarte-McEliece. Also* $\Pi\kappa = \Pi\lambda$, κ *is all-unity if and only if* λ *is all-unity,* $\kappa = \emptyset$ *if and only if* $\lambda = \emptyset$, *and* $|\kappa| = |\lambda| - k(p-1)$ *for some positive integer* k *if* λ *is not reduced.*

Proof. If $\lambda = \emptyset$ it is already reduced. It is not hard to see that $\mathrm{Co}_R(\emptyset) = \emptyset$ and that no other set collapses to the empty set.

Henceforth, we assume that $\lambda \neq \emptyset$. We shall describe an algorithm that will produce a finite sequence of multisets $\lambda^{(0)}, \ldots, \lambda^{(m)}$. Let $\lambda^{(0)} = \lambda$. If $\lambda^{(i)}$ is not reduced, then let $(h, a) \in H \times A$ be such that $(\lambda^{(i)})_{h,a} \geq p$. If $h < e-1$, set $\lambda^{(i+1)} = \lambda^{(i)} - p(h,a) + (h+1, a)$, and if $h = e-1$, set $\lambda^{(i+1)} = \lambda^{(i)} - p(e-1, a) + (0, a^q)$. Of course $\lambda^{(i+1)} \neq \emptyset$. Since S is q-closed, note that $\lambda^{(i+1)} \in \mathbb{N}[S]$. Also note that $\Pi\lambda^{(i+1)} = \Pi\lambda^{(i)}$ and that $\lambda^{(i+1)}$ is all-unity if and only if $\lambda^{(i)}$ is all-unity (since there is no element whose order is divisible by p in A). Further, note that $\Sigma\,\mathrm{pr}_H\,\lambda^{(i+1)} = \Sigma\,\mathrm{pr}_H\,\lambda^{(i)}$, so that $\lambda^{(i+1)}$ is Delsarte-McEliece if and only if $\lambda^{(i)}$ is Delsarte-McEliece. We claim that $\mathrm{Co}_R(\lambda^{(i+1)}) = \mathrm{Co}_R(\lambda^{(i)})$. If $r \in R$ is not in the same q-class as a, it is clear that $\left[\mathrm{Co}_R(\lambda^{(i+1)})\right]_r = \left[\mathrm{Co}_R(\lambda^{(i)})\right]_r$. So let $s \in R$ be the representative of the q-class of a. Choose $j \in \{0, 1, \ldots, e_s - 1\}$ so that $a = s^{q^j}$. If $j < e_s - 1$

or $h < e-1$, then it is easy to show that

$$\sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i+1)}_{k,s^{q^n}} = \sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i)}_{k,s^{q^n}},$$

so clearly $\left[\mathrm{Co}_R(\lambda^{(i+1)})\right]_s = \left[\mathrm{Co}_R(\lambda^{(i)})\right]_s$. If $j = e_s - 1$ and $h = e-1$, then it is easy to show that

$$\sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i+1)}_{k,s^{q^n}} = \left(\sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i)}_{k,s^{q^n}}\right) - q^{e_s} + 1,$$

so that

$$\sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i+1)}_{k,s^{q^n}} \equiv \sum_{n=0}^{e_s-1}\sum_{k\in H} q^n p^k \lambda^{(i)}_{k,s^{q^n}} \pmod{q^{e_s}-1},$$

and the sums on both sides are strictly positive (since $\lambda^{(i+1)}$ and $\lambda^{(i)}$ each have some element of the form (k,b) with b in the q-class of a). Thus, by the definition of Co_R, we have $\left[\mathrm{Co}_R(\lambda^{(i+1)})\right]_s = \left[\mathrm{Co}_R(\lambda^{(i)})\right]_s$ in this case also. So we have shown $\mathrm{Co}_R(\lambda^{(i+1)}) = \mathrm{Co}_R(\lambda^{(i)})$.

Note that $\left|\lambda^{(i+1)}\right| = \left|\lambda^{(i)}\right| - (p-1)$, so that this procedure must eventually terminate. Let $\lambda^{(m)}$ be the last term; it must be reduced. Furthermore, $\lambda^{(m)}$ has all the properties that the lemma claims for κ.

We now show that there is only one reduced $\mu \in \mathbb{N}[H \times A]$ such that $\mathrm{Co}_R(\mu) = \mathrm{Co}_R(\lambda)$. This will follow if we show that no two reduced elements of $\mathbb{N}[H \times A]$ collapse to the same element of $\mathbb{N}[R]$. So suppose that μ and $\nu \in \mathbb{N}[H \times A]$ are reduced multisets with $\mathrm{Co}_R(\mu) = \mathrm{Co}_R(\nu)$, and we shall show that $\mu = \nu$. Let $r \in R$ be given. Since μ is reduced, we have $0 \le \sum_{i=0}^{e_r-1}\sum_{h\in H} q^i p^h \mu_{h,r^{q^i}} \le q^{e_r} - 1$, so that $(\mathrm{Co}_R(\mu))_r = \sum_{i=0}^{e_r-1}\sum_{h\in H} q^i p^h \mu_{h,r^{q^i}}$. Likewise, $(\mathrm{Co}_R(\nu))_r = \sum_{i=0}^{e_r-1}\sum_{h\in H} q^i p^h \nu_{h,r^{q^i}}$. So we have

$$\sum_{i=0}^{e_r-1}\sum_{h=0}^{e-1} p^{ie+h} \mu_{h,r^{q^i}} = \sum_{i=0}^{e_r-1}\sum_{h=0}^{e-1} p^{ie+h} \nu_{h,r^{q^i}},$$

and since $0 \le \mu_{h,r^{q^i}}, \nu_{h,r^{q^i}} < p$ for all i, we must have $\mu_{h,r^{q^i}} = \nu_{h,r^{q^i}}$ for all i and h. That is, $\mu_{h,a} = \nu_{h,a}$ for all $a \in \mathrm{Cl}_q(r)$ and $h \in H$, but $r \in R$ was arbitrary, so $\mu = \nu$.

Although there might be many ways to construct the sequence $\lambda^{(0)}, \ldots, \lambda^{(m)}$ in our procedure above, this uniqueness property shows that the final term is always the same.

Note that we never used R in the definition of this sequence $\lambda^{(0)}, \ldots, \lambda^{(m)}$, so the final multiset in the sequence is independent of R. □

This lemma shows us that if $\lambda \in \mathbb{N}[H \times A]$, then there is a unique reduced $\kappa \in \mathbb{N}[H \times A]$ such that $\mathrm{Co}_R(\kappa) = \mathrm{Co}_R(\lambda)$ for any set R of q-class representatives of A. Using the same terminology as we did for multisets in $\mathbb{N}[A]$, we call this κ the *reduction of* λ and denote it by $\mathrm{Red}(\lambda)$. Then we obtain results analogous to Corollaries 2.22 and 2.23.

Corollary 2.26. *Suppose that* $\lambda_1, \lambda_2 \in \mathbb{N}[H \times A]$ *and* R *is a set of* q*-class representatives of* A*. Then* $\mathrm{Red}(\lambda_1) = \mathrm{Red}(\lambda_2)$ *if and only if* $\mathrm{Co}_R(\lambda_1) = \mathrm{Co}_R(\lambda_2)$*.*

In view of Lemma 2.20, we have the following result:

Corollary 2.27. *Suppose that* $\lambda \in \mathbb{N}[H \times A]$ *and* R *is a set of* q*-class representatives of* A*. Suppose that* $c \in \mathrm{GR}(p^d, e)[A]$ *such that* $\tilde{c}(a)$ *is zero or a power of* $\pi(\zeta_{q'-1})$ *for all* $a \in A$*. Let* C *be the element in* $\mathbb{Z}_p[\zeta_{q'-1}][A]$ *with* $\tilde{C} = \tau \circ \tilde{c}$*. Then* $\tilde{c}(\lambda) = \tilde{c}(\mathrm{Red}(\lambda))$ *and* $\tilde{C}(\lambda) = \tilde{C}(\mathrm{Red}(\lambda))$*.*

We transport the notion of reduction to elements of $\mathbb{N}[I \times H \times A]$, where I is some finite set. The *reduction* of $\lambda \in \mathbb{N}[I \times H \times A]$ is the element $\kappa \in \mathbb{N}[I \times H \times A]$ with $\kappa_i = \mathrm{Red}(\lambda_i)$ for all $i \in I$. Then we obtain an analogue of Corollary 2.24 above.

Corollary 2.28. *Let* I *be a finite set. For each* $i \in I$*, let* S_i *be a* q*-closed subset of* A*, and suppose that* $\lambda \in \mathbb{N}[I \times H \times A]$ *with* $\lambda_i \in \mathbb{N}[H \times S_i]$ *for each* $i \in I$*. Then for each* $i \in I$*, we have* $(\mathrm{Red}(\lambda))_i \in \mathbb{N}[H \times S_i]$*. For each* $i \in I$*,* $(\mathrm{Red}(\lambda))_i$ *is Delsarte-McEliece if and only if* λ_i *is Delsarte-McEliece. Also* $\Pi\,\mathrm{Red}(\lambda) = \Pi\lambda$ *and* $\mathrm{Red}(\lambda)$ *is all-unity if and only if* λ *is all-unity. Furthermore, for each* $i \in I$*,* $(\mathrm{Red}(\lambda))_i = \emptyset$ *if and only if* $\lambda_i = \emptyset$*, and* $|(\mathrm{Red}(\lambda))_i| = |\lambda_i| - k_i(p-1)$ *for some nonnegative integer* k_i*. If* λ *is not reduced, at least one of these* k_i *is strictly positive. If* R *is a set of* p*-class representatives of* A*, then* $\mathrm{Red}(\lambda)$ *has* $\mathrm{Co}_R([\mathrm{Red}(\lambda)]_i) = \mathrm{Co}_R(\lambda_i)$ *for each* $i \in I$*.*

2.7 The Frobenius Action on Accounts

The material in this section is used in various places (in the proofs of Theorems 4.18, 5.12, 6.13, and 7.14) to prove that certain terms in our p-adic estimates are fixed by the Frobenius

automorphism Fr. This is done to prove that such terms, known to be in $\mathbb{Z}_p[\zeta_{q'-1}]$, are actually elements of $\mathbb{Z}_p$ (which is comforting, since they are supposed to be p-adic estimates of elements of $\mathbb{Z}$). Readers should probably ignore this section until they encounter the Frobenius action in the proofs of the aforementioned theorems. The development here is repetitious, as in the previous section, because we need several variants of the same idea. The proofs are routine, but we include them with a fair amount of detail for the record.

When $e = 1$, i.e., when $q = p$, we introduce the *Frobenius action*, denoted $\mathrm{Fr_A}$, on the group A. We let $\mathrm{Fr_A}(a) = a^p$. Note that $\mathrm{Fr_A}^{e'}(a) = a^{q'} = a$, by our choice of e' and q'. Thus $\mathrm{Fr_A}$ is a permutation of A. Also note that the orbits of $\mathrm{Fr_A}$ are the p-classes. We extend $\mathrm{Fr_A}$ to act on elements of $\mathbb{Z}[A]$ by sending $\sum_{a\in A} \lambda_a a$ to $\sum_{a\in A} \lambda_a \mathrm{Fr_A}(a) = \sum_{a\in A} \lambda_a a^p$. Note that $\mathrm{Fr_A}^{e'}(\lambda) = \lambda$ for any $\lambda \in \mathbb{Z}[A]$, so $\mathrm{Fr_A}$ is a permutation of $\mathbb{Z}[A]$. Also note that $\mathrm{Fr_A}$ preserves size. There are many other such useful properties that we summarize here:

Lemma 2.29. *If $e = 1$, then $\mathrm{Fr_A}$ is a permutation of $\mathbb{Z}[A]$ with $\mathrm{Fr_A}^{e'}$ the identity. $\mathrm{Fr_A}$ preserves size. $\mathrm{Fr_A}$ takes multisets to multisets and $(\mathrm{Fr_A}(\lambda))! = \lambda!$ for all $\lambda \in \mathbb{N}[A]$. If S is a p-closed set and $\lambda \in \mathbb{Z}[S]$, then $\mathrm{Fr_A}(\lambda) \in \mathbb{Z}[S]$. Additionally, $\mathrm{Fr_A}(\lambda)$ is all-unity if and only if λ is all-unity. Further, $\Pi\,\mathrm{Fr_A}(\lambda) = (\Pi\lambda)^p$, so that $\mathrm{Fr_A}(\lambda)$ is unity-product if and only if λ is unity-product. If $c \in \mathbb{Z}/p^d\mathbb{Z}[A]$ and C is the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$, and if $\lambda \in \mathbb{Z}[A]$, then $\tilde{C}(\mathrm{Fr_A}(\lambda)) = \mathrm{Fr}(\tilde{C}(\lambda))$.*

Proof. It has already been noted that $\mathrm{Fr_A}$ is a size-preserving permutation with $\mathrm{Fr_A}^{e'}$ the identity. Since $\mathrm{Fr_A}$ permutes the elements of A, if we list the $|A|$ coefficients in the formal sum $\lambda = \sum_{a\in A} \lambda_a a$ and then list the $|A|$ coefficients in the formal sum $\mathrm{Fr_A}(\lambda) = \sum_{a\in A} \lambda_a a^p$, we get the same list modulo ordering. Thus λ takes multisets to multisets and $\mathrm{Fr_A}(\lambda)! = \lambda!$. Since the orbits of the action of $\mathrm{Fr_A}$ on A are p-classes, $\mathrm{Fr_A}$ always takes an element of a p-closed set S into the same set S. So $\mathrm{Fr_A}$ takes $\mathbb{Z}[S]$ into itself. In particular, $\mathrm{Fr_A}$ maps all-unity accounts to all-unity accounts, and furthermore, if $\mathrm{Fr_A}(\lambda)$ is all-unity, then $\lambda = \mathrm{Fr_A}^{e'}(\lambda)$ is all-unity. Note that $\Pi\,\mathrm{Fr_A}(\lambda) = \prod_{a\in A} a^{(\mathrm{Fr_A}(\lambda))_a} = \prod_{a\in A} (a^p)^{(\mathrm{Fr_A}(\lambda))_{a^p}} = \prod_{a\in A} (a^p)^{\lambda_a} = (\Pi\lambda)^p$.

Finally, suppose that $c \in \mathbb{Z}/p^d\mathbb{Z}[A]$ and C is the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then by Lemma 2.9, we have $C \in \mathbb{Z}_p[A]$. Now suppose that $\lambda \in \mathbb{Z}[A]$. Then $\tilde{C}(\mathrm{Fr_A}(\lambda)) =$

$\prod_{a\in A}\tilde{C}(a)^{(\mathrm{Fr_A}(\lambda))_a}=\prod_{a\in A}\tilde{C}(a^p)^{(\mathrm{Fr_A}(\lambda))_{a^p}}=\prod_{a\in A}\tilde{C}(a^p)^{\lambda_a}$. Now use Proposition 2.8 (recognizing that $q=p$ since $e=1$) to obtain $\tilde{C}(\mathrm{Fr_A}(\lambda))=\prod_{a\in A}\mathrm{Fr}(\tilde{C}(a))^{\lambda_a}=\mathrm{Fr}(\tilde{C}(\lambda))$. □

If I is a finite set, we extend the Frobenius action $\mathrm{Fr_A}$ to $\mathbb{Z}[I\times A]$ so that if $\lambda\in\mathbb{Z}[I\times A]$, $(\mathrm{Fr_A}(\lambda))_i=\mathrm{Fr_A}(\lambda_i)$. We can easily deduce what we need to know about this action on $\mathbb{Z}[I\times A]$ from the above lemma.

Corollary 2.30. *If $e=1$, then $\mathrm{Fr_A}$ is a permutation of $\mathbb{Z}[I\times A]$ with ${\mathrm{Fr_A}}^{e'}$ the identity. $\mathrm{Fr_A}$ preserves size. Furthermore, if $\lambda\in\mathbb{Z}[I\times A]$, then $|(\mathrm{Fr_A}(\lambda))_i|=|\lambda_i|$ for all $i\in I$. Thus $\mathrm{pr}_I\,\mathrm{Fr_A}(\lambda)=\mathrm{pr}_I\,\lambda$. $\mathrm{Fr_A}$ takes multisets to multisets and $(\mathrm{Fr_A}(\lambda))!=\lambda!$ for all $\lambda\in\mathbb{N}[A]$. If S_i is a p-closed set for each $i\in I$, and if $\lambda_i\in\mathbb{Z}[S_i]$ for each $i\in I$, then $(\mathrm{Fr_A}(\lambda))_i\in\mathbb{Z}[S_i]$ for each $i\in I$. Additionally, $\mathrm{Fr_A}(\lambda)$ is all-unity if and only if λ is all-unity. Further, $\Pi\,\mathrm{Fr_A}(\lambda)=(\Pi\lambda)^p$, so that $\mathrm{Fr_A}(\lambda)$ is unity-product if and only if λ is unity-product. Suppose that $c_i\in\mathbb{Z}/p^d\mathbb{Z}[A]$ for each $i\in I$ and that C_i is the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C}_i=\tau\circ\tilde{c}_i$ for each $i\in I$. If $\lambda\in\mathbb{Z}[I\times A]$, then $\prod_{i\in I}\tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i)=\mathrm{Fr}\left(\prod_{i\in I}\tilde{C}_i(\lambda)\right)$.*

For any value of e, we also define the Frobenius action $\mathrm{Fr_A}$ as a function from the set $H\times A$ to itself, wherein

$$\mathrm{Fr_A}(h,a)=\begin{cases}(h+1,a) & \text{if } h<e-1,\\ (0,a^q) & \text{if } h=e-1.\end{cases}$$

Note that ${\mathrm{Fr_A}}^e(h,a)=(h,a^q)$, and so ${\mathrm{Fr_A}}^{ee'}(h,a)=(h,a^{q'})=(h,a)$, by our choice of e' and q'. Thus $\mathrm{Fr_A}$ is a permutation of $H\times A$. Also note that the orbits of $\mathrm{Fr_A}$ are sets of the form $H\times B$, where B is a q-class in A. We extend $\mathrm{Fr_A}$ to act on elements of $\mathbb{Z}[H\times A]$ by sending $\sum_{(h,a)\in H\times A}\lambda_{h,a}(h,a)$ to $\sum_{(h,a)\in H\times A}\lambda_{h,a}\,\mathrm{Fr_A}(h,a)$. Note that ${\mathrm{Fr_A}}^{ee'}(\lambda)=\lambda$ for any $\lambda\in\mathbb{Z}[A]$, so $\mathrm{Fr_A}$ is a permutation of $\mathbb{Z}[H\times A]$. Also note that $\mathrm{Fr_A}$ preserves size. There are many other such useful properties, analogous to those in Lemma 2.29, which we summarize here:

Lemma 2.31. *$\mathrm{Fr_A}$ is a permutation of $\mathbb{Z}[H\times A]$ with ${\mathrm{Fr_A}}^{ee'}$ the identity. $\mathrm{Fr_A}$ preserves size. $\mathrm{Fr_A}$ takes multisets to multisets and $(\mathrm{Fr_A}(\lambda))!=\lambda!$ for all $\lambda\in\mathbb{N}[H\times A]$. If S is a q-closed set and $\lambda\in\mathbb{Z}[H\times S]$, then $\mathrm{Fr_A}(\lambda)\in\mathbb{Z}[H\times S]$. Additionally, $\mathrm{Fr_A}(\lambda)$ is all-unity*

if and only if λ is all-unity. Further, $\Pi \operatorname{Fr}_{\mathrm{A}}(\lambda) = (\Pi\lambda)^p$, so that $\operatorname{Fr}_{\mathrm{A}}(\lambda)$ is unity-product if and only if λ is unity-product. We have $\Sigma \operatorname{pr}_H(\operatorname{Fr}_{\mathrm{A}}(\lambda)) = p\,(\Sigma \operatorname{pr}_H \lambda)$, so that $\operatorname{Fr}_{\mathrm{A}}(\lambda)$ is Delsarte-McEliece if and only if λ is Delsarte-McEliece. If $c \in \mathrm{GR}(p^d, e)[A]$ and C is the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$, and if $\lambda \in \mathbb{Z}[H \times A]$, then $\tilde{C}(\operatorname{Fr}_{\mathrm{A}}(\lambda)) = \operatorname{Fr}(\tilde{C}(\lambda))$.

Proof. It has already been noted above that $\operatorname{Fr}_{\mathrm{A}}$ is a size-preserving permutation with ${\operatorname{Fr}_{\mathrm{A}}}^{ee'}$ the identity. Since $\operatorname{Fr}_{\mathrm{A}}$ permutes the elements of $H \times A$, if we list the $e|A|$ coefficients in the formal sum $\lambda = \sum_{(h,a)\in H\times A} \lambda_{h,a}(h,a)$ and then list the $e|A|$ coefficients in the formal sum $\operatorname{Fr}_{\mathrm{A}}(\lambda) = \sum_{(h,a)\in H\times A} \lambda_{h,a} \operatorname{Fr}_{\mathrm{A}}(h,a)$, we get the same list modulo ordering. Thus λ takes multisets to multisets and $\operatorname{Fr}_{\mathrm{A}}(\lambda)! = \lambda!$. Recall that the orbits of the action of $\operatorname{Fr}_{\mathrm{A}}$ on $H \times A$ are Cartesian products of H with q-classes. Thus, if S is q-closed, then $\operatorname{Fr}_{\mathrm{A}}$ always takes an element of $H \times S$ into the same set $H \times S$. So $\operatorname{Fr}_{\mathrm{A}}$ takes $\mathbb{N}[H \times S]$ into itself. Therefore $\operatorname{Fr}_{\mathrm{A}}$ takes all-unity accounts to all-unity accounts, and furthermore, if $\operatorname{Fr}_{\mathrm{A}}(\lambda)$ is all-unity, then $\lambda = {\operatorname{Fr}_{\mathrm{A}}}^{ee'}(\lambda)$ is all-unity.

We now show that $\Pi \operatorname{Fr}_{\mathrm{A}}(\lambda) = (\Pi\lambda)^p$. First we verify this for the account that is a singleton set $\{(h,a)\}$. We write this account as the formal sum $1(h,a)$, or just (h,a). Indeed, if $h < e-1$, we have $\Pi \operatorname{Fr}_{\mathrm{A}}(h,a) = \Pi(h+1,a) = a^{p^{h+1}} = (\Pi(h,a))^p$. On the other hand, if $h = e-1$, then $\Pi \operatorname{Fr}_{\mathrm{A}}(e-1,a) = \Pi(0,a^q) = a^q = \left(a^{p^{e-1}}\right)^p = (\Pi(e-1,a))^p$. Now we consider an arbitrary $\lambda \in \mathbb{Z}[H \times A]$. By the properties of Π, we can calculate $\Pi \operatorname{Fr}_{\mathrm{A}}(\lambda) = \Pi\left(\sum_{(h,a)\in H\times A} \lambda_{h,a} \operatorname{Fr}_{\mathrm{A}}(h,a)\right) = \prod_{(h,a)\in H\times A} (\Pi \operatorname{Fr}_{\mathrm{A}}(h,a))^{\lambda_{h,a}} = \prod_{(h,a)\in H\times A} (\Pi(h,a))^{p\lambda_{h,a}} = \left[\Pi\left(\sum_{(h,a)\in H\times A} \lambda_{h,a}(h,a)\right)\right]^p = (\Pi\lambda)^p$.

Next, we show that $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}(\lambda) = p\,(\Sigma \operatorname{pr}_H \lambda)$. First we check this for the singleton set (h,a) (we are representing it as a formal sum, since it is an account). Indeed, if $h < e-1$, then $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}((h,a)) = \Sigma \operatorname{pr}_H(h+1,a) = p^{h+1} = p\Sigma \operatorname{pr}_H(h,a)$. If $h = e-1$, recall that $\Sigma\colon \mathbb{Z}[H] \to \mathbb{Z}/(q-1)\mathbb{Z}$, and then check $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}((e-1,a)) = \Sigma \operatorname{pr}_H(0,a^q) = 1 = q = p(p^{e-1}) = p\Sigma \operatorname{pr}_H(e-1,a)$ in $\mathbb{Z}/(q-1)\mathbb{Z}$. Then, for an arbitrary $\lambda \in \mathbb{Z}[H \times A]$, we have $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}(\lambda) = \Sigma \operatorname{pr}_H\left(\sum_{(h,a)\in H\times A} \lambda_{h,a} \operatorname{Fr}_{\mathrm{A}}(h,a)\right) = \sum_{(h,a)\in H\times A} \lambda_{h,a} (\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}(h,a)) = \sum_{(h,a)\in H\times A} \lambda_{h,a} p\,(\Sigma \operatorname{pr}_H(h,a))$. Therefore, we have $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}(\lambda) = p\Sigma \operatorname{pr}_H\left(\sum_{(h,a)\in H\times A} \lambda_{h,a}(h,a)\right) = p\Sigma \operatorname{pr}_H \lambda$. Since p is coprime to $q-1$, this means that $\Sigma \operatorname{pr}_H \lambda = 0$ if and only if $\Sigma \operatorname{pr}_H \operatorname{Fr}_{\mathrm{A}}(\lambda) = 0$, i.e., λ is Delsarte-McEliece if

and only if $\mathrm{Fr_A}(\lambda)$ is Delsarte-McEliece.

Finally, suppose that $c \in \mathrm{GR}(p^d, e)[A]$ and C is the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Then by Lemma 2.9, we have $C \in \mathbb{Z}_p[\zeta_{q-1}][A]$. Now suppose that $\lambda \in \mathbb{Z}[H \times A]$. We want to show that $\tilde{C}(\mathrm{Fr_A}(\lambda)) = \mathrm{Fr}(\tilde{C}(\lambda))$. First we verify this when λ is the singleton set (h, a). Indeed, if $h < e-1$, we have $\tilde{C}(\mathrm{Fr_A}((h,a))) = \tilde{C}((h+1,a)) = \mathrm{Fr}^{h+1}(\tilde{C}(a)) = \mathrm{Fr}\left(\tilde{C}((h,a))\right)$. On the other hand, if $h = e-1$, then we have $\tilde{C}(\mathrm{Fr_A}((e-1,a))) = \tilde{C}((0,a^q)) = \tilde{C}(a^q)$. But now use Proposition 2.8 to get $\tilde{C}(a^q) = \mathrm{Fr}^e(\tilde{C}(a)) = \mathrm{Fr}\left(\tilde{C}((e-1,a))\right)$. Now let λ be an arbitrary element of $\mathbb{Z}[H \times A]$, and recall that $\tilde{C}(\lambda_1 + \lambda_2) = \tilde{C}(\lambda_1)\tilde{C}(\lambda_2)$, so that $\tilde{C}(\mathrm{Fr_A}(\lambda)) = \tilde{C}\left(\sum_{(h,a)\in H\times A} \lambda_{h,a} \mathrm{Fr_A}(h,a)\right) = \prod_{(h,a)\in H\times A}\left(\tilde{C}\left(\mathrm{Fr_A}(h,a)\right)\right)^{\lambda_{h,a}}$. Then use our result for singleton sets to obtain $\tilde{C}(\mathrm{Fr_A}(\lambda)) = \prod_{(h,a)\in H\times A} \mathrm{Fr}\left(\tilde{C}\left((h,a)\right)\right)^{\lambda_{h,a}} = \mathrm{Fr}\left[\prod_{(h,a)\in H\times A}\left(\tilde{C}\left((h,a)\right)\right)^{\lambda_{h,a}}\right] = \mathrm{Fr}\left(\tilde{C}(\lambda)\right)$. □

If I is a finite set, we extend the Frobenius action $\mathrm{Fr_A}$ to $\mathbb{Z}[I \times H \times A]$ so that if $\lambda \in \mathbb{Z}[I \times H \times A]$, then $(\mathrm{Fr_A}(\lambda))_i = \mathrm{Fr_A}(\lambda_i)$. We can easily deduce what we need to know about this action on $\mathbb{Z}[I \times H \times A]$ from the above lemma.

Corollary 2.32. $\mathrm{Fr_A}$ *is a permutation of* $\mathbb{Z}[I \times H \times A]$ *with* $\mathrm{Fr_A}^{ee'}$ *the identity.* $\mathrm{Fr_A}$ *preserves size of accounts. Furthermore, if* $\lambda \in \mathbb{Z}[I \times H \times A]$*, then* $|(\mathrm{Fr_A}(\lambda))_i| = |\lambda_i|$ *for all* $i \in I$*.* $\mathrm{Fr_A}$ *takes multisets to multisets and* $(\mathrm{Fr_A}(\lambda))! = \lambda!$ *for all* $\lambda \in \mathbb{N}[I \times H \times A]$*. If* $\{S_i\}_{i\in I}$ *is a family of q-closed sets, and if* $\lambda \in \mathbb{Z}[I \times H \times A]$ *with* $\lambda_i \in \mathbb{Z}[H \times S_i]$ *for each* i*, then* $(\mathrm{Fr_A}(\lambda))_i \in \mathbb{Z}[H \times S_i]$ *for each* $i \in I$*. Additionally,* $\mathrm{Fr_A}(\lambda)$ *is all-unity if and only if* λ *is all-unity. Further,* $\Pi \mathrm{Fr_A}(\lambda) = (\Pi\lambda)^p$*, so that* $\mathrm{Fr_A}(\lambda)$ *is unity-product if and only if* λ *is unity-product. For each* $i \in I$*,* $\Sigma \mathrm{pr}_H([\mathrm{Fr_A}(\lambda)]_i) = p\Sigma \mathrm{pr}_H(\lambda_i)$*. Thus* $(\mathrm{Fr_A}(\lambda))_i$ *is Delsarte-McEliece for all* $i \in I$ *if and only if* λ_i *is Delsarte-McEliece for all* $i \in I$*. Suppose* $c_i \in \mathrm{GR}(p^d, e)[A]$ *for each* $i \in I$*. Suppose that* C_i *is the element of* $\mathbb{Z}_p[\zeta_{q'-1}][A]$ *with* $\tilde{C}_i = \tau \circ \tilde{c}_i$ *for each* $i \in I$*. If* $\lambda \in \mathbb{Z}[I \times H \times A]$*, then* $\prod_{i\in I} \tilde{C}_i\left([\mathrm{Fr_A}(\lambda)]_i\right) = \mathrm{Fr}\left(\prod_{i\in I} \tilde{C}(\lambda_i)\right)$.

2.8 Polynomial Notations and Facts

This brief section develops some notations that we shall use to express and manipulate polynomials. We also introduce the binomial coefficient polynomials here. Finally, we

record some basic results about polynomials that we shall need when we want to prove that bounds on p-adic valuations of weights are sharp.

Suppose that J is a finite index set with some (total) ordering, and suppose that we are considering polynomials with coefficients in some ring R and indeterminates $\{x_j : j \in J\}$. To indicate that f is such a polynomial, we sometimes represent the list of all indeterminates (arranged in order of increasing index) by $\mathbf{x}$ and write $f(\mathbf{x}) \in R[\mathbf{x}]$. We also use the alternative notation $f(\{x_j\}_{j\in J}) \in R[\{x_j\}_{j\in J}]$ to mean the same thing. If our index set is a product of sets, say $J = I \times K$, then we shall abbreviate $x_{(i,k)}$ by x_{ik}.

The notion of accounts, introduced in the previous section, may be used to express such polynomials more efficiently. For example, if $\mu \in \mathbb{N}[J]$, then $\mathbf{x}^\mu$ will be used as shorthand for the monomial $\prod_{j\in J} x_j^{\mu_j}$. Thus any polynomial f in our indeterminates $\mathbf{x}$ can be written as $f(\mathbf{x}) = \sum_{\mu\in\mathbb{N}[J]} f_\mu \mathbf{x}^\mu$, where the coefficients f_μ are in the ring R and almost all f_μ are zero. Furthermore, suppose we have a collection of elements $\{a_j\}_{j\in J}$ in R. Then we may represent the list of them (in order of increasing index) by $\mathbf{a}$. Of course $f(\mathbf{a})$ is the value of the polynomial when each indeterminate x_j is replaced by the value a_j. For convenience of expression, we introduce the notation $f(\{x_j = a_j\}_{j\in J})$, or just $f(\{x_j = a_j\})$ if the index set is clear, to mean the same thing as $f(\mathbf{a})$. If $J = \{j_1, \ldots, j_s\}$, we can also use the notation $f(\{x_{j_1} = a_{j_1}, \ldots, x_{j_s} = a_{j_s}\})$. If $K \subseteq J$ and we have a collection of elements $\{a_k\}_{k\in K}$ in R, then we use the notation $f(\{x_k = a_k\}_{k\in K})$ to indicate the polynomial in the variables $\{x_i : i \in J \setminus K\}$ obtained when we replace the variable x_k with a_k for each $k \in K$. If $K = \{k_1, \ldots, k_t\}$, we can also use the notation $f(\{x_{k_1} = a_{k_1}, \ldots, x_{k_t} = a_{k_t}\})$ to mean the same thing.

We often make use of the binomial coefficient polynomials, which are defined as

$$\binom{x}{n} = \begin{cases} 0 & \text{if } n < 0, \\ 1 & \text{if } n = 0, \\ \frac{x(x-1)\ldots(x-n+1)}{n!} & \text{if } n > 0. \end{cases}$$

Note that these polynomials, when regarded as functions, map $\mathbb{N}$ into $\mathbb{N}$. They also map $\mathbb{Z}_p$ into $\mathbb{Z}_p$, by a simple argument employing the p-adic topology in the complete metric space

$\mathbb{Q}_p$. For the binomial coefficient polynomials are p-adically continuous (being polynomials) and $\mathbb{N}$ is dense in the closed set $\mathbb{Z}_p$.

We now present a basic result that we shall use every time we want to prove the sharpness of our lower bounds on p-adic valuations of weights in codes. We follow it with a lemma upon which it depends and a useful corollary of that lemma.

Lemma 2.33. *Suppose that $\mathbf{x} = (x_1, \ldots, x_n)$ is a list of indeterminates, and suppose that for each $i \in \{1, \ldots, n\}$, S_i is a finite subset of $\mathbb{Z}_p[\zeta_{q'-1}]$ wherein no two elements are congruent modulo p. Suppose that $f(\mathbf{x}) \in \mathbb{Q}_p(\zeta_{q'-1})[\mathbf{x}]$ is not the zero polynomial, that m is the minimum p-adic valuation of the coefficients of $f(\mathbf{x})$, and that the degree of f in x_i is less than $|S_i|$ for each i. Then $f(b_1, \ldots, b_n) \equiv 0 \pmod{p^m}$ for all $b_1, \ldots, b_n \in \mathbb{Z}_p[\zeta_{q'-1}]$, but there is some $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$ such that $f(a_1, \ldots, a_n) \not\equiv 0 \pmod{p^{m+1}}$.*

Proof. By scaling the polynomial by a power of p, it suffices to prove this for $m = 0$. It is clear that if the coefficients of f are in $\mathbb{Z}_p[\zeta_{q'-1}]$, and if we replace the indeterminates by elements of $\mathbb{Z}_p[\zeta_{q'-1}]$, then the resulting value is in $\mathbb{Z}_p[\zeta_{q'-1}]$. So it only remains to show that there is some $\mathbf{a} \in S_1 \times \cdots \times S_n$ such that $f(\mathbf{a}) \not\equiv 0 \pmod{p}$. Let $\bar{f}(\mathbf{x}) \in \mathbb{F}_{q'}[\mathbf{x}]$ be the reduction modulo p of f, and for each $i \in \{1, \ldots, n\}$, let $\bar{S}_i \subseteq \mathbb{F}_{q'}$ be the set of elements obtained by reducing the elements of S_i modulo p. Note that $\bar{f}(\mathbf{x})$ is not the zero polynomial since f has a coefficient with zero p-adic valuation. Also note that $\left|\bar{S}_i\right| = |S_i|$ since no two elements of S_i are equivalent modulo p. Then we need to show that $\bar{f}(\mathbf{x})$ is nonzero at some point in $\bar{S}_1 \times \cdots \times \bar{S}_n$. But this follows from Lemma 2.34 below, a standard result. □

Lemma 2.34. *Suppose that K is a field, $\mathbf{x} = (x_1, \ldots, x_n)$ is a list of indeterminates, and suppose that S_i is a finite subset of K for $i = 1, \ldots, n$. Suppose that $f(\mathbf{x}) \in K[\mathbf{x}]$ is not the zero polynomial and that the degree of f in x_i is less than $|S_i|$ for each i. Then there is some $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. This is a well-known result, presented as Lemma 3.10 in [18]. □

Corollary 2.35. *Suppose that K is a field, $\mathbf{x} = (x_1, \ldots, x_n)$ is a list of indeterminates, and suppose that S_i is a finite subset of K for $i = 1, \ldots, n$. Suppose that $f(\mathbf{x}), g(\mathbf{x}) \in K[\mathbf{x}]$ are*

distinct polynomials whose degrees in x_i are less than $|S_i|$ for each i. Then there is some $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$ such that $f(a_1, \ldots, a_n) \neq g(a_1, \ldots, a_n)$.

Chapter 3

The Abstract Theorem

This brief chapter settles once and for all certain calculations that we shall use over and over again. These calculations will accomplish the same end as those displayed in the presentation of Wilson's method at the beginning of Section 1.3, but here we consider circumstances of much greater complexity. The higher degree of complexity is needed to handle the more exotic forms of counting polynomials that we have devised (see Section 1.3 for a brief overview) and which we shall apply in the next chapters. What is presented here are theorems (actually, one theorem in utmost generality and its corollaries) which take as their input counting polynomials and give as their output p-adic estimates of weights. Nowhere in this chapter do we learn how to construct good counting polynomials. In each of the succeeding chapters, we consider different problems, and use various methods to construct the appropriate counting polynomials. So the results in this chapter are merely ghosts of theorems. They all need counting polynomials to be applied usefully. We begin with a calculation which is essentially the repeated application of the distributive law and of combinatorial repackaging of unwieldy sums over sets of sequences into more manageable sums over multisets. We also make use of the fact that $\sum_{a \in A} \langle a, b \rangle$ is zero unless $b = 1_A$; this fact is the source of the unity-product condition that arises over and over in this work (for example, in the definition of the parameters $\omega(\mathcal{C})$, $\ell(\mathcal{C})$, and their relatives in the Introduction).

Proposition 3.1. *Suppose that $t \geq 1$, $I = \{1, 2, \ldots, t\}$, and $C_1, \ldots, C_t \in \mathbb{Z}_p[\zeta_{q-1}][A]$. Let $\mathbf{x}$ be the list of indeterminates in $\{x_{ih} : (i, h) \in I \times H\}$, listed in some order. Suppose that*

$f(\mathbf{x}) \in \mathbb{Q}_p(\zeta_{q-1})[\mathbf{x}]$ *with* $f(\mathbf{x}) = \sum_{\mu \in \mathbb{N}[I\times H]} f_\mu \mathbf{x}^\mu$. *Then*

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = |A| \sum_{\mu\in\mathbb{N}[I\times H]} \mu! f_\mu \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \mathrm{pr}_{I\times H}\,\lambda=\mu\\ \Pi\lambda=1_A}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i).$$

Proof. By linearity, it suffices to consider $f(\mathbf{x}) = \mathbf{x}^\mu$ for some $\mu \in \mathbb{N}[I \times H]$ and show that

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = |A|\mu! \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \mathrm{pr}_{I\times H}\,\lambda=\mu\\ \Pi\lambda=1_A}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i). \tag{3.1}$$

In this case,

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = \sum_{a\in A} \prod_{(i,h)\in I\times H} \mathrm{Fr}^h\left(C_i(a)\right)^{\mu_{i,h}},$$

and we use the inversion formula for the scaled Fourier transform to obtain

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = \sum_{a\in A} \prod_{(i,h)\in I\times H} \mathrm{Fr}^h\left(\sum_{b\in A}\tilde{C}_i(b)\langle b,a\rangle\right)^{\mu_{i,h}}. \tag{3.2}$$

Now use the distributive law to get

$$\mathrm{Fr}^h\left(\sum_{b\in A}\tilde{C}_i(b)\langle b,a\rangle\right)^{\mu_{i,h}} = \sum_{b_1,b_2,\ldots,b_{\mu_{i,h}}\in A}\ \prod_{j=1}^{\mu_{i,h}} \mathrm{Fr}^h\left(\tilde{C}_i(b_j)\langle b_j,a\rangle\right).$$

We convert this from a sum over sequences of length $\mu_{i,h}$ of elements in A to a sum over multisets of size $\mu_{i,h}$ of elements in A. Recall that there are $\frac{|\nu|!}{\nu!}$ distinct ways to arrange the $|\nu|$ elements of a multiset ν into a sequence of length $|\nu|$. Thus

$$\mathrm{Fr}^h\left(\sum_{b\in A}\tilde{C}_i(b)\langle b,a\rangle\right)^{\mu_{i,h}} = \sum_{\substack{\nu\in\mathbb{N}[A]\\ |\nu|=\mu_{i,h}}} \frac{\mu_{i,h}!}{\nu!}\prod_{b\in A}\mathrm{Fr}^h\left(\tilde{C}_i(b)\langle b,a\rangle\right)^{\nu_b}.$$

We take the product of this over all $h \in H$ and we apply the distributive law again to obtain

$$\prod_{h\in H} \mathrm{Fr}^h \left(\sum_{b\in A} \tilde{C}_i(b)\langle b, a\rangle \right)^{\mu_{i,h}} = \sum_{\substack{\nu_0,\ldots,\nu_{e-1}\in\mathbb{N}[A] \\ |\nu_0|=\mu_{i,0},\ldots,|\nu_{e-1}|=\mu_{i,e-1}}} \prod_{h\in H} \left[\frac{\mu_{i,h}!}{\nu_h!} \prod_{b\in A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{(\nu_h)_b} \right].$$

Then we repackage the sum over sequences as a sum over multisets to get

$$\begin{aligned} \prod_{h\in H} \mathrm{Fr}^h \left(\sum_{b\in A} \tilde{C}_i(b)\langle b, a\rangle \right)^{\mu_{i,h}} &= \sum_{\substack{\kappa\in\mathbb{N}[H\times A] \\ \mathrm{pr}_H\, \kappa=\mu_i}} \prod_{h\in H} \left[\frac{\mu_{i,h}!}{\kappa_h!} \prod_{b\in A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{\kappa_{h,b}} \right] \\ &= \sum_{\substack{\kappa\in\mathbb{N}[H\times A] \\ \mathrm{pr}_H\, \kappa=\mu_i}} \frac{\mu_i!}{\kappa!} \prod_{(h,b)\in H\times A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{\kappa_{h,b}}. \end{aligned}$$

Then we take the product of this over all $i \in I$ and we apply the distributive law yet again to obtain

$$\begin{aligned} &\prod_{(i,h)\in I\times H} \mathrm{Fr}^h \left(\sum_{b\in A} \tilde{C}_i(b)\langle b, a\rangle \right)^{\mu_{i,h}} \\ &\qquad = \sum_{\substack{\kappa_1,\ldots,\kappa_t\in\mathbb{N}[H\times A] \\ \mathrm{pr}_H\, \kappa_j=\mu_j}} \prod_{i\in I} \left[\frac{\mu_i!}{\kappa_i!} \prod_{(h,b)\in H\times A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{(\kappa_i)_{h,b}} \right]. \end{aligned}$$

Convert the sum over sequences to a sum over multisets to get

$$\prod_{(i,h)\in I\times H} \mathrm{Fr}^h \left(\sum_{b\in A} \tilde{C}_i(b)\langle b, a\rangle \right)^{\mu_{i,h}} = \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A] \\ \mathrm{pr}_{I\times H}\, \lambda=\mu}} \prod_{i\in I} \left[\frac{\mu_i!}{\lambda_i!} \prod_{(h,b)\in H\times A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{\lambda_{i,h,b}} \right],$$

and so

$$\prod_{(i,h)\in I\times H} \mathrm{Fr}^h \left(\sum_{b\in A} \tilde{C}_i(b)\langle b, a\rangle \right)^{\mu_{i,h}} = \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A] \\ \mathrm{pr}_{I\times H}\, \lambda=\mu}} \frac{\mu!}{\lambda!} \prod_{(i,h,b)\in I\times H\times A} \mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{\lambda_{i,h,b}}. \tag{3.3}$$

Now note that

$$\mathrm{Fr}^h \left(\tilde{C}_i(b)\langle b, a\rangle \right)^{\lambda_{i,h,b}} = \mathrm{Fr}^h \left(\tilde{C}_i(b) \right)^{(\lambda_i)_{h,b}} \langle b, a\rangle^{p^h \lambda_{i,h,b}},$$

because $\langle a, b\rangle$ is always a power of $\zeta_{q'-1}$, and Fr takes such roots of unity to their pth powers. Then by Lemma 2.5, we have

$$\mathrm{Fr}^h\left(\tilde{C}_i(b)\langle b, a\rangle\right)^{\lambda_{i,h,b}} = \mathrm{Fr}^h\left(\tilde{C}_i(b)\right)^{(\lambda_i)_{h,b}}\left\langle b^{p^h\lambda_{i,h,b}}, a\right\rangle.$$

If we take the product of both sides of this equation over all $(i,h,b) \in I \times H \times A$ and use the compact notations developed in Section 2.5, we obtain

$$\prod_{(i,h,b)\in I\times H\times A} \mathrm{Fr}^h\left(\tilde{C}_i(b)\langle b, a\rangle\right)^{\lambda_{i,h,b}} = \left(\prod_{i\in I}\tilde{C}_i(\lambda_i)\right)\langle \Pi\lambda, a\rangle.$$

Using this with (3.3), we obtain

$$\prod_{(i,h)\in I\times H} \mathrm{Fr}^h\left(\sum_{b\in A}\tilde{C}_i(b)\langle b, a\rangle\right)^{\mu_{i,h}} = \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \mathrm{pr}_{I\times H}\,\lambda=\mu}} \frac{\mu!}{\lambda!}\left(\prod_{i\in I}\tilde{C}_i(\lambda_i)\right)\langle \Pi\lambda, a\rangle,$$

so that, in view of (3.2), we have

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = \sum_{a\in A}\sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \mathrm{pr}_{I\times H}\,\lambda=\mu}} \frac{\mu!}{\lambda!}\left(\prod_{i\in I}\tilde{C}_i(\lambda_i)\right)\langle \Pi\lambda, a\rangle.$$

The only term on the right-hand side that has dependence on a is $\langle \Pi\lambda, a\rangle$. Using Lemma 2.5, we obtain

$$\sum_{a\in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h\left(C_i(a)\right)\right\}\right) = |A| \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \mathrm{pr}_{I\times H}\,\lambda=\mu\\ \Pi\lambda=1_A}} \frac{\mu!}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i),$$

which is (3.1), which is what we need to show. □

Now we use this calculation to derive our abstract theorem. Much of the theorem is given over to dealing with the problem of codewords whose Fourier transforms do not vanish at 1_A. The normalized weight (see Section 2.4) is deployed to deal with this issue.

Theorem 3.2 (Abstract Theorem). *Let* $m, t \geq 1$, $I = \{1, 2, \ldots, t\}$, $S_1, \ldots, S_t \subseteq$

A, and $c_1, \dots, c_t \in \mathrm{GR}(p^d, e)[A]$ with $\hat{c}_i$ supported on S_i for each $i \in I$. Suppose that $\mathrm{wt}\colon \mathrm{GR}(p^d, e)^t \to \mathbb{Z}$ *is a t-wise weight function. For each $i \in I$, let C_i be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C}_i = \tau \circ \tilde{c}_i$. Let $\mathbf{x}$ be a list (in some order) of the indeterminates in $\{x_{ih} : (i,h) \in I \times H\}$. Let $f(\mathbf{x}) = \sum_{\mu \in \mathbb{N}[I \times H]} f_\mu \mathbf{x}^\mu \in \mathbb{Q}_p(\zeta_{q-1})[\mathbf{x}]$ with $\mathrm{wt}(\pi(r_1), \dots, \pi(r_t)) \equiv f\left(\left\{x_{ih} = \mathrm{Fr}^h(r_i)\right\}\right) \pmod{p^m}$ for all $r_1, \dots, r_t \in \mathbb{Z}_p[\zeta_{q-1}]$. Then*

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \dots, c_t) \equiv |A| \sum_{\mu \in \mathbb{N}[I \times H]} \mu! f_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times H \times A], \mathrm{pr}_{I \times H}\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A(\lambda_1) \in \mathbb{N}[S_1], \dots, \mathrm{pr}_A(\lambda_t) \in \mathbb{N}[S_t]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}. \tag{3.4}$$

Proof. Note that since $\hat{c}_i$ is supported on S_i, so is $\tilde{c}_i$, and so is $\tilde{C}_i = \tau \circ \tilde{c}_i$ (because $\tau(0) = 0$). Thus if $\lambda \in \mathbb{N}[I \times H \times A]$ with $\mathrm{pr}_A(\lambda_i) \notin \mathbb{N}[S_i]$ for some $i \in I$, then $\tilde{C}_i(\lambda_i) = \prod_{(h,a) \in H \times A} \mathrm{Fr}^h(\tilde{C}_i(a))^{\lambda_{i,h,a}} = 0$. Because of this, we claim that it will suffice for us to prove the special case when $S_1 = S_2 = \cdots = S_t = A$, i.e.,

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \dots, c_t) \equiv |A| \sum_{\mu \in \mathbb{N}[I \times H]} \mu! f_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times H \times A], \mathrm{pr}_{I \times H}\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}, \tag{3.5}$$

when $c_1, \dots, c_t$ are allowed to be arbitrary in $\mathrm{GR}(p^d, e)[A]$. For if we consider some particular $c_1, \dots, c_t$ with each $\hat{c}_i$ supported on S_i, then we may restrict the sum to those λ with $\mathrm{pr}_A(\lambda_i) \in \mathbb{N}[S_i]$ for all $i \in I$, and so obtain (3.4).

So we shall prove (3.5) for arbitrary $c_1, \dots, c_t \in \mathrm{GR}(p^d, e)[A]$. By Lemma 2.9, we know that $C_i \in \mathbb{Z}_p[\zeta_{q-1}][A]$ and $\pi(C_i) = c_i$ for each $i \in I$, and we use our polynomial f to obtain

$$\mathrm{wt}(c_1(a), \dots, c_t(a)) \equiv f\left(\left\{x_{ih} = \mathrm{Fr}^h(C_i(a))\right\}\right) \pmod{p^m}$$

for each $a \in A$, so that

$$\mathrm{wt}(c_1, \dots, c_t) \equiv \sum_{a \in A} f\left(\left\{x_{ih} = \mathrm{Fr}^h(C_i(a))\right\}\right) \pmod{p^m}.$$

We can apply Proposition 3.1 to obtain

$$\operatorname{wt}(c_1,\dots,c_t) \equiv |A| \sum_{\mu\in\mathbb{N}[I\times H]} \mu! f_\mu \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A]\\ \operatorname{pr}_{I\times H}\lambda=\mu\\ \Pi\lambda=1_A}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}.$$

Now we separate the sum into two parts to segregate those multisets λ that are all-unity, thus obtaining

$$\begin{aligned}\operatorname{wt}(c_1,\dots,c_t) \equiv |A| &\sum_{\mu\in\mathbb{N}[I\times H]} \mu! f_\mu \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A],\operatorname{pr}_{I\times H}\lambda=\mu\\ \Pi\lambda=1_A,\operatorname{pr}_A\lambda\in\mathbb{N}[\{1_A\}]}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i)\\ &+ |A| \sum_{\mu\in\mathbb{N}[I\times H]} \mu! f_\mu \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A],\operatorname{pr}_{I\times H}\lambda=\mu\\ \Pi\lambda=1_A,\operatorname{pr}_A\lambda\notin\mathbb{N}[\{1_A\}]}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}.\end{aligned}$$

The first term on the right-hand side is a polynomial function of the terms $\operatorname{Fr}^h(\tilde{C}_i(1_A))$ with $i\in I$ and $h\in H$, i.e., there is some polynomial $\rho(\mathbf{x})\in\mathbb{Q}_p(\zeta_{q-1})[\mathbf{x}]$ so that

$$\begin{aligned}\operatorname{wt}(c_1,\dots,c_t) \equiv{}& \rho\left(\left\{x_{ih}=\operatorname{Fr}^h[\tau(\tilde{c}_i(1_A))]\right\}\right)\\ &+ |A| \sum_{\mu\in\mathbb{N}[I\times H]} \mu! f_\mu \sum_{\substack{\lambda\in\mathbb{N}[I\times H\times A],\operatorname{pr}_{I\times H}\lambda=\mu\\ \Pi\lambda=1_A,\operatorname{pr}_A\lambda\notin\mathbb{N}[\{1_A\}]}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}, \quad (3.6)\end{aligned}$$

where we have used the fact that $\tilde{C}_i=\tau\circ\tilde{c}_i$.

For this paragraph, let us suppose that $c_1,\dots,c_t$ are constant words in $\operatorname{GR}(p^d,e)[A]$. By Lemma 2.7, each word c_i has $\tilde{c}_i(a)=0$ for $a\neq 1_A$ and $c_i(b)=\tilde{c}_i(1_A)$ for all $b\in A$. Since $\tau(0)=0$, this means that for each $i\in I$ we have $\tilde{C}_i(a)=0$ for $a\neq 1_A$, so the second term on the right-hand side of the congruence (3.6) vanishes, and we have

$$\operatorname{wt}(c_1,\dots,c_t) \equiv \rho\left(\left\{x_{ih}=\operatorname{Fr}^h[\tau(\tilde{c}_i(1_A))]\right\}\right) \pmod{p^m}.$$

Since $c_i(b)=\tilde{c}_i(1_A)$ for all $b\in A$, we have

$$|A|\operatorname{wt}\left(\tilde{c}_1(1_A),\dots,\tilde{c}_t(1_A)\right) \equiv \rho\left(\left\{x_{ih}=\operatorname{Fr}^h[\tau(\tilde{c}_i(1_A))]\right\}\right) \pmod{p^m}.$$

Note that as we vary the word c_i over all constant words, the Fourier coefficient $\tilde{c}_i(1_A)$ varies over $\mathrm{GR}(p^d, e)$. Thus

$$|A| \operatorname{wt}(r_1, \ldots, r_t) \equiv \rho\left(\left\{x_{ih} = \mathrm{Fr}^h(\tau(r_i))\right\}\right) \pmod{p^m}, \tag{3.7}$$

for all $r_1, \ldots, r_t \in \mathrm{GR}(p^d, e)$.

Now we return to the consideration of arbitrary $c_1, \ldots, c_t \in \mathrm{GR}(p^d, e)[A]$. Note that $\tilde{c}_i(1_A) = |A|^{-1} \sum_{b \in A} c_i(b) \in \mathrm{GR}(p^d, e)$ for all $i \in I$. Thus we may employ (3.7) in (3.6) to obtain

$$\begin{aligned}\operatorname{wt}(c_1, \ldots, c_t) \equiv{}& |A| \operatorname{wt}\left(\tilde{c}_1(1_A), \ldots, \tilde{c}_t(1_A)\right) \\ &+ |A| \sum_{\mu \in \mathbb{N}[I \times H]} \mu! f_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times H \times A], \operatorname{pr}_{I \times H} \lambda = \mu \\ \Pi\lambda = 1_A, \operatorname{pr}_A \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m},\end{aligned}$$

which is (3.5), which is what we were to show. □

The following three corollaries are just specializations of the abstract theorem. That they follow directly from the abstract theorem can be seen by those who are familiar enough with the account notations and operations (see Section 2.5). For those readers who are not at ease with accounts, we include the proofs, which are tedious set-theoretic manipulations.

Corollary 3.3 (Single-Word Weights over Galois Rings). *Let $m \geq 1$, $S \subseteq A$, and $c \in \mathrm{GR}(p^d, e)[A]$ with $\hat{c}$ supported on S. Suppose that* $\operatorname{wt}\colon \mathrm{GR}(p^d, e) \to \mathbb{Z}$ *is a weight function. Let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Let $\mathbf{x}$ be a list (in some order) of the indeterminates in $\{x_h : h \in H\}$. Let $f(\mathbf{x}) = \sum_{\mu \in \mathbb{N}[H]} f_\mu \mathbf{x}^\mu \in \mathbb{Q}_p(\zeta_{q-1})[\mathbf{x}]$ with $\operatorname{wt}(\pi(r)) \equiv f\left(\left\{x_h = \mathrm{Fr}^h(r)\right\}\right) \pmod{p^m}$ for all $r \in \mathbb{Z}_p[\zeta_{q-1}]$. Then*

$$\operatorname{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\mu \in \mathbb{N}[H]} \mu! f_\mu \sum_{\substack{\lambda \in \mathbb{N}[H \times S], \operatorname{pr}_H \lambda = \mu \\ \Pi\lambda = 1_A, \operatorname{pr}_A \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^m}. \tag{3.8}$$

Proof. Set $t = 1$, $I = \{1\}$, $S_1 = S$, $c_1 = c$, and $C_1 = C$. Let $\mathbf{y}$ be a list (in some order) of the indeterminates in $\{y_{ih} : (i, h) \in I \times H\}$, and let $g(\mathbf{y}) = \sum_{\mu \in \mathbb{N}[I \times H]} g_\mu \mathbf{y}^\mu$ with $g_\mu = f_{\mu_1}$.

