On Divisible Codes over Finite Fields

Thesis by

Xiaoyu Liu

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2006

(Submitted May 24, 2006)

In memory of my grandfather

Lingyun Shaohan He

Acknowledgements

Foremost, I would like to acknowledge the guidance from my advisor, Rick Wilson, who got me interested in this line of research and helped me through many challenging situations. Next, I wish to thank the others on my committee – David Wales, Dinakar Ramakrishnan and Cheng-Yeaw Ku – for their willingness to help.

I thank the California Institute of Technology, and especially the Department of Mathematics, for providing me with an opportunity to pursue my Ph.D. degree, and supporting me for five wonderful years.

Appreciation also goes to the department staff: Elizabeth Wood, Stacey Croomes, Kathy Carreon, and Pamela Fong, for all their help that makes my everyday life easier so that I can focus my attention on research.

Finally, and most of all, I want to thank my parents, who have always been an endless source of love and support to me.

Abstract

We study a certain kind of linear codes, namely divisible codes, over finite fields. These codes, introduced by Harold N. Ward, have the property that all codeword weights share a common divisor larger than 1. These are interesting error-correcting codes because many optimal codes and/or classical codes exhibit nontrivial divisibility.

We first introduce an upper bound on dimensions of divisible codes in terms of their weight spectrums, as well as a divisibility criteria for linear codes over arbitrary finite fields. Both the bound and the criteria are given by Ward, and these are the primary results that initiate this work.

Our first result proves an equivalent condition of Ward's bound, which involves only some property of the weight distribution, but not any other properties (including the linearity) of the code. This equivalent condition consequently provides an alternative (and more elementary) proof of Ward's bound, and from the equivalence we extend Ward's bound to certain nonlinear codes.

Another perspective of the equivalence gives rise to our second result, which studies weights modulo a prime power in divisible codes. This is generalized from weights modulo a prime power in linear codes, and yields much better results than the linear code version does. With a similar method we propound a new bound that is proved to be better than Ward's bound.

Our third result concerns binary divisible codes of maximum dimension with given lengths. We start with level one and level two codes, which are well described from this point of view. For higher level codes we prove an induction theorem by using the binary version of the divisibility criteria, as well as Ward's bound and the new generated bound. Moreover, this induction theorem allows us to determine the exact bound and the codes that attain the bound for level three codes of relatively small length.

Contents

Chapter 1

Introduction

Let p be a prime, and let l be a positive integer. Set $q = p^l$. Let $\mathbb{F}_q$ denote the field of q elements. A q-ary *linear code* of *length* n and *dimension* k, or an $[n,k]_q$ code for short, is a k-dimensional subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is said to be the *alphabet* of the code. Linear codes form a large class of error-correcting codes, which includes various subclasses all of great importance in coding theory. From now on, we shall occasionally mention definitions and results on linear codes from the encyclopedic references [PW72] and [MS77] without further citing them.

Suppose C is an $[n,k]_q$ code. Any basis of C forms a k by n matrix G that is called a *generator matrix* of C, and C is uniquely determined by any of its generator matrices. The *Hamming weight* $\mathrm{wt}(c)$ of any *codeword* $c \in C$ is defined to be the number of nonzero coordinates in c. The *weight enumerator* $w(x)$ of C, or $w_C(x)$, is a polynomial written as

$$w(x) = \sum_{c \in C} x^{\mathrm{wt}(c)} = \sum_{i=0}^{n} w_i x^i,$$

where each coefficient w_i, $0 \le i \le n$, represents the number of codewords of weight i in C. The *MacWilliams transform* of $w(x)$ is defined as

$$w^{\perp}(x) = q^{-k}(1+(q-1)x)^n w\left(\frac{1-x}{1+(q-1)x}\right), \tag{1.1}$$

which is also a polynomial in x. For any two vectors $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$ define their *inner* or *scalar product* as $a \cdot b = a_1 b_1 + \cdots + a_n b_n$. If $a \cdot b = 0$, a and b are said to be *orthogonal*. The *dual* or *orthogonal code* $C^{\perp}$ of C is the set of vectors in $\mathbb{F}_q^n$ that are orthogonal to all codewords in C, and obviously $C^{\perp}$ is an $[n, n-k]_q$ code. The well-known

MacWilliams identity asserts that the weight enumerator of $C^\perp$ is exactly the MacWilliams transform $w^\perp(x)$ as defined in (1.1). Moreover, C is called *self-orthogonal* or *weakly self-dual* if $C \subseteq C^\perp$, (*strictly*) *self-dual* if $C^\perp = C$, and *formally self-dual* if $w_{C^\perp}(x) = w_C(x)$. Self-dual codes are automatically formally self-dual due to the MacWilliams identity. In addition to the code length n and dimension k, another important parameter of the linear code C is the so called *minimum weight*, by which we mean the minimum Hamming weight of the nonzero codewords in C. An $[n, k]_q$ code of minimum weight d may also be denoted as an $[n, k, d]_q$ code.

In this work, we are interested in a certain kind of linear codes that exhibits nontrivial divisibility such that all codeword weights have a common divisor greater than one. Such codes are named by Harold N. Ward as *divisible codes*. The simplest divisible code is a *replicated code*, which is created by repeating each coordinate in a selected code a certain number of times. Besides, several families of classical codes exhibit nontrivial divisibility. Moreover, their dimensions are usually larger than those for replicated codes of the same divisor and length. As a matter of fact, we shall discuss divisible codes mainly in two aspects: bounds for divisible codes; and divisibility properties of linear codes. This opening chapter consisting of two sections is an introduction to the entire thesis. Section 1.1 introduces the background of divisible codes including the origination and the description of these codes, as well as the previous results that initiate this work. Section 1.2 outlines our new results. Throughout this thesis, p, q, and l are as above set, and unless otherwise stated, C is a q-ary linear code of length n.

1.1 Background

Divisible codes were introduced by Ward [War81] in 1981. A q-ary *divisible code* is a linear code over the field $\mathbb{F}_q$ whose codewords all have weights divisible by some integer $\Delta > 1$, where Δ is called a *divisor* of the code. Ward proved that if a divisor Δ of a divisible code is relatively prime to the field characteristic, then the code is merely equivalent[1] to a Δ-folded[2] replicated code. Thus for a q-ary divisible code C, one is most interested in the case where the greatest divisor of C equals p^e for some integer $e \geq 1$. In such a case, C is

[1] A code C_1 is said to be *equivalent* to another code C_2 if, after rearranging its coordinates, C_1 will be the same as C_2.

[2] A Δ-*folded* replicated code is a replicated code created by repeating each coordinate in a selected code Δ times.

said to be of (divisibility) *level* e. Suppose t is an integer that is relatively prime to p, and let C be a level e code as above defined. Then any t-folded replication of C is also called a level e code. In other words, a q-ary divisible code C is of level e if and only if the exponent of the highest power of p that divides the greatest divisor of C equals e.

The study of divisible codes was motivated by a theorem of Gleason and Pierce giving constraints on the divisor and field size for divisible codes that are formally self-dual, and Ward [War81] recast the theorem as follows:

Theorem 1.1 (Gleason and Pierce). *Suppose C is a q-ary divisible code of length n, dimension $k = \lfloor n/2 \rfloor$, and greatest divisor $\Delta > 1$. Then the possibilities for q and Δ are limited to the following types:*

I. $q = \Delta = 2$;

II. $q = 2$, $\Delta = 4$, *and C is self-orthogonal. Moreover, C is self-dual if n is even;*

III. $q = \Delta = 3$, *and C is self-orthogonal. Moreover, C is self-dual if n is even;*

IV. $q = 4$, $\Delta = 2$*;*

V. $\Delta = 2$, *and C is equivalent to the code obtained by duplicating each entry in the codewords of $\mathbb{F}_q^k$ and adding on a* 0 *if n is odd;*

VI. $\Delta = 3$, *and C is equivalent to the code with generator matrix* $(1, 1, 1)$*;*

VII. $q = \Delta = 4$, *and C is equivalent to the code with generator matrix*

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \omega & \omega^2 \end{pmatrix},$$

where $\mathbb{F}_4 = \mathbb{F}_2(\omega)$.

The Roman numeral appropriate to C is customarily called the *type*[3] of C. All codes covered by Theorem 1.1 may be viewed as divisible codes of length n attaining the largest conceivable dimension, except when $q = \Delta = 2$. Satisfactory bounds on dimension of divisible codes in terms of length and divisibility level are not known in general. However, Ward

[3] A code of type I or IV may also be of type V, and a code of type III may also be of type VI.

[War92] stated as follows an upper bound for the dimension of a divisible code depending on its weight spectrum.[4]

Theorem 1.2 (Ward [War92]). *Let C be a q-ary divisible code whose nonzero weights are among the m consecutive multiples $w_1 = (b-m+1)\Delta$, $\ldots$, $w_m = b\Delta$ of the divisor Δ. Then*

$$\dim C \leq m\left(\frac{v_p(\Delta)}{l}+1\right)+\frac{1}{l}\, v_p\left(\binom{b}{m}\right), \tag{1.2}$$

where the p-adic valuation $v_p(x)$ is defined to be the exponent of the highest power of p that divides x. By convention, $v_p(0)=\infty$.

We call bound (1.2) *Ward's bound.* Besides the original character-theoretic proof [War92], Ward [War01a] gave another combinatorial proof of this bound. One of the main applications of the bound is providing upper bounds on minimum weight for formally self-dual codes, or equivalently, codes of even lengths in Theorem 1.1. Before Ward's work, the best known such bound for type I codes was the bound of Conway and Sloane [CS90], which says that the minimum weight of a type I code of even length n is at most $2\lfloor (n+6)/10 \rfloor$, except for some low values of n. Ward improved the bound to $\lfloor (n+4\log_2 n+12)/6 \rfloor$, which is asymptotically stronger. For type II codes, Ward's bound generally cannot beat the best known upper bound, $4\lfloor n/24 \rfloor + 4$, given by Mallows and Sloane [MS73]. However, the technique in Ward's proof is more elementary. Later on, Rains [Rai98] gave an analogous (and better) bound for type I codes that says that the minimum weight for a type I code of even length n is at most $4\lfloor n/24 \rfloor + 4$, except for $n \equiv 22 \pmod{24}$, when the bound is $4\lfloor n/24 \rfloor + 6$.

Besides the bound, Ward [War90] presented a divisibility criteria for linear codes by employing the technique of *combinatorial polarization* in the system of *p-adic numbers.*[5] The books by Serre [Ser79] and Cassels [Cas86] are references for what follows. Let $\mathbb{Q}_p$ be the field of p-adic numbers, let $\mathbb{Q}_q$ be the splitting field of $x^q - x$ over $\mathbb{Q}_p$, and let $\mathbb{Z}_q$ be the ring of integers[6] of $\mathbb{Q}_q$. $\mathbb{Z}_q$ is a *discrete valuation ring.* Suppose $\mathfrak{P}$ is the (unique) nonzero prime ideal of $\mathbb{Z}_q$. Consider $\mathbb{Z}_q \xrightarrow{\pi} \mathbb{Z}_q/\mathfrak{P} \xrightarrow{\sigma} \mathbb{F}_q$, where π is the *residue class map* and σ is an isomorphism. Then $\mathbb{Z}_q/\mathfrak{P}$, which is isomorphic to $\mathbb{F}_q$, is the *residue field* of $\mathbb{Z}_q$.

[4] The *weight spectrum* of a code is the list of nonzero weights its codewords may have.

[5] p-adic numbers are the completion of $\mathbb{Q}$ with respect to the p-adic metric, which defines the p-adic norm of any rational number $x = p^a r/s$ (r, s are integers not divisible by p) as p^{-a}.

[6] Each p-adic number x can be uniquely represented by $\sum_{j=m}^{\infty} a_j p^j$, with m an integer, and $0 \leq a_j \leq p-1$ integers. When $m \geq 0$, x is called a p-adic integer, and m is called the *order* of x.

Moreover, $\mathbb{Z}_q$ contains the full group U_{q-1} of $(q-1)$-st roots of unity, and $R = U_{q-1} \cup \{0\}$ maps one-to-one onto $\mathbb{F}_q$ under $\sigma \circ \pi$. For each $x \in \mathbb{Z}_q$, there is a unique member $\tilde{\mathrm{T}}(x) \in R$ for which $x \equiv \tilde{\mathrm{T}}(x) \pmod{p}$. $\tilde{\mathrm{T}}(x)$ is called the *Teichmüller representative* of x, and R is the set of Teichmüller representatives. Lifting $\tilde{\mathrm{T}}$ by $\sigma \circ \pi$, the *Teichmüller lift* $\mathrm{T}(\alpha)$ of $\alpha \in \mathbb{F}_q$ is the member of R corresponding to α for which the diagram

$$\begin{tikzcd}
\mathbb{Z}_q/\mathfrak{P} \arrow[r, "\sigma"] & \mathbb{F}_q \arrow[d, "\mathrm{T}"'] \\
\mathbb{Z}_q \arrow[u, "\pi"] \arrow[r, "\tilde{\mathrm{T}}"] & R
\end{tikzcd}$$

is commutative. The Teichmüller lift $\mathrm{T} : \mathbb{F}_q \to R$ gives a one-to-one correspondence from the code alphabet $\mathbb{F}_q$ to the set of Teichmüller representatives in p-adic integers, which allows us to deal with divisibility properties for q-ary codes by means of weight polarization. For any vector $c = (c_1, \ldots, c_n)$ in $\mathbb{F}_q^n$, the Teichmüller lift of c is defined componentwise as $\mathbf{T}(c) = (\mathrm{T}(c_1), \ldots, \mathrm{T}(c_n))$. For each $1 \leq i \leq n$, let $\lambda_i(\cdot)$ represent the i-th coordinate operator. Define a *form* $M = (r_1, \ldots, r_m)$ as

$$M(\mathbf{T}(c_1), \ldots, \mathbf{T}(c_m)) = \sum_{i=1}^{n} \lambda_i(\mathbf{T}(c_1)^{r_1} \ldots \mathbf{T}(c_m)^{r_m}), \tag{1.3}$$

where each c_j, $1 \leq j \leq m$, is a vector in $\mathbb{F}_q^n$, and the product in the right hand side of (1.3) is taken componentwise. For any integer u, let $\delta_p(u)$ represent the sum of the digits of u when written base p. For any p-adic integer v, let $\mathrm{ord}(v)$ represent the order of p in v. Then the divisibility criteria is as follows:

Theorem 1.3 (Ward [War90]). *Let C be a q-ary linear code with spanning set $\mathfrak{B}$. Then p^e is a divisor of C if and only if*

$$e \leq \frac{1}{p-1} \sum_{i=1}^{m} \delta_p(r_i) - l + \mathrm{ord}(M(\mathbf{T}(b_1), \ldots, \mathbf{T}(b_m)))$$

for all $M = (r_1, \ldots, r_m)$ with $\sum_{i=1}^{m} r_i \equiv 0 \pmod{q-1}$, and all choices of $b_1, \ldots, b_m \in \mathfrak{B}$.

Applications of the criteria involve giving alternative proofs for the theorem of Ax [Ax64] and the divisibility properties of generalized Reed-Muller codes, as well as examining divisibility properties and existence of Griesmer codes. These codes, together with the divisible formally self-dual codes as stated in the theorem of Gleason and Pierce, are the most conspicuous classical codes that exhibit nontrivial divisibility.

Generalized Reed-Muller Codes. An $[n,k]_q$ code C is said to be *cyclic* if for every codeword $c = (c_0, c_1, \ldots, c_{n-1})$, the right cyclic shift $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a codeword. Identify each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ with a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]$ modulo $x^n - 1$. Then for any cyclic code C there exists a unique polynomial $g(x)$ that is monic and has the smallest degree among all nonzero polynomials in C, and $g(x)$ is known as the *generator polynomial* of C in the sense that $C = \langle g(x) \rangle$ in $\mathbb{F}_q[x]/(x^n - 1)$. Suppose m is a positive integer and $j = \sum_{i=0}^{m-1} a_i q^i$, where $0 \le a_i < q$ for $i = 0, 1, \ldots, m-1$. Then we define $\delta_q(j) = \sum_{i=0}^{m-1} a_i$. The *shortened r-th order generalized Reed-Muller* (*GRM*) *code* of length $n = q^m - 1$ over $\mathbb{F}_q$ is the cyclic code with generator polynomial

$$g(x) = \prod^{(r)} (x - \alpha^j),$$

where α is a primitive element in $\mathbb{F}_{q^m}$ and the upper index (r) indicates that the product is taken over integers j with $0 \le j < q^m - 1$ and $0 \le \delta_q(j) < (q-1)m - r$. The *r-th order GRM code* of length $n = q^m$ has a generator matrix G^* obtained from the generator matrix G of the shortened GRM code by adjoining a column of 0's and then a row of 1's. Binary generalized Reed-Muller codes are simply called *Reed-Muller codes*, and an alternative definition of (binary) Reed-Muller codes is given in Section 1.2. The theorem of Ax asserts that the r-th order GRM code of length $n = q^m$ is divisible by $\Delta = q^{\lceil m/r \rceil - 1}$. Moreover, this divisor is the highest power of p that divides the code, or equivalently, the code is of divisibility level $l(\lceil m/r \rceil - 1)$. Ward [War90] concluded this divisibility property for GRM codes by applying the criteria stated in Theorem 1.3.

