Weights Modulo a Prime Power in Divisible Codes and a Related Bound

Xiaoyu Liu

***Abstract*—In this paper, we generalize the theorem given by R. M. Wilson about weights modulo p^t in linear codes to a divisible code version. Using a similar idea, we give an upper bound for the dimension of a divisible code by some divisibility property of its weight enumerator modulo p^e. We also prove that this bound implies Ward's bound for divisible codes. Moreover, we see that in some cases, our bound gives better results than Ward's bound.**

***Index Terms*—Bounds, divisible codes, weight enumerators.**

I. Introduction

DIVISIBLE codes were introduced by H. N. Ward in [1]. A *divisible code* is a linear code whose codewords all have weights divisible by some integer $\Delta > 1$, where Δ is called a *divisor* of the code.

Let p be a prime, and $q = p^l, l \geq 1$, be a prime power. Let $\mathbb{F}_q$ denote the field of q elements. Recall that a q-ary linear code of length n and dimension d is a d-dimensional subspace of $\mathbb{F}_q^n$.

Ward proved in [1] that if a divisor of a divisible code is relatively prime to the field characteristic, then the code is merely equivalent to a replicated code. So for a q-ary divisible code C, we are most interested in the case where the greatest divisor of C equals p^k for some integer $k \geq 1$. In such case, C is said to be of (divisibility) *level* k. Moreover, we may regard nondivisible codes as level 0 codes. Suppose the codewords in a level 0 q-ary code are gathered in classes according to their weights modulo p^t. Then the following theorem gives a sufficient condition for the sizes of all classes to be divisible by p^e.

Theorem 1.1: (cf. [2, Th. 4.2].) Let p be a prime and $q = p^l$ for some integer $l \geq 1$. Suppose C is a linear code over the field $\mathbb{F}_q$. Let $N(j, p^t)$ denote the number of codewords in C that have weights congruent to j modulo p^t. If

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

then

$$N(j, p^t) \equiv 0 \pmod{p^e}$$

for all integers j.

In Section II, we will generalize this result to level k divisible codes, where k can be any positive integer. The proof of the above theorem was based on the following lemma, which is also essential in our generalization.

Manuscript received August 24, 2005; revised May 29, 2006.

The author is with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: xiaoyu@its.caltech.edu).

Communicated by A. Ashikhmin, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.881708

Lemma 1.2: (cf. [2, Lemma 1.1].) Let p be a prime, and t and e positive integers. Let f be an integer-valued function on the integers that is periodic of period p^t. 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

$$w(j) \equiv f(j) \pmod{p^e}$$

for all integers j. The coefficients c_i are integers and, moreover,

$$c_i \equiv 0 \pmod{p^l}$$

whenever $i \geq (l(p-1)+1)p^{t-1}$.

Recall that $\binom{x}{n}$, $n \geq 0$ an integer, is regarded as the polynomial $x(x-1)\ldots(x-n+1)/n!$.

Theorem 1.1 actually gives an upper bound for the dimension of a linear code with $N(j, p^t) \not\equiv 0 \pmod{p^e}$ for some j. In Section III, we will generalize this upper bound to level k divisible codes and it turns out that the bound is determined by the power of $1 - x^{p^k}$ in the weight enumerator modulo p^e. Moreover, we will show that this generalized bound implies Ward's bound [3]. In Section IV, we will see some applications of our bound, which gives better results than Ward's bound in certain cases.

II. Weight Modulo a Prime Power in Divisible Codes

In this section, we will generalize Theorem 1.1 to a divisible code version. Before stating our main theorem, we need give the following lemma.

Lemma 2.1: Let p be a prime and $q = p^l$ for some integer $l \geq 1$. Suppose C is a q-ary linear code of length n and dimension d. Let $f(\mathbf{x}) = x_{i_1}^{a_1} \ldots x_{i_r}^{a_r}$ be a monomial defined on $\{0,1\}^n$ with $a_j \geq 1$ for all $1 \leq j \leq r$. Define $\mathbf{c}^*$ for each $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ as $\mathbf{c}^* = (|c_1|, \ldots, |c_n|)$, where $|c_i| = 0$ if $c_i = 0$, and $|c_i| = 1$ if $c_i \neq 0, 1 \leq i \leq n$. Then

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

Proof: Let C_0 be the subcode of C that vanishes on the corresponding r coordinates. Then $\dim C_0 \geq d - r$. Since f takes the same value on any coset of C_0, we have

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

Remark 2.2: Suppose f is an integer-coefficient polynomial that involves exactly r variables of $x_1, \ldots, x_n$. Then for a d dimensional q-ary linear code C of length n, we still have

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

by applying Lemma 2.1 to each monomial in f.

Let p be a prime. For any integer x, we denote by $v_p(x)$ the exponent of the highest power of p that divides x. By convention, $v_p(0) = \infty$. The function v_p is called *p-adic valuation*. Another lemma we need here gives lower bounds for the p-adic valuation of some numbers that will be useful later.