Then $\mathrm{wt}(\pi(r_1)) \equiv g\left(\left\{y_{1,h} = \mathrm{Fr}^h(r_1)\right\}\right) \pmod{p^m}$ for all $r_1 \in \mathbb{Z}_p[\zeta_{q-1}]$. So by the abstract theorem above, keeping in mind that $t = 1$, $I = \{1\}$, $S_1 = S$, $c_1 = c$, and $C_1 = C$, we have

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\mu \in \mathbb{N}[I \times H]} \mu! g_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times H \times A], \mathrm{pr}_{I \times H}\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A(\lambda_1) \in \mathbb{N}[S]}} \frac{1}{\lambda!} \tilde{C}(\lambda_1) \pmod{p^m}.$$

Note that $\mu \mapsto \mathrm{pr}_H\, \mu$ is a bijection from $\mathbb{N}[I \times H]$ to $\mathbb{N}[H]$. Let $\Phi \colon \mathbb{N}[H] \to \mathbb{N}[I \times H]$ be the inverse of this map. Likewise, note that $\lambda \mapsto \mathrm{pr}_{H \times A}\, \lambda$ is a bijection from $\mathbb{N}[I \times H \times A]$ to $\mathbb{N}[H \times A]$. Let $\Psi \colon \mathbb{N}[H \times A] \to \mathbb{N}[I \times H \times A]$ be the inverse of this map. Because these maps Φ and Ψ are bijective, they enable us to re-index our sums. We do this, noting that $\lambda_1 = \mathrm{pr}_{H \times A}\, \lambda$, to get

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\nu \in \mathbb{N}[H]} \Phi(\nu)! g_{\Phi(\nu)} \sum_{\substack{\kappa \in \mathbb{N}[H \times A], \mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\nu) \\ \Pi\Psi(\kappa) = 1_A, \mathrm{pr}_A\, \Psi(\kappa) \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A\, \kappa \in \mathbb{N}[S]}} \frac{1}{\Psi(\kappa)!} \tilde{C}(\kappa) \pmod{p^m}.$$

Note that $\Phi(\nu)! = \nu!$ and $\Psi(\kappa)! = \kappa!$. Also recall that $g_\mu = f_{\mu_1} = f_{\mathrm{pr}_H\, \mu}$, so that $g_{\Phi(\nu)} = f_\nu$. Further, note that $(\mathrm{pr}_{I \times H}\, \Psi(\kappa))_{1,h} = (\mathrm{pr}_H\, \kappa)_h$ for all $h \in H$, so that $\mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\mathrm{pr}_H\, \kappa)$. So, by the bijectivity of Φ, the condition $\mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\nu)$ is equivalent to the condition $\mathrm{pr}_H\, \kappa = \nu$. Also note that $\Pi\Psi(\kappa) = \Pi\kappa$ and $\mathrm{pr}_A\, \Psi(\kappa) = \mathrm{pr}_A\, \kappa$. Thus, we have

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\nu \in \mathbb{N}[H]} \nu! f_\nu \sum_{\substack{\kappa \in \mathbb{N}[H \times A], \mathrm{pr}_H\, \kappa = \nu \\ \Pi\kappa = 1_A, \mathrm{pr}_A\, \kappa \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A\, \kappa \in \mathbb{N}[S]}} \frac{1}{\kappa!} \tilde{C}(\kappa) \pmod{p^m},$$

and note that the conditions $\kappa \in \mathbb{N}[H \times A]$ and $\mathrm{pr}_A\, \kappa \in \mathbb{N}[S]$ can be combined into the single condition $\kappa \in \mathbb{N}[H \times S]$ to obtain (3.8). □

Corollary 3.4 (Multi-Word Weights over $\mathbb{Z}/p^d\mathbb{Z}$). *Let $m, t \geq 1$, $I = \{1, 2, \ldots, t\}$, $S_1, \ldots, S_t \subseteq A$, and $c_1, \ldots, c_t \in \mathbb{Z}/p^d\mathbb{Z}[A]$ with $\hat{c}_i$ supported on S_i for each $i \in I$. Suppose that $\mathrm{wt} \colon (\mathbb{Z}/p^d\mathbb{Z})^t \to \mathbb{Z}$ is a t-wise weight function. For each $i \in I$, let C_i be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C}_i = \tau \circ \tilde{c}_i$. Let $\mathbf{x}$ be a list (in some order) of the indeterminates in $\{x_i : i \in I\}$. Let $f(\mathbf{x}) = \sum_{\mu \in \mathbb{N}[I]} f_\mu \mathbf{x}^\mu \in \mathbb{Q}_p[\mathbf{x}]$ with $\mathrm{wt}(\pi(r_1), \ldots, \pi(r_t)) \equiv f\left(\{x_i = r_i\}\right)$*

$(\mathrm{mod}\ p^m)$ *for all* $r_1, \ldots, r_t \in \mathbb{Z}_p$. *Then*

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\mu \in \mathbb{N}[I]} \mu! f_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_1 \in \mathbb{N}[S_1], \ldots, \lambda_t \in \mathbb{N}[S_t]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}. \tag{3.9}$$

Proof. Here we have $H = \{0\}$. We let the $\mathbf{y}$ denote a list (in some order) of the indeterminates in $\{y_{ih} : (i,h) \in I \times H\}$, and we let $g(\mathbf{y}) = \sum_{\mu \in \mathbb{N}[I \times H]} g_\mu \mathbf{y}^\mu$ with $g_\mu = f_{\mathrm{pr}_I\, \mu}$. Then $\mathrm{wt}(\pi(r_1), \ldots, \pi(r_t)) \equiv g\left(\left\{y_{i,0} = \mathrm{Fr}^0(r_i)\right\}\right) \pmod{p^m}$ for all $r_1, \ldots, r_t \in \mathbb{Z}_p$. Thus, by our abstract theorem above, we have

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\mu \in \mathbb{N}[I \times H]} \mu! g_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times H \times A], \mathrm{pr}_{I \times H}\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A(\lambda_1) \in \mathbb{N}[S_1], \ldots, \mathrm{pr}_A(\lambda_t) \in \mathbb{N}[S_t]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}.$$

Note that $\mu \mapsto \mathrm{pr}_I\, \mu$ is a bijection from $\mathbb{N}[I \times H]$ to $\mathbb{N}[I]$. Let $\Phi \colon \mathbb{N}[I] \to \mathbb{N}[I \times H]$ be the inverse of this map. Likewise, note that $\lambda \mapsto \mathrm{pr}_{I \times A}\, \lambda$ is a bijection from $\mathbb{N}[I \times H \times A]$ to $\mathbb{N}[I \times A]$. Let $\Psi \colon \mathbb{N}[I \times A] \to \mathbb{N}[I \times H \times A]$ be the inverse of this map. Because these maps Φ and Ψ are bijective, they enable us to re-index our sums to obtain

$$\begin{aligned} &\mathrm{wt}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv \\ &\qquad |A| \sum_{\nu \in \mathbb{N}[I]} \Phi(\nu)! g_{\Phi(\nu)} \sum_{\substack{\kappa \in \mathbb{N}[I \times A], \mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\nu) \\ \Pi\Psi(\kappa) = 1_A, \mathrm{pr}_A\, \Psi(\kappa) \notin \mathbb{N}[\{1_A\}] \\ \mathrm{pr}_A([\Psi(\kappa)]_1) \in \mathbb{N}[S_1], \ldots, \mathrm{pr}_A([\Psi(\kappa)]_t) \in \mathbb{N}[S_t]}} \frac{1}{\Psi(\kappa)!} \prod_{i \in I} \tilde{C}_i([\Psi(\kappa)]_i) \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\mathrm{mod}\ p^m). \end{aligned}$$

Note that $\Phi(\nu)! = \nu!$ and $\Psi(\kappa)! = \kappa!$. Also recall that $g_\mu = f_{\mathrm{pr}_I\, \mu}$, so that $g_{\Phi(\nu)} = f_\nu$. Further, note that $(\mathrm{pr}_{I \times H}\, \Psi(\kappa))_{i,0} = (\mathrm{pr}_I\, \kappa)_i$ for all $i \in I$, so that $\mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\mathrm{pr}_I\, \kappa)$. So, by the bijectivity of Φ, the condition $\mathrm{pr}_{I \times H}\, \Psi(\kappa) = \Phi(\nu)$ is equivalent to the condition $\mathrm{pr}_I\, \kappa = \nu$. Also note that $\Pi\Psi(\kappa) = \Pi\kappa$ and $\mathrm{pr}_A\, \Psi(\kappa) = \mathrm{pr}_A\, \kappa$. Finally, for each $i \in I$ and $a \in A$, we have $[\mathrm{pr}_A([\Psi(\kappa)]_i)]_a = \sum_{h \in H} ([\Psi(\kappa)]_i)_{h,a} = ([\Psi(\kappa)]_i)_{0,a} = [\Psi(\kappa)]_{i,0,a} = \kappa_{i,a} =$

$(\kappa_i)_a$, so that $\mathrm{pr}_A([\Psi(\kappa)]_i) = \kappa_i$. Thus, we have

$$\mathrm{wt}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\nu \in \mathbb{N}[I]} \nu! f_\nu \sum_{\substack{\kappa \in \mathbb{N}[I \times A], \mathrm{pr}_I\, \kappa = \nu \\ \Pi\kappa = 1_A, \mathrm{pr}_A\, \kappa \notin \mathbb{N}[\{1_A\}] \\ \kappa_1 \in \mathbb{N}[S_1], \ldots, \kappa_t \in \mathbb{N}[S_t]}} \frac{1}{\kappa!} \prod_{i \in I} \tilde{C}_i([\Psi(\kappa)]_i) \pmod{p^m}. \quad (3.10)$$

Now, note that for each $i \in I$ and $\kappa \in \mathbb{N}[I \times A]$, we have

$$\tilde{C}_i([\Psi(\kappa)]_i) = \prod_{(h,a) \in H \times A} = \mathrm{Fr}^h(\tilde{C}_i(a))^{([\Psi(\kappa)]_i)_{h,a}},$$

but $H = \{0\}$, so that we have

$$\tilde{C}_i([\Psi(\kappa)]_i) = \prod_{a \in A} \tilde{C}_i(a)^{([\Psi(\kappa)]_i)_{0,a}}.$$

Since $([\Psi(\kappa)]_i)_{0,a} = [\Psi(\kappa)]_{i,0,a} = \kappa_{i,a} = (\kappa_i)_a$, we have

$$\begin{aligned} \tilde{C}_i([\Psi(\kappa)]_i) &= \prod_{a \in A} \tilde{C}_i(a)^{(\kappa_i)_a} \\ &= \tilde{C}_i(\kappa_i), \end{aligned}$$

which, when substituted into (3.10), gives (3.9), which is what we were to prove. □

Corollary 3.5 (Single-Word Weights over $\mathbb{Z}/p^d\mathbb{Z}$). *Let $m \geq 1$, $S \subseteq A$, and $c \in \mathbb{Z}/p^d\mathbb{Z}[A]$ with $\hat{c}$ supported on S. Suppose that* $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ *is a weight function. Let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. Let $f(x) = \sum_{j \in \mathbb{N}} f_j x^j \in \mathbb{Q}_p[x]$ with $\mathrm{wt}(\pi(r)) \equiv f(r) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$. Then*

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{j \in \mathbb{N}} j! f_j \sum_{\substack{\lambda \in \mathbb{N}[S], |\lambda| = j \\ \Pi\lambda = 1_A, \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^m}. \quad (3.11)$$

Proof. Set $t = 1$, $I = \{1\}$, $S_1 = S$, $c_1 = c$, and $C_1 = C$. Let $\mathbf{y}$ be the list of indeterminates in $\{y_i : i \in I\}$ (which consists of the single indeterminate y_1) and let $g(\mathbf{y}) = \sum_{\mu \in \mathbb{N}[I]} g_\mu \mathbf{y}^\mu$, where $g_\mu = f_{\mu_1}$. Then $\mathrm{wt}(\pi(r_1)) \equiv g(\{y_1 = r_1\}) \pmod{p^m}$ for all $r_1 \in \mathbb{Z}_p$. So by Corollary

3.4, keeping in mind that $t = 1$, $I = \{1\}$, $S_1 = S$, $c_1 = c$, and $C_1 = C$, we have

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\mu \in \mathbb{N}[I]} \mu! g_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I\, \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_1 \in \mathbb{N}[S]}} \frac{1}{\lambda!} \tilde{C}(\lambda_1) \pmod{p^m}.$$

Note that $\mu \mapsto |\mu|$ (which is the same as $\mu \mapsto \mu_1$) is a bijection from $\mathbb{N}[I]$ to $\mathbb{N}$. Let $\Phi\colon \mathbb{N} \to \mathbb{N}[I]$ be the inverse of this map. Likewise, note that $\lambda \mapsto \mathrm{pr}_A\, \lambda$ is a bijection from $\mathbb{N}[I \times A]$ to $\mathbb{N}[A]$. Let $\Psi\colon \mathbb{N}[A] \to \mathbb{N}[I \times A]$ be the inverse of this map. Because these maps Φ and Ψ are bijective, they enable us to re-index our sums. We do this, noting that $\lambda_1 = \mathrm{pr}_A\, \lambda$, to get

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{j \in \mathbb{N}} \Phi(j)! g_{\Phi(j)} \sum_{\substack{\kappa \in \mathbb{N}[A], \mathrm{pr}_I\, \Psi(\kappa) = \Phi(j) \\ \Pi\Psi(\kappa) = 1_A, \mathrm{pr}_A\, \Psi(\kappa) \notin \mathbb{N}[\{1_A\}] \\ \kappa \in \mathbb{N}[S]}} \frac{1}{\Psi(\kappa)!} \tilde{C}(\kappa) \pmod{p^m}.$$

Note that $\Phi(j)! = j!$ and $\Psi(\kappa)! = \kappa!$. Also recall that $g_\mu = f_{\mu_1} = f_{|\mu|}$, so that $g_{\Phi(j)} = f_j$. Further, note that $(\mathrm{pr}_I\, \Psi(\kappa))_1 = |\kappa|$, so that $\mathrm{pr}_I\, \Psi(\kappa) = \Phi(|\kappa|)$. So, by the bijectivity of Φ, the condition $\mathrm{pr}_I\, \Psi(\kappa) = \Phi(j)$ is equivalent to the condition $|\kappa| = j$. Also note that $\Pi\Psi(\kappa) = \Pi\kappa$ and $\mathrm{pr}_A\, \Psi(\kappa) = \kappa$. Thus, we have

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{j \in \mathbb{N}} j! f_j \sum_{\substack{\kappa \in \mathbb{N}[A], |\kappa| = j \\ \Pi\kappa = 1_A, \kappa \notin \mathbb{N}[\{1_A\}] \\ \kappa \in \mathbb{N}[S]}} \frac{1}{\kappa!} \tilde{C}(\kappa) \pmod{p^m}.$$

The condition $\kappa \in \mathbb{N}[A]$ is redundant, given the condition $\kappa \in \mathbb{N}[S]$, so we are done. □

Having set down this abstract theorem and its corollaries, we are now ready to obtain p-adic estimates of weights as soon as we construct appropriate counting polynomials. We present our four main results in the next four chapters, each of which includes the construction of polynomials and the application of such polynomials with the abstract theorem (or one of its corollaries) to obtain weight congruences.

Chapter 4

Zero Counts, Hamming Weights, and Generic Weights in $\mathbb{Z}/p^d\mathbb{Z}[A]$

In this chapter, we investigate p-adic valuations of weights in Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$. Thus we set $e = 1$ throughout this chapter. The two main results we obtain are Theorems 4.18 and 4.21, specializations of which were presented in the Introduction as Theorems 1.8 and 1.7. We recall these specializations here:

Theorem 4.1 (Theorem 4.18, specialized). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, and $\mathrm{zer}(c) \not\equiv |A| \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$ for some $c \in \mathcal{C}$. Equivalently, $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, and $\mathrm{ham}(c) \not\equiv 0 \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$ for some $c \in \mathcal{C}$.*

Theorem 4.2 (Theorem 4.21, specialized). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Let $r \in \mathbb{Z}/p^d\mathbb{Z}$ with $r \neq 0$, and let $c \in \mathcal{C}$. Then the number of occurrences of the symbol r in the word c is a multiple of $p^{\ell^{ss}(\mathcal{C})}$.*

In order to understand these theorems, one must understand the definitions of $\ell^{ss}(\mathcal{C})$ and $\ell^{ss}_{mc}(\mathcal{C})$ given in Section 1.1 of the Introduction. The parameters $\ell^{ss}(\mathcal{C})$ and $\ell^{ss}_{mc}(\mathcal{C})$ are defined there using unity-product sequences of elements in the support of the Fourier transform of the code. In this chapter, and indeed in the rest of the thesis, they will be defined (equivalently) using multisets rather than sequences. For this reason, knowledge of the notations for accounts in Section 2.5 will be indispensable in this chapter.

The above theorems (or rather, more general forms of them) are proved using Corollary 3.4 and suitable counting polynomials. In Section 4.1, we introduce the Newton expansion,

which is the basic tool for constructing counting polynomials. In Section 4.2, we construct our counting polynomials. Note that we do not construct a single-variable polynomial f that approximates the lift of a weight function wt. That is, we do not construct $f(x) \in \mathbb{Q}_p[x]$ so that $f(r) \equiv \mathrm{wt}(\pi(r)) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$, and then use it with Corollary 3.5 to approximate weights. Rather, we construct a multivariable polynomial $f(x_0, \ldots, x_{d-1})$ that will approximate weights in a somewhat strange fashion, namely $f(r_0, \ldots, r_{d-1}) \equiv \mathrm{wt}(\pi(r_0 + pr_1 + \cdots + p^{d-1}r_{d-1})) \pmod{p^m}$ for all $r_0, \ldots, r_{d-1} \in \mathbb{Z}_p$. This polynomial is designed to respect the scoring system described in Section 1.1 of the Introduction. There the scoring system was described for use with sequences; in Section 4.2 the scoring system is defined (equivalently) in terms of multisets. In Section 4.2, we do not speak specifically about weight functions, but show how to make counting polynomials that approximate functions $F(x_0, \ldots, x_{d-1})$ that have the property that

$$\begin{aligned} F(x_0, x_1, \ldots, x_{d-2}, x_{d-1}) &= F(x_0 + p^d, x_1, \ldots, x_{d-2}, x_{d-1}) \\ &= F(x_0, x_1 + p^{d-1}, \ldots, x_{d-2}, x_{d-1}) \\ &= \cdots \\ &= F(x_0, x_1, \ldots, x_{d-2} + p^2, x_{d-1}) \\ &= F(x_0, x_1, \ldots, x_{d-2}, x_{d-1} + p). \end{aligned}$$

For any weight function $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$, the function $\mathrm{wt}(\pi(x_0 + px_1 + \cdots + p^{d-1}x_{d-1}))$ will have this property.

In Section 4.3, we introduce the notion of a *sectioned weight function*. For $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$, the sectioned weight function $\mathrm{wt}_{\mathrm{sec}}\colon (\mathbb{Z}/p^d\mathbb{Z})^d \to \mathbb{Z}$ is given by $\mathrm{wt}_{\mathrm{sec}}(r_0, \ldots, r_{d-1}) = \mathrm{wt}(r_0 + pr_1 + \cdots + p^{d-1}r_{d-1})$. Thus the polynomials developed in Section 4.2 approximate sectioned weight functions. Then Section 4.3 shows how the scaled Fourier-induced breakdown of codewords (introduced in Section 2.3) works together with the sectioned weight functions. Indeed, the scaled Fourier-induced breakdown expresses a codeword c as a linear combination $\sum_{i=0}^{d-1} p^i c^{(i)}$, and so $\mathrm{wt}(c) = \mathrm{wt}_{\mathrm{sec}}(c^{(0)}, \ldots, c^{(d-1)})$.

In Sections 4.4 and 4.5, we use our counting polynomials that approximate sectioned

weights, along with Corollary 3.4, to prove the theorems that are the goals of this chapter. In Section 4.4, we introduce the parameter $\ell^{ss}_{mc}(\mathcal{C})$ using multisets, and then prove Theorem 4.18, which is a generalized version of Theorem 1.8 (Theorem 4.1 above). In Section 4.5, we introduce the parameter $\ell^{ss}(\mathcal{C})$ using multisets, and then prove Theorem 4.21, which is a generalized version of Theorem 1.7 (Theorem 4.2 above).

Finally, in Section 4.6, we compare our results with previous ones. Since previous results used the parameters $\ell_{mc}(\mathcal{C})$ and $\ell(\mathcal{C})$ (see Section 1.1 of the Introduction), we introduce these parameters (using multisets here rather than the sequences of the Introduction). Then we compare (in Proposition 4.22) the relative magnitudes of $\ell(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C})$, thus enabling us to compare our results with past results.

4.1 Finite Differences and Newton Expansions

In this section, we let D stand for any subset of $\mathbb{Z}_p$ such that $r \in D$ implies $r+1 \in D$ (so D could be $\mathbb{N}$ or $\mathbb{Z}$ or all of $\mathbb{Z}_p$). We consider the $\mathbb{Q}_p$-vector space of functions $f\colon D \to \mathbb{Q}_p$. We define the *finite difference operator*, denoted Δ, to be the operator on this space with

$$(\Delta F)(x) = F(x+1) - F(x).$$

We also define the *translation (*or *shift) operator*, denoted T, to be the operator in this space with

$$(TF)(x) = F(x+1).$$

Note that $\Delta = T - \mathrm{Id}$, where Id is the identity operator.

We also let t be a positive integer and consider the $\mathbb{Q}_p$-vector space of functions of the form $F\colon D^t \to \mathbb{Q}_p$. We define the *finite difference operator in variable* x_k, denoted Δ_k, to be the operator on the space of such functions with

$$(\Delta_k F)(r_0, \ldots, r_{t-1}) = F(x_0, \ldots, x_{k-1}, 1+x_k, x_{k+1}, \ldots, x_{t-1}) - F(x_0, \ldots, x_{t-1}).$$

Similarly, we define the *translation (*or *shift) operator in variable* x_k, denoted T_k, to be the

operator in this space with

$$(T_k F)(x_0, \ldots, x_{t-1}) = F(x_x, \ldots, x_{k-1}, 1 + x_k, x_{k+1}, \ldots, x_{t-1}).$$

Note that $\Delta_k = T_k - \mathrm{Id}$.

For multivariable scenarios, we adopt the simplifying notation that for any letter a, the corresponding boldface letter $\mathbf{a}$ stands for the t-tuple $a_0, \ldots, a_{t-1}$. We also use the abbreviations $\mathbf{x}^{\mathbf{n}} = x_0^{n_0} \cdots x_{t-1}^{n_{t-1}}$ and

$$\binom{\mathbf{x}}{\mathbf{n}} = \binom{x_0}{n_0} \ldots \binom{x_{t-1}}{n_{t-1}}.$$

Furthermore, we set $\Delta^{\mathbf{n}} = \Delta_0^{n_0} \ldots \Delta_{t-1}^{n_{t-1}}$. For convenience, we introduce the t-tuples $\mathbf{e}^0, \ldots, \mathbf{e}^{t-1}$, where $\mathbf{e}_i^j = 0$ if $i \neq j$ and $\mathbf{e}_i^i = 1$. We also use $\mathbf{0}$ to represent the t-tuple of all zeroes. For any j-tuple $a_0, \ldots, a_{j-1}$, we use the notation $\mathrm{Box}(a_0, \ldots, a_{j-1})$ to denote the set $\{0, 1, \ldots, a_0\} \times \cdots \times \{0, 1, \ldots, a_{j-1}\}$.

Note that $\Delta_k^j = (T_k - \mathrm{Id})^j = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} T_k^i$. Also note that all the operators Δ_j and T_k are pairwise commutative. Furthermore, substitution of a number $b_j \in \mathbb{Z}_p$ for a variable x_j commutes with T_k and Δ_k if $k \neq j$. That is, if $j \neq k$, then

$$T_k(F(x_0, \ldots, x_{j-1}, b_j, x_{j+1}, \ldots, x_{t-1})) = (T_k F)(x_0, \ldots, x_{j-1}, b_j, x_{j+1}, \ldots, x_{t-1})$$

and

$$\Delta_k(F(x_0, \ldots, x_{j-1}, b_j, x_{j+1}, \ldots, x_{t-1})) = (\Delta_k F)(x_0, \ldots, x_{j-1}, b_j, x_{j+1}, \ldots, x_{t-1})$$

for all $b_j \in \mathbb{Z}_p$. In the following lemma, we note that the values that a function takes on $\mathbb{N}^t$ are deducible from the values of its finite differences at the origin:

Lemma 4.3. *Let $t \geq 1$, $F \colon D^t \to \mathbb{Q}_p$, and $\mathbf{b} \in \mathbb{N}^t$. Then*

$$F(\mathbf{b}) = \sum_{\mathbf{i} \in \mathrm{Box}(\mathbf{b})} (\Delta^{\mathbf{i}} F)(\mathbf{0}) \binom{\mathbf{b}}{\mathbf{i}}.$$

Proof. We induct on t. For $t = 1$, we must show that $F(b_0) = \sum_{i_0=0}^{b_0} (\Delta_0^{i_0} F)(0)\binom{b_0}{i_0}$. We use $\Delta_0^{i_0} = \sum_{j=0}^{i_0} (-1)^{i_0-j}\binom{i_0}{j} T_0^j$ to calculate

$$\sum_{i_0=0}^{b_0} (\Delta_0^{i_0} F)(0)\binom{b_0}{i_0} = \sum_{i_0=0}^{b_0}\sum_{j=0}^{i_0} (-1)^{i_0-j}\binom{i_0}{j} F(j)\binom{b_0}{i_0}.$$

Since $\binom{i_0}{j}\binom{b_0}{i_0} = \binom{b_0}{j}\binom{b_0-j}{i_0-j}$, we have

$$\begin{aligned}
\sum_{i_0=0}^{b_0} (\Delta_0^{i_0} F)(0)\binom{b_0}{i_0} &= \sum_{i_0=0}^{b_0}\sum_{j=0}^{i_0} (-1)^{i_0-j}\binom{b_0}{j}\binom{b_0-j}{i_0-j} F(j) \\
&= \sum_{j=0}^{b_0}\sum_{i_0=j}^{b_0} (-1)^{i_0-j}\binom{b_0}{j}\binom{b_0-j}{i_0-j} F(j) \\
&= \sum_{j=0}^{b_0} F(j)\binom{b_0}{j}\sum_{k=0}^{b_0-j} (-1)^k\binom{b_0-j}{k}.
\end{aligned}$$

But $\sum_{k=0}^{b_0-j} (-1)^k\binom{b_0-j}{k} = 0$ unless $j = b_0$ (in which case it is 1), so that

$$\sum_{i_0=0}^{b_0} (\Delta_0^{i_0} F)(0)\binom{b_0}{i_0} = F(b_0).$$

Now suppose that $t > 1$ and that the lemma holds for functions with $t-1$ or fewer variables. Set $G(x_0) = F(x_0, b_1, \ldots, b_{t-1})$, so that by the base case we have

$$G(b_0) = \sum_{i_0=0}^{b_0} (\Delta_0^{i_0} G)(0)\binom{b_0}{i_0},$$

or, since substitution of $b_1, \ldots, b_{t-1}$ for $x_1, \ldots, x_{t-1}$ commutes with application of Δ_0,

$$F(b_0, \ldots, b_{t-1}) = \sum_{i_0=0}^{b_0} (\Delta_0^{i_0} F)(0, b_1, \ldots, b_{t-1})\binom{b_0}{i_0}.$$

Define $F_j(x_1, \ldots, x_{t-1}) = (\Delta_0^j F)(0, x_1, \ldots, x_{t-1})$ for $j = 0, \ldots, b_0$, so that

$$F(b_0, \ldots, b_{t-1}) = \sum_{i_0=0}^{b_0} F_{i_0}(b_1, \ldots, b_{t-1})\binom{b_0}{i_0}.$$

Now apply the induction hypothesis to the functions F_{i_0} to obtain

$$F(b_0,\ldots,b_{t-1}) = \sum_{i_0=0}^{b_0}\sum_{i_1=0}^{b_1}\cdots\sum_{i_{t-1}=0}^{b_{t-1}} (\Delta_1^{i_1}\ldots\Delta_{t-1}^{i_{t-1}}F_{i_0})(0,\ldots,0)\binom{\mathbf{b}}{\mathbf{i}}. \tag{4.1}$$

But note that

$$\begin{aligned}(\Delta_1^{i_1}\ldots\Delta_{t-1}^{i_{t-1}}F_{i_0})&(\{x_1=0,\ldots,x_{t-1}=0\})\\ &= \left(\Delta_1^{i_1}\ldots\Delta_{t-1}^{i_{t-1}}\left[(\Delta_0^{i_0}F)(\{x_0=0\})\right]\right)(\{x_1=0,\ldots,x_{t-1}=0\}).\end{aligned}$$

Then use the fact that the substitution of the value 0 for the indeterminate x_0 commutes with the finite difference operators $\Delta_1,\ldots,\Delta_{t-1}$, and the fact that Δ_0 commutes with $\Delta_1,\ldots,\Delta_{t-1}$ to obtain

$$(\Delta_1^{i_1}\ldots\Delta_{t-1}^{i_{t-1}}F_{i_0})(0,\ldots,0) = (\Delta_0^{i_0}\ldots\Delta_{t-1}^{i_{t-1}}F)(0,\ldots,0),$$

which, with (4.1), completes the proof. □

Corollary 4.4. *Let $F\colon D^t \to \mathbb{Q}_p$ and $\mathbf{b}\in\mathbb{N}$. Then $f(\mathbf{x}) = \sum_{\mathbf{i}\in\mathrm{Box}(\mathbf{b})}\left(\Delta^{\mathbf{i}}F\right)(\mathbf{0})\binom{\mathbf{x}}{\mathbf{i}}$ is the unique polynomial in $\mathbb{Q}_p[\mathbf{x}]$ that agrees with F on $\mathrm{Box}(\mathbf{b})$ and whose degree in each indeterminate x_k is less than or equal to b_k.*

Proof. If we evaluate $f(\mathbf{x})$ at any point $\mathbf{a}\in\mathrm{Box}(\mathbf{b})$, we note that $\binom{a_i}{i_1} = 0$ if $i_1 > a_i$, and so we obtain

$$f(\mathbf{a}) = \sum_{\mathbf{i}\in\mathrm{Box}(\mathbf{a})}(\Delta^{\mathbf{i}}F)(\mathbf{0})\binom{\mathbf{a}}{\mathbf{i}},$$

which equals $F(\mathbf{a})$ by the lemma. Corollary 2.35 tells us that there is no other polynomial agreeing with F on $\mathrm{Box}(\mathbf{b})$ and having the degree of each x_k at most b_k. □

If $\{c_{\mathbf{i}}\}_{\mathbf{i}\in\mathbb{N}^t}$ is a family of elements of $\mathbb{Q}_p$, then

$$\sum_{\mathbf{i}\in\mathbb{N}^t} c_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$$

gives a well-defined function from $\mathbb{N}^t$ to $\mathbb{Q}_p$, because $\binom{a_j}{i_j} = 0$ if $i_j > a_j$, so that all but

finitely many terms vanish in our sum when we substitute $\mathbf{x} = \mathbf{a}$. Furthermore, if all the coefficients $c_{\mathbf{i}}$ are elements of $\mathbb{Z}_p$, then this function maps $\mathbb{N}^t$ into $\mathbb{Z}_p$, since each binomial coefficient maps $\mathbb{N}$ into $\mathbb{Z}_p$. In fact, we shall show that all functions from $\mathbb{N}^t$ to $\mathbb{Q}_p$ can be obtained in this form.

Proposition 4.5. *Let $F\colon \mathbb{N}^t \to \mathbb{Q}_p$. Then there exists a unique family $\{f_{\mathbf{i}}\}_{\mathbf{i}\in\mathbb{N}^t}$ of coefficients in $\mathbb{Q}_p$ such that*

$$F(\mathbf{x}) = \sum_{\mathbf{i}\in\mathbb{N}^t} f_{\mathbf{i}} \binom{\mathbf{x}}{\mathbf{i}}. \tag{4.2}$$

In fact, $f_{\mathbf{i}} = (\Delta^{\mathbf{i}} F)(\mathbf{0})$. Furthermore, for any $m \in \mathbb{Z}$, we have $F(\mathbb{N}^t) \subseteq p^m\mathbb{Z}_p$ if and only if $f_{\mathbf{i}} \in p^m\mathbb{Z}_p$ for all $\mathbf{i} \in \mathbb{N}^t$.

Proof. First we show that the proposed coefficients work. Let $\mathbf{b} \in \mathbb{N}^t$. Since $\binom{b_i}{i_1} = 0$ if $i_1 > b_i$, we have

$$\sum_{\mathbf{i}\in\mathbb{N}^t} (\Delta^{\mathbf{i}} F)(\mathbf{0}) \binom{\mathbf{b}}{\mathbf{i}} = \sum_{\mathbf{i}\in \mathrm{Box}(\mathbf{b})} (\Delta^{\mathbf{i}} F)(\mathbf{0}) \binom{\mathbf{b}}{\mathbf{i}},$$

but the last expression is equal to $F(\mathbf{b})$ by Lemma 4.3 above.

To show uniqueness it suffices to show that if $\{c_{\mathbf{i}}\}_{\mathbf{i}\in\mathbb{N}^t}$ is a family of coefficients in $\mathbb{Q}_p$, not all zero, then the function

$$C(\mathbf{x}) = \sum_{\mathbf{i}\in\mathbb{N}^t} c_{\mathbf{i}} \binom{\mathbf{x}}{\mathbf{i}}$$

does not vanish everywhere. Choose $\mathbf{j}$ subject to $c_{\mathbf{j}} \neq 0$ and $j_0 + \cdots + j_{t-1}$ minimal. Then

$$C(\mathbf{j}) = \sum_{\mathbf{i}\in \mathrm{Box}(\mathbf{j})} c_{\mathbf{i}} \binom{\mathbf{j}}{\mathbf{i}},$$

since $\binom{j_k}{i_k}$ vanishes when $i_k > j_k$ for any k. But by the minimality property of $\mathbf{j}$, all terms in the summation have $c_{\mathbf{i}} = 0$, except the term with $\mathbf{i} = \mathbf{j}$. So $C(\mathbf{j}) = c_{\mathbf{j}} \neq 0$.

Finally, if $m \in \mathbb{Z}$ and if all the coefficients $f_{\mathbf{i}}$ are in $p^m\mathbb{Z}_p$, then clearly F maps all of $\mathbb{N}^t$ into $p^m\mathbb{Z}_p$, since the binomial coefficient polynomials map $\mathbb{N}$ into $\mathbb{N}$. Conversely, if $m \in \mathbb{Z}$ and F maps all of $\mathbb{N}^t$ into $p^m\mathbb{Z}_p$, then all the finite differences $f_{\mathbf{i}} = (\Delta^{\mathbf{i}} F)(\mathbf{0})$ are also in $p^m\mathbb{Z}_p$. □

We call the expansion in (4.2) the *Newton expansion* of the function F. If $G\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$,

we define the Newton expansion of G to be the Newton expansion of the restriction of G to $\mathbb{N}^t$. The coefficients in the expansion are called the *Newton coefficients*. In general, the Newton expansion of $G\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$ need not agree with G on ${\mathbb{Z}_p}^t \smallsetminus \mathbb{N}^t$ (e.g., consider what happens if G is the characteristic function of $\mathbb{N}^t$), but the general case will not concern us. We are interested in approximating certain well-behaved functions with polynomials. We say that a polynomial $f(\mathbf{x}) \in \mathbb{Q}_p[\mathbf{x}]$ *approximates G (uniformly) modulo p^m on ${\mathbb{Z}_p}^t$* to mean that $f(\mathbf{r}) \equiv G(\mathbf{r}) \pmod{p^m}$ for all $\mathbf{r} \in {\mathbb{Z}_p}^t$. The following lemma shows that we can obtain polynomial approximations to G in certain circumstances by truncating the Newton expansion:

Lemma 4.6. *Let $F\colon {\mathbb{Z}_p}^t \to \mathbb{Q}_p$ be a p-adically continuous function and let $\sum_{\mathbf{i}\in\mathbb{N}^t} f_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$ be its Newton expansion. Suppose that there is some finite subset S of $\mathbb{N}^t$ such that $f_{\mathbf{i}} \equiv 0 \pmod{m}$ for all $\mathbf{i} \notin S$. Then the polynomial $f(\mathbf{x}) = \sum_{\mathbf{i}\in S} f_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$ has the property that $f(\mathbf{b}) \equiv F(\mathbf{b}) \pmod{p^m}$ for all $\mathbf{b} \in {\mathbb{Z}_p}^t$.*

Proof. Let $G(\mathbf{x}) = F(\mathbf{x}) - f(\mathbf{x})$. We want to show that G maps all of ${\mathbb{Z}_p}^t$ into $p^m\mathbb{Z}_p$, i.e., that $G^{-1}(p^m\mathbb{Z}_p) = {\mathbb{Z}_p}^t$. Note that G has a Newton expansion whose coefficients all vanish modulo p^m, so by Proposition 4.5, G maps $\mathbb{N}^t$ into $p^m\mathbb{Z}_p$, i.e., $\mathbb{N}^t \subseteq G^{-1}(p^m\mathbb{Z}_p)$. Also note G is p-adically continuous since F (as given) and f (a polynomial) are continuous. Note that $p^m\mathbb{Z}_p$ is a closed subset of $\mathbb{Q}_p$ in the p-adic topology, so $G^{-1}(p^m\mathbb{Z}_p)$ is a closed set. So we know that $G^{-1}(p^m\mathbb{Z}_p)$ is a closed set containing $\mathbb{N}^t$, but $\mathbb{N}^t$ is a dense subset of ${\mathbb{Z}_p}^t$, so $G^{-1}(p^m\mathbb{Z}_p) = {\mathbb{Z}_p}^t$. □

In the next section, we shall be concerned with functions invariant under certain translations. Thus it will be important to know the effects of translation on the Newton expansion of a function. The reader should recall our compact vectorial notations introduced at the beginning of this section.

Lemma 4.7. *Let $F\colon D^t \to \mathbb{Z}_p$ have Newton expansion $\sum_{\mathbf{i}\in\mathbb{N}^t} f_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$, let $k \in \{0, 1, \ldots, t-1\}$, and let $j \in \mathbb{N}$. Then the translated function $T_k^j F$ has Newton expansion $\sum_{\mathbf{i}\in\mathbb{N}^t} g_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$ with coefficients $g_{\mathbf{i}} = \sum_{h=0}^{j}\binom{j}{h} f_{\mathbf{i}+h\mathbf{e}^k}$.*

Proof. We prove this by induction on j. The $j = 0$ case is trivial. Suppose $j = 1$. Let $\mathbf{b} \in \mathbb{N}^t$ be given. Then

$$(T_k F)(\mathbf{b}) = \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}} \binom{\mathbf{b} + \mathbf{e}^k}{\mathbf{i}}.$$

Now we use Pascal's identity $\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1}$ to obtain

$$(T_k F)(\mathbf{b}) = \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}} \left[\binom{\mathbf{b}}{\mathbf{i}} + \binom{\mathbf{b}}{\mathbf{i} - \mathbf{e}^k} \right],$$

so that

$$(T_k F)(\mathbf{b}) = \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}} \binom{\mathbf{b}}{\mathbf{i}} + \sum_{\mathbf{i} \in \mathbb{N}} f_{\mathbf{i}} \binom{\mathbf{b}}{\mathbf{i} - \mathbf{e}^k},$$

since all but finitely many terms of these sequences vanish. Recall the convention that $\binom{x}{-1} = 0$, so we have

$$\begin{aligned}
(T_k F)(\mathbf{b}) &= \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}} \binom{\mathbf{b}}{\mathbf{i}} + \sum_{\substack{\mathbf{i} \in \mathbb{N}^t \\ i_k \geq 1}} f_{\mathbf{i}} \binom{\mathbf{b}}{\mathbf{i} - \mathbf{e}^k} \\
&= \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}} \binom{\mathbf{b}}{\mathbf{i}} + \sum_{\mathbf{i} \in \mathbb{N}^t} f_{\mathbf{i}+\mathbf{e}^k} \binom{\mathbf{b}}{\mathbf{i}} \\
&= \sum_{\mathbf{i} \in \mathbb{N}^t} \left(f_{\mathbf{i}} + f_{\mathbf{i}+\mathbf{e}^k} \right) \binom{\mathbf{b}}{\mathbf{i}},
\end{aligned}$$

which proves our lemma in the case $j = 1$.

Now suppose $j > 1$. Let $\Phi = T_k^{j-1} F$, which has Newton expansion $\sum_{\mathbf{i} \in \mathbb{N}^t} \varphi_{\mathbf{i}} \binom{\mathbf{x}}{\mathbf{i}}$ with $\varphi_{\mathbf{i}} = \sum_{h=0}^{j-1} \binom{j-1}{h} f_{\mathbf{i}+h\mathbf{e}^k}$. By the base case proved above, the Newton expansion of $T_k \Phi = T_k^j F$ is $\sum_{\mathbf{i} \in \mathbb{N}^t} g_{\mathbf{i}} \binom{\mathbf{x}}{\mathbf{i}}$ with $g_{\mathbf{i}} = \varphi_{\mathbf{i}} + \varphi_{\mathbf{i}+\mathbf{e}^k}$. So, recalling our convention that $\binom{x}{-1} = 0$ and Pascal's identity, we have

$$\begin{aligned}
g_{\mathbf{i}} &= \sum_{h=0}^{j-1} \binom{j-1}{h} f_{\mathbf{i}+h\mathbf{e}^k} + \sum_{h=0}^{j-1} \binom{j-1}{h} f_{\mathbf{i}+(h+1)\mathbf{e}^k} \\
&= \sum_{h=0}^{j} \left(\binom{j-1}{h} + \binom{j-1}{h-1} \right) f_{\mathbf{i}+h\mathbf{e}^k} \\
&= \sum_{h=0}^{j} \binom{j}{h} f_{\mathbf{i}+h\mathbf{e}^k}.
\end{aligned}$$

□

4.2 Construction of Counting Polynomials

Now we use Newton expansions and Lemma 4.6 to make polynomials that will be used to p-adically approximate weights. For a positive integer t, consider a function $F(x_0, \ldots, x_{t-1})$ from ${\mathbb{Z}_p}^t$ to $\mathbb{Q}_p$. We say that F is (p,t)-*periodic* if

$$T_0^{p^t} F = T_1^{p^{t-1}} F = \cdots = T_{t-1}^{p} F = F.$$

Note that such functions are p-adically continuous; in fact, they are constant on a sufficiently small neighborhood of any given point.

Given a t-tuple of integers $\mathbf{n} = (n_0, \ldots, n_{t-1})$, we define $|\mathbf{n}| = n_0 + \cdots + n_{t-1}$, and if all the elements of the t-tuple are nonnegative, we define $\mathbf{n}! = n_0! n_1! \cdots n_{t-1}!$. We define the *score* of $\mathbf{n}$, denoted $\mathrm{Sc}(\mathbf{n})$, to be

$$\mathrm{Sc}(n_0, \ldots, n_{t-1}) = \sum_{i=0}^{t-1} p^i n_i.$$

Note that for any $\mathbf{n}$, we have

$$\mathrm{Sc}\,(\mathbf{n}) \equiv |\mathbf{n}| \pmod{p-1}. \tag{4.3}$$

For $s \in \mathbb{N}$ and $\mathbf{n} \in \mathbb{Z}^t$, we define the *s-tier* of $\mathbf{n}$, denoted $\mathrm{Ti}_s(\mathbf{n})$, to be

$$\mathrm{Ti}_s(n_0, \ldots, n_{t-1}) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(n_0, \ldots, n_{t-1}) - p^{s-1}}{(p-1)p^{s-1}} \right\rfloor \right\}.$$

In this section, we shall always want to calculate the t-tiers of t-tuples.

For $k \in \{0, 1, \ldots, t-1\}$, a t-tuple $\mathbf{n} = (n_0, \ldots, n_{t-1})$ is said to be *k-starting* if $n_0 = \cdots = n_{k-1} = 0$ and $n_k \neq 0$. The t-tuple $\mathbf{n}$ is said to be *k-critical* if it is k-starting and $\mathrm{Ti}_t\left(\mathbf{n} + \mathbf{e}^k\right) > \mathrm{Ti}_t\left(\mathbf{n}\right)$. A t-tuple is said to be *critical* if it is k-critical for any $k \in \{0, 1, \ldots, t-1\}$. The critical t-tuples will be important when we want to prove the sharpness of our bounds on p-adic valuations of weights. We first give a characterization of critical t-tuples.

Lemma 4.8. *Let* $k \in \{0, 1, \ldots, t-1\}$ *and let* $\mathbf{n} = (n_0, \ldots, n_{t-1}) \in \mathbb{N}^t$. *Then* $\mathbf{n}$ *is* k*-critical if and only if it is* k*-starting and* $\mathrm{Sc}(\mathbf{n}) = [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1} - p^k$. *Thus* $|\mathbf{n}| \equiv \mathrm{Sc}(\mathbf{n}) \equiv 0 \pmod{p-1}$ *if* $\mathbf{n}$ *is* k*-critical. If* $\mathbf{n}$ *is* k*-critical and* $n_k, \ldots, n_{t-2} < p$, *then* $n_k = \cdots = n_{t-2} = p-1$ *and* $n_{t-1} = (p-1)(\mathrm{Ti}_t(\mathbf{n}) + 1)$.

Proof. Suppose that $\mathbf{n}$ is k-critical. By definition $\mathbf{n}$ is k-starting, and furthermore, we have $\mathrm{Ti}_t\left(\mathbf{n} + \mathbf{e}^k\right) > \mathrm{Ti}_t(\mathbf{n})$, so that $\mathrm{Sc}\left(\mathbf{n} + \mathbf{e}^k\right) \geq [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1}$. Thus

$$\mathrm{Sc}(\mathbf{n}) \geq [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1} - p^k.$$

On the other hand, by the definition of t-tier,

$$\mathrm{Sc}(\mathbf{n}) < [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1}.$$

$\mathrm{Sc}(\mathbf{n})$ is a multiple of p^k since $\mathbf{n}$ is k-starting. But there is only one multiple of p^k that satisfies both our inequalities for $\mathrm{Sc}(\mathbf{n})$, namely, $\mathrm{Sc}(\mathbf{n}) = [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1} - p^k$. Note that this score is divisible by $p-1$ and that $\mathrm{Sc}(\mathbf{n}) \equiv |\mathbf{n}| \pmod{p-1}$ by (4.3).

Conversely, suppose $\mathbf{n}$ is k-starting and $\mathrm{Sc}(\mathbf{n}) = [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1} - p^k$. Then $\mathrm{Sc}\left(\mathbf{n} + \mathbf{e}^k\right) = [(\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1) + 1]\, p^{t-1}$, so that $\mathrm{Ti}_t\left(\mathbf{n} + \mathbf{e}^k\right) = \mathrm{Ti}_t(\mathbf{n}) + 1 > \mathrm{Ti}_t(\mathbf{n})$. So $\mathbf{n}$ is k-critical.

Now suppose $\mathbf{n}$ is k-critical and $n_k, \ldots, n_{t-2} < p$. By the first part of the lemma, we know that $\mathrm{Sc}(\mathbf{n}) \equiv p^{t-1} - p^k \pmod{p^{t-1}}$, so that $n_k p^k + \cdots + n_{t-2} p^{t-2} \equiv p^{t-1} - p^k \pmod{p^{t-1}}$. By the upper bounds on $n_k, \ldots, n_{t-2}$, we have $0 \leq n_k p^k + \cdots + n_{t-2} p^{t-2} \leq p^{t-1} - p^k$, which is a range shorter in length that p^{t-1}. Therefore, our congruence modulo p^{t-1} for $n_k p^k + \cdots + n_{t-2} p^{t-2}$ exactly determines the value to be $p^{t-1} - p^k$, which forces $n_k = \cdots = n_{t-2} = p-1$. Thus $\mathrm{Sc}(\mathbf{n}) = (n_{t-1}+1)p^{t-1} - p^k$, and the first part of this lemma then tells us that $n_{t-1} = (\mathrm{Ti}_t(\mathbf{n}) + 1)(p-1)$. □

The next two lemmas show that the coefficients in the Newton expansion of a (p,t)-periodic function satisfy certain recursion relations. These relations are used to show that the Newton coefficients $f_{\mathbf{i}}$ of a (p,t)-periodic function tend to zero (in the p-adic sense) as $\mathrm{Sc}(\mathbf{i})$ tends to infinity.

Lemma 4.9. *Let $F\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$ be (p,t)-periodic with Newton expansion $\sum_{\mathbf{i}\in\mathbb{N}^t} f_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$, let $k \in \{0,1,\ldots,t-2\}$, and let $\mathbf{h} \in \mathbb{N}^t$ with $h_k \geq p$. Then $f_{\mathbf{h}-p\mathbf{e}^k+\mathbf{e}^{k+1}} = f_{\mathbf{h}} + \sum_{j=1}^{p-1}\binom{p}{j} f_{\mathbf{h}-j\mathbf{e}^k}$.*

Proof. Since F is (p,t)-periodic, we have $T_k^p F = T_{k+1}F$. Then employ Lemma 4.7 on both sides of this equation to compute the Newton coefficient for the $(\mathbf{h}-p\mathbf{e}^k)$-term (i.e., the coefficient in front of $\binom{\mathbf{x}}{\mathbf{h}-p\mathbf{e}^k}$ in the Newton expansion). We obtain

$$\sum_{i=0}^{p}\binom{p}{i} f_{\mathbf{h}-p\mathbf{e}^k+i\mathbf{e}^k} = \sum_{j=0}^{1}\binom{1}{j} f_{\mathbf{h}-p\mathbf{e}^k+j\mathbf{e}^{k+1}}.$$

The $i=0$ term on the left matches the $j=0$ term on the right, and the $i=p$ term on the left is just $f_{\mathbf{h}}$, so we get

$$f_{\mathbf{h}} + \sum_{i=1}^{p-1}\binom{p}{i} f_{\mathbf{h}-p\mathbf{e}^k+i\mathbf{e}^k} = f_{\mathbf{h}-p\mathbf{e}^k+\mathbf{e}^{k+1}}.$$

Now re-index the sum on the left with $j=p-i$ to obtain what we were to prove. □

Lemma 4.10. *Let $F\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$ be (p,t)-periodic with Newton expansion $\sum_{\mathbf{i}\in\mathbb{N}^t} f_{\mathbf{i}}\binom{\mathbf{x}}{\mathbf{i}}$, and let $\mathbf{h} \in \mathbb{N}^t$ with $h_{t-1} \geq p$. Then $f_{\mathbf{h}} + \sum_{j=1}^{p-1}\binom{p}{j} f_{\mathbf{h}-j\mathbf{e}^{t-1}} = 0$.*

Proof. Since F is (p,t)-periodic, we have $T_{t-1}^p F = F$. Then employ Lemma 4.7 on the left-hand side to compute the Newton coefficient for the $(\mathbf{h}-p\mathbf{e}^{t-1})$-term (i.e., the coefficient in front of $\binom{\mathbf{x}}{\mathbf{h}-p\mathbf{e}^{t-1}}$ in the Newton expansion). We obtain

$$\sum_{i=0}^{p}\binom{p}{i} f_{\mathbf{h}-p\mathbf{e}^{t-1}+i\mathbf{e}^{t-1}} = f_{\mathbf{h}-p\mathbf{e}^{t-1}}.$$

The $i=0$ term on the left matches the right-hand side, and the $i=p$ term on the left is just $f_{\mathbf{h}}$, so we get

$$f_{\mathbf{h}} + \sum_{i=1}^{p-1}\binom{p}{i} f_{\mathbf{h}-p\mathbf{e}^{t-1}+i\mathbf{e}^{t-1}} = 0.$$

Now re-index the sum on the left with $j=p-i$ to obtain what we were to prove. □

Now we show that the above recursions force the Newton coefficients $f_{\mathbf{i}}$ of a (p,t)-periodic function F to decay (p-adically) as the t-tier of $\mathbf{i}$ increases. Furthermore, we obtain some

additional information on $f_{\mathbf{i}}$ when $\mathbf{i}$ is critical. This latter information will be critical in proofs of the sharpness of certain of our bounds on the p-adic valuations of weights in codes.

Theorem 4.11. *Let $F\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$ be (p,t)-periodic with Newton expansion $\sum_{\mathbf{n}\in\mathbb{N}^t} f_{\mathbf{n}}\binom{\mathbf{x}}{\mathbf{n}}$. Then $v_p(f_{\mathbf{n}}) \geq \mathrm{Ti}_t(\mathbf{n})$ for all $\mathbf{n} \in \mathbb{N}$. Furthermore, suppose that*

$$F(r_0,\ldots,r_{t-1}) = \begin{cases} 1 & \text{if } r_0 + pr_1 + \cdots + p^{t-1}r_{t-1} \equiv 0 \pmod{p^t}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.4}$$

for all $r_0,\ldots,r_{t-1} \in \mathbb{Z}_p$. Then $f_{\mathbf{0}} = 1$, and if $\mathbf{n}$ is critical, we have $f_{\mathbf{n}} \equiv (-p)^{\mathrm{Ti}_t(\mathbf{n})} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}}$.

Proof. First we devise a well-ordering relation $\preceq$ on $\mathbb{N}^t$, and then we induct with respect to the ordering. If $\mathbf{m},\mathbf{n} \in \mathbb{N}^t$ with $\mathrm{Sc}(\mathbf{m}) < \mathrm{Sc}(\mathbf{n})$, then $\mathbf{m} \prec \mathbf{n}$. Among the elements of $\mathbb{N}^t$ that have the same score, we order them lexicographically, i.e., $(m_0,\ldots,m_{t-1}) \prec (n_0,\ldots,n_{t-1})$ means that there is some i such that the two t-tuples agree in positions 0 to $i-1$, but $m_i < n_i$. There are only finitely many elements of $\mathbb{N}^t$ with a given score, so the lexicographic ordering well-orders the elements of like score. Thus $\prec$ is a well-ordering relation.

First we prove the lower bound on the p-adic valuation of the Newton coefficients by induction with respect to our ordering. By Proposition 4.5, we know that all Newton coefficients of F are in $\mathbb{Z}_p$, and there is nothing more to show for those elements, such as $(0,\ldots,0)$, whose t-tier is zero. So assume that $\mathbf{n} = (n_0,\ldots,n_{t-1})$ with $\mathrm{Ti}_t(\mathbf{n}) > 0$, or equivalently, that $\mathrm{Sc}(\mathbf{n}) \geq p^d$.

Let us first examine the case when $n_j \geq p$ for some $j < t-1$. By Lemma 4.9 above, we have

$$f_{\mathbf{n}-p\mathbf{e}^j+\mathbf{e}^{j+1}} = f_{\mathbf{n}} + \sum_{i=1}^{p-1} \binom{p}{i} f_{\mathbf{n}-i\mathbf{e}^j}.$$

Then note that $\mathbf{n} - p\mathbf{e}^j + \mathbf{e}^{j+1}$ has the same score (and thus the same t-tier) as $\mathbf{n}$, but

$\mathbf{n} - p\mathbf{e}^j + \mathbf{e}^{j+1} \prec \mathbf{n}$. Therefore, by induction $v_p\left(f_{\mathbf{n}} - p\mathbf{e}^j + \mathbf{e}^{j+1}\right) \geq \mathrm{Ti}_t(\mathbf{n})$. So

$$f_{\mathbf{n}} + \sum_{i=1}^{p-1} \binom{p}{i} f_{\mathbf{n}-i\mathbf{e}^j} \equiv 0 \pmod{p^{\mathrm{Ti}_t(\mathbf{n})}}. \tag{4.5}$$

Now note that the t-tuples $\mathbf{n} - i\mathbf{e}^j$ in the sum over i have strictly lower scores than $\mathbf{n}$, but $\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^j) = \mathrm{Sc}(\mathbf{n}) - ip^j \geq \mathrm{Sc}(\mathbf{n}) - (p-1)p^{t-1}$, since $i \leq p-1$ and $j \leq t-1$. Thus $\mathrm{Ti}_t\left(\mathbf{n} - i\mathbf{e}^j\right) \geq \mathrm{Ti}_t(\mathbf{n}) - 1$ for $i = 1, \ldots, p-1$. Then, since $\mathbf{n} - i\mathbf{e}^j \prec \mathbf{n}$, we can use the induction hypothesis to say that $v_p\left(f_{\mathbf{n}-i\mathbf{e}^j}\right) \geq \mathrm{Ti}_t(\mathbf{n}) - 1$. On the other hand, all the binomial coefficients $\binom{p}{i}$ with $0 < i < p$ are divisible by p, so the terms of the sum over i in (4.5) all have p-adic valuation at least $\mathrm{Ti}_t(\mathbf{n})$. So $f_{\mathbf{n}} \equiv 0 \pmod{p^{\mathrm{Ti}_t(\mathbf{n})}}$.

Next we examine the case when $n_j < p$ for all $j < t-1$. Then $\mathrm{Sc}(\mathbf{n}) < p^{t-1} + n_{t-1}p^{t-1}$, but since $\mathrm{Ti}_t(\mathbf{n}) > 0$, we must have $n_{t-1} \geq p$. We now apply Lemma 4.10 to obtain

$$f_{\mathbf{n}} + \sum_{i=1}^{p-1} \binom{p}{i} f_{\mathbf{n}-i\mathbf{e}^{t-1}} = 0. \tag{4.6}$$

Now note that the t-tuples $\mathbf{n} - i\mathbf{e}^{t-1}$ in the sum over i have strictly lower scores than $\mathbf{n}$, but $\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^{t-1}) \geq \mathrm{Sc}(\mathbf{n}) - (p-1)p^{t-1}$, since $i \leq p-1$. Thus $\mathrm{Ti}_t\left(\mathbf{n} - i\mathbf{e}^{t-1}\right) \geq \mathrm{Ti}_t(\mathbf{n}) - 1$ for $i = 1, \ldots, p-1$. Then, since $\mathbf{n} - i\mathbf{e}^{t-1} \prec \mathbf{n}$, we can use the induction hypothesis to say that $v_p\left(f_{\mathbf{n}-i\mathbf{e}^{t-1}}\right) \geq \mathrm{Ti}_t(\mathbf{n}) - 1$. On the other hand, all the binomial coefficients $\binom{p}{i}$ with $0 < i < p$ are divisible by p, so the terms of the sum over i in (4.6) all have p-adic valuation at least $\mathrm{Ti}_t(\mathbf{n})$. So $f_{\mathbf{n}} \equiv 0 \pmod{p^{\mathrm{Ti}_t(\mathbf{n})}}$. This completes the induction proof of the lower bound on p-adic valuations of coefficients.

Now suppose that F satisfies (4.4). Then $f_{\mathbf{0}} = (\Delta^{\mathbf{0}}F)(\mathbf{0}) = F(\mathbf{0}) = 1$. We prove the congruence for Newton coefficients with critical indices by induction with respect to our ordering. For the base of our induction, we shall prove the congruence for all critical $\mathbf{n} = (n_0, \ldots, n_{t-1})$ with $n_i < p$ for all i. So suppose that $k \in \{0, 1, \ldots, t-1\}$ and $\mathbf{n} = (n_0, \ldots, n_{t-1})$ is k-critical with $n_i < p$ for all i. Then by Lemma 4.8 above, we have $n_0 = \cdots = n_{k-1} = 0$, $n_k = \cdots = n_{t-2} = p-1$, and $n_{t-1} = (p-1)\left(\mathrm{Ti}_t(\mathbf{n}) + 1\right)$. This forces $\mathrm{Ti}_t(\mathbf{n}) = 0$ and $n_{t-1} = p-1$. So $n_0 = \cdots = n_{k-1} = 0$ and $n_k = \cdots = n_{t-1} = p-1$ and we

must show $f_{\mathbf{n}} \equiv 1 \pmod{p}$. Let $S = \{0, 1, \ldots, p-1\}$ and consider truncation

$$f(x_0, \ldots, x_{t-1}) = \sum_{i_k, \ldots, i_{t-1} \in S} f_{0,\ldots,0,i_k,\ldots,i_{t-1}} \binom{x_k}{i_k} \cdots \binom{x_{t-1}}{i_{t-1}} \tag{4.7}$$

of the Newton expansion for F. By Corollary 4.4, this polynomial agrees with $F(x_1, \ldots, x_t)$ on the set $U = \{(r_0, \ldots, r_t) : r_0 = \cdots = r_{k-1} = 0, r_k \in S, \ldots, r_{t-1} \in S\}$. That is,

$$f(r_0, \ldots, r_{t-1}) = \begin{cases} 1 & \text{if } r_0 + \cdots + p^{t-1} r_{t-1} \equiv 0 \pmod{p^t}, \\ 0 & \text{otherwise,} \end{cases}$$

for all $\mathbf{r} \in U$. This is equivalent to saying that

$$f(r_0, \ldots, r_{t-1}) = \begin{cases} 1 & \text{if } r_k + \cdots + p^{t-k-1} r_{t-1} \equiv 0 \pmod{p^{t-k}}, \\ 0 & \text{otherwise,} \end{cases}$$

for all $\mathbf{r} \in U$. But the only way that $r_k + \cdots + p^{t-k-1} r_{t-1}$ can vanish modulo p^{t-k} as we vary $r_k, \ldots, r_{t-1}$ over $S = \{0, 1, \ldots, p-1\}$ is for $r_k = \cdots = r_{t-1} = 0$. That is

$$f(r_0, \ldots, r_{t-1}) = \begin{cases} 1 & \text{if } r_k = \cdots = r_{t-1} = 0, \\ 0 & \text{otherwise,} \end{cases}$$

for all $\mathbf{r} \in U$. Lemma 4.4 also tells us that $f(x_1, \ldots, x_t)$ is the unique polynomial in $\mathbb{Q}_p[x_k, \ldots, x_{t-1}]$ of degree at most $p-1$ in each indeterminate that takes these values on U. So we know that

$$f(x_1, \ldots, x_t) = \prod_{i=k}^{t-1} (-1)^{p-1} \binom{x_i - 1}{p-1}.$$

Note that the coefficient of the monomial $x_k^{p-1} \cdots x_{t-1}^{p-1}$ in $f(x_1, \ldots, x_{t-1})$ is $\left(\frac{(-1)^{p-1}}{(p-1)!}\right)^{t-k}$. But the only term in the definition (4.7) of f that can give rise to a monomial of this degree is the term with $i_k = \cdots = i_{t-1} = p-1$, and so, matching coefficients, we see that $f_{\mathbf{n}} = (-1)^{(p-1)(t-k)} \equiv 1 \pmod{p}$.

Now the induction step. We suppose that $\mathbf{n} = (n_0, \ldots, n_{t-1})$ is k-critical and has $n_j \geq p$

for some j. We first examine the case when $j < t-1$. Of course $j \geq k$ since $n_i = 0$ for $i < k$. In this case, consider the t-tuple $\mathbf{m} = \mathbf{n} - p\mathbf{e}^j + \mathbf{e}^{j+1}$. This new t-tuple has the same score (and therefore the same t-tier) as $\mathbf{n}$, but it is lexicographically lower, hence $\mathbf{m} \prec \mathbf{n}$. By Lemma 4.9 above, we have

$$f_{\mathbf{m}} = f_{\mathbf{n}} + \sum_{i=1}^{p-1} \binom{p}{i} f_{\mathbf{n}-i\mathbf{e}^j}. \tag{4.8}$$

Now note that the t-tuples $\mathbf{n} - i\mathbf{e}^j$ in the sum over i have strictly lower scores than $\mathbf{n}$, but $\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^j) = \mathrm{Sc}\,(\mathbf{n}) - ip^j \geq \mathrm{Sc}\,(\mathbf{n}) - (p-1)p^j$, since $i \leq p-1$. By Lemma 4.8, $\mathrm{Sc}\,(\mathbf{n}) = [(\mathrm{Ti}_t\,(\mathbf{n}) + 1)\,(p-1) + 1]\,p^{t-1} - p^k$, so that

$$\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^j) \geq [(\mathrm{Ti}_t\,(\mathbf{n}) + 1)\,(p-1) + 1]\,p^{t-1} - p^k - (p-1)p^j$$

for $i = 1, \ldots, p-1$. Thus $\mathrm{Ti}_t\left(\mathbf{n} - i\mathbf{e}^j\right) \geq \left\lfloor \mathrm{Ti}_t\,(\mathbf{n}) + 1 - \frac{p^k + (p-1)p^j}{(p-1)p^{t-1}} \right\rfloor$ for $i = 1, \ldots, p-1$. But recall that $k \leq j < t-1$, so that $p^k + (p-1)p^j \leq p^{j+1} \leq p^{t-1}$, so that $\mathrm{Ti}_t\left(\mathbf{n} - i\mathbf{e}^j\right) = \mathrm{Ti}_t\,(\mathbf{n})$ for $i = 1, \ldots, p-1$. Thus, by the first part of the theorem, we have $v_p\,(f_{\mathbf{n}-i\mathbf{e}^j}) \geq \mathrm{Ti}_t\,(\mathbf{n})$ for $i = 1, \ldots, p-1$. Since the binomial coefficients $\binom{p}{i}$ with $0 < i < p$ are divisible by p, this means that all the terms in the sum over i in (4.8) vanish modulo $p^{\mathrm{Ti}_t(\mathbf{n})+1}$. So

$$f_{\mathbf{m}} \equiv f_{\mathbf{n}} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}} \tag{4.9}$$

Now we claim that $\mathbf{m} = \mathbf{n} - p\mathbf{e}^j + \mathbf{e}^{j+1}$ is k-starting. Since $\mathbf{n}$ is k-starting, this is obvious if $j > k$. Otherwise we would have $k = j < t-1$, and then note that $\mathrm{Sc}\,(\mathbf{n}) \equiv -p^k \pmod{p^{k+1}}$ by Lemma 4.8, which implies that $n_k \equiv -1 \pmod{p}$; since $p \leq n_j = n_k$, this means that $n_k \geq 2p-1$, so that $m_k \geq p-1 > 0$. Thus $\mathbf{m}$ is indeed k-starting. Also recall that $\mathrm{Sc}\,(\mathbf{m}) = \mathrm{Sc}\,(\mathbf{n})$, so Lemma 4.8 tells us that $\mathbf{m}$ is k-critical like $\mathbf{n}$. Since $\mathbf{m} \prec \mathbf{n}$ with $\mathrm{Ti}_t\,(\mathbf{m}) = \mathrm{Ti}_t\,(\mathbf{n})$, the induction hypothesis tells us that $f_{\mathbf{m}} \equiv (-p)^{\mathrm{Ti}_t(\mathbf{n})} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}}$. This, combined with (4.9), completes the induction step in the case where $n_j \geq p$ for some $j < t-1$.

So we are left to analyze the case where $\mathbf{n}$ is a k-critical t-tuple with $n_{t-1} \geq p$ and

$n_j < p$ for all $j < t-1$. We now apply Lemma 4.10 to obtain

$$f_{\mathbf{n}} + \sum_{i=1}^{p-1} \binom{p}{i} f_{\mathbf{n}-i\mathbf{e}^{t-1}} = 0. \tag{4.10}$$

Now note that the t-tuples $\mathbf{n} - i\mathbf{e}^{t-1}$ in the sum over i have strictly lower scores than $\mathbf{n}$. If $0 < i \leq p-2$, then $\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^{t-1}) \geq \mathrm{Sc}\,(\mathbf{n}) - (p-2)p^{t-1}$. By Lemma 4.8, $\mathrm{Sc}\,(\mathbf{n}) \geq (\mathrm{Ti}_t\,(\mathbf{n}) + 1)\,(p-1)p^{t-1}$, so that $\mathrm{Sc}(\mathbf{n} - i\mathbf{e}^{t-1}) \geq [\mathrm{Ti}_t\,(\mathbf{n})(p-1) + 1]\,p^{t-1}$ for $0 < i \leq p-2$. Therefore, $\mathrm{Ti}_t\left(\mathbf{n} - i\mathbf{e}^{t-1}\right) \geq \mathrm{Ti}_t\,(\mathbf{n})$ for $0 < i \leq p-2$. Then the first part of the theorem tells us that $v_p\left(f_{\mathbf{n}-i\mathbf{e}^{t-1}}\right) \geq \mathrm{Ti}_t\,(\mathbf{n})$ for such i. Since the binomial coefficients $\binom{p}{i}$ with $0 < i < p-1$ are divisible by p, this means that the $i = 1, \ldots, p-2$ terms in the sum over i in (4.10) vanish modulo $p^{\mathrm{Ti}_t(\mathbf{n})+1}$. So

$$f_{\mathbf{n}} \equiv -p f_{\mathbf{n}-(p-1)\mathbf{e}^{t-1}} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}}. \tag{4.11}$$

Let $\mathbf{m} = \mathbf{n} - (p-1)\mathbf{e}^{t-1}$. Note that since $n_{t-1} \geq p$, we have $\mathrm{Sc}\,(\mathbf{n}) \geq p^t$, so $\mathrm{Ti}_t\,(\mathbf{n}) \geq 1$. Then note that $\mathrm{Sc}\,(\mathbf{m}) = \mathrm{Sc}\,(\mathbf{n}) - (p-1)p^{t-1} \geq p^{t-1}$, so that $\mathrm{Ti}_t\,(\mathbf{m}) = \mathrm{Ti}_t\,(\mathbf{n}) - 1$. By Lemma 4.8, $\mathrm{Sc}\,(\mathbf{n}) = [(\mathrm{Ti}_t\,(\mathbf{n}) + 1)\,(p-1) + 1]\,p^{t-1} - p^k$, so that

$$\begin{aligned}\mathrm{Sc}\,(\mathbf{m}) &= [\mathrm{Ti}_t\,(\mathbf{n})(p-1) + 1]\,p^{t-1} - p^k \\ &= [(\mathrm{Ti}_t\,(\mathbf{m}) + 1)\,(p-1) + 1]\,p^{t-1} - p^k.\end{aligned}$$

Note that $\mathbf{m}$ is k-starting just like $\mathbf{n}$, so that Lemma 4.8 tells us that $\mathbf{m}$ is k-critical. Furthermore, $\mathbf{m} \prec \mathbf{n}$, so we may apply the induction hypothesis to it to obtain $f_{\mathbf{m}} \equiv (-p)^{\mathrm{Ti}_t(\mathbf{m})} \pmod{p^{\mathrm{Ti}_t(\mathbf{m})+1}}$. Combining this with (4.11), and recalling that $\mathrm{Ti}_t\,(\mathbf{n}) = \mathrm{Ti}_t\,(\mathbf{m}) + 1$, we obtain $f_{\mathbf{n}} \equiv (-p)^{\mathrm{Ti}_t(\mathbf{n})} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}}$. This completes the induction proof. □

With this knowledge of the Newton expansions of (p,t)-periodic functions, we now construct polynomials that p-adically approximate such functions.