Griesmer Codes. Given integers k and d, denote by $n_q(k,d)$ the smallest integer n such that there exists an $[n,k,d]_q$ code. In 1960 Griesmer [Gri60] proved that for binary codes, one has $n_2(k,d) \ge \sum_{i=0}^{k-1} \lceil d/2^i \rceil$. In 1965 Solomon and Stiffler [SS65] generalized the result to linear codes over arbitrary finite fields, which says that $n_q(k,d) \ge \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. This is called the *Griesmer bound*. A code meeting the bound is called a *Griesmer code*. Dodunekov and Manev [DM90] showed that for a binary Griesmer code, the power of 2 dividing the minimum weight is a divisor of the code. Making use of the divisibility criteria, Ward [War98] extended the result to Griesmer codes over prime fields, which says that for a p-ary Griesmer code, the power of p dividing the minimum weight is a divisor of the code. Ward [War01b] conjectured that any q-ary Griesmer code has a divisor p^{e+1}/q, where e is the exponent of the highest power of p that divides the minimum weight of the code, and proved his conjecture when $q = 4$ or $e = v_p(q)$. Baumert and McEliece [BM73] proved that for any given k, binary Griesmer codes exist for sufficiently large d. Hamada and Tamari [HT80] and Dodunekov [Dod84] generalized this result to q-ary codes. However, the existence of Griesmer codes with relatively small minimum distances is still an interesting problem. Various researchers [DHM87, HN92, GH94, DGS99, LM99, Mar99, LRM03, War04] have worked on this problem when $k = 3, 4, 5, 6, 7, 8, 9$ and $q = 2, 3, 4, 5, 7, 8, 9$. Divisibility properties of Griesmer codes were employed by Ward [War98] to prove the non-existence of Griesmer codes over small prime fields with certain parameters k and d.

1.2 New Results

We present three new results that are initiated from the previous work on divisible codes in the following three chapters, respectively.

Our first result, presented in Chapter 2, concerns Ward's bound. The main theorem gives as follows a sufficient and necessary condition of Ward's bound involving only the values of the m consecutive multiples of Δ, but not any property (including the linearity) of the code:

Theorem 1.4. *Suppose $w_1 = (b - m + 1)\Delta$, $\ldots$, $w_m = b\Delta$ are m consecutive multiples of the divisor Δ. Then Ward's bound*

$$k \leq m\left(\frac{v_p(\Delta)}{l} + 1\right) + \frac{1}{l}\, v_p\left(\binom{b}{m}\right)$$

holds if and only if there exist integers a_{w_1}, $\ldots$, a_{w_m} such that the following $m + 1$ congruences

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &\equiv -1 \pmod{q^k} \\ \binom{w_1}{j} a_{w_1} + \cdots + \binom{w_m}{j} a_{w_m} &\equiv 0 \pmod{q^{k-j}}, \quad j = 1, 2, \ldots, m \end{aligned}$$

are satisfied.

Applications of this equivalent condition include an alternative proof of Theorem 1.2, as well as an analogous bound for binary $\mathbb{Z}_4$-linear codes.[7]

Another perspective of Theorem 1.4 is that it indicates the possibility of improving Ward's bound. Since Ward's bound is determined by the weight spectrum, one natural question is: Can it be improved when some weights in the middle of the spectrum are missing? Our second result, presented in Chapter 3, tries to answer this question. Inspired by a theorem of Wilson [Wil03] about weights modulo a prime power in linear codes, we examine weights modulo p^s, s a positive integer, in q-ary divisible codes.

Theorem 1.5. *Let e, t, and s be positive integers. Suppose C is a q-ary level e divisible code. Let $N(j,p^m)$ denote the number of codewords in C that have weights congruent to j modulo p^m. If*

$$\dim C > (\frac{e}{l}+1)((s(p-1)+1)p^{t-1}-1),$$

then for all integers j

$$N(jp^e, p^{e+t}) \equiv 0 \pmod{p^s}. \tag{1.4}$$

This theorem actually provides an upper bound on dimension of divisible codes that do not endure the property (1.4). Further, we "generalize" Theorem 1.5 as follows to provide an upper bound on dimension of divisible codes involving some divisibility property of weight enumerator modulo p^s, and show that our new bound improves Ward's bound.

Theorem 1.6. *Let $e \geq 1$, $r \geq 0$, $s \geq 1$ be integers, and let C be a q-ary level e divisible code. Suppose that the weight enumerator of C is $w(x^{p^e})$, where $w(x) \equiv (1-x)^r g(x) \pmod{p^s}$ for some integer-coefficient polynomial g with $g(1) \not\equiv 0 \pmod{p^s}$. Then*

$$\dim C < r(\frac{e}{l}+1) + \frac{s}{l}.$$

Note that both Ward's bound and the bound given in Theorem 1.6 provide bounds on dimensions of divisible codes without involving code length. These bounds are usually attainable when the code length is sufficiently large. However, for relatively short (compared to the width of the weight spectrum, or the degree of the weight enumerator modulo a prime

[7] These are binary (nonlinear) codes with details given in Section 2.2.

power) codes, these bounds may often be improved spectacularly, because both bounds follow from the linearity of the code, and the divisibility property requires more than the linearity of the code. Thus the more interesting bound on dimensions of divisible codes relies on the code length. No such bound is known in general. Nevertheless, our third result, presented in Chapter 4, discusses upper bounds on the dimension of level e binary divisible codes of given length by detailed analyzing the structure of such codes. The discussion is started from a well-known fact about level one and level two codes, given by the following theorem:

Theorem 1.7. *Suppose C is a binary linear code with length n and level e. Then*

(i) *if $e = 1$ then $\dim C \leq n - 1$, with equality if and only if C is the code consists of all words of even weights;*

(ii) *if $e = 2$ then $\dim C \leq n/2$, with equality if and only if C is a doubly even self-dual code in which case $8|n$.*

For level $e \geq 3$ codes, we start with codes of length $n = 2^{e+1}$. Ward's bound or the bound given in Theorem 1.6 gives that the dimension of such codes is at most $e + 2$. Moreover, the bound is attained if and only if the code is equivalent to the first order Reed-Muller code of the given length. In general, The *r-th order Reed-Muller code* of length $L = 2^n$, denoted $\mathrm{RM}[r, n]$, is the binary linear code whose 2^n coordinate positions are indexed by the vectors $u_1, \ldots, u_L$ in $\mathbb{F}_2^n$, and where there is one codeword $(f(u_1), \ldots, f(u_L))$ for every multi-linear polynomial $f(x) = f(x_1, \ldots, x_n)$, $x = (x_1, \ldots, x_n)$, of total degree at most r over $\mathbb{F}_2$. Note that this is just the binary case of the r-th order generalized Reed-Muller codes. Our conjecture is that when the code length is $2^{e+1}m$, then the dimension is bounded from above by $m(e + 2)$, and the bound is attained if and only if the code is equivalent to the concatenation of m copies of $\mathrm{RM}[1, e + 1]$. Here the concatenation of C_1 and C_2 simply means $C_1 \oplus C_2$, the direct sum of C_1 and C_2. Though the conjecture remains unproved, a weaker induction theorem is developed as follows:

Theorem 1.8. *Let $e \geq 1$, $m \geq 2$ be integers, and set $n = 2^{e+1}m$. Suppose the dimension of a binary level e divisible code of length $n - 2^{e+1}$ is at most $(m - 1)(e + 2)$. Suppose also that such a code is unique up to equivalence if its dimension equals $(m - 1)(e + 2)$. Then if C is a binary level e divisible code of length n, and there exists some codeword of weight*

2^{e+1} *in* C*, then* $\dim C \leq m(e+2)$*. Moreover, if* $\dim C = m(e+2)$ *such code* C *is equivalent to the concatenation of* m *copies of* $\mathrm{RM}[1, e+1]$.

This theorem, together with the hypothesis that any binary level e divisible code of maximum dimension contains a codeword of weight 2^{e+1}, will assure the above conjecture. Though the hypothesis remains unproved in general, it can be shown true when n is relatively small. Thus for binary level three codes of relatively small length, we prove the following theorem:

Theorem 1.9. *Let* C *be a level three binary code of length* n*, where* n *is* 16*,* 32*,* 48*,* 64*,* 80*,* 96*, or* 112*. Then the dimension of* C *cannot exceed* $5n/16$*. Moreover, for those listed lengths except* $n = 112$*, such a code of dimension* $5n/16$ *is equivalent to the concatenation of* $n/16$ *copies of the* $\mathrm{RM}[1, 4]$.

Chapter 2

On Ward's Bound

We discuss more about Ward's bound in this chapter. In Section 2.1 we first prove an equivalent condition of the bound, and conclude that the bound is a consequence of the fact that the MacWilliams transform of the weight enumerator has integer coefficients. Further, we provide an example to show that the integrality of the MacWilliams transform implies more than Ward's bound. Moreover, for a single or double weighted code, we show that the integrality of the MacWilliams transform is indeed equivalent to the bound. In Section 2.2, we first briefly revisit $\mathbb{Z}_4$-linear codes, then give an analogous bound for nonlinear binary codes obtained from $\mathbb{Z}_4$-linear codes using the fact that the MacWilliams transform of the weight enumerator of such a code has integer coefficients.

2.1 An Equivalence of Ward's Bound

Suppose C is an $[n,k]_q$ code whose nonzero codeword weights are among the m consecutive multiples $w_1 = (b-m+1)\Delta, \ldots, w_m = b\Delta$ of the divisor Δ. Recall Ward's bound says that

$$k \le m\left(\frac{v_p(\Delta)}{l}+1\right)+\frac{1}{l}\,v_p\left(\binom{b}{m}\right),$$

which is equivalent to

$$v_p\left(\frac{w_1\ldots w_m}{m!}\right) \ge l(k-m). \tag{2.1}$$

Now put aside the code C, and consider just inequality (2.1) that involves nothing more than the values of m, k, and the m consecutive multiples $w_1,\ldots,w_m$. By an "equivalence" of Ward's bound, we simply mean a sufficient and necessary condition such that inequality (2.1) holds. As a matter of fact, we claim that (2.1) holds if and only if there exist m

integers $a_{w_1}, \ldots, a_{w_m}$, such that the following $m+1$ congruences

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &\equiv -1 \qquad (\mathrm{mod}\ q^k) \\ \binom{w_1}{j} a_{w_1} + \cdots + \binom{w_m}{j} a_{w_m} &\equiv \ \ 0 \qquad (\mathrm{mod}\ q^{k-j}), \quad j = 1, 2, \ldots, m \end{aligned} \tag{2.2}$$

are satisfied.

2.1.1 Proof of the Equivalence

The proof of the equivalence embraces two directions, and we shall first show that if (2.1) holds then the set of congruence equations (2.2) has an integer solution. Consider, instead of the congruence equations, the following m *equations* on the m variables $a_{w_1}, \ldots, a_{w_m}$:

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &= -1 \\ \binom{w_1}{j} a_{w_1} + \cdots + \binom{w_m}{j} a_{w_m} &= \ \ 0, \quad j = 1, 2, \ldots, m-1. \end{aligned} \tag{2.3}$$

Our first goal is to find the solution of (2.3). The *coefficient matrix* of (2.3) is

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ w_1 & w_2 & \cdots & w_m \\ \vdots & \vdots & \ddots & \vdots \\ \binom{w_1}{m-1} & \binom{w_2}{m-1} & \cdots & \binom{w_m}{m-1} \end{pmatrix}. \tag{2.4}$$

Then the solution of (2.3) is

$$\begin{pmatrix} a_{w_1} \\ a_{w_2} \\ \vdots \\ a_{w_m} \end{pmatrix} = B \begin{pmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where B is the inverse matrix of A. For convenience, write b_{ij} as the (i,j)-th entry of B. Then $a_{w_i} = -b_{i1}$ for all $1 \le i \le m$. Let A_{ij} be the (i,j)-th minor of A. Then

$$b_{i1} = (-1)^{i+1} \frac{\det A_{1i}}{\det A},$$

hence

$$a_{w_i} = (-1)^i \frac{\det A_{1i}}{\det A}. \tag{2.5}$$

Lemma 2.1. *Suppose A is the m by m matrix as set in* (2.4)*. Then*

$$\det A = \frac{\prod_{1\le r<s\le m}(w_s - w_r)}{2!\dots(m-1)!}, \tag{2.6}$$

and for each $1 \le i \le m$

$$\det A_{1i} = \frac{w_1 \dots w_m}{w_i} \frac{\prod_{\substack{1\le r<s\le m \\ r,s\neq i}}(w_s - w_r)}{2!\dots(m-1)!}. \tag{2.7}$$

Proof. Note that adding a multiple of one row to another row of a square matrix does not change the determinant. Thus

$$\det A = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_1 & w_2 & \dots & w_m \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_1^{m-1}}{(m-1)!} & \frac{w_2^{m-1}}{(m-1)!} & \dots & \frac{w_m^{m-1}}{(m-1)!} \end{pmatrix} = \frac{1}{2!\dots(m-1)!}\det M,$$

where

$$M = \begin{pmatrix} 1 & 1 & \dots & 1 \\ w_1 & w_2 & \dots & w_m \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{m-1} & w_2^{m-1} & \dots & w_m^{m-1} \end{pmatrix}$$

is a Vandermonde matrix with $\det M = \prod_{1\le r<s\le m}(w_s - w_r)$. Therefore,

$$\det A = \frac{\prod_{1\le r<s\le m}(w_s - w_r)}{2!\dots(m-1)!},$$

as desired. Then for any $1 \le i \le m$, consider the $(1, i)$-th minor

$$A_{1i} = \begin{pmatrix} w_1 & \dots & w_{i-1} & w_{i+1} & \dots & w_m \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \binom{w_1}{m-1} & \dots & \binom{w_{i-1}}{m-1} & \binom{w_{i+1}}{m-1} & \dots & \binom{w_m}{m-1} \end{pmatrix}.$$

By the same reason we have

$$\begin{aligned}
\det A_{1i} &= \det \begin{pmatrix} w_1 & \dots & w_{i-1} & w_{i+1} & \dots & w_m \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \frac{w_1^{m-1}}{(m-1)!} & \dots & \frac{w_{i-1}^{m-1}}{(m-1)!} & \frac{w_{i+1}^{m-1}}{(m-1)!} & \dots & \frac{w_m^{m-1}}{(m-1)!} \end{pmatrix} \\
&= \frac{w_1 \dots w_{i-1} w_{i+1} \dots w_m}{2! \dots (m-1)!} \det M_i,
\end{aligned}$$

where

$$M_i = \begin{pmatrix} 1 & \dots & 1 & 1 & \dots & 1 \\ w_1 & \dots & w_{i-1} & w_{i+1} & \dots & w_m \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ w_1^{m-2} & \dots & w_{i-1}^{m-2} & w_{i+1}^{m-2} & \dots & w_m^{m-2} \end{pmatrix}$$

is also a Vandermonde matrix, and

$$\det M_i = \prod_{\substack{1 \le r < s \le m \\ r,s \ne i}} (w_s - w_r).$$

Therefore,

$$\det A_{1i} = \frac{w_1 \dots w_m}{w_i} \frac{\prod_{\substack{1 \le r < s \le m \\ r,s \ne i}} (w_s - w_r)}{2! \dots (m-1)!}.$$

□

Since $w_1, \dots, w_m$ are distinct, $\det A \neq 0$. Thus it is valid to plug (2.6) and (2.7) in (2.5), and we conclude that the (unique) solution $(a_{w_1}, \dots, a_{w_m})$ of (2.3) is

$$\begin{aligned}
a_{w_i} &= (-1)^i \frac{w_1 \dots w_m}{w_i} \frac{\prod_{\substack{1 \le r < s \le m \\ r,s \ne i}} (w_s - w_r)}{\prod_{1 \le r < s \le m} (w_s - w_r)} \\
&= (-1)^i \frac{w_1 \dots w_m}{w_i} \frac{1}{\prod_{\substack{1 \le r < s \le m \\ r=i \text{ or } s=i}} (w_s - w_r)} \\
&= (-1)^i \frac{w_1 \dots w_{i-1}}{\prod_{1 \le r < i} (w_i - w_r)} \frac{w_{i+1} \dots w_m}{\prod_{i < s \le m} (w_s - w_i)} \\
&= (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i} \qquad (2.8)
\end{aligned}$$

for all $1 \le i \le m$. Note that (2.8) may also be viewed as a solution of the first m congruence equations in (2.2). Then we shall consider the last congruence equation in (2.2).

Lemma 2.2. *Let a_{w_i}, $1 \le i \le m$, be as set in* (2.8). *Then*

$$\sum_{i=1}^{m} \binom{w_i}{m} a_{w_i} = (-1)^m \frac{w_1 \dots w_m}{m!}. \tag{2.9}$$

Proof. Plug (2.8) in the left hand side of (2.9), we have

$$\begin{aligned}
& \sum_{i=1}^{m} \binom{w_i}{m} a_{w_i} \\
= & \sum_{i=1}^{m} \binom{w_i}{m} (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i} \\
= & \sum_{i=1}^{m} \frac{(b-m+i)\Delta \dots [(b-m+i)\Delta - m+1]}{m!} (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i} \\
= & \sum_{i=1}^{m} \sum_{t=1}^{m} c_t (b-m+i)^t (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i} \\
= & \sum_{t=1}^{m} c_t \sum_{i=1}^{m} (b-m+i)^t (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i},
\end{aligned}$$

where c_t does not depend on i, and $c_m = \Delta^m / m!$. For all integers $1 \le t \le m$,

$$\begin{aligned}
& \sum_{i=1}^{m} (b-m+i)^t (-1)^i \binom{b-m+i-1}{i-1} \binom{b}{m-i} \\
= & \sum_{i=1}^{m} (-1)^i (b-m+i)^{t-1} m \binom{b}{m} \binom{m-1}{i-1} \\
= & m \binom{b}{m} \sum_{i=0}^{m-1} (-1)^{i+1} \binom{m-1}{i} (b-m+1+i)^{t-1} \\
= & \begin{cases} (-1)^m m! \binom{b}{m} & \text{if} \quad t = m, \\ 0 & \text{if} \quad 1 \le t \le m-1. \end{cases}
\end{aligned}$$

The last step above follows from an induction proof on m. Therefore,

$$\sum_{i=1}^{m} \binom{w_i}{m} a_{w_i} = c_m (-1)^m m! \binom{b}{m} = (-1)^m \Delta^m \binom{b}{m} = (-1)^m \frac{w_1 \dots w_m}{m!}.$$

□

Now if (2.1) holds then Lemma 2.2 asserts that (2.8) gives a solution of (2.2), and one direction of the proof is accomplished.

For the other direction, we shall show that if (2.2) has an integer solution then the inequality (2.1) holds. Still let A be the coefficient matrix of (2.3) as set in (2.4). First note that by Lemma 2.1,

$$\det A = \frac{\prod_{1\le r<s\le m}(w_s - w_r)}{2!\dots(m-1)!} = \prod_{r=1}^{m-1}\frac{\prod_{s=r+1}^{m}(w_s - w_r)}{(m-r)!} = \prod_{r=1}^{m-1}\Delta^{m-r} = \Delta^{m(m-1)/2}.$$

Therefore, if $p \nmid \Delta$ then the set of equations (2.3) is still nonsingular when modulo q^{k-m}. Thus in this case, any integer solution of the first m congruences in (2.2) satisfies that

$$a_{w_i} \equiv (-1)^i \binom{b-m+i-1}{i-1}\binom{b}{m-i} \pmod{q^{k-m}}.$$

Consequently the fact that (2.2) has an integer solution implies that

$$(-1)^m \frac{w_1 \dots w_m}{m!} = \sum_{i=1}^{m} \binom{w_i}{m} (-1)^i \binom{b-m+i-1}{i-1}\binom{b}{m-i} \equiv 0 \pmod{q^{k-m}},$$

hence (2.1) holds. Now we assume that $p \mid \Delta$. In other words, $v_p(\Delta) \ge 1$. Suppose $(a_{w_1}, \dots, a_{w_m})$ is an integer solution of (2.2), and write

$$\tilde{A} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & w_1 & w_2 & \dots & w_m \\ 0 & \binom{w_1}{2} & \binom{w_2}{2} & \dots & \binom{w_m}{2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \binom{w_1}{m} & \binom{w_2}{m} & \dots & \binom{w_m}{m} \end{pmatrix}.$$

Then there exist integers s_0, s_1, s_2, …, s_m such that

$$\tilde{A} \begin{pmatrix} 1 \\ a_{w_1} \\ a_{w_2} \\ \vdots \\ a_{w_m} \end{pmatrix} = \begin{pmatrix} s_0 q^k \\ s_1 q^{k-1} \\ s_2 q^{k-2} \\ \vdots \\ s_m q^{k-m} \end{pmatrix} = q^{k-m} \begin{pmatrix} s_0 q^m \\ s_1 q^{m-1} \\ s_2 q^{m-2} \\ \vdots \\ s_m \end{pmatrix}.$$

Therefore,

$$\begin{pmatrix} 1 \\ a_{w_1} \\ a_{w_2} \\ \vdots \\ a_{w_m} \end{pmatrix} = q^{k-m}\tilde{B} \begin{pmatrix} s_0 q^m \\ s_1 q^{m-1} \\ s_2 q^{m-2} \\ \vdots \\ s_m \end{pmatrix}, \tag{2.10}$$

where $\tilde{B}$ is the inverse of $\tilde{A}$. For any integer $0 \leq i \leq m$, write b_i as the $(1, i+1)$-entry of $\tilde{B}$, and write A_i as the $(i+1, 1)$-st minor of $\tilde{A}$. Then the first row of (2.10) gives that

$$1 = q^{k-m}(b_0 s_0 q^m + b_1 s_1 q^{m-1} + b_2 s_2 q^{m-1} + \cdots + b_m s_m), \tag{2.11}$$

where

$$b_i = (-1)^i \frac{\det A_i}{\det \tilde{A}} = (-1)^i \frac{\det A_i}{\det A_0} \tag{2.12}$$

for all $0 \leq i \leq m$. Note that as $w_1, \ldots, w_m$ are nonzero, the following lemma asserts that $\det \tilde{A} = \det A_0 \neq 0$. Thus $\tilde{A}$ is nonsingular, and (2.12) is valid.

Lemma 2.3. *Let A_i be as above set. Then for any integer $0 \leq i \leq m$*

$$\det A_i = \frac{\prod_{1 \leq r < s \leq m}(w_s - w_r)}{2! \ldots m!} \sum_{s=0}^{i} (-1)^s \binom{i}{s} (w_1 - s) \ldots (w_m - s). \tag{2.13}$$

Proof. We shall use induction on i to prove (2.13). For convenience, write

$$\lambda = \frac{\prod_{1 \leq r < s \leq m}(w_s - w_r)}{2! \ldots m!}.$$

By a similar argument as in the proof of Lemma 2.1, $\det A_0 = \lambda w_1 \ldots w_m$. Therefore, Lemma 2.3 is true when $i = 0$. Now assume that for some positive integer i (2.13) holds for all $0 \leq r < i \leq m$, and compute $\det A_i$. Consider the following matrix:

$$M_i = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ i & w_1 & \ldots & w_m \\ \vdots & \vdots & \ddots & \vdots \\ \binom{i}{m} & \binom{w_1}{m} & \ldots & \binom{w_m}{m} \end{pmatrix}.$$

Observe that $\det M_i = \lambda(w_1 - i)\dots(w_m - i)$. On the other hand,

$$\det M_i = \sum_{r=0}^{i}(-1)^r \binom{i}{r} \det A_r.$$

Therefore,

$$\begin{aligned}
&\det A_i \\
= \;& (-1)^i \left(\lambda(w_1 - i)\dots(w_m - i) - \sum_{r=0}^{i-1}(-1)^r \binom{i}{r} \det A_r \right) \\
= \;& (-1)^i \lambda \left((w_1 - i)\dots(w_m - i) - \sum_{r=0}^{i-1}(-1)^r \binom{i}{r} \sum_{s=0}^{r}(-1)^s \binom{r}{s} (w_1 - s)\dots(w_m - s) \right) \\
= \;& (-1)^i \lambda \left((w_1 - i)\dots(w_m - i) - \sum_{s=0}^{i-1}(-1)^s (w_1 - s)\dots(w_m - s) \sum_{r=s}^{i-1}(-1)^r \binom{i}{r}\binom{r}{s} \right) \\
= \;& (-1)^i \lambda \left((w_1 - i)\dots(w_m - i) - \sum_{s=0}^{i-1}(-1)^s (w_1 - s)\dots(w_m - s)(-1)^{i-1} \binom{i}{s} \right) \\
= \;& \lambda \sum_{s=0}^{i}(-1)^s \binom{i}{s} (w_1 - s)\dots(w_m - s),
\end{aligned}$$

as desired. By induction, Lemma 2.3 is true for all $0 \le i \le m$. □

Plugging (2.13) in (2.12), we get

$$b_i = (-1)^i \frac{\sum_{s=0}^{i}(-1)^s \binom{i}{s} (w_1 - s)\dots(w_m - s)}{w_1 \dots w_m}$$

for all $0 \le i \le m$. Write

$$t_i = \frac{1}{i!} \sum_{s=0}^{i}(-1)^s \binom{i}{s} (w_1 - s)\dots(w_m - s).$$

Then (2.11) becomes

$$1 = q^{k-m} \frac{\sum_{i=0}^{m}(-1)^i \frac{i!}{m!} t_i s_i q^{m-i}}{\frac{w_1 \dots w_m}{m!}}.$$

Therefore,

$$\frac{w_1 \dots w_m}{m!} = q^{k-m} \sum_{i=0}^{m}(-1)^i \frac{i!}{m!} t_i s_i q^{m-i}.$$

Now in order that inequality (2.1) holds, it suffices to show that

$$v_p(t_i) \geq v_p\left(\frac{m!}{i!}\right) - l(m-i) \tag{2.14}$$

for all $0 \leq i \leq m$.

Lemma 2.4. *For $1 \leq j \leq m$, let the number*

$$\sigma_m(j) = \sum_{1 \leq \alpha_1 < \cdots < \alpha_j \leq m} \alpha_1 \ldots \alpha_j$$

be the summation of all products of j distinct numbers in $\{1, \ldots, m\}$. Then the p-adic valuation of $\sigma_m(j)$ satisfies

$$v_p(\sigma_m(j)) \geq v_p\left(\frac{m!}{(m-j)!}\right) - \frac{2j}{p-1}.$$

Proof. First we prove by induction on j that

$$\sigma_m(j) = \sum_{i=1}^{j} l_{j,i} \binom{m+1}{j+i}, \tag{2.15}$$

where the coefficients

$$l_{j,i} = \begin{cases} j! & \text{if} \quad i = 1, \\ (2j-1)!! & \text{if} \quad i = j, \\ (i+j-1)(l_{j-1,i} + l_{j-1,i-1}) & \text{if} \quad 2 \leq i \leq j-1. \end{cases} \tag{2.16}$$

Note that we may recursively decide from (2.16) the value of $l_{j,i}$ for any $1 \leq i \leq j \leq m$. Note also that (2.16) asserts that all $l_{j,1}$'s and $l_{i,i}$'s are integers. Moreover, any $l_{j,i}$ is an integer as long as the "previous" $l_{j-1,i}$ and $l_{j-1,i-1}$ are both integers. Therefore, if (2.16) is satisfied then all $l_{j,i}$'s are integers. Since

$$\sigma_m(1) = \sum_{i=1}^{m} i = \binom{m+1}{2},$$

(2.15) holds for the base case $j = 1$. Assume that (2.15) is true for $\sigma_m(j-1)$. Note the fact that the difference between $\sigma_m(j)$ and $\sigma_{m-1}(j)$ is exactly $m\sigma_{m-1}(j-1)$. Thus we may deduce that

$$\begin{aligned}
&\sigma_m(j)-\sigma_{m-1}(j)\\
= \;& m\sum_{i=1}^{j-1} l_{j-1,i}\binom{m}{j+i-1}\\
= \;& \sum_{i=1}^{j-1}(m-j-i+1)l_{j-1,i}\binom{m}{j+i-1}+\sum_{i=1}^{j-1}(j+i-1)l_{j-1,i}\binom{m}{j+i-1}\\
= \;& \sum_{i=1}^{j-1}(j+i)l_{j-1,i}\binom{m}{j+i}+\sum_{i=1}^{j-1}(j+i-1)l_{j-1,i}\binom{m}{j+i-1}\\
= \;& \sum_{i=2}^{j}(j+i-1)l_{j-1,i-1}\binom{m}{j+i-1}+\sum_{i=1}^{j-1}(j+i-1)l_{j-1,i}\binom{m}{j+i-1}\\
= \;& \sum_{i=2}^{j-1}(i+j-1)(l_{j-1,i-1}+l_{j-1,i})\binom{m}{j+i-1}+jl_{j-1,1}\binom{m}{j}+(2j-1)l_{j-1,j-1}\binom{m}{2j-1}\\
= \;& \sum_{i=1}^{j} l_{j,i}\binom{m}{j+i-1}.
\end{aligned}$$

So as $\sigma_j(j)=j!$, we have

$$\begin{aligned}
\sigma_m(j) &= \sigma_j(j)+\sum_{k=j}^{m-1}(\sigma_{k+1}(j)-\sigma_k(j))\\
&= j!+\sum_{k=j}^{m-1}\sum_{i=1}^{j} l_{j,i}\binom{k+1}{j+i-1}\\
&= \sum_{i=1}^{j} l_{j,i}\left(\binom{j+1}{j+i}+\sum_{k=j}^{m-1}\binom{k+1}{j+i-1}\right)\\
&= \sum_{i=1}^{j} l_{j,i}\binom{m+1}{j+i}.
\end{aligned}$$

Therefore (2.15) holds for all integers $1\le j\le m$. Note that $v_p(n!)\le(n-1)/(p-1)$ for all positive integers n, which follows from Legendre's formula [UH39]: $v_p(n!)=\sum_{r=1}^{\infty}\lfloor n/p^r\rfloor$. Thus for each term in the above summation, the p-adic valuation

$$\begin{aligned}
v_p\left(\binom{m+1}{j+i}\right) &\ge v_p\left(\frac{m!}{(m-j)!}\right)-v_p((j+i)!)\\
&\ge v_p\left(\frac{m!}{(m-j)!}\right)-\frac{2j}{p-1}
\end{aligned}$$

for $1 \leq i \leq j$. Since all the coefficients $l_{j,i}$'s are integers, $\sigma_m(j)$ has a p-adic valuation no less than this. □

As an extension of Lemma 2.4 we consider arbitrary consecutive integers $b-m+1, \ldots, b$ instead of the first m consecutive integers. Let $\tilde{\sigma}_m(j)$ denote the summation of all products of j numbers in these m integers. Then

$$\begin{aligned}\tilde{\sigma}_m(j) &= \sum_{1\leq\alpha_1<\cdots<\alpha_j\leq m} (b-m+\alpha_1)\ldots(b-m+\alpha_j) \\ &= \sum_{s=0}^{j}(b-m)^{j-s}\binom{m-s}{j-s}\sigma_m(s).\end{aligned}$$

For each term in the above summation, the p-adic valuation

$$\begin{aligned}& v_p\left(\binom{m-s}{j-s}\sigma_m(s)\right) \\ \geq\ & v_p\left(\frac{(m-s)!}{(j-s)!(m-j)!}\right) + v_p\left(\frac{m!}{(m-s)!}\right) - \frac{2s}{p-1} \\ =\ & v_p\left(\frac{m!}{(m-j)!}\right) - v_p((j-s)!) - \frac{2s}{p-1} \\ \geq\ & v_p\left(\frac{m!}{(m-j)!}\right) - \frac{j-s}{p-1} - \frac{2s}{p-1} \\ \geq\ & v_p\left(\frac{m!}{(m-j)!}\right) - \frac{2j}{p-1}.\end{aligned}$$

Thus for $\tilde{\sigma}_m(j)$ we still have

$$v_p(\tilde{\sigma}_m(j) \geq v_p\left(\frac{m!}{(m-j)!}\right) - \frac{2j}{p-1}.$$

Moreover, suppose $W_m(j)$ is the summation of all products of j numbers in $\{w_1, \ldots, w_m\}$. Remember that $w_1, \ldots, w_m$ are consecutive multiples of Δ. Thus

$$W_m(j) = \sum_{1\leq\alpha_1<\cdots<\alpha_j\leq m} w_{\alpha_1}\ldots w_{\alpha_j} = \Delta^j\tilde{\sigma}_m(j).$$

By the assumption that $v_p(\Delta) \geq 1$, we have

$$v_p(W_m(j)) \geq v_p\left(\frac{m!}{(m-j)!}\right) - \frac{j}{p-1}. \tag{2.17}$$

Now turn back to look at

$$\begin{aligned} t_i &= \frac{1}{i!}\sum_{s=0}^{i}(-1)^s\binom{i}{s}(w_1-s)\dots(w_m-s) \\ &= \frac{1}{i!}\sum_{s=0}^{i}(-1)^s\binom{i}{s}\sum_{j=0}^{m}(-s)^{m-j}W_m(j) \\ &= (-1)^{m+i}\sum_{j=0}^{m}(-1)^jW_m(j)\left(\frac{1}{i!}\sum_{s=0}^{i}(-1)^{i-s}s^{m-j}\binom{i}{s}\right) \\ &= (-1)^{m+i}\sum_{j=0}^{m-i}(-1)^jW_m(j)S(m-j,i), \qquad (2.18) \end{aligned}$$

where $S(m-j,i)$ represents the Stirling number of the second kind [LW92]. As a matter of fact,

$$S(m-j,i)=\frac{(m-j)!}{i!}\sum\frac{1}{r_1!\dots r_i!},$$

where the summation runs over the partitions $r_1+\dots+r_i$ of $m-j$ into i nonzero parts. Since

$$v_p(r_1!\dots r_i!)\le\frac{r_1-1}{p-1}+\dots+\frac{r_i-1}{p-1}=\frac{m-j-i}{p-1},$$

we deduce that

$$v_p(S(m-j,i))\ge v_p\left(\frac{(m-j)!}{i!}\right)-\frac{m-j-i}{p-1}.$$

Together with (2.17), the p-adic valuation of each term in the summation of (2.18) is at least

$$v_p\left(\frac{m!}{(m-j)!}\right)-\frac{j}{p-1}+v_p\left(\frac{(m-j)!}{i!}\right)-\frac{m-j-i}{p-1}\ge v_p\left(\frac{m!}{i!}\right)-l(m-i).$$

Therefore, the p-adic valuation of t_i is no less than this, hence (2.14) holds as desired.

Now the main theorem of this section is established.

Theorem 2.5. *Suppose $w_1=(b-m+1)\Delta$, ..., $w_m=b\Delta$ are m consecutive multiples of the divisor Δ. Then Ward's bound*[1]

$$k\le m\left(\frac{v_p(\Delta)}{l}+1\right)+\frac{1}{l}\,v_p\left(\binom{b}{m}\right)$$

[1] Though it does not involve a code, we call the inequality Ward's bound because the right hand side is exactly of the form of Ward's bound.

holds if and only if the set of congruence equations

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &\equiv -1 \pmod{q^k} \\ \binom{w_1}{j} a_{w_1} + \cdots + \binom{w_m}{j} a_{w_m} &\equiv 0 \pmod{q^{k-j}}, \quad j = 1, 2, \ldots, m \end{aligned}$$

has an integer solution $(a_{w_1}, \ldots, a_{w_m})$.

2.1.2 Further Comments

Note that Theorem 2.5 gives an equivalent condition for Ward's bound: that is, the set of congruence equations (2.2) has an integer solution. Moreover, (2.2) is partial of

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &\equiv -1 \qquad \pmod{q^k} \\ \tbinom{w_1}{j} a_{w_1} + \cdots + \tbinom{w_m}{j} a_{w_m} &\equiv 0 \qquad \pmod{q^{k-j}}, \quad j = 1, 2, \ldots, k-1, \end{aligned} \tag{2.19}$$

and $(a_{w_1}, \ldots, a_{w_m})$ is an integer solution of (2.19) if and only if the MacWilliams transform

$$w^{\perp}(x) = \frac{1}{q^k}(1 + (q-1)x)^n w\left(\frac{1-x}{1+(q-1)x}\right) \tag{2.20}$$

of $w(x) = 1 + a_{w_1}x^{w_1} + \cdots + a_{w_m}x^{w_m}$ has integer coefficients, as is implied by Theorem 2.6 below. The parameter n in (2.20) is an integer no less than the degree of $w(x)$.