Theorem 4.12. *Let $m \geq 1$ and let $F\colon {\mathbb{Z}_p}^t \to \mathbb{Z}_p$ be (p,t)-periodic. There exists a poly-*

nomial

$$f(\mathbf{x}) = \sum_{\substack{\mathbf{n}\in\mathbb{N}^t \\ \mathrm{Ti}_t(\mathbf{n})<m}} f_{\mathbf{n}} \binom{\mathbf{x}}{\mathbf{n}}, \tag{4.12}$$

with all $f_{\mathbf{n}} \in \mathbb{Z}_p$*, such that* $f(\mathbf{r}) \equiv F(\mathbf{r}) \pmod{p^m}$ *for all* $\mathbf{r} \in {\mathbb{Z}_p}^t$*. For each* $\mathbf{n} \in \mathbb{N}^t$ *with* $\mathrm{Ti}_t(\mathbf{n}) < m$*, we have* $v_p(f_{\mathbf{n}}) \geq \mathrm{Ti}_t(\mathbf{n})$*.*

Suppose further that

$$F(\mathbf{r}) = \begin{cases} 1 & \text{if } r_0 + pr_1 + \cdots + p^{t-1}r_{t-1} \equiv 0 \pmod{p^t}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.13}$$

for all $\mathbf{r} \in {\mathbb{Z}_p}^t$*. Then* $f_{\mathbf{0}} = 1$ *and if* $\mathbf{n} \in \mathbb{N}^t$ *is critical with* $\mathrm{Ti}_t(\mathbf{n}) < m$*, we also have* $f_{\mathbf{n}} \equiv (-p)^{\mathrm{Ti}_t(\mathbf{n})} \pmod{p^{\mathrm{Ti}_t(\mathbf{n})+1}}$*. Furthermore, if* F *is as given in* (4.13)*, there exists a polynomial*

$$g(\mathbf{x}) = \sum_{\substack{\mathbf{n}\in\mathbb{N}^t, \mathrm{Ti}_t(\mathbf{n})<m \\ |\mathbf{n}|\equiv 0 \pmod{p-1}}} g_{\mathbf{n}}\mathbf{x}^{\mathbf{n}}$$

in $\mathbb{Q}_p[\mathbf{x}]$ *such that (i)* $g(\mathbf{r}) \equiv F(\mathbf{r}) \pmod{p^m}$ *for all* $\mathbf{r} \in {\mathbb{Z}_p}^t$*, (ii)* $g_{\mathbf{0}} = 1$*, and (iii) if* $\mathbf{n}$ *is critical with* $\mathrm{Ti}_t(\mathbf{n}) = m - 1$*, then* $\mathbf{n}!g_{\mathbf{n}} \equiv (-p)^{m-1} \pmod{p^m}$*.*

Proof. Recall that any (p,t)-periodic function is p-adically continuous. Therefore, the existence of the polynomial f for a generic (p,t)-periodic function F is guaranteed by applying Theorem 4.11 and Lemma 4.6, with the set S in Lemma 4.6 equal to the set $\{\mathbf{n} \in \mathbb{N}^t : \mathrm{Ti}_t(\mathbf{n}) < m\}$. (This set is finite because only finitely many $\mathbf{n}$ have a certain t-tier.) Indeed, the coefficient $f_{\mathbf{n}}$ of our polynomial f is precisely the Newton coefficient for the term $\binom{\mathbf{x}}{\mathbf{n}}$ in the Newton expansion of F . Thus the bounds on valuations of coefficients and the congruences for certain coefficients (in the special case when F is given by (4.13)) follow from the bounds and congruences given in Theorem 4.11. Furthermore, if F is given by (4.13), we have $f_{\mathbf{0}} = 1$.

Now suppose that F is given by (4.13). Given the polynomial f described in the first

half of the theorem, consider the polynomial

$$g(\mathbf{x}) = \frac{1}{p-1} \sum_{h=0}^{p-2} f(\zeta_{p-1}^h \mathbf{x}).$$

Since ζ_{p-1} is a unit in $\mathbb{Z}_p$, we have $F(\zeta_{p-1}^h \mathbf{r}) = F(\mathbf{r})$ for all $h \in \mathbb{Z}$ and $\mathbf{r} \in {\mathbb{Z}_p}^t$. Thus $f(\zeta_{p-1}^h \mathbf{r}) \equiv f(\mathbf{r}) \pmod{p^m}$ for all $h \in \mathbb{Z}$ and $\mathbf{r} \in {\mathbb{Z}_p}^t$. Therefore $g(\mathbf{r}) \equiv f(\mathbf{r}) \equiv F(\mathbf{r}) \pmod{p^m}$ for all $\mathbf{r} \in {\mathbb{Z}_p}^t$. Note that if we expand out the terms $\binom{\mathbf{x}}{\mathbf{n}}$ to write $f(\mathbf{x}) = \sum_{\substack{\mathbf{n} \in \mathbb{N}^t \\ \mathrm{Ti}_t(\mathbf{n}) < m}} c_{\mathbf{n}} \mathbf{x}^{\mathbf{n}}$, then

$$g(\mathbf{x}) = \sum_{\substack{\mathbf{n} \in \mathbb{N}^t, \mathrm{Ti}_t(\mathbf{n}) < m \\ |\mathbf{n}| \equiv 0 \pmod{p-1}}} c_{\mathbf{n}} \mathbf{x}^{\mathbf{n}}. \tag{4.14}$$

In particular, $g(\mathbf{x})$ has the same constant term as $f(\mathbf{x})$, namely, 1. Suppose $\mathbf{h}$ is k-critical with $\mathrm{Ti}_t(\mathbf{h}) = m-1$. We want to calculate the coefficient of $\mathbf{x}^{\mathbf{h}}$ in $g(\mathbf{x})$. Since $\mathbf{h}$ is critical, $|\mathbf{h}| \equiv 0 \pmod{p-1}$ by Lemma 4.8. Thus $g(\mathbf{x})$ and $f(\mathbf{x})$ have the same coefficient for $\mathbf{x}^{\mathbf{h}}$, namely, $c_{\mathbf{h}}$. We want to relate $c_{\mathbf{h}}$ to the coefficients $f_{\mathbf{n}}$ in (4.12). Thus, we want to see which terms in the sum in (4.12) might involve the monomial $\mathbf{x}^{\mathbf{h}}$. Note that the monomial $\mathbf{x}^{\mathbf{h}}$ can occur in $\binom{\mathbf{x}}{\mathbf{n}}$ only if $n_j \geq h_j$ for all j and only if $n_j = 0$ for all j such that $h_j = 0$. So the monomial $\mathbf{x}^{\mathbf{h}}$ can occur in $\binom{\mathbf{x}}{\mathbf{n}}$ only if $\mathbf{n}$ is k-starting and $\mathrm{Sc}(\mathbf{n}) \geq \mathrm{Sc}(\mathbf{h})$. But since $\mathbf{h}$ is k-critical, Lemma 4.8 shows that any k-starting t-tuple with a strictly higher score than $\mathrm{Sc}(\mathbf{h})$ will be in a higher t-tier; such t-tuples are not included in our sum. So we need only consider those t-tuples $\mathbf{n}$ in our sum that are k-starting, that have the same score as $\mathbf{h}$, and that have $n_j \geq h_j$ for all j. But the second condition forces equality in all the inequalities of the third condition, showing that the only term in the sum in (4.12) that can involve the monomial $\mathbf{x}^{\mathbf{h}}$ is the term with $\mathbf{n} = \mathbf{h}$. So the coefficient of $\mathbf{x}^{\mathbf{h}}$ in $f(\mathbf{x})$ is $c_{\mathbf{h}} = \frac{f_{\mathbf{h}}}{\mathbf{h}!}$. This is also the coefficient of $\mathbf{x}^{\mathbf{h}}$ in $g(\mathbf{x})$, as we noted above. Now $\mathbf{h}! c_{\mathbf{h}} = f_{\mathbf{h}}$, and recall that $f_{\mathbf{h}}$ is the Newton coefficient for the $\binom{\mathbf{x}}{\mathbf{h}}$-term in the Newton expansion of F. So we know from Theorem 4.11 that $f_{\mathbf{h}} \equiv (-p)^{m-1} \pmod{p^m}$. □

In later chapters, we shall also want single-variable polynomials p-adically approximating certain functions that are constant on cosets of $p^t\mathbb{Z}_p$ in $\mathbb{Z}_p$. Such approximations as we need can be obtained easily from the polynomials we just constructed.

Corollary 4.13. *Let $m \geq 1$ and let $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be a function with $F(a) = F(b)$ whenever $a \equiv b \pmod{p^t}$. Let $d_j = [j(p-1)+1]p^{t-1} - 1$ for $j \in \mathbb{N}$. There exists a polynomial*

$$f(x) = \sum_{n=0}^{d_m} f_n \binom{x}{n},$$

with all $f_n \in \mathbb{Z}_p$ such that $f(r) \equiv F(r) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$. If $n > d_j$ then $v_p(f_n) \geq j$.

Suppose further that

$$F(r) = \begin{cases} 1 & \text{if } r \equiv 0 \pmod{p^t}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.15}$$

for all $r \in \mathbb{Z}_p$. Then $f_0 = 1$ and if $n = d_j$ for some $j = 1, 2, \ldots, m$, then we have $f_n \equiv (-p)^{j-1} \pmod{p^j}$. Furthermore, if F is as in (4.15), there exists a polynomial

$$g(x) = \sum_{\substack{0 \leq n \leq d_m \\ p-1 \mid n}} g_n x^n$$

of degree d_m in $\mathbb{Q}_p[x]$ such that (i) $g(r) \equiv F(r) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$, (ii) $g_0 = 1$, and (iii) $d_m! g_{d_m} \equiv (-p)^{m-1} \pmod{p^m}$.

Proof. We set $F^*(\mathbf{x}) = F(x_0 + px_1 + \cdots + p^{t-1}x_{t-1})$, and it is not hard to check that F^* is (p,t)-periodic. So Theorem 4.12 provides us with a polynomial

$$f^*(\mathbf{x}) = \sum_{\substack{\mathbf{n} \in \mathbb{N}^t \\ \mathrm{Ti}_t(\mathbf{n}) < m}} f^*_{\mathbf{n}} \binom{\mathbf{x}}{\mathbf{n}}$$

in $\mathbb{Q}_p[\mathbf{x}]$ that agrees with $F^*(\mathbf{x})$ modulo p^m everywhere on ${\mathbb{Z}_p}^t$. In particular, we have $f^*(r, 0, 0, \ldots, 0) \equiv F(r) \pmod{p^m}$ for all $r \in \mathbb{Z}_p$. So if we set $f(x) = f^*(x, 0, 0, \ldots, 0)$, we obtain a polynomial in $\mathbb{Q}_p[x]$ of the form

$$f(x) = \sum_{\substack{n \in \mathbb{N} \\ \mathrm{Ti}_t(n,0,0,\ldots,0) < m}} f^*_{(n,0,0,\ldots,0)} \binom{x}{n},$$

which agrees with $F(x)$ modulo p^m on $\mathbb{Z}_p$. So $f(x) = \sum_{n=0}^{d_m} f^*_{(n,0,0,\ldots,0)} \binom{x}{n}$. If $n > d_j$, then

$\mathrm{Ti}_t(n,0,0,\ldots,0) \geq j$, so we know that $v_p\left(f^*_{(n,0,0,\ldots,0)}\right) \geq j$ from Theorem 4.12.

Now suppose that $F(x)$ is given by (4.15). Then $F^*(\mathbf{x})$ is given by (4.13), and so Theorem 4.12 gives us additional information. If $n = d_j$ for some $j \in \{1,\ldots,m\}$, then $(n,0,0,\ldots,0)$ is 0-starting and $\mathrm{Sc}((n,0,0,\ldots,0)) = d_j = [j(p-1)+1]p^{t-1}-1$, so that $(n,0,0,\ldots,0)$ is of t-tier $j-1$, and by Lemma 4.8 we see that $(n,0,0,\ldots,0)$ is critical. Thus, from Theorem 4.12, we know that $f^*_{(n,0,0,\ldots,0)} \equiv (-p)^{j-1} \pmod{p^j}$. Also $f^*_{(0,\ldots,0)} = 1$ from Theorem 4.12.

Furthermore, Theorem 4.12 furnishes a polynomial

$$g^*(\mathbf{x}) = \sum_{\substack{\mathbf{n}\in\mathbb{N}^t, \mathrm{Ti}_t(\mathbf{n})<m \\ |\mathbf{n}|\equiv 0 \pmod{p-1}}} g^*_{\mathbf{n}}\mathbf{x}^{\mathbf{n}}$$

in $\mathbb{Q}_p[\mathbf{x}]$ that agrees with $F^*(\mathbf{x})$ modulo p^m on ${\mathbb{Z}_p}^t$ and has $g_{(0,\ldots,0)} = 1$. Furthermore, if $\mathbf{n}$ is critical and of t-tier $m-1$, then $\mathbf{n}!g_{\mathbf{n}} \equiv (-p)^{m-1} \pmod{p^m}$. Set $g(x) = g^*(x,0,0,\ldots,0)$, so that

$$g(x) = \sum_{\substack{n\in\mathbb{N} \\ \mathrm{Ti}_t(n,0,0,\ldots,0)<m \\ p-1\nmid n}} g^*_{(n,0,0,\ldots,0)}x^n,$$

and $g(x)$ agrees with $F(x)$ modulo p^m on $\mathbb{Z}_p$. Now $g(x) = \sum_{\substack{0\leq n\leq d_m \\ p-1\nmid n}} g^*_{(n,0,0,\ldots,0)}x^n$ and has constant term 1. Furthermore, if $n = d_m$, then $(n,0,0,\ldots,0)$ is 0-critical and of t-tier $m-1$ by the calculation in the previous paragraph, so that we know $d_m!g^*_{(d_m,0,0,\ldots,0)} \equiv (-p)^{m-1} \pmod{p^m}$ from Theorem 4.12. □

4.3 Sectioned Weights

In this section, we show how the polynomials of Theorem 4.12 are relevant to estimating weights. Before we do this, we discuss some preliminaries that will be vital to understanding the rest of the chapter. Recall that in this chapter we have set $e = 1$, so that we are working with codes in the algebra $\mathbb{Z}/p^d\mathbb{Z}[A]$. We continue the convention (started in Section 4.1) that for any letter a, the corresponding boldface letter $\mathbf{a}$ stands for the t-tuple $a_0,\ldots,a_{t-1}$, but for the rest of the chapter, we specialize to the case when $t = d$, so that $\mathbf{a} = (a_0,\ldots,a_{d-1})$.

We set $I = \{0, 1, \ldots, d-1\}$ and consider accounts in $\mathbb{Z}[I]$ to be d-tuples of integers, i.e., we identify $\mu \in \mathbb{Z}[I]$ with the d-tuple $(\mu_0, \mu_1, \ldots, \mu_{d-1}) \in \mathbb{Z}^d$. Then for $\mu \in \mathbb{Z}[I]$, the score of μ, denoted $\mathrm{Sc}\,(\mu)$, is defined to be $\sum_{i=0}^{d-1} p^i \mu_i$, following the definition in Section 4.2. For $s \in \mathbb{N}$, the s-tier of μ, denoted $\mathrm{Ti}_s(\mu)$, is also defined just as in Section 4.2. In fact, we shall be interested only in d-tiers here. Therefore, for the rest of this chapter, we define *tier* to mean d-tier and write Ti to mean Ti_d. So $\mathrm{Ti}\,(\mu) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(\mu) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}$. We also transport the notion of score and tier to elements of $\mathbb{Z}[I \times A]$. The score of $\lambda \in \mathbb{Z}[I \times A]$, denoted $\mathrm{Sc}\,(\lambda)$, is just $\mathrm{Sc}\,(\mathrm{pr}_I\,\lambda)$, and the tier of λ, denoted $\mathrm{Ti}\,(\lambda)$, is just $\mathrm{Ti}\,(\mathrm{pr}_I\,\lambda)$. This means that $\mathrm{Sc}\,(\lambda) = \sum_{i=0}^{d-1} p^i |\lambda_i|$ and $\mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(\lambda) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}$. So of course

$$\mathrm{Sc}\,(\lambda) \equiv |\lambda| \pmod{p-1} \tag{4.16}$$

for any $\lambda \in \mathbb{Z}[I \times A]$. We also transport to $\mathbb{Z}[I \times A]$ the notion of an account being k-starting or k-critical (for $k \in I$); to say that $\lambda \in \mathbb{Z}[I \times A]$ is k-starting (resp., k-critical) is to say that $\mathrm{pr}_I\,\lambda$ is k-starting (resp., k-critical). In consonance with our established terminology, we say that λ is critical to mean that it is k-critical for some k.

Throughout this chapter, we suppose that we have a code $\mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$ and $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$ is the tower of supports of the Fourier transform of $\mathcal{C}$. We suppose that not all the S_i are subsets of $\{1_A\}$, i.e., that at least one of the S_i contains an element of A that is not the identity. Otherwise we have a trivial situation: $\mathcal{C}$ consists only of constant words, and then $\mathrm{wt}(c) = |A|\,\mathrm{wt}(\tilde{c}(1_A))$ for all $c \in \mathcal{C}$, i.e., $\mathrm{wt}^{\mathrm{norm}}(c) = 0$ for all $c \in \mathcal{C}$.

If we have a weight function $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$, we define a related d-wise weight function, called the *sectioning of* wt, denoted $\mathrm{wt}_{\mathrm{sec}}\colon (\mathbb{Z}/p^d\mathbb{Z})^d \to \mathbb{Z}$, which is defined by

$$\mathrm{wt}_{\mathrm{sec}}(r_0, \ldots, r_{d-1}) = \mathrm{wt}(r_0 + pr_1 + \cdots + p^{d-1}r_{d-1})$$

for all $r_0, \ldots, r_{d-1} \in \mathbb{Z}/p^d\mathbb{Z}$.

Recall the canonical expansion of the scaled Fourier transform and the scaled Fourier-induced breakdown of codewords, which were defined in Section 2.3 (before Proposition 2.8). For $c \in \mathcal{C}$ and $i \in I$, $c^{(i)}$ denotes the ith component of the scaled Fourier-induced breakdown

of c, and $\tilde{c}^{(i)}$ denotes the ith component in the canonical expansion of $\tilde{c}$. Throughout this chapter, we often use the more convenient symbol c_i as a synonym for $c^{(i)}$. Thus $c = \sum_{i=0}^{d-1} p^i c^{(i)} = \sum_{i=0}^{d-1} p^i c_i$ and $\tilde{c} = \sum_{i=0}^{d-1} p^i \tilde{c}^{(i)} = \sum_{i=0}^{d-1} p^i \tilde{c}_i$.

The scaled Fourier-induced breakdown of our word is designed to work with the sectioned weight function. Note that Proposition 2.8 tells us that $c^{(i)} \in \mathbb{Z}/p^d\mathbb{Z}[A]$ for all $i \in \{0, 1, \ldots, d-1\}$, so we can apply our sectioned weight function to these words to obtain

$$\begin{aligned}
\mathrm{wt}_{\mathrm{sec}}(c^{(0)}, \ldots, c^{(d-1)}) &= \sum_{a \in A} \mathrm{wt}_{\mathrm{sec}}(c_a^{(0)}, \ldots, c_a^{(d-1)}) \\
&= \sum_{a \in A} \mathrm{wt}(c_a^{(0)} + \cdots + p^{d-1} c_a^{(d-1)}) \\
&= \sum_{a \in A} \mathrm{wt}(c_a),
\end{aligned}$$

so that (using the synonym c_i for $c^{(i)}$)

$$\mathrm{wt}_{\mathrm{sec}}(c_0, \ldots, c_{d-1}) = \mathrm{wt}(c). \tag{4.17}$$

Also note that

$$\begin{aligned}
\mathrm{wt}_{\mathrm{sec}}^{\mathrm{norm}}(c_0, \ldots, c_{d-1}) &= \mathrm{wt}_{\mathrm{sec}}(c_0, \ldots, c_{d-1}) - |A| \mathrm{wt}_{\mathrm{sec}}(\tilde{c}_0(1_A), \ldots, \tilde{c}_{d-1}(1_A)) \\
&= \mathrm{wt}(c) - |A| \, \mathrm{wt}(\tilde{c}_0(1_A) + \cdots + p^{d-1} \tilde{c}_{d-1}(1_A)) \\
&= \mathrm{wt}(c) - |A| \, \mathrm{wt}(\tilde{c}(1_A)),
\end{aligned}$$

that is,

$$\mathrm{wt}_{\mathrm{sec}}^{\mathrm{norm}}(c_0, \ldots, c_{d-1}) = \mathrm{wt}^{\mathrm{norm}}(c). \tag{4.18}$$

Now we show that the sectioned weight functions lift to (p, d)-periodic functions. We examine the function $F \colon {\mathbb{Z}_p}^d \to \mathbb{Z}$ given by

$$F(\mathbf{r}) = \mathrm{wt}_{\mathrm{sec}}(\pi(r_0), \ldots, \pi(r_{d-1})).$$

Note that for any $j \in I$, $k \in \mathbb{N}$, and $\mathbf{r} \in {\mathbb{Z}_p}^d$, we have

$$\begin{aligned} F(\mathbf{r} + k\mathbf{e}^j) &= \mathrm{wt}_{\mathrm{sec}}(\pi(r_0), \pi(r_1), \ldots, \pi(r_{j-1}), k + \pi(r_j), \pi(r_{j+1}), \ldots, \pi(r_{d-1})) \\ &= \mathrm{wt}(\pi(r_0) + p\pi(r_1) + \cdots + p^{d-1}\pi(r_{d-1}) + kp^j). \end{aligned}$$

Therefore, if $j < d-1$,

$$F(\mathbf{r} + p\mathbf{e}^j) = F(\mathbf{r} + \mathbf{e}^{j+1}),$$

and

$$\begin{aligned} F(\mathbf{r} + p\mathbf{e}^{d-1}) &= \mathrm{wt}(\pi(r_0) + p\pi(r_1) + \cdots + p^{d-1}\pi(r_{d-1}) + p^d) \\ &= \mathrm{wt}(\pi(r_0) + p\pi(r_1) + \cdots + p^{d-1}\pi(r_{d-1})) \\ &= \mathrm{wt}_{\mathrm{sec}}(\pi(r_0), \ldots, \pi(r_{d-1})) \\ &= F(\mathbf{r}). \end{aligned}$$

Thus F is (p, d)-periodic. So F, which is the lift of our sectioned weight function, can be approximated using the polynomials of Theorem 4.12. We use such approximations in the next two sections to prove the main results (Theorems 4.18 and 4.21) of this chapter.

4.4 Zero Count and Hamming Weight

In this section, we shall prove Theorem 4.18, our sharp lower bound on the p-adic valuations of Hamming weights of words of codes in $\mathbb{Z}/p^d\mathbb{Z}[A]$. In order to p-adically estimate zero counts, we construct a set $\Lambda_{mc}^{ss}(\mathcal{C})$ of multisets in $\mathbb{N}[I \times A]$ and use $\Lambda_{mc}^{ss}(\mathcal{C})$ to define the parameter $\ell_{mc}^{ss}(\mathcal{C})$, which had been defined in Section 1.1 of the Introduction by way of sequences. We prefer the multiset-based definition here because it will make our calculations easier. We define

$$\begin{aligned} \Lambda_{mc}^{ss}(\mathcal{C}) = \{\lambda \in \mathbb{N}[I \times A] : \lambda_0 \in \mathbb{N}[S_0], \ldots, \lambda_{d-1} \in \mathbb{N}[S_{d-1}], \\ \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}], |\lambda| \equiv 0 \pmod{p-1}\}. \end{aligned} \quad (4.19)$$

We claim that $\Lambda_{mc}^{ss}(\mathcal{C})$ is nonempty. By assumption, we have some k such that there exists $a \in S_k$ with $a \neq 1_A$. Let n be the group-theoretic order of a. Then note that the multiset λ with $(p-1)n$ instances of the pair (k, a) and no other elements is a unity-product but not all-unity multiset in $\mathbb{N}[I \times A]$ with $(p-1)n$ elements and with $\lambda_i \in \mathbb{N}[S_i]$ for all $i \in I$. Since $\Lambda_{mc}^{ss}(\mathcal{C}) \neq \emptyset$, we may set

$$\omega_{mc}^{ss}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})} \mathrm{Sc}\,(\lambda) \tag{4.20}$$

and

$$\ell_{mc}^{ss}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})} \mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\omega_{mc}^{ss}(\mathcal{C}) - p^{t-1}}{(p-1)p^{t-1}} \right\rfloor\right\}. \tag{4.21}$$

At this point we begin to use the notion of reduction defined in Section 2.6. We prove a lemma about how reduction affects scores and tiers of accounts.

Lemma 4.14. *Suppose that $\lambda \in \mathbb{N}[I \times A]$ is k-starting. Then $\mathrm{Red}(\lambda) \in \mathbb{N}[I \times A]$ is k-starting. If λ is not reduced, then $\mathrm{Sc}\,(\mathrm{Red}(\lambda)) = \mathrm{Sc}\,(\lambda) - j(p-1)p^k$ for some positive integer j. If $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$, then $\mathrm{Red}(\lambda) \in \Lambda_{mc}^{ss}(\mathcal{C})$. Furthermore, if $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}^{ss}(\mathcal{C})$, then $\mathrm{Ti}\,(\mathrm{Red}(\lambda)) = \ell_{mc}^{ss}(\mathcal{C})$.*

Proof. Since $\lambda_i = \emptyset$ for $i < k$ and $\lambda_k \neq \emptyset$, we have $(\mathrm{Red}(\lambda))_i = \emptyset$ for $i < k$ and $(\mathrm{Red}(\lambda))_k \neq \emptyset$ by Lemma 2.24. So $\mathrm{Red}(\lambda)$ is k-starting. Furthermore, if λ is not reduced, then for each $i \in \{k, k+1, \ldots, d-1\}$, we have $|\mathrm{Red}(\lambda_i)| = |\lambda_i| - j_i(p-1)$ for some $j_i \in \mathbb{N}$, and at least one of $j_k, \ldots, j_{d-1}$ is strictly positive. Thus $\mathrm{Sc}\,(\mathrm{Red}(\lambda)) = \mathrm{Sc}\,(\lambda) - \sum_{i=k}^{d-1}(p-1)p^i j_i$. The last sum is a strictly positive integer multiple of $(p-1)p^k$. Now suppose that $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$. Then $|\mathrm{Red}(\lambda)| \equiv |\lambda| \equiv 0 \pmod{p-1}$, and Lemma 2.24 shows us that λ is unity-product and not all-unity with $\lambda_i \in \mathbb{N}[S_i]$ for all $i \in I$. So $\mathrm{Red}(\lambda) \in \Lambda_{mc}^{ss}(\mathcal{C})$. Since reduction never increases score, it never increases tier. So if $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ and $\mathrm{Ti}\,(\lambda) = \ell_{mc}^{ss}(\mathcal{C})$, by the minimality of $\ell_{mc}^{ss}(\mathcal{C})$, we must have $\mathrm{Ti}\,(\mathrm{Red}(\lambda)) = \ell_{mc}^{ss}(\mathcal{C})$ also. □

We also note some particular properties of those $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ of minimal tier. These facts are used to prove the sharpness of our bound on the p-adic valuations of Hamming weights.

Lemma 4.15. *Let Λ_ℓ be the set of all $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ that are reduced and have $\mathrm{Ti}\,(\lambda) = \ell_{mc}^{ss}(\mathcal{C})$. Then*

(i) $\Lambda_\ell \neq \emptyset$.

(ii) *If we chose $\lambda \in \Lambda_\ell$ with $\mathrm{pr}_I\,\lambda = (|\lambda_0|, \ldots, |\lambda_{d-1}|)$ lexicographically minimal, then λ is critical.*

(iii) *If $\lambda \in \Lambda_\ell$ is critical, then there is no $\kappa \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\kappa \neq \lambda$, $\mathrm{Red}(\kappa) = \lambda$, and $\mathrm{Ti}\,(\kappa) = \ell_{mc}^{ss}(\mathcal{C})$.*

(iv) *Thus, there exists a critical $\lambda \in \Lambda_\ell$ such that there is no $\kappa \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\kappa \neq \lambda$, $\mathrm{Red}(\kappa) = \lambda$, and $\mathrm{Ti}\,(\kappa) = \ell_{mc}^{ss}(\mathcal{C})$.*

Proof. By definition, $\{\mu \in \Lambda_{mc}^{ss}(\mathcal{C}) : \mathrm{Ti}\,(\mu) = \ell_{mc}^{ss}(\mathcal{C})\}$ is not empty, so take κ in this set and let $\lambda = \mathrm{Red}(\kappa)$. Then $\lambda \in \{\mu \in \Lambda_{mc}^{ss}(\mathcal{C}) : \mathrm{Ti}\,(\mu) = \ell_{mc}^{ss}(\mathcal{C})\}$ by Lemma 4.14. This proves (i).

Now suppose $\lambda \in \Lambda_\ell$ is chosen so that $\mathrm{pr}_I\,\lambda = (|\lambda_0|, \ldots, |\lambda_{d-1}|)$ lexicographically minimal. Set $k \in I$ so that λ is k-starting and set $a \in S_k$ so that $\lambda_{(k,a)} > 0$. We now divide the proof into cases for different values of k.

If $k = d-1$, then the condition $|\lambda| \equiv 0 \pmod{p-1}$ means that $(|\lambda_0|, \ldots, |\lambda_{d-1}|) = (0, 0, \ldots, 0, (p-1)n)$ for some integer n. This n must be strictly positive since $\emptyset$ is all-unity, hence not in $\Lambda_{mc}^{ss}(\mathcal{C})$. Note that $\ell_{mc}^{ss}(\mathcal{C}) = \mathrm{Ti}\,(\lambda) = n-1$, so $\mathrm{Sc}\,(\lambda) = n(p-1)p^{d-1} = (\mathrm{Ti}\,(\lambda)+1)(p-1)p^{d-1}$. Thus λ is critical by Lemma 4.8.

In the case where $k < d-1$, let $\mu = \lambda - (k,a) + (k+1,a)$. Since $S_k \subseteq S_{k+1}$, we have $\mu_j \in \mathbb{N}[S_j]$ for all j. Also note that $\Pi\mu = \Pi\lambda = 1_A$, that $\mathrm{pr}_A\,\mu = \mathrm{pr}_A\,\lambda \notin \mathbb{N}[\{1_A\}]$, and that $|\mu| = |\lambda|$, so that $|\mu| \equiv 0 \pmod{p-1}$. So $\mu \in \Lambda_{mc}^{ss}(\mathcal{C})$. Set $\nu = \mathrm{Red}(\mu)$, which is in $\Lambda_{mc}^{ss}(\mathcal{C})$ by Lemma 4.14. Note that μ is k-starting or $(k+1)$-starting, and so ν is also k-starting or $(k+1)$-starting by Lemma 4.14. Furthermore, Lemma 2.24 tells us that $|\nu_k| \leq |\mu_k| = |\lambda_k| - 1$, so that $\mathrm{pr}_I\,\nu$ is lexicographically less than $\mathrm{pr}_I\,\lambda$. This means that $\nu \notin \Lambda_\ell$. Since $\nu \in \Lambda_{mc}^{ss}(\mathcal{C})$ and ν is reduced, this means that $\mathrm{Ti}\,(\nu) > \mathrm{Ti}\,(\lambda) = \ell_{mc}^{ss}(\mathcal{C})$. So $\mathrm{Sc}\,(\nu) \geq [(p-1)(\ell_{mc}^{ss}(\mathcal{C})+1)+1]p^{d-1}$. Since $\nu = \mathrm{Red}(\mu)$, we have $\mathrm{Sc}\,(\mu) \geq [(p-1)(\ell_{mc}^{ss}(\mathcal{C})+$

$1)+1]p^{d-1}$ by Lemma 4.14. So

$$\mathrm{Sc}\,(\lambda) - p^k + p^{k+1} \geq [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1},$$

and thus

$$\mathrm{Sc}\,(\lambda) \geq [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - (p-1)p^k. \tag{4.22}$$

Of course, since λ is k-starting, its score is a multiple of p^k. Since $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$, we have $|\lambda| \equiv 0 \pmod{p-1}$, so $\mathrm{Sc}\,(\lambda) \equiv 0 \pmod{p-1}$ by (4.16). So $\mathrm{Sc}\,(\lambda)$ is a multiple of $(p-1)p^k$. Note that the right-hand side of inequality (4.22) is

$$[(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - (p-1)p^k \equiv p^k \pmod{(p-1)p^k}.$$

Since $\mathrm{Sc}\,(\lambda) \equiv 0 \pmod{(p-1)p^k}$, we can improve inequality (4.22) to get

$$\begin{aligned}\mathrm{Sc}\,(\lambda) &\geq [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - (p-1)p^k + (p-2)p^k \\ &= [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - p^k,\end{aligned}$$

but since $\mathrm{Ti}\,(\lambda) = \ell^{ss}_{mc}(\mathcal{C})$, we have $\mathrm{Sc}\,(\lambda) < [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1}$. Since λ is k-starting, $p^k \mid \mathrm{Sc}\,(\lambda)$, so that our last two inequalities force $\mathrm{Sc}\,(\lambda) = [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - p^k$. Then Lemma 4.8 tells us that λ is k-critical. This proves (ii).

Suppose that $\lambda \in \Lambda_\ell$ is k-critical and $\mu \in \Lambda^{ss}_{mc}(\mathcal{C})$ with $\mu \neq \lambda$ and $\mathrm{Red}(\mu) = \lambda$. We shall show that $\mathrm{Ti}\,(\mu) > \ell^{ss}_{mc}(\mathcal{C})$. Since λ is k-starting, so is μ by Lemma 4.14. Furthermore, μ is not reduced since it is not equal to λ, so $\mathrm{Sc}\,(\mu) \geq \mathrm{Sc}\,(\lambda) + p^k(p-1)$ by Lemma 4.14. But $\mathrm{Sc}\,(\lambda) = [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} - p^k$ by Lemma 4.8, so $\mathrm{Sc}\,(\mu) \geq [(p-1)(\ell^{ss}_{mc}(\mathcal{C})+1)+1]p^{d-1} + (p-2)p^k$, which forces $\mathrm{Ti}\,(\mu) > \ell^{ss}_{mc}(\mathcal{C})$. This proves (iii), and (iv) follows from (i), (ii), and (iii). □

We recall the counting polynomials we devised in the Section 4.2 and cast them into the notation of this section.

Theorem 4.16 (part of Theorem 4.12). *For each $m \geq 1$, there exists a polynomial*

$$f^{(m)}(\mathbf{x}) = \sum_{\substack{\mu \in \mathbb{N}[I], \mathrm{Ti}(\mu) < m \\ |\mu| \equiv 0 \pmod{p-1}}} f_\mu^{(m)} \mathbf{x}^\mu$$

in $\mathbb{Q}_p[\mathbf{x}]$ with the property that $f^{(m)}(r_0, \ldots, r_{d-1}) \equiv \mathrm{zer}_{\mathrm{sec}}(\pi(r_0), \ldots, \pi(r_{d-1})) \pmod{p^m}$ for all $r_0, \ldots, r_{d-1} \in \mathbb{Z}_p$. If $\mu \in \mathbb{N}[I]$ is critical and $\mathrm{Ti}\,(\mu) = m-1$, then $\mu! f_\mu^{(m)} \equiv (-p)^{m-1} \pmod{p^m}$.

Proof. The polynomial $f^{(m)}(\mathbf{x})$ here is just $g(\mathbf{x})$ from Theorem 4.12 with $t = d$, where we have used our identification of d-tuples with accounts in $\mathbb{N}[I]$ and noted that for any $r_0, \ldots, r_{d-1} \in \mathbb{Z}_p$,

$$\begin{aligned} \mathrm{zer}_{\mathrm{sec}}(\pi(r_0), \ldots, \pi(r_{d-1})) &= \mathrm{zer}(\pi(r_0) + \cdots + p^{d-1}\pi(r_{d-1})) \\ &= \mathrm{zer}(\pi(r_0 + \cdots + p^{d-1} r_{d-1})), \end{aligned}$$

so that $\mathrm{zer}_{\mathrm{sec}}(\pi(x_0), \ldots, \pi(x_{d-1}))$ is the function $F(x_0, \ldots, x_{d-1})$ defined in (4.13) of Theorem 4.12. The polynomial $g(\mathbf{x})$ of that theorem approximates $F(\mathbf{x})$ modulo p^m on all of ${\mathbb{Z}_p}^d$. □

Now we are ready to estimate zero counts. The following proposition is the main calculation:

Proposition 4.17. *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. Let $m \geq 1$ and let $f^{(m)}(\mathbf{x})$ be the polynomial described in Theorem 4.16. For each $c \in \mathcal{C}$ and $i \in I$, we let C_i be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$. For any $c \in \mathcal{C}$, we have*

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < m}} \frac{(\mathrm{pr}_I\, \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m},$$

where $\Lambda_{mc}^{ss}(\mathcal{C})$ is as defined in (4.19) above.

Proof. By Corollary 3.4, we have

$$\operatorname{zer}_{\mathrm{sec}}^{\mathrm{norm}}(c_0,\dots,c_{d-1}) \equiv |A| \sum_{\mu\in\mathbb{N}[I]} \mu! f_\mu^{(m)} \sum_{\substack{\lambda\in\mathbb{N}[I\times A],\operatorname{pr}_I\lambda=\mu\\ \Pi\lambda=1_A,\operatorname{pr}_A\lambda\notin\mathbb{N}[\{1_A\}]\\ \lambda_0\in\mathbb{N}[S_0],\dots,\lambda_{d-1}\in\mathbb{N}[S_{d-1}]}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}.$$

By (4.18), the left-hand side becomes $\operatorname{zer}^{\mathrm{norm}}(c)$. We can restrict the sum over μ to those μ with $\operatorname{Ti}(\mu) < m$ and $|\mu| \equiv 0 \pmod{p-1}$, since $f_\mu^{(m)} = 0$ otherwise (by Theorem 4.16). With this restriction on μ, the condition that $\operatorname{pr}_I\lambda = \mu$ implies $|\lambda| \equiv 0 \pmod{p-1}$. So the inner sum on the right-hand side sums over those $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\operatorname{pr}_I\lambda = \mu$. Thus

$$\begin{aligned}\operatorname{zer}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\substack{\mu\in\mathbb{N}[I],\operatorname{Ti}(\mu)<m\\ |\mu|\equiv 0 \pmod{p-1}}} \mu! f_\mu^{(m)} \sum_{\substack{\lambda\in\Lambda_{mc}^{ss}(\mathcal{C})\\ \operatorname{pr}_I\lambda=\mu}} \frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}\\ &\equiv |A| \sum_{\substack{\mu\in\mathbb{N}[I],\operatorname{Ti}(\mu)<m\\ |\mu|\equiv 0 \pmod{p-1}}} \sum_{\substack{\lambda\in\Lambda_{mc}^{ss}(\mathcal{C})\\ \operatorname{pr}_I\lambda=\mu}} \frac{(\operatorname{pr}_I\lambda)! f_{\operatorname{pr}_I\lambda}^{(m)}}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m},\end{aligned}$$

but then the condition on the cardinality of μ can be dropped (if $|\mu|$ is not divisible by $p-1$, then neither is $|\lambda|$ if $\lambda = \operatorname{pr}_I\mu$, so then there is no $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\operatorname{pr}_I\lambda = \mu$). Also, the condition $\lambda = \operatorname{pr}_I\mu$ means that λ and μ will always have the same score and tier, so we can shift the condition on tier to the sum over λ. Thus

$$\begin{aligned}\operatorname{zer}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\mu\in\mathbb{N}[I]} \sum_{\substack{\lambda\in\Lambda_{mc}^{ss}(\mathcal{C})\\ \operatorname{pr}_I\lambda=\mu\\ \operatorname{Ti}(\lambda)<m}} \frac{(\operatorname{pr}_I\lambda)! f_{\operatorname{pr}_I\lambda}^{(m)}}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}\\ &\equiv |A| \sum_{\substack{\lambda\in\Lambda_{mc}^{ss}(\mathcal{C})\\ \operatorname{Ti}(\lambda)<m}} \frac{(\operatorname{pr}_I\lambda)! f_{\operatorname{pr}_I\lambda}^{(m)}}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i) \pmod{p^m}.\end{aligned}$$

□

Now we derive our generalization of McEliece's Theorem.

Theorem 4.18. *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. With $\ell_{mc}^{ss}(\mathcal{C})$ as defined in* (4.21)*, we have* $\operatorname{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, and* $\operatorname{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}}$ *for some $c \in \mathcal{C}$. Equivalently,* $\operatorname{ham}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, and* $\operatorname{ham}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}}$ *for some $c \in \mathcal{C}$. More precisely, if $f^{(\ell_{mc}^{ss}(\mathcal{C})+1)}(\mathbf{x})$ is the polynomial described*

in Theorem 4.16, and if we let C_i be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$ for each $i \in I$ and $c \in \mathcal{C}$, then

$$\operatorname{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}}, \tag{4.23}$$

and the expression on the right-hand side assumes values in $p^{\ell_{mc}^{ss}(\mathcal{C})}\mathbb{Z}_p$ for all $c \in \mathcal{C}$, but there is some $c \in \mathcal{C}$ such that this expression is not in $p^{\ell_{mc}^{ss}(\mathcal{C})+1}\mathbb{Z}_p$.

Proof. If $\ell_{mc}^{ss}(\mathcal{C}) = 0$, the congruence $\operatorname{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}}$ for all $c \in \mathcal{C}$ is obvious. If $\ell_{mc}^{ss}(\mathcal{C}) > 0$, we use Proposition 4.17 above (setting $m = \ell_{mc}^{ss}(\mathcal{C})$) to obtain

$$\operatorname{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C}))}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}},$$

where $f^{(\ell_{mc}^{ss}(\mathcal{C}))}(\mathbf{x})$ is the polynomial described in Theorem 4.16, and $\Lambda_{mc}^{ss}(\mathcal{C})$ is as defined in (4.19). But by the definition of $\ell_{mc}^{ss}(\mathcal{C})$ as the minimum tier of any element in $\Lambda_{mc}^{ss}(\mathcal{C})$, we see that the sum on the right-hand side of this congruence is empty, thus proving $\operatorname{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}}$.

Now we prove that $\operatorname{zer}^{\mathrm{norm}}(c)$ is not always divisible by $p^{\ell_{mc}^{ss}(\mathcal{C})+1}$, along with the more precise statements at the end of the statement of the theorem, including congruence (4.23). Note that the claim that $\operatorname{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}}$ for some $c \in \mathcal{C}$ is not trivial if $\ell_{mc}^{ss}(\mathcal{C}) = 0$, so we allow for this possibility. In any case, we use Proposition 4.17 again, but this time with $m = \ell_{mc}^{ss}(\mathcal{C}) + 1$, to get

$$\operatorname{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}},$$

with $f^{(\ell_{mc}^{ss}(\mathcal{C})+1)}(\mathbf{x}) \in \mathbb{Q}_p[\mathbf{x}]$ as described in Theorem 4.16. We have omitted to sum over those λ with $\mathrm{Ti}\,(\lambda) < \ell_{mc}^{ss}(\mathcal{C})$, for there are no such $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ by the definition of $\ell_{mc}^{ss}(\mathcal{C})$.

This last congruence is (4.23), which we were to show. Let

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i),$$

which is the right-hand side of (4.23). Note that the coefficients of $f^{(\ell_{mc}^{ss}(\mathcal{C})+1)}(\mathbf{x})$ are in $\mathbb{Q}_p$ (see Theorem 4.16) and note that $\tilde{C}_i(a) \in \mathbb{Z}_p[\zeta_{q'-1}]$ for all $i \in I$ and $a \in A$ (because $\tilde{C}(a) \in \mathbb{Z}_p[\zeta_{q'-1}]$ for all $a \in A$). Thus $Y(c) \in \mathbb{Q}_p(\zeta_{q'-1})$. We shall show that $Y(c)$ is actually in the smaller field $\mathbb{Q}_p$. To do this, it suffices to show that it is fixed by Fr. We now use the Frobenius action $\mathrm{Fr_A}$ introduced in Section 2.7. By Lemma 2.30, we note that $\mathrm{Fr_A}$ restricted to $\Lambda_{mc}^{ss}(\mathcal{C})$ is a permutation of $\Lambda_{mc}^{ss}(\mathcal{C})$. Furthermore, by the same lemma, we note that if $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$, then $\mathrm{pr}_I \mathrm{Fr_A}(\lambda) = \mathrm{pr}_I \lambda$. So $\mathrm{Fr_A}$ preserves score and tier. So $\mathrm{Fr_A}$ permutes the set of $\lambda \in \Lambda_{mc}^{ss}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}^{ss}(\mathcal{C})$. Thus we have

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \mathrm{Fr_A}(\lambda))! f_{\mathrm{pr}_I \mathrm{Fr_A}(\lambda)}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\mathrm{Fr_A}(\lambda)!} \prod_{i \in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i).$$

By Lemma 2.30, we have $\mathrm{pr}_I \mathrm{Fr_A}(\lambda) = \mathrm{Fr_A}(\lambda)$, $\mathrm{Fr_A}(\lambda)! = \lambda!$, and $\prod_{i \in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i) = \mathrm{Fr}\left(\prod_{i \in I} \tilde{C}_i(\lambda_i)\right)$, so that

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\lambda!} \mathrm{Fr}\left(\prod_{i \in I} \tilde{C}_i(\lambda)_i\right).$$

Since the coefficients of $f^{(\ell_{mc}^{ss}(\mathcal{C})+1)}(\mathbf{x})$ are in $\mathbb{Q}_p$ (see Theorem 4.16), we have

$$\begin{aligned} Y(c) &= \mathrm{Fr}\left(|A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell_{mc}^{ss}(\mathcal{C})+1)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i)\right) \\ &= \mathrm{Fr}(Y(c)), \end{aligned}$$

so that $Y(c) \in \mathbb{Q}_p$. We have already proved that $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})}}$ for all $c \in \mathcal{C}$. Since $\mathrm{zer}^{\mathrm{norm}}(c) \equiv Y(c) \pmod{p^{\ell_{mc}^{ss}(\mathcal{C})+1}}$ (this is (4.23)), we know that $Y(c) \in p^{\ell_{mc}^{ss}(\mathcal{C})}\mathbb{Z}_p$

for all $c \in \mathcal{C}$. So to finish our proof, we must show that there is some $c \in \mathcal{C}$ such that $\mathrm{zer}^{\mathrm{norm}}(c) \equiv Y(c) \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$ does not vanish modulo $p^{\ell^{ss}_{mc}(\mathcal{C})+1}$.

To prove this, we shall use the notion of collapse introduced in Section 2.6. Note that $\tilde{c}_i(a)$ is zero or a power of $\pi(\zeta_{q'-1})$ for all $a \in A$ and $i \in I$, since $\tilde{c}_i$ is the ith component of the canonical expansion of $\tilde{c}$. We let R be a set of p-class representatives of A and apply Lemma 2.18 to (4.23) to obtain

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}_{mc}(\mathcal{C})}} \frac{(\mathrm{pr}_I\, \lambda)! f^{(\ell^{ss}_{mc}(\mathcal{C})+1)}_{\mathrm{pr}_I\, \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}.$$

If we define Λ_ℓ to be the set of elements of $\Lambda^{ss}_{mc}(\mathcal{C})$ that are reduced and of tier $\ell^{ss}_{mc}(\mathcal{C})$, we have

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\lambda \in \Lambda_\ell} \sum_{\substack{\mu \in \Lambda^{ss}_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\mu) = \ell^{ss}_{mc}(\mathcal{C}) \\ \mathrm{Red}(\mu) = \lambda}} \frac{(\mathrm{pr}_I\, \mu)! f^{(\ell^{ss}_{mc}(\mathcal{C})+1)}_{\mathrm{pr}_I\, \mu}}{\mu!} \prod_{i \in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}},$$

since the reduction of any $\mu \in \Lambda^{ss}_{mc}(\mathcal{C})$ with $\mathrm{Ti}\,(\mu) = \ell^{ss}_{mc}(\mathcal{C})$ is an element λ of Λ_ℓ by Lemma 4.14, and for such a μ, we have $\mathrm{Co}_R(\mu_i) = \mathrm{Co}_R(\lambda_i)$ for $i \in I$ by Lemma 2.24. For each $\lambda \in \Lambda_\ell$, set

$$B_\lambda = |A| \sum_{\substack{\mu \in \Lambda^{ss}_{mc}(\mathcal{C}), \mathrm{Ti}(\mu) = \ell^{ss}_{mc}(\mathcal{C}) \\ \mathrm{Red}(\mu) = \lambda}} \frac{(\mathrm{pr}_I\, \mu)! f^{(\ell^{ss}_{mc}(\mathcal{C})+1)}_{\mathrm{pr}_I\, \mu}}{\mu!}, \tag{4.24}$$

which is an element of $\mathbb{Q}_p$ since the coefficients $f^{(\ell^{ss}_{mc}(\mathcal{C})+1)}_{\mu}$ are in $\mathbb{Q}_p$. Then

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv \sum_{\lambda \in \Lambda_\ell} B_\lambda \prod_{i \in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}. \tag{4.25}$$

Note that the right-hand side of (4.25) is a $\mathbb{Q}_p$-linear combination of terms of the form

$$D_\lambda = \prod_{i \in I} \prod_{r \in R \cap S_i} \tilde{C}_i(r)^{(\mathrm{Co}_R(\lambda_i))_r}, \tag{4.26}$$

where we have restricted the second product of (4.26) to $R \cap S_i$ in view Lemma 2.17 and the fact that $\lambda_i \in \mathbb{N}[S_i]$ for all $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$ and $i \in I$. Note that no two terms D_λ and $D_{\lambda'}$ with

$\lambda, \lambda' \in \Lambda_\ell$ have exactly the same exponents for all the terms $\tilde{C}_i(r)$, since that would imply that $\mathrm{Co}_R(\lambda_i) = \mathrm{Co}_R(\lambda'_i)$ for all i, which would force $\lambda = \lambda'$, since λ and λ' are reduced (see Corollary 2.22). Also note that the exponent $(\mathrm{Co}_R(\lambda_i))_r$ of $\tilde{C}_i(r)$ in D_λ is less than p^{e_r} by the definition of Co_R. (Recall that e_r denotes the cardinality of the p-class of r in A.) As we vary c over all words in $\mathcal{C}$, Lemma 2.14 tells us that the values in $\{\tilde{C}_i(r) : i \in I, r \in R \cap S_i\}$ vary over $\prod_{i\in I}\prod_{r\in R\cap S_i} V_{i,r}$, where $V_{i,r}$ is the set containing 0 and all the powers of $\zeta_{p^{e_r}-1}$. Since no two elements of $V_{i,r}$ are equal to each other modulo p, and since $|V_{i,r}| = p^{e_r}$, which is strictly greater than the highest exponent of $\tilde{C}_i(r)$ appearing in any term (4.26) of (4.25), we may apply Lemma 2.33 to conclude that the minimum p-adic valuation of the right-hand side of (4.25) as c runs through $\mathcal{C}$ is precisely the minimum of the p-adic valuations of the coefficients B_λ as λ runs through Λ_ℓ. So the first half of the theorem tells us that all such coefficients have p-adic valuation at least $\ell^{ss}_{mc}(\mathcal{C})$. We shall show that one such coefficient has p-adic valuation precisely $\ell^{ss}_{mc}(\mathcal{C})$; this will complete our proof.

By Lemma 4.15, there exists a critical $\kappa \in \Lambda_\ell$ such that there is no $\mu \in \Lambda^{ss}_{mc}(\mathcal{C})$ with $\mu \neq \kappa$, $\mathrm{Ti}\,(\mu) = \ell^{ss}_{mc}(\mathcal{C})$, and $\mathrm{Red}(\mu) = \kappa$. Thus the coefficient B_κ, as defined in (4.24), is just

$$B_\kappa = |A|\frac{(\mathrm{pr}_I\,\kappa)!f_{\mathrm{pr}_I\,\kappa}^{(\ell^{ss}_{mc}(\mathcal{C})+1)}}{\kappa!}.$$

Since κ is reduced, we have $\kappa_{i,a} < p$ for all $i \in I$ and $a \in A$ by definition, so the denominator of the fraction is a p-adic unit. Since $|A|$ is coprime to p, we have

$$v_p\left(B_\kappa\right) = v_p\left((\mathrm{pr}_I\,\kappa)!f_{\mathrm{pr}_I\,\kappa}^{(\ell^{ss}_{mc}(\mathcal{C})+1)}\right).$$

Since κ is critical and $\mathrm{Ti}\,(\kappa) = \ell^{ss}_{mc}(\mathcal{C})$, this means that $\mathrm{pr}_I\,\kappa \in \mathbb{N}[I]$ is critical and of tier $\ell^{ss}_{mc}(\mathcal{C})$, so that Theorem 4.16 tells us that $v_p\left((\mathrm{pr}_I\,\kappa)!f_{\mathrm{pr}_I\,\kappa}^{(\ell^{ss}_{mc}(\mathcal{C})+1)}\right) = \ell^{ss}_{mc}(\mathcal{C})$. This completes our proof that there is some word c with $\mathrm{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}}$.

The statements about $\mathrm{ham}^{\mathrm{norm}}$ come immediately, since we showed that $\mathrm{ham}^{\mathrm{norm}}(c) = -\mathrm{zer}^{\mathrm{norm}}(c)$ in Section 2.4. □

4.5 Generic Weights

In this section, we consider an arbitrary weight function $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ and devise lower bounds on the p-adic valuations of weights (as measured with wt) of words of codes in $\mathbb{Z}/p^d\mathbb{Z}[A]$. Note that wt might be symb_r for some $r \in \mathbb{Z}/p^d\mathbb{Z}$, so that we might be counting the number of instances of a particular symbol in our codewords. We form the sectioned weight $\mathrm{wt}_{\mathrm{sec}}\colon (\mathbb{Z}/p^d\mathbb{Z})^d \to \mathbb{Z}$ as described in Section 4.3, and we follow a course not unlike that of the previous section, where we were considering zero counts and Hamming weights. However, here we do not prove the sharpness of our lower bounds, so the proof of Theorem 4.21 here will be considerably simpler than the proof of Theorem 4.18 in the previous section.

In order to p-adically estimate generic weights, we construct a set $\Lambda^{ss}(\mathcal{C})$ of multisets in $\mathbb{N}[I \times A]$ and use $\Lambda^{ss}(\mathcal{C})$ to define the parameter $\ell^{ss}(\mathcal{C})$, which had been defined using sequences in Section 1.1 of the Introduction. We prefer the multiset-based definition here because it will make our calculations easier. We define

$$\Lambda^{ss}(\mathcal{C}) = \{\lambda \in \mathbb{N}[I \times A] : \lambda_0 \in \mathbb{N}[S_0], \ldots, \lambda_{d-1} \in \mathbb{N}[S_{d-1}], \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}]\}. \tag{4.27}$$

Note that $\Lambda^{ss}_{mc}(\mathcal{C})$, which was defined in the last section, is a subset of $\Lambda^{ss}(\mathcal{C})$. The multisets in $\Lambda^{ss}_{mc}(\mathcal{C})$ are the multisets $\lambda \in \Lambda^{ss}(\mathcal{C})$ that satisfy the additional modular condition $|\lambda| \equiv 0 \pmod{p-1}$. Thus $\Lambda^{ss}(\mathcal{C})$ is nonempty, for we showed that $\Lambda^{ss}_{mc}(\mathcal{C})$ is nonempty. Since $\Lambda^{ss}_{mc}(\mathcal{C}) \neq \emptyset$, we may set

$$\omega^{ss}(\mathcal{C}) = \min_{\lambda \in \Lambda^{ss}(\mathcal{C})} \mathrm{Sc}\,(\lambda) \tag{4.28}$$

and

$$\ell^{ss}(\mathcal{C}) = \min_{\lambda \in \Lambda^{ss}(\mathcal{C})} \mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\omega^{ss}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}. \tag{4.29}$$

Note that since $\Lambda^{ss}_{mc}(\mathcal{C}) \subseteq \Lambda^{ss}(\mathcal{C})$, we have $\omega^{ss}_{mc}(\mathcal{C}) \geq \omega^{ss}(\mathcal{C})$ and $\ell^{ss}_{mc}(\mathcal{C}) \geq \ell^{ss}(\mathcal{C})$. In Proposition 4.22 of Section 4.6, we shall see that $\ell^{ss}_{mc}(\mathcal{C})$ is strictly greater than $\ell^{ss}(\mathcal{C})$ for infinitely many codes.

We recall the counting polynomials that we devised in Section 4.2 and cast them into the notation of this section.

Theorem 4.19 (part of Theorem 4.12). *Let* $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ *be an arbitrary weight function. For each* $m \geq 1$*, there exists a polynomial*

$$f^{(m)}(\mathbf{x}) = \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m}} f_\mu^{(m)} \mathbf{x}^\mu$$

in $\mathbb{Q}_p[\mathbf{x}]$ *with the property that* $f^{(m)}(r_0, \ldots, r_{d-1}) \equiv \mathrm{wt}_{\mathrm{sec}}(\pi(r_0), \ldots, \pi(r_{d-1})) \pmod{p^m}$ *for all* $r_0, \ldots, r_{d-1} \in \mathbb{Z}_p$*.*

Proof. Consider the function $F\colon {\mathbb{Z}_p}^d \to \mathbb{Z}$ given by $F(\mathbf{r}) = \mathrm{wt}_{\mathrm{sec}}(\pi(r_1), \ldots, \pi(r_{d-1}))$ for all $\mathbf{r} \in {\mathbb{Z}_p}^d$. This function is (p, d)-periodic by the discussion at the end of Section 4.3. Therefore, we may apply Theorem 4.12 with $t = d$ to obtain a polynomial

$$h(\mathbf{x}) = \sum_{\substack{\mathbf{n} \in \mathbb{N}^t \\ \mathrm{Ti}(\mathbf{n}) < m}} h_{\mathbf{n}} \binom{\mathbf{x}}{\mathbf{n}},$$

with all $h_{\mathbf{n}} \in \mathbb{Z}_p$, such that $h(\mathbf{r}) \equiv F(\mathbf{r}) \pmod{p^m}$ for all $\mathbf{r} \in {\mathbb{Z}_p}^d$. If we expand out any term $\binom{\mathbf{x}}{\mathbf{n}}$ into a $\mathbb{Q}$-linear combination of monomials, all monomials $\mathbf{x}^{\mathbf{j}}$ that appear have $j_i \leq n_i$ for all $i \in I$, so that $\mathrm{Ti}\,(\mathbf{j}) \leq \mathrm{Ti}\,(\mathbf{n})$. Thus we can write

$$h(\mathbf{x}) = \sum_{\substack{\mathbf{n} \in \mathbb{N}^t \\ \mathrm{Ti}(\mathbf{j}) < m}} c_{\mathbf{j}} \mathbf{x}^{\mathbf{j}},$$

with all $c_{\mathbf{j}} \in \mathbb{Q}_p$. Since we identify elements of $\mathbb{N}[I]$ with d-tuples, this is precisely the form of polynomial that we were seeking. □

Now we are ready to estimate weights. The following proposition is the basic calculation:

Proposition 4.20. *Let* $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ *be an arbitrary weight function. Let* $\mathcal{C}$ *be a code in* $\mathbb{Z}/p^d\mathbb{Z}[A]$*. Let* $m \geq 1$ *and let* $f^{(m)}(\mathbf{x})$ *be the polynomial described in Theorem 4.19, which approximates* $\mathrm{wt}_{\mathrm{sec}}(\pi(\cdot), \ldots, \pi(\cdot))$ *modulo* p^m*. For each* $c \in \mathcal{C}$ *and* $i \in I$*, we let* C_i *be the*

element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ *such that* $\tilde{C}_i = \tau \circ \tilde{c}_i$. *For any* $c \in \mathcal{C}$, *we have*

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < m}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m},$$

where $\Lambda^{ss}(\mathcal{C})$ *is as defined in* (4.27) *above.*

Proof. By Corollary 3.4, we have

$$\mathrm{wt}^{\mathrm{norm}}_{\mathrm{sec}}(c_0, \ldots, c_{d-1}) \equiv |A| \sum_{\mu \in \mathbb{N}[I]} \mu! f^{(m)}_{\mu} \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A \lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_0 \in \mathbb{N}[S_0], \ldots, \lambda_{d-1} \in \mathbb{N}[S_{d-1}]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}.$$

By (4.18), the left-hand side becomes $\mathrm{wt}^{\mathrm{norm}}(c)$. Note that the inner sum on the right-hand side sums over those $\lambda \in \Lambda^{ss}(\mathcal{C})$ with $\mathrm{pr}_I \lambda = \mu$. We can restrict the sum over μ to those μ with $\mathrm{Ti}\,(\mu) < m$, since $f^{(m)}_{\mu} = 0$ otherwise (by Theorem 4.19). Thus

$$\begin{aligned} \mathrm{zer}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m}} \mu! f^{(m)}_{\mu} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m} \\ &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m}} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}, \end{aligned}$$

but then condition $\lambda = \mathrm{pr}_I \mu$ means that λ and μ will always have the same score and tier, so we can shift the condition on tier to the sum over λ. Thus

$$\begin{aligned} \mathrm{zer}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\mu \in \mathbb{N}[I]} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu \\ \mathrm{Ti}(\lambda) < m}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m} \\ &\equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < m}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m}. \end{aligned}$$

□

Now we can set bounds on the p-adic valuations of weights.

Theorem 4.21. *Let* $\mathrm{wt}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$ *be an arbitrary weight function. Let* $\mathcal{C}$ *be a code in* $\mathbb{Z}/p^d\mathbb{Z}[A]$. *With* $\ell^{ss}(\mathcal{C})$ *as defined in* (4.29), *we have* $\mathrm{wt}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell^{ss}(\mathcal{C})}}$ *for all*

$c \in \mathcal{C}$.

Proof. For each $c \in \mathcal{C}$ and $i \in I$, we let C_i be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$. If $\ell^{ss}(\mathcal{C}) = 0$, the congruence $\mathrm{wt}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell^{ss}(\mathcal{C})}}$ for all $c \in \mathcal{C}$ is trivial. If $\ell^{ss}_{mc}(\mathcal{C}) > 0$, we use Proposition 4.20 above (setting $m = \ell^{ss}(\mathcal{C})$) to obtain

$$\mathrm{wt}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f^{(\ell^{ss}(\mathcal{C}))}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^{\ell^{ss}(\mathcal{C})}},$$

where $f^{(\ell^{ss}(\mathcal{C}))}(\mathbf{x})$ is the polynomial described in Theorem 4.19, and $\Lambda^{ss}(\mathcal{C})$ is as defined in (4.27). But by the definition of $\ell^{ss}(\mathcal{C})$ as the minimum tier of any element in $\Lambda^{ss}(\mathcal{C})$, we see that the sum on the right-hand side of this congruence is empty, thus proving the theorem. □

4.6 Comparison with Previous Work

Many of the previous results on zero counts and other weights in Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$ do not use the parameters $\omega^{ss}_{mc}(\mathcal{C})$, $\ell^{ss}_{mc}(\mathcal{C})$, $\omega^{ss}(\mathcal{C})$, and $\ell^{ss}(\mathcal{C})$ introduced in Sections 4.4 and 4.5. They instead use parameters like $\omega_{mc}(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\omega(\mathcal{C})$, and $\ell(\mathcal{C})$, which were discussed (along with the aforementioned parameters) in Section 1.1 of the Introduction. The latter group of parameters can be computed solely from knowledge of the support of the Fourier transform of the code, while the former group of parameters requires full knowledge of the tower of supports. We shall define the parameters $\omega_{mc}(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\omega(\mathcal{C})$, and $\ell(\mathcal{C})$ in this section using a construction with multisets. These parameters were defined in the Introduction using sequences, but we shall prefer the multiset-based definitions to facilitate comparison with the parameters $\omega^{ss}_{mc}(\mathcal{C})$, $\ell^{ss}_{mc}(\mathcal{C})$, $\omega^{ss}(\mathcal{C})$, and $\ell^{ss}(\mathcal{C})$, which we have already defined.