Theorem 2.6 (Wilson [Wil03]). *Let* a_0, a_1, …, a_n *be integers, let* r, k, *and* s *be positive integers, and let* $w(x) = \sum_{i=0}^{n} a_i x^i$. *Then*

$$\frac{1}{r^k}(1 + (r^s - 1)x)^n w\left(\frac{1-x}{1+(r^s-1)x}\right)$$

has integer coefficients if and only if

$$\sum_{i=0}^{n} a_i \binom{i}{j} \equiv 0 \pmod{r^{k-sj}}$$

for all $j = 0, 1, \ldots, \lfloor k/s \rfloor$.

The proof of the theorem is due to Wilson, employing merely elementary linear algebra. Apply Theorem 2.6 with $r = q$ and $s = 1$, we conclude that (2.19) is solvable if and only if (2.20) has integer coefficients.

Suppose C is an $[n,k]_q$ code of weight spectrum $\{w_1,\ldots,w_m\}$, and suppose there are a_{w_i}, $1 \le i \le m$, codewords of weight w_i. Let $w(x) = 1 + a_{w_1}x^{w_1} + \cdots + a_{w_m}x^{w_m}$ denote the weight enumerator of C, let $w^\perp(x)$ denote the MacWilliams transform of $w(x)$, and let $C^\perp$ denote the dual code of C. We summarize this section as follows:

$$\begin{tikzcd}
\text{C is a linear code} \arrow[d, Rightarrow] & \\
\text{$w^\perp(x)$ is the weight enumerator of $C^\perp$} \arrow[d, Rightarrow] & \\
\text{$w^\perp(x)$ has integer coefficients} \arrow[r, Leftrightarrow, "\text{Theorem 2.6}"] & \text{(2.19) has an integer solution} \arrow[d, Rightarrow] \\
\text{Ward's bound holds} \arrow[r, Leftrightarrow, "\text{Theorem 2.5}"] & \text{(2.2) has an integer solution}
\end{tikzcd}$$

This figure clearly shows that Ward's bound follows from the linearity of the code. More precisely, Ward's bound is a consequence of the fact that the MacWilliams transform of the weight enumerator has integer coefficients. However, the integrality of the MacWilliams transform of the weight enumerator implies more than Ward's bound, as is shown by the following example:

Example. Let $p = q = 2$ and $m = 3$. Suppose $w_1 = 6$, $w_2 = 9$, $w_3 = 12$, and $k = 5$. Then Ward's bound is attained:

$$v_p\left(\frac{w_1w_2w_3}{3!}\right) = 2 = k - m.$$

In other words, if C is a binary linear code with nonzero weights 6, 9, and 12, then Ward's bound asserts that $\dim C \le 5$. On the other hand, the MacWilliams transform of the weight enumerator $w(x) = 1 + a_{w_1}x^{w_1} + a_{w_2}x_{w_2} + a_{w_3}x^{w_3}$ has integer coefficients if and only if the following congruences are satisfied:

$$\begin{array}{rcl}
a_{w_1} + a_{w_2} + a_{w_3} & \equiv & -1 \pmod{32} \\
6a_{w_1} + 9a_{w_2} + 12a_{w_3} & \equiv & 0 \pmod{16} \\
15a_{w_1} + 36a_{w_2} + 66a_{w_3} & \equiv & 0 \pmod{8} \\
20a_{w_1} + 84a_{w_2} + 220a_{w_3} & \equiv & 0 \pmod{4} \\
15a_{w_1} + 126a_{w_2} + 465a_{w_3} & \equiv & 0 \pmod{2}
\end{array} \quad .$$

Simplifying the above congruences, we get

$$a_{w_1} + a_{w_2} + a_{w_3} \equiv -1 \pmod{32}, \tag{2.21}$$

$$6a_{w_1} + 9a_{w_2} + 12a_{w_3} \equiv 0 \pmod{16}, \tag{2.22}$$

$$7a_{w_1} + 4a_{w_2} + 2a_{w_3} \equiv 0 \pmod{8}, \tag{2.23}$$

$$a_{w_1} + a_{w_3} \equiv 0 \pmod{2}. \tag{2.24}$$

By (2.23), a_{w_1} is even. Then a_{w_3} is also even by (2.24), and a_{w_2} is odd by (2.21). However, a_{w_2} is even by (2.22), which is a contradiction. Therefore, the whole set of all $k = 5$ congruence equations has no integer solution. Thus in this special case, the integrality of the MacWilliams transform implies more than Ward's bound, and the bound may be improved to $\dim C \leq 4$. However, this is still not the exact bound for binary linear codes with weight spectrum $6, 9, 12$, as linearity of the code implies more than integrality of the MacWilliams transform of the weight enumerator. As in this example, $6, 9, 12$ are multiples of the divisor $\Delta = 3$, and it is relatively prime to the field characteristic $p = 2$. Therefore, a binary linear code C with weight spectrum $6, 9, 12$ must be equivalent to a 3-folded replication of a binary linear code with weight spectrum $2, 3, 4$, and such a code has dimension at most 3.

Though generally Ward's bound (2.1) does not imply (2.19) being solvable, it is the case for single and double weighted codes. That is, for linear code C of one or two nonzero weights, Ward's bound holds if and only if the MacWilliams transform of the weight enumerator of C has integer coefficients, if and only if the set of congruence equations (2.19) has an integer solution, as is shown by the following theorem:

Theorem 2.7. *When $m = 1$ or 2, Ward's bound* (2.1) *holds if and only if the set of congruences* (2.19) *has an integer solution.*

Proof. Theorem 2.5 asserts that if (2.19) is solvable then Ward's bound (2.1) holds. Now it suffices to show the other direction that (2.1) implies (2.19) being solvable.

For $m = 1$, (2.1) says that $v_p(w_1) \geq l(k-1)$. Then for all integers $1 \leq j \leq k-1$,

$$v_p\left(\binom{w_1}{j}\right) = v_p\left(\frac{w_1}{j}\binom{w_1 - 1}{j-1}\right) \geq v_p(w_1) - v_p(j) \geq l(k-1) - l(j-1) = l(k-j).$$

Thus $a_{w_1} = -1$ is a solution of (2.19).

Now assume $m = 2$. Then (2.1) says that

$$v_p\left(\frac{w_1 w_2}{2}\right) \geq l(k-2).$$

By (2.8) and Lemma 2.2, $a_{w_1} = -b$, $a_{w_2} = b-1$ is a solution of (2.2). We claim that this is also a solution of (2.19), and it suffices to check the remaining congruences in (2.19) where $3 \leq j \leq k-1$. Note that

$$\begin{aligned} & \binom{w_1}{j} a_{w_1} + \binom{w_2}{j} a_{w_2} \\ = \quad & -\frac{w_1}{j}\binom{w_1-1}{j-1} b + \frac{w_2}{j}\binom{w_2-1}{j-1}(b-1) \\ = \quad & \frac{w_1 w_2}{j!}\left(\frac{(w_1+\Delta-1)\ldots(w_1+\Delta-t+1)-(w_1-1)\ldots(w_1-t+1)}{\Delta}\right). \end{aligned}$$

Since $\Delta \mid (w_1+\Delta-1)\ldots(w_1+\Delta-t+1)-(w_1-1)\ldots(w_1-t+1)$, we have

$$v_p\left(\binom{w_1}{j} a_{w_1} + \binom{w_2}{j} a_{w_2}\right) \geq v_p\left(\frac{w_1 w_2}{j!}\right) = v_p(w_1 w_2) - v_p(j!).$$

If $p = 2$, then

$$v_p(w_1 w_2) = v_p\left(\frac{w_1 w_2}{2}\right) + 1 \geq l(k-2) + 1, \quad v_p(j!) \leq j-1 \leq l(j-2)+1.$$

If $p \neq 2$, then

$$v_p(w_1 w_2) = v_p\left(\frac{w_1 w_2}{2}\right) \geq l(k-2), \quad v_p(j!) \leq \frac{j-1}{2} \leq l(j-2).$$

Therefore, we always have $v_p(w_1 w_2) - v_p(j!) \geq l(k-j)$, hence $a_{w_1} = -b$, $a_{w_2} = b-1$ is indeed a solution of (2.19). □

Note that the previous example shows that for triple-weighted codes, we do not have similar results as given by Theorem 2.7.

2.2 An Analogous Bound on Binary $\mathbb{Z}_4$-Linear Codes

In the previous section, we conclude that Ward's bound is a consequence of the fact that the MacWilliams transform of the weight enumerator has integer coefficients. Thus the linearity of the code is just a sufficient, but not a necessary, condition for Ward's bound being held. For some nonlinear codes with the property that the weight enumerator has integral MacWilliams transform, Ward's bound still holds, though in such cases the concept of "dimension" is meaningless. As a matter of fact, for a q-ary (nonlinear) code C, we bound $\log_q |C|$ instead of $\dim C$, where $|C|$ denotes the size of the code, that is, the number of codewords in C.

In this section, we first introduce $\mathbb{Z}_4$-linear codes, then show that binary codes obtained from $\mathbb{Z}_4$-linear codes are examples of such codes that their weight enumerators have integral MacWilliams transforms. Finally we develop a bound for these codes analogous to Ward's bound for linear codes.

2.2.1 $\mathbb{Z}_4$-Linear Codes

Let $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ be the ring of integers modulo 4, let n be a positive integer, and let $\mathbb{Z}_4^n$ be the set of n-tuples over $\mathbb{Z}_4$. $\mathbb{Z}_4^n$ is an additive Abelian group, where addition is defined componentwise as $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$, for all $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in $\mathbb{Z}_4^n$. Any subgroup $\tilde{C}$ of $\mathbb{Z}_4^n$ is called a $\mathbb{Z}_4$-*linear code* of *length* n. Note that the size of any $\mathbb{Z}_4$-linear code $\tilde{C}$ must be a power of 2.

For any $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{Z}_4^n$, define their *inner product* as $a \cdot b = a_1 b_1 + \cdots + a_n b_n$. If $a \cdot b = 0$, a and b are said to be *orthogonal*. Suppose $\tilde{C}$ is a $\mathbb{Z}_4$-linear code of length n. Define the *dual code* of $\tilde{C}$ to be

$$\tilde{C}^{\perp} = \{c \in \mathbb{Z}_4^n : c \cdot \tilde{c} = 0, \text{ for all } \tilde{c} \in \tilde{C}\},$$

which is also a $\mathbb{Z}^4$-linear code.

We use 0, 1, 2, 3 to represent the elements in $\mathbb{Z}_4$. The *Lee weights* of $0, 1, 2, 3 \in \mathbb{Z}_4$, denoted by $w_L(0)$, $w_L(1)$, $w_L(2)$, $w_L(3)$, respectively, are defined as

$$w_L(0) = 0, \quad w_L(1) = w_L(3) = 1, \quad w_L(2) = 2.$$

The *Lee weight* $w_L(c)$ of any $c = (c_1, \ldots, c_n) \in \mathbb{Z}_4^n$ is defined as $w_L(c) = \sum_{i=1}^n w_L(c_i)$, the summation of the Lee weights of all its components. Then the *Lee weight enumerator* of a

$\mathbb{Z}_4$-linear code $\tilde{C}$ of length n is defined to be

$$\mathrm{Lee}_{\tilde{C}}(x) = \sum_{\tilde{c} \in \tilde{C}} x^{w_L(\tilde{c})} = \sum_{i=0}^{2n} L_i x^i,$$

where L_i, $0 \leq i \leq 2n$, represents the number of codewords of Lee weight i in $\tilde{C}$. Note that there is a generalization of the MacWilliams identity for $\mathrm{Lee}_{\tilde{C}}$.

Theorem 2.8 ([Wan97]). *Let $\tilde{C}$ be a $\mathbb{Z}_4$-linear code of length n. Then*

$$\mathrm{Lee}_{\tilde{C}^{\perp}}(x) = \frac{1}{|\tilde{C}|}(1+x)^{2n}\mathrm{Lee}_{\tilde{C}}\left(\frac{1-x}{1+x}\right). \tag{2.25}$$

Note that the right hand side of (2.25) may be viewed as the MacWilliams transform of $\mathrm{Lee}_{\tilde{C}}(x)$. Thus Theorem 2.8 says that the Lee weight enumerator of the dual code is exactly the MacWilliams transform of the Lee weight enumerator of the original $\mathbb{Z}_4$-linear code. Since any Lee weight enumerator must have integer coefficients, we are interested in binary codes whose weight enumerator equals the Lee weight enumerator of some $\mathbb{Z}_4$-linear code.

2.2.2 Binary Images of $\mathbb{Z}_4$-Linear Codes

Consider the following bijection from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$:

$$\begin{array}{rccc} \phi: & \mathbb{Z}_4 & \longrightarrow & \mathbb{F}_2^2 \\ & 0 & \mapsto & 00 \\ & 1 & \mapsto & 01 \\ & 2 & \mapsto & 11 \\ & 3 & \mapsto & 10 \end{array}.$$

ϕ is called the *Gray map*. Extend ϕ to a bijection from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$ and denote the map as

$$\begin{array}{rccc} \tilde{\phi}: & \mathbb{Z}_4^n & \longrightarrow & \mathbb{F}_2^{2n} \\ & (c_1, \ldots, c_n) & \mapsto & (\phi(c_1), \ldots, \phi(c_n)) \end{array}.$$

Then $\tilde{\phi}$ maps any $\mathbb{Z}_4$-linear code $\tilde{C}$ of length n to a binary code $C = \tilde{\phi}(\tilde{C})$ of length $2n$, and generally C is not linear. C is called the *binary image* of $\tilde{C}$ under the Gray map, or simply, the binary image of $\tilde{C}$. Moreover, a binary code C is called $\mathbb{Z}_4$-*linear* if after a permutation of its coordinates, it is the binary image of a $\mathbb{Z}_4$-linear code. The Nordstrom-Robinson code, the Preparata codes, the Kerdock codes, the Geothals codes, and the Delsarte-Geothals codes are all examples of binary codes that exhibit $\mathbb{Z}_4$-linearity.

One of the advantages of the Gray map is that the Hamming weight of any binary image is exactly the Lee weight of its pre-image. As a result, there is an analogous theorem directly deduced from Theorem 2.8.

Theorem 2.9 ([Wan97]). *Let $\tilde{C}$ be a $\mathbb{Z}_4$-linear code of length n, and let $\tilde{C}^\perp$ be its dual code. Let $C = \tilde{\phi}(\tilde{C})$ and $C^\perp = \tilde{\phi}(\tilde{C}^\perp)$ be their binary images. Then the (Hamming) weight enumerators $w_C(x)$ and $w_{C^\perp}(x)$ of C and $C^\perp$, respectively, are related by the binary MacWilliams identity*

$$w_{C^\perp}(x) = \frac{1}{|C|}(1+x)^{2n} w_C\left(\frac{1-x}{1+x}\right).$$

2.2.3 Bounds on Binary $\mathbb{Z}_4$-Linear Codes

Here we present an application of Theorem 2.5 to binary $\mathbb{Z}_4$-linear codes, which is given by the following corollary:

Corollary 2.10. *Let C be a binary $\mathbb{Z}_4$-linear code of length $2n$ and size 2^k. Suppose the nonzero weights of C are among the m consecutive multiples $w_1 = (b-m+1)\Delta$, ..., $w_m = b\Delta$ of the divisor Δ. Then the size of C is bounded from above by*

$$k \leq m(v_2(\Delta)+1) + v_2\left(\binom{b}{m}\right). \tag{2.26}$$

Proof. By Theorem 2.9, the MacWilliams transform of the weight enumerator $w_C(x)$ has integer coefficients. Thus by Theorem 2.6, there exist integers $a_{w_1}, \ldots, a_{w_m}$ such that

$$\begin{aligned} a_{w_1} + \cdots + a_{w_m} &\equiv -1 \pmod{2^k} \\ \binom{w_1}{j} a_{w_1} + \cdots + \binom{w_m}{j} a_{w_m} &\equiv 0 \pmod{2^{k-j}}, \quad \text{for all } 1 \leq j \leq k-1. \end{aligned}$$

Therefore, Theorem 2.5 asserts bound (2.26). □

Chapter 3

Weights Modulo a Prime Power and a Related Bound

We continue to discuss bounds on dimensions of divisible codes in this chapter. Recall that Ward's bound is determined by the weight spectrum. In other words, absence of intermediate weights does not affect the bound. However, we see from the following example that the bound may be improved dramatically if some certain weights are missing from the spectrum.

Example. Let C be a binary k-dimensional level e divisible code whose nonzero weights are among the odd multiples of 2^e. Suppose there are a_i codewords of weight $(2i-1)2^e$, for all positive integers i. Then consider the first two congruence equations in (2.19):

$$\begin{aligned} \sum_{i\geq 1} a_i &\equiv -1 \pmod{2^k}, && (3.1) \\ \sum_{i\geq 1} (2i-1)2^e a_i &\equiv 0 \pmod{2^{k-1}}. && (3.2) \end{aligned}$$

Since $\sum_{i\geq 1} a_i$ and $\sum_{i\geq 1}(2i-1)a_i$ are of the same parity, (3.1) gives that $\sum_{i\geq 1}(2i-1)a_i$ is odd. Therefore, $e \geq k-1$ by (3.2), hence $\dim C \leq e+1$ no matter how wide the weight spectrum is. Thus this is a much better bound than Ward's bound.

Our main goal in this chapter is to improve Ward's bound, at least when additional information on the weight distribution is given.

Note first that nondivisible linear codes may be regarded as level zero codes. The following theorem gives a sufficient condition for the weights modulo p^t in a level zero q-ary code being divisible by p^s:

Theorem 3.1 (Wilson [Wil03]). *Suppose C is a q-ary linear code. Let $N(j, p^t)$ denote the number of codewords in C that have weights congruent to j modulo p^t. If*

$$\dim C \geq (s(p-1)+1)p^{t-1}$$

then $N(j, p^t) \equiv 0 \pmod{p^s}$ for all integers j.

Theorem 3.1 actually gives an upper bound for the dimension of a linear code with $N(j, p^t) \not\equiv 0 \pmod{p^s}$ for some j. In other words, if there exist integers j, t, and s such that $N(j, p^t) \not\equiv 0 \pmod{p^s}$ for a q-ary linear code C then the dimension of C is bounded from above by $(s(p-1)+1)p^{t-1} - 1$. As a first attempt to improve Ward's bound, we generalize this result in Section 3.1 to level e divisible codes, where e can be any positive integer. This generalized result is called *weights modulo a prime power in divisible codes.* The proof of Theorem 3.1 is based on the following lemma, which is also essential in our generalization.

Lemma 3.2 (Wilson [Wil03]). *Let t and s be positive integers, and let f be an integer-valued function on the integers that is periodic of period p^t. Then there exists a polynomial*

$$w(x) = c_0 + c_1 x + c_2 \binom{x}{2} + \cdots + c_d \binom{x}{d}$$

of degree $d \leq (e(p-1)+1)p^{t-1} - 1$ so that $w(j) \equiv f(j) \pmod{p^s}$ for all integers j. The coefficients c_i are integers, and $c_i \equiv 0 \pmod{p^m}$ whenever $i \geq (m(p-1)+1)p^{t-1}$.

The result on weights modulo a prime power in divisible codes, by a similar reason, gives an upper bound on dimension of divisible codes with $N(j, p^t) \not\equiv 0 \pmod{p^s}$ for some j. In Section 3.2 we further "generalize" this upper bound of level e divisible codes, and it turns out that the bound is determined by the order of $1 - x^{p^e}$ in the weight enumerator modulo p^s. We call this new bound a *related bound*, and show that this generalized bound implies Ward's bound.

In Section 3.3 we compare Ward's bound, the related bound, and the bound following from weights modulo a prime power in divisible codes. Moreover, we present several applications of the related bound and the bound from weights modulo a prime power, which give better results than Ward's bound in certain cases.

3.1 Weights Modulo a Prime Power in Divisible Codes

In this section, our goal is to generalize Theorem 3.1 about weights modulo a prime power in linear codes to a divisible code version. Before stating our main theorem, we give the following lemma:

Lemma 3.3. *Suppose C is an $[n,k]_q$ code. Let $f(x) = x_{i_1}^{a_1} \dots x_{i_r}^{a_r}$, $x = (x_1, \dots, x_n)$, be a monomial defined on $\{0,1\}^n$ with $a_j \geq 1$ for all $1 \leq j \leq r$. Define c^* for each n-tuple $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ as $c^* = (|c_1|, \dots, |c_n|)$, where $|c_i| = 0$ if $c_i = 0$, and $|c_i| = 1$ if $c_i \neq 0$ for all $1 \leq i \leq n$. Then*

$$\sum_{c \in C} f(c^*) \equiv 0 \pmod{q^{k-r}}.$$

Proof. Let C_0 be the subcode of C that vanishes on the r coordinates $x_{i_1}, \dots, x_{i_r}$. Note that C_0 is the kernel of the linear projection of C on the corresponding r-dimensional space. Therefore, $\dim C_0 \geq k - r$. Since f takes the same value on any coset of C_0, we have

$$\sum_{c \in C} f(c^*) \equiv 0 \pmod{q^{k-r}},$$

as desired. □

Throughout this section, e represents a nonnegative integer, C is set to be a q-ary level e divisible code,[1] and $N(j, p^m)$ denotes the number of codewords in C that have weights congruent to j modulo p^m. Since all codeword weights of C are divisible by p^e, we have $N(j, p^m) = 0$ for all m, j such that $m \geq e$ and $j \not\equiv 0 \pmod{p^e}$. Therefore, we are interested in a condition for the dimension of C that asserts that all the numbers $N(jp^e, p^{e+t})$ are always divisible by p^e. This result, as a generalization of Theorem 3.1, is the main theorem of this section, which is called weights modulo a prime power in divisible codes.

Theorem 3.4. *If the dimension of C satisfies*

$$\dim C > (\frac{e}{l} + 1)[(s(p-1)+1)p^{t-1} - 1],$$

then $N(jp^e, p^{e+t}) \equiv 0 \pmod{p^s}$ for all integers j.

[1] Actually we may assume that C is divisible by p^e. That is, the divisibility level of C is *at least* e. However, it does not affect our result whether C is assumed to be of level exactly e or at least e.

Proof. Theorem 3.1 asserts the $e = 0$ case.

Now we assume that $e \geq 1$. By Lemma 3.2, there exists a polynomial

$$\begin{aligned} g(z) &= \sum_{i=0}^{(s(p-1)+1)p^{t-1}-1} c_i \binom{z-1}{i} \\ &\equiv \begin{cases} 1 \pmod{p^s} & \text{if } z \equiv j \pmod{p^t}, \\ 0 \pmod{p^s} & \text{otherwise,} \end{cases} \end{aligned}$$

where $c_i \equiv 0 \pmod{p^m}$ whenever $i \geq (m(p-1)+1)p^{t-1}$. Let $f(x) = g((x_1 + \cdots + x_n)/p^e)$, and let c^* be as defined in Lemma 3.3. Then $N(jp^e, p^{e+t}) \equiv \sum_{c \in C} f(c^*) \pmod{p^s}$.

For each term

$$c_i \binom{z-1}{i}, \quad 0 \leq i \leq (s(p-1)+1)p^{t-1} - 1,$$

in $g(z)$ the corresponding term in $f(x)$ is

$$c_i \binom{(x_1 + \cdots + x_n)/p^e - 1}{i} = \frac{c_i}{i!\, p^{ei}}(x_1 + \cdots + x_n - p^e) \ldots (x_1 + \cdots + x_n - i\, p^e).$$

The coefficient of the monomial $x_{j_1}^{a_1} \ldots x_{j_r}^{a_r}$, $a_1, \ldots, a_r \geq 1$, is

$$\frac{c_i}{i!\, p^{ei}} (-1)^u \frac{(i-u)!}{a_1! \ldots a_r!} \sigma_i(u) p^{eu},$$

where $u = i - (a_1 + \cdots + a_r)$, and $\sigma_i(u)$ is as defined in Lemma 2.4. Then the p-adic valuation of the coefficient is at least

$$\begin{aligned} & v_p\left(\frac{c_i}{i!\, p^{ei}} \frac{(i-u)!}{a_1! \ldots a_r!}\right) + v_p\left(\frac{i!}{(i-u)!}\right) - \frac{2u}{p-1} + eu \\ \geq\ & v_p(c_i) - \frac{a_1 - 1}{p-1} - \cdots - \frac{a_r - 1}{p-1} - ei - \frac{2u}{p-1} + eu \\ =\ & v_p(c_i) - i(e + \frac{1}{p-1}) + (e - \frac{1}{p-1})u + \frac{r}{p-1} \\ \geq\ & -(e + \frac{1}{p-1})[(s(p-1)+1)p^{t-1} - 1] + \frac{r}{p-1}. \end{aligned}$$

Note that $0 \leq r \leq (s(p-1)+1)p^{t-1} - 1$. So the number

$$l(\dim C - r) - (e + \frac{1}{p-1})[(s(p-1)+1)p^{t-1} - 1] + (s-1) + \frac{r}{p-1}$$

attains its minimum

$$l \dim C - (e+l)[(s(p-1)+1)p^{t-1}-1] + (e-1)$$

when $r = (s(p-1)+1)p^{t-1}-1$. Hence by Lemma 3.3,

$$\sum_{c \in C} f(c^*) \equiv 0 \pmod{p^{l \dim C - (e+l)[(s(p-1)+1)p^{t-1}-1]+(e-1)}}.$$

Therefore, if we have

$$\dim C > (\frac{e}{l}+1)[(s(p-1)+1)p^{t-1}-1]$$

then $N(jp^e, p^{e+t}) \equiv \sum_{c \in C} f(c^*) \equiv 0 \pmod{p^s}$. □

Remark. For divisible codes over prime fields, the bound for $\dim C$ given in the above theorem is the best possible for all integers $t \geq 1$, $e \geq 0$, and $s \geq 1$. To see this, we consider the concatenation C of $m = (s(p-1)+1)p^{t-1}-1$ copies of the $(e+1)$-dimensional dual Hamming codes.[2] The dimension of C is $(e+1)[(s(p-1)+1)p^{t-1}-1]$. Note that each dual Hamming code has single nonzero weight p^e. So the number of codewords in C with weights divisible by p^{e+t} is

$$N(0, p^{e+t}) = \sum_{0 \leq ip^t \leq m} (p^{e+1}-1)^{ip^t} \binom{m}{ip^t}.$$

Let $\lambda = -(p^{e+1}-1) \equiv 1 \pmod{p}$. Note the fact that

$$(\lambda x - 1)^{(s(p-1)+1)p^{t-1}-1} \equiv (-p)^{s-1} \sum_{j=0}^{p^t-1} x^j \pmod{p^s, x^{p^t}-1},$$

which is given by Formula (6.3) in [Wil03]. That is,

$$(\lambda x - 1)^m = (-p)^{s-1} \sum_{j=0}^{p^t-1} x^j + p^s f(x) + (x^{p^t}-1)g(x)$$

for some integer-coefficient polynomials f and g. Let ω be a primitive p^t-th root of unity.

[2] A q-ary k-dimensional *dual Hamming code* is a q-ary linear code of length $n = (q^k-1)/(q-1)$, generated by a k by n matrix whose column vectors are pairwise linearly independent q-ary vectors of length k

Plug in $x = \omega^j$ for all $0 \leq j \leq p^t - 1$, we have that

$$\begin{aligned} (\lambda\omega^0 - 1)^m &= (-p)^{s-1}p^t + p^s f(\omega^0), \\ (\lambda\omega^j - 1)^m &= p^s f(\omega^j), \quad 1 \leq j \leq p^t - 1. \end{aligned}$$

Note also that

$$\sum_{j=0}^{p^t-1} (\lambda\omega^j - 1)^m = (-1)^m p^t \sum_i (p^{e+1} - 1)^{ip^t} \binom{m}{ip^t}.$$

Therefore,

$$(-1)^m p^t \sum_i (p^{e+1} - 1)^{ip^t} \binom{m}{ip^t} = (-p)^{s-1}p^t + p^s \sum_{j=0}^{p^t-1} f(\omega^j).$$

Suppose $f(x) = \sum_{i=0}^{u} a_i x^i$, where a_i's, $0 \leq i \leq u$, are integers. Then

$$\sum_{j=0}^{p^t-1} f(\omega^j) = \sum_{j=0}^{p^t-1} \sum_{i=0}^{u} a_i (\omega^j)^i = \sum_{i=0}^{u} a_i \sum_{j=0}^{p^t-1} (\omega^i)^j = p^t \left(\sum_{0 \leq ip^t \leq u} a_{ip^t} \right) = p^t M,$$

where M is some integer. Therefore

$$(-1)^m p^t \sum_i (p^{e+1} - 1)^{ip^t} \binom{m}{ip^t} = (-p)^{s-1}p^t + p^s p^t M.$$

As a result,

$$\begin{aligned} N(0, p^{e+t}) &= \sum_i (p^{e+1} - 1)^{ip^t} \binom{(s(p-1)+1)p^{t-1} - 1}{ip^t} \\ &\equiv (-1)^{(s(p-1)+1)p^{t-1}+s} p^{s-1} \\ &\not\equiv 0 \pmod{p^s}. \end{aligned}$$

Thus the bound for $\dim C$ given in the theorem is the best possible for all $t \geq 1$, $e \geq 0$, and $s \geq 1$. Note that here C is assumed to be a p-ary code. However, for codes over arbitrary finite fields we do not have a similar result concerning the sharpness of the bound.

Note that when $e = 0$, Theorem 3.4 coincides with Theorem 3.1. Note also that we may view level $e \geq 1$ divisible codes just as linear codes and apply Theorem 3.1 instead of Theorem 3.4. However, the bound for the dimension of C given in Theorem 3.4 turns out to be much better than that given in Theorem 3.1.

3.2 A Related Bound

In this section, we "generalize" Theorem 3.4 in the following sense. Suppose C is a q-ary linear code of divisibility level e. Then we have

$$N(jp^e, p^{e+t}) \equiv 0 \pmod{p}, \quad 0 \leq j < p^t$$

if and only if $w(x) \equiv (1-x)^{p^t} g(x) \pmod{p}$, where $N(j, p^m)$ denotes the number of codewords in C that have weights congruent to j modulo p^m, $w(x^{p^e})$ denotes the weight enumerator of C, and g is some integer-coefficient polynomial. Therefore, Theorem 3.4 asserts that

$$\dim C \leq (\frac{e}{l} + 1)(p^t - 1)$$

if the order of $1-x$ in $w(x)$ modulo p is at most $p^t - 1$. This bound works well when the order of $1 - x$ in $w(x)$ modulo p exactly equals $p^t - 1$ for some positive integer t. Nevertheless, it does not seem a good bound when the order is not as such. As an extreme example, suppose that the order equals p^{t-1}, which is much less than $p^t - 1$. However, the bound for the dimension remains the same when applying Theorem 3.4. Therefore, the goal of this section is to provide a good bound for the dimension when the order of $1 - x$ in $w(x)$ modulo p^s equals an arbitrary integer m. Before stating the main theorem, we give the following lemma:

Lemma 3.5. *Let f be an integer-coefficient polynomial with $f(0) = 1$. Suppose m is the largest possible integer such that $f(x) \equiv (1-x)^m g(x) \pmod{p^s}$ for some integer-coefficient polynomial g with $g(0) = 1$. Then*

$$\sum_{i \geq 0} \binom{i-1}{j} f_i \begin{cases} \equiv 0 \pmod{p^s} & \text{if} \quad 0 \leq j < m, \\ \not\equiv 0 \pmod{p^s} & \text{if} \quad j = m, \end{cases}$$

where f_i denotes the coefficient of x^i in f.

Proof. Use induction on m, and first consider the base case $m = 0$. As $f(x)$ modulo p^s has no factor of $1 - x$, we have that

$$\sum_{i \geq 0} \binom{i-1}{m} f_i = \sum_{i \geq 0} f_i = f(1) \not\equiv 0 \pmod{p^s},$$

as desired. Now assume that for some $m \geq 0$ the lemma holds and consider then case when $f(x) \equiv (1-x)^{m+1}g(x) \pmod{p^s}$, where $g(1) \not\equiv 0 \pmod{p^s}$. Let $h(x) = (1-x)^m g(x)$. By induction hypothesis,[3]

$$\sum_{i\geq 0} \binom{i-1}{j} h_i \begin{cases} \equiv 0 \pmod{p^s} & \text{if} \quad 0 \leq j < m, \\ \not\equiv 0 \pmod{p^s} & \text{if} \quad j = m, \end{cases}$$

where h_i is the coefficient of x^i in h. Observe that for $j = 0$

$$\sum_{i\geq 0} \binom{i-1}{j} f_j = \sum_{i\geq 0} f_i = f(1) \equiv 0 \pmod{p^s}.$$

Now we assume that $j \geq 1$. As $f(x) \equiv (1-x)h(x) \pmod{p^s}$, we have

$$f_i \equiv \begin{cases} 1 & \pmod{p^s} \quad \text{if} \quad i = 0, \\ h_i - h_{i-1} & \pmod{p^s} \quad \text{if} \quad i \geq 1. \end{cases}$$

Therefore

$$\begin{aligned} \sum_{i\geq 0} \binom{i-1}{j} f_i &\equiv \binom{-1}{j} + \sum_{i\geq 1} \binom{i-1}{j} (h_i - h_{i-1}) \\ &= \sum_{i\geq 0} \binom{i-1}{j} h_i - \sum_{i\geq 1} \binom{i-2}{j-1} h_{i-1} - \sum_{i\geq 1} \binom{i-2}{j} h_{i-1} \\ &= -\sum_{i\geq 0} \binom{i-1}{j-1} h_i \begin{cases} \equiv 0 \pmod{p^s} & \text{if} \quad 1 \leq j < m+1, \\ \not\equiv 0 \pmod{p^s} & \text{if} \quad j = m+1, \end{cases} \end{aligned}$$

as desired. □

Remark. Given the same assumptions as in Lemma 3.5, we also have

$$\sum_{i\geq 0} \binom{i}{j} f_i \begin{cases} \equiv 0 \pmod{p^s} & \text{if} \quad 0 \leq j < m, \\ \not\equiv 0 \pmod{p^s} & \text{if} \quad j = m, \end{cases}$$

by a similar argument or by the fact that

$$\binom{i}{j} = \binom{i-1}{j} + \binom{i-1}{j-1}.$$

[3] Here we use that fact that $g(x)$ modulo p^s has $1-x$ as a factor if and only if $p^s | g(1)$.

Now we may state the main theorem of this section.