First of all, we recall from Section 4.2 the definitions of the score and s-tier of a t-tuple. For $(n_0, \ldots, n_{t-1}) \in \mathbb{Z}^t$, we defined the score, $\mathrm{Sc}\,(n_0, \ldots, n_{t-1}) = n_0 + \cdots + p^{t-1} n_{t-1}$, and the s-tier, $\mathrm{Ti}_s(n_0, \ldots, n_{t-1}) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(n_0,\ldots,n_{t-1}) - p^{s-1}}{(p-1)p^{s-1}} \right\rfloor \right\}$. In Section 4.3, we set the convention (which we retain here) that $I = \{0, 1, \ldots, d-1\}$, so that elements $\mu \in \mathbb{Z}[I]$

are simply d-tuples $(\mu_0, \ldots, \mu_{d-1})$. We also made the convention (which still holds for the remainder of this chapter) that the term "tier" always means d-tier and Ti always means Ti_d. Thus $\mathrm{Ti}\,(n_0, \ldots, n_{t-1}) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(n_0,\ldots,n_{t-1})-p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}$. Furthermore, we extended the notion of score and tier to accounts $\lambda \in \mathbb{Z}[I \times A]$, so that the score of $\lambda \in \mathbb{Z}[I \times A]$ is the score of $\mathrm{pr}_I\,\lambda \in \mathbb{Z}[I]$, and the tier of $\lambda \in \mathbb{Z}[I \times A]$ is the tier of $\mathrm{pr}_I\,\lambda \in \mathbb{Z}[I]$. Then we defined $\ell^{ss}_{mc}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C})$ in Sections 4.4 and 4.5 using scores and tiers of multisets in $\mathbb{N}[I \times A]$.

We shall also use these notions with 1-tuples, i.e., with single numbers, in this section. Thus for $n \in \mathbb{Z}$, we have $\mathrm{Sc}\,(n) = n$, and $\mathrm{Ti}\,(n) = \max\left\{0, \left\lfloor \frac{n-p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}$. We also transport the notion of score and tier to elements of $\mathbb{Z}[A]$. The score of $\lambda \in \mathbb{Z}[A]$, denoted $\mathrm{Sc}\,(\lambda)$, is just $\mathrm{Sc}\,(|\lambda|) = |\lambda|$, and the tier of λ, denoted $\mathrm{Ti}\,(\lambda)$, is just $\mathrm{Ti}\,(|\lambda|)$. Because $\mathrm{Sc}\,(\lambda) = |\lambda|$ for $\lambda \in \mathbb{Z}[A]$, we shall usually use $|\cdot|$ rather than $\mathrm{Sc}\,(\cdot)$ for such accounts.

Recall that we are always considering a code $\mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$ with tower of supports $S_0 \subseteq \cdots \subseteq S_{d-1}$. We shall always set $S = S_{d-1}$, which is the minimal support of the Fourier transform. We continue to assume that at least one of the sets S_i contains an element $a \in A \smallsetminus \{1_A\}$. Thus S contains this element a. We define

$$\Lambda_{mc}(\mathcal{C}) = \{\lambda \in \mathbb{N}[S] : \Pi\lambda = 1_A, \mathrm{pr}_A\,\lambda \notin \mathbb{N}[\{1_A\}], |\lambda| \equiv 0 \pmod{p-1}\}. \tag{4.30}$$

We claim that $\Lambda_{mc}(\mathcal{C})$ is nonempty. By assumption, there exists $a \in S$ with $a \neq 1_A$. Let n be the group-theoretic order of a. Then note that the multiset λ with $(p-1)n$ instances of the element a and no other elements is a unity-product but not all-unity multiset in $\mathbb{N}[S]$ with $(p-1)n$ elements. Since $\Lambda_{mc}(\mathcal{C}) \neq \emptyset$, we may set

$$\omega_{mc}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}(\mathcal{C})} |\lambda| \tag{4.31}$$

and

$$\ell_{mc}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}(\mathcal{C})} \mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\omega_{mc}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}. \tag{4.32}$$

We also define

$$\Lambda(\mathcal{C}) = \{\lambda \in \mathbb{N}[S] : \Pi\lambda = 1_A, \mathrm{pr}_A\,\lambda \notin \mathbb{N}[\{1_A\}]\}. \tag{4.33}$$

Since $\Lambda_{mc}(\mathcal{C}) \subseteq \Lambda(\mathcal{C})$, we know that $\Lambda(\mathcal{C})$ is not empty. Thus we may set

$$\omega(\mathcal{C}) = \min_{\lambda \in \Lambda(\mathcal{C})} |\lambda| \tag{4.34}$$

and

$$\ell(\mathcal{C}) = \min_{\lambda \in \Lambda(\mathcal{C})} \mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\omega(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor \right\}. \tag{4.35}$$

Most previous works use the parameters $\ell_{mc}(\mathcal{C})$ and $\ell(\mathcal{C})$. Therefore, we compare them with each other and with $\ell^{ss}_{mc}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C})$. The proof of the following proposition is straightforward, but lengthy, so we delay its appearance until the end of this section.

Proposition 4.22. *Let $e = 1$. For any code $\mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$, we have*

(i) $\omega(\mathcal{C}) \leq \omega_{mc}(\mathcal{C})$ *and* $\ell(\mathcal{C}) \leq \ell_{mc}(\mathcal{C})$;

(ii) $\omega^{ss}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$ *and* $\ell^{ss}(\mathcal{C}) \leq \ell^{ss}_{mc}(\mathcal{C})$;

(iii) $\omega(\mathcal{C}) \leq \omega^{ss}(\mathcal{C})$ *and* $\ell(\mathcal{C}) \leq \ell^{ss}(\mathcal{C})$; *and*

(iv) $\omega_{mc}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$ *and* $\ell_{mc}(\mathcal{C}) \leq \ell^{ss}_{mc}(\mathcal{C})$.

If $p = 2$, then equality holds in (i) *and* (ii). *If $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module, then equality holds in* (iii) *and* (iv). *Thus for $d = 1$, equality holds in* (iii) *and* (iv).

For each $p > 2$ and $d > 1$, there are infinitely many codes such that the inequalities in (i)–(iv) *are simultaneously strict, with $\ell(\mathcal{C}) < \ell_{mc}(\mathcal{C}) < \ell^{ss}(\mathcal{C}) < \ell^{ss}_{mc}(\mathcal{C})$. Indeed, we can find a family of codes where, for any M, there exists a code in the family such that each term in our chain of inequalities is greater than the last by M or more.*

If $p = 2$, then for each $d > 1$, there are infinitely many codes such that the inequalities in (iii) *(or equivalently, in* (iv)*) are strict and where $\omega(\mathcal{C})$ and $\omega^{ss}(\mathcal{C})$ are even. Indeed, we can find a family of codes wherein $\ell^{ss}(\mathcal{C}) - \ell(\mathcal{C})$ and $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ are unbounded as $\mathcal{C}$ runs over the family.*

For each $p > 2$ and $d \geq 1$, there are infinitely many codes that are free $\mathbb{Z}/p^d\mathbb{Z}$-modules such that strict inequality holds in (i) *(or equivalently, in* (ii)*). Indeed, we can find a family of codes wherein $\ell_{mc}(\mathcal{C}) - \ell(\mathcal{C})$ is unbounded as $\mathcal{C}$ runs over the family.*

In all instances of strict inequality mentioned above, the groups A underlying the codes can be chosen to be cyclic, and the codes themselves can be chosen so that 1_A is not in the supports of their Fourier transforms. Furthermore, in instances where $p = 2$, the groups A can be chosen to be cyclic groups, each of which has order $2^n - 1$ for some integer n (but not the same integer n for all codes).

Finally, for $p = 2$ and for each $d \geq 1$, there exist infinitely many cyclic codes $\mathcal{C}$, each of length $2^n - 1$ for some n, that are free $Z/2^d\mathbb{Z}$-modules with 1_A not in the supports of their Fourier transforms, and that have $\omega(\mathcal{C})$ even.

Now that we have some notion of the relationship between the four parameters $\ell(\mathcal{C})$, $\ell_{mc}(\mathcal{C})$, $\ell^{ss}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C})$, we can compare our theorems with previous results. The strongest result on Hamming weights and zero counts in Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$ was published by this author as part of this research program.

Theorem 4.23 (D. J. Katz [29]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. With $\ell_{mc}(\mathcal{C})$ as defined in* (4.32)*, we have* $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$. Equivalently,* $\mathrm{ham}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$.*

Theorem 4.18 gives a stronger lower bound on p-adic valuations of normalized weights because $\ell^{ss}_{mc}(\mathcal{C}) \geq \ell_{mc}(\mathcal{C})$ by Proposition 4.22. Indeed, Proposition 4.22 shows that $\ell^{ss}_{mc}(\mathcal{C}) > \ell_{mc}(\mathcal{C})$ for infinitely many codes. Furthermore, Theorem 4.18 shows that the bounds it furnishes are sharp, while Theorem 4.23 here includes no information about sharpness, even though its bound is sharp for free $\mathbb{Z}/p^d\mathbb{Z}$-modules. This sharpness is a consequence of Theorem 4.18 and the fact (from Proposition 4.22) that $\ell^{ss}_{mc}(\mathcal{C}) = \ell_{mc}(\mathcal{C})$ when $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module.

The strongest result on generic weights is due to Wilson, although a slightly generalized version has been published by the author as part of this research program.

Theorem 4.24 (Wilson [65]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with A cyclic and with 1_A not in the support S of the Fourier transform of $\mathcal{C}$. Let $\ell(\mathcal{C})$ be as defined in* (4.35)*. For any $r \in \mathbb{Z}/p^d\mathbb{Z}$ with $r \neq 0$ and any $c \in \mathcal{C}$, the number of instances of symbol r in c is divisible by $p^{\ell(\mathcal{C})}$.*

The author generalized this result of Wilson to produce a version that assumes neither that A is cyclic nor that $1_A \notin S$. Recall from Section 2.4 that symb_r is the weight function that counts the number of instances of the symbol r in a codeword c. Thus $\text{symb}_r^{\text{norm}}(c)$ is the number of instances of r in c unless $\tilde{c}(1_A) = r$, in which case $\text{symb}_r^{\text{norm}}(c)$ is $-|A|$ plus the number of instances of r.

Theorem 4.25 (D. J. Katz [29]). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. Let $\ell(\mathcal{C})$ be as defined in* (4.35). *For any $r \in \mathbb{Z}/p^d\mathbb{Z}$, we have* $\text{symb}_r^{\text{norm}} \equiv 0 \pmod{p^{\ell(\mathcal{C})}}$.

Theorem 4.21 is stronger than both of these (Theorems 4.24 and 4.25). For Theorem 4.21 can be applied with the weight function wt set equal to symb_r, thus giving a theorem resembling Theorem 4.25 above, but with $\ell^{ss}(\mathcal{C})$ in place of $\ell(\mathcal{C})$. Proposition 4.22 tells us that $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$ for all codes and that $\ell^{ss}(\mathcal{C}) > \ell(\mathcal{C})$ for infinitely many codes. Thus Theorem 4.21 is stronger than Theorems 4.25 and 4.24 for infinitely many codes.

The first analogues of McEliece's theorem for Hamming weights and generic weights in Abelian codes over $\mathbb{Z}/p^d\mathbb{Z}$ were the results of Calderbank, Li, and Poonen [7]. We shall see that these results are weaker than Theorems 4.23 and 4.24 presented above, and hence weaker than Theorems 4.18 and 4.21 proved in this thesis. For Hamming weights, Calderbank, Li, and Poonen give a theorem for cyclic codes over $\mathbb{Z}/4\mathbb{Z}$.

Theorem 4.26 (Calderbank-Li-Poonen [7]). *Let $p = 2$ and let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$ with A cyclic and 1_A not in the support S of the Fourier transform of $\mathcal{C}$. Then* $\text{ham}(c)$ *is divisible by* $\max\left\{2^{\left\lceil \frac{\omega(\mathcal{C})}{2} \right\rceil - 2}, 2^{\left\lceil \frac{\omega(\mathcal{C})}{3} \right\rceil - 1}\right\}$.

Note that when $\mathbb{Z}/p^d\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$, $\ell_{mc}(\mathcal{C}) = \ell(\mathcal{C})$ (by Proposition 4.22), and $\ell(\mathcal{C}) = \max\left\{0, \left\lfloor \frac{\omega(\mathcal{C})}{2} \right\rfloor - 1\right\}$ (see (4.35)). Note also that $\omega(\mathcal{C}) \geq 2$, since we cannot have a unity-product and not all-unity element of $\mathbb{N}[A]$ with less than two elements. Thus, for admissible values of $\omega(\mathcal{C})$, we have $\ell_{mc}(\mathcal{C}) \geq \max\left\{\left\lceil \frac{\omega(\mathcal{C})}{2} \right\rceil - 2, \left\lceil \frac{\omega(\mathcal{C})}{3} \right\rceil - 1\right\}$, with equality when $\omega(\mathcal{C})$ is 2, 4, or an odd number, and with strict inequality (the left-hand side is one larger than the right) when $\omega(\mathcal{C})$ is an even number greater than or equal to 6. Thus, Theorem 4.26 is not as strong Theorem 4.23, and hence not as strong as Theorem 4.18.

For generic weights, Calderbank, Li, and Poonen give a theorem for cyclic codes over $\mathbb{Z}/2^d\mathbb{Z}$.

Theorem 4.27 (Calderbank-Li-Poonen [7]). *Let $p = 2$ and let $\mathcal{C}$ be a code in $\mathbb{Z}/2^d\mathbb{Z}[A]$ with A cyclic and 1_A not in the support S of the Fourier transform of $\mathcal{C}$. Then for any nonzero symbol $r \in \mathbb{Z}/p^d\mathbb{Z}$, the number of instances of r in any $c \in \mathcal{C}$ is divisible by $2^{\left\lceil \frac{\omega(\mathcal{C})}{2^{d-1}} \right\rceil - 2}$.*

Note that when $p = 2$, we have $\ell(\mathcal{C}) = \max\left\{0, \left\lfloor \frac{\omega(\mathcal{C})}{2^{d-1}} \right\rfloor - 1\right\}$ (see (4.35)). When $\omega(\mathcal{C}) < 2^d$, neither Theorem 4.24 nor Theorem 4.27 tells us anything, so we shall compare the two results when $\omega(\mathcal{C}) \geq 2^d$. Note that $\ell(\mathcal{C}) \geq \left\lceil \frac{\omega(\mathcal{C})}{2^{d-1}} \right\rceil - 2$ for all values of $\omega(\mathcal{C}) \geq 2^d$, with the left-hand side greater by one if $2^{d-1} \mid \omega(\mathcal{C})$. Otherwise the two sides of our inequality are equal. Thus, Theorem 4.27 is not as strong as Theorem 4.24, and hence not as strong as Theorem 4.21.

In the case when $d = 1$, i.e., in the case when $\mathbb{Z}/p^d\mathbb{Z}$ is the prime field $\mathbb{F}_p$, we shall recover from Theorem 4.18 the theorem of McEliece on the zero counts of cyclic codes over $\mathbb{F}_p$ (Theorem 1 of [37], presented in part as Theorem 1.1). When $d = 1$, all codes are free $\mathbb{Z}/p^d\mathbb{Z}$-modules (since they are $\mathbb{F}_p$-vector spaces), so $\ell^{ss}_{mc}(\mathcal{C}) = \ell_{mc}(\mathcal{C})$ by Proposition 4.22. The following theorem synthesizes the actual content of the theorem McEliece stated, along with other comments made in McEliece's paper, while adapting it to the notation and terminology of this thesis. The only sense in which it is more general than the theorem of McEliece is that McEliece assumes that the group A is cyclic. Since removing this assumption is not difficult, we have labeled the theorem here as "slightly generalized." Indeed, Delsarte and McEliece [18] later removed this assumption when they generalized this theorem to Abelian codes over arbitrary finite fields (see Theorem 1.2 in the Introduction).

Theorem 4.28 (McEliece [37], slightly generalized). *Let $d = 1$. Let $\mathcal{C}$ be a code in $\mathbb{F}_p[A]$. For each $c \in \mathcal{C}$, we let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C} = \tau \circ \tilde{c}$. Let $\Lambda_{mc}(\mathcal{C})$ and $\ell_{mc}(\mathcal{C})$ be as defined in (4.30) and (4.32). Then for each $c \in \mathcal{C}$, we have*

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A|(-p)^{\ell_{mc}(\mathcal{C})} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ |\lambda| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^{\ell_{mc}(\mathcal{C})+1}}, \tag{4.36}$$

where $\lambda!$ *is a unit in* $\mathbb{Z}_p$ *for each* $\lambda \in \Lambda_{mc}(\mathcal{C})$ *with* $|\lambda| = (\ell_{mc}(\mathcal{C}) + 1)(p-1)$. *Furthermore,*

$$\sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ |\lambda| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{\tilde{C}(\lambda)}{\lambda!}$$

assumes values in $\mathbb{Z}_p$, *and so* $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$. *There is some* $c \in \mathcal{C}$ *such that* $\mathrm{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$.

We defer the derivation of this theorem from Theorem 4.18 for a moment to develop some tools that will help in the proof. These tools will also be useful in the proof of Proposition 4.22, which, as promised, concludes this section.

We have been comparing the results of this chapter, which use the parameters $\ell^{ss}_{mc}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C})$, with previous results, which use the parameters $\ell_{mc}(\mathcal{C})$ and $\ell(\mathcal{C})$. Since $\ell_{mc}(\mathcal{C})$ and $\ell(\mathcal{C})$ are based on cardinalities of multisets in $\mathbb{N}[A]$ and $\ell^{ss}_{mc}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C})$ are based on cardinalities of multisets in $\mathbb{N}[I \times A]$, we first devise a correspondence between such accounts that will help us to relate these parameters.

For the rest of this section, let $\Phi\colon \mathbb{N}[I \times A] \to \mathbb{N}[A]$ be defined by $\Phi(\lambda) = \sum_{i \in I} \lambda_i$, and let $\Psi\mathbb{N}[A] \to \mathbb{N}[I \times A]$ be defined so that $\Psi(\kappa)$ is the multiset λ with $\lambda_i = \emptyset$ for all $i \in \{0, 1, \ldots, d-2\}$ and $\lambda_{d-1} = \kappa$. Then we have the following basic facts about these maps:

Lemma 4.29. *Let* $\lambda \in \mathbb{N}[I \times A]$ *and* $\kappa \in \mathbb{N}[A]$. *Then*

(i) $\Phi \circ \Psi$ *is the identity on* $\mathbb{N}[A]$, *so that* Φ *is surjective and* Ψ *is injective.*

(ii) Φ *and* Ψ *preserve the cardinality of multisets.*

(iii) $\Pi\Phi(\lambda) = \Pi\lambda$ *and* $\Pi\Psi(\kappa) = \Pi\kappa$.

(iv) $\Phi(\lambda)$ *is all-unity if and only if* λ *is all unity;* $\Psi(\kappa)$ *is all-unity if and only if* κ *is all-unity.*

(v) *If* $\lambda_i \in \mathbb{N}[S_i]$ *for all* $i \in I$, *then* $\Phi(\lambda) \in \mathbb{N}[S]$, *and if* $\kappa \in \mathbb{N}[S]$, *then* $(\Psi(\kappa))_i \in \mathbb{N}[S_i]$ *for all* $i \in I$.

(vi) $\Phi(\Lambda^{ss}(\mathcal{C})) = \Lambda(\mathcal{C})$ *and* $\Phi(\Lambda^{ss}_{mc}(\mathcal{C})) = \Lambda_{mc}(\mathcal{C})$.

(vii) *If* $\lambda \in \mathbb{N}[I \times A]$, *then* $|\Phi(\lambda)| \leq \mathrm{Sc}\,(\lambda)$ *and* $\mathrm{Ti}\,(\Phi(\lambda)) \leq \mathrm{Ti}\,(\lambda)$.

(viii) *If* $\kappa \in \mathbb{N}[A]$, *then* $\mathrm{Sc}\,(\Psi(\kappa)) = p^{d-1}|\kappa|$ *and* $\mathrm{Ti}\,(\Psi(\kappa)) \geq \mathrm{Ti}\,(\kappa)$.

(ix) *If* $d = 1$, *then* Ψ *and* Φ *are inverses of each other,* $|\Phi(\lambda)| = \mathrm{Sc}\,(\lambda)$, $\mathrm{Ti}\,(\Phi(\lambda)) = \mathrm{Ti}\,(\lambda)$, *and* $\Phi(\lambda)! = \lambda!$.

Proof. The first two statements are obvious. To prove (iii), we note that we have $\Pi\Phi(\lambda) = \Pi\left(\sum_{i\in I}\lambda_i\right) = \prod_{i\in I}(\Pi\lambda_i) = \Pi\lambda$. Then $\Pi\Psi(\kappa) = \Pi\Phi(\Psi(\kappa)) = \Pi\kappa$. The fourth statement is obvious. To prove (v), note that $S = S_{d-1}$ and that $S_i \subseteq S_{d-1}$ for all $i \in I$. Thus if $\lambda_i \in \mathbb{N}[S_i]$ for all $i \in I$, then we clearly have $\Phi(\lambda) \in \mathbb{N}[S]$. Conversely, if $\kappa \in \mathbb{N}[S]$, then $(\Psi(\kappa))_{d-1} \in \mathbb{N}[S_{d-1}]$ and $(\Psi(\kappa))_i = \emptyset \in \mathbb{N}[S_i]$ for $i < d-1$. To prove (vi), note that (iii)–(v) show that $\Phi(\Lambda^{ss}(\mathcal{C})) \subseteq \Lambda(\mathcal{C})$ and $\Psi(\Lambda(\mathcal{C})) \subseteq \Lambda^{ss}(\mathcal{C})$. Since Φ is a left-inverse of Ψ, this proves that $\Phi(\Lambda^{ss}(\mathcal{C})) = \Lambda(\mathcal{C})$. Likewise, (ii)–(v) show that $\Phi(\Lambda^{ss}_{mc}(\mathcal{C})) \subseteq \Lambda_{mc}(\mathcal{C})$ and $\Psi(\Lambda_{mc}(\mathcal{C})) \subseteq \Lambda^{ss}_{mc}(\mathcal{C})$. Again, since Φ is a left-inverse of Ψ, this proves that $\Phi(\Lambda^{ss}_{mc}(\mathcal{C})) = \Lambda_{mc}(\mathcal{C})$. For (vii), note that $|\Phi(\lambda)| = |\lambda| \leq \mathrm{Sc}\,(\lambda)$. For (viii), note that $\mathrm{Sc}\,(\Psi(\kappa)) = p^{d-1}|\Psi(\kappa)| = p^{d-1}|\kappa|$. For (ix), Ψ and Φ are clearly inverses when $d = 1$. Furthermore, if $d = 1$ and $\lambda \in \mathbb{N}[I \times A]$, then we have $\mathrm{Sc}\,(\lambda) = |\lambda| = |\Phi(\lambda)|$ and $\Phi(\lambda)! = \lambda_0! = \lambda!$. □

Now we give the proof McEliece's theorem (Theorem 4.28) as a consequence of Theorem 4.18.

Proof of Theorem 4.28. Note that here $I = \{0\}$, so that for any $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$, the account $\mathrm{pr}_I\,\lambda$ is the 1-tuple with entry $|\lambda_0| = |\lambda|$. Further, if $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$, then $\mathrm{Sc}\,(\lambda) = |\lambda|$ and $\mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{|\lambda|-1}{p-1} \right\rfloor\right\} = \frac{|\lambda|}{p-1} - 1$, where the last equality uses the fact that $|\lambda| \equiv 0 \pmod{p-1}$ and $|\lambda| > 0$ for all $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$. Therefore, to say that $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$ is of tier m is precisely to say that $|\lambda| = (m+1)(p-1)$. With this in mind, we specialize congruence (4.23) in Theorem 4.18 for the case $d = 1$ to obtain

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda\in\Lambda^{ss}_{mc}(\mathcal{C}) \\ |\lambda|=(\ell^{ss}_{mc}(\mathcal{C})+1)(p-1)}} \frac{|\lambda|!\, f_{|\lambda|}^{(\ell^{ss}_{mc}(\mathcal{C})+1)}}{\lambda!}\tilde{C}_0(\lambda_0) \pmod{p^{\ell^{ss}_{mc}(\mathcal{C})+1}},$$

where $f^{(\ell_{mc}^{ss}(\mathcal{C})+1)}(\mathbf{x})$ is the polynomial described in Theorem 4.16. Equivalently, we have

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ |\lambda| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{|\lambda|! f_{|\lambda|}^{(\ell_{mc}(\mathcal{C})+1)}}{\lambda!} \tilde{C}_0(\lambda_0) \pmod{p^{\ell_{mc}(\mathcal{C})+1}}, \tag{4.37}$$

since $\ell_{mc}^{ss}(\mathcal{C}) = \ell_{mc}(\mathcal{C})$ when $d = 1$ by Proposition 4.22. Let

$$Y(c) = \sum_{\substack{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) \\ |\lambda| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{[(\ell_{mc}(\mathcal{C})+1)(p-1)]! f_{(\ell_{mc}(\mathcal{C})+1)(p-1)}^{(\ell_{mc}(\mathcal{C})+1)}}{\lambda!} \tilde{C}_0(\lambda_0),$$

which is the right-hand side of congruence (4.37). By Theorem 4.18 (along with the fact that $\ell_{mc}^{ss}(\mathcal{C}) = \ell_{mc}(\mathcal{C})$ from Proposition 4.22), we know that $Y(c)$ assumes values in $p^{\ell_{mc}(\mathcal{C})}\mathbb{Z}_p$ for all $c \in \mathcal{C}$, but that there is some $c \in \mathcal{C}$ such that $Y(c)$ is not in $p^{\ell_{mc}(\mathcal{C})+1}\mathbb{Z}_p$. We shall show that $Y(c)$ is closely related to the right-hand side of congruence (4.36).

To do this, we use the maps $\Phi\colon \mathbb{N}[I \times A] \to \mathbb{N}[A]$ and $\Psi\colon \mathbb{N}[A] \to \mathbb{N}[I \times A]$ defined before Lemma 4.29. In Lemma 4.29, (ix), (vi), (ii) we see that Φ is a bijection with inverse Ψ, $\Phi(\Lambda_{mc}^{ss}(\mathcal{C})) = \Lambda_{mc}(\mathcal{C})$, and Φ preserves cardinality, so Ψ establishes a bijection between $\{\kappa \in \Lambda_{mc}(\mathcal{C}) : |\kappa| = \ell_{mc}^{ss}(\mathcal{C})\}$ and $\{\lambda \in \Lambda_{mc}^{ss}(\mathcal{C}) : |\lambda| = \ell_{mc}^{ss}(\mathcal{C})\}$. Thus we may re-index our sum

$$Y(c) = |A| \sum_{\substack{\kappa \in \Lambda_{mc}(\mathcal{C}) \\ |\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{[(\ell_{mc}(\mathcal{C})+1)(p-1)]! f_{(\ell_{mc}(\mathcal{C})+1)(p-1)}^{(\ell_{mc}(\mathcal{C})+1)}}{\Psi(\kappa)!} \tilde{C}_0([\Psi(\kappa)]_0).$$

Furthermore, by the definition of Ψ and the fact that $d = 1$, we have $[\Psi(\kappa)]_0 = \kappa$. We also have $\tilde{C}_0 = \tilde{C}$ by the definition of the canonical expansion and since $d = 1$. Also note that Lemma 4.29, (ix) tells us that $\Psi(\kappa)! = \kappa!$. So we have

$$Y(c) = |A| \sum_{\substack{\kappa \in \Lambda_{mc}(\mathcal{C}) \\ |\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} [(\ell_{mc}(\mathcal{C})+1)(p-1)]! f_{(\ell_{mc}(\mathcal{C})+1)(p-1)}^{(\ell_{mc}(\mathcal{C})+1)} \frac{\tilde{C}(\kappa)}{\kappa!}.$$

This is quite close to the right-hand side of (4.36). Now note that the 1-tuple $(\ell_{mc}(\mathcal{C}) + 1)(p-1)$ is critical (see the definition before Lemma 4.8) and of tier $\ell_{mc}(\mathcal{C})$, so that Theorem

4.16 tells us that $[(\ell_{mc}(\mathcal{C})+1)(p-1)]!f^{(\ell_{mc}(\mathcal{C})+1)}_{(\ell_{mc}(\mathcal{C})+1)(p-1)} \equiv (-p)^{\ell_{mc}(\mathcal{C})} \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$. Since $f^{(\ell_{mc}(\mathcal{C})+1)}(\mathbf{x}) \in \mathbb{Q}_p[\mathbf{x}]$ by Theorem 4.16, this means that there is some unit $u \in \mathbb{Z}_p$ with $u \equiv 1 \pmod{p}$ such that $u[(\ell_{mc}(\mathcal{C})+1)(p-1)]!f^{(\ell_{mc}(\mathcal{C})+1)}_{(\ell_{mc}(\mathcal{C})+1)(p-1)} = (-p)^{\ell_{mc}(\mathcal{C})}$. Since $Y(c)$ always vanishes modulo $p^{\ell_{mc}(\mathcal{C})}$, we have $Y(c) \equiv uY(c) \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$ for all $c \in \mathcal{C}$.

Recall that $Y(c)$ was defined to be the right-hand side of (4.37). Thus we have

$$\begin{aligned}
\operatorname{zer}^{\operatorname{norm}}(c) &\equiv Y(c) \pmod{p^{\ell_{mc}(\mathcal{C})+1}} \\
&\equiv uY(c) \pmod{p^{\ell_{mc}(\mathcal{C})+1}} \\
&= |A|(-p)^{\ell_{mc}(\mathcal{C})} \sum_{\substack{\kappa \in \Lambda_{mc}(\mathcal{C}) \\ |\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{\tilde{C}(\kappa)}{\kappa!},
\end{aligned}$$

which gives us (4.36). We know that u is a unit in $\mathbb{Z}_p$, that $Y(c) \in p^{\ell_{mc}(\mathcal{C})}\mathbb{Z}_p$ for all $c \in \mathcal{C}$, and that $Y(c) \notin p^{\ell_{mc}(\mathcal{C})+1}\mathbb{Z}_p$ for some $c \in \mathcal{C}$. So we know that $uY(c) \in p^{\ell_{mc}(\mathcal{C})}\mathbb{Z}_p$ for all $c \in \mathcal{C}$ and that $uY(c) \notin p^{\ell_{mc}(\mathcal{C})+1}\mathbb{Z}_p$ for some $c \in \mathcal{C}$. Thus

$$\sum_{\substack{\kappa \in \Lambda_{mc}(\mathcal{C}) \\ |\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)}} \frac{\tilde{C}(\kappa)}{\kappa!}$$

is an element of $\mathbb{Z}_p$ for all $c \in \mathcal{C}$ and is not an element of $p\mathbb{Z}_p$ for some $c \in \mathcal{C}$. So $\operatorname{zer}^{\operatorname{norm}} \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, and $\operatorname{zer}^{\operatorname{norm}} \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$ for some $c \in \mathcal{C}$.

Finally, we claim that all $\kappa \in \Lambda_{mc}(\mathcal{C})$ with $|\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)$ are reduced. If not, then Lemma (2.21) would give us a $\nu \in \Lambda_{mc}(\mathcal{C})$ with $|\nu| \leq \ell_{mc}(\mathcal{C})(p-1)$, so that $\operatorname{Ti}(\nu) < \ell_{mc}(\mathcal{C})$, thus contradicting the definition of $\ell_{mc}(\mathcal{C})$. Thus all $\kappa \in \Lambda_{mc}(\mathcal{C})$ with $|\kappa| = (\ell_{mc}(\mathcal{C})+1)(p-1)$ have $\kappa_a < p$ for all $a \in A$, so that $\kappa!$ is a unit in $\mathbb{Z}_p$. □

We conclude this chapter with the proof of Proposition 4.22.

Proof of Proposition 4.22. Looking at definitions (4.33), (4.30), (4.27), and (4.19) of $\Lambda(\mathcal{C})$, $\Lambda_{mc}(\mathcal{C})$, $\Lambda^{ss}(\mathcal{C})$, and $\Lambda^{ss}_{mc}(\mathcal{C})$, we see that $\Lambda(\mathcal{C}) \supseteq \Lambda_{mc}(\mathcal{C})$ and $\Lambda^{ss}(\mathcal{C}) \supseteq \Lambda^{ss}_{mc}(\mathcal{C})$. This shows that $\omega(\mathcal{C}) \leq \omega_{mc}(\mathcal{C})$ and $\omega^{ss}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$, so that $\ell(\mathcal{C}) \leq \ell_{mc}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C}) \leq \ell^{ss}_{mc}(\mathcal{C})$, which proves (i) and (ii).

Let $\lambda \in \Lambda^{ss}(\mathcal{C})$ with $\operatorname{Sc}(\lambda)$ and $\operatorname{Ti}(\lambda)$ minimal, i.e., $\operatorname{Sc}(\lambda) = \omega^{ss}(\mathcal{C})$ and $\operatorname{Ti}(\lambda) = \ell^{ss}(\mathcal{C})$.

Then by Lemma 4.29, (vi) and (vii), we have $\Phi(\lambda) \in \Lambda(\mathcal{C})$, $|\Phi(\lambda)| \leq \mathrm{Sc}\,(\lambda) = \omega^{ss}(\mathcal{C})$, and $\mathrm{Ti}\,(\Phi(\lambda)) \leq \mathrm{Ti}\,(\lambda) = \ell^{ss}(\mathcal{C})$. So $\omega(\mathcal{C}) \leq \omega^{ss}(\mathcal{C})$ and $\ell(\mathcal{C}) \leq \ell^{ss}(\mathcal{C})$. This proves (iii). By the same argument, if $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$ with $\mathrm{Sc}\,(\lambda) = \omega^{ss}_{mc}(\mathcal{C})$ and $\mathrm{Ti}\,(\lambda) = \ell^{ss}_{mc}(\mathcal{C})$, then $\Phi(\lambda) \in \Lambda_{mc}(\mathcal{C})$ with $|\Phi(\lambda)| \leq \mathrm{Sc}\,(\lambda) = \omega^{ss}_{mc}(\mathcal{C})$ and $\mathrm{Ti}\,(\Phi(\lambda)) \leq \mathrm{Ti}\,(\lambda) = \ell^{ss}_{mc}(\mathcal{C})$, so that $\omega_{mc}(\mathcal{C}) \leq \omega^{ss}_{mc}(\mathcal{C})$ and $\ell_{mc}(\mathcal{C}) \leq \ell^{ss}_{mc}(\mathcal{C})$. This proves (iv).

If $p = 2$, then the condition $|\lambda| \equiv 0 \pmod{p-1}$ in the definitions (4.30) and (4.19) of $\Lambda_{mc}(\mathcal{C})$ and $\Lambda^{ss}_{mc}(\mathcal{C})$ is trivial, so that $\Lambda_{mc}(\mathcal{C}) = \Lambda(\mathcal{C})$ (compare (4.30) with (4.33)) and $\Lambda^{ss}_{mc}(\mathcal{C}) = \Lambda^{ss}(\mathcal{C})$ (compare (4.19) with (4.27)). Thus, equality holds in (i) and (ii) in this case.

Suppose that $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module in this paragraph. Then $S_0 = \cdots = S_{d-1} = S$ by Lemma 2.13. Let $\kappa \in \Lambda(\mathcal{C})$. Then we set $\lambda \in \mathbb{N}[I \times A]$ so that $\lambda_0 = \kappa$ and $\lambda_i = \emptyset$ for all $i \in I$ with $i \neq 0$. Since $\kappa \in \mathbb{N}[S]$ and $S_0 = S$, we have $\lambda_0 \in \mathbb{N}[S_0]$, and of course $\lambda_i \in \mathbb{N}[S_i]$ for all $i \neq 0$. Also $\Pi\lambda = \Pi\lambda_0 = \Pi\kappa = 1_A$, and λ is not all-unity since κ is not all-unity. So $\lambda \in \Lambda^{ss}(\mathcal{C})$. Furthermore, if we originally had $\kappa \in \Lambda_{mc}(\mathcal{C})$, then $|\lambda| = |\kappa| \equiv 0 \pmod{p-1}$, so that $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$. So $\lambda \in \Lambda^{ss}(\mathcal{C})$ (resp., $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$) if $\kappa \in \Lambda(\mathcal{C})$ (resp., $\kappa \in \Lambda_{mc}(\mathcal{C})$). Also note that $\mathrm{Sc}\,(\lambda) = |\kappa|$, so that $\mathrm{Ti}\,(\lambda) = \mathrm{Ti}\,(\kappa)$. Suppose we had chosen $\kappa \in \Lambda(\mathcal{C})$ (resp., $\kappa \in \Lambda_{mc}(\mathcal{C})$) so that $|\kappa| = \omega(\mathcal{C})$ and $\mathrm{Ti}\,(\kappa) = \ell(\mathcal{C})$ (resp., $|\kappa| = \omega_{mc}(\mathcal{C})$ and $\mathrm{Ti}\,(\kappa) = \ell_{mc}(\mathcal{C})$). Then the λ that we have derived from κ by the procedure outlined above has $\lambda \in \Lambda^{ss}(\mathcal{C})$ with $\mathrm{Sc}\,(\lambda) = |\kappa| = \omega(\mathcal{C})$ and $\mathrm{Ti}\,(\lambda) = \mathrm{Ti}\,(\kappa) = \ell(\mathcal{C})$ (resp., $\lambda \in \Lambda^{ss}_{mc}(\mathcal{C})$ with $\mathrm{Sc}\,(\lambda) = |\kappa| = \omega_{mc}(\mathcal{C})$ and $\mathrm{Ti}\,(\lambda) = \mathrm{Ti}\,(\kappa) = \ell_{mc}(\mathcal{C})$). Thus $\omega^{ss}(\mathcal{C}) \leq \omega(\mathcal{C})$ and $\ell^{ss}(\mathcal{C}) \leq \ell(\mathcal{C})$ (resp., $\omega^{ss}_{mc}(\mathcal{C}) \leq \omega_{mc}(\mathcal{C})$ and $\ell^{ss}_{mc}(\mathcal{C}) \leq \ell_{mc}(\mathcal{C})$). These inequalities, combined with the opposite inequalities (iii) (resp., (iv)), show that $\omega^{ss}(\mathcal{C}) = \omega(\mathcal{C})$, $\ell^{ss}(\mathcal{C}) = \ell(\mathcal{C})$, $\omega^{ss}_{mc}(\mathcal{C}) = \omega_{mc}(\mathcal{C})$, and $\ell^{ss}_{mc}(\mathcal{C}) = \ell_{mc}(\mathcal{C})$ when $\mathcal{C}$ is a free $\mathbb{Z}/p^d\mathbb{Z}$-module. If $d = 1$, all codes are free $\mathbb{F}_p$-modules, since all $\mathbb{F}_p$-modules (i.e., $\mathbb{F}_p$-vector spaces) are free.

We construct two families of codes (for arbitrary p and d) that will allow us to prove our inequalities to be strict for infinitely many codes. To help us in our proofs, we define the *p-ary weight* of any nonnegative integer k, denoted $w_p(k)$, to be the sum of the digits in the p-ary expansion of k, i.e., if $k = k_0 + k_1 p + \cdots + k_s p^s$ with $0 \leq k_j < p$ for all j, then $w_p(k) = k_0 + \cdots + k_s$.

The first construction: Set $m > 0$ and let $n = p^{2(d-1)+m}$. We let A be the cyclic group of order $(p^n - 1)/(p - 1)$ generated by γ. For each k, set $T_k = \{\gamma^j : j \in \mathbb{N}, w_p(j) = k\}$. Note that since $w_p(pj) = w_p(j)$, each set T_k is p-closed. We set $S_0 = T_1$, $S_1 = T_1 \cup T_p$, ..., $S_{d-1} = T_1 \cup T_p \cup \cdots \cup T_{p^{d-1}}$. These are p-closed sets, which form the tower of supports of our code $\mathcal{C}$, whose Fourier transform has minimal support $S = S_{d-1}$.

We claim that $1_A \notin S$. For if this were not the case, then we would have $1_A \in T_{p^k}$ for some $k \in \{0, 1, \ldots, d-1\}$. That is, we could write $1_A = \gamma^j$ for some $j \in \mathbb{N}$ with $w_p(j) = p^k$. Thus we would have some $j \in \mathbb{N}$ with $w_p(j) = p^k$ and $j \equiv 0 \pmod{(p^n - 1)/(p - 1)}$. So we would have a sequence of p^k elements, each a power of p, whose sum vanishes modulo $(p^n-1)/(p-1)$. We can reduce each element of the sequence modulo p^n-1 to get a sequence of p^k elements, with each element in $\{1, p, \ldots, p^{n-1}\}$, where the sum of the sequence vanishes modulo $(p^n - 1)/(p - 1)$. If any element $p^i \in \{1, p, \ldots, p^{n-1}\}$ occurs more than p times in the sequence, replace p occurrences of it with a single occurrence of either p^{i+1} (if $i < n-1$) or with a single occurrence of 1 (if $i = n - 1$). If we continue to do this until no element of $\{1, p, \ldots, p^{n-1}\}$ occurs more than p times, then we obtain a nonempty sequence of at most p^k elements, with each element in $\{1, p, \ldots, p^{n-1}\}$, where the sum of the sequence vanishes modulo $(p^n - 1)/(p - 1)$ and where no term is repeated more than $p - 1$ times. Thus, the sum of this last sequence is at most $(p-1)(1 + p + \cdots + p^{n-1}) = p^n - 1$. So the sum of the last sequence is $j(p^n - 1)/(p - 1)$ for some positive $j \leq p - 1$. Since p-ary representations are unique, we know that our last sequence has precisely j instances of each element of $\{1, p, \ldots, p^{n-1}\}$. So our last sequence has at least n terms. Thus $p^{2(d-1)+m} = n \leq p^k \leq p^{d-1}$, which is a contradiction since $m > 0$. So indeed 1_A is not in the minimal support of the Fourier transform of our code.

Now we want to calculate $\omega^{ss}_{mc}(\mathcal{C}), \omega^{ss}(\mathcal{C}), \omega_{mc}(\mathcal{C})$, and $\omega(\mathcal{C})$ for our code. We shall often convert statements about multisets into statements about sequences, and vice versa, in our calculations. We say that a sequence of elements in A is *unity-product* to mean that the product of the elements in the sequence is 1_A. Before begin our calculations, we make an observation that will simplify the computation.

Observation: We claim that if we want to calculate $\omega^{ss}(\mathcal{C})$ (resp., $\omega^{ss}_{mc}(\mathcal{C})$), then it suffices

to compute the minimum score among those λ in $\Lambda^{ss}(\mathcal{C})$ (resp., $\Lambda^{ss}_{mc}(\mathcal{C})$) with $\lambda_i = \emptyset$ for $i > 0$. For if $\lambda_{i,a} > 0$ for some $i > 0$ and $a \in S_i$, then note that $a \in T_{p^j}$ for some $j \leq i$. By the definition of T_{p^j}, the element a can be written as a product of a sequence of p^j elements in T_1, say $a_1, \ldots, a_{p^j}$. Then consider the account $\kappa = \lambda - (i, a) + \sum_{k=1}^{p^j}(0, a_k)$. This account has the same product as λ, so it is unity-product, and it is clearly not all-unity since $1_A \notin T_1$. Furthermore $S_0 = T_1$, so $\lambda_0 \in \mathbb{N}[S_0]$, and of course $\lambda_i \in \mathbb{N}[S_i]$ for $i > 0$. If λ is in $\Lambda^{ss}_{mc}(\mathcal{C})$, then note that $|\kappa| = |\lambda| + p^j - 1$, so $|\kappa| \equiv |\lambda| \equiv 0 \pmod{p-1}$. All of this shows that if λ is in $\Lambda^{ss}(\mathcal{C})$ (resp., $\Lambda^{ss}_{mc}(\mathcal{C})$), then κ is also in $\Lambda^{ss}(\mathcal{C})$ (resp., $\Lambda^{ss}_{mc}(\mathcal{C})$). Furthermore $\mathrm{Sc}\,(\kappa) = \mathrm{Sc}\,(\lambda) + p^j - p^i \leq \mathrm{Sc}\,(\lambda)$. We can keep repeating this procedure until we obtain an account $\nu \in \Lambda^{ss}(\mathcal{C})$ (resp., $\Lambda^{ss}_{mc}(\mathcal{C})$) with $\nu_1 = \cdots = \nu_{d-1} = \emptyset$ and $\mathrm{Sc}\,(\nu) \leq \mathrm{Sc}\,(\lambda)$. So there exists an account λ in $\Lambda^{ss}(\mathcal{C})$ (resp., $\Lambda^{ss}_{mc}(\mathcal{C})$) of minimal score such that $\lambda_1 = \cdots = \lambda_{d-1} = \emptyset$. This observation shows that

$$\omega^{ss}(\mathcal{C}) = \min\{|\lambda| : \lambda \in \mathbb{N}[S_0], \Pi\lambda = 1_A\} \tag{4.38}$$

and

$$\omega^{ss}_{mc}(\mathcal{C}) = \min\{|\lambda| : \lambda \in \mathbb{N}[S_0], \Pi\lambda = 1_A, |\lambda| \equiv 0 \pmod{p-1}\}. \tag{4.39}$$

These facts will be used in the next two paragraphs to calculate $\omega^{ss}(\mathcal{C})$ and $\omega^{ss}_{mc}(\mathcal{C})$.

By the observation (4.39), we see that computing $\omega^{ss}_{mc}(\mathcal{C})$ is tantamount to finding the minimum of the lengths of the (nonempty) unity-product sequences consisting of elements in $S_0 = T_1$ and having lengths divisible by $p-1$. (We also must be sure that not all terms in a given sequence are equal to 1_A, but since $1_A \notin S_0$, this is automatic.) Since the elements in our sequence are from $T_1 = \{\gamma, \gamma^p, \ldots, \gamma^{p^{n-1}}\}$, our task is tantamount to finding the minimum length of a nonempty sequence of integers in $E = \{1, p, \ldots, p^{n-1}\}$ with the sum of the sequence congruent to 0 modulo $(p^n - 1)/(p-1)$ and with the length of the sequence divisible by $p-1$. Suppose we have such a minimum-length sequence. Note that no element of E occurs more than $p-1$ times, for if p^j occurred p or more times, we could replace p instances of p^j with a single instance of p^{j+1} (if $j < n-1$) or a single instance of 1 (if $j = n-1$) to obtain another sequence, shorter by $p-1$ elements, whose sum is also divisible

by $(p^n-1)/(p-1)$. So we already know that the length of our sequence is less than or equal to $n(p-1)$, and the sum of its terms is at most p^n-1, with equality occurring if and only if we have exactly $p-1$ instances of each element in E. Furthermore, since each element in the sequence is congruent to 1 modulo $p-1$, the sum of the sequence will also be congruent to zero modulo $p-1$. Now note that $(p^n-1)/(p-1) \equiv n \equiv 1 \pmod{p-1}$, and so $\gcd(p-1,(p^n-1)/(p-1))=1$. So the sum of the elements in our sequence will be congruent to zero modulo p^n-1. Since we know that the sum of our elements is strictly positive and at most p^n-1, this means the sum of our elements is exactly p^n-1, so our sequence has $p-1$ instances of each element of E. Thus $\omega_{mc}^{ss}(\mathcal{C}) = n(p-1) = (p-1)p^{2(d-1)+m}$.

The computation of $\omega^{ss}(\mathcal{C})$ is similar to that of $\omega_{mc}^{ss}(\mathcal{C})$. By the observation (4.38), we see that computing $\omega^{ss}(\mathcal{C})$ is tantamount to finding the minimum of the lengths of the (nonempty) unity-product sequences consisting of elements in $S_0 = T_1$. This, in turn, is tantamount to finding the minimum length of a nonempty sequence of integers in $E = \{1, p, \ldots, p^{n-1}\}$ with the sum of the sequence congruent to 0 modulo $(p^n-1)/(p-1)$. Suppose we have such a minimum-length sequence. Note that no element of E occurs more than $p-1$ times, by the same argument used in the previous paragraph, where we were computing $\omega_{mc}^{ss}(\mathcal{C})$. So we already know that the length of our sequence is less than or equal to $n(p-1)$, and the sum of its terms is at most p^n-1. The sum of our sequence is strictly positive, so it is $k(p^n-1)/(p-1)$ for some $k \in \{1,2,\ldots,p-1\}$. Note that $w_p(k(p^n-1)/(p-1)) = kn \geq n$ for all $k \in \{1,2,\ldots,p-1\}$, and $w_p(a) = 1$ for all $a \in E$. Further, note that $w_p(a+b) \leq w_p(a) + w_p(b)$ for any $a, b \in \mathbb{N}$; this is a well-known fact (proved in [18] as Lemma 3.7). So we cannot have fewer than n terms in our sequence; otherwise the p-ary weight of the sum would be less than n, contradicting what we just showed. On the other hand, we can have precisely n elements in our sequence: $1 + p + \cdots + p^{n-1} = (p^n-1)/(p-1)$. So $\omega^{ss}(\mathcal{C}) = n = p^{2(d-1)+m}$.

Now we compute $\omega_{mc}(\mathcal{C})$. This is tantamount to finding the minimum length of a (nonempty) unity-product sequence of length divisible by $p-1$ consisting of elements of $S = S_{d-1} = T_1 \cup T_p \cup \cdots \cup T_{p^{d-1}}$. Suppose we have such a minimum-length sequence, and it has $s(p-1)$ elements. For any given term a in the sequence, there is some $j \in \{0,1,\ldots,d-1\}$

such that $a \in T_{p^j}$, so we can write a as a product of a selection of p^j terms in $T_1 = S_0$. Suppose we replace each a in our minimal sequence with such a selection whose product is a. We get a new sequence consisting of elements in S_0, the length of this new sequence is divisible by $p-1$, and the product of the elements in this sequence is 1_A. Since each replacement removes one element and adds at most p^{d-1} in its place, the length of this new sequence is at most $s(p-1)p^{d-1}$. If we set λ_0 equal to the multiset of the terms in this sequence and let $\lambda_i = \emptyset$ for $i \in \{1, 2, \ldots, d-1\}$, then we have an element λ of $\Lambda^{ss}_{mc}(\mathcal{C})$ with $\mathrm{Sc}\,(\lambda) = s(p-1)p^{d-1}$, so that $s(p-1)p^{d-1} \geq \omega^{ss}_{mc}(\mathcal{C})$. But $\omega^{ss}_{mc}(\mathcal{C}) = n(p-1)$, so $sp^{d-1} \geq n$, and thus $s \geq p^{d-1+m}$. So our sequence has at least $(p-1)p^{d-1+m}$ elements. We claim that it has precisely this many elements; we shall construct a unity-product sequence of elements of $T_{p^{d-1}} \subseteq S_{d-1} = S$ with this many elements. Actually, we do something equivalent: we shall construct a sequence of $(p-1)p^{d-1+m}$ integers whose p-ary weights are all p^{d-1} and whose sum is congruent to 0 modulo $(p^n-1)/(p-1)$. In fact, the sum of our integers will be $p^n - 1$, which is an integer of p-ary weight $n(p-1) = p^{d-1}(p-1)p^{d-1+m}$. As such, $p^n - 1$ can be written as the sum of $(p-1)p^{d-1+m}$ integers of p-ary weight p^{d-1}. (Write $p^n - 1$ as a sum of $p^{d-1}(p-1)p^{d-1-m}$ powers of p, using its p-ary expansion. Group these in groups of p^{d-1}. The p-ary weight of the sum of each group is precisely p^{d-1} since there are no "carries" when we add, for there are only $p-1$ occurrences of any p^j with $0 \leq j < n$.) Thus, we have shown that $\omega_{mc}(\mathcal{C}) = (p-1)p^{d-1+m}$.

Finally, we compute $\omega(\mathcal{C})$. This is tantamount to finding the minimum length of a (nonempty) unity-product sequence consisting of elements of $S = S_{d-1} = T_1 \cup T_p \cup \cdots \cup T_{p^{d-1}}$. Suppose we have such a minimum-length sequence, and it has s elements. We proceed by the same argument in the previous paragraph to obtain a new unity-product sequence of length at most sp^{d-1} consisting of elements in S_0. If we set λ_0 equal to the multiset of the terms in this sequence and let $\lambda_i = \emptyset$ for $i \in \{1, 2, \ldots, d-1\}$, then we have an element λ of $\Lambda^{ss}(\mathcal{C})$ with $\mathrm{Sc}\,(\lambda) = sp^{d-1}$, so that $sp^{d-1} \geq \omega^{ss}(\mathcal{C})$. But $\omega^{ss}(\mathcal{C}) = n$, so $sp^{d-1} \geq n$, and thus $s \geq p^{d-1+m}$. We claim that $s = p^{d-1-m}$ precisely; we shall construct a unity-product sequence of elements of $T_{p^{d-1}} \subseteq S_{d-1} = S$ with this many elements. Actually, we do something equivalent: we shall construct a sequence of p^{d-1+m} integers whose p-ary weights

are all p^{d-1} and whose sum is congruent to 0 modulo $(p^n-1)/(p-1)$. In fact, the sum of our integers will be $(p^n-1)/(p-1)$, which is an integer of p-ary weight $n = p^{d-1}p^{d-1+m}$. As such, $(p^n-1)/(p-1)$ can be written as the sum of p^{d-1+m} integers of p-ary weight p^{d-1}. (See the argument used at the end of the previous paragraph.) Thus, we have shown that $\omega(\mathcal{C}) = p^{d-1+m}$.

To summarize: In our first construction, we have shown $\omega(\mathcal{C}) = p^{d-1+m}$, $\omega_{mc}(\mathcal{C}) = (p-1)p^{d-1+m}$, $\omega^{ss}(\mathcal{C}) = p^{2(d-1)+m}$, and $\omega^{ss}_{mc}(\mathcal{C}) = (p-1)p^{2(d-1)+m}$. Thus $\ell(\mathcal{C}) = (p^m-1)/(p-1)$, $\ell_{mc}(\mathcal{C}) = p^m-1$, $\ell^{ss}(\mathcal{C}) = (p^{d-1+m}-1)/(p-1)$, and $\ell^{ss}_{mc}(\mathcal{C}) = p^{d-1+m}-1$. Recall that m is an arbitrary positive integer. If $p > 2$ and $d > 1$, we have $\ell(\mathcal{C}) < \ell_{mc}(\mathcal{C}) < \ell^{ss}(\mathcal{C}) < \ell^{ss}_{mc}(\mathcal{C})$. In fact, as m tends to infinity, the difference between any two terms in our chain of inequalities tends to infinity. If $p = 2$ and $d > 1$, then $\ell(\mathcal{C}) < \ell^{ss}(\mathcal{C})$, and note that $\omega(\mathcal{C}) = 2^{d-1+m}$ and $\omega^{ss}(\mathcal{C}) = 2^{2(d-1)+m}$ are even in these cases. Furthermore, as m tends to infinity, the differences $\ell^{ss}(\mathcal{C}) - \ell(\mathcal{C})$ and $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ tend to infinity.

Now we make a second construction, a family of codes that are free $\mathbb{Z}/p^d\mathbb{Z}$-modules such that $\ell(\mathcal{C}) < \ell_{mc}(\mathcal{C})$ (or equivalently, $\ell^{ss}(\mathcal{C}) < \ell^{ss}_{mc}(\mathcal{C})$) if $p > 2$. We let p and d be arbitrary until further notice.

The second construction: We again set $m > 0$, let $n = p^{2(d-1)+m}$, and let A be the cyclic group of order $(p^n-1)/(p-1)$ generated by γ. As before, for each k, we set $T_k = \{\gamma^j : j \in \mathbb{N}, w_p(j) = k\}$, a p-closed set. This time, however, we set $S_0 = \cdots = S_{d-1} = T_1$. This is the tower of supports of our code $\mathcal{C}$, which is a free $\mathbb{Z}/p^d\mathbb{Z}$-module by Lemma 2.13, and whose Fourier transform has minimal support $S = S_{d-1} = T_1$. As in the first construction, we note that 1_A is not in the minimal support S of the Fourier transform of our code.

First we compute $\omega_{mc}(\mathcal{C})$. This is tantamount to finding the minimum length of a (nonempty) unity-product sequence of length divisible by $p-1$ whose terms are elements in $S = T_1$. We have already done this in the computation of $\omega^{ss}_{mc}(\mathcal{C})$ in the previous construction. The minimum length of such a sequence is $n(p-1)$. So $\omega_{mc}(\mathcal{C}) = n(p-1) = (p-1)p^{2(d-1)+m}$.

Next we compute $\omega(\mathcal{C})$. This is tantamount to finding the minimum length of a (nonempty) unity-product sequence whose terms are elements in $S = T_1$. We have al-

ready done this in the computation of $\omega^{ss}(\mathcal{C})$ in the previous construction. The minimum length of such a sequence is n. So $\omega_{mc}(\mathcal{C}) = n = p^{2(d-1)+m}$.

To summarize: In our second construction, we have shown $\omega(\mathcal{C}) = p^{2(d-1)+m}$ and $\omega_{mc}(\mathcal{C}) = (p-1)p^{2(d-1)+m}$. Thus $\ell(\mathcal{C}) = (p^{d-1+m}-1)/(p-1)$ and $\ell_{mc}(\mathcal{C}) = p^{d-1+m}-1$. If $p > 2$, we have $\ell(\mathcal{C}) < \ell_{mc}(\mathcal{C})$ for any m. As m tends to infinity, the difference between $\ell(\mathcal{C})$ and $\ell_{mc}(\mathcal{C})$ tends to infinity.

Note that in both the first and second constructions, the group A was always a cyclic group, and 1_A was never in the minimal support of the Fourier transform of the code. When $p = 2$, we were working with A the cyclic group of order $2^n - 1$. Finally, note that if we set $p = 2$ in the second construction, then our codes are free $\mathbb{Z}/2^d\mathbb{Z}$-modules and have $\omega(\mathcal{C})$ even. $\square$

Chapter 5

Lee Weights in $\mathbb{Z}/p^d\mathbb{Z}[A]$

We now discuss analogues of McEliece's theorem for the Lee weight function $\mathrm{lee}\colon \mathbb{Z}/p^d\mathbb{Z} \to \mathbb{Z}$. See Section 2.4 for the definition of Lee weight. We set $e = 1$ throughout the chapter, so that we are working with codes in the algebra $\mathbb{Z}/p^d\mathbb{Z}[A]$. We always suppose that we have a code $\mathcal{C} \subseteq \mathbb{Z}/p^d\mathbb{Z}[A]$ and that $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{d-1}$ is the tower of supports of the Fourier transform of $\mathcal{C}$. We set $S = S_{d-1}$, which is the support of the Fourier transform of our code $\mathcal{C}$. We suppose that not all the S_i are subsets of $\{1_A\}$, i.e., that at least one of the S_i contains an element of A that is not the identity. Otherwise we have a trivial situation: $\mathcal{C}$ consists only of constant words and then $\mathrm{wt}(c) = |A|\,\mathrm{wt}(\tilde{c}(1_A))$ for all $c \in \mathcal{C}$, i.e., $\mathrm{wt}^{\mathrm{norm}}(c) = 0$ for all $c \in \mathcal{C}$.

We shall continue to use the set $\Lambda^{ss}(\mathcal{C})$ and the associated parameters $\omega^{ss}(\mathcal{C})$ and $\ell^{ss}(\mathcal{C})$ as defined in (4.27), (4.28), and (4.29). Our analogue of McEliece's theorem for generic weight functions (Theorem 4.21) can be specialized immediately for the Lee weight to give the following:

Theorem 5.1 (Theorem 4.21, specialized). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. With $\ell^{ss}(\mathcal{C})$ as defined in* (4.29)*, we have* $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell^{ss}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$.*

For odd p, this is superior to a previous result of the author, given below as Theorem 5.2. The previous result uses the parameter $\ell(\mathcal{C})$ defined in (4.35). We should keep this parameter in mind for the rest of this chapter, along with the set $\Lambda(\mathcal{C})$ and the parameter $\omega(\mathcal{C})$, as defined in (4.33) and (4.34). The result on Lee weights for p an odd prime was published by the author as a portion of the research program described in this thesis.

Theorem 5.2 (D. J. Katz [29]). *Let p be odd. Let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. With $\ell(\mathcal{C})$ as defined in* (4.35)*, we have* $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell(\mathcal{C})}}$ *for all* $c \in \mathcal{C}$.

Theorem 5.1 is superior to Theorem 5.2 since $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$ by Proposition 4.22. Indeed, that proposition shows that strict inequality holds for infinitely many codes. The author is not aware of any other analogues McEliece's theorem for Lee weights in $\mathbb{Z}/p^d\mathbb{Z}[A]$ with odd p.

For $p = 2$, more work has been done. Wilson proved the following result for codes in $Z/2^d\mathbb{Z}[A]$:

Theorem 5.3 (Wilson [67]). *Let $p = 2$. Let $\mathcal{C}$ be a code in $\mathbb{Z}/2^d\mathbb{Z}[A]$ with A cyclic and 1_A not in the support of the Fourier transform of $\mathcal{C}$. With $\ell(\mathcal{C})$ as defined in* (4.35)*, we have* $\mathrm{lee}(c) \equiv 0 \pmod{2^{\left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1}}$ *for all* $c \in \mathcal{C}$.

It is not difficult to remove Wilson's assumptions that A is cyclic and $1_A \notin S$. This generalization was presented by the author:

Theorem 5.4 (D. J. Katz [29]). *Let $p = 2$. Let $\mathcal{C}$ be a code in $\mathbb{Z}/2^d\mathbb{Z}[A]$. With $\ell(\mathcal{C})$ as defined in* (4.35)*, we have* $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{2^{\left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1}}$ *for all* $c \in \mathcal{C}$.

To compare this theorem with Theorem 5.1, we must compare $\ell^{ss}(\mathcal{C}) = \left\lfloor \frac{\omega^{ss}(\mathcal{C})}{2^{d-1}} \right\rfloor - 1$ with $\left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1$. By Proposition 4.22, we can make a family of codes where $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ is unbounded as $\mathcal{C}$ ranges over the family. Thus, there are infinitely many codes where $\ell^{ss}(\mathcal{C}) \geq \left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1$, and thus where Theorem 5.1 is stronger than Theorem 5.4. On the other hand, if we consider codes that are free $\mathbb{Z}/2^d\mathbb{Z}$-modules, then for these codes we have $\omega^{ss}(\mathcal{C}) = \omega(\mathcal{C})$ and $\ell^{ss}(\mathcal{C}) = \ell(\mathcal{C})$ by Proposition 4.22. In this case, we see that Theorem 5.1 states that the normalized Lee weight has 2-adic valuation at least $\ell^{ss}(\mathcal{C}) = \ell(\mathcal{C}) = \max\left\{0, \left\lfloor \frac{\omega(\mathcal{C})}{2^{d-1}} \right\rfloor - 1\right\} \leq \left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1$. So in this case, Theorem 5.1 is weaker than Theorem 5.4. Note that $\left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1$ is always strictly positive (since $\omega(\mathcal{C})$ cannot be 1 or 0, because any element of $\Lambda(\mathcal{C})$ is a unity-product but not all-unity multiset, and hence has at least two elements). Indeed, if we assume $d \geq 2$ (in the $d = 1$ case, Lee weight coincides with Hamming weight on $\mathbb{F}_2$, and we already have a sharp bound for p-adic valuations of Hamming weights), then we have $\left\lfloor \frac{\omega(\mathcal{C})-2}{2^{d-1}} \right\rfloor + 1 \geq \max\left\{ \left\lfloor \frac{\omega(\mathcal{C})}{2^{d-1}} \right\rfloor, 1 \right\} = \ell(\mathcal{C}) + 1$, so in fact

Theorem 5.4 is stronger than Theorem 5.1 in all cases when $d \geq 2$ and $\mathcal{C}$ is a free $\mathbb{Z}/2^d\mathbb{Z}$-module. Since the two theorems (5.1 and 5.4) are not strictly comparable, one should use whichever gives a stronger 2-divisibility criterion.

There are other results in the literature that treat of the special case of Lee weights in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. The first result, due to Helleseth, Kumar, Moreno, and Shanbhag, is not phrased as a theorem for Abelian codes, but rather for $\mathbb{Z}/4\mathbb{Z}$-linear trace codes. To connect it with our results, we define the *$\mathbb{Z}/4\mathbb{Z}$-linear trace code of length 2^n with tower of supports $S_0 \subseteq S_1$* as follows: Let $n > 1$, let A be the cyclic group of order $2^n - 1$, let $S_0 \subseteq S_1$ be 2-closed subsets of A, and let $\mathcal{C}$ be the cyclic code of length $2^n - 1$ with tower of supports $S_0 \subseteq S_1$. Then the $\mathbb{Z}/4\mathbb{Z}$-linear trace code of length 2^n with tower of supports $S_0 \subseteq S_1$ is obtained from $\mathcal{C}$ by appending to the end of each word $c \in \mathcal{C}$ the symbol $\tilde{c}(1_A)$. We write each of these extended words as $(c|\tilde{c}(1_A))$. When we discuss $\mathbb{Z}/4\mathbb{Z}$-linear trace codes, we always let $\mathcal{C}$ be the underlying cyclic code, and we write $\mathcal{C}^{\text{ext}}$ for the $\mathbb{Z}/4\mathbb{Z}$-linear trace code. If $c \in \mathcal{C}^{\text{ext}}$, the Lee weight of a codeword is simply the sum of the Lee weights of the letters in the word, i.e., $\text{lee}(c|\tilde{c}(1_A)) = \text{lee}(c) + \text{lee}(\tilde{c}(1_A))$, and so we have $\text{lee}(c|\tilde{c}(1_A)) \equiv \text{lee}(c) - |A|\,\text{lee}(\tilde{c}(1_A)) \pmod{2^n}$ since $|A| = 2^n - 1$, i.e.,

$$\text{lee}(c|\tilde{c}(1_A)) \equiv \text{lee}^{\text{norm}}(c) \pmod{2^n}. \tag{5.1}$$

That is, the Lee weight of a word in $\mathcal{C}^{\text{ext}}$ is congruent modulo 2^n to the normalized Lee weight of the corresponding word in $\mathcal{C}$. Now we can present the theorem of Helleseth, Kumar, Moreno, and Shanbhag.

Theorem 5.5 (Helleseth-Kumar-Moreno-Shanbhag [25]). *Suppose that $\mathcal{C}^{\text{ext}}$ is the $\mathbb{Z}/4\mathbb{Z}$-linear trace code of length 2^n with tower of supports $S_0 \subseteq S_1$. Then $\text{lee}(c) \equiv 0 \pmod{2^{\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1}}$ for all $c \in \mathcal{C}^{\text{ext}}$.*

In view of (5.1), we have the following equivalent statement:

Theorem 5.6 (equivalent to Theorem 5.5). *Let $n > 1$ and suppose that $\mathcal{C} \subseteq \mathbb{Z}/4\mathbb{Z}[A]$ with A the cyclic group of order $2^n - 1$. Then $\text{lee}^{\text{norm}}(c) \equiv 0 \pmod{2^{\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1}}$ for all $c \in \mathcal{C}$.*

Proof. The equivalence of this theorem and the previous one will follow immediately from (5.1) if we can show that $n \geq \lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1$. But recall that the minimal support $S = S_1$ of the Fourier transform of our code $\mathcal{C}$ is always assumed to contain some a with $a \neq 1_A$. Of course S_1 contains $a, a^2, \ldots, a^{2^{n-1}}$, because sets in the tower of supports are 2-closed. Note that $a^{2^n-1} = 1_A$, and let $\lambda \in \mathbb{N}[I \times A]$ be the multiset with $\lambda_0 = \emptyset$ and λ_1 the multiset with one instance of each of $a, a^2, \ldots, a^{2^{n-1}}$. Then λ is an element of $\Lambda(\mathcal{C})$ with score $2n$, proving that $\omega^{ss}(\mathcal{C}) \leq 2n$. Thus $\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1 < n$. □

Note that this theorem is superior to Theorem 5.1 if we specialize Theorem 5.1 to cyclic codes of length $2^n - 1$ over $\mathbb{Z}/4\mathbb{Z}$. For in this case, Theorem 5.1 asserts that the normalized Lee weight has 2-adic valuation at least $\ell^{ss}(\mathcal{C}) = \lfloor \omega^{ss}(\mathcal{C})/2 \rfloor - 1$. Theorem 5.6 is not strictly comparable to the specialization of Theorem 5.4 to cyclic codes of length $2^n - 1$ over $\mathbb{Z}/4\mathbb{Z}$, which asserts that the normalized Lee weight is divisible by $\lfloor \omega(\mathcal{C})/2 \rfloor$. Proposition 4.22 tells us that we can find an infinite family of such codes in which $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ is unbounded as $\mathcal{C}$ runs over the family. Thus the specialization of Theorem 5.4 to cyclic codes of length $2^n - 1$ is weaker than Theorem 5.6 for infinitely many codes. On the other hand, if we restrict our attention to codes that are free $\mathbb{Z}/4\mathbb{Z}$-modules, then $\omega^{ss}(\mathcal{C}) = \omega(\mathcal{C})$ and $\ell^{ss}(\mathcal{C}) = \ell(\mathcal{C})$ by Proposition 4.22, and then Theorem 5.4 (specialized to cyclic codes of length $2^n - 1$ that are free $\mathbb{Z}/4\mathbb{Z}$-modules) is stronger than Theorem 5.6. For Theorem 5.4 asserts that the normalized Lee weight has 2-adic valuation at least $\lfloor \omega(\mathcal{C})/2 \rfloor$, while Theorem 5.6 asserts that the 2-adic valuation is at least $\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1 = \lceil \omega(\mathcal{C})/2 \rceil - 1$. These bounds are equal if $\omega(\mathcal{C})$ is odd, but the former is greater than the latter by 1 if $\omega(\mathcal{C})$ is even. Proposition 4.22 shows that there are infinitely many cyclic codes $\mathcal{C}$, each of length $2^n - 1$ for some integer n (but not the same n for all the codes), that are free $\mathbb{Z}/4\mathbb{Z}$-modules with $\omega(\mathcal{C})$ even.

One should note that Wilson's result (Theorem 5.3) was an improvement of a result of Calderbank, Li, and Poonen. Like Wilson, these authors assume that A is a cyclic group and that $1_A \notin S$.

Theorem 5.7 (Calderbank-Li-Poonen [7]). *Suppose that $\mathcal{C} \subseteq \mathbb{Z}/4\mathbb{Z}[A]$ with A cyclic and 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then* $\mathrm{lee}(c) \equiv 0 \pmod{2^{\lceil \omega(\mathcal{C})/2 \rceil - 1}}$ *for all $c \in \mathcal{C}$.*

Note that it is not as strong as the specialization of Theorem 5.3 to codes over $\mathbb{Z}/4\mathbb{Z}$, which asserts that the Lee weights have 2-adic valuation at least $\lfloor \omega(\mathcal{C})/2 \rfloor$. So Theorem 5.3 gives strictly more information when $\omega(\mathcal{C})$ is even, as it is for infinitely many codes (see Proposition 4.22). Note that Theorem 5.6 is narrower in scope than Theorem 5.7, since the former only considers the case when A is cyclic of order $2^n - 1$ for some $n > 1$. However, in this special case, Theorem 5.6 is stronger, since $\omega^{ss}(\mathcal{C}) \geq \omega(\mathcal{C})$ by Proposition 4.22.

The goal of this chapter is to make a single sharp lower bound for 2-adic valuations of Lee weights in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. To this end, we shall prove Theorem 5.12, a slightly specialized form of which was presented in the Introduction as Theorem 1.9. Here we present a simplified version that contains the essence of what we shall prove later.

Theorem 5.8 (Theorem 5.12, simplified). *Let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$. Then we have* $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+1}}$ *for all $c \in \mathcal{C}$, and* $\mathrm{lee}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$ *for some $c \in \mathcal{C}$.*

This theorem is stronger (for codes over $\mathbb{Z}/4\mathbb{Z}$) than all the results above. It is stronger than Theorem 5.1 (specialized to codes over $\mathbb{Z}/4\mathbb{Z}$), which asserts that the 2-adic valuations of normalized Lee weights are at least $\ell^{ss}(\mathcal{C})$. Theorem 5.8 is also stronger than Theorem 5.3 and its generalization, Theorem 5.4, when these are specialized to codes over $\mathbb{Z}/4\mathbb{Z}$. The latter theorems assert that the 2-adic valuations of normalized Lee weights are at least $\lfloor \omega(\mathcal{C})/2 \rfloor = \ell(\mathcal{C}) + 1$, and $\ell^{ss}(\mathcal{C}) \geq \ell(\mathcal{C})$ by Proposition 4.22. Indeed, the same proposition tells us that there is a family of cyclic codes (with 1_A not in the minimal supports of their Fourier transforms) such that $\ell^{ss}(\mathcal{C}) - \ell(\mathcal{C})$ is unbounded as $\mathcal{C}$ varies over the family. Theorem 5.8 is then stronger than Theorem 5.7 since Theorem 5.3 is stronger than Theorem 5.7. Finally, Theorem 5.8 (when specialized to cyclic codes with A of order $2^n - 1$) is stronger than Theorem 5.6. For Theorem 5.6 asserts that the 2-adic valuations of normalized Lee weights are at least $\lceil \omega^{ss}(\mathcal{C})/2 \rceil - 1$, while Theorem 5.8 asserts a lower bound of $\lfloor \omega^{ss}(\mathcal{C})/2 \rfloor$. The latter bound is no better when $\omega^{ss}(\mathcal{C})$ is odd, but is greater by one when $\omega^{ss}(\mathcal{C})$ is even. Indeed, by Proposition 4.22, we can make a family of codes where the underlying group of each code is cyclic with order $2^n - 1$ for some n (not the same n for each code), where 1_A is not in the minimal support of the Fourier transform of any code, where $\omega(\mathcal{C})$ and $\omega^{ss}(\mathcal{C})$ are

even for all the codes, and where $\omega^{ss}(\mathcal{C}) - \omega(\mathcal{C})$ is unbounded as $\mathcal{C}$ runs through the family. For this family, Theorem 5.8 will give a stronger lower bound on the 2-adic valuations of Lee weights of codewords than one would get by taking the maximum of all the bounds furnished by all the other theorems mentioned above.

The methods used in this chapter are similar to those of the previous chapter. Readers should familiarize themselves with the material in that chapter first. In Section 5.1, we specialize the definitions and conventions of Section 4.3 so that we can use them for Lee weights in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. In Section 5.2, we use techniques like those of Section 4.2 to produce counting polynomials that can be used to estimate Lee weights. We then use these polynomials in Section 5.3 to prove Theorem 5.12 (Theorem 5.8 above).

5.1 Sectioned Lee Weight

For the rest of this chapter, we set $p = 2$ and $d = 2$, so that our codes are ideals in $\mathbb{Z}/4\mathbb{Z}[A]$. Our goal is to prove Theorem 5.12. The method we shall use is quite similar to the method we used to prove Theorem 4.18 in Chapter 4. We shall devise a counting polynomial that will approximate the sectioning of the Lee weight (see Section 4.3 for the notion of a sectioning of a weight function, which we review below). We shall then use our polynomial in conjunction with Corollary 3.4 to give 2-adic estimates of Lee weights in our codes.

We review the notions of Section 4.3, specializing them for $p = 2$ and $d = 2$ here. We use the convention that for any letter a, the corresponding boldface letter $\mathbf{a}$ stands for the ordered pair (a_0, a_1). We set $I = \{0, 1\}$ and consider accounts in $\mathbb{Z}[I]$ to be pairs of integers, i.e., we identify $\mu \in \mathbb{Z}[I]$ with the pair $(\mu_0, \mu_1) \in \mathbb{Z}^2$. We use abbreviated notations that are the specialization to pairs of the compact notations for t-tuples in Section 4.1. So we use abbreviation that if $\mu \in \mathbb{Z}[I]$, then $\mathbf{x}^\mu = x_0^{\mu_0} x_1^{\mu_1}$ and

$$\binom{\mathbf{x}}{\mu} = \binom{x_0}{\mu_0}\binom{x_1}{\mu_1}.$$

Furthermore, we set $\Delta^\mu = \Delta_0^{\mu_0}\Delta_1^{\mu_1}$. We set $\mathbf{e}^0 = (1, 0)$ and $\mathbf{e}^1 = (0, 1)$. We also use $\mathbf{0}$ to

represent $(0,0)$.

We use the definitions of the score and the s-tier, as set down in Section 4.2. We specialize these notions here for $p = d = 2$. Thus, if $\mu \in \mathbb{Z}[I]$, then $\mathrm{Sc}\,(\mu) = \mu_0 + 2\mu_1$ and $\mathrm{Ti}_s(\mu) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(\mu)}{2^{s-1}} \right\rfloor - 1\right\}$. In fact, we shall be interested only in d-tiers here. Therefore, for the rest of the chapter, we define *tier* to mean d-tier and write Ti to mean Ti_d. This is the same convention adopted in Section 4.3 of Chapter 4 and used to the end of that chapter. Here we have specialized to the case $d = 2$, so $\mathrm{Ti} = \mathrm{Ti}_d = \mathrm{Ti}_2$. Thus $\mathrm{Ti}(\mu) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(\mu)}{2} \right\rfloor - 1\right\} = \max\left\{0, \lfloor \frac{\mu_0}{2} \rfloor + \mu_1 - 1\right\}$. Note that $\mathrm{Ti}\,(\mu) = \lfloor \frac{\mu_0}{2} \rfloor + \mu_1 - 1$ unless $\mu = (0,0)$ or $(1,0)$. We also use notion of k-starting and k-critical from Section 4.2. When we specialize these for $p = d = 2$, we see that a multiset $\mu \in \mathbb{N}[I]$ is 0-critical if and only if μ_0 is odd and $\mathrm{Sc}\,(\mu) \geq 3$, and μ is 1-critical if and only if μ is 1-starting. We also transport the notion of score and tier to elements of $\mathbb{Z}[I \times A]$. The score of $\lambda \in \mathbb{Z}[I \times A]$, denoted $\mathrm{Sc}\,(\lambda)$, is just $\mathrm{Sc}\,(\mathrm{pr}_I\,\lambda)$, and the tier of λ, denoted $\mathrm{Ti}\,(\lambda)$, is just $\mathrm{Ti}\,(\mathrm{pr}_I\,\lambda)$. This means that $\mathrm{Sc}\,(\lambda) = |\lambda_0| + 2|\lambda_1|$ and $\mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\mathrm{Sc}(\lambda)}{2} \right\rfloor - 1\right\}$. Along with this, we transport to $\mathbb{Z}[I \times A]$ the notion of an account being k-starting or k-critical (for $k \in I$); to say that $\lambda \in \mathbb{Z}[I \times A]$ is k-starting (resp., k-critical) is to say that $\mathrm{pr}_I\,\lambda$ is k-starting (resp., k-critical). As in Section 4.2, we say that λ is critical to mean that it is k-critical for some k. Thus, λ is 0-starting if $\lambda_0 \neq \emptyset$, and λ is 1-starting if $\lambda_0 = \emptyset$ and $\lambda_1 \neq \emptyset$. Furthermore, λ is 0-critical if and only if $|\lambda_0|$ is odd and $\mathrm{Sc}\,(\lambda) \geq 3$, and λ is 1-critical if and only if $\lambda_0 = \emptyset$ and $\lambda_1 \neq \emptyset$, i.e., if and only if λ is 1-starting.

For the rest of this chapter, we suppose that we have a code $\mathcal{C} \subseteq \mathbb{Z}/4\mathbb{Z}[A]$ and $S_0 \subseteq S_1$ is the tower of supports of the Fourier transform of $\mathcal{C}$. As always, we let S be the support of the Fourier transform of $\mathcal{C}$, so $S = S_1$ here. We continue to assume that not all the S_i are subsets of $\{1_A\}$, i.e., that at least one of the S_i contains an element of A that is not the identity.

We now devise the sectioning of our Lee weight function $\mathrm{lee}\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}$, according to the definition given in Section 4.3. We review the definition here for our special case. The sectioning of lee is a 2-wise weight function denoted $\mathrm{lee}_{\mathrm{sec}}\colon (\mathbb{Z}/4\mathbb{Z})^2 \to \mathbb{Z}$, and defined by

$$\mathrm{lee}_{\mathrm{sec}}(r_0, r_1) = \mathrm{lee}(r_0 + 2r_1),$$

for all $r_0, r_1 \in \mathbb{Z}/4\mathbb{Z}$.

Recall the canonical expansion of the scaled Fourier transform and the scaled Fourier-induced breakdown of codewords, which we defined in Section 2.3 (before Proposition 2.8). For $c \in \mathcal{C}$ and $i \in I$, $c^{(i)}$ denotes the ith component of the scaled Fourier-induced breakdown of c, and $\tilde{c}^{(i)}$ denotes the ith component in the canonical expansion of $\tilde{c}$. Throughout this chapter, we often use the more convenient symbol c_i as a synonym for $c^{(i)}$. Thus $c = c^{(0)} + 2c^{(1)} = c_0 + 2c_1$ and $\tilde{c} = \tilde{c}^{(0)} + 2\tilde{c}^{(1)} = \tilde{c}_0 + 2\tilde{c}_1$. By (4.17) in Section 4.3, we have

$$\mathrm{lee}_{\mathrm{sec}}(c_0, c_1) = \mathrm{lee}(c),$$

and by (4.18) in the same section, we have

$$\mathrm{lee}_{\mathrm{sec}}^{\mathrm{norm}}(c_0, c_1) = \mathrm{lee}^{\mathrm{norm}}(c). \tag{5.2}$$

Now we consider the lift of $\mathrm{lee}_{\mathrm{sec}}$, that is, the function $F\colon {\mathbb{Z}_2}^2 \to \mathbb{Z}$ given by $F(\mathbf{r}) = \mathrm{lee}_{\mathrm{sec}}(\pi(r_0), \pi(r_1))$. By the last paragraph of Section 4.3, we see that $F(\mathbf{r} + 2\mathbf{e}^0) = F(\mathbf{r} + \mathbf{e}^1)$ and $F(\mathbf{r} + 2\mathbf{e}^1) = F(\mathbf{r})$. Thus F is $(2,2)$-periodic, using the definition of (p,t)-periodic from Section 4.2. This is the function that we shall approximate with a counting polynomial.

5.2 Construction of Counting Polynomials

We are ready to construct a counting polynomial to use with Corollary 3.4 in our estimation of Lee weights in $\mathbb{Z}/4\mathbb{Z}[A]$.

Theorem 5.9. *Let $F\colon {\mathbb{Z}_2}^2 \to \mathbb{Z}$ be given by*

$$F(\mathbf{r}) = \begin{cases} 0 & \text{if } r_0 + 2r_1 \equiv 0 \pmod 4, \\ 1 & \text{if } r_0 + 2r_1 \equiv 1, 3 \pmod 4, \\ 2 & \text{if } r_0 + 2r_1 \equiv 2 \pmod 4, \end{cases}$$

i.e., $F(\mathbf{r}) = \mathrm{lee}_{\mathrm{sec}}(\pi(r_0), \pi(r_1))$. Suppose that $\sum_{\mu \in \mathbb{N}[I]} F_\mu \binom{\mathbf{x}}{\mu}$ is the Newton expansion of F.

Then $F_{(0,0)} = 0$ *and if* $\mu = (\mu_0, \mu_1) \neq (0,0)$*, then* $F_\mu = (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} \gamma_{\mu_0}$*, where*

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

Thus $v_2(F_\mu) \geq \mathrm{Ti}\,(\mu) + 1$ *unless* $\mu = (1,0)$*.*

Proof. First we devise a well-ordering relation $\preceq$ on $\mathbb{N}^2$, and then we induct with respect to the ordering. If $\mu, \nu \in \mathbb{N}^2$ with $\mathrm{Sc}\,(\mu) < \mathrm{Sc}\,(\nu)$, then we declare $\mu \prec \nu$. Among the elements of $\mathbb{N}^2$ that have the same score, we order them lexicographically, i.e., $\kappa = (\kappa_0, \kappa_1) \prec \lambda = (\lambda_0, \lambda_1)$ means that $\kappa_0 < \lambda_0$ or that $\kappa_0 = \lambda_0$ and $\kappa_1 < \lambda_1$. There are only finitely many elements of $\mathbb{N}^2$ with a given score, so the lexicographic ordering well-orders the elements of like score. Thus $\prec$ is a well-ordering relation.

As the base of our induction, we use Proposition 4.5 to compute a few of the Newton coefficients. We compute $F_{(0,0)} = (\Delta^{(0,0)}F)(0,0) = 0$, $F_{(1,0)} = (\Delta^{(1,0)}F)(0,0) = F(1,0) - F(0,0) = 1$, $F_{(0,1)} = (\Delta^{(0,1)}F)(0,0) = F(0,1) - F(0,0) = 2$, and $F_{(1,1)} = (\Delta^{(1,1)}F)(0,0) = F(1,1) - F(1,0) - F(0,1) + F(0,0) = 1 - 1 - 2 + 0 = -2$. Note that these values for $F_{(i,j)}$ with $0 \leq i, j \leq 1$ are as we claim them to be in the statement of the theorem.

Now we proceed by induction to compute F_μ where $\mu_0 \geq 2$ or $\mu_1 \geq 2$. First we examine the case when $\mu_0 \geq 2$. Recall that F is $(2,2)$-periodic by the discussion at the end of Section 5.1. So we use Lemma 4.9 to see that $F_{\mu+(-2,1)} = F_\mu + 2F_{\mu-(1,0)}$, i.e., $F_\mu = F_{\mu+(-2,1)} - 2F_{\mu-(1,0)}$. Note that $\mu + (-2,1)$ has the same score as μ but is lexicographically lower, so $\mu + (-2,1) \prec \mu$. Also $\mu - (1,0)$ has a lower score than μ does, so $\mu - (1,0) \prec \mu$. Thus we may apply our induction hypothesis to $F_{\mu+(-2,1)}$ and $F_{\mu-(1,0)}$. Furthermore, note that neither $\mu + (-2,1)$ nor $\mu - (1,0)$ is $(0,0)$ (the latter is not $(0,0)$, since $\mu_0 \geq 2$). Thus we have $F_\mu = (-1)^{|\mu|} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} \gamma_{\mu_0-2} - 2(-1)^{|\mu|} 2^{\lfloor (\mu_0-1)/2 \rfloor + \mu_1} \gamma_{\mu_0-1}$ by induction. So

$$F_\mu = \begin{cases} (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} (\gamma_{\mu_0-1} - \gamma_{\mu_0-2}) & \text{if } \mu_0 \text{ is even}, \\ (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} (2\gamma_{\mu_0-1} - \gamma_{\mu_0-2}) & \text{if } \mu_0 \text{ is odd}. \end{cases}$$

Note that $\gamma_{j-1} - \gamma_{j-2} = \gamma_j$ if j is even. Note also that $2\gamma_{j-1} - \gamma_{j-2} = \gamma_j$ if j is odd. So $F_\mu = (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} \gamma_{\mu_0}$, which is what we need to show.

Now we examine the case when $\mu_1 \geq 2$. Here we use Lemma 4.10 to see that $F_\mu + 2F_{\mu-(0,1)} = 0$, i.e., $F_\mu = -2F_{\mu+(0,-1)}$. Note that $\mu + (0,-1)$ has a lower score than μ does, so $\mu + (0,-1) \prec \mu$. Thus we may apply our induction hypothesis to $F_{\mu+(0,-1)}$. Furthermore, note that $\mu + (0,-1)$ is not $(0,0)$, since $\mu_1 \geq 2$. Thus we have $F_\mu = -2(-1)^{|\mu|} 2^{\lfloor \mu_0/2 \rfloor + \mu_1 - 1} \gamma_{\mu_0}$ by induction. So $F_\mu = (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} \gamma_{\mu_0}$, which is what we need to show.

Finally, recall that for $\mu \in \mathbb{N}[I]$, $\mathrm{Ti}\,(\mu) = \lfloor \mu_0/2 \rfloor + \mu_1 - 1$ unless $\mu = (0,0)$ or $(1,0)$. Also recall that $F_{(0,0)} = 0$. Thus $v_2(F_\mu) \geq \mathrm{Ti}\,(\mu) + 1$ for $\mu \neq (1,0)$. □

Now we can truncate the Newton expansion in our theorem to obtain counting polynomials.

Theorem 5.10. *Let* $F\colon {\mathbb{Z}_2}^2 \to \mathbb{Z}$ *be given by*

$$F(\mathbf{r}) = \begin{cases} 0 & \text{if } r_0 + 2r_1 \equiv 0 \pmod 4, \\ 1 & \text{if } r_0 + 2r_1 \equiv 1, 3 \pmod 4, \\ 2 & \text{if } r_0 + 2r_1 \equiv 2 \pmod 4, \end{cases}$$

i.e., $F(\mathbf{r}) = \mathrm{lee}_{\mathrm{sec}}(\pi(r_0), \pi(r_1)) = \mathrm{lee}(\pi(r_0 + 2r_1))$. *Then the polynomial* $f^{(1)}(\mathbf{x}) = x_0$ *has the property that* $f^{(1)}(\mathbf{r}) \equiv F(\mathbf{r}) \pmod 2$ *for all* $\mathbf{r} \in {\mathbb{Z}_2}^2$.

For each $m \geq 2$, *there exists a polynomial*

$$f^{(m)}(\mathbf{x}) = \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m-1}} F_\mu^{(m)} \binom{\mathbf{x}}{\mu}, \tag{5.3}$$

with all $F_\mu^{(m)} \in \mathbb{Z}_2$, *such that* $f^{(m)}(\mathbf{r}) \equiv F(\mathbf{r}) \pmod{2^m}$ *for all* $\mathbf{r} \in {\mathbb{Z}_2}^2$. *Furthermore,* $F_{(0,0)}^{(m)} = 0$ *and if* $\mu \neq (0,0)$ *with* $\mathrm{Ti}\,(\mu) < m - 1$, *we have* $F_\mu^{(m)} = (-1)^{|\mu|+1} 2^{\lfloor \mu_0/2 \rfloor + \mu_1} \gamma_{\mu_0}$,

where

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

We can write $f^{(m)}(\mathbf{x}) = \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m-1}} f_\mu^{(m)} \mathbf{x}^\mu$, *with all* $f_\mu^{(m)} \in \mathbb{Q}_2$ *and* $f_{(0,0)} = 0$. *If* μ *is critical with* $\mathrm{Ti}\,(\mu) = m-2$, *then* $\mu! f_\mu = (-1)^{|\mu|+1} 2^{m-1} \gamma_{\mu_0}$ *and* $v_2\,(\mu! f_\mu) = m-1$.

Proof. It is almost immediate that $f^{(1)}(\mathbf{x}) = x_0$ approximates F modulo 2 on $\mathbb{Z}_2$. We prove the rest of the theorem. Let $m \geq 2$. Recall from the discussion at the end of Section 5.1 that F is $(2,2)$-periodic. A (p,t)-periodic function is p-adically continuous, as noted in Section 4.2. Therefore, the existence of the polynomial $f^{(m)}$ approximating F modulo 2^m is guaranteed by applying Theorem 5.9 and Lemma 4.6, with the set S in Lemma 4.6 equal to the set $\{\mu \in \mathbb{N}[I] : \mathrm{Ti}\,(\mu) < m-1\}$. (This set is finite because only finitely many μ have a certain tier.) Indeed, the coefficient F_μ of our polynomial f is precisely the Newton coefficient for the term $\binom{\mathbf{x}}{\mu}$ in the Newton expansion of F. Since Theorem 5.9 tells us that $v_2(F_\mu) \geq \mathrm{Ti}\,(\mu) + 1$ (unless $\mu = (1,0)$, which has tier 0), the set S includes all μ such that $v_2(F_\mu) < m$, so that Lemma 4.6 is truly applicable.

We can expand out the terms $\binom{\mathbf{x}}{\mu}$ in our expression (5.3) to obtain

$$f^{(m)}(\mathbf{x}) = \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m-1}} f_\mu^{(m)} \mathbf{x}^\mu.$$

Note that $\binom{\mathbf{x}}{\mu}$ has no constant term unless $\mu = (0,0)$, so $f_{(0,0)}^{(m)} = F_{(0,0)}^{(m)} = 0$.

Suppose that $\nu \in \mathbb{N}[I]$ is critical and of tier $m-2$. We want to compute the coefficient $f_\nu^{(m)}$ in terms of the coefficients $F_\mu^{(m)}$. The only terms $F_\mu^{(m)} \binom{\mathbf{x}}{\mu}$ in the expansion (5.3) which have the monomial $\mathbf{x}^\nu$ are those with $\mu_0 \geq \nu_0$ and $\mu_1 \geq \nu_1$, with $\mu_0 = 0$ if $\nu_0 = 0$, and with $\mu_1 = 0$ if $\nu_1 = 0$.

Thus, if ν is 0-critical, we need only consider terms $F_\mu^{(m)} \binom{\mathbf{x}}{\mu}$ in the expansion (5.3) with $\mu = \nu + (i,j)$ for some $i, j \geq 0$. But because ν is 0-critical, $\nu + (i,j)$ will have tier strictly higher than $\mathrm{Ti}\,(\nu) = m-2$ unless $(i,j) = (0,0)$. So the only term in the expansion (5.3)

we need to consider is $F_\nu^{(m)}\binom{\mathbf{x}}{\nu}$.

Likewise, if ν is 1-critical, we need only consider terms $F_\mu^{(m)}\binom{\mathbf{x}}{\mu}$ in the expansion (5.3) with $\mu = \nu + (0, j)$ for some $j \geq 0$. But because ν is 1-critical, $\nu + (0, j)$ will have tier strictly higher than $\mathrm{Ti}\,(\nu) = m - 2$ unless $j = 0$. So the only term in the expansion (5.3) we need to consider is $F_\nu^{(m)}\binom{\mathbf{x}}{\nu}$.

In both cases, the coefficient $f_\nu^{(m)}$ of $\mathbf{x}^\nu$ in $f^{(m)}(\mathbf{x})$ is $\frac{1}{\nu!}F_\nu^{(m)}$. Thus we have $\nu! f_\nu^{(m)} = (-1)^{|\nu|+1}2^{m-1}\gamma_{\nu_0}$ by what we already know about the coefficient $F_\nu^{(m)}$. Note that if ν is 0-critical, then ν_0 is odd, and if ν is 1-critical, then ν_0 is zero. But $v_2\,(\gamma_i) = 0$ if i is odd or zero, so if ν is critical, then $v_2\left(\nu! f_\nu^{(m)}\right) = m - 1$. □

5.3 Lee Weights in $\mathbb{Z}/4\mathbb{Z}[A]$

Now we are almost ready to state and prove our theorem on Lee weights in Abelian codes over $\mathbb{Z}/4\mathbb{Z}$. The reader should recall the definitions of $\Lambda^{ss}(\mathcal{C})$, $\omega^{ss}(\mathcal{C})$, and $\ell^{ss}(\mathcal{C})$ in (4.27), (4.28), and (4.29). We begin with a calculation that 2-adically approximates Lee weights.

Proposition 5.11. *Let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$. For each $c \in \mathcal{C}$ and $i \in I$, we let C_i be the element of $\mathbb{Z}_2[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$. Let $m \geq 2$ and let $f^{(m)}(\mathbf{x})$ be the polynomial described in Theorem 5.10. For any $c \in \mathcal{C}$, we have*

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < m-1}} \frac{(\mathrm{pr}_I\,\lambda)!\, f^{(m)}_{\mathrm{pr}_I\,\lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^m},$$

where $\Lambda^{ss}(\mathcal{C})$ is as defined in (4.27) above. We always have $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod 2$.

Proof. By Corollary 3.4, we have

$$\mathrm{lee}^{\mathrm{norm}}_{\mathrm{sec}}(c_0, c_1) \equiv |A| \sum_{\mu \in \mathbb{N}[I]} \mu! f_\mu^{(m)} \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I\,\lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A\,\lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_0 \in \mathbb{N}[S_0], \lambda_1 \in \mathbb{N}[S_1]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^m}.$$

By (5.2), the left-hand side becomes $\mathrm{lee}^{\mathrm{norm}}(c)$. We can restrict the sum over μ to those μ with $\mathrm{Ti}\,(\mu) < m - 1$, since $f_\mu^{(m)} = 0$ otherwise (by Theorem 5.10). The conditions on the

inner sum, other than the condition $\mathrm{pr}_I \lambda = \mu$, are tantamount to saying that $\lambda \in \Lambda^{ss}(\mathcal{C})$. Thus

$$\begin{aligned}\mathrm{lee}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m-1}} \mu! f_\mu^{(m)} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^m} \\ &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I] \\ \mathrm{Ti}(\mu) < m-1}} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^m},\end{aligned}$$

and the condition $\lambda = \mathrm{pr}_I \mu$ implies that λ and μ will always have the same score and tier, so we can shift the condition on tier to the sum over λ. Thus

$$\begin{aligned}\mathrm{lee}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\mu \in \mathbb{N}[I]} \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{pr}_I \lambda = \mu \\ \mathrm{Ti}(\lambda) < m-1}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^m} \\ &\equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < m-1}} \frac{(\mathrm{pr}_I \lambda)! f^{(m)}_{\mathrm{pr}_I \lambda}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^m},\end{aligned}$$

which is what we were to show.

Now we approximate normalized Lee weight modulo 2. Here we use the polynomial $f^{(1)}(\mathbf{x}) = x_0 = \mathbf{x}^{(1,0)}$ from Theorem 5.10. We apply Corollary 3.4 with this polynomial to obtain

$$\mathrm{lee}^{\mathrm{norm}}_{\mathrm{sec}}(c_0, c_1) \equiv |A| \sum_{\mu \in \mathbb{N}[I]} \mu! f^{(1)}_\mu \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I \lambda = \mu \\ \Pi\lambda = 1_A, \mathrm{pr}_A \lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_0 \in \mathbb{N}[S_0], \lambda_1 \in \mathbb{N}[S_1]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2}.$$

As before, (5.2) shows that the left-hand side is $\mathrm{lee}^{\mathrm{norm}}(c)$. Now $f_\mu = 0$ unless $\mu = (1,0)$, so that we have

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| f^{(1)}_{(1,0)} \sum_{\substack{\lambda \in \mathbb{N}[I \times A], \mathrm{pr}_I \lambda = (1,0) \\ \Pi\lambda = 1_A, \mathrm{pr}_A \lambda \notin \mathbb{N}[\{1_A\}] \\ \lambda_0 \in \mathbb{N}[S_0], \lambda_1 \in \mathbb{N}[S_1]}} \frac{1}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2}.$$

But now note that if $\mathrm{pr}_I \lambda = (1,0)$, then $|\lambda| = 1$, and then λ cannot simultaneously be

unity-product and not all-unity. So the sum on the right-hand side is empty, and we have $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod 2$. □

Now we can prove our sharp lower bound on the 2-adic valuations of normalized Lee weights of words of codes in $\mathbb{Z}/4\mathbb{Z}[A]$.

Theorem 5.12. *Let $\mathcal{C}$ be a code in $\mathbb{Z}/4\mathbb{Z}[A]$. With $\ell^{ss}(\mathcal{C})$ as defined in (4.29), we have $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+1}}$ for all $c \in \mathcal{C}$, and $\mathrm{lee}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$ for some $c \in \mathcal{C}$. More precisely, if $f^{(\ell^{ss}(\mathcal{C})+2)}(\mathbf{x})$ is the polynomial described in Theorem 5.10, and if we let C_i be the element of $\mathbb{Z}_2[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$ for each $i \in I$ and $c \in \mathcal{C}$, then*

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^{\ell^{ss}(\mathcal{C})+2}}, \tag{5.4}$$

and the expression on the right-hand side assumes values in $2^{\ell^{ss}(\mathcal{C})+1}\mathbb{Z}_2$ for all $c \in \mathcal{C}$, but there is some $c \in \mathcal{C}$ such that this expression is not in $2^{\ell^{ss}(\mathcal{C})+2}\mathbb{Z}_2$.

Proof. When $\ell^{ss}(\mathcal{C}) = 0$, the congruence $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod 2$ for all $c \in \mathcal{C}$ comes immediately from Proposition 5.11 above. If $\ell^{ss}(\mathcal{C}) > 0$, we use Proposition 5.11 above (setting $m = \ell^{ss}(\mathcal{C}) + 1$) to obtain

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I \lambda)! f_{\mathrm{pr}_I \lambda}^{(\ell^{ss}(\mathcal{C})+1)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{2^{\ell^{ss}(\mathcal{C})+1}},$$

where $f^{(\ell^{ss}(\mathcal{C})+1)}(\mathbf{x})$ is the polynomial described in Theorem 5.10, and $\Lambda^{ss}(\mathcal{C})$ is as defined in (4.27). But by the definition of $\ell^{ss}(\mathcal{C})$ as the minimum tier of any element in $\Lambda^{ss}(\mathcal{C})$, we see that the sum on the right-hand side of this congruence is empty, thus proving $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+1}}$.

Now we prove that $\mathrm{lee}^{\mathrm{norm}}(c)$ is not always divisible by $2^{\ell^{ss}(\mathcal{C})+2}$, along with the more precise statements at the end of the statement of this theorem, including congruence (5.4). In the rest of the proof, we return to considering $\ell^{ss}(\mathcal{C})$ arbitrary (possibly zero). We use

Proposition 5.11 again, but this time with $m = \ell^{ss}(\mathcal{C}) + 2$, to get

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\, \lambda)! f_{\mathrm{pr}_I\, \lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i) \pmod{p^{\ell^{ss}(\mathcal{C})+2}},$$

with $f^{(\ell^{ss}(\mathcal{C})+2)}(\mathbf{x}) \in \mathbb{Q}_2[\mathbf{x}]$ as described in Theorem 5.10. We have omitted to sum over λ with $\mathrm{Ti}\,(\lambda) < \ell^{ss}(\mathcal{C})$ since there are no such $\lambda \in \Lambda^{ss}(\mathcal{C})$ by the definition of $\ell^{ss}(\mathcal{C})$. This last congruence is (5.4), which we were to show. Let

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\, \lambda)! f_{\mathrm{pr}_I\, \lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \prod_{i \in I} \tilde{C}_i(\lambda_i),$$

which is the right-hand side of (5.4). Note that the coefficients of $f^{(\ell^{ss}(\mathcal{C})+2)}(\mathbf{x})$ are in $\mathbb{Q}_2$ (see Theorem 5.10), and note that $\tilde{C}_i(a) \in \mathbb{Z}_2[\zeta_{q'-1}]$ for all $i \in I$ and $a \in A$ (because $\tilde{C}(a) \in \mathbb{Z}_2[\zeta_{q'-1}]$ for all $a \in A$). Thus $Y(c) \in \mathbb{Q}_2(\zeta_{q'-1})$. We shall show that $Y(c)$ is actually in the smaller field $\mathbb{Q}_2$. To do this, it suffices to show that it is fixed by Fr. We use the Frobenius action $\mathrm{Fr_A}$ introduced in Section 2.7. By Lemma 2.30, we note that $\mathrm{Fr_A}$ restricted to $\Lambda^{ss}(\mathcal{C})$ is a permutation of $\Lambda^{ss}(\mathcal{C})$. Furthermore, by the same lemma, we note that if $\lambda \in \Lambda^{ss}(\mathcal{C})$, then $\mathrm{pr}_I\, \mathrm{Fr_A}(\lambda) = \mathrm{pr}_I\, \lambda$. So $\mathrm{Fr_A}$ preserves score and tier. Thus $\mathrm{Fr_A}$ permutes the set of $\lambda \in \Lambda^{ss}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell^{ss}(\mathcal{C})$. So we have

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\, \mathrm{Fr_A}(\lambda))! f_{\mathrm{pr}_I\, \mathrm{Fr_A}(\lambda)}^{(\ell^{ss}(\mathcal{C})+2)}}{\mathrm{Fr_A}(\lambda)!} \prod_{i \in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i).$$

By Lemma 2.30, we have $\mathrm{pr}_I\, \mathrm{Fr_A}(\lambda) = \mathrm{pr}_I\, \lambda$, $\mathrm{Fr_A}(\lambda)! = \lambda!$, and $\prod_{i \in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i) = \mathrm{Fr}\left(\prod_{i \in I} \tilde{C}_i(\lambda_i)\right)$, so that

$$Y(c) = |A| \sum_{\substack{\lambda \in \Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\, \lambda)! f_{\mathrm{pr}_I\, \lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \mathrm{Fr}\left(\prod_{i \in I} \tilde{C}_i(\lambda_i)\right).$$

Since the coefficients of $f^{(\ell^{ss}(\mathcal{C})+2)}(\mathbf{x})$ are in $\mathbb{Q}_2$ (see Theorem 5.10), we have

$$\begin{aligned} Y(c) &= \mathrm{Fr}\left(|A| \sum_{\substack{\lambda\in\Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda)=\ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\,\lambda)!\, f_{\mathrm{pr}_I\,\lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \right) \\ &= \mathrm{Fr}(Y(c)), \end{aligned}$$

so that $Y(c) \in \mathbb{Q}_2$. We have already proved that $\mathrm{lee}^{\mathrm{norm}}(c) \equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+1}}$ for all $c \in \mathcal{C}$. Since $\mathrm{lee}^{\mathrm{norm}}(c) \equiv Y(c) \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$ (this is (5.4)), we know that $Y(c) \in 2^{\ell^{ss}(\mathcal{C})+1}\mathbb{Z}_2$ for all $c \in \mathcal{C}$. So to finish our proof, we must show that there is some $c \in \mathcal{C}$ such that $\mathrm{lee}^{\mathrm{norm}}(c) \equiv Y(c) \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$ does not vanish modulo $2^{\ell^{ss}(\mathcal{C})+2}$.

To prove this, we shall use the notions of collapse and reduction introduced in Section 2.6. Note that $\tilde{c}_i(a)$ is a zero or a power of $\pi(\zeta_{q'-1})$ for all $a \in A$ and $i \in I$, since $\tilde{c}_i$ is the ith component of the canonical expansion of $\tilde{c}$. We let R be a set of p-class representatives of A and apply Lemma 2.18 to (5.4) to obtain

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda\in\Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\lambda)=\ell^{ss}(\mathcal{C})}} \frac{(\mathrm{pr}_I\,\lambda)!\, f_{\mathrm{pr}_I\,\lambda}^{(\ell^{ss}(\mathcal{C})+2)}}{\lambda!} \prod_{i\in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{2^{\ell^{ss}(\mathcal{C})+2}}.$$

If we define Λ_ℓ to be the set of elements of $\Lambda^{ss}(\mathcal{C})$ that are reduced and of tier $\ell^{ss}(\mathcal{C})$, we have

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv |A| \sum_{\lambda\in\Lambda_\ell} \sum_{\substack{\mu\in\Lambda^{ss}(\mathcal{C}) \\ \mathrm{Ti}(\mu)=\ell^{ss}(\mathcal{C}) \\ \mathrm{Red}(\mu)=\lambda}} \frac{(\mathrm{pr}_I\,\mu)!\, f_{\mathrm{pr}_I\,\mu}^{(\ell^{ss}(\mathcal{C})+2)}}{\mu!} \prod_{i\in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{2^{\ell^{ss}(\mathcal{C})+2}},$$

since the reduction of any $\mu \in \Lambda^{ss}(\mathcal{C})$ with $\mathrm{Ti}\,(\mu) = \ell^{ss}(\mathcal{C})$ is an element λ of Λ_ℓ by Lemma 4.14, and for such a μ, we have $\mathrm{Co}_R(\mu_i) = \mathrm{Co}_R(\lambda_i)$ for $i \in I$ by Lemma 2.24. For each $\lambda \in \Lambda_\ell$, set

$$B_\lambda = |A| \sum_{\substack{\mu\in\Lambda^{ss}(\mathcal{C}),\mathrm{Ti}(\mu)=\ell^{ss}(\mathcal{C}) \\ \mathrm{Red}(\mu)=\lambda}} \frac{(\mathrm{pr}_I\,\mu)!\, f_{\mathrm{pr}_I\,\mu}^{(\ell^{ss}(\mathcal{C})+2)}}{\mu!}, \tag{5.5}$$

which is an element of $\mathbb{Q}_2$ since the coefficients $f_\mu^{(\ell^{ss}(\mathcal{C})+2)}$ are in $\mathbb{Q}_2$. Then

$$\mathrm{lee}^{\mathrm{norm}}(c) \equiv \sum_{\lambda\in\Lambda_\ell} B_\lambda \prod_{i\in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \pmod{2^{\ell^{ss}(\mathcal{C})+2}}. \tag{5.6}$$

Note that the right-hand side of (5.6) is a $\mathbb{Q}_2$-linear combination of terms of the form

$$D_\lambda = \prod_{i\in I} \prod_{r\in R\cap S_i} \tilde{C}_i(r)^{(\mathrm{Co}_R(\lambda_i))_r}, \tag{5.7}$$

where we have restricted the second product of (5.7) to $R \cap S_i$ in view Lemma 2.17 and the fact that $\lambda_i \in \mathbb{N}[S_i]$ for all $\lambda \in \Lambda^{ss}(\mathcal{C})$. Note that no two terms D_λ and $D_{\lambda'}$ with $\lambda, \lambda' \in \Lambda_\ell$ have exactly the same exponents for all the terms $\tilde{C}_i(r)$, since that would imply that $\mathrm{Co}_R(\lambda_i) = \mathrm{Co}_R(\lambda_i')$ for all i, which would force $\lambda = \lambda'$, since λ and λ' are reduced (see Corollary 2.22). Also note that the exponent $(\mathrm{Co}_R(\lambda_i))_r$ of $\tilde{C}_i(r)$ in D_λ is less than 2^{e_r} by the definition of Co_R. (Recall that e_r denotes the cardinality of the 2-class of r in A.) As we vary c over all words in $\mathcal{C}$, Lemma 2.14 tells us that the values in $\{\tilde{C}_i(r) : i \in I, r \in R \cap S_i\}$ vary over $\prod_{i\in I}\prod_{r\in R\cap S_i} V_{i,r}$, where $V_{i,r}$ is the set containing 0 and all the powers of $\zeta_{2^{e_r}-1}$. Since no two elements of $V_{i,r}$ are equal to each other modulo 2, and since $|V_{i,r}| = 2^{e_r}$, which is strictly greater than the highest exponent of $\tilde{C}_i(r)$ appearing in any term (5.7) of (5.6), we may apply Lemma 2.33 to conclude that the minimum of the 2-adic valuations of codeword weights in $\mathcal{C}$ is precisely the minimum of the 2-adic valuations of the coefficients B_λ as λ runs over Λ_ℓ. So the first half of the theorem tells us that all such coefficients have 2-adic valuation at least $\ell^{ss}(\mathcal{C}) + 1$. We shall show that one such coefficient has 2-adic valuation precisely $\ell^{ss}(\mathcal{C}) + 1$; this will complete our proof.

We now wish to use Lemma 4.15, which provides facts about elements of tier $\ell^{ss}_{mc}(\mathcal{C})$ in $\Lambda^{ss}_{mc}(\mathcal{C})$. Since $p = 2$, we have $\Lambda^{ss}_{mc}(\mathcal{C}) = \Lambda^{ss}(\mathcal{C})$ (compare the definitions in (4.19) and (4.27)), and so $\ell^{ss}_{mc}(\mathcal{C}) = \ell^{ss}(\mathcal{C})$ (compare the definitions in (4.21) and (4.29) or see Proposition 4.22). Thus Lemma 4.15 is applicable here, and tells us that there exists a critical $\kappa \in \Lambda_\ell$ such that there is no $\mu \in \Lambda^{ss}(\mathcal{C})$ with $\mu \neq \kappa$, $\mathrm{Ti}\,(\mu) = \ell^{ss}(\mathcal{C})$, and $\mathrm{Red}(\mu) = \kappa$.

Thus the coefficient B_κ, as defined in (5.5), is just

$$B_\kappa = |A| \frac{(\mathrm{pr}_I \kappa)! f_{\mathrm{pr}_I \kappa}^{(\ell^{ss}(\mathcal{C})+2)}}{\kappa!}.$$

Since κ is reduced, we have $\kappa_{i,a} < 2$ for all $i \in I$ and $a \in A$ by definition, so the denominator of the fraction is 1. Since $|A|$ is coprime to 2, we have

$$v_2\left(B_\kappa\right) = v_2\left((\mathrm{pr}_I \kappa)! f_{\mathrm{pr}_I \kappa}^{(\ell^{ss}(\mathcal{C})+2)}\right).$$

Since κ is critical and $\mathrm{Ti}\,(\kappa) = \ell^{ss}(\mathcal{C})$, this means that $\mathrm{pr}_I \kappa \in \mathbb{N}[I]$ is critical and of tier $\ell^{ss}(\mathcal{C})$, so that Theorem 5.10 tells us that $v_2\left((\mathrm{pr}_I \kappa)! f_{\mathrm{pr}_I \kappa}^{(\ell^{ss}(\mathcal{C})+2)}\right) = \ell^{ss}(\mathcal{C}) + 1$. This completes our proof that there is some word $c \in \mathcal{C}$ with $\mathrm{lee}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{2^{\ell^{ss}(\mathcal{C})+2}}$. $\square$

Chapter 6

Zero Counts and Hamming Weights in $\mathrm{GR}(p^d, e)[A]$

In this chapter, we investigate the p-adic behavior of zero counts and Hamming weights in Abelian codes over arbitrary Galois rings. The main result of this chapter is Theorem 6.12, which was presented (in a specialized form) in the Introduction as Theorem 1.10. We recall the specialized version here:

Theorem 6.1 (Theorem 6.12, specialized). *Let $\mathcal{C}$ be a code in $\mathrm{GR}(p^d, e)[A]$ with 1_A not in the support of the Fourier transform of $\mathcal{C}$. Then $\mathrm{zer}(c) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$, or equivalently, $\mathrm{ham}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$.*

In order to understand this theorem, one must understand the definition of $\ell_{mc}(\mathcal{C})$ given in Section 1.1 of the Introduction. There we defined $\ell_{mc}(\mathcal{C})$ using unity-product sequences that consisted of elements in the support of the Fourier transform of the code, along with the pth powers of such elements. In this chapter, we shall define $\ell_{mc}(\mathcal{C})$ equivalently using multisets rather than sequences. In the special case where $e = 1$, we shall recover the multiset-based definition of $\ell_{mc}(\mathcal{C})$ given in (4.32) of Chapter 4. For arbitrary e, the construction that gives $\ell_{mc}(\mathcal{C})$ is somewhat more complicated. As always, the reader must be familiar with the definitions and notations for accounts in Section 2.5 to understand our presentation of such matters.

To prove the above theorem, we shall devise counting polynomials that will enable us to use Corollary 3.3 to p-adically approximate zero counts of words in Abelian codes over an arbitrary Galois ring $\mathrm{GR}(p^d, e)$. Looking at Corollary 3.3, we can see that we need, for

each $m \geq 1$, a polynomial $f^{(m)}(x_0, x_1, \ldots, x_{e-1}) \in \mathbb{Q}_p(\zeta_{q-1})[x_0, x_1, \ldots, x_{e-1}]$ such that

$$f^{(m)}(r, \mathrm{Fr}(r), \ldots, \mathrm{Fr}^{e-1}(r)) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } r \equiv 0 \pmod{p^d}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases} \tag{6.1}$$

for all $r \in \mathbb{Z}_p[\zeta_{q-1}]$. The first three sections (6.1–6.3) of this chapter will be dedicated to the construction of such polynomials. In Section 6.4, we shall employ them to prove Theorem 6.12 (the more precise version of Theorem 6.1 above). In Section 6.5, we compare our results with previous work. Since we are not aware of any prior generalization of McEliece's theorem to codes over arbitrary Galois rings, we consider the special cases $d = 1$ (codes over $\mathbb{F}_q$) and $e = 1$ (codes over $\mathbb{Z}/p^d\mathbb{Z}$) and compare with existing results in these scenarios.

Our starting point for the counting polynomial construction is Corollary 4.13 to Theorem 4.12, whose relevant contents we repeat here:

Proposition 6.2 (part of Corollary 4.13). *Let $t, m \geq 1$ and set $d_{t,m} = [m(p-1)+1]p^{t-1} - 1$. Then there exists a polynomial*

$$g^{(t,m)}(x) = \sum_{\substack{0 \leq n \leq d_{t,m} \\ p-1 \mid n}} g_n^{(t,m)} x^n$$

of degree $d_{t,m}$ in $\mathbb{Q}_p[x]$ such that

$$g^{(t,m)}(r) \equiv \begin{cases} 1 \pmod{p^m} & \textit{if } r \equiv 0 \pmod{p^t}, \\ 0 \pmod{p^m} & \textit{otherwise,} \end{cases}$$

for all $r \in \mathbb{Z}_p$. Furthermore, $d_{t,m}! g_{d_{t,m}}^{(t,m)} \equiv (-p)^{m-1} \pmod{p^m}$.

So $g^{(t,m)}$ approximates uniformly modulo p^m the characteristic function of the ideal $p^t\mathbb{Z}_p$ in the ring $\mathbb{Z}_p$. However, the polynomial $f^{(m)}$ that we seek (see (6.1)) must approximate the characteristic function of the ideal $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in the ring $\mathbb{Z}_p[\zeta_{q-1}]$. So we need to adapt the polynomials $g^{(t,m)}$ to work on this larger domain. The basic insight is to apply the trace to elements of $\mathbb{Z}_p[\zeta_{q-1}]$ to obtain elements of $\mathbb{Z}_p$, and then apply the polynomials $g^{(t,m)}$ to

the resulting elements in $\mathbb{Z}_p$. However, this path is fraught with technical difficulties, which we shall now examine and overcome.

Before moving on, we fix some common notations. Throughout this chapter, $\mathbf{x}$ will denote the list $x_0, \ldots, x_{e-1}$ of indeterminates and Tr will stand for Tr_1^e. Recall from Section 2.5 that $H = \{0, 1, \ldots, e-1\}$. We identify accounts in $\mathbb{N}[H]$ with e-tuples of integers: $\mu \in \mathbb{N}[H]$ is identified with the e-tuple $(\mu_0, \ldots, \mu_{e-1})$. Thus the notation $\mathbf{x}^\mu$ is shorthand for $x_0^{\mu_0} x_1^{\mu_1} \ldots x_{e-1}^{\mu_{e-1}}$ as described in Section 2.8. Also recall from Section 2.5 the compact notation that if $\mu \in \mathbb{N}[H]$ and $a \in \mathbb{Q}_p(\zeta_{q'-1})$ or $a \in \mathrm{GR}(p^d, ee')$, then $\mathrm{Fr}^\mu(a) = \prod_{h \in H} \left(\mathrm{Fr}^h(a)\right)^{\mu_h}$.

6.1 Trace and the p-Adic Valuation

The main difficulty with the trace function is that it does not preserve p-adic valuation. That is, for any $t \geq 1$, we can have $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a \not\equiv 0 \pmod{p^t}$ but with $\mathrm{Tr}(a) \equiv 0 \pmod{p^t}$. This can be seen by taking some $a = \pi_1(\zeta_{q-1})^k \in \mathbb{F}_q$ such that $\mathrm{Tr}(a) = 0$ and setting $b = \zeta_{q-1}^k$. Then commutativity of Tr with π_1 shows that $\mathrm{Tr}(b) \equiv 0 \pmod{p}$. Thus $\mathrm{Tr}(p^{t-1}b) = p^{t-1}\,\mathrm{Tr}(b) \equiv 0 \pmod{p^t}$, even though $p^{t-1}b \not\equiv 0 \pmod{p^t}$. In doing this exercise, we should have noted that trace does respect p-adic valuation in a certain sense: it never decreases p-adic valuation, for $\mathrm{Tr}(p^t r) = p^t\,\mathrm{Tr}(r)$.

We could exploit this property by setting R_t to be a set of representatives of the equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]$ and considering the average $|R_t|^{-1} \sum_{r \in R_t} g^{(t,m)}(\mathrm{Tr}(rx))$. If $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a = p^{v_p(a)}u$, and we vary r over R_t, the value ru should run through a set of representatives of equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]$. Thus, by the commutativity of π_t with Tr, the values $\mathrm{Tr}(ru) \pmod{p^t}$ should always run through the same set in $\mathbb{Z}/p^t\mathbb{Z}$ as r runs through R_t, regardless of the exact value of the unit u. Therefore, since $\mathrm{Tr}(ra) = p^{v_p(a)}\,\mathrm{Tr}(ru)$, the values of $\mathrm{Tr}(ra) \pmod{p^t}$ should vary over a subset of $\mathbb{Z}/p^t\mathbb{Z}$ that depends only on $v_p(a)$. Because the value modulo p^m of $g^{(t,m)}(s)$ is sensitive only to the congruence class modulo p^t of $s \in \mathbb{Z}_p$, this means that $|R_t|^{-1} \sum_{r \in R_t} g^{(t,m)}(\mathrm{Tr}(ra))$ should depend only on the p-adic valuation of a. This sketch has given the essence of the procedure, but it is not perfect in all details. It can be improved upon by replacing the set R_t with a smaller set of elements that nonetheless still have enough "p-adic uniformity"

to give a viable averaging procedure. The motivation for this substitution is that we can divide by fewer powers of p when we perform the averaging, thus minimizing the loss of p-adic accuracy of the final averaged function.

To set up our averaging procedure, which we call *trace-averaging*, we need precise versions of all the ideas in the previous paragraph. In particular, we must compute how many of the elements of $\mathrm{GR}(p^t, e)$ with a given valuation k are taken by trace to 0. So for $k \in \{0, 1, \ldots, t-1, \infty\}$, we define

$$\eta_k^t = \frac{\left|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k, \mathrm{Tr}(r) = 0\}\right|}{|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k\}|}. \tag{6.2}$$

We want to compute these fractions. Their values are given in Lemma 6.4 below, which is the goal of this section.

Recall that $\mathrm{Tr}(a) = \sum_{h=0}^{e-1} \mathrm{Fr}^h(a)$ and that Tr is a $\mathbb{Z}/p^t\mathbb{Z}$-linear map from $\mathrm{GR}(p^t, e)$ to $\mathbb{Z}/p^t\mathbb{Z}$. $\mathrm{Tr}\colon \mathrm{GR}(p^t, e) \to \mathbb{Z}/p^t\mathbb{Z}$ is also surjective because $\mathrm{Tr}\colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}_p$ is surjective and Tr commutes with π_t. This leads to a simple result, which will help in our proof of Lemma 6.4.

Lemma 6.3. *Let $t \geq 1$. For each $a \in \mathrm{GR}(p^t, e)$, there is some $b \in \mathrm{GR}(p^t, e)$ with $a \equiv b \pmod{p}$ and $\mathrm{Tr}(b) \in \{0, 1, \ldots, p-1\}$.*

Proof. Let $a \in \mathrm{GR}(p^d, e)$ and let $u \in \{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}/p^t\mathbb{Z}$ with $u \equiv \mathrm{Tr}(a) \pmod{p}$. Then choose $v \in \mathbb{Z}/p^t\mathbb{Z}$ with $\mathrm{Tr}(a) - u = pv$, and choose $w \in \mathrm{GR}(p^t, e)$ with $\mathrm{Tr}(w) = v$. Set $b = a - pw$ and note that $\mathrm{Tr}(b) = \mathrm{Tr}(a) - p\,\mathrm{Tr}(w) = \mathrm{Tr}(a) - pv = u$. □

Using this lemma, we construct a set U of representatives of equivalence classes modulo p in $\mathrm{GR}(p^t, e)$ such that $\mathrm{Tr}(u) \in \{0, 1, \ldots, p-1\}$ for each $u \in U$. We insist that 0 be the representative in U for the class $p\mathrm{GR}(p^t, e)$. We also define a set $V = \{u \in U : \mathrm{Tr}(u) = 0\}$, and we note that $0 \in V$. For the rest of this section, U and V will denote these sets.

Since U is a set of representatives of equivalence classes modulo p in $\mathrm{GR}(p^t, e)$, we have $|U| = q$, and each element of $a \in \mathrm{GR}(p^t, e)$ can be written uniquely as $\sum_{i=0}^{t-1} a_i p^i$, with each $a_i \in U$. By the commutativity of π_1 with Tr, the number of elements in U that are mapped by trace into $p\left(\mathbb{Z}/p^t\mathbb{Z}\right)$ is the same as the number of elements in $\mathbb{F}_q$ that are mapped by

trace to 0, i.e., q/p. So $|V| = q/p$. Now we are ready to calculate the fractions η_k^t.

Lemma 6.4. *Let $t \geq 1$. For $0 \leq k < t$, we have*

$$\left|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k\}\right| = (q-1)q^{t-1-k}$$

and

$$\left|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k, \mathrm{Tr}(r) = 0\}\right| = \left(\frac{q}{p} - 1\right)\left(\frac{q}{p}\right)^{t-1-k}.$$

Thus, with η_k^t as defined in (6.2)*, we have*

$$\eta_k^t = \left(\frac{q-p}{q-1}\right)p^{-t+k}.$$

Furthermore, $\eta_\infty^t = 1$.

Proof. Since 0 is the only element of $\mathrm{GR}(p^t, e)$ with infinite valuation, clearly $\eta_\infty^t = 1$. So henceforth we assume that k is a nonnegative integer less than t. As noted above, each element $r \in \mathrm{GR}(p^t, e)$ can be written uniquely as $\sum_{i=0}^{t-1} r_i p^i$, with each $r_i \in U$. The valuation of this element is k if and only if $r_0 = \cdots = r_{k-1} = 0$ and $r_k \neq 0$. Since $|U| = q$, this means that $\left|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k\}\right| = (q-1)q^{t-1-k}$. The trace of this element r is $\mathrm{Tr}(r) = \sum_{i=0}^{t-1} p^i \mathrm{Tr}(r_i)$. Since $\mathrm{Tr}(u) \in \{0, 1, \ldots, p-1\}$ for all $u \in U$, we see that the last expression is simply the p-ary expansion of r. Thus, $\mathrm{Tr}(r) = 0$ if and only if $\mathrm{Tr}(r_i) = 0$ for all i, i.e., if and only if $r_i \in V$ for all i. Thus, the elements $r \in \mathrm{GR}(p^t, e)$ with $v_p(r) = k$ and $\mathrm{Tr}(r) = 0$ are those with $r_0 = \cdots = r_{k-1} = 0$, $r_k \in V \setminus \{0\}$, and $r_{k+1}, \ldots, r_{t-1} \in V$. So $\left|\{r \in \mathrm{GR}(p^t, e) : v_p(r) = k\}\right| = \left(\frac{q}{p} - 1\right)\left(\frac{q}{p}\right)^{t-1-k}$. Then the value we claimed for η_k^t follows. □

This lemma shows us that although trace does not preserve the p-adic valuation, the probability that an element $a \in \mathrm{GR}(p^t, e)$ has $\mathrm{Tr}(a) = 0$ increases as $v_p(a)$ increases.

6.2 Trace-Averaged Characteristic Functions

Now we devise the averaging procedure that we sketched at the beginning of Section 6.1. It will be simpler at first to consider the effects of this averaging on the exact characteristic function of the ideal $p^t\mathbb{Z}_p$ in $\mathbb{Z}_p$, rather than on the polynomial approximations thereto.

Lemma 6.5. *Let $t \geq 1$ and suppose that $F_t \colon \mathbb{Z}_p \to \{0,1\}$ is the characteristic function of $p^t\mathbb{Z}_p$ in $\mathbb{Z}_p$. Let R be a set of representatives of equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]^\times$. Define $F_t^\dagger \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ by $F_t^\dagger(x) = \sum_{r\in R} F_t(\mathrm{Tr}(rx))$. Then*

$$F_t^\dagger(a) = \begin{cases} p^{v_p(a)}\left(\frac{q}{p}-1\right)\left(\frac{q}{p}\right)^{t-1} & \text{if } v_p(a) < t, \\ (q-1)q^{t-1} & \text{if } v_p(a) \geq t, \end{cases}$$

for any $a \in \mathbb{Z}_p[\zeta_{q-1}]$. Thus $F_t^\dagger$, as defined here, is independent of the choice of the set R.