Theorem 3.6. *Let e be a nonnegative integer, and let C be a q-ary level e divisible code. Suppose that the weight enumerator of C is $w(x^{p^e})$, and m is the largest possible integer such that $w(x) \equiv (1-x)^m g(x) \pmod{p^e}$ for some integer-coefficient polynomial g. Then*

$$\dim C < (\frac{e}{l}+1)m + \frac{s}{l}.$$

Proof. First we deal with the $e = 0$ case separately. Let

$$f(c) = \binom{\mathrm{wt}(c)}{m}.$$

By the remark of Lemma 3.5, $\sum_{c \in C} f(c) \not\equiv 0 \pmod{p^s}$. On the other hand, Theorem 2.6 asserts that the MacWilliams transform

$$w^{\perp}(x) = q^{\dim C}(1+(q-1)x)^n w\left(\frac{1-x}{1+(q-1)x}\right)$$

of the weight enumerator $w(x) = \sum_{i=0}^{n} w_i x^i$ has integer coefficients if and only if

$$\sum_{i \geq 0} w_i \binom{i}{j} \equiv 0 \pmod{q^{\dim C - j}}$$

for all $0 \leq j < \dim C$. Take $j = m$ and we have that $\sum_{c \in C} f(c) \equiv 0 \pmod{q^{\dim C - m}}$. Therefore $l(\dim C - m) < s$, or equivalently,

$$\dim C < m + \frac{s}{l}.$$

Now we assume that $e \geq 1$ and let

$$f(x) = \binom{(x_1 + \cdots + x_n)/p^e - 1}{m}.$$

Let c^* be as defined in Lemma 3.3. By Lemma 3.5,

$$\sum_{c \in C} f(c^*) = \sum_{i \geq 0} \binom{i-1}{m} w_i \not\equiv 0 \pmod{p^s}, \tag{3.3}$$

where w_i denotes the coefficient of x^i in w. On the other hand,

$$f(x) = \frac{1}{m!\ p^{em}}(x_1 + \cdots + x_n - p^e) \ldots (x_1 + \cdots + x_n - mp^e).$$

The coefficient of the monomial $x_{j_1}^{a_1} \ldots x_{j_r}^{a_r}$, $a_1, \ldots, a_r \geq 1$, is

$$\frac{1}{m!\ p^{em}}(-1)^j \frac{(m-j)!}{a_1! \ldots a_r!} \sigma_m(j) p^{ej},$$

where $j = m - (a_1 + \cdots + a_r)$ and $\sigma_m(j)$ is as defined in Lemma 2.4. By a similar argument as in the proof of Theorem 3.4, the p-adic valuation of the coefficient is at least

$$-(e + \frac{1}{p-1})m + \frac{r}{p-1}.$$

Thus by Lemma 3.3,

$$\sum_{c \in C} f(c^*) \equiv 0 \pmod{p^{l(\dim C - r) - (e + \frac{1}{p-1})m + \frac{r}{p-1}}}$$

when $r = m$. That is, when

$$l(\dim C - r) - (e + \frac{1}{p-1})m + \frac{r}{p-1}$$

attains its minimum

$$l \dim C - (e + l)m$$

for $0 \leq r \leq m$. As a result, $\sum_{c \in C} f(c^*) \equiv 0 \pmod{p^{l \dim C - (e+l)m}}$. Compare with (3.3), we have

$$\dim C < (\frac{e}{l} + 1)m + \frac{s}{l},$$

as desired. □

Remark. We highly suspect that the result in Lemma 2.4 can be improved to

$$v_p(\sigma_m(j)) \geq v_p\left(\frac{m!}{(m-j)!}\right) - \frac{j}{p-1},$$

so that we need not deal with $e = 0$ case separately in both proofs of Theorem 3.4 and

Theorem 3.6. Moreover, if this is the case, we need not deal with $p \nmid \Delta$ case separately in the proof of Theorem 2.5.

Remark. Theorem 3.6 says that if the weight enumerator $w(x^{p^e})$ of a q-ary level e code C satisfies that $w(x) \equiv (1-x)^m g(x) \pmod{p^s}$, where m is the largest possible, then

$$m > \frac{l \dim C - s}{e + l}.$$

This actually gives a restriction for the weight enumerator $w(x^{p^e})$ of the code C. Precisely, for any positive integer s,

$$w(x^{p^e}) \equiv (1 - x^{p^e})^{\lfloor \frac{l \dim C - s}{e+l} \rfloor + 1} g(x^{p^e}) \pmod{p^s}$$

for some integer-coefficient polynomial g.

Remark. When $s = 1$, Theorem 3.4 is just a special case of Theorem 3.6 by taking $m = p^t - 1$. However, Theorem 3.4 is not simply covered by Theorem 3.6 when $s > 1$. Formula (2.9) in [Wil03] says that

$$\sum_{i \equiv j \pmod{p^t}} (-1)^i \binom{(s(p-1)+1)p^{t-1}}{i} \equiv 0 \pmod{p^s}$$

for all integers j. So $(1-x)^{(s(p-1)+1)p^{t-1}} \equiv (1 - x^{p^t}) h(x) \pmod{p^s}$ for some integer-coefficient polynomial h. Note that the above power $(s(p-1)+1)p^{t-1}$ is the smallest one we can achieve here to make the congruence holds. As a result, we need to assume that

$$\dim C \geq (\frac{e}{l} + 1)[(s(p-1)+1)p^{t-1} - 1] + \frac{s}{l},$$

which is a little stronger than assuming, as in Theorem 3.4, that

$$\dim C > (\frac{e}{l} + 1)[(s(p-1)+1)p^{t-1} - 1].$$

Then Theorem 3.6 asserts that $w(x) \equiv (1-x)^{(s(p-1)+1)p^{t-1}} g(x) \pmod{p^s}$ for some integer-coefficient polynomial g. Therefore $w(x) \equiv (1 - x^{p^t}) h(x) g(x) \pmod{p^s}$, which is equivalent to $N(jp^k, p^{k+t}) \equiv 0 \pmod{p^e}$ for all integers j.

Remark. For divisible codes over prime fields, the bound given in Theorem 3.6 is sharp for all integers $e, m \geq 0$ when $s = 1$. To see this, we consider the concatenation C of m copies of $(e+1)$-dimensional dual Hamming codes. The dimension of C is $(e+1)m$, and the weight enumerator $w(x^{p^e})$ of C satisfies $w(x) \equiv (1-x)^m \pmod{p}$. However, for the case when $s > 1$ or for the codes over arbitrary finite fields, we do not have similar results concerning the sharpness of the bound.

Comparing Ward's bound with our bound given in Theorem 3.6, we see that our bound is better than Ward's bound. In other words, we may deduce Ward's bound from Theorem 3.6, but not vice versa. In this section we will just show that Theorem 3.6 implies Theorem 1.2. In the next section we will give some examples in which the bound in Theorem 3.6 is indeed better than Ward's bound.

Proposition 3.7. *Let p be a prime and $f(x) = 1 + c_{b-m+1}x^{b-m+1} + \cdots + c_b x^b$, where $c_{b-m+1}, \ldots, c_b$ are nonnegative integers. Suppose*

$$s = v_p\left(\binom{b}{m}\right) + 1,$$

and $f(x) \equiv (1-x)^u g(x) \pmod{p^e}$ for some integer-coefficient polynomial g. Then $u \leq m$.

Proof. It suffices to show that $f(x) \not\equiv (1-x)^{m+1} g(x) \pmod{p^e}$ for any integer-coefficient polynomial g. Otherwise suppose $f(x) \equiv (1-x)^{m+1} g(x) \pmod{p^s}$ for some g. Then as $\deg(f) \leq b$, we may write $g(x) = g_0 + g_1 x + \cdots + g_{b-m-1}x^{b-m-1}$. We claim that

$$g_i \equiv \binom{m+i}{i} \pmod{p^s}$$

for all $0 \leq i \leq b-m$. First note that

$$(1-x)^{m+1} = \sum_{i=0}^{m+1} (-1)^i \binom{m+1}{i} x^i.$$

Since the coefficients of $x, x^2, \ldots, x^{b-m}$ in $f(x)$ are all zero, we have

$$\sum_{j=0}^{e} (-1)^j \binom{m+1}{j} g_{e-j} \equiv 0 \pmod{p^s}$$

for all $0 \leq e \leq b-m$. Now we will prove our claim by induction on i. Base case $i = 0$: Consider the above congruences. The one with $e = 0$ gives

$$g_0 \equiv 1 = \binom{m+0}{0} \pmod{p^s}.$$

Assume that for some $1 \leq i \leq b-m$, our claim is true for all $0 \leq j < i$. Then the congruence with $e = i$ gives

$$g_i \equiv \sum_{j=1}^{i} (-1)^{j-1} \binom{m+1}{j} \binom{m+i-j}{i-j} = \binom{m+i}{i} \pmod{p^e}.$$

Therefore,

$$g_{b-m} \equiv \binom{b}{b-m} = \binom{b}{m} \not\equiv 0 \pmod{p^s},$$

which gives a contradiction! □

We see that Ward's bound can be directly derived from Theorem 3.6 by applying Proposition 3.7. Moreover, from the proof of Proposition 3.7 we see that when Ward's bound is attained, one can completely determine the weight enumerator modulo p^s, where

$$s = v_p\left(\binom{b}{m}\right) + e + l.$$

Thus if we have any extra information about the weight distribution that contradicts this property, then the bound can be improved. We will discuss this more in the next section.

3.3 Applications

We have shown in the previous section that our so-called related bound implies Ward's bound. Note that Ward's bound is determined by the spectrum of the weights and there is no difference if some middle terms are missing, but our bound is determined by the weight enumerator modulo p^s. Therefore, in some certain cases our bound gives better results.

For example, let us consider the q-ary level e divisible codes whose nonzero weights are among $rp^e, (r+p)p^e, (r+2p)p^e, \ldots, (r+mp)p^e$, where r is some integer such that $0 < r < p$.

Ward's bound says that the dimension of such codes cannot exceed

$$(mp+1)\left(\frac{e}{l}+1\right)+\frac{1}{l}\,v_p\left(\binom{mp+r}{mp+1}\right).$$

By applying Theorem 3.6, we see that no matter how large m is, the dimension is always at most $e/l+1$, which is quite an improvement. Actually, this is the same as the bound for constant weight codes of the same divisibility level.

Corollary 3.8. *Suppose C is a q-ary linear code of level e. If there exists some integer r with $0 < r < p$ such that all codewords in C have weights congruent to rp^e modulo p^{e+1}, then*

$$\dim C \leq \frac{e}{l}+1.$$

Proof. Let $w(x^{p^e})$ be the weight enumerator of C. Then

$$w(x) = 1 + a_r x^r + a_{r+p}x^{r+p} + \cdots + a_{r+mp}x^{r+mp},$$

where m is some nonnegative integer. If $w(1) \neq 0 \pmod{p}$, then there is no integer-coefficient polynomial g such that $w(x) \equiv (1-x)g(x) \pmod{p}$. Otherwise

$$w(x) \equiv (1-x)(1+x+\cdots+x^{r-1}) + (1-x)^p x^r g(x^p) \pmod{p},$$

for some integer-coefficient polynomial g. Since $0 < r < p$ and $p \geq 2$, the power of $1-x$ in $w(x)$ modulo p is at most 1. By Theorem 3.6,

$$\dim C \leq \frac{e}{l}+1.$$

□

Corollary 3.8 is a generalization of the example given at the beginning of this chapter. More generally, if we assume that C is a q-ary level e code without nonzero weights divisible by p^{e+1}, then Theorem 3.4 asserts that

$$\dim C \leq (\frac{e}{l}+1)(p-1).$$

We see that for these codes, both Theorem 3.4 and Theorem 3.6 yield better bounds than

Ward's bound. However, the following example shows that sometimes when Theorem 3.4 fails, Theorem 3.6 still may improve Ward'd bound:

Example. Let C be a binary level two code with nonzero weights among 16, 20, 28, and 32. In other words, the weight 24 is missing from the spectrum. Then Ward's bound gives

$$\dim C \leq 5(1+2) + v_2\left(\binom{8}{5}\right) = 18.$$

Theorem 3.4 fails because the best conclusion we may get from the weight distribution is $N(0,64) \not\equiv 0 \pmod{2}$. Thus Theorem 3.4 gives

$$\dim C \leq (1+2)(2^4-1) = 45,$$

which is far worse than Ward's bound. However, Theorem 3.6 works as follows: Let $w(x^4)$ denote the weight enumerator of C, and assume that $w(x) \equiv (1-x)^5 g(x) \pmod{16}$ for some $g \in \mathbb{Z}[x]$. Then by the proof of Proposition 3.7, we have

$$\begin{aligned} w(x) &\equiv (1-x)^5\left(1+\binom{5}{1}x+\binom{6}{2}x^2+\binom{7}{3}x^3\right) \\ &\equiv 1-6x^4+8x^6-3x^8 \pmod{16}. \end{aligned}$$

This contradicts the fact that C has no codeword of weight 24. Therefore Theorem 3.6 yields

$$\dim C \leq 4(1+2) + (4-1) = 15,$$

which is better than Ward's bound.

We further generalize Corollary 3.8 by assuming that there are t, $t < p$, series of nonzero weights in a q-ary level e code C:

$$\begin{array}{llll} r_1p^e, & (r_1+p)p^e, & \ldots, & (r_1+m_1p)p^e, \\ r_2p^e, & (r_2+p)p^e, & \ldots, & (r_2+m_2p)p^e, \\ \vdots & \vdots & \vdots & \vdots \\ r_tp^e, & (r_t+p)p^e, & \ldots, & (r_t+m_tp)p^e, \end{array}$$

where all m_j's, $1 \leq j \leq t$, are nonnegative integers and all r_j's, $1 \leq j \leq t$, are integers such that $0 < r_1 < \cdots < r_t < p$. The following corollary says that the dimension of such a code satisfies

$$\dim C \le t\left(\frac{e}{l}+1\right).$$

Corollary 3.9. *Suppose C is a q-ary linear code of level e. If there exists some integers $r_1, \ldots, r_t$ with $0 < r_1 < \cdots < r_t < p$ such that all codewords in C have weights congruent to one of $r_j p^e$, $1 \le j \le t$, modulo p^{e+1}, then*

$$\dim C \le t\left(\frac{e}{l}+1\right).$$

Proof. Let $w(x^{p^e})$ be the weight enumerator of C. Then

$$w(x) = 1 + \sum_{i=0}^{m_1} a_{r_1+ip}x^{r_1+ip} + \cdots + \sum_{i=0}^{m_t} a_{r_t+ip}x^{r_t+ip},$$

where m_j, $1 \le j \le t$, are some nonnegative integers. Note that for any positive integer i and $1 \le j \le t$, $x^{r_j} - x^{r_j+ip} \equiv x^{r_j}(1-x)^p(1+x+\cdots+x^{i-1})^p \pmod p$. Therefore $w(x) \equiv 1 + c_1x^{r_1} + \cdots + c_tx^{r_t} + (1-x)^p g(x) \pmod p$ for some integer-coefficient polynomial g, and some integers $0 \le c_1, \ldots, c_t < p$ such that $1 + c_1 + \cdots + c_t \equiv 0 \pmod p$. We want to show that the order of $1-x$ in $w(x)$ modulo p is at most t. Otherwise, we should have $f(x) = 1 + c_1x^{r_1} + \cdots + c_tx^{r_t} \equiv (1-x)^{t+1}h(x) \pmod p$ for some integer-coefficient polynomial h. Then the j-th derivative of f satisfies that $f^{(j)}(x) \equiv (1-x)^{t+1-j}h_j(x) \pmod p$ for some integer-coefficient polynomials h_j for all integers $1 \le j \le t$. Thus $f^{(j)}(1) \equiv 0 \pmod p$ for all $0 \le j \le t$. Therefore,

$$\begin{array}{rcll} c_1 + \cdots + c_t & \equiv & -1 & \pmod p, \\ \binom{r_1}{j}c_1 + \cdots + \binom{r_t}{j}c_t & \equiv & 0 & \pmod p \quad 1 \le j \le t, \end{array}$$

which is impossible. Hence the order of $1-x$ in $w(x)$ modulo p is at most t and we get,

$$\dim C \le t\left(\frac{e}{l}+1\right)$$

by applying Theorem 3.6. □

The previous corollaries concern only level e codes without nonzero weights a multiple of p^{e+1}. For a level e code that does have some nonzero weights divisible by p^{e+1}, we cannot draw any general conclusion by Theorem 3.6. Yet as a first step, we may examine binary codes with exactly two nonzero weights.

Suppose C is a binary level e code whose nonzero weights are $w_1 = 2^e n$ and $w_2 = 2^e m$, with n odd and m even.[4] Let s be the 2-adic valuation of m, and N be the number of codewords in C of weight $2^e n$. Let $w(x^{2^e})$ denote the weight enumerator of C.

Case 1: $v_2(N) \geq s+1$. Then

$$w(x) \equiv 1 - x^m = (1-x)(1+x+\cdots+x^{m-1}) \pmod{2^{s+1}}.$$

Note that for even integers m, $1+x+\cdots+x^{m-1}$ modulo 2^{s+1} has no more factor of $1-x$. Thus by Theorem 3.6, $\dim C < (e+1)+(s+1)$. That is,

$$\dim C \leq e + v_2(m) + 1.$$

Case 2: $v_2(N) = d < s$. Then

$$\begin{aligned} w(x) &\equiv 1 + (2^d - 1)x^m - 2^d x^n \\ &\equiv (1 - x^m) + 2^d(x^m - x^n) \\ &\equiv (1-x)(1+x+\cdots+x^{m-1} + 2^d f(x)) \pmod{2^{d+1}}, \end{aligned}$$

where $f(x)$ is an integer-coefficient polynomial with $f(1) \equiv 1 \pmod 2$. As a matter of fact, $1+x+\cdots+x^{m-1}+2^d f(x)$ modulo 2^{d+1} has no more factor of $1-x$. Hence by Theorem 3.6, $\dim C < (e+1)+(d+1)$. Therefore,

$$\dim C \leq e + v_2(m).$$

Case 3: $v_2(N) = s$. Then

$$\begin{aligned} w(x) \equiv 1 - x^m &= (1-x)(1+x+\cdots+x^{m-1}) \\ &\equiv (1-x)^2(1+2x+\cdots+(m-1)x^{m-2}) \pmod{2^s}. \end{aligned}$$

[4] Note that if both n and m are odd integers, then C is a code as described in Corollary 3.8; and if both n and m are even integers, then the divisibility level of C is at least $e+1$.

As $1 + 2x + \cdots + (m-1)x^{m-2}$ modulo 2^s has no more factor of $1 - x$, again by Theorem 3.6, $\dim C < 2(e+1) + s$. That is,

$$\dim C \leq 2e + v_2(m) + 1.$$

As a conclusion, we always have

$$\dim C \leq 2e + v_2(m) + 1 = v_2(w_1) + v_2(w_2) + 1 \tag{3.4}$$

as a bound. We see that the bound can be attained when $m = 2n$, by letting C be the concatenation of two n-folded replicated $(e+1)$-dimensional dual Hamming codes.

If $n > 2m$, we claim that the bound can be improved to

$$\dim C \leq e + v_2(m) + 1,$$

since in this case, all codewords of weight $2^e m$ (plus the zero word) form a subcode C_1. Write $C = C_1 \bigoplus C_2$, where C_2 has constant nonzero weight $2^e n$. Then $\dim C = \dim C_1 + \dim C_2$. If $\dim C_1 \geq v_2(m) + 1$, note that $v_2(N) = \dim C_1$, so it falls in the above case 1. Therefore, $\dim C \leq e + v_2(m) + 1$; if $\dim C_1 \leq v_2(m)$, note that $\dim C_2 \leq e + 1$, so we still have $\dim C \leq e + v_2(m) + 1$. To see this bound is sharp for any e, m, and $n > 2m$, we may let C be generated by $(G \quad \mathbf{1})$, where G is the generating matrix of the t-folded, $t = m/2^{v_2(m)}$, replicated $(e+v_2(m)+1)$-dimensional dual Hamming code, and $\mathbf{1}$ represents the $e+v_2(m)+1$ by $(n-m)2^e$ all one matrix. Then C has nonzero weights $2^e m$ and $2^e n$, and dimension $e + v_2(m) + 1$. Note that the construction simply requires $n > m$.