Proof. Let $a \in \mathbb{Z}_p[\zeta_{q-1}]$. First let us consider the case when $v_p(a) \geq t$. Then $v_p(ra) \geq t$ for all $r \in R$, so $v_p(\mathrm{Tr}(ra)) \geq t$ for all $r \in R$. So $F_t(\mathrm{Tr}(ra)) = 1$ for all $r \in R$, and so $F_t^\dagger(a) = |R|$. Since R is a set of representatives of equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]^\times$, the cardinality of R is equal to the number of elements of $\mathrm{GR}(p^t,e)$ that do not vanish modulo p. So by Lemma 6.4, $|R| = (q-1)q^{t-1}$.

Now let us consider the case when $v_p(a) < t$. Write $a = p^k b$ with $b \in \mathbb{Z}_p[\zeta_{q-1}]^\times$. As r runs through R, the value $\pi_t(r)$ runs through the units of $\mathrm{GR}(p^t,e)$, and so $\pi_t(rb)$ also runs through the units of $\mathrm{GR}(p^t,e)$. We employ canonical expansions of elements of $\mathrm{GR}(p^t,e)$ to see that if $\pi_t(rb)$ has canonical expansion $u_0 + pu_1 + \cdots + p^{t-1}u_i$, then $\pi_t(ra)$ has canonical expansion $p^k u_0 + p^{k+1}u_1 + \cdots + p^{t-1}u_{t-1-k}$. That is, the value of $\pi_t(ra)$ depends only on the equivalence class modulo p^{t-k} of $\pi_t(rb)$. As r runs through R, we see that $\pi_{t-k}(rb)$ ranges over the units of $\mathrm{GR}(p^{t-k},e)$, taking each value an equal number of times. Thus, as r runs through R, the value $\pi_t(ra)$ ranges over $\{s \in \mathrm{GR}(p^t,e) : v_p(s) = k\}$, taking each value in this set an equal number of times. Therefore, as r runs through R, $\mathrm{Tr}(\pi_t(ra))$ must achieve the value 0 precisely $\eta_k^t|R|$ times. Since Tr commutes with π_t, this means that $\mathrm{Tr}(ra) \equiv 0$

(mod p^t) for precisely $\eta_k^t|R|$ values of r in R. So

$$\begin{aligned} F_t^\dagger(a) &= \eta_k^t|R| \\ &= \left(\frac{q-p}{q-1}\right) p^{-t+k}(q-1)q^{t-1} \\ &= p^k \left(\frac{q}{p} - 1\right) \left(\frac{q}{p}\right)^{t-1}. \end{aligned}$$

□

We now have a function $F_t^\dagger \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ that is sensitive to the p-adic valuation of its argument, but not to the specific equivalence class modulo p^t in which its argument lies. We now make linear combinations of the functions $F_t^\dagger$ for various t to produce the characteristic function of the ideal $p^t\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$.

Lemma 6.6. *For each $t \geq 1$, let $F_t^\dagger \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ be as defined in Lemma 6.5. Define $G \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ by*

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

Then G is the characteristic function of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$.

Proof. First, let us suppose that $a \in p^d\mathbb{Z}_p[\zeta_{q-1}]$. Then using the definition of G and the values of $F_i^\dagger(a)$ from Lemma 6.5 above, we have

$$\begin{aligned} G(a) &= \frac{p}{(p-1)q^d} \left[F_d^\dagger(a) - \left(\frac{q}{p} - 1\right) \left(1 + \sum_{i=1}^{d-1} F_i^\dagger(a)\right)\right] \\ &= \frac{p}{(p-1)q^d} \left[(q-1)q^{d-1} - \left(\frac{q}{p} - 1\right) \left(1 + \sum_{i=1}^{d-1} (q-1)q^{i-1}\right)\right] \\ &= \frac{p}{(p-1)q^d} \left[(q-1)q^{d-1} - \left(\frac{q}{p} - 1\right) q^{d-1}\right] \\ &= 1. \end{aligned}$$

On the other hand, suppose that $b \in \mathbb{Z}_p[\zeta_{q-1}]$ with $v_p(b) < d$. Set $k = v_p(b)$. Then by

the definition of G, we have

$$G(b) = \frac{p}{(p-1)q^d}\left[F_d^\dagger(b) - \left(\frac{q}{p} - 1\right)\left(1 + \sum_{i=1}^{d-1} F_i^\dagger(b)\right)\right]. \tag{6.3}$$

Using the values of $F_i^\dagger(b)$ given in Lemma 6.5, we have

$$\begin{aligned} 1 + \sum_{i=1}^{k} F_i^\dagger(b) &= 1 + \sum_{i=1}^{k} (q-1)q^{i-1} \\ &= q^k \end{aligned}$$

and

$$\begin{aligned} \sum_{i=k+1}^{d-1} F_i^\dagger(b) &= \sum_{i=k+1}^{d-1} p^k \left(\frac{q}{p} - 1\right)\left(\frac{q}{p}\right)^{i-1} \\ &= p^k\left[\left(\frac{q}{p}\right)^{d-1} - \left(\frac{q}{p}\right)^{k}\right] \\ &= p^k\left(\frac{q}{p}\right)^{d-1} - q^k, \end{aligned}$$

and so

$$\left(\frac{q}{p} - 1\right)\left(1 + \sum_{i=1}^{d-1} F_i^\dagger(b)\right) = p^k\left(\frac{q}{p} - 1\right)\left(\frac{q}{p}\right)^{d-1}.$$

By Lemma 6.5, this is equal to $F_d^\dagger(b)$. So (6.3) tells us that $G(b) = 0$ in this case. □

At this point, we could use the averaging technique in the lemma we just proved to obtain a polynomial-based approximation to the characteristic function G of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$. For G is seen to be a linear combination of the functions $F_i^\dagger$(as defined in Lemma 6.5), and each $F_i^\dagger$ is an averaged version of the characteristic function F_i of the ideal $p^i\mathbb{Z}_p$ in $\mathbb{Z}_p$. Since the polynomial $g^{(i,m)}$ of Proposition 6.2 approximates F_i uniformly modulo p^m on $\mathbb{Z}_p$, we could perform the same averaging technique on $g^{(i,m)}$ to obtain a function $G^{(i,m)}$ that approximates $F_i^\dagger$ uniformly modulo p^m on $\mathbb{Z}_p[\zeta_{q-1}]$. In fact, to obtain an approximation modulo p^m of G, we should have an approximation modulo p^{m+de-1} of each $F_i^\dagger$, since we multiply each $F_i^\dagger$ by a coefficient with p-adic valuation $-de+1$ to get the linear combination

that equals G. (See the lemma above for these coefficients.) Thus, we would start with the polynomials $g^{(i,m-1+de)}(x)$ for $i = 1, \ldots, d$. So we would need to work with polynomials of degree as high as $[(m-1+de)(p-1)+1]p^{d-1}-1$ (the degree of $g^{(d,m-1+de)}$) in this procedure.

We would like to keep the degrees of the polynomials we use as low as possible to keep the calculations with Corollary 3.3 as simple as possible. If we devise an averaging procedure more carefully, we can arrange so that we do not need to divide by so many powers of p in our calculations, thus allowing us to start with less p-adically accurate (hence lower degree) polynomial approximations. We shall still average a function $f(x)$ by taking $\sum_{r \in R} f(\mathrm{Tr}(rx))$ for some set R of units in $\mathbb{Z}_p[\zeta_{q-1}]$, but we shall not always use an entire set of representatives of the equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]^\times$.

Here we define the sets used in our averaging construction; these definitions will remain in force for the rest of this chapter. For each positive t, let $\mathrm{GR}(p^t,e)^{\equiv 1}$ be the subgroup of $\mathrm{GR}(p^t,e)^\times$ consisting of all elements that are congruent to 1 modulo p. Since $\mathbb{Z}/p^t\mathbb{Z} \subseteq \mathrm{GR}(p^t,e)$, we have $(\mathbb{Z}/p^t\mathbb{Z})^\times \subseteq \mathrm{GR}(p^t,e)^\times$, and so $(\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}$ is a subgroup of $\mathrm{GR}(p^t,e)^{\equiv 1}$. Let $\mathrm{GR}(p^t,e)^\sharp$ be a set of representatives of equivalence classes modulo $(\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}$ in the group $\mathrm{GR}(p^t,e)^{\equiv 1}$, where we insist that $1 \in \mathrm{GR}(p^t,e)^\sharp$. Note that if $t = 1$, then $\mathbb{Z}/p^t\mathbb{Z} = \mathbb{F}_p$, $\mathrm{GR}(p^t,e) = \mathbb{F}_q$, and so $(\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1} = \mathrm{GR}(p^t,e)^{\equiv 1} = \{1\}$, and thus $\mathrm{GR}(p^t,e)^\sharp = \{1\}$. Also note that if $e = 1$, then $\mathrm{GR}(p^t,e) = \mathbb{Z}/p^t\mathbb{Z}$, and so $\mathrm{GR}(p^t,e)^{\equiv 1} = (\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}$, and thus $\mathrm{GR}(p^t,e)^\sharp = \{1\}$. Now we lift our sets to subsets of $\mathbb{Z}_p[\zeta_{q-1}]^\times$ with the Teichmüller lift. Let $U_t = \tau\left((\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}\right)$ and $V_t = \tau\left(\mathrm{GR}(p^t,e)^\sharp\right)$. Since τ lifts elements of $\mathbb{Z}/p^t\mathbb{Z}$ into $\mathbb{Z}_p$, we have $U_t \subseteq {\mathbb{Z}_p}^\times$. Furthermore, if $t = 1$ or $e = 1$, we have $V_t = \{\tau(1)\} = \{1\}$. Let $W_t = \{u\zeta_{q-1}^j v : u \in U_t, 0 \le j < q-1, v \in V_t\}$.

Each element in $\mathrm{GR}(p^t,e)^\times$ can be represented uniquely as a product of a power of $\pi_t(\zeta_{q-1})$ and an element in $\mathrm{GR}(p^t,e)^{\equiv 1}$. Each element in $\mathrm{GR}(p^t,e)^{\equiv 1}$ can be represented uniquely as a product of an element in $(\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}$ and an element in $\mathrm{GR}(p^t,e)^\sharp$. Therefore, each element of $\mathrm{GR}(p^t,e)^\times$ can be represented uniquely as a product $u\left(\pi_t(\zeta_{q-1})^j\right)v$ with $u \in (\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}$, $0 \le j < q-1$, and $v \in \mathrm{GR}(p^t,e)^\sharp$. Thus, $\pi_t(W_t) = \mathrm{GR}(p^t,e)^\times$, and W_t is a set of representatives of the equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]^\times$. Now we can

describe our improved averaging procedure.

Lemma 6.7. *Let $t \geq 1$ and let $F_t \colon \mathbb{Z}_p \to \{0,1\}$ be the characteristic function of $p^t\mathbb{Z}_p$ in $\mathbb{Z}_p$. Let $F_t^\dagger$ be as defined in Lemma 6.5. Let V_t be as defined above in this section. Define $F_t^* \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ by $F_t^*(x) = \sum_{j=0}^{q-2} \sum_{v \in V_t} F_t(\mathrm{Tr}(\zeta_{q-1}^j vx))$. Then $F_t^*(x) = p^{-t+1} F_t^\dagger(x)$.*

Proof. Use W_t as the set R of representatives of equivalence classes modulo p^t in $\mathbb{Z}_p[\zeta_{q-1}]^\times$ in Lemma 6.5 to get

$$\begin{aligned} F^\dagger(x) &= \sum_{w \in W_t} F_t(\mathrm{Tr}(wx)) \\ &= \sum_{u \in U_t} \sum_{j=0}^{q-2} \sum_{v \in V_t} F_t\left(\mathrm{Tr}\left(u\zeta_{q-1}^j vx\right)\right). \end{aligned}$$

Note that $U_t \subseteq {\mathbb{Z}_p}^\times$ and Tr is $\mathbb{Z}_p$-linear. Also note that $F_t(ux) = F_t(x)$ for any $u \in U_t$ because F_t is the characteristic function of the ideal p^t in $\mathbb{Z}_p$. Thus

$$\begin{aligned} F^\dagger(x) &= \sum_{u \in U_t} \sum_{j=0}^{q-2} \sum_{v \in V_t} F_t\left(u\,\mathrm{Tr}\left(\zeta_{q-1}^j vx\right)\right) \\ &= \sum_{u \in U_t} \sum_{j=0}^{q-2} \sum_{v \in V_t} F_t\left(\mathrm{Tr}\left(\zeta_{q-1}^j vx\right)\right) \\ &= |U_t| F^*(x), \end{aligned}$$

and note that $|U_t| = \left|(\mathbb{Z}/p^t\mathbb{Z})^{\equiv 1}\right| = p^{t-1}$ to finish the proof. □

Now we linearly combine the functions F_i^* to obtain the characteristic function of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$.

Lemma 6.8. *For each $t \geq 1$, let $F_t^* \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ be as defined in Lemma 6.7. Define $J \colon \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ by*

$$J(x) = \frac{p^d}{(p-1)q^d}\left[F_d^*(x) - \left(\frac{q}{p} - 1\right)\left(p^{-d+1} + \sum_{i=1}^{d-1} p^{-d+i} F_i^*(x)\right)\right].$$

Then J is the characteristic function of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$.

Proof. For each $t \geq 1$, we define $F_t^\dagger : \mathbb{Z}_p[\zeta_{q-1}] \to \mathbb{Z}$ as in Lemma 6.5. Then Lemma 6.6 tells us that

$$G(x) = \frac{p}{(p-1)q^d}\left[F_d^\dagger(x) - \left(\frac{q}{p} - 1\right)\left(1 + \sum_{i=1}^{d-1} F_i^\dagger(x)\right)\right]$$

is the characteristic function of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$. Now Lemma 6.7 tells us that $F_t^\dagger(x) = p^{t-1}F_t^*(x)$ for each $t \geq 1$, so that

$$\begin{aligned} G(x) &= \frac{p}{(p-1)q^d}\left[p^{d-1}F_d^*(x) - \left(\frac{q}{p} - 1\right)\left(1 + \sum_{i=1}^{d-1} p^{i-1}F_i^*(x)\right)\right] \\ &= \frac{p^d}{(p-1)q^d}\left[F_d^*(x) - \left(\frac{q}{p} - 1\right)\left(p^{-d+1} + \sum_{i=1}^{d-1} p^{-d+i}F_i^*(x)\right)\right] \\ &= J(x), \end{aligned}$$

which is what we were to show. □

This lemma provides an archetype for the polynomial approximations that will be devised in the next section.

6.3 Trace-Averaged Counting Polynomials

Now we shall apply our averaging procedures to polynomials. If we were to apply one of our averaging procedures (like those used in Lemma 6.5 or Lemma 6.7) directly to a polynomial, we would obtain a polynomial function of the terms $\{\mathrm{Fr}^h(x) : h \in H\}$. In general, such functions need not be polynomials in x. For example, $f(x) = \mathrm{Fr}(x) - x$ vanishes on all of $\mathbb{Z}_p$, but not on all of $\mathbb{Z}_p[\zeta_{q-1}]$, so it cannot be a polynomial in $\mathbb{Q}_p(\zeta_{q-1})[x]$. Although we could proceed with the larger class of "polynomials with automorphisms applied to their indeterminates," we prefer to work with polynomials in the usual sense. Therefore, we shall define a slightly different averaging procedure that takes single-variable polynomials to multivariable polynomials.

If $f(x) \in \mathbb{Q}_p[x]$ and $t \geq 1$, we define the *t-trace-average of* $f(x)$, denoted $\mathfrak{T}_t f(\mathbf{x})$, to be

the multivariable polynomial in $\mathbb{Q}_p(\zeta_{q-1})[\mathbf{x}]$ given by

$$\mathfrak{T}_t f(x_0, \ldots, x_{e-1}) = \sum_{j=0}^{q-2} \sum_{v \in V_t} f\left(\sum_{h \in H} \mathrm{Fr}^h(\zeta_{q-1}^j v) x_h \right).$$

These polynomials are designed to be evaluated at elements of $\mathbb{Z}_p[\zeta_{q-1}]^e$ that are equal to $(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a))$ for some $a \in \mathbb{Z}_p[\zeta_{q-1}]$, since

$$\mathfrak{T}_t f(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) = \sum_{j=0}^{q-2} \sum_{v \in V_t} f\left(\mathrm{Tr}(\zeta_{q-1}^j v a) \right) \tag{6.4}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$. The next lemma investigates how t-trace-averaging affects a polynomial. The reader should recall the material from Section 2.5 on multisets, including the definition of a Delsarte-McEliece multiset. The reader should also recall the compact notations introduced there, some of which were reviewed at the beginning of this chapter (just prior to Section 6.1).

Lemma 6.9. *Suppose that $t \geq 1$ and $f(x) = \sum_{i=0}^{n} f_i x^i$ is a polynomial in $\mathbb{Q}_p[x]$ of degree n. For each $\mu \in \mathbb{N}[H]$, set $\rho_{t,\mu} = \sum_{v \in V_t} \mathrm{Fr}^{\mu}(v)$. Then for all $t, e \geq 1$, we have*

$$\mathfrak{T}_t f(\mathbf{x}) = (q-1) \sum_{i=0}^{n} i! f_i \sum_{\substack{\mu \in \mathbb{N}[H] \\ \Sigma\mu = 0, |\mu| = i}} \frac{\rho_{t,\mu}}{\mu!} \mathbf{x}^{\mu}. \tag{6.5}$$

Thus $\mathfrak{T}_t f(\mathbf{x})$ is of degree at most n. If $t = 1$ or $e = 1$, then $\rho_{t,\mu} = 1$ for all $\mu \in \mathbb{N}[H]$, and so we have

$$\mathfrak{T}_t f(\mathbf{x}) = (q-1) \sum_{i=0}^{n} i! f_i \sum_{\substack{\mu \in \mathbb{N}[H] \\ \Sigma\mu = 0, |\mu| = i}} \frac{\mathbf{x}^{\mu}}{\mu!}.$$

Proof. Since $\mathfrak{T}_t$ is $\mathbb{Q}_p$-linear, it suffices to consider $f(x) = x^n$. Then we have

$$\begin{aligned} \mathfrak{T}_t f(\mathbf{x}) &= \sum_{j=0}^{q-2} \sum_{v \in V_t} \left(\sum_{h \in H} \mathrm{Fr}^h(\zeta_{q-1}^j v) x_h \right)^n \\ &= \sum_{j=0}^{q-2} \sum_{v \in V_t} \sum_{h_1, \ldots, h_n \in H} \prod_{i=1}^{n} \mathrm{Fr}^{h_i}(\zeta_{q-1}^j v) x_{h_i}. \end{aligned}$$

We want to sum over multisets of elements in H rather than sequences. Recall that if $\mu \in \mathbb{N}[H]$, there are $\frac{|\mu|!}{\mu!}$ distinct ways of arranging the elements of μ into a sequence of $|\mu|$ terms. Thus, we have

$$\begin{aligned}
\mathfrak{T}_t f(\mathbf{x}) &= \sum_{j=0}^{q-2} \sum_{v \in V_t} \sum_{\substack{\mu \in \mathbb{N}[H] \\ |\mu|=n}} \frac{|\mu|!}{\mu!} \prod_{h \in H} \left(\mathrm{Fr}^h(\zeta_{q-1}^j v) x_h \right)^{\mu_h} \\
&= \sum_{j=0}^{q-2} \sum_{v \in V_t} \sum_{\substack{\mu \in \mathbb{N}[H] \\ |\mu|=n}} \frac{n!}{\mu!} \mathrm{Fr}^\mu(\zeta_{q-1}^j) \mathrm{Fr}^\mu(v) \mathbf{x}^\mu \\
&= n! \sum_{\substack{\mu \in \mathbb{N}[H] \\ |\mu|=n}} \frac{1}{\mu!} \mathbf{x}^\mu \sum_{v \in V_t} \mathrm{Fr}^\mu(v) \sum_{j=0}^{q-2} \mathrm{Fr}^\mu(\zeta_{q-1}^j),
\end{aligned}$$

and so, using the definition of $\rho_{t,\mu}$ given in the statement of the lemma, we have

$$\mathfrak{T}_t f(\mathbf{x}) = n! \sum_{\substack{\mu \in \mathbb{N}[H] \\ |\mu|=n}} \frac{\rho_{t,\mu}}{\mu!} \mathbf{x}^\mu \sum_{j=0}^{q-2} \mathrm{Fr}^\mu(\zeta_{q-1}^j). \tag{6.6}$$

Let us examine the last sum in our last expression, i.e.,

$$\begin{aligned}
\sum_{j=0}^{q-2} \mathrm{Fr}^\mu(\zeta_{q-1}^j) &= \sum_{j=0}^{q-2} \prod_{h \in H} \mathrm{Fr}^h(\zeta_{q-1}^j)^{\mu_h} \\
&= \sum_{j=0}^{q-2} \prod_{h \in H} \zeta_{q-1}^{j p^h \mu_h} \\
&= \sum_{j=0}^{q-2} \zeta_{q-1}^{j \sum_{h \in H} p^h \mu_h}.
\end{aligned}$$

This sum will be zero unless $\sum_{h \in H} p^h \mu_h \equiv 0 \pmod{q-1}$, i.e., unless $\Sigma\mu = 0$, in which case the sum is $q-1$. So, returning to (6.6), we have

$$\mathfrak{T}_t f(\mathbf{x}) = (q-1) n! \sum_{\substack{\mu \mathbb{N}[H] \\ \Sigma\mu=0, |\mu|=n}} \frac{\rho_{t,\mu}}{\mu!} \mathbf{x}^\mu.$$

Thus (6.5) holds for any monomial $f(x) = x^n$, and so, by $\mathbb{Q}_p$-linearity, for any polynomial.

If $\mu \in \mathbb{N}[H]$, the degree of $\mathbf{x}^\mu$ is $|\mu|$, so the degree of the polynomial $\mathfrak{T}_t f(\mathbf{x})$ is not higher than the degree of $f(x)$. Furthermore, if $t = 1$ or $e = 1$, then $V_t = \{1\}$, so that $\rho_{t,\mu} = 1$ for all $\mu \in \mathbb{N}[H]$. □

Now we are ready to construct a polynomial approximating the characteristic function of the ideal $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$.

Proposition 6.10. *Let $m \geq 1$. For each $t, n \geq 1$, let $g^{(t,n)}$ be the polynomial described in Proposition 6.2. For each $t \in \{1, 2, \ldots, d\}$, set $G^{(t,m)}(\mathbf{x}) = \mathfrak{T}_t g^{(t,m+ed-t)}(\mathbf{x})$. Let*

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

Then

$$f^{(m)}(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a \equiv 0 \pmod{p^d}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$. Let $d_m = [(m + (e-1)d)(p-1) + 1]p^{d-1} - 1$. We can write

$$f^{(m)} = \sum_{\substack{\mu \in \mathbb{N}[H] \\ \Sigma\mu = 0, |\mu| \leq d_m}} f_\mu^{(m)} \mathbf{x}^\mu,$$

where all the coefficients $f_\mu^{(m)}$ are in $\mathbb{Q}_p(\zeta_{q-1})$. Thus, the degree of $f^{(m)}$ is at most d_m.

Proof. Proposition 6.2 says that $g^{(t,m+ed-t)}$ approximates uniformly modulo p^{m+ed-t} the characteristic function of the ideal $p^t\mathbb{Z}_p$ in $\mathbb{Z}_p$. We call this characteristic function F_t, as in Lemma 6.7. We shall show that $G^{(t,m)}$, the averaged version of $g^{(t,m+ed-t)}$, approximates the function F_t^* defined in Lemma 6.7. By (6.4), we have

$$\begin{aligned} G^{(t,m)}(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) &= \sum_{j=0}^{q-2} \sum_{v \in V_t} g^{(t,m+ed-t)}(\mathrm{Tr}(\zeta_{q-1}^j va)) \\ &\equiv \sum_{j=0}^{q-2} \sum_{v \in V_t} F_t(\mathrm{Tr}(\zeta_{q-1}^j va)) \pmod{p^{m+ed-t}} \\ &\equiv F_t^*(a) \pmod{p^{m+ed-t}} \end{aligned}$$

for each $a \in \mathbb{Z}_p[\zeta_{q-1}]$. Thus

$$\frac{p^d}{(p-1)q^d} G^{(d,m)}(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \equiv \frac{p^d}{(p-1)q^d} F_d^*(a) \pmod{p^m} \tag{6.7}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$, and for each $i \in \{1, 2, \ldots, d-1\}$, we have

$$\begin{aligned} -\frac{p^d}{(p-1)q^d}\left(\frac{q}{p}-1\right) p^{-d+i} G^{(i,m)}(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \\ \equiv -\frac{p^d}{(p-1)q^d}\left(\frac{q}{p}-1\right) p^{-d+i} F_i^*(a) \pmod{p^m}. \end{aligned} \tag{6.8}$$

Now add congruence (6.7) and all the congruences (6.8) for $i = 1, 2, \ldots, d-1$, and then add the constant $-\frac{p^d}{(p-1)q^d}\left(\frac{q}{p}-1\right) p^{-d+1}$ to both sides of the resulting congruence to obtain

$$\begin{aligned} f^{(m)}(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \\ \equiv \frac{p^d}{(p-1)q^d}\left[F_d^*(a) - \left(\frac{q}{p}-1\right)\left(p^{-d+1} + \sum_{i=1}^{d-1} p^{-d+i} F_i^*(a)\right)\right] \pmod{p^m} \end{aligned}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$. By Lemma 6.8, the right-hand side of this congruence is $J(a)$, where J is the characteristic function of $p^d\mathbb{Z}_p[\zeta_{q-1}]$ in $\mathbb{Z}_p[\zeta_{q-1}]$. This proves that $f^{(m)}(\mathbf{x})$ takes the values (modulo p^m) we claimed on all of $\mathbb{Z}_p[\zeta_{q-1}]$.

Lemma 6.9 shows us that for each $i \in \{1, 2, \ldots, d\}$, we may write the polynomial $G^{(i,m)}(\mathbf{x}) = \sum_{\mu \in B_{i,m}} G_\mu^{(i,m)} \mathbf{x}^\mu$, where $B_{i,m}$ is the set of all Delsarte-McEliece multisets $\mu \in \mathbb{N}[H]$ such that $|\mu|$ is less than or equal to the degree $[(m+ed-i)(p-1)+1]p^{i-1}-1$ of the polynomial $g^{(i,m+ed-i)}$. We claim that the maximum of these degrees is the degree of $g^{(d,m+ed-d)}$, i.e., $[(m+(e-1)d)(p-1)+1]p^{d-1}-1$, which is the value d_m defined in the statement of this proposition. We prove our claim by showing that $N(i) = [(m+ed-i)(p-1)+1]p^{i-1} - 1$

is an increasing function of i for $1 \leq i \leq d$. Note that if $1 \leq i < d$, then

$$\begin{aligned} N(i+1) - N(i) &= [(m+ed-i-1)(p-1)+1]p^i - [(m+ed-i)(p-1)+1]p^{i-1} \\ &= [(m+ed-i-1)p(p-1)+p-(m+ed-i)(p-1)-1]p^{i-1} \\ &= [(m+ed-i-1)p(p-1)-(m+ed-i-1)(p-1)]p^{i-1} \\ &= (m+ed-i-1)(p-1)^2p^{i-1} \\ &\geq (m+(e-1)d)(p-1)^2p^{i-1} \\ &> 0. \end{aligned}$$

Thus $B_{1,m} \subseteq B_{2,m} \subseteq \cdots \subseteq B_{d,m}$. So each $G^{(i,m)}$ can be written $G^{(i,m)} = \sum_{\mu \in B_{d,m}} G_\mu^{(i,m)} \mathbf{x}^\mu$, and so $f^{(m)}$ can also be written

$$\begin{aligned} f^{(m)} &= \sum_{\mu \in B_{d,m}} f_\mu^{(m)} \mathbf{x}^\mu \\ &= \sum_{\substack{\mu \in \mathbb{N}[H] \\ \Sigma\mu = 0, |\mu| \leq d_m}} f_\mu^{(m)} \mathbf{x}^\mu. \end{aligned}$$

Thus the degree of $f^{(m)}$ is at most d_m. We know from Proposition 6.2 that the coefficients of each $g^{(t,n)}(x)$ are in $\mathbb{Q}_p$. Thus the coefficients of $G^{(i,m)}(\mathbf{x})$, and hence the coefficients of $f^{(m)}(\mathbf{x})$, are in $\mathbb{Q}_p(\zeta_{q-1})$ by the definition of the i-trace-average of a polynomial. □

This proposition gives us the counting polynomials that we shall use with Corollary 3.3 to estimate zero counts of words in $\mathrm{GR}(p^d, e)[A]$.

6.4 Zero Count and Hamming Weight

We are now ready to investigate the p-adic behavior of zero counts of words in $\mathrm{GR}(p^d, e)[A]$. Throughout this chapter, we suppose that we have a code $\mathcal{C} \subseteq \mathrm{GR}(p^d, e)[A]$ and that S is the minimal support of the Fourier transform of $\mathcal{C}$. We suppose that S is not a subset of $\{1_A\}$, i.e., that S contains an element of A that is not the identity. Otherwise we have a trivial situation: $\mathcal{C}$ consists only of constant words, and then $\mathrm{zer}(c) = |A| \,\mathrm{zer}(\tilde{c}(1_A))$ for all

$c \in \mathcal{C}$.

Before we present our calculations, we define the parameter $\ell_{mc}(\mathcal{C})$ first mentioned in Section 1.1 of the Introduction. There $\ell_{mc}(\mathcal{C})$ was defined using sequences; here we define it (equivalently) using multisets. First we define

$$\Lambda_{mc}(\mathcal{C}) = \{\lambda \in \mathbb{N}[H \times S] : \Pi\lambda = 1_A, \mathrm{pr}_A\, \lambda \notin \mathbb{N}[\{1_A\}], \Sigma\, \mathrm{pr}_H\, \lambda = 0\}. \tag{6.9}$$

Note that the last condition on λ states that λ is Delsarte-McEliece. We claim that $\Lambda_{mc}(\mathcal{C})$ is nonempty. By assumption there exists $a \in S$ with $a \neq 1_A$. Let n be the group-theoretic order of a. Consider the multiset λ with $(q-1)n$ instances of the pair $(0, a)$ and no other elements. This λ is a unity-product but not all-unity multiset in $\mathbb{N}[H \times S]$ with $\Sigma\, \mathrm{pr}_H\, \lambda = 0$. So $\Lambda_{mc}(\mathcal{C}) \neq \emptyset$. Note that Lemma 2.16 tells us that all elements of $\Lambda_{mc}(\mathcal{C})$ have cardinality divisible by $p-1$ and greater than or equal to $e(p-1)$. For each $\lambda \in \Lambda_{mc}(\mathcal{C})$, we define the *tier of* λ, denoted $\mathrm{Ti}\,(\lambda)$, to be

$$\mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{|\lambda| - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1)\right\}. \tag{6.10}$$

Since $\Lambda_{mc}(\mathcal{C}) \neq \emptyset$, we may set

$$\omega_{mc}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}(\mathcal{C})} |\lambda| \tag{6.11}$$

and

$$\ell_{mc}(\mathcal{C}) = \min_{\lambda \in \Lambda_{mc}(\mathcal{C})} \mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{\omega_{mc}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1)\right\}. \tag{6.12}$$

In Section 6.5, we shall show that when $e = 1$, these parameters $\omega_{mc}(\mathcal{C})$ and $\ell_{mc}(\mathcal{C})$ are the same as the parameters with the same names defined in (4.31) and (4.32).

Now we can state and prove our p-adic estimates of zero counts. We start by combining Corollary 3.3 with the counting polynomials from Proposition 6.10 to provide estimates modulo an arbitrary power of p.

Proposition 6.11. *Let $\mathcal{C}$ be a code in $\mathrm{GR}(p^d, e)[A]$. Let $m \geq 1$ and let $f^{(m)}(\mathbf{x})$ be the polynomial described in Proposition 6.10. For each $c \in \mathcal{C}$, we let C be the element of*

$\mathbb{Z}_p[\zeta_{q'-1}][A]$ *such that* $\tilde{C} = \tau \circ \tilde{c}$. *For any* $c \in \mathcal{C}$, *we have*

$$\operatorname{zer}^{\text{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \operatorname{Ti}(\lambda) < m}} \frac{(\operatorname{pr}_H \lambda)! f^{(m)}_{\operatorname{pr}_H \lambda}}{\lambda!} \tilde{C}(\lambda) \pmod{p^m},$$

where $\Lambda_{mc}(\mathcal{C})$ *is as defined in* (6.9).

Proof. Note that the polynomial $f^{(m)}(\mathbf{x})$ in Proposition 6.10 has the property that

$$f^{(m)}(a, \operatorname{Fr}(a), \ldots, \operatorname{Fr}^{e-1}(a)) \equiv \operatorname{zer}(\pi(a)) \pmod{p^m}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$. Set $d_m = [(m + (e-1)d)(p-1) + 1]p^{d-1} - 1$, which is the upper bound on the degree of $f^{(m)}(\mathbf{x})$ given in Proposition 6.10. Then Corollary 3.3 tells us that

$$\operatorname{zer}^{\text{norm}}(c) \equiv |A| \sum_{\mu \in \mathbb{N}[H]} \mu! f^{(m)}_\mu \sum_{\substack{\lambda \in \mathbb{N}[H \times S], \operatorname{pr}_H \lambda = \mu \\ \Pi\lambda = 1_A, \operatorname{pr}_A \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^m}.$$

We may restrict the sum over μ to the set of Delsarte-McEliece multisets with cardinality less than d_m, because Proposition 6.10 tells us that $f^{(m)}_\mu = 0$ if μ does not meet these additional conditions. So

$$\operatorname{zer}^{\text{norm}}(c) \equiv |A| \sum_{\substack{\mu \in \mathbb{N}[H] \\ \Sigma\mu = 0, |\mu| \le d_m}} \mu! f^{(m)}_\mu \sum_{\substack{\lambda \in \mathbb{N}[H \times S], \operatorname{pr}_H \lambda = \mu \\ \Pi\lambda = 1_A, \operatorname{pr}_A \lambda \notin \mathbb{N}[\{1_A\}]}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^m}.$$

Since the sum over λ has the condition $\operatorname{pr}_H \lambda = \mu$, the condition $\Sigma\mu = 0$ in the first sum can be replaced by the condition $\Sigma \operatorname{pr}_H \lambda = 0$ in the second sum, which shows that the second sum is the sum over those $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $\operatorname{pr}_H \lambda = \mu$. We use this, and the fact

that $|\mathrm{pr}_H \lambda| = |\lambda|$, to obtain

$$\begin{aligned}
\mathrm{zer}^{\mathrm{norm}}(c) &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[H] \\ |\mu| \le d_m}} \mu! f_\mu^{(m)} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{pr}_H \lambda = \mu}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^m} \\
&\equiv |A| \sum_{\mu \in \mathbb{N}[H]} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ |\lambda| \le d_m, \mathrm{pr}_H \lambda = \mu}} \frac{\mathrm{pr}_H \lambda! f_{\mathrm{pr}_H \lambda}^{(m)}}{\lambda!} \tilde{C}(\lambda) \pmod{p^m} \\
&\equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ |\lambda| \le d_m}} \frac{\mathrm{pr}_H \lambda! f_{\mathrm{pr}_H \lambda}^{(m)}}{\lambda!} \tilde{C}(\lambda) \pmod{p^m}.
\end{aligned}$$

We claim that the condition $|\lambda| \le d_m$ is equivalent to $\mathrm{Ti}\,(\lambda) < m$; showing this will finish the proof. Note that $\mathrm{Ti}\,(\lambda) < m$ if and only if $\left\lfloor \frac{|\lambda| - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor - d(e-1) < m$, and this is equivalent to $|\lambda| - p^{d-1} < (m + d(e-1))(p-1)p^{d-1}$. This, in turn, is equivalent to $|\lambda| < [(m + d(e-1))(p-1) + 1]p^{d-1}$, which is equivalent to $|\lambda| \le d_m$. □

This calculation leads immediately to an analogue of McEliece's theorem for Abelian codes over Galois rings.

Theorem 6.12. *Let $\mathcal{C}$ be a code in $\mathrm{GR}(p^d, e)[A]$. With $\ell_{mc}(\mathcal{C})$ as defined in* (6.12)*, we have $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$. Equivalently, $\mathrm{ham}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ for all $c \in \mathcal{C}$.*

Proof. If $\ell_{mc}(\mathcal{C}) = 0$, then the claims of the theorem are trivial. So assume $\ell_{mc}(\mathcal{C}) > 0$ henceforth. For each $c \in \mathcal{C}$, we let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ with $\tilde{C} = \tau \circ \tilde{c}$. By Proposition 6.11 above (setting $m = \ell_{mc}(\mathcal{C})$), we have

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) < \ell_{mc}(\mathcal{C})}} \frac{(\mathrm{pr}_H \lambda)! f_{\mathrm{pr}_H \lambda}^{(\ell_{mc}(\mathcal{C}))}}{\lambda!} \tilde{C}(\lambda) \pmod{p^{\ell_{mc}(\mathcal{C})}},$$

where $f^{(\ell_{mc}(\mathcal{C}))}(\mathbf{x})$ is the polynomial described in Proposition 6.10, and $\Lambda_{mc}(\mathcal{C})$ is as defined in (6.9). By the definition of $\ell_{mc}(\mathcal{C})$ as the minimum tier of any element of $\Lambda_{mc}(\mathcal{C})$, the sum on the right-hand side is empty, thus giving the desired congruence for $\mathrm{zer}^{\mathrm{norm}}$. The congruence for $\mathrm{ham}^{\mathrm{norm}}$ follows immediately from the fact that $\mathrm{ham}^{\mathrm{norm}}(c) = -\mathrm{zer}^{\mathrm{norm}}(c)$

for all $c \in \mathrm{GR}(p^d, e)[A]$, as was shown in Section 2.4. □

For the remainder of this chapter, we shall see how these results compare with earlier results in the special cases when $d = 1$ and $e = 1$. In the $d = 1$ case, we obtain in fullness the theorem of Delsarte and McEliece [18]. When we set $e = 1$, we obtain a weakened form of Theorem 4.18.

6.5 Comparison with Previous Work

At the beginning of this chapter, we noted that we are not aware of any generalization of McEliece's theorem to codes over arbitrary Galois rings. So we have no such results with which to compare Proposition 6.11 and Theorem 6.12. Instead, we show here that we can obtain previous results if we specialize to the case $d = 1$ (codes over $\mathbb{F}_q$) and to the case $e = 1$ (codes over $\mathbb{Z}/p^d\mathbb{Z}$).

First we show that we can retrieve the theorem of Delsarte and McEliece from Proposition 6.11 in the special case when $d = 1$. Before we proceed, we note that when $d = 1$, we have $\mathrm{Ti}\,(\lambda) = \max\left\{0, \left\lfloor \frac{|\lambda|-1}{p-1} \right\rfloor - (e-1)\right\}$. If we apply this to a Delsarte-McEliece element $\lambda \in \mathbb{N}[H \times A]$, then we note that $|\lambda|$ is divisible by $p-1$ (see Lemma 2.16). Thus $\mathrm{Ti}\,(\lambda) = \max\left\{0, \frac{|\lambda|}{p-1} - e\right\}$ for all λ with $\Sigma\,\mathrm{pr}_H\,\lambda = 0$ (and thus for all $\lambda \in \Lambda_{mc}(\mathcal{C})$). Lemma 2.16 tells us that nonempty Delsarte-McEliece multisets have cardinality at least $e(p-1)$, so

$$\mathrm{Ti}\,(\lambda) = \frac{|\lambda|}{(p-1)} - e \tag{6.13}$$

for all nonempty Delsarte-McEliece multisets $\lambda \in \mathbb{N}[H \times A]$ (and thus for all $\lambda \in \Lambda_{mc}(\mathcal{C})$).

Now we are ready to present the Delsarte-McEliece theorem. Although the following theorem is cast into our own notation and terminology, it is equivalent to the original.

Theorem 6.13 (Delsarte-McEliece [18]). *Let $\mathcal{C}$ be a code in $\mathbb{F}_q[A]$. For each $c \in \mathcal{C}$, let C be the element of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C} = \tau \circ \tilde{c}$. Let $\Lambda_{mc}(\mathcal{C})$ and $\ell_{mc}(\mathcal{C})$ be as defined*

in (6.9) *and* (6.12). *Then for any* $c \in \mathcal{C}$, *we have*

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A|(-1)^{e-1}(-p)^{\ell_{mc}(\mathcal{C})} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^{\ell_{mc}(\mathcal{C})+1}}, \tag{6.14}$$

where $\lambda!$ *is a unit in* $\mathbb{Z}_p$ *for each* $\lambda \in \Lambda_{mc}(\mathcal{C})$ *with* $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$. *Furthermore,*

$$\sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})}} \frac{\tilde{C}(\lambda)}{\lambda!}$$

assumes values in $\mathbb{Z}_p$, *and so* $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all* $c \in \mathcal{C}$. *There is some* $c \in \mathcal{C}$ *such that* $\mathrm{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$.

Proof. Throughout this proof, we have $d = 1$, since our Galois ring $\mathrm{GR}(p^d, e)$ is the field $\mathbb{F}_q$. We apply Proposition 6.11 with $m = \ell_{mc}(\mathcal{C}) + 1$ to obtain

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})}} \frac{(\mathrm{pr}_H\, \lambda)! f^{(\ell_{mc}(\mathcal{C})+1)}_{\mathrm{pr}_H\, \lambda}}{\lambda!}\ \tilde{C}(\lambda) \pmod{p^{\ell_{mc}(\mathcal{C})+1}}, \tag{6.15}$$

where $f^{(\ell_{mc}(\mathcal{C})+1)}(\mathbf{x})$ is the polynomial described in Proposition 6.10, and where we have used the fact that $\ell_{mc}(\mathcal{C})$ is the minimum tier of the elements in $\Lambda_{mc}(\mathcal{C})$ to rewrite the condition $\mathrm{Ti}\,(\lambda) < \ell_{mc}(\mathcal{C}) + 1$ in the sum as $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$.

Let us examine the coefficients of polynomial $f^{(\ell_{mc}(\mathcal{C})+1)}(\mathbf{x})$. The only ones that actually matter for our calculation are those of the form $f^{(\ell_{mc}(\mathcal{C})+1)}_{\mathrm{pr}_H\, \lambda}$ where $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$. By (6.13), the last condition is equivalent to $|\lambda| = (p-1)(\ell_{mc}(\mathcal{C}) + e)$. So we are interested in the coefficients $f^{(\ell_{mc}(\mathcal{C})+1)}_{\mu}$ with μ Delsarte-McEliece and $|\mu| = (p-1)(\ell_{mc}(\mathcal{C}) + e)$. For brevity we set $n = (p-1)(\ell_{mc}(\mathcal{C}) + e)$.

Since $d = 1$, Proposition 6.10 tells us that

$$f^{(\ell_{mc}(\mathcal{C})+1)}(\mathbf{x}) = \frac{p}{(p-1)q} G^{(1,\ell_{mc}(\mathcal{C})+1)}(\mathbf{x}) - \frac{q-p}{(p-1)q},$$

where

$$G^{(1,\ell_{mc}(\mathcal{C})+1)}(\mathbf{x}) = \mathfrak{T}_1 g^{(1,\ell_{mc}(\mathcal{C})+e)}(\mathbf{x}),$$

where, in turn, $g^{(1,\ell_{mc}(\mathcal{C})+e)}(x)$ is the polynomial described in Proposition 6.2. There we find that $g^{(1,\ell_{mc}(\mathcal{C})+e)}(x)$ has degree n, and if we write $g^{(1,\ell_{mc}(\mathcal{C})+e)}(x) = \sum_{j=0}^{n} g_j x^j$, then $n!g_n \equiv (-p)^{\ell_{mc}(\mathcal{C})+e-1} \pmod{p^{\ell_{mc}(\mathcal{C})+e}}$. Lemma 6.9 tells us that if $\mu \in \mathbb{N}[H]$ is Delsarte-McEliece with $|\mu| = n$, then the coefficient of $\mathbf{x}^\mu$ in $G^{(1,\ell_{mc}(\mathcal{C})+1)}(\mathbf{x})$ is $\frac{(q-1)n!g_n}{\mu!}$. Thus, for any Delsarte-McEliece multiset $\mu \in \mathbb{N}[H]$ with $|\mu| = n$, we have

$$f_\mu^{(\ell_{mc}(\mathcal{C})+1)} = \frac{p(q-1)}{(p-1)q} n!g_n \frac{1}{\mu!}.$$

Thus, returning to (6.15), we have

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A| \frac{p(q-1)}{(p-1)q} n!g_n \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^{\ell_{mc}(\mathcal{C})+1}}. \tag{6.16}$$

Recall that $n!g_n \equiv (-p)^{\ell_{mc}(\mathcal{C})+e-1} \pmod{p^{\ell_{mc}(\mathcal{C})+e}}$ and that $|A|$ is always assumed to be coprime to p. Thus we have

$$|A| \frac{p(q-1)}{(p-1)q} n!g_n \equiv |A| \frac{p(q-1)}{(p-1)q} (-p)^{\ell_{mc}(\mathcal{C})+e-1} \pmod{p^{\ell_{mc}(\mathcal{C})+1}},$$

so that

$$|A| \frac{p(q-1)}{(p-1)q} n!g_n \equiv |A|(-1)^{e-1}(-p)^{\ell_{mc}(\mathcal{C})} \pmod{p^{\ell_{mc}(\mathcal{C})+1}}. \tag{6.17}$$

We now use the notion of reduction introduced in Section 2.6. We claim that all $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$ are reduced. For if any $\lambda \in \Lambda_{mc}(\mathcal{C})$ were not reduced, then $\mathrm{Red}(\lambda) \in \Lambda_{mc}(\mathcal{C})$ by Lemma 2.25, and furthermore (by the same lemma), $|\mathrm{Red}(\lambda)| \leq |\lambda| - (p-1)$, so $\mathrm{Ti}\,(\mathrm{Red}(\lambda)) < \mathrm{Ti}\,(\lambda)$ by (6.13). Thus no $\lambda \in \Lambda_{mc}(\mathcal{C})$ of minimal tier can be non-reduced. This means that $\lambda!$ is a unit in $\mathbb{Z}_p$ for each $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$. Since scaled Fourier coefficients always lie in $\mathbb{Z}_p[\zeta_{q'-1}]$, this means that $\sum_{\lambda \in \Lambda_{mc}(\mathcal{C}), \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})} \frac{\tilde{C}(\lambda)}{\lambda!}$ is in $\mathbb{Z}_p[\zeta_{q'-1}]$, i.e., has nonnegative p-adic valuation. We use this fact and (6.17) in (6.16) to obtain

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv |A|(-1)^{e-1}(-p)^{\ell_{mc}(\mathcal{C})} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}) \\ \mathrm{Ti}(\lambda) = \ell_{mc}(\mathcal{C})}} \frac{\tilde{C}(\lambda)}{\lambda!} \pmod{p^{\ell_{mc}(\mathcal{C})+1}},$$

which is (6.14), which we were to show. Since $\sum_{\lambda\in\Lambda_{mc}(\mathcal{C}),\mathrm{Ti}(\lambda)=\ell_{mc}(\mathcal{C})} \frac{\tilde{C}(\lambda)}{\lambda!}$ has nonnegative valuation, we always have

$$\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}.$$

For the rest of the proof, we define Λ_ℓ to be the set of $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $\mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C})$. We shall show that $\sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\lambda)}{\lambda!}$ assumes values in $\mathbb{Z}_p$. Since it assumes values in $\mathbb{Z}_p[\zeta_{q'-1}]$, it suffices to show that it is fixed by Fr. We use the Frobenius action $\mathrm{Fr_A}$ introduced in Section 2.7. Lemma 2.31 tells us that $\mathrm{Fr_A}$ restricted to $\Lambda_{mc}(\mathcal{C})$ is a permutation of $\Lambda_{mc}(\mathcal{C})$. By the same lemma, $\mathrm{Fr_A}$ preserves the sizes of multisets, so it also preserves their tiers. Thus $\mathrm{Fr_A}$ restricts to a permutation of Λ_ℓ, and so

$$\sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\lambda)}{\lambda!} = \sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\mathrm{Fr_A}(\lambda))}{(\mathrm{Fr_A}(\lambda))!}.$$

By Lemma 2.31, we have

$$\begin{aligned}\sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\lambda)}{\lambda!} &= \sum_{\lambda\in\Lambda_\ell} \frac{\mathrm{Fr}(\tilde{C}(\lambda))}{\lambda!} \\ &= \mathrm{Fr}\left(\sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\lambda)}{\lambda!}\right).\end{aligned}$$

This shows that our sum is indeed an element of $\mathbb{Z}_p$.

Finally, we must show that there is some $c \in \mathcal{C}$ such that $\mathrm{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$. In view of (6.14), it suffices to show that

$$\sum_{\lambda\in\Lambda_\ell} \frac{\tilde{C}(\lambda)}{\lambda!} \not\equiv 0 \pmod{p}$$

for some $c \in \mathcal{C}$. We shall use the notion of collapse introduced in Section 2.6. Let R be a set of q-class representatives of A. Note that $\tilde{c}(a) \in \mathbb{F}_{q'}$ for all $a \in A$, so that $\tilde{c}(a)$ is always

zero or a power of $\pi(\zeta_{q'-1})$. Thus, by Lemma 2.20, we have

$$\sum_{\lambda\in\Lambda_\ell}\frac{\tilde{C}(\lambda)}{\lambda!}=\sum_{\lambda\in\Lambda_\ell}\frac{\tilde{C}(\mathrm{Co}_R(\lambda))}{\lambda!},$$

so it suffices to show that the right-hand side, i.e.,

$$\sum_{\lambda\Lambda_\ell}\frac{\tilde{C}(\mathrm{Co}_R(\lambda))}{\lambda!}, \tag{6.18}$$

does not vanish modulo p for some $c\in\mathcal{C}$. Note that the expression (6.18) is a $\mathbb{Q}_p$-linear combination of terms of the form

$$D_\lambda=\prod_{r\in R\cap S}\tilde{C}(r)^{(\mathrm{Co}_R(\lambda))_r}, \tag{6.19}$$

where we have restricted the product to $R\cap S$ in view of Lemma 2.19 and the fact that $\lambda\in\mathbb{N}[H\times S]$ for all $\lambda\in\Lambda_{mc}(\mathcal{C})$. Note that no two terms D_λ and $D_{\lambda'}$ with $\lambda,\lambda'\in\Lambda_\ell$ have exactly the same exponents for all the terms $\tilde{C}(r)$, since that would imply that $\mathrm{Co}_R(\lambda)=\mathrm{Co}_R(\lambda')$. This, in turn, would force $\lambda=\lambda'$, since λ and λ' are reduced (see Corollary 2.26). Also note that the exponent $(\mathrm{Co}_R(\lambda))_r$ of $\tilde{C}(r)$ in D_λ is less than q^{e_r} by the definition of Co_R. (Recall that e_r denotes the cardinality of the q-class of r in A.) As we vary c over all words in $\mathcal{C}$, Lemma 2.14 tells us that the values in $\{\tilde{C}(r):r\in R\cap S\}$ vary over $\prod_{r\in R\cap S}V_{0,r}$, where $V_{0,r}$ is the set containing 0 and all the powers of $\zeta_{q^{e_r}-1}$. Since no two elements of $V_{0,r}$ are equal to each other modulo p, and since $|V_{0,r}|=q^{e_r}$, which is strictly greater than the highest exponent of $\tilde{C}(r)$ appearing in any term (6.19) of (6.18), we may apply Lemma 2.33 to conclude that the minimum p-adic valuation achieved by (6.18) as c runs through $\mathcal{C}$ is precisely the minimum of the p-adic valuations of the coefficients $\frac{1}{\lambda!}$ for $\lambda\in\Lambda_\ell$. But we have already shown that each $\lambda!$ is a unit in $\mathbb{Z}_p$, so (6.18) does not vanish modulo p for some $c\in\mathcal{C}$. □

Now we show that if $e=1$, i.e., if $\mathrm{GR}(p^d,e)=\mathbb{Z}/p^d\mathbb{Z}$, we obtain a weakened version of Theorem 4.18. We set $e=1$ for the rest of this chapter. Thus we have $q=p$ and $H=\{0\}$. If $\lambda\in\mathbb{N}[H\times A]$, then $\Sigma\,\mathrm{pr}_H\,\lambda=|\lambda|=|\lambda_0|$, where these cardinalities are regarded as

elements of $\mathbb{Z}/(p-1)\mathbb{Z}$. Thus λ is Delsarte-McEliece if and only if $|\lambda_0| \equiv 0 \pmod{p-1}$. Since $H = \{0\}$, note that $\Pi\lambda = \Pi(\lambda_0)$ and $\mathrm{pr}_A \lambda = \lambda_0$. Thus our definition (6.9) of $\Lambda_{mc}(\mathcal{C})$ is equivalent to

$$\Lambda_{mc}(\mathcal{C}) = \{\lambda \in \mathbb{N}[\{0\} \times S] : \Pi(\lambda_0) = 1_A, \lambda_0 \notin \mathbb{N}[\{1_A\}], |\lambda_0| \equiv 0 \pmod{p-1}\}.$$

So the multisets in $\Lambda_{mc}(\mathcal{C})$ are in one-to-one correspondence with the multisets in

$$K_{mc}(\mathcal{C}) = \{\kappa \in \mathbb{N}[S] : \Pi\kappa = 1_A, \kappa \notin \mathbb{N}[\{1_A\}], |\kappa| \equiv 0 \pmod{p-1}\},$$

by the correspondence $\Phi\colon \Lambda_{mc}(\mathcal{C}) \to K_{mc}(\mathcal{C})$ that maps λ to λ_0. Note that $K_{mc}(\mathcal{C})$ is identical to the definition (4.30) of $\Lambda_{mc}(\mathcal{C})$ used in Chapter 4 (but, of course, different from the definition of $\Lambda_{mc}(\mathcal{C})$ used here). The correspondence Φ preserves the cardinality of multisets, so that $\min_{\lambda\in\Lambda_{mc}(\mathcal{C})} |\lambda| = \min_{\kappa\in K_{ms}(\mathcal{C})} |\kappa|$. Thus the parameter $\omega_{mc}(\mathcal{C})$, as defined in (6.11) of this chapter, is identical (in the case $e = 1$) to the parameter of the same name, as defined in (4.31) of Chapter 4. When we specialize our definition (6.10) of tier to the case $e = 1$, we obtain

$$\mathrm{Ti}(\lambda) = \max\left\{0, \left\lfloor \frac{|\lambda| - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}.$$

Note that this exactly matches the notion of tier used in Chapter 4 (see the discussion at the beginning of Section 4.3). When $e = 1$, our definition (6.12) of $\ell_{mc}(\mathcal{C})$ becomes

$$\ell_{mc}(\mathcal{C}) = \min_{\lambda\in\Lambda_{mc}(\mathcal{C})} \mathrm{Ti}(\lambda) = \max\left\{0, \left\lfloor \frac{\omega_{mc}(\mathcal{C}) - p^{d-1}}{(p-1)p^{d-1}} \right\rfloor\right\}.$$

Thus the parameter $\ell_{mc}(\mathcal{C})$, as defined here, is identical (in the case $e = 1$) to the parameter of the same name, as defined in (4.32) of Chapter 4.

Now we are in a position to compare the specialization of Theorem 6.12 (when $e = 1$) with previous results. Here is the specialization:

Corollary 6.14 (to Theorem 6.12, equivalent to Theorem 4.23). *Let $e = 1$ and let $\mathcal{C}$ be a code in $\mathbb{Z}/p^d\mathbb{Z}[A]$. Let $\ell_{mc}(\mathcal{C})$ be as defined in* (4.32) *(or, equivalently as in*

(6.12)*. Then* $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all* $c \in \mathcal{C}$*. Equivalently,* $\mathrm{ham}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all* $c \in \mathcal{C}$*.*

We note that this corollary of Theorem 6.12 is Theorem 4.23, which was shown to be a weakened version of Theorem 4.18 in Section 4.6. It is not surprising that we do not recover our best results for codes over $\mathbb{Z}/p^d\mathbb{Z}$ from Theorem 6.12, for it uses the parameter $\ell_{mc}(\mathcal{C})$, which is sensitive only to the support of the Fourier transform of the code, but not sensitive to the structure of the tower of supports of the Fourier transform.

Chapter 7

Simultaneous Zeroes in $\mathbb{F}_q[A]$

Let us recall that the Delsarte-McEliece theorem (Theorem 1.2) gives p-adic estimates of the zero counts of words in an ideal (code) $\mathcal{C}$ of $\mathbb{F}_q[A]$. The version we record here is more general than Theorem 1.2 of the Introduction; here we allow for the possibility that 1_A is in the support of the Fourier transform of our code.

Theorem 7.1 (Delsarte-McEliece [18]). *Let $\mathcal{C}$ be a code in $\mathbb{F}_q[A]$. Let $\ell_{mc}(\mathcal{C})$ be as defined in* (6.12). *Then* $\mathrm{zer}^{\mathrm{norm}}(c) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})}}$ *for all $c \in \mathcal{C}$, and there is some $c \in \mathcal{C}$ with* $\mathrm{zer}^{\mathrm{norm}}(c) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C})+1}}$.

Even this version is not as detailed as what Delsarte and McEliece actually proved; the full version is given as Theorem 6.13 in Section 6.5. In this chapter we shall prove a generalization (Theorem 7.14) of this theorem, which will p-adically estimate the simultaneous zero count of a finite collection of words $c_1, \ldots, c_t \in \mathbb{F}_q[A]$. (See Section 2.4 for a definition of the simultaneous zero count.) We recall the simplified version of Theorem 7.14 which was presented in the Introduction.

Theorem 7.2 (Theorem 7.14, simplified). *Let $t \geq 1$ and let $\mathcal{C}_1, \ldots, \mathcal{C}_t$ be codes in $\mathbb{F}_q[A]$ with 1_A not in the supports of their Fourier transforms. Then* $\mathrm{zer}(c_1, \ldots, c_t) \equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}}$ *for all $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. There are some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$ such that* $\mathrm{zer}(c_1, \ldots, c_t) \not\equiv |A| \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}}$.

In order to understand this theorem, one must recall the definition of $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, which was presented just before the statement of the theorem itself in Section 1.2. This parameter was defined there using unity-product sequences that consisted of elements in

the various supports of the Fourier transforms of the codes, along with the pth powers of such elements. In this chapter, we shall define $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ equivalently using multisets rather than sequences. In the special case where $t = 1$, we shall recover the multiset-based definition of $\ell_{mc}(\mathcal{C})$ given in (6.12) of Chapter 6. As always, the reader must be familiar with the definitions and notations for accounts in Section 2.5 to understand our presentation of such matters.

To prove our generalization of the Delsarte-McEliece theorem, we shall devise counting polynomials that will enable us to use Theorem 3.2 to p-adically approximate simultaneous zero counts. The first four sections (7.1–7.4) of this chapter will be dedicated to the construction of such polynomials. In Section 7.5, we shall employ them to prove Theorem 7.14 (the more precise version of Theorem 7.2 above). In the rest of the chapter, we show that the theorem of N. M. Katz (Theorem 1.12) is a consequence of Theorem 7.14. In Section 7.6, we discuss the theorems of Chevalley-Warning, Ax, and N. M. Katz. In Section 7.7, we discuss preliminary results that are used to obtain the theorem of N. M. Katz from Theorem 7.14. This includes a refined analysis of the result of Kasami, Lin, and Peterson, which states that punctured Reed-Muller codes are cyclic [28]. In Section 7.8, we prove the theorem of N. M. Katz and an associated statement on the sharpness of the theorem.

Before we proceed with our polynomial construction, we set some definitions and notations that will hold throughout the chapter. We fix $d = 1$, so that our Galois ring $\mathrm{GR}(p^d, e)$ is the finite field $\mathbb{F}_q$. We set t a positive integer and set $I = \{1, 2, \ldots, t\}$. The set I will index our collection of t codewords $c_1, \ldots, c_t \in \mathbb{F}_q[A]$. In the next four sections (7.1–7.4), we shall construct a counting polynomial in the te indeterminates in $\{x_{ih} \colon i \in I, h \in H\}$. This counting polynomial will be used with Theorem 3.2 to p-adically estimate simultaneous zero counts in $\mathbb{F}_q[A]$. For each $i \in I$, we use $\mathbf{x}_i$ to denote the list of indeterminates with first index equal to i, i.e.,

$$\mathbf{x}_i = x_{i,0}, x_{i,1}, \ldots, x_{i,e-1}.$$

Indeed, we adopt the convention (for the rest of the chapter) that if a is a letter, then the boldface letter $\mathbf{a}$ will always indicate the e-tuple $a_0, \ldots, a_{e-1}$. Note that e-tuples of integers can be identified with accounts on H: $\mu \in \mathbb{Z}[H]$ is identified with the e-tuple $\mu_0, \ldots, \mu_{e-1}$.

We use $\underline{\mathbf{x}}$ to denote our full list of indeterminates, i.e.,

$$\begin{aligned}\underline{\mathbf{x}} &= \mathbf{x}_1, \ldots, \mathbf{x}_t \\ &= x_{1,0}, x_{1,1}, \ldots, x_{1,e-1}, x_{2,0}, x_{2,1}, \ldots, x_{2,e-1}, \ldots, x_{t,0}, x_{t,1}, \ldots, x_{t,e-1}.\end{aligned}$$

We also adopt the convention that if a is any letter, then $\underline{\mathbf{a}}$ will always indicate the t-tuple of e-tuples

$$\mathbf{a}_1, \ldots, \mathbf{a}_t = a_{1,0}, a_{1,1}, \ldots, a_{1,e-1}, a_{2,0}, a_{2,1}, \ldots, a_{2,e-1}, \ldots, a_{t,0}, a_{t,1}, \ldots, a_{t,e-1}.$$

Note that t-tuples of e-tuples of integers can be identified with accounts on $I \times H$, i.e., if $\mu \in \mathbb{Z}[I \times H]$, then we identify each $\mu_i \in \mathbb{Z}[H]$ with an e-tuple, as already noted. Then μ is identified with the t-tuple of e-tuples $\mu_1, \ldots, \mu_t$. We adopt the convention that $\mathbf{a}^{\mathbf{b}} = \prod_{h \in H} a_h^{b_h}$ and $\underline{\mathbf{a}}^{\underline{\mathbf{b}}} = \prod_{(i,h) \in I \times H} a_{i,h}^{b_{i,h}}$.

We devise a function for measuring the size of Delsarte-McEliece multisets in $\mathbb{N}[H]$. Recall from Lemma 2.15 that all Delsarte-McEliece multisets have cardinality divisible by $p-1$, and that the nonempty ones have cardinality at least $e(p-1)$. We introduce the symbol ∞ and define $W \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ by

$$W(n) = \begin{cases} 0 & \text{if } n = 0, \\ \frac{n}{p-1} - e & \text{if } p-1 \mid n \text{ and } n \geq e(p-1), \\ \infty & \text{otherwise.} \end{cases} \tag{7.1}$$

In conjunction with calculations involving this function, we use the convention that ∞ plus anything is ∞, and that ∞ is greater than any integer. We extend the definition of W so that if $a_1, \ldots, a_t$ is a t-tuple of integers, then $W(a_1, \ldots, a_t) = W(a_1) + \cdots + W(a_t)$.

Since W is used to measure cardinalities of multisets, we make special notations to streamline its use in such cases. If $\mu \in \mathbb{Z}[H]$, then we define $L(\mu) = W(|\mu|)$. Note that Lemma 2.15 implies that $L(\mu) < \infty$ if μ is a Delsarte-McEliece multiset. If $\mu_1, \ldots, \mu_t$ is t-tuple of accounts in $\mathbb{Z}[H]$, then we define $L(\mu_1, \ldots, \mu_k) = L(\mu_1) + \cdots + L(\mu_k) =$

$W(|\mu_1|,\dots,|\mu_k|)$. An account $\nu \in \mathbb{Z}[I \times H]$ is considered to be the t-tuple $\nu_1,\dots,\nu_t$ of accounts in $\mathbb{Z}[H]$, so we have $L(\nu) = \sum_{i\in I} W(|\nu_i|)$.