If $m > 2n$, we claim that the bound can be improved to

$$\dim C \leq e + 1.$$

Since in this case all codewords of weight $2^e n$ (plus the zero word) form a subcode C_1, so $N \equiv 1 \pmod 2$, and hence Theorem 3.4 gives that $\dim C \leq e + 1$. Moreover, this bound is sharp as it can be attained by letting C be generated by $(G \quad \mathbf{1})$, where G is the generating matrix of the n-folded replicated $(e+1)$-dimensional dual Hamming code, and $\mathbf{1}$ represents the $e+1$ by $(m-n)2^e$ all one matrix. Note that this construction simply requires $m > n$.

If $n < 2m$ and $m < 2n$, we cannot decide whether the bound (3.4) is sharp or not. The following examples show that either case may occur depending on the value of m, n, and e.

Example. ($e = 1$, $m = 2$, $n = 3$.)

Bound (3.4) gives that $\dim C \leq 4$, where the nonzero weights of C are 4 and 6. We see that *the bound can be attained* by letting C be generated by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}_{4\times 9}.$$

Example. ($e = 1$, $m = 4$, $n = 7$.)

Bound (3.4) gives that $\dim C \leq 5$, where the nonzero weights of C are 8 and 14. Suppose $c \in C$ has weight 14. Let I be the complement of the support of c. Let C_I denote the projection code of C on I. Then C_I has no nonzero weights other than 1, 4, 7. Weight 1 can also be eliminated as C_I is linear. Thus $\dim C_I \leq 2 \cdot 0 + v_2(4) + 1 = 3$. Note that c is the only codeword in C that vanishes on I. Therefore $\dim C \leq 1 + 3 = 4 < 5$, and hence *the bound cannot be attained*. Moreover, 4 is the exact bound in this case as we may let C be generated by

$$\begin{pmatrix} 111111110000000 & 111111 \\ 111100001111000 & 111111 \\ 110011001100110 & 111111 \\ 101010101010101 & 111111 \end{pmatrix}_{4\times 21}.$$

Note that this exact bound is just $e + v_2(m) + 1$.

Inspired by this example we see that generally if $m < n < 2m$ and $2(2m - n) < n - m$, that is, $5m/3 < n < 2m$, then the bound can be improved to $\dim C \leq e + v_2(m) + 1$ by an induction proof on e. Moreover, the bound is sharp because the same construction as before in the $n > 2m$ case still works here.

Similarly if $5n/3 < m < 2n$, the bound can be improved to $\dim C \leq e + 2$ by an induction proof on e. Note that the base case says that if C has nonzero weights m and n, with m even, n odd, and $5n/3 < m < 2n$, then $\dim C = 2$. We see that the bound is sharp by the following inductive construction: Let C_0 be the 2-dimensional code with one codeword of weight m, and two codewords of weight n, and G_0 be the generating matrix of C_0. Then for any $i \geq 1$, let C_i be generated by

$$G_i = \begin{pmatrix} G_{i-1} & G_{i-1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix},$$

where the $\mathbf{0}$ in the first row is a zero matrix, and the second row $(\mathbf{1} \quad \mathbf{0} \quad \mathbf{1})$ represents a codeword of weight $2^e m$. Note that by this construction, each C_e has nonzero weights $2^e m$ and $2^e n$, and dimension $e + 2$.

Example. ($e = 1$, $m = 4$, $n = 3$.)

The bound (3.4) gives that $\dim C \leq 5$, where the nonzero weights of C are 8 and 6. Suppose $c \in C$ has weight 8. Let I be the complement of the support of c. Let C_I denote the projection code of c on I. Then C_I has no nonzero weights other than 2, 3, 4. If at least one of 2, 3, 4 is missing, then $\dim C_I \leq 3$. Otherwise, C_I must be equivalent to the code generated by

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

So $\dim C_I = 3$. Since c is the only nontrivial word in C that vanishes on I, $\dim C = 1 + \dim C_I \leq 4$. Therefore, the *bound cannot be attained.* Moreover, dimension 4 can be attained by letting C be generated by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}_{4\times 14}.$$

Chapter 4

Binary Divisible Codes of Maximum Dimension

Both Ward's bound and our new bounds given in Chapter 3 depend on weight distribution, but not length of the divisible codes. These bounds are derived from the linearity of the codes, and work well when the code length is sufficiently large. However, for divisible codes of relatively small length (in comparison to the width of the weight spectrum or the degree of the weight enumerator) these bounds are weak because the divisibility properties often require more than the linearity of such codes. Nevertheless, it is interesting to bound the dimension in terms of the code length and divisibility level. With this intention, we study *binary* divisible codes of certain length and level that achieve maximum dimension.

Throughout this chapter, we suppose that C is a binary divisible code of length n and level e. When $e = 1$ or 2, we have a complete description of such codes that attain the maximum dimension. The result is stated in Section 4.1. When $e \geq 3$, we prove an induction theorem in Section 4.2, which is applied to study level three codes of small lengths in Section 4.3.

4.1 Level One and Level Two Codes

The following theorem is a well-known result, and we provide an elementary proof here.

Theorem 4.1. *Suppose C is a binary level e code of length n. Then*

(i) *if $e = 1$ then $\dim C \leq n - 1$, with equality if and only if C is the code consists of all words of even weights;*

(ii) *if $e = 2$ then $\dim C \leq n/2$, with equality if and only if C is a type* II[1] *self-dual code in which case $8|n$.*

Proof. (i) Trivial, since every codeword in a level one binary code has even weight, and all words of even lengths in $\mathbb{F}_2^n$ form a level one code.

(ii) For any two codewords $a, b \in C$ we have $4|w(a)$, $4|w(b)$, and $4|w(a+b)$. Therefore $a \cdot b = 0$ and so C is self-orthogonal. This implies that $\dim C \leq n/2$. Now suppose $\dim C = n/2$ and as C is self-orthogonal, C must be a type II self-dual code. Consider the all one word $\mathbf{1}$. Since $4|w(a)$ for all $a \in C$, $\mathbf{1} \in C^\perp = C$. Thus as $4|w(\mathbf{1})$ we get $4|n$. Let $w(x)$ be the weight enumerator of C. Then the MacWilliams transform of $w(x,y)$,[2]

$$w\left(\frac{1}{\sqrt{2}}(x+y), \frac{1}{\sqrt{2}}(x-y)\right),$$

is the weight enumerator of $C^\perp = C$. Therefore

$$w(x,y) = w\left(\frac{1}{\sqrt{2}}(x+y), \frac{1}{\sqrt{2}}(x-y)\right).$$

Also as C is divisible by 4 and $4|n$, we have $w(x,y) = w(ix,y)$. Let

$$S = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}.$$

Then

$$(ST)^3 = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix},$$

where $\omega = -(1+i)/\sqrt{2}$ is a primitive 8th root of unity. Since both S and T preserve w, $(ST)^3$ also preserves w. Hence we have $w(x,y) = w(\omega x, \omega y) = \omega^n w(x,y)$. Therefore $8|n$. □

As a matter of fact, Theorem 4.1 provides an exact upper bound on dimension of level one and level two binary divisible codes of fixed length n, and describes all codes that attain the bound.

[1] Refer to Theorem 1.1.

[2] This is another form of the weight enumerator, which defines $w(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i$, where a_i represents the number of codewords of weight i.

4.2 Higher Level Codes

Now we want to extend the problem to codes of a higher level $e \geq 3$. In other words, we want to find:

- an exact upper bound for the dimension of length n binary linear codes of divisibility level e; and
- the codes that attain this bound.

A test for a code to be divisible is developed by Harold N. Ward in [War90], as stated in Theorem 1.3. The following proposition is just the binary case of Theorem 1.3, for which we give an elementary proof:

Proposition 4.2. *C is a binary linear code of divisibility level at least e if and only if for any spanning set $\mathfrak{B}$ of C we have*

$$2^{e+1-j} | \mathrm{wt}(c_1 \dots c_j) \tag{4.1}$$

for all $1 \leq j \leq e$ and $c_1, \dots, c_j \in \mathfrak{B}$, where $c_1 \dots c_j$ is the componentwise product of $c_1, \dots, c_j$.

Proof. Suppose C is divisible by 2^e. We use induction on j to prove (4.1). Base case $j = 1$ is trivially true as each codeword has a weight divisible by 2^e. Assume that (4.1) holds for some $j - 1$. Then as

$$\mathrm{wt}(c_1 + \cdots + c_j) = \sum_{i=1}^{j} (-2)^{i-1} \sum_{1 \leq \alpha_1 < \cdots < \alpha_i \leq j} \mathrm{wt}(c_{\alpha_1} \dots c_{\alpha_i}), \tag{4.2}$$

for all $c_1, \dots, c_j \in \mathfrak{B}$, we have $(-2)^{j-1}\mathrm{wt}(c_1 \dots c_j) \equiv 0 \pmod{2^e}$. Therefore (4.1) also holds for j.

On the other hand, suppose (4.1) holds for all integers $1 \leq j \leq e$ and $c_1, \dots, c_j \in \mathfrak{B}$. Since $\mathfrak{B}$ is a spanning set of C, any codeword $c \in C$ is a linear combination $c = c_1 + \cdots + c_k$ for some $c_1, \dots, c_k \in \mathfrak{B}$. Then (4.2) together with (4.1) assert that $\mathrm{wt}(c)$ is divisible by 2^e. Therefore, the code C is divisible by 2^e. □

Denote the set of binary linear codes of length n and divisibility level e as $\mathcal{C}(n, e)$. By assuming that $C \in \mathcal{C}(n, e)$ and the all-one-word is in C, n must be a multiple of 2^e. Note that on the other hand, if n is a multiple of 2^e, the all-one-word must be in C in order that its dimension attains the maximum. Now we start with the first nontrivial case where $n = 2^{e+1}$.

Theorem 4.3. *Suppose $C \in \mathcal{C}(n,e)$, where $n = 2^{e+1}$ and $e \geq 0$. Then the dimension of C cannot exceed $e+2$. Moreover, such a code C is equivalent to the first order Reed-Muller code* $\mathrm{RM}[1,e+1]$ *if* $\dim C = e+2$.

Proof. Write $k = \dim C$. Let C_1 be a $(k-1)$-dimensional subcode of C such that the all-one-word $\mathbf{1} \notin C_1$. Then all the nonzero codeword in C_1 has weight 2^e. By Ward's bound, $k - 1 \leq e + 1$. That is, $k \leq e+2$. If $k = e+2$, C_1 is a code of length 2^{e+1}, single nonzero weight 2^e, and dimension $e+1$, so it is equivalent to the $(e+1)$-dimensional dual Hamming code. Therefore, C is equivalent to $\mathrm{RM}[1, e+1]$. □

Our next step deals with code length $n = 2^{e+2}$, and we have a similar theorem as follows:

Theorem 4.4. *Suppose $C \in \mathcal{C}(n,e)$, where $n = 2^{e+2}$ and $e \geq 3$. Then the dimension of C cannot exceed $2(e+2)$. Moreover, such a code C is equivalent to the concatenation* $\mathrm{RM}[1,e+1] \oplus \mathrm{RM}[1,e+1]$ *if* $\dim C = 2(e+2)$.

Proof. Let $k = \dim C$. First we prove that $k \leq 2(e+2)$ by induction on e. Otherwise assume $k = 2e+5$, and there exists some codeword c with weight 2^{e+1} by Corollary 3.8. Let I be the support of c and J be the complement of I. Let C_1 be the projection of C on I and C_0 be the subcode of C that vanishes on I. Then

$$\dim C = \dim C_1 + \dim C_0.$$

C_1 is divisible by 2^{e-1} by Proposition 4.2. Thus $C_1 \in \mathcal{C}(2^{e+1}, e-1)$. When $e = 3$, $\dim C_1 \leq 2^e = 2(e+1)$ by Theorem 4.1; and when $e \geq 4$, $\dim C_1 \leq 2(e+1)$ by induction hypothesis. Ignoring the zero-coordinates, $C_0 \in \mathcal{C}(2^{e+1}, e)$. So by Theorem 4.3, $\dim C_0 \leq e+2$. If C_1 is also divisible by 2^e, then $\dim C_1 \leq e+2$ again by Theorem 4.3. Hence $\dim C \leq 2(e+2)$. Moreover, if $\dim C = 2(e+2)$ then C is equivalent to $\mathrm{RM}[1,e+1] \oplus \mathrm{RM}[1,e+1]$, still by Theorem 4.3.

Now suppose there exists some $c_1 \in C_1$ such that $2^{e-1} | \mathrm{wt}(c_1)$ but $2^e \nmid \mathrm{wt}(c_1)$. Let c_1' be the codeword in C whose projection on I is c_1. Since c, $\mathbf{1}$, and $\mathbf{1} + c$ are all codewords in

C, we may assume that after rearranging the coordinates,[3] c_1' looks like

$$\begin{array}{cccccccc} 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 \\ L & & & & K & & & \end{array},$$

where each block contains 2^{e-1} 0's or 1's. Note that we assume that the first four blocks form I. Now suppose $c_0 \in C_0$. Then the support of c_0 must either include K or disjoint with K by Proposition 4.2. Since $\mathbf{1} + c \in C_0$, we may assume $K \subseteq \operatorname{supp}(c_0)$. In order that $\dim C_0 \geq 3$, there must exist a basis of C_0 that looks like

$$\begin{array}{cccccccc} 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 1\ldots1 & 0\ldots0 & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 \\ L & & & & K & & & \end{array}.$$

Thus $\dim C_0$ cannot exceed 3, and $\dim C = 2e + 5$ implies that $\dim C_1 = 2(e+1)$ (which is the maximum by Theorem 4.3), and $\dim C_0 = 3$. By symmetry, we know that the following words are also in C:

$$\begin{array}{cccccccc} 1\ldots1 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 \\ 1\ldots1 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 \\ 1\ldots1 & 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 & 0\ldots0 \\ L & & & & K & & & \end{array}.$$

Therefore a basis for C_1 contains

$$\begin{array}{cccc} 1\ldots1 & 0\ldots0 & 0\ldots0 & 0\ldots0 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 1\ldots1 & 0\ldots0 \\ 0\ldots0 & 0\ldots0 & 0\ldots0 & 1\ldots1 \\ L & & & \end{array}.$$

Let C_2 be the subcode of C_1 generated by the above four codewords and let C_3 be such that $C_1 = C_2 \oplus C_3$. Then all codewords in C_1 that are not divisible by 2^e must be in C_2.

[3] Rearrangement of coordinates is always allowed, and we just mention it here once and for all.

Now there is a 3-dimensional subcode C_4 of C_2 with divisor 2^e. Consider $C_5 = C_3 \oplus C_4$, which is of length 2^{e+1} and divisor 2^e. So by Theorem 4.3, $\dim C_5 \leq e+2$. Since

$$\dim C_1 = \dim C_2 + \dim C_3 = \dim C_3 + \dim C_4 + 1 = \dim C_5 + 1 \leq e+3,$$

we know that $\dim C = \dim C_1 + \dim C_0 \leq e + 6 < 2e + 5$. Therefore we must always have $\dim C \leq 2(e+2)$ for all $e \geq 3$.

Now suppose $\dim C = 2(e+2)$. Besides the case we already have, which gives

$$C = \mathrm{RM}[1, e+1] \oplus \mathrm{RM}[1, e+1],$$

there are two other possibilities for $\dim C_1$ and $\dim C_0$, which we want to eliminate by using induction on e.

(i) $\dim C_1 = 2(e+1)$, $\dim C_0 = 2$.

If $e = 3$, there are exactly two cases of C_1 up to equivalence. The generator matrices for C in the two cases are as follows:

Case (a). C is generated by

$$G = \left(\begin{array}{cccc}
11110000 & & 11110000 & \\
00001111 & \mathbf{0} & 00001111 & \mathbf{0} \\
11001100 & & 11001100 & \\
10101010 & & 10101010 & \\
& 11110000 & & 11110000 \\
& 00001111 & & 00001111 \\
\mathbf{0} & 11001100 & \mathbf{0} & 11001100 \\
& 10101010 & & 10101010 \\
\mathbf{0} & \mathbf{0} & 11111111 & 00000000 \\
& & 00000000 & 11111111
\end{array} \right),$$

where $\mathbf{0}$'s represent zero matrices of proper sizes, and C_1 is equivalent $\mathrm{RM}[1,3] \oplus \mathrm{RM}[1,3]$ generated by the upper left 16 by 8 minor of G. Note that this code is equivalent to $\mathrm{RM}[1, e+1] \oplus \mathrm{RM}[1, e+1]$.

Case (b). C is generated by

$$G = \begin{pmatrix} 1111000000000000 & \\ 0011110000000000 & \\ 0000111100000000 & \\ 0000001111000000 & A \\ 0000000011110000 & \\ 0000000000111100 & \\ 0000000000001111 & \\ 1010101010101010 & \\ \mathbf{0} & 1111111100000000 \\ & 0000000011111111 \end{pmatrix},$$

where $\mathbf{0}$ is a zero matrix, and A is some 16 by 8 $\{0,1\}$-matrix. However, no matter what A stands for, we cannot complete the generator matrix G without violating Proposition 4.2.

If $e \geq 4$, C_1 is equivalent to $\mathrm{RM}[1,e] \oplus \mathrm{RM}[1,e]$ by the induction hypothesis, and a generator matrix for C is similar as in case (a), which implies that C is equivalent to $\mathrm{RM}[1,e+1] \oplus \mathrm{RM}[1,e+1]$.

(ii) $\dim C_1 = 2e+1$, $\dim C_0 = 3$.

Since (i) cannot give any new code, a similar argument as above leads to $\dim C \leq e+6 < 2e+4$ for all $e \geq 3$.

Therefore up to equivalence there is a unique $C \in \mathcal{C}(2^{e+2}, e)$ with dimension $2(e+2)$. Moreover, it is the concatenation $\mathrm{RM}[1,e+1] \oplus \mathrm{RM}[1,e+1]$ of two copies of the first order Reed-Muller code. □

Now our idea is to generalize Theorem 4.4 for larger code length n by an induction proof. The following theorem guarantees that if there always exists a codeword of weight 2^{e+1}, then the induction will go on well:

Theorem 4.5. *Suppose the dimension of a level e code of length $n - 2^{e+1}$ ($n = m \cdot 2^{e+1}$ and $m \geq 2$ an integer) cannot exceed $(m-1)(e+2)$, and suppose such a code is unique up to equivalence if its dimension equals $(m-1)(e+2)$. Then if $C \in \mathcal{C}(n,e)$, and there exists some codeword of weight 2^{e+1}, then $\dim C \leq m(e+2)$. Moreover, if $\dim C = m(e+2)$, such a code C is equivalent to the concatenation $\mathrm{RM}[1,e+1]^m$ of m copies of the first order*

Reed-Muller code.

Proof. Let $c \in C$, and $\mathrm{wt}(c) = 2^{e+1}$. Let I be the support of c and J be the complement of I. Let C_1 be the projection of C on I and C_0 be the subcode of C that vanishes on I. Still, we have $\dim C = \dim C_1 + \dim C_0$. Note that C_1 is of level $e-1$ and C_0 is of level e. Let C_2 be a maximum level e subcode of C_1. Then we may write a basis of C_1 as $\mathfrak{B} = \{c_1, \ldots, c_r, b_1, \ldots, b_s, a_1, \ldots, a_t\}$, where $\{b_1, \ldots, b_s, a_1, \ldots, a_t\}$ is a basis of C_2. Moreover, $2^{e-1} | \mathrm{wt}(c_i)$ but $2^e \nmid \mathrm{wt}(c_i)$, so we may assume that $\mathrm{wt}(c_i) = 2^{e-1}$ for all $1 \leq i \leq r$. And suppose

$$\{(c_1, c_1'), \ldots, (c_r, c_r'), (b_1, \mathbf{0}), \ldots, (b_s, \mathbf{0}), (a_1, a_1'), \ldots, (a_t, a_t'), (\mathbf{0}, d_1), \ldots, (\mathbf{0}, d_l)\}$$

is a basis of C, where $\{(\mathbf{0}, d_1), \ldots, (\mathbf{0}, d_l)\}$ is a basis of C_0. We also know that

$$\{a_1', \ldots, a_t', d_1, \ldots, d_l\}$$

forms a basis of a level e code of length $n - 2^{e+1}$. Thus $t + l \leq (m-1)(e+2)$. Moreover $r + s + t \leq 2(e+1)$ by Theorem 4.4. If $s = e+2$ then $r = 0$ by Proposition 4.2, and $t = 0$ by Theorem 4.3. Therefore

$$\dim C = r + s + t + l \leq e + 2 + (m-1)(e+2) = m(e+2),$$

and $\dim C = m(e+2)$ implies that $\dim C_0 = (m-1)(e+2)$, thus it is equivalent to $\mathrm{RM}[1, e+1]^{m-1}$ by the hypothesis. So as C_1 is another copy of $\mathrm{RM}[1, e+1]$, C is equivalent to $\mathrm{RM}[1, e+1]^m$. If $4 \leq s \leq e+1$ then we still have $r = 0$ by Proposition 4.2. Therefore

$$\dim C = r + s + t + l \leq 0 + (e+1) + (m-1)(e+2) < m(e+2).$$

If $s = 3$ then $r \leq 1$ by Proposition 4.2. Still, we have

$$\dim C = r + s + t + l \leq 1 + 3 + (m-1)(e+2) < m(e+2).$$

Therefore, we may suppose from now on that $s = 1$ or 2.

First we will show $r \leq e$ by induction on e. There must exist a codeword $\tilde{c} \in C_2$ with weight 2^e. Otherwise Corollary 3.8 alone asserts that $r \leq e$. Now consider the codewords $c_1, \ldots, c_r \in C_1$. If for some c_i, $1 \leq i \leq r$, we have the *componentwise product* $c_i\tilde{c} = c_i$, then $\langle \tilde{c_i} \rangle + \tilde{C_2}$ is divisible by 2^{e-1}, where $\tilde{}$ represents the projection on the support of $\tilde{c}$. Therefore we may assume that there is no c_j with $c_j\tilde{c} = \mathbf{0}$, otherwise $\langle c_i + c_j \rangle \oplus C_2$ is divisible by 2^e which contradicts that C_2 is maximal. If there are some $c_j \neq c_k$ distinct from c_i with $c_j\tilde{c} = c_j$ and $c_k\tilde{c} = c_k$, then by Proposition 4.2, there is no such c_h that $\mathrm{wt}(c_h\tilde{c}) = 2^{e-2}$. Thus by apply Theorem 4.3 on $\tilde{C_2}$ we have that $r \leq e$. If there is exactly one $c_j \neq c_i$ with $c_j\tilde{c} = c_j$, then again by Proposition 4.2 there is at most one c_h with $\mathrm{wt}(c_h\tilde{c}) = 2^{e-2}$. Thus $r \leq 3 \leq e$. Suppose for all $1 \leq j \leq r$ with $j \neq i$, we have $\mathrm{wt}(c_j\tilde{c}) = 2^{e-2}$. Then for $e = 3$, there exists at most one such c_j with $c_ic_j = \mathbf{0}$ and one such c_k with $w(c_ic_k) = 2$. Thus $r \leq 3 = e$. For $e > 3$, by the induction hypothesis we have $r - 1 \leq e - 1$. That is, $r \leq e$.

Since $s = 1$ or 2 and $r \leq e$, we have $\dim C = r+s+t+l \leq 2+e+(m-1)(e+2) = m(e+2)$, and $\dim C = m(e+2)$ implies that $r = e$, $s = 2$. Moreover, we cannot make $\dim C = m(e+2)$ if $r = e$, $s = 2$, and $0 < t < e$. Otherwise we have to construct the following codewords satisfying that the weight of the componentwise product of each h, $2 \leq h \leq e$, of them is a multiple of 2^{e+1-h}:

$$\{(b_1 \cdot b_j, b), (\mathbf{0}, \mathbf{1}), (\mathbf{0}, b_1), \ldots, (\mathbf{0}, b_{j-1}), (b_j, b_j), (b_{j+1}, b_{j+1}), \ldots, (b_{e+1}, b_{e+1})\},$$

where $\{\mathbf{1}, b_1, \ldots, b_{e+1}\}$ is a basis for $\mathrm{RM}[1, e+1]$, and $3 \leq j \leq e+1$. To see that there exists no proper b that satisfies the construction, we may just let $h = e - j + 2$ and consider for all $1 \leq k \leq j$ the following codewords: $(b_1b_j, b), (\delta_{kj}b_k, b_k), (b_{j+1}, b_{j+1}), \ldots, (b_{e+1}, b_{e+1})$. Now the only undiscussed case is that of $r = e$, $s = 2$, and $t = 0$ or e. In order that $\dim C = m(e+2)$, C_0 must be equivalent to $\mathrm{RM}[1, e+1]^{m-1}$ by the hypothesis. Moreover, a generator matrix for C must look like

$$\begin{pmatrix} B_0 & \mathbf{0} & A_1 & \ldots & A_{m-1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \ldots & \mathbf{0} \\ \multicolumn{2}{c}{B_1} & G & \ldots & \mathbf{0} \\ \multicolumn{2}{c}{\vdots} & \vdots & \ddots & \vdots \\ \multicolumn{2}{c}{B_{m-1}} & \mathbf{0} & \ldots & G \end{pmatrix},$$

where both G and

$$\begin{pmatrix} B_0 \\ \mathbf{1} \end{pmatrix}$$

are generator matrices for $\mathrm{RM}[1, e+1]$, and each B_i, $1 \leq i \leq m-1$, contains 0 or e linearly independent vectors. By Proposition 4.2, there must be exactly one of the B_i's containing e linearly independent vectors and others are $\mathbf{0}$ matrices. Therefore C is equivalent to $\mathrm{RM}[1, e+1]^m$. □

Note that if the length of the level e code C is an odd multiple 2^e, then we have a similar theorem as follows:

Theorem 4.6. *Let C be a level e code of length $(2m+1)2^e$, where $m \geq 2$. Suppose the dimension of any level e code with length $(2m-1)2^e$ cannot exceed $(m-1)(e+2)+1$ and attains the bound if and only if the code is equivalent to the direct sum of $\mathrm{RM}[1, e+1]^{m-1}$ and a 1-dimensional code generated by a weight 2^e word. Moreover, assume that there exists a codeword of weight 2^{e+1}. Then $\dim C \leq m(e+2)+1$ and equality happens if and only if C is equivalent to the direct sum of $\mathrm{RM}[1, e+1]^m$ and a 1-dimensional code generated by a weight 2^e word.*

Proof. Similar to Theorem 4.5. □

Note that Theorem 4.6 is also developed for inductively studying binary code of level e of general length n. The base case for the induction is $m = 1$. We may prove this by a similar argument as in Theorem 4.4, except that we take a weight 2^e codeword as c.

The hypothesis about the existence of a weight 2^{e+1} codeword is essential for the induction step to work. Though it seems quite reasonable, we have not figured out a proof of that.

Conjecture 4.7. *Let C be a level e code of length $m2^e$ with m a positive integer. Suppose the dimension of C attains the maximum value among such codes. Then there exists a codeword in C with weight 2^{e+1}.*

4.3 Level Three Codes of Small Lengths

For level e codes with relatively small lengths, the absence of weight 2^{e+1} codewords may cause dramatic decreasing in the code dimension. Thus Conjecture 4.7 may be proved true for such codes. In this section we deal with level three codes of length $8m$ where $2 \le m \le 14$. First we consider the case of even m's.

Theorem 4.8. *Let $C \in \mathcal{C}(n,3)$ where n is* 16*,* 32*,* 48*,* 64*,* 80*, or* 96*. Then the dimension of C cannot exceed $5n/16$. Moreover, such a code of dimension $5n/16$ is equivalent to* $\mathrm{RM}[1,4]^{n/16}$*.*

Proof. Theorem 4.3 and 4.4 give $n = 16$ and 32 cases. Then it suffices to prove that Conjecture 4.7 is true for $n = 48$ to 112 cases.

For $n = 48$, absence of weight 16 codeword implies that no codewords is divisible by 16 except for the all-one-word. Thus Corollary 3.8 gives that $\dim C \le 5 < 15$, hence C is not the best one we can get.

For $n = 64$, absence of weight 16 codewords gives $\{8, 24, 32, 40, 56, 64\}$ as the range of the nonzero weights. All codewords of weights $8, 56, 64$ must lie in a subspace of dimension less than or equal to 5. Consider the complement subcode C' whose nonzero weights are $24, 32, 40$. By Ward's bound,

$$\dim C' \le 3(3+1) + v\left(\binom{5}{3}\right) = 13.$$

Therefore such code C has dimension $\dim C \le 5 + 13 = 18 < 20$.

For $n = 80$, if both 16 and 32 are missed in the weight range, then again Corollary 3.8 gives that $\dim C \le 5 < 25$. Otherwise suppose a weight 32 codeword c does exist, but a weight 16 codeword does not. Let I be the support of c and J be the complement of I. Let C_1 be the projection of C on I, and C_0 be the subcode that vanishes on I. Then $\dim C = \dim C_1 + \dim C_0$. Since C_1 is divisible by 4, we have $\dim C_1 \le 16$ by Theorem 4.1. As the nonzero weights of C_0 are among $\{8, 24, 40, 48\}$, Corollary 3.8 again gives that $\dim C_0 \le 5$. Therefore $\dim C \le 16 + 5 = 21 < 25$.

For $n = 96$, absence of weight 16 codes implies that there are at most 15 codewords of weight 8. Then linear programming bound gives $\dim C \le 28 < 30$. □

Theorem 4.9. *Let $C \in \mathcal{C}(112,3)$. Then the dimension of C cannot exceed* 35*.*

Proof. If there exists a codeword of weight 16, then by Theorem 4.5, $\dim C \le 35$. Now suppose there exists no codeword of length 16. Then the number of weight 8 codewords is at most 15. Thus linear programming bound gives $\dim C \le 35$. □

Consider also codes with length n, which is an odd multiple of 8.

Theorem 4.10. *Let $C \in \mathcal{C}(n,3)$ where n is 24, 40, 56, 72, or 88. Then the dimension of C cannot exceed $5(n-8)/16+1$. Moreover, such a code of dimension $5(n-8)/16+1$ is equivalent to the direct sum of $\mathrm{RM}[1,4]^{n/16}$ and a 1-dimensional subcode generated by a weight 8 codeword.*

Proof. Similar to Theorem 4.8. □

Theorem 4.11. *Let $C \in \mathcal{C}(104,3)$. Then the dimension of C cannot exceed 31.*

Proof. Similar to Theorem 4.9. □

From the above discussion we see that by assuming Conjecture 4.7, level e binary codes with $e \geq 3$ that attain maximum possible dimension are merely copies of the first order Reed-Muller codes. This property is quite different from level two codes, that is, the doubly even self-dual codes. As we know, the number of selfdual codes of length n grows rapidly as n goes to infinity. Moreover, the minimum distance can also be sufficiently large.

Bibliography

[Ax64] J. Ax, "Zeros of polynomials over finite fields," *Amer. J. Math.,* vol. 86, pp. 255–261, 1964.

[BM73] L. D. Baumert and R. J. McEliece, "A note on the Griesmer bound," *IEEE Trans. Inform. Theory,* vol. 19, pp. 134–135, 1973.

[Cas86] J. W. S. Cassels, *Local Fields,* Cambridge University Press, Cambridge, 1986.

[CS90] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, 1990.

[DGS99] S. M. Dodunekov, S. Guritman, J. Simonis, "Some new results on the minimum length of binary linear codes of dimension nine," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2543–2546, 1999.

[DHM87] S. M. Dodunekov, T. Helleseth, N. L. Manev, Ø. Ytrehus, "New bounds on binary linear codes of dimension eight," *IEEE Trans. Inform. Theory*, vol. 33, pp. 917–919, 1987.

[DM90] S. M. Dodunekov and N. L. Manev, "Minimum possible block length of a linear code for some distance," *Problems Inform. Transmission*, vol. 26, pp. 173–176, 1990.

[Dod84] S. M. Dodunekov, "Minimum possible block length of a linear q-ary code with specified dimension and code distance," *Problems Inform. Transmission*, vol. 20, pp. 239–249, 1984.

[GH94] P. Greenough and R. Hill, "Optimal linear codes over GF(4)," *Discrete Math.*, vol. 125, pp. 187–199, 1994.

[Gri60] J. H. Griesmer, “A bound for error-correcting codes,” *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.

[HN92] R. Hill and D. E. Newton, “Optimal ternary linear codes,” *Designs, Codes and Cryptography*, vol. 2, pp. 137–157, 1992.

[HT80] N. Hamada and F. Tamari, “Construction of optimal codes and optimal factorial designs using linear programming,” *Ann. Discrete Math.*, vol. 6, pp. 175–188, 1980.

[LM99] I. Landjev and T. Maruta, “On the minimum length of quaternary linear codes of dimension five,” *Discrete Math.*, vol. 202, pp. 145–161, 1999.

[LRM03] I. N. Landjev, A. Rousseva, T. Maruta, R. Hill, “On optimal codes over the field with five elements,” *Designs, Codes and Cryptography*, vol. 29, pp. 165–175, 2003.

[LW92] J. H. Van Lint and R. M. Wilson, *A Course in Combinatorics,* Cambridge University Press, Cambridge, 1992.

[Mar99] T. Maruta, “On the minimum length of q-ary linear codes of dimension four,” *Discrete Math.*, vol. 208/209, pp. 427–435, 1999.

[MS73] C. L. Mallows and N. J. A. Sloane, “An upper bound for self-dual codes,” *Inform. Contr.,* vol. 22, pp. 188–200, 1973.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes,* North-Holland Pub. Co., Amsterdam, 1977.

[PW72] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes,* MIT Press, Cambridge, 1972.

[Rai98] E. M. Rains, “Shadow bounds for self-dual codes,” *IEEE Trans. Inform. Theory,* vol. 44, pp. 134–139, 1998.

[Ser79] J.-P. Serre, *Local Fields,* Springer-Verlag, New York, 1979.

[SS65] G. Solomon and J. J. Stiffler, “Algebraically punctured cyclic codes,” *Inform. Contr.*, vol. 8, pp. 170–179, 1965.

[UH39] J. V. Uspensky and M. A. Heaslit, *Elementary Number Theory,* McGraw-Hill, New York, 1939.

[Wan97] Z.-X. Wan, *Quaternary Codes,* World Scentific Pub., Singapore, 1997.

[War01a] H. N. Ward, "The divisible code bound revisited," *J. Combin. Theory, Ser. A,* vol. 94, pp. 34–50, 2001.

[War01b] H. N. Ward, "Divisible codes–a survey," *Serdica Math. J.*, vol. 27, pp. 263–278, 2001.

[War04] H. N. Ward, "A sequence of unique quaternary Griesmer Codes," *Designs, Codes and Cryptography*, vol. 33, pp. 71–85, 2004.

[War81] H. N. Ward, "Divisible codes," *Arch. Math.,* vol. 36, pp. 485–499, 1981.

[War90] H. N. Ward, "Weight polarization and divisibility," *Discrete Math.*, vol. 83, pp. 315–326, 1990.

[War92] H. N. Ward, "A bound for divisible codes," *IEEE Trans. Inform. Theory,* vol. 38, pp. 191–194, 1992.

[War98] H. N. Ward, "Divisibility of codes meeting the Griesmer bound," *J. Combin. Theory Ser. A*, vol. 83, pp. 79–93, 1998.

[Wil03] R. M. Wilson, "A lemma on polynomials modulo p^m and applications to coding theory," *Proc. of Int. Workshop on Comb., Linear Algebra, and Graph Coloring,* 2003.