We transplant the streamlined notations of the last paragraph to accounts in $\mathbb{Z}[H \times A]$. If $\lambda \in \mathbb{Z}[H\times A]$, we set $L(\lambda) = W(|\lambda|)$. If $\lambda_1,\dots,\lambda_t$ is a t-tuple of accounts in $\mathbb{Z}[H\times A]$, then we set $L(\lambda_1,\dots,\lambda_t) = W(|\lambda_1|)+\cdots+W(|\lambda_t|)$. An account $\kappa \in \mathbb{Z}[I\times H\times A]$ is considered to be the t-tuple $\kappa_1,\dots,\kappa_t$ of accounts in $\mathbb{Z}[H\times A]$, so we have $L(\kappa) = \sum_{i\in I} W(|\kappa_i|)$.

Throughout this chapter, we always use Tr (without indices) to mean Tr_1^e. Thus Tr denotes the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ and the trace from $\mathbb{Q}_p(\zeta_{q-1})$ to $\mathbb{Q}_p$, where context indicates which version is being used.

7.1 Averaged Polynomials

The goal of Sections 7.1–7.4 is the construction of a counting polynomial $f^{(m)}(\underline{\mathbf{x}}) \in \mathbb{Q}_p[\underline{\mathbf{x}}]$ that has the property that

$$f\left(\left\{x_{ih} = \mathrm{Fr}^h(a_i)\right\}\right) \equiv \begin{cases} 1 & \text{if } a_1 \equiv \cdots \equiv a_t \equiv 0 \pmod p, \\ 0 & \text{otherwise,} \end{cases}$$

for all $a_1,\dots,a_t \in \mathbb{Z}_p[\zeta_{q-1}]$. We essentially use the trace-averaging method of Chapter 6, although we do so in a somewhat more careful fashion to simplify our calculations later.

In our constructions, we use averaged versions of the binomial coefficient polynomials. We set

$$\left\{\begin{matrix} x \\ n \end{matrix}\right\} = \frac{1}{p-1}\sum_{i=0}^{p-2}\binom{\zeta_{p-1}^i x}{n}.$$

This polynomial maps $\mathbb{Z}_p$ into $\mathbb{Z}_p$ since $\binom{x}{n}$ maps $\mathbb{Z}_p$ into $\mathbb{Z}_p$. It is easy to see the effect that this form of averaging has on polynomials; we record it as a lemma without proof.

Lemma 7.3. *Let $f(x) = \sum_{i=0}^n f_i x^i \in \mathbb{Q}_p[x]$. Then*

$$\frac{1}{p-1}\sum_{j=0}^{p-2} f(\zeta_{p-1}^j x) = \sum_{\substack{0\le i\le n \\ p-1\mid i}} f_i x^i.$$

In particular, $\left\{ {x \atop n} \right\}$ *involves only monomials whose degrees are multiples of* $p-1$.

We introduce another form of averaged binomial coefficient polynomial. Set

$$\begin{bmatrix} \mathbf{y} \\ n \end{bmatrix} = \begin{bmatrix} y_0, \ldots, y_{e-1} \\ n \end{bmatrix} = \frac{1}{q-1} \sum_{i=0}^{q-2} \binom{\sum_{h \in H} \zeta_{q-1}^{ip^h} y_h}{n}. \tag{7.2}$$

Note that $\begin{bmatrix} \mathbf{y} \\ 0 \end{bmatrix} = 1$. The following lemma shows how $\begin{bmatrix} \mathbf{y} \\ n \end{bmatrix}$ can be used to map an element of $\mathbb{Z}_p[\zeta_{q-1}]$ into $\mathbb{Z}_p$.

Lemma 7.4. *For each* $a \in \mathbb{Z}_p[\zeta_{q-1}]$, $\begin{bmatrix} a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a) \\ n \end{bmatrix} = \frac{1}{q-1} \sum_{i=0}^{q-2} \binom{\mathrm{Tr}(\zeta_{q-1}^i a)}{n}$, *which is an element of* $\mathbb{Z}_p$.

Proof. For $a \in \mathbb{Z}_p[\zeta_{q-1}]$, we have

$$\begin{aligned} \begin{bmatrix} a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a) \\ n \end{bmatrix} &= \frac{1}{q-1} \sum_{i=0}^{q-2} \binom{\sum_{h \in H} \zeta_{q-1}^{ip^h} \mathrm{Fr}^h(a)}{n} \\ &= \frac{1}{q-1} \sum_{i=0}^{q-2} \binom{\sum_{h \in H} \mathrm{Fr}^h(\zeta_{q-1}^i a)}{n} \\ &= \frac{1}{q-1} \sum_{i=0}^{q-2} \binom{\mathrm{Tr}(\zeta_{q-1}^i a)}{n}. \end{aligned}$$

Since $\zeta_{q-1}^i a$ is in $\mathbb{Z}_p[\zeta_{q-1}]$, its trace is in $\mathbb{Z}_p$, and $\binom{x}{n}$ maps $\mathbb{Z}_p$ into $\mathbb{Z}_p$. □

Now we are ready to see how the form of averaging used in the definition (7.2) of $\begin{bmatrix} \mathbf{y} \\ n \end{bmatrix}$ affects polynomials.

Lemma 7.5. *Let* $f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbb{Q}_p[x]$. *Then*

$$\frac{1}{q-1} \sum_{j=0}^{q-2} f\left(\sum_{h \in H} \zeta_{q-1}^{jp^h} y_h \right) = \sum_{i=0}^{n} i! f_i \sum_{\substack{\mu \in \mathbb{N}[H], |\mu| = i \\ \Sigma \mu = 0}} \frac{\mathbf{y}^\mu}{\mu!}.$$

Proof. By linearity, we may assume that $f(x) = x^n$. Then

$$\frac{1}{q-1} \sum_{j=0}^{q-2} \left(\sum_{h \in H} \zeta_{q-1}^{jp^h} y_h \right)^n = \frac{1}{q-1} \sum_{j=0}^{q-2} \sum_{h_1, \ldots, h_n \in H} \prod_{i=1}^{n} (\zeta_{q-1}^{jp^{h_i}} y_{h_i}).$$

We recast the final sum as a sum over multisets rather than sequences to get

$$\frac{1}{q-1}\sum_{j=0}^{q-2}\left(\sum_{h\in H}\zeta_{q-1}^{jp^h}y_h\right)^n = \frac{1}{q-1}\sum_{j=0}^{q-2}\sum_{\substack{\mu\in\mathbb{N}[H]\\|\mu|=n}}\frac{n!}{\mu!}\prod_{h\in H}(\zeta_{q-1}^{jp^h}y_h)^{\mu_h},$$

where we recall that a multiset $\mu \in \mathbb{N}[H]$ of cardinality n can be arranged into $n!/\mu!$ distinct n-tuples of elements in H. Then, using our compact notation $\mathbf{y}^\mu$, we have

$$\begin{aligned}\frac{1}{q-1}\sum_{j=0}^{q-2}\left(\sum_{h\in H}\zeta_{q-1}^{jp^h}y_h\right)^n &= \frac{n!}{q-1}\sum_{j=0}^{q-2}\sum_{\substack{\mu\in\mathbb{N}[H]\\|\mu|=n}}\frac{\mathbf{y}^\mu}{\mu!}\prod_{h\in H}\zeta_{q-1}^{j\mu_h p^h}\\ &= n!\sum_{\substack{\mu\in\mathbb{N}[H]\\|\mu|=n}}\frac{\mathbf{y}^\mu}{\mu!}\left(\frac{1}{q-1}\right)\sum_{j=0}^{q-2}\zeta_{q-1}^{j\sum_{h\in H}\mu_h p^h}\\ &= n!\sum_{\substack{\mu\in\mathbb{N}[H],|\mu|=n\\ \Sigma\mu=0}}\frac{\mathbf{y}^\mu}{\mu!},\end{aligned}$$

where the last equality comes about since the sum over j will be $q-1$ or zero, respectively, depending on whether $\Sigma\mu = 0$ or not. □

This gives rise to the useful observation that $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}$ vanishes entirely for certain values of n.

Corollary 7.6. *For* $0 < n < e(p-1)$, $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix} = 0$.

Proof. Suppose that $0 < n < e(p-1)$. Then $f(x) = \binom{x}{n}$ is a polynomial of the form $f(x) = \sum_{i=1}^{n} f_i x^i$. So $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix} = 0$ follows from Lemma 7.5 and the fact (from Lemma 2.15) that there are no nonempty Delsarte-McEliece multisets of cardinality less than $e(p-1)$. □

Now we know enough about our averaged binomial coefficient polynomials to employ them in the construction of counting polynomials.

7.2 Polynomials on $\mathbb{Z}_p$

Our first step in the construction of the polynomial $f^{(m)}(\underline{\mathbf{x}})$ described at the beginning of Section 7.1 is to make a version of $f^{(m)}(\underline{\mathbf{x}})$ in the special case when $t = 1$ and $e = 1$. The

latter condition means that $q = p$, so that ζ_{q-1} is a root of unity of order $p-1$, and so $\mathbb{Z}_p[\zeta_{q-1}] = \mathbb{Z}_p$. So we seek a polynomial $f^{(m)}(y)$ that maps $p\mathbb{Z}_p$ into $1 + p^m\mathbb{Z}_p$, and maps the units of $\mathbb{Z}_p$ into $p^m\mathbb{Z}_p$. Fortunately, such a polynomial has already been found.

Proposition 7.7 (Wilson [66], [65]). *For any $m \geq 1$, there exists a polynomial*

$$f(x) = \sum_{i=0}^{m(p-1)} f_i \binom{x}{i},$$

with each $f_i \in \mathbb{Z}_p$, and with the property that

$$f(a) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a \equiv 0 \pmod{p}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases}$$

for all $a \in \mathbb{Z}_p$. Furthermore $v_p(f_i) \geq k$ whenever $i > k(p-1)$. In addition, $f_0 = 1$ and $f_{k(p-1)} \equiv (-p)^{k-1} \pmod{p^k}$ when $0 < k \leq m$.

Proof. A polynomial with all the desired properties is given by Corollary 4.13, specialized with $t = 1$. □

For the purposes of keeping our calculations simple, we shall want a counting polynomial whose form is slightly different from that of the polynomial we just obtained. We can construct a polynomial of the same degree, but with the added property that it has an expansion in terms of the functions $\left\{\binom{x}{(p-1)k}\right\}$. To do this, we shall employ the following result:

Lemma 7.8. *If $n \geq 0$, then*

$$\left\{\binom{x}{n}\right\} = \sum_{\substack{0 \leq k \leq n \\ p-1 \mid k}} c_k \left\{\binom{x}{k}\right\},$$

for some coefficients $c_k \in \mathbb{Z}_p$.

Proof. We proceed by induction on n, with the $n = 0$ case trivial. In fact, all cases where $p - 1 \mid n$ are trivial. So suppose that $n > 0$ and $p - 1 \nmid n$. As our induction hypothesis, we assume that if $m < n$, then $\left\{\binom{x}{m}\right\}$ is a $\mathbb{Z}_p$-linear combination of the polynomials $\left\{\binom{x}{(p-1)i}\right\}$ with $(p-1)i \leq m$.

By Lemma 7.3, $\left\{ {x \atop n} \right\}$ has degree strictly less than n. We can write $\left\{ {x \atop n} \right\}$ as a linear combination of the binomial coefficient polynomials

$$\left\{ {x \atop n} \right\} = \sum_{j=0}^{n-1} c_j \binom{x}{j}, \tag{7.3}$$

where $c_0 = \left\{ {0 \atop n} \right\}$ and $c_j = \left\{ {j \atop n} \right\} - \sum_{i=0}^{j-1} c_i \binom{j}{i}$ for $0 < j < n$. These c_j are elements of $\mathbb{Z}_p$, since $\left\{ {x \atop n} \right\}$ maps $\mathbb{Z}_p$ into $\mathbb{Z}_p$. We average both sides of (7.3) to obtain

$$\frac{1}{p-1} \sum_{k=0}^{p-2} \left\{ {\zeta_{p-1}^k x \atop n} \right\} = \sum_{j=0}^{n-1} c_j \left\{ {x \atop j} \right\}.$$

But Lemma 7.3 shows that $\left\{ {x \atop n} \right\}$ has only monomials whose degrees are divisible by $p-1$, so that by the same lemma, we have $\frac{1}{p-1} \sum_{k=0}^{p-2} \left\{ {\zeta_{p-1}^k x \atop n} \right\} = \left\{ {x \atop n} \right\}$. Thus

$$\left\{ {x \atop n} \right\} = \sum_{j=0}^{n-1} c_j \left\{ {x \atop j} \right\}.$$

Now the induction hypothesis shows that the terms $\left\{ {x \atop j} \right\}$ on the right-hand side are $\mathbb{Z}_p$-linear combinations of functions $\left\{ {x \atop k(p-1)} \right\}$ with $k(p-1) \le n-1$. □

Now we can obtain the polynomial we want.

Proposition 7.9. *For each $m \ge 1$, there exists a polynomial*

$$h(x) = \sum_{\substack{0 \le i \le m(p-1) \\ p-1 \mid i}} h_i \left\{ {x \atop i} \right\}$$

with each $h_i \in \mathbb{Z}_p$, $h_0 = 1$, $h_{j(p-1)} \equiv (-p)^{j-1} \pmod{p^j}$ for $0 < j \le m$, and with the property that

$$h(a) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a \equiv 0 \pmod{p}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases}$$

for all $a \in \mathbb{Z}_p$.

Proof. Let $f(x) = \sum_{i=0}^{m(p-1)} f_i \binom{x}{i}$ be the polynomial furnished by Proposition 7.7. If we set

$$\begin{aligned} g(x) &= \frac{1}{p-1} \sum_{j=0}^{p-2} f(\zeta_{p-1}^j x) \\ &= \sum_{i=0}^{m(p-1)} f_i \left\{ {x \atop i} \right\}, \end{aligned}$$

then since $v_p(\zeta_{p-1}) = 0$, we have $f(\zeta_{p-1}^j a) \equiv f(a) \pmod{p^m}$ for all $a \in \mathbb{Z}_p$ and $j \in \mathbb{N}$. Thus $g(a) \equiv f(a) \pmod{p^m}$ for all $a \in \mathbb{Z}_p$.

By Lemma 7.8, $g(x)$ can be written as

$$g(x) = \sum_{\substack{0 \le i \le m(p-1) \\ p-1 | i}} g_i \left\{ {x \atop i} \right\},$$

where $g_{i(p-1)}$ is of the form

$$g_{i(p-1)} = f_{i(p-1)} + \sum_{j=i(p-1)+1}^{m(p-1)} c_j f_j,$$

for some coefficients $c_j \in \mathbb{Z}_p$. Since $v_p(f_j) \ge i$ for $j > i(p-1)$, we have $g_{i(p-1)} \equiv f_{i(p-1)} \equiv (-p)^{i-1} \pmod{p^i}$ for $i > 0$. Note that $g_0 = g(0) \equiv f(0) \equiv 1 \pmod{p^m}$, so that if we set

$$h(x) = 1 + \sum_{\substack{0 < i \le m(p-1) \\ p-1 | i}} g_i \left\{ {x \atop i} \right\},$$

then $h(a) \equiv g(a) \equiv f(a) \pmod{p^m}$ for all $a \in \mathbb{Z}_p$. This $h(x)$ has all the properties we seek. □

7.3 Polynomials on $\mathbb{Z}_p[\zeta_{q-1}]$

In Proposition 7.9, we obtained a polynomial that approximates uniformly modulo p^m the characteristic function of the ideal $p\mathbb{Z}_p$ in the ring $\mathbb{Z}_p$. In this section, we want to generalize this to obtain a polynomial that approximates uniformly modulo p^m the characteristic function of the ideal $p\mathbb{Z}_p[\zeta_{q-1}]$ in the ring $\mathbb{Z}_p[\zeta_{q-1}]$. In terms of our goal for Sections 7.1–

7.4, i.e., the polynomial $f^{(m)}(\underline{\mathbf{x}}_1)$ described at the beginning of Section 7.1, this section provides the construction of $f^{(m)}$ in the special case when $t = 1$, just as the polynomial we found in Proposition 7.9 is the special case of $f^{(m)}$ when $t = 1$ and $e = 1$. This last polynomial will be the foundation of our construction here.

We shall begin to use the multivariable polynomials $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}$ in this section. Consider the averaging procedure that is used to obtain $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}$ from $\binom{x}{n}$. It is essential to the upcoming construction to note that if we apply this procedure to $\left\{{x \atop n}\right\}$, then we also obtain $\begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}$.

Lemma 7.10. *For any $n \geq 0$, we have*

$$\frac{1}{q-1}\sum_{k=0}^{q-2}\left\{{\sum_{h\in H}\zeta_{q-1}^{kp^h}y_h \atop n}\right\} = \begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}.$$

Proof. Since $p-1 \mid q-1$, $\zeta_{p-1} = \zeta_{q-1}^m$ for some integer m. Thus

$$\begin{aligned}
\frac{1}{q-1}\sum_{k=0}^{q-2}\left\{{\sum_{h\in H}\zeta_{q-1}^{p^hk}y_h \atop n}\right\} &= \frac{1}{q-1}\sum_{k=0}^{q-2}\frac{1}{p-1}\sum_{j=0}^{p-2}\binom{\zeta_{p-1}^j\sum_{h\in H}\zeta_{q-1}^{p^hk}y_h}{n}\\
&= \frac{1}{p-1}\sum_{j=0}^{p-2}\frac{1}{q-1}\sum_{k=0}^{q-2}\binom{\sum_{h\in H}\zeta_{p-1}^{j}\zeta_{q-1}^{p^hk}y_h}{n}\\
&= \frac{1}{p-1}\sum_{j=0}^{p-2}\frac{1}{q-1}\sum_{k=0}^{q-2}\binom{\sum_{h\in H}\zeta_{p-1}^{p^hj}\zeta_{q-1}^{p^hk}y_h}{n}\\
&= \frac{1}{p-1}\sum_{j=0}^{p-2}\frac{1}{q-1}\sum_{k=0}^{q-2}\binom{\sum_{h\in H}\zeta_{q-1}^{p^h(k+jm)}y_h}{n}\\
&= \frac{1}{p-1}\sum_{j=0}^{p-2}\frac{1}{q-1}\sum_{k=0}^{q-2}\binom{\sum_{h\in H}\zeta_{q-1}^{p^hk}y_h}{n}\\
&= \frac{1}{q-1}\sum_{k=0}^{q-2}\binom{\sum_{h\in H}\zeta_{q-1}^{p^hk}y_h}{n}\\
&= \begin{bmatrix}\mathbf{y}\\ n\end{bmatrix}.
\end{aligned}$$

□

Now we use this averaging method to construct the polynomial we want. The construction is a refined variation on the $d = 1$ case of Proposition 6.10. To understand this construction, given as the next proposition, the reader should recall the definition of the function W given in equation (7.1) above.

Proposition 7.11. *For each $m \geq 1$, there exists a polynomial*

$$h(\mathbf{y}) = \sum_{\substack{i \in \mathbb{N} \\ W(i) < m}} h_i \begin{bmatrix} \mathbf{y} \\ i \end{bmatrix},$$

with each $h_i \in \mathbb{Z}_p$, $h_0 = 1$, $h_i \equiv (-1)^{e-1}(-p)^{W(i)} \pmod{p^{W(i)+1}}$ for each $i > 0$, and with the property that

$$h(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a \equiv 0 \pmod{p}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases} \tag{7.4}$$

for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$.

Proof. Let $f(x)$ be the polynomial of Proposition 7.9 that has

$$f(a) \equiv \begin{cases} 1 \pmod{p^{m+e-1}} & \text{if } a \equiv 0 \pmod{p}, \\ 0 \pmod{p^{m+e-1}} & \text{otherwise,} \end{cases}$$

for all $a \in \mathbb{Z}_p$. Set $g(\mathbf{y}) = \sum_{j=0}^{q-2} f(\sum_{h \in H} \zeta_{q-1}^{p^h j} y_h)$. Then for each $a \in \mathbb{Z}_p[\zeta_{q-1}]$, we have $g(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) = \sum_{j=0}^{q-2} f(\mathrm{Tr}(\zeta_{q-1}^j a))$.

Note that Tr maps $\mathbb{Z}_p[\zeta_{q-1}]$ into $\mathbb{Z}_p$, and recall that Tr commutes with reduction modulo p. If $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a \equiv 0 \pmod{p}$, then $\zeta_{q-1}^j a \pmod{p}$ is 0 in $\mathbb{F}_q$ for all j, and so $\mathrm{Tr}(\zeta_{q-1}^j a) \pmod{p}$ is 0 in $\mathbb{F}_p$ for all j. Therefore $f(\mathrm{Tr}(\zeta_{q-1}^j a)) \equiv 1 \pmod{p^{m+e-1}}$ for all j, and so $g(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \equiv q - 1 \pmod{p^{m+e-1}}$ for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a \equiv 0 \pmod{p}$.

On the other hand, if $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a \not\equiv 0 \pmod{p}$, then $\zeta_{q-1}^j a \pmod{p}$ runs through the units of $\mathbb{F}_q$ as j runs from 0 to $q-2$. Since Tr is a $\mathbb{F}_p$-linear map from $\mathbb{F}_q$ onto $\mathbb{F}_p$, $\mathrm{Tr}(\zeta_{q-1}^j a) \pmod{p}$ runs through $\mathbb{F}_p$, taking each nonzero value precisely q/p times and taking the value zero precisely $(q/p) - 1$ times. Thus $g(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \equiv (q/p) - 1 \pmod{p^{m+e-1}}$ for all $a \in \mathbb{Z}_p[\zeta_{q-1}]$ with $a \not\equiv 0 \pmod{p}$.

Now we set $h(\mathbf{y}) = \frac{p}{(p-1)q} g(\mathbf{y}) - \frac{q-p}{(p-1)q}$, so that $h(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a))$ is the desired value modulo p^m for each $a \in \mathbb{Z}_p[\zeta_{q-1}]$ (as in (7.4)). It remains to show that $h(\mathbf{y})$ has the

desired form. Recall that the polynomial $f(x)$ supplied by Proposition 7.9 has the form

$$f(x) = \sum_{\substack{0 \le i \le (m+e-1)(p-1) \\ p-1 | i}} f_i \left\{ {x \atop i} \right\},$$

where each $f_i \in \mathbb{Z}_p$, $f_0 = 1$, and $f_{j(p-1)} \equiv (-p)^{j-1} \pmod{p^j}$ for $0 < j \le m+e-1$. Then

$$\begin{aligned} g(\mathbf{y}) &= \sum_{\substack{0 \le i \le (m+e-1)(p-1) \\ p-1 | i}} f_i \sum_{k=0}^{q-2} \left\{ {\sum_{h \in H} \zeta_{q-1}^{kp^h} y_h \atop i} \right\} \\ &= \sum_{\substack{0 \le i \le (m+e-1)(p-1) \\ p-1 | i}} f_i (q-1) \begin{bmatrix} \mathbf{y} \\ i \end{bmatrix}, \end{aligned}$$

where we have used Lemma 7.10 in the second equality. Now $f_0 = 1$, so that

$$h(\mathbf{y}) = \begin{bmatrix} \mathbf{y} \\ 0 \end{bmatrix} + \sum_{\substack{0 < i \le (m+e-1)(p-1) \\ p-1 | i}} f_i \frac{p(q-1)}{(p-1)q} \begin{bmatrix} \mathbf{y} \\ i \end{bmatrix}.$$

Corollary 7.6 above shows that $\begin{bmatrix} \mathbf{y} \\ i \end{bmatrix} = 0$ when $0 < i < e(p-1)$, so that

$$h(\mathbf{y}) = \begin{bmatrix} \mathbf{y} \\ 0 \end{bmatrix} + \sum_{\substack{e(p-1) \le i \le (m+e-1)(p-1) \\ p-1 | i}} f_i \frac{p(q-1)}{(p-1)q} \begin{bmatrix} \mathbf{y} \\ i \end{bmatrix}.$$

Then observe that the last sum indexes over all strictly positive integers i for which $W(i) < m$. Furthermore, for any such integer i, we have $f_i \equiv (-p)^{i/(p-1)-1} \pmod{p^{i/(p-1)}}$, so that

$$f_i \frac{p(q-1)}{(p-1)q} \equiv (-1)^{e-1} (-p)^{W(i)} \pmod{p^{W(i)+1}}. \qquad \square$$

7.4 Counting Polynomials

Now we are ready to construct the polynomial $f^{(m)}(\underline{\mathbf{x}})$ announced at the beginning of Section 7.1 as the goal of Sections 7.1–7.4. We shall use this polynomial to derive our generalization of the Delsarte-McEliece theorem. We build on the polynomial furnished by Proposition 7.11, which is the special case of $f^{(m)}$ when $t = 1$.

Proposition 7.12. *For any $m, t \geq 1$, there exists a polynomial $f^{(m)}(\underline{\mathbf{x}})$ with coefficients in $\mathbb{Q}_p$ and variables in $\{x_{ih} : i \in I, h \in H\}$ such that*

$$f^{(m)}\left(\left\{x_{ih} = \mathrm{Fr}^h(a_i)\right\}\right) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } a_1 \equiv \cdots \equiv a_t \equiv 0 \pmod{p}, \\ 0 \pmod{p^m} & \text{otherwise,} \end{cases} \tag{7.5}$$

for all $a_1, \ldots, a_t \in \mathbb{Z}_p[\zeta_{q-1}]$. Furthermore, $f^{(m)}(\underline{\mathbf{x}})$ is of the form

$$f^{(m)}(\underline{\mathbf{x}}) = \sum_{\substack{i_1,\ldots,i_t \in \mathbb{N} \\ W(i_1,\ldots,i_t) < m}} c^{(m)}_{i_1,\ldots,i_t} \prod_{j=1}^{t} \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}, \tag{7.6}$$

with each $c^{(m)}_{i_1,\ldots,i_t} \in \mathbb{Z}_p$, $c_{0,\ldots,0} = 1$, and

$$c^{(m)}_{i_1,\ldots,i_t} \equiv (-1)^{(e-1)\sum_{j=1}^{t}(1-\delta(i_j,0))}(-p)^{W(i_1,\ldots,i_t)} \pmod{p^{W(i_1,\ldots,i_t)+1}}. \tag{7.7}$$

We can also write

$$f^{(m)}(\underline{\mathbf{x}}) = \sum_{\substack{\mu \in \mathbb{N}[I \times H] \\ \Sigma\mu_1 = \cdots = \Sigma\mu_t = 0 \\ L(\mu_1,\ldots,\mu_t) < m}} f^{(m)}_{\mu} \underline{\mathbf{x}}^{\mu}, \tag{7.8}$$

where each $f^{(m)}_{\mu} \in \mathbb{Q}_p$.

Furthermore, if $\mu \in \mathbb{N}[I \times H]$ with $\Sigma\mu_1 = \cdots = \Sigma\mu_t = 0$ and $L(\mu_1, \ldots, \mu_t) = m - 1$, i.e., if μ is a t-tuple of Delsarte-McEliece multisets with $W(|\mu_1|) + \cdots + W(|\mu_t|) = m - 1$, then $f^{(m)}_{\mu} = \frac{c_{|\mu_1|,\ldots,|\mu_t|}}{\mu!}$, so that

$$\mu! f^{(m)}_{\mu} \equiv (-1)^{(e-1)\sum_{j=1}^{t}(1-\delta(|\mu_j|,0))}(-p)^{m-1} \pmod{p^m}. \tag{7.9}$$

Proof. Let

$$h(\mathbf{y}) = \sum_{\substack{i \in \mathbb{N} \\ W(i) < m}} h_i \begin{bmatrix} \mathbf{y} \\ i \end{bmatrix}$$

be the polynomial furnished by Proposition 7.11. Note that $h_0 = 1$ and $h_i \in \mathbb{Z}_p$ with $v_p(h_i) = W(i)$ for all i. Then set $g(\underline{\mathbf{x}}) = h(\mathbf{x}_1) \cdots h(\mathbf{x}_t)$. Note that $g(\underline{\mathbf{x}})$ takes the values

modulo p^m that we desire on $\mathbb{Z}_p[\zeta_{q-1}]^{te}$ (as in (7.5)), and it has the form

$$g(\underline{\mathbf{x}}) = \sum_{\substack{i_1,\ldots,i_t \in \mathbb{N} \\ W(i_1),\ldots,W(i_t)<m}} h_{i_1} \cdots h_{i_t} \prod_{j=1}^{t} \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix},$$

with each $h_{i_1} \cdots h_{i_t} \in \mathbb{Z}_p$, $h_0^t = 1$, and

$$h_{i_1} \cdots h_{i_t} \equiv (-1)^{(e-1)\sum_{j=1}^{t}(1-\delta(i_j,0))}(-p)^{W(i_1,\ldots,i_t)} \pmod{p^{W(i_1,\ldots,i_t)+1}}.$$

The only way in which $g(\underline{\mathbf{x}})$ might not comply with the conditions we seek in (7.6) is that it might contain some terms of the form

$$h_{i_1} \cdots h_{i_t} \prod_{j=1}^{t} \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}$$

for which $W(i_1) + \cdots + W(i_t) \geq m$. For these terms, $h_{i_1} \cdots h_{i_t}$ vanishes modulo p^m, and note that $\begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}$ maps each point $(a, \mathrm{Fr}(a), \ldots, \mathrm{Fr}^{e-1}(a)) \in \mathbb{Z}_p[\zeta_{q-1}]^e$ into $\mathbb{Z}_p$. So we may drop these terms without changing the value modulo p^m that the polynomial takes at relevant points in $\mathbb{Z}_p[\zeta_{q-1}]^{te}$. That is, set

$$f(\underline{\mathbf{x}}) = \sum_{\substack{i_1,\ldots,i_t \in \mathbb{N} \\ W(i_1)+\cdots+W(i_t)<m}} h_{i_1} \cdots h_{i_t} \prod_{j=1}^{t} \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}.$$

This shows that there is a polynomial of form (7.6) that satisfies (7.5).

To get the second expression for $f(\underline{\mathbf{x}})$, use Lemma 7.5 to write

$$\prod_{j=1}^{t} \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix} = \sum_{\substack{\mu_1,\ldots,\mu_t \in \mathbb{N}[H] \\ |\mu_1| \leq i_1,\ldots,|\mu_t| \leq i_t \\ \Sigma\mu_1 = \cdots = \Sigma\mu_t = 0}} \Gamma_{\mu_1,\ldots,\mu_t} \mathbf{x}_1^{\mu_1} \cdots \mathbf{x}_t^{\mu_t},$$

where each $\Gamma_{\mu_1,\ldots,\mu_t} \in \mathbb{Q}_p$. We do this for all such terms with $W(i_1,\ldots,i_t) < m$, since these are the ones appearing in (7.6). Note that since each μ_j in our expression is a Delsarte-McEliece multiset, we have $L(\mu_j) \neq \infty$. Since each $|\mu_j| \leq i_j$, we have $L(\mu_j) \leq W(i_j)$, and

so $L(\mu_1, \ldots, \mu_t) < m$. Therefore, whenever $i_1, \ldots, i_t \in \mathbb{N}$ with $W(i_1, \ldots, i_t) < m$, we have

$$\prod_{j=1}^{t} \begin{bmatrix} x_j \\ i_j \end{bmatrix} = \sum_{\substack{\mu \in \mathbb{N}[I \times H] \\ L(\mu_1, \ldots, \mu_t) < m \\ \Sigma\mu_1 = \cdots = \Sigma\mu_t = 0}} G_\mu x_1^{\mu_1} \cdots x_t^{\mu_t},$$

for some coefficients $G_\mu \in \mathbb{Q}_p$. We may substitute this into the first expression (7.6) for $f(\underline{\mathbf{x}})$ to obtain the second expression (7.8) for $f(\underline{\mathbf{x}})$.

Suppose we have a t-tuple $\mu = (\mu_1, \ldots, \mu_t)$ of Delsarte-McEliece multisets with $L(\mu_1, \ldots, \mu_t) = m - 1$. Then Lemma 7.5 shows that there is no $\underline{\mathbf{x}}^\mu = \mathbf{x}_1^{\mu_1} \cdots \mathbf{x}_t^{\mu_t}$ term in the polynomial $\prod_{j=1}^t \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}$ unless $i_j \geq |\mu_j|$ for all j, and unless $i_j = 0$ for all j such that $|\mu_j| = 0$. (For the second condition, note that $\binom{x}{n}$ has no constant term unless $n = 0$, so that $\begin{bmatrix} \mathbf{y} \\ n \end{bmatrix}$ has no constant term unless $n = 0$.) If $i_j \geq |\mu_j|$ for all j and $i_k > |\mu_k|$ for some particular k, then either we have $i_k > |\mu_k| = 0$, or we have $W(i_1, \ldots, i_t) > L(\mu_1, \ldots, \mu_t) = m - 1$. Thus, if we are considering $\prod_{j=1}^t \begin{bmatrix} \mathbf{x}_j \\ i_j \end{bmatrix}$ where $W(i_1, \ldots, i_t) < m$, then there is no $\underline{\mathbf{x}}^\mu = x_1^{\mu_1} \cdots x_t^{\mu_t}$ term unless $i_j = |\mu_j|$ for $j = 1, \ldots, t$. In this case, Lemma 7.5 tells us that the coefficient for the term $\underline{\mathbf{x}}^\mu = \mathbf{x}_1^{\mu_1} \cdots \mathbf{x}_t^{\mu_t}$ in $\prod_{j=1}^t \begin{bmatrix} x_j \\ |\mu_j| \end{bmatrix}$ is $\prod_{j=1}^t \frac{1}{\mu_j!} = \frac{1}{\mu!}$. So if we compare (7.6) with (7.8), we see that

$$\frac{c^{(m)}_{|\mu_1|, \ldots, |\mu_t|}}{\mu!} = f_\mu^{(m)}.$$

The congruence (7.9) for $\mu! f_\mu^{(m)}$ then follows from this and (7.7). □

With this polynomial, we are now ready to prove our generalization of the Delsarte-McEliece theorem.

7.5 Simultaneous Zero Count in $\mathbb{F}_q[A]$

For the remainder of this chapter, we suppose that we have a family of codes $\mathcal{C}_1, \ldots, \mathcal{C}_t \subseteq \mathbb{F}_q[A]$. For each $i \in I$, let S_i be the minimal support of the Fourier transform of $\mathcal{C}_i$. We suppose that not all the S_i are subsets of $\{1_A\}$, i.e., that at least one of the S_i contains an element of A that is not the identity. Otherwise we have a trivial situation: each $\mathcal{C}_i$ consists only of constant words and then $\operatorname{zer}(c_1, \ldots, c_t) = |A| \operatorname{zer}(\tilde{c_1}(1_A), \ldots, \tilde{c_t}(1_A))$ for all

$c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$.

Before we present our calculations, we define the parameter $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ first mentioned in Section 1.1 of the Introduction. There $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ was defined using sequences; here we define it (equivalently) using multisets. First we define

$$\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) = \{\lambda \in \mathbb{N}[I \times H \times A] : \mathrm{pr}_A(\lambda_1) \in \mathbb{N}[S_1], \ldots, \mathrm{pr}_A(\lambda_t) \in \mathbb{N}[\times S_t],$$
$$\Pi\lambda = 1_A, \mathrm{pr}_A \lambda \notin \mathbb{N}[\{1_A\}], \Sigma\,\mathrm{pr}_H(\lambda_1) = \cdots = \Sigma\,\mathrm{pr}_H(\lambda_t) = 0\}. \quad (7.10)$$

We claim that $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ is nonempty. By assumption we have some $k \in I$ such that there exists $a \in S_k$ with $a \neq 1_A$. Let n be the group-theoretic order of a. Consider the multiset λ that has $(q-1)n$ instances of the pair $(k, 0, a)$ and no other elements. Then λ is a unity-product but not all-unity multiset in $\mathbb{N}[I \times H \times A]$. Furthermore $\lambda_i \in \mathbb{N}[H \times S_i]$ and $\Sigma\,\mathrm{pr}_H(\lambda_i) = 0$ for all $i \in I$. So $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$. Since $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \neq \emptyset$, we may set

$$\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) = \min_{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)} L(\lambda). \quad (7.11)$$

Note that if $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, then λ_i is a Delsarte-McEliece multiset for each i, so $L(\lambda) = L(\lambda_1, \ldots, \lambda_t)$ is always finite and nonnegative by the comments following (7.1). At the end of this section, we shall show that when $t = 1$ the parameter $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, as defined here, is the same as $\ell_{mc}(\mathcal{C}_1)$, as defined in (6.12).

To p-adically estimate simultaneous zero counts in $\mathbb{F}_q[A]$, we combine Theorem 3.2 with Proposition 7.12.

Proposition 7.13. *Let $t, m \geq 1$, let $f^{(m)}(\underline{\mathbf{x}})$ be the polynomial described in Proposition 7.12, and write*

$$f^{(m)}(\underline{\mathbf{x}}) = \sum_{\substack{\mu \in \mathbb{N}[I \times H] \\ \Sigma\mu_1 = \cdots = \Sigma\mu_t = 0 \\ L(\mu) < m}} f_\mu^{(m)} \underline{\mathbf{x}}^\mu,$$

where each $f_\mu^{(m)} \in \mathbb{Q}_p$. For each $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$, let $C_1, \ldots, C_t$ be the elements of

$\mathbb{Z}_p[\zeta_{q'-1}][A]$ *such that* $\tilde{C}_i = \tau \circ \tilde{c}_i$ *for each* i. *Then for each* $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$, *we have*

$$\operatorname{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \\ L(\lambda) < m}} f^{(m)}_{\operatorname{pr}_{I\times H}\lambda} \frac{(\operatorname{pr}_{I\times H}\lambda)!}{\lambda!} \prod_{i=1}^{t} \tilde{C}_i(\lambda_i) \pmod{p^m},$$

where $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ *is as defined in* (7.10) *above.*

Proof. Note that if $f^{(m)}(\underline{\mathbf{x}})$ is the polynomial described in Proposition 7.12, and $a_1, \ldots, a_t \in \mathbb{Z}_p[\zeta_{q-1}]$, we have $f\left(\{x_{ih} = \mathrm{Fr}^h(a_i)\}\right) \equiv \operatorname{zer}(\pi(a_1), \ldots, \pi(a_t)) \pmod{p^m}$. Thus we may apply Theorem 3.2, to obtain

$$\operatorname{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\mu \in \mathbb{N}[I\times H]} \mu! f^{(m)}_{\mu} \sum_{\substack{\lambda \in \mathbb{N}[I\times H\times A], \operatorname{pr}_{I\times H}\lambda = \mu \\ \Pi\lambda = 1_A, \operatorname{pr}_A \lambda \notin \mathbb{N}[\{1_A\}] \\ \operatorname{pr}_A(\lambda_1) \in \mathbb{N}[S_1], \ldots, \operatorname{pr}_A(\lambda_t) \in \mathbb{N}[S_t]}} \frac{1}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \pmod{p^m}.$$

We can restrict the sum over μ to those μ with $L(\mu) < m$ and $\Sigma\mu_1 = \cdots = \Sigma\mu_t = 0$, since $f^{(m)}_{\mu} = 0$ otherwise (see Proposition 7.12). With this restriction on μ, the condition $\operatorname{pr}_{I\times H}\lambda = \mu$ implies that $\Sigma \operatorname{pr}_H(\lambda_i) = 0$ for all $i \in I$. Thus the inner sum on the right-hand side sums over those $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with $\operatorname{pr}_{I\times H}\lambda = \mu$. So

$$\begin{aligned}
\operatorname{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) &\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I\times H], L(\mu) < m \\ \Sigma\mu_1 = \cdots = \Sigma\mu_t = 0}} \mu! f^{(m)}_{\mu} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \\ \operatorname{pr}_{I\times H}\lambda = \mu}} \frac{1}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \pmod{p^m} \\
&\equiv |A| \sum_{\substack{\mu \in \mathbb{N}[I\times H] \\ L(\mu) < m}} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \\ \operatorname{pr}_{I\times H}\lambda = \mu}} f^{(m)}_{\operatorname{pr}_{I\times H}\lambda} \frac{(\operatorname{pr}_{I\times H}\lambda)!}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \pmod{p^m}.
\end{aligned}$$

The condition $\lambda = \operatorname{pr}_{I\times H}\mu$ also implies that the condition $L(\mu) < m$ in the first sum can be replaced with the condition $L(\lambda) < m$ in the second sum, and so

$$\begin{aligned}
\operatorname{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) &\equiv |A| \sum_{\mu \in \mathbb{N}[I\times H]} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \\ L(\lambda) < m, \operatorname{pr}_{I\times H}\lambda = \mu}} f^{(m)}_{\operatorname{pr}_{I\times H}\lambda} \frac{(\operatorname{pr}_{I\times H}\lambda)!}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \pmod{p^m} \\
&\equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t) \\ L(\lambda) < m}} f^{(m)}_{\operatorname{pr}_{I\times H}\lambda} \frac{(\operatorname{pr}_{I\times H}\lambda)!}{\lambda!} \prod_{i\in I} \tilde{C}_i(\lambda_i) \pmod{p^m}. \qquad \square
\end{aligned}$$

Now we can prove our generalization for simultaneous zero counts of the Delsarte-

McEliece theorem.

Theorem 7.14. *Let $t \geq 1$ and let $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ and $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ be as defined in* (7.10) *and* (7.11) *above. For each $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$, let $C_1, \ldots, C_t$ be the elements of $\mathbb{Z}_p[\zeta_{q'-1}][A]$ such that $\tilde{C}_i = \tau \circ \tilde{c}_i$ for each i. Then for each $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$, we have*

$$\mathrm{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)} \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t), \\ L(\lambda)=\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}} \Gamma_\lambda \prod_{i=1}^{t} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}}, \tag{7.12}$$

where

$$\Gamma_\lambda = \frac{|A|}{\lambda!}(-1)^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+(e-1)\sum_{i=1}^{t}(1-\delta(|\lambda_i|,0))}.$$

Γ_λ is a unit in $\mathbb{Z}_p$ for each $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ such that $L(\lambda) = \ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$. Furthermore,

$$\sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t), \\ L(\lambda)=\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}} \Gamma_\lambda \prod_{i=1}^{t} \tilde{C}_i(\lambda_i)$$

assumes values in $\mathbb{Z}_p$, and so $\mathrm{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}}$ for all words $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. There are some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$ such that $\mathrm{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}}$.

Proof. Throughout this proof we use ℓ_{mc} as an abbreviation for $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$. We apply Proposition 7.13 with $m = \ell_{mc} + 1$ to obtain

$$\mathrm{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \equiv |A| \sum_{\substack{\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t) \\ L(\lambda)=\ell_{mc}}} f^{(\ell_{mc}+1)}_{\mathrm{pr}_{I\times H}\,\lambda} \frac{(\mathrm{pr}_{I\times H}\,\lambda)!}{\lambda!} \prod_{i=1}^{t} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}+1}}, \tag{7.13}$$

where $f^{(\ell_{mc}(\mathcal{C})+1)}(\underline{\mathbf{x}})$ is the polynomial described in Proposition 7.12, and where we have rewritten the $L(\lambda) < \ell_{mc} + 1$ condition in the sum as $L(\lambda) = \ell_{mc}$, since ℓ_{mc} is defined to be the minimum value of $L(\lambda)$ for any $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$.

We investigate the coefficients of polynomial $f^{(\ell_{mc}+1)}(\underline{\mathbf{x}})$. The only ones that actually matter for our calculation are those of the form $f_{\mathrm{pr}_{I\times H}\,\lambda}$ for $\lambda \in \Lambda_{mc}(\mathcal{C})$ with $L(\lambda) = \ell_{mc}$. Since $L(\mathrm{pr}_{I\times H}\,\lambda) = L(\lambda)$ by the definition of L, this means that we need only consider $f^{(\ell_{mc}+1)}_{\mu}$ with $L(\mu) = \ell_{mc}$. Further, we can narrow our attention to those $f^{(\ell_{mc}+1)}_{\mu}$ with

all of $\mu_1, \ldots, \mu_t$ Delsarte-McEliece, since $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ implies that $(\mathrm{pr}_{I\times H}\,\lambda)_i$ is Delsarte-McEliece for all $i \in I$. Then Proposition 7.12 tells us that for all such μ, we have

$$\mu! f_\mu^{(m)} \equiv (-1)^{(e-1)\sum_{j=1}^t (1-\delta(|\mu_j|,0))}(-p)^{\ell_{mc}} \pmod{p^{\ell_{mc}+1}}.$$

So for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, we have

$$(\mathrm{pr}_{I\times H}\,\lambda)! f_{\mathrm{pr}_{I\times H}\,\lambda}^{(\ell_{mc}+1)} \equiv (-1)^{(e-1)\sum_{j=1}^t (1-\delta(|\lambda_j|,0))}(-p)^{\ell_{mc}} \pmod{p^{\ell_{mc}+1}}, \tag{7.14}$$

where we have noted that $\left|(\mathrm{pr}_{I\times H}\,\lambda)_j\right| = |\mathrm{pr}_H(\lambda_j)| = |\lambda_j|$.

We now use the notion of reduction introduced in Section 2.6. We claim that all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with $L(\lambda) = \ell_{mc}$ are reduced. To see this, let us suppose that $\kappa \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with κ not reduced. Then $\mathrm{Red}(\kappa) \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ by Lemma 2.28, and furthermore (by the same lemma) $|[\mathrm{Red}(\kappa)]_i| \leq |\kappa_i|$ for all $i \in I$, and $|[\mathrm{Red}(\kappa)]_j| \leq |\kappa_j| - (p-1)$ for some $j \in I$. This means that $\kappa_j \neq \emptyset$, and so by the same lemma, $\mathrm{Red}(\kappa_j) \neq \emptyset$, so that $L([\mathrm{Red}(\kappa)]_j) \leq L(\kappa_j) - 1$. Of course $L([\mathrm{Red}(\kappa)]_i) \leq L(\kappa_i)$ for all $i \in I$, so we have $L(\mathrm{Red}(\kappa)) \leq L(\kappa) - 1$. Since $\mathrm{Red}(\kappa) \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, this means that $L(\mathrm{Red}(\kappa)) \geq \ell_{mc}$, and so $L(\kappa) > \ell_{mc}$. This completes our proof that all elements λ in $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with $L(\lambda) = \ell_{mc}$ are reduced.

Since all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ with $L(\lambda) = \ell_{mc}$ are reduced, $\lambda!$ is a unit in $\mathbb{Z}_p$ for each such λ. In particular, recall our claim in the statement of the theorem that the terms

$$\Gamma_\lambda = \frac{|A|}{\lambda!}(-1)^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+(e-1)\sum_{i=1}^t (1-\delta(|\lambda_i|,0))}$$

are units in $\mathbb{Z}_p$ for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ such that $L(\lambda) = \ell_{mc}$. This is now clear. Also note that the scaled Fourier coefficients $\tilde{C}_i(a)$ always lie in $\mathbb{Z}_p[\zeta_{q'-1}]$, so that $\frac{1}{\lambda!}\prod_{i\in I}\tilde{C}_i(\lambda_i)$ is in $\mathbb{Z}_p[\zeta_{q'-1}]$, i.e., has nonnegative p-adic valuation, for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ such that $L(\lambda) = \ell_{mc}$. We use this fact, the congruence (7.14), and the definition of Γ_λ to deduce

from (7.13) that

$$\mathrm{zer}^{\mathrm{norm}}(c_1,\ldots,c_t) \equiv p^{\ell_{mc}} \sum_{\substack{\lambda\in\Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)\\ L(\lambda)=\ell_{mc}}} \Gamma_\lambda \prod_{i=1}^{t} \tilde{C}_i(\lambda_i) \pmod{p^{\ell_{mc}+1}}, \tag{7.15}$$

which is the first congruence (7.12) that we were to prove. Since the coefficients Γ_λ occurring in the sum on the right-hand side are units in $\mathbb{Z}_p$ and since the scaled Fourier coefficients are always in $\mathbb{Z}_p[\zeta_{q'-1}]$, the right-hand side vanishes modulo $p^{\ell_{mc}}$ to give

$$\mathrm{zer}^{\mathrm{norm}}(c_1,\ldots,c_t) \equiv 0 \pmod{p^{\ell_{mc}}}.$$

For the rest of the proof, we define Λ_ℓ to be the set of $\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$ with $L(\lambda) = \ell_{mc}$. We now show that $\sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \prod_{i\in I} \tilde{C}_i(\lambda_i)$ assumes values in $\mathbb{Z}_p$. Since it assumes values in $\mathbb{Z}_p[\zeta_{q'-1}]$, it suffices to show that it is fixed by Fr. We use the Frobenius action $\mathrm{Fr_A}$ introduced in Section 2.7. By Lemma 2.32, we note that $\mathrm{Fr_A}$ restricted to $\Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$ is a permutation of $\Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$. We also note that $|[\mathrm{Fr_A}(\lambda)]_i| = |\lambda_i|$ for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$ and $i \in I$, so that $L(\mathrm{Fr_A}(\lambda)) = L(\lambda)$ for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$. Thus $\mathrm{Fr_A}$ permutes the elements of Λ_ℓ, and so

$$\sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \prod_{i\in I} \tilde{C}_i(\lambda_i) = \sum_{\lambda\in\Lambda_\ell} \Gamma_{\mathrm{Fr_A}(\lambda)} \prod_{i\in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i).$$

From Lemma 2.32, we have learned that $|[\mathrm{Fr_A}(\lambda)]_i| = |\lambda_i|$ for all $i \in I$, and we also learn that $(\mathrm{Fr_A}(\lambda))! = \lambda!$. Thus, $\Gamma_{\mathrm{Fr_A}(\lambda)} = \Gamma_\lambda$ for all λ. Using this fact and invoking Lemma 2.32 again on the product $\prod_{i\in I} \tilde{C}_i([\mathrm{Fr_A}(\lambda)]_i)$, we have

$$\begin{aligned}\sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \prod_{i\in I} \tilde{C}_i(\lambda_i) &= \sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \,\mathrm{Fr}\left(\prod_{i\in I} \tilde{C}_i(\lambda_i)\right)\\ &= \mathrm{Fr}\left(\sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \prod_{i\in I} \tilde{C}_i(\lambda_i)\right),\end{aligned}$$

where we have used the fact that $\Gamma_\lambda \in \mathbb{Z}_p$ in the second equality. This finishes the proof that $\sum_{\lambda\in\Lambda_\ell} \Gamma_\lambda \prod_{i\in I} \tilde{C}_i(\lambda_i)$ is in $\mathbb{Z}_p$.

To finish the proof, we must show that there are some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$ such that $\mathrm{zer}^{\mathrm{norm}}(c_1, \ldots, c_t) \not\equiv 0 \pmod{p^{\ell_{mc}+1}}$. In view of (7.12), it suffices to show that

$$\sum_{\lambda \in \Lambda_\ell} \Gamma_\lambda \prod_{i \in I} \tilde{C}_i(\lambda_i) \not\equiv 0 \pmod{p}$$

for some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. To do this, we shall use the notion of collapse introduced in Section 2.6. Let R be a set of q-class representatives of A. Note that $\tilde{C}_i(a)$ is zero or a power of $\pi(\zeta_{q'-1})$ for each $i \in I$ and $a \in A$, since $\tilde{C}_i(a)$ is the Teichmüller lift of $\tilde{c}_i(a) \in \mathbb{F}_{q'}$. By Lemma 2.20, we have

$$\sum_{\lambda \in \Lambda_\ell} \Gamma_\lambda \prod_{i \in I} \tilde{C}_i(\lambda_i) = \sum_{\lambda \in \Lambda_\ell} \Gamma_\lambda \prod_{i \in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)),$$

so it suffices to show that the right-hand side, i.e.,

$$\sum_{\lambda \in \Lambda_\ell} \Gamma_\lambda \prod_{i \in I} \tilde{C}_i(\mathrm{Co}_R(\lambda_i)) \tag{7.16}$$

does not vanish modulo p for some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. Note that the expression (7.16) is a $\mathbb{Z}_p$-linear combination of terms of the form

$$D_\lambda = \prod_{i \in I} \prod_{r \in R \cap S_i} \tilde{C}_i(r)^{(\mathrm{Co}_R(\lambda_i))_r}, \tag{7.17}$$

where we have restricted the second product to $R \cap S_i$ in view of Lemma 2.19 and because $\lambda_i \in \mathbb{N}[H \times S_i]$ for all $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ and $i \in I$. Note that no two terms D_λ and $D_{\lambda'}$ with $\lambda, \lambda' \in \Lambda_\ell$ have exactly the same exponents for all the terms $\tilde{C}_i(r)$, since that would imply that $\mathrm{Co}_R(\lambda_i) = \mathrm{Co}_R(\lambda'_i)$ for all $i \in I$, which would force $\lambda = \lambda'$, since λ and λ' are reduced (see Corollary 2.26). Also note that the exponent $(\mathrm{Co}_R(\lambda_i))_r$ of $\tilde{C}_i(r)$ in D_λ is less than q^{e_r} by the definition of Co_R. (Recall that e_r denotes the cardinality of the q-class of r in A.) For each $i \in I$, as we vary c_i over $\mathcal{C}_i$, Lemma 2.14 tells us that the values in $\{\tilde{C}_i(r) : r \in R \cap S_i\}$ vary over $\prod_{r \in R \cap S_i} V_{0,r}$ where $V_{0,r}$ is the set containing 0 and all the powers of $\zeta_{q^{e_r}-1}$. So as we vary $c_1, \ldots, c_t$ over $\mathcal{C}_1 \times \cdots \times \mathcal{C}_t$, the values in

$\{\tilde{C}_i(r) : i \in I, r \in R \cap S_i\}$ vary over $\prod_{i \in I} \prod_{r \in R \cap S_i} V_{0,r}$. Since no two elements of $V_{0,r}$ are equal to each other modulo p, and since $|V_{0,r}| = q^{e_r}$, which is strictly greater than the highest exponent of $\tilde{C}_i(r)$ appearing in any term (7.17) of (7.16), we may apply Lemma 2.33 to conclude that the minimum p-adic valuation achieved by (7.16) as $c_1, \ldots, c_t$ runs through $\mathcal{C}_1 \times \cdots \times \mathcal{C}_t$ is precisely the minimum of the p-adic valuations of the coefficients Γ_λ for $\lambda \in \Lambda_\ell$. But we have already shown that each Γ_λ is a unit in $\mathbb{Z}_p$, so 7.16 does not vanish modulo p for some $c_1 \in \mathcal{C}_1, \ldots, c_t \in \mathcal{C}_t$. □

We can obtain the Delsarte-McEliece theorem (Theorem 7.1) by setting $t = 1$ in the theorem we have just proved. In fact, we recover the precise version of the Delsarte-McEliece theorem (Theorem 6.13) in full detail, as we now show. We suppose that $t = 1$ for the rest of this section, so that $I = \{1\}$.

Consider the size-preserving bijection $\Phi : \mathbb{Z}[I \times H \times A] \to \mathbb{Z}[H \times A]$ that takes λ to λ_1. Then Φ restricts to a bijection from $\Lambda_{mc}(\mathcal{C}_1)$, as defined in (7.10) here, to $\Lambda_{mc}(\mathcal{C}_1)$, as defined in (6.9) in Chapter 6.

Consider the notion of the tier of an account $\lambda \in \mathbb{N}[H \times A]$, denoted by $\mathrm{Ti}\,(\lambda)$ and defined in (6.10) in Chapter 6. In (6.13) of Section 6.5, we showed that $\mathrm{Ti}\,(\kappa) = \frac{|\kappa|}{(p-1)} - e$ if κ is a nonempty Delsarte-McEliece multiset in $\mathbb{N}[H \times A]$. (Of course $\mathrm{Ti}\,(\emptyset) = 0$ by the definition (6.10) of tier.) Therefore $L(\lambda) = L(\lambda_1) = \mathrm{Ti}\,(\lambda_1) = \mathrm{Ti}\,(\Phi(\lambda))$ for any λ in $\Lambda_{mc}(\mathcal{C}_1)$ (with $\Lambda_{mc}(\mathcal{C}_1)$ as defined in (7.11) here). Thus $\ell_{mc}(\mathcal{C}_1)$, as defined in (7.11) here, is equal to $\ell_{mc}(\mathcal{C}_1)$, as defined in (6.12) in Chapter 6.

Now we can use Φ to identify the range of summation $\{\lambda \in \Lambda_{mc}(\mathcal{C}_1) : L(\lambda) = \ell_{mc}(\mathcal{C}_1)\}$ in (7.12) of Theorem 7.14 with the range of summation $\{\lambda \in \Lambda_{mc}(\mathcal{C}_1) : \mathrm{Ti}\,(\lambda) = \ell_{mc}(\mathcal{C}_1)\}$ in (6.14) of Theorem 6.13. In Theorem 7.14, we have $\Gamma_\lambda = |A| \frac{(-1)^{\ell_{mc}(\mathcal{C}_1)+(e-1)}}{(\Phi(\lambda))!}$ for all λ in the sum in (7.12), since $\lambda \neq \emptyset$ implies $\lambda_1 \neq \emptyset$ and since $\lambda! = \lambda_1! = (\Phi(\lambda))!$. Thus, in view of our correspondence Φ, the coefficients in (7.12) of Theorem 7.14 match those in (6.14) of Theorem 6.13, and so we can recover the latter theorem from the former.

For the rest of this chapter, we shall apply Theorem 7.14 to the study of algebraic sets over finite fields. First we provide some historical background on such researches.

7.6 Theorems of Chevalley-Warning, Ax, and N. M. Katz

After proving Theorem 7.1, Delsarte and McEliece employed their result to prove a theorem of Ax on the cardinalities of algebraic sets over finite fields. If $f_1, \ldots, f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$, then we use $V(f_1, \ldots, f_t)$ to denote the subset of $\mathbb{F}_q^n$ consisting of the simultaneous zeroes of $f_1, \ldots, f_t$. Just as the Delsarte-McEliece theorem counts the zeroes of a word in an Abelian code, so the Ax theorem counts the zeroes of a polynomial.

Theorem 7.15 (Ax [2]). *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a nonconstant polynomial of degree $\mathfrak{d}$. Let ν be the least nonnegative integer greater than or equal to $(n - \mathfrak{d})/\mathfrak{d}$. Then $|V(f)|$ is divisible by q^ν.*

Ax's proof is based upon the Stickelberger theorem on Gauss sums. The Ax theorem is an improvement of the theorem of Warning [62], which shows that p divides $|V(f)|$ when the degree $\mathfrak{d}$ of f is less than the number n of variables. Warning's theorem generalizes and strengthens a theorem of Chevalley [15], which shows that if $n > \mathfrak{d}$ and f has no constant term, then f has a nontrivial zero.

Ax also proved that his theorem is sharp in the sense that when $n > \mathfrak{d}$, there exists a polynomial f of degree $\mathfrak{d}$ such that $|V(f)|$ is not divisible by $pq^{\lceil (n-\mathfrak{d})/\mathfrak{d} \rceil}$. Write $n = a\mathfrak{d} + b$ with $0 < b \leq \mathfrak{d}$, and set

$$g(x_1, \ldots, x_{a\mathfrak{d}}) = \begin{cases} 0 & \text{if } a = 0, \\ x_1 \ldots x_{\mathfrak{d}} + \cdots + x_{(a-1)\mathfrak{d}+1} \ldots x_{a\mathfrak{d}} & \text{otherwise.} \end{cases}$$

When $n > \mathfrak{d}$, i.e., when $a > 0$, Ax shows that

$$f(x_1, \ldots, x_n) = \begin{cases} g(x_1, \ldots, x_{a\mathfrak{d}}) & \text{if } b = 1, \\ g(x_1, \ldots, x_{a\mathfrak{d}}) + x_{a\mathfrak{d}+1} \ldots x_n & \text{otherwise,} \end{cases} \tag{7.18}$$

is a polynomial of degree $\mathfrak{d}$ with $|V(f)|$ not divisible by $pq^{\lceil (n-\mathfrak{d})/\mathfrak{d} \rceil}$. Of course, f is homo-

geneous if and only if $b = 1$ or $b = \mathfrak{d}$. Modifying this construction slightly, we set

$$h(x_1, \ldots, x_n) = \begin{cases} g(x_1, \ldots, x_{a\mathfrak{d}}) & \text{if } a > 0 \text{ and } b = 1, \\ g(x_1, \ldots, x_{a\mathfrak{d}}) + x_{a\mathfrak{d}+1} \ldots x_{n-1} x_n^{\mathfrak{d}-b+1} & \text{otherwise,} \end{cases}$$

which is always homogeneous of degree $\mathfrak{d}$. Note that $|V(h)|$ is clearly not divisible by p if $n \leq \mathfrak{d}$, i.e., if $a = 0$. If $n > \mathfrak{d}$, it is not hard to show that $|V(h)| = |V(f)|$, where f is as defined in (7.18). Thus we have the following statement of sharpness:

Proposition 7.16 (Homogeneous Sharpness of Ax's Theorem). *Let $n, \mathfrak{d} \geq 1$ and let ν be the least nonnegative integer greater than or equal to $(n - \mathfrak{d})/\mathfrak{d}$. Then there is a homogeneous polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $\mathfrak{d}$ such that $|V(f)|$ is not divisible by pq^ν.*

Delsarte and McEliece show that Theorem 7.15 is a consequence of their own theorem (Theorem 7.1) applied to the algebra $\mathbb{F}_q[A]$ where A is the cyclic group of units in the field $\mathbb{F}_{q^n}$. Their proof makes use of a correspondence between the elements of this algebra and polynomial functions on the punctured affine space $\mathbb{F}_q^n \setminus \{(0, \ldots, 0)\}$. In this correspondence, polynomials of low degree correspond to elements of the group algebra whose Fourier transforms have small supports (see Corollary 2 of [28] and Theorem 5.1 of [18]). We shall revisit this correspondence soon.

The papers of Chevalley [15] and Warning [62] also tell us about $V(f_1, \ldots, f_t)$ for a collection $f_1, \ldots, f_t$ of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$. In particular, Warning shows that if the sum of the degrees of the polynomials is less than the number n of variables, then p divides $|V(f_1, \ldots, f_t)|$. N. M. Katz generalized the theorem of Ax in the same direction to give a result for algebraic sets determined by collections of polynomials.

Theorem 7.17 (N. M. Katz [30]). *Let $f_1, \ldots f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$ be nonconstant polynomials of degrees $\mathfrak{d}_1 \leq \cdots \leq \mathfrak{d}_t$, respectively. Let ν be the least nonnegative integer greater than or equal to $\left(n - \sum_{i=1}^t \mathfrak{d}_i\right)/\mathfrak{d}_t$. Then $|V(f_1, \ldots, f_t)|$ is divisible by q^ν.*

N. M. Katz's proof is based on Dwork's p-adic theory of the zeta function [22], [45]. The paper of N. M. Katz also includes the following claim of sharpness for this result:

Proposition 7.18 (Homogeneous Sharpness of N. M. Katz's Theorem). *Let n and $\mathfrak{d}_1 \leq \cdots \leq \mathfrak{d}_t$ be positive integers, and let ν be the least nonnegative integer greater than or equal to $\left(n - \sum_{i=1}^{t} \mathfrak{d}_i\right)/\mathfrak{d}_t$. Then there are homogeneous polynomials $f_1, \ldots, f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degrees $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ such that $|V(f_1, \ldots, f_t)|$ is not divisible by pq^{ν}.*

When $n \leq \sum_{i=1}^{t} \mathfrak{d}_i$, N. M. Katz constructs homogeneous polynomials of the prescribed degrees such that $V(f_1, \ldots, f_t)$ is a single point. When $n > \sum_{i=1}^{t} \mathfrak{d}_i$, he uses the same construction to form homogeneous polynomials $f_1, \ldots, f_{t-1}$ of the prescribed degrees that involve the first $\mathfrak{d}_1 + \cdots + \mathfrak{d}_{t-1}$ indeterminates and that simultaneously vanish only when these variables are all zero. Then it suffices to find a homogeneous polynomial f_t of degree $\mathfrak{d}_t$ in $n' = n - \sum_{i=1}^{t-1} \mathfrak{d}_i$ indeterminates that vanishes on a subset B of $\mathbb{F}_q^{n'}$ with $|B|$ not divisible by pq^{ν}. Since $\nu = \left\lceil \left(n - \sum_{i=1}^{t} \mathfrak{d}_i\right)/\mathfrak{d}_t \right\rceil = \lceil (n' - \mathfrak{d}_t)/\mathfrak{d}_t \rceil$, this argument shows that to demonstrate Proposition 1.5, it suffices to prove the $t = 1$ case, which is precisely Proposition 7.16 proved here. In his paper, N. M. Katz incorrectly asserts ([30], page 498, lines 2–3) that the paper of Ax [2] contains Proposition 7.16, whereas we have seen that Ax's construction (shown in equation (7.18) above) is not always homogeneous. In any case, we have seen in the discussion preceding Proposition 7.16 that this deficiency is easily overcome.

It should be noted that improvements to Theorem 7.17 have been obtained in [1], [38], [39], and [40]. The researchers in last three papers were motivated by ideas in coding theory, in particular, the work of McEliece on p-divisibility of weights in cyclic codes.

Since the Ax theorem is a consequence of the Delsarte-McEliece theorem, it is natural to ask whether the theorem of N. M. Katz is the consequence of Theorem 7.14. We answer this question affirmatively in this rest of this chapter.

7.7 Polynomials and Group Algebras

To show that Theorem 7.14 implies the theorem of N. M. Katz, we make use of an $\mathbb{F}_q$-algebra epimorphism Ψ from $\mathbb{F}_q[x_1, \ldots, x_n]$ to the group algebra $(\mathbb{F}_q[A], \cdot)$, where A is the group of units of $\mathbb{F}_{q^n}$, and where one should note that multiplication in $\mathbb{F}_q[x_1, \ldots, x_n]$ is transformed to pointwise multiplication in $\mathbb{F}_q[A]$ rather than to the usual convolution

operation. For the rest of this chapter, we set n to be a positive integer and we set $A = \mathbb{F}_{q^n}^{\times}$, which is a cyclic group of order $q^n - 1$. It is important to note that henceforth we shall always consider $\mathbb{F}_q[A]$ with convolution and $(\mathbb{F}_q[A], \cdot)$ as one and the same $\mathbb{F}_q$-vector space, and we use the two different multiplication operations as the need arises. As per our convention, we always explicitly note when we are using pointwise multiplication, since it is not the standard multiplicative operation. For example, although Ψ is an $\mathbb{F}_q$-algebra homomorphism from $\mathbb{F}_q[x_1, \ldots, x_n]$ to $(\mathbb{F}_q[A], \cdot)$, we shall often consider the situation when a subset of $\mathbb{F}_q[x_1, \ldots, x_n]$ is mapped by Ψ to a convolution ideal (i.e., a code) in $\mathbb{F}_q[A]$. The epimorphism Ψ that we shall employ is the same one used by Delsarte and McEliece [18] to prove Ax's theorem (Theorem 7.15) from their own theorem (Theorem 7.1). We shall present Ψ below after some preliminary discussion on polynomial functions in affine space.

First note that all functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ are polynomial functions because the domain is finite. Let $\mathfrak{I}$ be the ideal in $\mathbb{F}_q[x_1, \ldots, x_n]$ generated by $x_1^q - x_1$, $\ldots$, $x_n^q - x_n$ and let $\mathfrak{I}'$ be the ideal generated by $\mathfrak{I}$ and $(x_1^{q-1} - 1) \cdots (x_n^{q-1} - 1)$. Notice that $\mathfrak{I}$ is the ideal of polynomials vanishing on $\mathbb{F}_q^n$. Thus any function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ can be uniquely represented as a polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ reduced modulo $\mathfrak{I}$, i.e., a polynomial in which any exponent of an indeterminate is less than q. Note also that $\mathfrak{I}'$ is the ideal of polynomials vanishing on the set $\mathbb{F}_{q^n} \setminus \{(0, \ldots, 0)\}$, which we call the *punctured affine space*. Thus any polynomial function on the punctured affine space is uniquely represented by a polynomial reduced modulo $\mathfrak{I}'$, i.e., a polynomial in which any exponent of an indeterminate is less than q and where the total degree is less than $n(q-1)$. We are concerned with polynomial functions on the punctured affine space because the epimorphism Ψ that we plan to use induces an isomorphism from $\mathbb{F}_q[x_1, \ldots, x_n]/\mathfrak{I}'$ to the algebra $(\mathbb{F}_q[A], \cdot)$.

We now show that we can restrict our attention to polynomials of degree less than n in the rest of this chapter. The conclusion of N. M. Katz's theorem (Theorem 7.17) is trivial if the sum of the degrees $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t$ is greater than or equal to the number n of variables, or equivalently, when the parameter ν defined there is zero. When $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t \geq n$, the statement regarding sharpness (Proposition 7.18) asserts that there are homogeneous polynomials $f_1, \ldots, f_t$ of degrees $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ such that $p \nmid |V(f_1, \ldots, f_t)|$. This

can be demonstrated by simple constructions. If $t \geq n$, then let each $f_i = x_{\min\{i,n\}}^{\mathfrak{d}_i}$, so that $V(f_1, \ldots, f_t) = \{(0, \ldots, 0)\}$. If $t < n$, then partition the set $\{x_1, \ldots, x_n\}$ into t nonempty sets $P_1, \ldots, P_t$ with $|P_i| \leq \mathfrak{d}_i$, and then let f_i be a monomial of total degree $\mathfrak{d}_i$ involving precisely those indeterminates in P_i. In this case,

$$\begin{aligned} |V(f_1, \ldots, f_t)| &= \prod_{i=1}^{t} \left(q^{|P_i|} - (q-1)^{|P_i|} \right) \\ &\equiv (-1)^{t+n} \pmod{p}. \end{aligned}$$

Thus we can confine our attention to the case when $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t < n$, so that all the polynomials have degrees less than n. The reductions modulo $\mathfrak{I}$ and modulo $\mathfrak{I}'$ of such polynomials are always identical to each other.

Now we describe the $\mathbb{F}_q$-algebra epimorphism Ψ from $\mathbb{F}_q[x_1, \ldots, x_n]$ to the group algebra $(\mathbb{F}_q[A], \cdot)$ (recall that $A = \mathbb{F}_{q^n}^{\times}$ in the rest of this chapter). We follow the presentation in the beginning of Section 5 of [18]. Fix an $\mathbb{F}_q$-basis $(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{F}_{q^n}$. Then set $\mathbb{F}_q^n \smallsetminus \{(0, \ldots, 0)\}$ in bijective correspondence with $\mathbb{F}_{q^n}^{\times}$ by the mapping $(u_1, \ldots, u_n) \mapsto u_1\alpha_1 + \cdots + u_n\alpha_n$. Each polynomial $f(x_1, \ldots, x_n)$ then corresponds to the function $\Psi(f)\colon \mathbb{F}_{q^n}^{\times} \to \mathbb{F}_q$ given by $\Psi(f)(u_1\alpha_1 + \cdots + u_n\alpha_n) = f(u_1, \ldots, u_n)$. Since $\Psi(f)$ is a function from A to $\mathbb{F}_q$, we may regard it as an element of the group algebra $\mathbb{F}_q[A]$, i.e., $\Psi(f)$ is regarded as the formal sum $\sum_{a \in A} c_a a$ with $c_a = \Psi(f)(a)$. Note that Ψ preserves $\mathbb{F}_q$-scalar multiplication and pointwise addition and multiplication of functions, so it is a homomorphism of $\mathbb{F}_q$-algebras from $\mathbb{F}_q[x_1, \ldots, x_n]$ to $(\mathbb{F}_q[A], \cdot)$. Since $\mathfrak{I}'$ is the ideal of polynomials that vanish on the punctured affine space, $\mathfrak{I}'$ is the kernel of Ψ. Furthermore, each function from $\mathbb{F}_q^n \smallsetminus \{(0, \ldots, 0)\}$ to $\mathbb{F}_q$ is representable by a unique polynomial reduced modulo $\mathfrak{I}'$, so each element of $\mathbb{F}_q[A]$ has a unique Ψ-preimage among such polynomials. So Ψ is an $\mathbb{F}_q$-algebra epimorphism and induces an $\mathbb{F}_q$-algebra isomorphism from $\mathbb{F}_q[x_1, \ldots, x_n]/\mathfrak{I}'$ to $(\mathbb{F}_q[A], \cdot)$. The definition of Ψ remains in force for the rest of this chapter.

Determining the set of simultaneous zeroes of a collection of polynomials is almost the same thing as determining the set of simultaneous zeroes of their images under Ψ. As $(u_1, \ldots, u_n)$ runs through $\mathbb{F}_q^n \smallsetminus \{(0, \ldots, 0)\}$, the quantity $u_1\alpha_1 + \cdots + u_n\alpha_n$ runs through

A. So we have the following observation:

Lemma 7.19. *Let* $f_1, \ldots, f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$. *Then*

$$|V(f_1, \ldots, f_t)| = \operatorname{zer}(\Psi(f_1), \ldots, \Psi(f_t)) + \prod_{i=1}^{t} \delta\left(f_i(0, \ldots, 0), 0\right).$$

The map Ψ is especially useful inasmuch as it maps low-degree polynomials to elements of $\mathbb{F}_q[A]$ whose Fourier transforms have small supports. The correspondence between the degree of f and the support of the Fourier transform of $\Psi(f)$ is given in Corollary 2 of [28] and is restated in terms closer to those of this thesis in Theorem 5.1 of [18]. Here we need to establish this correspondence in a way that is sensitive to whether or not our polynomials are homogeneous, so we shall present and prove a theorem (Theorem 7.21) that is a refinement of the result just mentioned.

Before we can prove Theorem 7.21, we need concrete expressions for the Fourier transform and Fourier inversion formula for our algebra $\mathbb{F}_q[A]$. Recall that $A = \mathbb{F}_{q^n}^{\times}$ is a cyclic group of order $q^n - 1$. Also recall that in Section 2.3 we defined e' to be the least integer such that $q^{e'} - 1$ is divisible by the exponent of A, and we set $q' = q^{e'}$. So plainly $e' = n$ here. Note that $\mathbb{F}_{q^n} = \mathbb{F}_{q'}$ is the quotient modulo p of $\mathbb{Z}_p[\zeta_{q'-1}]$. By convention, we have $\pi = \pi_d$, and since $d = 1$ in this chapter, we have $\pi = \pi_1$, that is, reduction modulo p. Since $\pi(\zeta_{q'-1})$ is a root of unity of order $q' - 1$ in $\mathbb{F}_{q'}$, we see that $A = \mathbb{F}_{q'}^{\times}$ is the cyclic group generated by $\pi(\zeta_{q'-1})$. We set $\gamma = \pi(\zeta_{q'-1})$ for convenience. The bilinear pairing introduced in Section 2.2 can then be taken as the function $\langle \gamma^i, \gamma^j \rangle = \zeta_{q'-1}^{ij}$. This is used to define the Fourier transform of functions in $\mathbb{Z}_p[\zeta_{q'-1}][A]$, which is given by

$$\hat{f}(\gamma^i) = \sum_{j=0}^{q^n-2} f(\gamma^j) \zeta_{q'-1}^{-ij},$$

with inversion formula

$$f(\gamma^i) = |A|^{-1} \sum_{j=0}^{q^n-2} \hat{f}(\gamma^j) \zeta_{q'-1}^{ij}.$$

This, in turn, induces the Fourier transform for functions $f \in \mathbb{F}_{q'}[A]$, which is given by

$$\hat{f}(\gamma^i) = \sum_{j=0}^{q^n-2} f(\gamma^j)\gamma^{-ij},$$

and the inversion formula is

$$f(\gamma^i) = |A|^{-1} \sum_{j=0}^{q^n-2} \hat{f}(\gamma^j)\gamma^{ij}. \tag{7.19}$$

We shall use this formula in our proof of Theorem 7.21 below.

To describe the correspondence between the degree of f and the support of the Fourier transform of $\Psi(f)$, we introduce the concept of the *q-ary weight* of a nonnegative integer, following [28] and [18]. If $k \in \mathbb{N}$, write the q-ary expansion $k = \sum_{i=0}^{\infty} k_i q^i$, where $0 \leq k_i < q$ for each i. Then the q-ary weight of k, denoted $w_q(k)$, is $\sum_{i=0}^{\infty} k_i$. We extend the notion of q-ary weight to elements of $\mathbb{F}_{q^n}^{\times}$; for any element $\beta \in \mathbb{F}_{q^n}^{\times}$, we choose the unique integer k with $0 \leq k < q^n - 1$ such that $\beta = \gamma^k$. Then the q-ary weight of β, denoted $w_q(\beta)$, is the q-ary weight of the integer k. Note that $w_q(\gamma) = 1$, except in the case when $q = 2$ and $n = 1$, wherein $w_q(\gamma) = 0$. We pause to state some other facts about the q-ary weight that we shall find useful later.

Lemma 7.20. *Let $m \geq 1$, let $j, k, j_1, \ldots, j_m$ be nonnegative integers, and let a, a_1, $\ldots$, $a_m \in A$. Then we have the following:*

(i) $w_q(j) \leq j$.

(ii) *If $0 \leq j < q^n - 1$ and $j \equiv k \pmod{q^n - 1}$, then $w_q(j) \leq w_q(k)$.*

(iii) $w_q(j) \equiv j \pmod{q-1}$.

(iv) $w_q(a^q) = w_q(a)$.

(v) $w_q(\gamma^{q^j}) = 1$ *unless* $n = 1$ *and* $q = 2$.

(vi) $\sum_{s=0}^{e-1} w_q(p^{j+s}) = (q-1)/(p-1)$.

(vii) $w_q\left(\sum_{i=1}^{m} j_i\right) \leq \sum_{i=1}^{m} w_q(j_i)$.

(viii) $w_q\left(\prod_{i=1}^m a_i\right) \leq \sum_{i=1}^m w_q(a_i)$.

(ix) $w_q\left(\sum_{i=1}^m j_i\right) \equiv \sum_{i=1}^m w_q(j_i) \pmod{q-1}$.

(x) $w_q\left(\prod_{i=1}^m a_i\right) \equiv \sum_{i=1}^m w_q(a_i) \pmod{q-1}$.

(xi) *If* $0 < \sum_{i=1}^m w_q(j_i) < n(q-1)$, *then* $\sum_{i=1}^m j_i \not\equiv 0 \pmod{q^n-1}$.

(xii) *If* $0 < \sum_{i=1}^m w_q(a_i) < n(q-1)$, *then* $\prod_{i=1}^m a_i \neq 1_A$.

(xiii) *If* $0 < m < n(q-1)$, $w_q(a_1) = \cdots = w_q(a_m) = 1$, *and* $a = \prod_{i=1}^m a_i$, *then* $0 < w_q(a) \leq m$ *and* $w_q(a) \equiv w_q(m) \pmod{q-1}$.

(xiv) $w_q\left(\prod_{i=1}^m j_i\right) \leq \prod_{i=1}^m w_q(j_i)$.

Proof. These are all routine; we refer the reader to [18] for more details. The inequality (i) is clear. Lemma 3.6 of [18] contains (ii). Congruence (iii) follows immediately from the definition of w_q. The equality (iv) follows from the fact that

$$\left(\gamma^{i_0+i_1q+\cdots+i_{n-1}q^{n-1}}\right)^q = \gamma^{i_{n-1}+i_0q+i_1q^2+\cdots+i_{n-2}q^{n-1}}.$$

Then (v) follows from (iv) and the fact that $w_q(\gamma) = 1$ unless $n = 1$ and $q = 2$. A routine calculation gives (vi). Lemma 3.7 of [18] contains (vii), and (viii) follows from this and (ii). The congruences (ix) and (x) follow easily from (iii). Lemma 3.6 of [18] states that if $j > 0$ and $j \equiv 0 \pmod{q^n-1}$, then $w_q(j) \geq n(q-1)$. This fact, along with (vii), proves (xi). Then (xii) follows from (xi). Claim (xiii) follows from (xii), (viii), (x), and (iii). Lemma 3.7 of [18] contains (xiv). □

With this notion of q-ary weight, we can relate the degree of the polynomial f to the support of the Fourier transform of $\Psi(f)$. We do so in the following theorem, which is a refined version of Corollary 2 in [28] and Theorem 5.1 in [18]:

Theorem 7.21. *Let* $\mathfrak{d}$ *be an integer with* $0 \leq \mathfrak{d} < n(q-1)$. *Then* Ψ *maps the* $\mathbb{F}_q$*-vector space of polynomials in* $\mathbb{F}_q[x_1, \ldots, x_n]$ *of degree less than or equal to* $\mathfrak{d}$ *onto the* $\mathbb{F}_q$*-vector space of functions in* $\mathbb{F}_q[A]$ *whose Fourier transforms are supported on the* q*-closed subset*

$\Upsilon_{\mathfrak{d}} = \{a \in A : w_q(a) \leq \mathfrak{d}\}$. *Furthermore, if* $\mathfrak{d} > 0$, *then* Ψ *maps the* $\mathbb{F}_q$*-vector space of polynomials in* $\mathbb{F}_q[x_1, \ldots, x_n]$ *that are homogeneous of degree* $\mathfrak{d}$ *onto the* $\mathbb{F}_q$*-vector space of functions in* $\mathbb{F}_q[A]$ *whose Fourier transforms are supported on the* q*-closed subset* $\Omega_{\mathfrak{d}} = \{a \in A : 0 < w_q(a) \leq \mathfrak{d}, w_q(a) \equiv w_q(\mathfrak{d}) \pmod{q-1}\}$.

Proof. That $\Upsilon_{\mathfrak{d}}$ and $\Omega_{\mathfrak{d}}$ as defined above are q-closed comes from the fact that $w_q(a^q) = w_q(a)$ for any $a \in A$ by Lemma 7.20(iv). Ψ maps the set of constant polynomials onto the set of constant functions in $\mathbb{F}_q[A]$; these are precisely the functions whose Fourier transforms are supported on $\{1_A\} = \Upsilon_0$. This special case of the first claim, together with the second claim regarding homogeneous polynomials, implies the first claim in its entirety. So we shall prove the second claim.

We fix $\mathfrak{d}$ with $0 < \mathfrak{d} < n(q-1)$ for the rest of the proof. Note that these bounds on $\mathfrak{d}$ allow us to exclude case when $q = 2$ and $n = 1$, which is pathological.

First we show that Ψ maps the homogeneous polynomials of degree $\mathfrak{d}$ to functions whose Fourier transforms are supported on $\Omega_{\mathfrak{d}}$. To do this, it suffices to consider monomials of degree $\mathfrak{d}$. Recall that $\alpha_1, \ldots, \alpha_n$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a nonzero homogeneous polynomial of degree one, i.e., a nonzero linear polynomial with no constant coefficient. Then consider the function $\varphi\colon \mathbb{F}_{q^n} \to \mathbb{F}_q$ given by $\varphi(u_1\alpha_1 + \cdots + u_n\alpha_n) = f(u_1, \ldots, u_n)$, where $u_1, \ldots, u_n$ range over $\mathbb{F}_q$. Comparing the definition of φ with the definition of $\Psi(f)$, we see that $\Psi(f)$ is just the restriction of φ to $\mathbb{F}_{q^n}^{\times}$. This function φ is a nontrivial $\mathbb{F}_q$-linear functional on $\mathbb{F}_{q^n}$, hence is of the form $\varphi(u) = \mathrm{Tr}_e^{ne}(\beta u)$ for some $\beta \in \mathbb{F}_{q^n}^{\times}$. In particular, consider polynomials of the form $f(x_1, \ldots, x_n) = x_i$ for $i \in \{1, \ldots, n\}$. Set $\xi_i = \Psi(x_i)$ for each i. Then there is some $\beta_i \in \mathbb{F}_{q^n}^{\times}$ such that $\xi_i(u) = \mathrm{Tr}_e^{ne}(\beta_i u)$ for all $u \in \mathbb{F}_{q^n}^{\times}$. One can use (7.19) and the bijectivity of the Fourier transform to check that $\hat{\xi}_i$ is the function in $(\mathbb{F}_{q^n})^A$ that has $\hat{\xi}_i(\gamma^{q^j}) = |A|\beta_i^{q^j}$ for all j and $\hat{\xi}_i(a) = 0$ for $a \notin \{\gamma^{q^j} : 0 \leq j < n\}$. So by Lemma 7.20(v), $\hat{\xi}_i$ is supported on Ω_1. (Recall that we have excluded the case when $q = 2$ and $n = 1$.)

We wish to show that an arbitrary monomial $f(x_1, \ldots, x_n) = x_1^{\mathfrak{d}_1} \cdots x_n^{\mathfrak{d}_n}$ with $\mathfrak{d}_1 + \cdots + \mathfrak{d}_n = \mathfrak{d}$ has the Fourier transform of $\Psi(f)$ supported on $\Omega_{\mathfrak{d}}$. To do this, we use nonstandard multiplications in our algebras, i.e., we use pointwise multiplication in $\mathbb{F}_q[A]$ and convolution

in $\mathbb{F}_q^A$. We adopt the notation that $\varepsilon^{\bullet k}$ is the pointwise product of k copies of $\varepsilon \in \mathbb{F}_{q'}[A]$ and η^{*k} is the convolution product of k copies of $\eta \in (\mathbb{F}_{q'})^A$. Since Ψ is an $\mathbb{F}_q$-algebra homomorphism from $\mathbb{F}_q[x_1, \ldots, x_n]$ into $(\mathbb{F}_q[A], \cdot)$, we have $\Psi(f) = \xi_1^{\bullet \mathfrak{d}_1} \cdot \xi_2^{\bullet \mathfrak{d}_2} \cdot \ldots \cdot \xi_n^{\bullet \mathfrak{d}_n}$. Recall from Proposition 2.6 that if $g_1 \cdot g_2 = h$, then $\hat{h} = |A|^{-1} \hat{g_1} * \hat{g_2}$. So the Fourier transform of $\Psi(f)$ is $|A|^{1-\mathfrak{d}} \hat{\xi}_1^{*\mathfrak{d}_1} * \cdots * \hat{\xi}_n^{*\mathfrak{d}_n}$. We want to show that this is supported on $\Omega_{\mathfrak{d}}$. In the previous paragraph, we observed that each $\hat{\xi}_i$ is supported on Ω_1. If $Y, Z \subseteq A$, we define the convolution of Y and Z, denoted $Y * Z$, to be $\{y * z : y \in Y, z \in Z\}$, and we define Y^{*k} to be the convolution product of k copies of Y. Then the Fourier transform of $\Psi(f)$ is supported on $\Omega_1^{*\mathfrak{d}}$, so it suffices to show that $\Omega_1^{*\mathfrak{d}} \subseteq \Omega_{\mathfrak{d}}$. Each element of Ω_1 has unit q-ary weight. Thus each element in $\Omega_1^{*\mathfrak{d}}$ is a product of $\mathfrak{d}$ elements of unit q-ary weight. Since $0 < \mathfrak{d} < n(q-1)$, Lemma 7.20(xiii) shows that each $a \in \Omega_1^{*\mathfrak{d}}$ has $0 < w_q(a) \leq \mathfrak{d}$ and $w_q(a) \equiv w_q(\mathfrak{d}) \pmod{q-1}$, i.e., that $a \in \Omega_{\mathfrak{d}}$. So $\Omega_1^{*\mathfrak{d}} \subseteq \Omega_{\mathfrak{d}}$, and therefore Ψ maps homogeneous polynomials of degree $\mathfrak{d}$ into the set of functions whose Fourier transforms are supported on $\Omega_{\mathfrak{d}}$.

Now it remains to show that Ψ maps the set P of homogeneous polynomials of degree $\mathfrak{d}$ *onto* the set R of functions whose Fourier transforms are supported on $\Omega_{\mathfrak{d}}$. We just showed that $\Psi(P) \subseteq R$; now we want to show that $\Psi(P) = R$. Since the sets involved are finite, it will suffice to show that $|\Psi(P)| \geq |R|$. Recall that the ideal $\mathfrak{I}'$, defined at the beginning of this section, is the kernel of Ψ. If we let Q be the set of reductions modulo $\mathfrak{I}'$ of elements in P, then $\Psi(Q) = \Psi(P)$ and Ψ is injective when restricted to Q. So it will suffice to show that $|Q| \geq |R|$. Recall that the set $\Omega_{\mathfrak{d}}$ is q-closed, so Lemma 2.13 tells us that $|R| = q^{|\Omega_{\mathfrak{d}}|}$.

So we need to show that $|Q| \geq q^{|\Omega_{\mathfrak{d}}|}$. Since the polynomials in P are of degree less than $n(q-1)$, their reductions modulo $\mathfrak{I}$ and reductions modulo $\mathfrak{I}'$ are the same. The set Q of reductions modulo $\mathfrak{I}$ of the elements in P is the $\mathbb{F}_q$-vector space whose basis is the set M of monomials of the form $x_1^{e_1} \ldots x_n^{e_n}$ where $0 \leq e_i < q$, $0 < e_1 + \cdots + e_n \leq \mathfrak{d}$, and $e_1 + \cdots + e_n \equiv \mathfrak{d} \pmod{q-1}$. Q contains M because any nonconstant monomial of degree u can be replaced with an equivalent monomial modulo $\mathfrak{I}$ of degree $u + (q-1)$ by replacing an indeterminate x_i with x_i^q. That M spans Q follows from the fact that any monomial of degree $\mathfrak{d}$ reduces modulo $\mathfrak{I}$ to a nonconstant monomial of degree $\mathfrak{d} - k(q-1)$ for some

$k \geq 0$.

Thus $Q = q^{|M|}$, and so we need to show that $|M| \geq |\Omega_{\mathfrak{d}}|$. We shall devise an injection θ from $\Omega_{\mathfrak{d}}$ into M. For any $\beta \in \Omega_{\mathfrak{d}}$, write $\beta = \gamma^{e_1+e_2q+\cdots+e_nq^{n-1}}$ with $0 \leq e_i < q$ for all i and $e_1 + \cdots + e_n < n(q-1)$. These e_i are uniquely determined by β. Then set $\theta(\beta) = x_1^{e_1} \ldots x_n^{e_n}$. Note that each e_i has $0 \leq e_i < q$, and note that not all e_i are equal to $q-1$. Thus $w_q(\beta) = e_1 + \cdots + e_n$, and since $\beta \in \Omega_{\mathfrak{d}}$, we know that $0 < e_1 + \cdots + e_n \leq \mathfrak{d}$ and $e_1 + \cdots + e_n \equiv w_q(\mathfrak{d}) \pmod{q-1}$. Since Lemma 7.20(iii) tells us that $w_q(\mathfrak{d}) \equiv \mathfrak{d} \pmod{q-1}$, we know that $\theta(\beta) \in M$. Furthermore, since the e_i are uniquely determined by β, θ is injective. □

7.8 Proof of the Theorem of N. M. Katz

Now we use Ψ to translate Theorem 7.14 from a statement about words in Abelian codes into a statement about polynomials. This gives us the following theorem, from which we shall deduce both the theorem of N. M. Katz (Theorem 7.17) and the associated statement concerning sharpness (Proposition 7.18).

Theorem 7.22. *Let $n, t \geq 1$ and let $S_1, \ldots, S_t$ be q-closed subsets of A, with at least one S_i not a subset $\{1_A\}$. For each i, let $\mathcal{C}_i$ be the convolution ideal (code) in $\mathbb{F}_q[A]$ consisting of those functions whose Fourier transforms are supported on S_i. Let $\mathcal{F}_1, \ldots, \mathcal{F}_t$ be sets of polynomials of degree less than $n(q-1)$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ such that $\Psi(\mathcal{F}_i) = \mathcal{C}_i$. Let $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ be as defined in* (7.11)*. For any $f_1 \in \mathcal{F}_1$, ..., $f_t \in \mathcal{F}_t$, we have*

$$|V(f_1, \ldots, f_t)| \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}}, \tag{7.20}$$

and there is some such selection of $f_1, \ldots f_t$ with

$$|V(f_1, \ldots, f_t)| \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}}. \tag{7.21}$$

Proof. Suppose $f_i \in \mathcal{F}_i$ for each i, and set $\varphi_i = \Psi(f_i)$. Then $\varphi_i \in \mathcal{C}_i$, so that $\hat{\varphi}_i$ is supported on S_i. Furthermore, as we vary f_i over $\mathcal{F}_i$, φ_i varies over the entire convolution ideal $\mathcal{C}_i$ of

functions in $\mathbb{F}_q[A]$ whose Fourier transforms are supported on S_i. Thus Theorem 7.14 tells us that

$$\mathrm{zer}^{\mathrm{norm}}(\varphi_1, \dots, \varphi_t) \equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\dots,\mathcal{C}_t)}} \tag{7.22}$$

for any $f_1 \in \mathcal{F}_1, \dots, f_t \in \mathcal{F}_t$, and

$$\mathrm{zer}^{\mathrm{norm}}(\varphi_1, \dots, \varphi_t) \not\equiv 0 \pmod{p^{\ell_{mc}(\mathcal{C}_1,\dots,\mathcal{C}_t)+1}} \tag{7.23}$$

for some such selection of $f_1, \dots, f_t$.

Note that

$$\begin{aligned}\hat{\varphi}_i(1_A) &= \sum_{a\in A} (\varphi_i)_a \\ &= -f_i(0,\dots,0) + \sum_{a_1,\dots,a_n \in \mathbb{F}_q} f_i(a_1,\dots,a_n).\end{aligned}$$

It is not difficult to see that $\sum_{a_1,\dots,a_n\in\mathbb{F}_q} x_1^{e_1}\dots x_n^{e_n} = 0$ unless $q-1 \mid e_1,\dots,e_n$ and $e_1,\dots,e_n > 0$. So polynomials of degree less than $n(q-1)$ vanish when we sum them over all points in $\mathbb{F}_q^n$. We are assuming that our polynomials f_i are of degree less than $n(q-1)$, so that $\hat{\varphi}_i(1_A) = -f_i(0,\dots,0)$. Thus $\tilde{\varphi}_i(1_A) = |A|^{-1}\hat{\varphi}_i(1_A)$ is zero if and only if $f_i(0,\dots,0) = 0$. So $\mathrm{zer}(\tilde{\varphi}_1(1_A),\dots,\tilde{\varphi}_t(1_A)) = \prod_{i=1}^t \delta(f_i(0,\dots,0),0)$. Thus, returning to (7.22) and (7.23), we have

$$\mathrm{zer}(\varphi_1,\dots,\varphi_t) \equiv |A| \prod_{i=1}^t \delta(f_i(0,\dots,0),0) \pmod{p^{\ell_{mc}(\mathcal{C}_1,\dots,\mathcal{C}_t)}}$$

for any $f_1 \in \mathcal{F}_1, \dots, f_t \in \mathcal{F}_t$, and

$$\mathrm{zer}(\varphi_1,\dots,\varphi_t) \not\equiv |A| \prod_{i=1}^t \delta(f_i(0,\dots,0),0) \pmod{p^{\ell_{mc}(\mathcal{C}_1,\dots,\mathcal{C}_t)+1}}$$

for some such selection of $f_1, \dots, f_t$.

Then apply Lemma 7.19 to see that

$$|V(f_1,\ldots,f_t)| \equiv (|A|+1)\prod_{i=1}^{t}\delta(f_i(0,\ldots,0),0) \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)}}$$

for any $f_1 \in \mathcal{F}_1,\ldots,f_t \in \mathcal{F}_t$, and

$$|V(f_1,\ldots,f_t)| \not\equiv (|A|+1)\prod_{i=1}^{t}\delta(f_i(0,\ldots,0),0) \pmod{p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}}$$

for some such selection of $f_1,\ldots,f_t$. We note that $|A|+1 = q^n$, which vanishes modulo $p^{\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)+1}$ if $\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t) < en$.

So the proof will be complete once we show that $\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t) < en$. Consider $\Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$, as defined in equation (7.10) of Section 7.5. Recall that in (7.11) we defined $\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t) = \min_{\lambda\in\Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)} L(\lambda)$. We shall prove that $\ell_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t) < en$ by finding an element $\lambda \in \Lambda_{mc}(\mathcal{C}_1,\ldots,\mathcal{C}_t)$ with $L(\lambda) < en$.

We represent accounts as formal sums in our construction of λ; see Section 2.5 to recall this notation. By our assumption about the sets S_i, we choose $k \in \{1,2,\ldots,t\}$ such that S_k contains some element $a \neq 1_A$. Then set $\lambda_k = (p-1)\sum_{j=0}^{n-1}\sum_{h\in H}(h, a^{q^j})$, and set λ_i to be the empty set for all $i \neq k$. This defines $\lambda \in \mathbb{N}[I\times H\times A]$. Since S_k is q-closed, λ_k is an element of $\mathbb{N}[S_k\times H]$; for $i\neq k$, λ_i is clearly in $\mathbb{N}[S_i\times H]$. Each $\mathrm{pr}_H\,\lambda_i$ with $i\neq k$ is trivially a Delsarte-McEliece multiset, and $\mathrm{pr}_H\,\lambda_k$ is the Delsarte-McEliece multiset with $n(p-1)$ instances of each element in H. Furthermore $\mathrm{pr}_A\,\lambda \notin \mathbb{N}[\{1_A\}]$ since $a\neq 1_A$. Finally

$$\begin{aligned}
\Pi\lambda &= \left(\prod_{j=0}^{n-1}\prod_{h=0}^{e-1} a^{q^j p^h}\right)^{p-1} \\
&= \left(\prod_{i=0}^{ne-1} a^{p^i}\right)^{p-1} \\
&= a^{(p-1)\sum_{i=0}^{ne-1} p^i} \\
&= a^{q^n-1} \\
&= 1_A.
\end{aligned}$$

So $\lambda \in \Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$, and note that $L(\lambda) = L(\lambda_k) = e(n-1) < en$. $\square$

We shall now show how this theorem can be regarded as an inchoate form of the theorem of N. M. Katz (Theorem 7.17) and the associated statement of sharpness (Proposition 7.18). We recall the content of these results for convenience. Theorem 7.17 states that if $f_1, \ldots f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$ are nonconstant polynomials of degrees $\mathfrak{d}_1 \leq \cdots \leq \mathfrak{d}_t$, respectively, and if we set ν to be the least nonnegative integer greater than or equal to $\left(n - \sum_{i=1}^{t} \mathfrak{d}_i\right)/\mathfrak{d}_t$, then $|V(f)|$ is divisible by q^ν. Proposition 7.18 states that there exist homogeneous polynomials $f_1, \ldots, f_t \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degrees $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ such that $|V(f_1, \ldots, f_t)|$ is not divisible by pq^ν. At the beginning of Section 7.7, we showed that these results are easy to obtain when $n \leq \mathfrak{d}_1 + \cdots + \mathfrak{d}_t$, so we shall assume that $n > \mathfrak{d}_1 + \cdots + \mathfrak{d}_t$ henceforth.

We now introduce a useful notation that will be used in the rest of this section. The reader should first recall the definitions of $\Lambda_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ and $\ell_{mc}(\mathcal{C}_1, \ldots, \mathcal{C}_t)$ in (7.10) and (7.11). If $\Xi_1, \ldots, \Xi_t$ are q-closed subsets of A, then define

$$\Lambda(\Xi_1, \ldots, \Xi_t) = \Lambda_{mc}(\mathcal{D}_1, \ldots, \mathcal{D}_t), \tag{7.24}$$

where $\mathcal{D}_1, \ldots, \mathcal{D}_t$ are the codes in $\mathbb{F}_q[A]$ such that Ξ_i is the support of $\mathrm{FT}(\mathcal{D}_i)$ for each i. Likewise, define

$$\ell(\Xi_1, \ldots, \Xi_t) = \ell_{mc}(\mathcal{D}_1, \ldots, \mathcal{D}_t). \tag{7.25}$$

This will provide a convenient notation, as it will be easier to focus on the supports of the Fourier transforms of the ideals than to focus on the ideals themselves.

If we want to prove Theorem 7.17, we use Theorem 7.22 in the case where each collection $\mathcal{F}_i$ of polynomials is equal to the set of $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg(f) \leq \mathfrak{d}_i$. Then Theorem 7.21 tells us that $\Psi(\mathcal{F}_i)$ is the code in $\mathbb{F}_q[A]$ whose Fourier transform has minimal support $\Upsilon_{\mathfrak{d}_i}$, as defined in that theorem. So we set each $S_i = \Upsilon_{\mathfrak{d}_i}$ in Theorem 7.22. If we can prove that $\ell(\Upsilon_{\mathfrak{d}_1}, \ldots, \Upsilon_{\mathfrak{d}_t}) = e\nu$, then (7.20) in Theorem 7.22 will imply Theorem 7.17.

If we want to prove Proposition 7.18, we use Theorem 7.22 in the case where each collection $\mathcal{F}_i$ of polynomials is equal to the set of homogeneous $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg(f) \leq \mathfrak{d}_i$. Then Theorem 7.21 tells us that $\Psi(\mathcal{F}_i)$ is the code in $\mathbb{F}_q[A]$ whose Fourier

transform has minimal support $\Omega_{\mathfrak{d}_i}$, as defined in that theorem. So we set each $S_i = \Omega_{\mathfrak{d}_i}$ in Theorem 7.22. If we can prove that $\ell(\Omega_{\mathfrak{d}_1}, \ldots, \Omega_{\mathfrak{d}_t}) = e\nu$, then (7.21) in Theorem 7.22 will imply Proposition 7.18.

We prove that $\ell(\Upsilon_{\mathfrak{d}_1}, \ldots, \Upsilon_{\mathfrak{d}_t}) = \ell(\Omega_{\mathfrak{d}_1}, \ldots, \Omega_{\mathfrak{d}_t}) = e\nu$ in Proposition 7.23 below, thus finishing our proof of Theorem 7.17 and Proposition 7.18. Before we do this, we pause to note that Theorem 7.22 can be regarded not only as an inchoate form of the theorem of N. M. Katz and the associated statement of sharpness, but also as an inchoate generalization of these results. For we can employ Theorem 7.22 in cases where the sets $S_1, \ldots, S_t$ are not all sets of the form Υ_j or all sets of the form Ω_j. That is, we may prescribe finer constraints on each polynomial f_i than merely setting the maximum degree or insisting that it be homogeneous of a certain degree. We must qualify this theorem as being an *inchoate* generalization of the theorem of N. M. Katz, since we obtain a true generalization only if we can calculate $\ell(S_1, \ldots, S_t)$ for the particular selection of $S_1, \ldots, S_t$ that we are considering. We finish this chapter with the promised calculation of $\ell(S_1, \ldots, S_t)$ when $S_1, \ldots, S_t$ are the sets relevant to the theorem of N. M. Katz and the associated statement of sharpness.

Proposition 7.23. *Let $n, t \geq 1$, let $\mathfrak{d}_1 \leq \cdots \leq \mathfrak{d}_t$ be positive integers with $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t < n$, and let $\nu = \lceil (n - \sum_{i=1}^{t} \mathfrak{d}_i)/\mathfrak{d}_t \rceil$. Let Υ_j and Ω_j be the sets defined in Theorem 7.21, and let Λ and ℓ be the functions defined in equations* (7.24) *and* (7.25) *above. Then*

$$\ell(\Upsilon_{\mathfrak{d}_1}, \ldots, \Upsilon_{\mathfrak{d}_t}) = \ell(\Omega_{\mathfrak{d}_1}, \ldots, \Omega_{\mathfrak{d}_t}) = e\nu.$$

Proof. Write Υ as a shorthand for $(\Upsilon_{\mathfrak{d}_1}, \ldots, \Upsilon_{\mathfrak{d}_t})$ and Ω as a shorthand for $(\Omega_{\mathfrak{d}_1}, \ldots, \Omega_{\mathfrak{d}_t})$. Since $\Omega_j \subseteq \Upsilon_j$ for all j, $\Lambda(\Omega) \subseteq \Lambda(\Upsilon)$, and so $\ell(\Omega) \geq \ell(\Upsilon)$. Therefore it suffices to show that $\ell(\Upsilon) \geq e\nu$ and $\ell(\Omega) \leq e\nu$. It will be useful for the reader to review the compact notations in Section 2.5, since these are used extensively in this proof.

First we show that $\ell(\Upsilon) \geq e\nu$, using an approach based on the proof by Delsarte and McEliece (see Lemma 5.1 of [18]) that Ax's theorem (Theorem 7.15) follows from their own

theorem (Theorem 7.1). Suppose that $\lambda \in \Lambda(\Upsilon)$. Since $\Pi\lambda = 1_A$, we have

$$\prod_{i=1}^{t} \prod_{a \in A} \prod_{h \in H} a^{p^h \lambda_{i,h,a}} = 1_A,$$

or equivalently,

$$\prod_{i=1}^{t} \prod_{j=0}^{q^n-2} \prod_{h \in H} \gamma^{j p^h \lambda_{i,h,\gamma^j}} = 1_A,$$

so that

$$\sum_{i=1}^{t} \sum_{j=0}^{q^n-2} \sum_{h \in H} j p^h \lambda_{i,h,\gamma^j} \equiv 0 \pmod{q^n - 1}.$$

Thus

$$\sum_{i=1}^{t} \sum_{j=0}^{q^n-2} \sum_{h \in H} j p^{h+s} \lambda_{i,h,\gamma^j} \equiv 0 \pmod{q^n - 1} \tag{7.26}$$

for any $s \geq 0$. Furthermore, since $\mathrm{pr}_A \lambda_i \notin \mathbb{N}[\{1_A\}]$ for some i, we know that $\lambda_{i,h,\gamma^j} \neq 0$ for some $i \in \{1, \ldots, t\}$, $h \in H$, and $j \in \{0, \ldots, q^n - 2\}$ with $j \neq 0$. So the sum in (7.26) is a sum of nonnegative numbers, at least one of which is strictly positive. Thus, by Lemma 7.20(xi), we know that

$$\sum_{i=1}^{t} \sum_{j=0}^{q^n-2} \sum_{h \in H} w_q\left(j p^{h+s} \lambda_{i,h,\gamma^j}\right) \geq n(q-1)$$

for any $s \geq 0$. So by Lemma 7.20(xiv),(i), we know that

$$\sum_{i=1}^{t} \sum_{j=0}^{q^n-2} \sum_{h \in H} w_q(j) w_q(p^{h+s}) \lambda_{i,h,\gamma^j} \geq n(q-1)$$

for any $s \geq 0$. Since $\lambda_i \in \mathbb{N}[H \times \Upsilon_{\mathfrak{d}_i}]$, $\lambda_{i,h,a}$ can be nonzero only if $w_q(a) \leq \mathfrak{d}_i$, i.e., λ_{i,h,γ^j} can be nonzero only for those $j \in \{0, \ldots, q^n - 2\}$ with $w_q(j) \leq \mathfrak{d}_i$. Thus

$$\sum_{i=1}^{t} \mathfrak{d}_i \sum_{j=0}^{q^n-2} \sum_{h \in H} w_q(p^{h+s}) \lambda_{i,h,\gamma^j} \geq n(q-1),$$

or equivalently,

$$\sum_{i=1}^{t} \mathfrak{d}_i \sum_{h \in H} w_q(p^{h+s}) (\mathrm{pr}_H(\lambda_i))_h \geq n(q-1),$$

for any $s \geq 0$. For each i, define u_i so that $u_i = 0$ if $|\lambda_i| = 0$ and $u_i = 1$ otherwise. Then

$$\sum_{i=1}^{t} \mathfrak{d}_i \left(-u_i(q-1) + \sum_{h \in H} w_q(p^{h+s})(\mathrm{pr}_H(\lambda_i))_h \right) \geq \left(n - \sum_{i=1}^{t} \mathfrak{d}_i \right)(q-1), \tag{7.27}$$

for any $s \geq 0$. Lemma 7.20(iii) tells us that

$$\sum_{h \in H} w_q(p^{h+s})(\mathrm{pr}_H(\lambda_i))_h \equiv \sum_{h \in H} p^{h+s}(\mathrm{pr}_H(\lambda_i))_h \pmod{q-1},$$

and since $\mathrm{pr}_H(\lambda_i)$ is Delsarte-McEliece for each i, the right-hand side of this congruence is zero modulo $q-1$. Thus the terms

$$-u_i(q-1) + \sum_{h \in H} w_q(p^{h+s})(\mathrm{pr}_H(\lambda_i))_h$$

on the left-hand side of (7.27) are multiples of $q-1$. These terms are also nonnegative because $u_i = 0$ when $\lambda_i = \emptyset$ and $u_i = 1$ when $|\lambda_i| > 0$; in the latter case the sum over H is strictly positive. Thus

$$\mathfrak{d}_t \sum_{i=1}^{t} \left(-u_i(q-1) + \sum_{h \in H} w_q(p^{h+s})(\mathrm{pr}_H(\lambda_i))_h \right) \geq \left(n - \sum_{i=1}^{t} \mathfrak{d}_i \right)(q-1),$$

and then

$$\begin{aligned} \sum_{i=1}^{t} \left(-u_i(q-1) + \sum_{h \in H} w_q(p^{h+s})(\mathrm{pr}_H(\lambda_i))_h \right) &\geq \left\lceil \frac{n - \sum_{i=1}^{t} \mathfrak{d}_i}{\mathfrak{d}_t} \right\rceil (q-1) \\ &= \nu(q-1) \end{aligned}$$

for any $s \geq 0$. Now sum both sides of the inequality over $s \in H$ to get

$$\sum_{i=1}^{t} \left(-u_i e(q-1) + \sum_{h \in H} \left(\frac{q-1}{p-1} \right) (\mathrm{pr}_H(\lambda_i))_h \right) \geq e\nu(q-1)$$

by Lemma 7.20(vi). Since $\sum_{h\in H}(\mathrm{pr}_H(\lambda_i))_h = |\mathrm{pr}_H(\lambda_i)| = |\lambda_i|$, we have

$$\sum_{i=1}^{t}(-u_i e(p-1) + |\lambda_i|) \geq e\nu(p-1).$$

Recall that $u_i = 0$ if $|\lambda_i| = 0$ and $u_i = 1$ otherwise. Thus $|\lambda_i| - u_i e(p-1) = (p-1)L(\lambda_i)$, and so

$$\sum_{i=1}^{t} L(\lambda_i) \geq e\nu,$$

that is, $L(\lambda) \geq e\nu$. Since $\lambda \in \Lambda(\Upsilon)$ was arbitrary, this proves that $\ell(\Upsilon) \geq e\nu$.

Now we prove that $\ell(\Omega) \leq e\nu$ by constructing explicitly an element $\lambda \in \Lambda(\Omega)$ with $L(\lambda) = e\nu$. We first define accounts that will be the building blocks of λ. For nonnegative integers u, v with $0 < v - u < n$, define the multiset

$$B_u^v = (p-1)\sum_{h\in H}\left(h, \gamma^{\sum_{j=u}^{v-1} q^j}\right).$$

Observe that $B_u^v \in \mathbb{N}[H \times A]$ and that $\mathrm{pr}_H B_u^v$ is the Delsarte-McEliece multiset with $p-1$ instances of each element in H. Also note that

$$\begin{aligned}\Pi B_u^v &= \left(\prod_{h\in H} \gamma^{p^h \sum_{j=u}^{v-1} q^j}\right)^{p-1} \\ &= \gamma^{(p-1)\sum_{h=0}^{e-1} p^h \sum_{j=u}^{v-1} q^j} \\ &= \gamma^{(p-1)\sum_{i=eu}^{ev-1} p^i},\end{aligned}$$

and so

$$\Pi B_u^v = \gamma^{q^v - q^u}. \tag{7.28}$$

We claim that $B_u^v \in \mathbb{N}[H \times \Omega_{v-u}]$. To prove this, it suffices to show that $\alpha = \gamma^{\sum_{j=u}^{v-1} q^j}$ is an element of Ω_{v-u}. Note that α is a product of $v-u$ elements of the form γ^{q^j}. Our given assumption $n > \mathfrak{d}_1 + \cdots + \mathfrak{d}_t$ forces $n > 1$, so that Lemma 7.20(v) shows that $w_q(\gamma^{q^j}) = 1$ for all j. So α is a product of $v-u$ elements of unit q-ary weight. Since $0 < v-u < n$, Lemma 7.20(xiii) tells us that $0 < w_q(\alpha) \leq v-u$ and $w_q(\alpha) \equiv w_q(v-u) \pmod{q-1}$. That is, $\alpha \in \Omega_{v-u}$.

Set $D(i) = \sum_{j=1}^{i} \mathfrak{d}_i$ for $i = 0, \ldots, t$ and $D(i) = D(t) + (i-t)\mathfrak{d}_t$ for $i = t+1, \ldots, t+\nu$. By the definition of ν, $D(t+\nu-1) < n$ and $n \le D(t+\nu) < n + \mathfrak{d}_t$. Since $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t < n$, we have $D(t+\nu) < 2n$. Let $r = D(t+\nu) - n$, so that $0 \le r < n$. Since $D(0) = 0$ and $D(t+\nu) \ge n$, there must be some positive i_0 with $i_0 \le t+\nu$ such that $D(i_0 - 1) \le r < D(i_0)$. Furthermore $i_0 < t+\nu$, for if $D(t+\nu-1) \le r < D(t+\nu)$, then we would have $\mathfrak{d}_t = D(t+\nu) - D(t+\nu-1) \ge D(t+\nu) - r = n$, in contradiction to our assumption that $\mathfrak{d}_1 + \cdots + \mathfrak{d}_t < n$.

We now continue our construction, approaching closer to our goal of forming an element $\lambda \in \Lambda(\Omega)$ with $L(\lambda) = e\nu$. Note that $D(i) - D(i-1) = \mathfrak{d}_{\min\{i,t\}}$ for all i with $1 \le i \le t+\nu$, so that $0 < D(i) - D(i-1) < n$ for all such i. For each $i \in \{1, \ldots, t+\nu\}$ with $i \ne i_0$, define $\mu_i = B^{D(i)}_{D(i-1)}$. Define

$$\mu_{i_0} = B^{D(i_0)}_{D(i_0-1)} - \left(0, \gamma^{\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}\right) + \left(0, \gamma^{1-q^r+\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}\right).$$

We claim that each μ_i is a multiset in $\mathbb{N}[H \times A]$ with $\mathrm{pr}_H \mu_i$ a Delsarte-McEliece multiset. This is clear for $i \ne i_0$ in light of what we have already proved about the accounts B^v_u above. Since $\mathrm{pr}_H \mu_{i_0} = \mathrm{pr}_H B^{D(i_0)}_{D(i_0-1)}$, $\mathrm{pr}_H \mu_{i_0}$ is Delsarte-McEliece. Since $B^{D(i_0)}_{D(i_0-1)}$ is a multiset with $p-1$ instances of the element $\left(0, \gamma^{\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}\right)$, μ_{i_0} has at least $p-2 \ge 0$ instances of this element. Clearly μ_{i_0} has a nonnegative number of instances of every other element, and so it is a multiset.

We claim that each μ_i is an element of $\mathbb{N}[H \times \Omega_{\mathfrak{d}_{\min\{i,t\}}}]$. Since $D(i) - D(i-1) = \mathfrak{d}_{\min\{i,t\}}$ for all $i \in \{1, \ldots, t+\nu\}$, what we have already proved about the accounts B^v_u shows that $B^{D(i)}_{D(i-1)} \in \mathbb{N}[H \times \Omega_{\mathfrak{d}_{\min\{i,t\}}}]$. This proves our claim for $i \ne i_0$, and also shows that proving the $i = i_0$ case is tantamount to showing that $\beta = \gamma^{1-q^r+\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}$ is an element of $\Omega_{\mathfrak{d}_{\min\{i_0,t\}}}$. Since $D(i_0 - 1) \le r < D(i_0)$, we see that β is a product of $D(i_0) - D(i_0 - 1) = \mathfrak{d}_{\min\{i_0,t\}}$ elements of the form γ^{q^j}. Recall that our condition $n > \mathfrak{d}_1 + \cdots + \mathfrak{d}_t$ forces $n > 1$, so that Lemma 7.20(v) shows that $w_q(\gamma^{q^j}) = 1$ for all j. Thus β is a product of $\mathfrak{d}_{\min\{i_0,t\}}$ elements of unit q-ary weight. Since $0 < \mathfrak{d}_{\min\{i_0,t\}} < n$, Lemma 7.20(xiii) tells us that $0 < w_q(\beta) \le \mathfrak{d}_{\min\{i_0,t\}}$ and $w_q(\beta) \equiv w_q(\mathfrak{d}_{\min\{i_0,t\}}) \pmod{q-1}$, i.e., that $\beta \in \Omega_{\mathfrak{d}_{\min\{i_0,t\}}}$. So each μ_i is indeed an element of $\mathbb{N}[H \times \Omega_{\mathfrak{d}_{\min\{i,t\}}}]$.

Now we are ready to construct λ. For $i < t$, let $\lambda_i = \mu_i$. Let $\lambda_t = \sum_{j=t}^{t+\nu} \mu_j$. This defines $\lambda \in \mathbb{N}[I \times H \times A]$. We claim that $\lambda \in \Lambda(\Omega)$. Note that what we have proved about the accounts μ_i tells us immediately that $\mathrm{pr}_H(\lambda_i)$ is a Delsarte-McEliece multiset and $\lambda_i \in \mathbb{N}[H \times \Omega_{\mathfrak{d}_i}]$ for each $i \in \{1, \ldots, t\}$. Since the λ_i are all nonempty and since $1_A \notin \Omega_j$ for all $j > 0$, we also know that $\mathrm{pr}_A \lambda \notin \mathbb{N}[\{1_A\}]$. In light of what we have just shown, our claim that $\lambda \in \Lambda(\Omega)$ will be established if we can show that $\Pi\lambda = 1_A$. Note that

$$\Pi\lambda = (\Pi\mu_1) \cdots (\Pi\mu_{t+\nu}) \,. \tag{7.29}$$

If $i \neq i_0$, then $\mu_i = B^{D(i)}_{D(i-1)}$, so (7.28) shows that $\Pi\mu_i = \gamma^{q^{D(i)} - q^{D(i-1)}}$. For $i = i_0$, we have

$$\begin{aligned} \Pi\mu_{i_0} &= \left(\gamma^{\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}\right)^{-1} \left(\gamma^{1-q^r+\sum_{j=D(i_0-1)}^{D(i_0)-1} q^j}\right) \Pi B^{D(i_0)}_{D(i_0-1)} \\ &= \gamma^{1-q^r} \gamma^{q^{D(i_0)} - q^{D(i_0-1)}}. \end{aligned}$$

Substituting the values of $\Pi\mu_i$ we just calculated into (7.29), we obtain

$$\begin{aligned} \Pi\lambda &= \gamma^{1-q^r} \prod_{i=1}^{t+\nu} \gamma^{q^{D(i)} - q^{D(i-1)}} \\ &= \gamma^{1-q^r} \gamma^{q^{D(t+\nu)} - q^{D(0)}}. \end{aligned}$$

Note that $D(0) = 0$ and $D(t+\nu) = n+r$, so we have $\Pi\lambda = \gamma^{q^{n+r} - q^r} = 1_A$. Thus $\lambda \in \Lambda(\Omega)$.

Now note that $|\mu_i| = e(p-1)$ for all i, so that $|\lambda_i| = e(p-1)$ for $i < t$ and $|\lambda_t| = (\nu+1)e(p-1)$. Thus $L(\lambda_i) = 0$ for $i < t$ and $L(\lambda_t) = e\nu$. Therefore $L(\lambda) = e\nu$, and so $\ell(\Omega) \leq e\nu$. This completes our proof. $\square$

Bibliography

[1] A. Adolphson and S. Sperber, *p-Adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci. École Norm. Sup. (4) **20** (1987), 545–556.

[2] J. Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.

[3] J. T. Blackford and D. K. Ray-Chaudhuri, *A transform approach to permutation groups of cyclic codes over Galois rings*, IEEE Trans. Inform. Theory **46** (2000), 2350–2358.

[4] I. F. Blake, *Codes over certain rings*, Information and Control **20** (1972), 396–404.

[5] ———, *Codes over integer residue rings*, Information and Control **29** (1975), 295–300.

[6] J.-P. Boly and W. J. van Gils, *Codes for combined symbol and digit error control*, IEEE Trans. Inform. Theory **34** (1988), 1286–1307.

[7] A. R. Calderbank, W.-C. W. Li, and B. Poonen, *A 2-adic approach to the analysis of cyclic codes*, IEEE Trans. Inform. Theory **43** (1997), 977–986.

[8] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, *Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions*, Advances in cryptology—EUROCRYPT 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 507–522.

[9] A. Canteaut, P. Charpin, and H. Dobbertin, *A new characterization of almost bent functions*, Fast Software Encryption 99, Lecture Notes in Comput. Sci., vol. 1636, Springer, Berlin, 1999, pp. 186–200.

[10] ———, *Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture*, IEEE Trans. Inform. Theory **46** (2000), 4–8.

[11] ———, *Weight divisibility of cyclic codes, highly nonlinear functions on* $\mathbf{F}_{2^m}$*, and crosscorrelation of maximum-length sequences*, SIAM J. Discrete Math. **13** (2000), 105–138.

[12] A. Canteaut and M. Videau, *Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis*, Advances in cryptology—EUROCRYPT 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, Springer, Berlin, 2002, pp. 518–533.

[13] C. Carlet, Z_{2^k}*-linear codes*, IEEE Trans. Inform. Theory **44** (1998), 1543–1547.

[14] ———, *On the divisibility properties and nonlinearity of resilient functions*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), 917–922.

[15] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.

[16] P. Delsarte, *Automorphisms of Abelian codes*, Philips Res. Rep. **25** (1970), 389–403.

[17] ———, *Weights of p-ary Abelian codes*, Philips Res. Rep. **26** (1971), 145–153.

[18] P. Delsarte and R. J. McEliece, *Zeros of functions in finite Abelian group algebras*, Amer. J. Math. **98** (1976), 197–224.

[19] B. K. Dey and B. S. Rajan, *Affine invariant extended cyclic codes over Galois rings*, IEEE Trans. Inform. Theory **50** (2004), 691–698.

[20] H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, *Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type*, IEEE Trans. Inform. Theory **47** (2001), 1473–1481.

[21] E. Dubois and A. N. Venetsanopoulos, *The discrete Fourier transform over finite rings with application to fast convolution*, IEEE Trans. Comput. **27** (1978), 586–593.

[22] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[23] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[24] T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), 209–232.

[25] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, *Improved estimates via exponential sums for the minimum distance of Z_4-linear trace codes*, IEEE Trans. Inform. Theory **42** (1996), 1212–1216.

[26] J. W. P. Hirschfeld and X. Hubaut, *Sets of even type in* PG(3, 4)*, alias the binary* (85, 24) *projective geometry code*, J. Combin. Theory Ser. A **29** (1980), 101–112.

[27] T. Kasami, *The weight enumerators for several classes of subcodes of the* 2*nd order binary Reed-Muller codes*, Information and Control **18** (1971), 369–394.

[28] T. Kasami, S. Lin, and W. W. Peterson, *New generalizations of the Reed-Muller codes. I. Primitive codes*, IEEE Trans. Inform. Theory **14** (1968), 189–199.

[29] D. J. Katz, *p-Adic valuation of weights in Abelian codes over $\mathbb{Z}_{p^d}$*, IEEE Trans. Inform. Theory **51** (2005), 281–305.

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

[31] F. J. MacWilliams, *Binary codes which are ideals in the group algebra of an Abelian group*, Bell System Tech. J. **49** (1970), 987–1011.

[32] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Co., Amsterdam, 1988.

[33] H. F. Mattson and G. Solomon, *A new treatment of Bose-Chaudhuri codes*, J. Soc. Indust. Appl. Math. **9** (1961), 654–669.

[34] B. R. McDonald, *Finite rings with identity*, Marcel Dekker Inc., New York, 1974.

[35] R. J. McEliece, *Linear recurring sequences over finite fields*, Ph.D. thesis, California Institute of Technology, Pasadena, 1967.

[36] ———, *On periodic sequences from* GF(q), J. Combinatorial Theory Ser. A **10** (1971), 80–91.

[37] ———, *Weight congruences for p-ary cyclic codes*, Discrete Math. **3** (1972), 177–192.

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

[39] ———, *Improvements of the Chevalley-Warning and the Ax-Katz theorems*, Amer. J. Math. **117** (1995), 241–244.

[40] O. Moreno, K. W. Shum, F. N. Castro, and P. V. Kumar, *Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications*, Proc. London Math. Soc. (3) **88** (2004), 545–564.

[41] A. A. Nechaev, *Kerdock's code in cyclic form*, Diskret. Mat. **1** (1989), 123–139, translation in Discrete Math. Appl. **1** (1991), 365–384.

[42] J. Pei, J. Cui, and S. Liu, *Cyclic codes over* GR(4^m) *which are also cyclic over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **49** (2003), 749–758.

[43] B. S. Rajan and M. U. Siddiqi, *A generalized DFT for Abelian codes over* Z_m, IEEE Trans. Inform. Theory **40** (1994), 2082–2090.

[44] C. Satyanarayana, *Lee metric codes over integer residue rings*, IEEE Trans. Inform. Theory **25** (1979), 250–254.

[45] J.-P. Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques*, Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, 69–85.

[46] ———, *A course in arithmetic*, Springer-Verlag, New York, 1973.

[47] ———, *Local fields*, Springer-Verlag, New York, 1979.

[48] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, *Improved binary codes and sequence families from Z_4-linear codes*, IEEE Trans. Inform. Theory **42** (1996), 1582–1587.

[49] P. Shankar, *On BCH codes over arbitrary integer rings*, IEEE Trans. Inform. Theory **25** (1979), 480–483.

[50] G. Solomon, *A weight formula for group codes*, IRE Trans. **IT-8** (1962), S 1–S 4.

[51] G. Solomon and R. McEliece, *Weights of cyclic codes*, J. Combinatorial Theory **1** (1966), 459–475.

[52] E. Spiegel, *Codes over Z_m*, Information and Control **35** (1977), 48–51.

[53] ———, *Codes over Z_m, revisited*, Information and Control **37** (1978), 100–104.

[54] K. T and B. S. Rajan, *Abelian codes over Galois rings closed under certain permutations*, IEEE Trans. Inform. Theory **49** (2003), 2242–2253.

[55] ———, *Consta-Abelian codes over Galois rings*, IEEE Trans. Inform. Theory **50** (2004), 367–380.

[56] M. van Eupen and J. H. van Lint, *On the minimum distance of ternary cyclic codes*, IEEE Trans. Inform. Theory **39** (1993), 409–422.

[57] J. H. van Lint and R. M. Wilson, *On the minimum distance of cyclic codes*, IEEE Trans. Inform. Theory **32** (1986), 23–40.

[58] H. N. Ward, *Combinatorial polarization*, Discrete Math. **26** (1979), 185–197.

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

[60] ———, *Weight polarization and divisibility*, Discrete Math. **83** (1990), 315–326.

[61] ———, *Divisors of codes of Reed-Muller type*, Discrete Math. **131** (1994), 311–323.

[62] E. Warning, *Bemerkung zur vorstehenden arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 76–83.

[63] S. K. Wasan, *On codes over Z_m*, IEEE Trans. Inform. Theory **28** (1982), 117–120.

[64] W. Willems, *A note on self-dual group codes*, IEEE Trans. Inform. Theory **48** (2002), 3107–3109.

[65] R. M. Wilson, *A lemma on polynomials modulo p^m and applications to coding theory*, Discrete Math., to appear.

[66] ———, *A remark on the number of codewords of weight congruent to j modulo p^e and the MacWilliams transform*, unpublished, 1995.

[67] ———, *A version for the Lee metric of a theorem of McEliece and weights of codewords in cyclic codes*, unpublished, 1995.