Lemma 2.3: Write

$$W_m(j) = \sum_{1\le\alpha_1<\cdots<\alpha_j\le m} \alpha_1 \ldots \alpha_j.$$

Then for any prime p, the p-adic valuation of $W_m(j)$ satisfies

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

Proof: First we prove by induction on j that

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

where $l_{j,i}$, $1 \le i \le j \le m$ are integers that satisfy

$$\begin{aligned} l_{j,1} &= j! \\ l_{j,i} &= (i+j-1)(l_{j-1,i} + l_{j-1,i-1}),\ 2 \le i \le j-1 \\ l_{j,j} &= (2j-1)!!. \end{aligned}$$

Since

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

our claim is true for the base case $j = 1$. Now suppose that the claim holds for $j-1$. Then we have

$$\begin{aligned} &W_m(j) - W_{m-1}(j) \\ &\quad = mW_{m-1}(j-1) \\ &\quad = m\sum_{i=1}^{j-1} l_{j-1,i}\binom{m}{j+i-1} \\ &\quad = \sum_{i=1}^{j-1}(m-j-i+1) l_{j-1,i}\binom{m}{j+i-1} \\ &\qquad + \sum_{i=1}^{j-1}(j+i-1) l_{j-1,i}\binom{m}{j+i-1} \\ &\quad = \sum_{i=1}^{j-1}(j+i) l_{j-1,i}\binom{m}{j+i} \\ &\qquad + \sum_{i=1}^{j-1}(j+i-1) l_{j-1,i}\binom{m}{j+i-1} \\ &\quad = \sum_{i=2}^{j}(j+i-1) l_{j-1,i-1}\binom{m}{j+i-1} \\ &\qquad + \sum_{i=1}^{j-1}(j+i-1) l_{j-1,i}\binom{m}{j+i-1} \\ &\quad = \sum_{i=2}^{j-1}(i+j-1)(l_{j-1,i-1} + l_{j-1,i})\binom{m}{j+i-1} \\ &\qquad + jl_{j-1,1}\binom{m}{j} + (2j-1) l_{j-1,j-1}\binom{m}{2j-1} \\ &\quad = \sum_{i=1}^{j} l_{j,i}\binom{m}{j+i-1}. \end{aligned}$$

So as $W_j(j) = j!$, we have

$$\begin{aligned} W_m(j) &= W_j(j) + \sum_{k=j}^{m-1}(W_{k+1}(j) - W_k(j)) \\ &= j! + \sum_{k=j}^{m-1}\sum_{i=1}^{j} l_{j,i}\binom{k+1}{j+i-1} \\ &= \sum_{i=1}^{j} l_{j,i}\left(\binom{j+1}{j+i} + \sum_{k=j}^{m-1}\binom{k+1}{j+i-1}\right) \\ &= \sum_{i=1}^{j} l_{j,i}\binom{m+1}{j+i}. \end{aligned}$$

Therefore our claim is true for all integers $1 \le j \le m$.

Note that

$$v_p(n!) \le \frac{n-1}{p-1}$$

for any positive integer n. So for each term in the above summation, the p-adic valuation is

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

$1 \le i \le j$. Therefore $W_m(j)$ has a p-adic valuation no less than this. □

Now here comes the divisible code version of Theorem 1.1.

Theorem 2.4: Let p be a prime and $q = p^l$ for some integer $l \ge 1$. Suppose k is some nonnegative integer and C is a level k divisible code over the field $\mathbb{F}_q$. Let $N(j, p^m)$ denote the number of codewords in C that have weights congruent to j modulo p^m. If

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

then

$$N(jp^k, p^{k+t}) \equiv 0 \pmod{p^e}$$

for all integers j.

Proof: Theorem 1.1 gives $k = 0$ case.

Now we assume that $k \geq 1$. By Lemma 1.2, there exists a polynomial

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

and where

$$c_i \equiv 0 \pmod{p^l}$$

whenever $i \geq (l(p-1)+1)p^{t-1}$. Let

$$f(\mathbf{x}) = g((x_1 + \cdots + x_n)/p^k)$$

and $\mathbf{c}^*$ be as defined in Lemma 2.1. Then

$$N(jp^k, p^{k+t}) \equiv \sum_{\mathbf{c} \in C} f(\mathbf{c}^*) \pmod{p^e}.$$

For each term

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

in $g(z)$, the corresponding term in $f(\mathbf{x})$ is

$$c_i \binom{(x_1 + \cdots + x_n)/p^k - 1}{i} = \frac{c_i}{i! p^{ki}} (x_1 + \cdots + x_n - p^k) \ldots (x_1 + \cdots + x_n - ip^k).$$

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

$$\frac{c_i}{i! p^{ki}} (-1)^s \frac{(i-s)!}{a_1! \ldots a_r!} W_i(s) p^{ks}$$

where $s = i - (a_1 + \cdots + a_r)$, and $W_i(s)$ is as defined in Lemma 2.3. Then the p-adic valuation of the coefficient is at least

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

The final step follows from the lower bound on $v_p(c_i)$. Note that $0 \leq r \leq (e(p-1)+1)p^{t-1} - 1$. So the number

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

attains its minimum when $r = (e(p-1)+1)p^{t-1} - 1$. Hence by Lemma 2.1

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

Therefore, if we have

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

then

$$N(jp^k, p^{k+t}) \equiv \sum_{\mathbf{c} \in C} f(\mathbf{c}^*) \equiv 0 \pmod{p^e}. \qquad \square$$

Remark 2.5: For divisible codes over prime fields, the bound for $\dim C$ given in the above theorem is the best possible for all integers $t \geq 1$, $k \geq 0$, and $e \geq 1$. To see this, we consider the concatenation C of $m = (e(p-1)+1)p^{t-1} - 1$ $(k+1)$-dimensional dual Hamming codes. The dimension of C is

$$(k+1)[(e(p-1)+1)p^{t-1} - 1].$$

Note that each dual Hamming code has single nonzero weight p^k. So the number of codewords in C with weights divisible by p^{k+t} is

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

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

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

which is given by [2, Formula (6.3)], i.e.,

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

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

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

Note that

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

So

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

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

$$\sum_{j=0}^{p^t-1} f(\omega^j) = \sum_{j=0}^{p^t-1}\sum_{i=0}^{s} a_i(\omega^j)^i = \sum_{i=0}^{s} a_i \sum_{j=0}^{p^t-1}(\omega^i)^j$$
$$= p^t \left(\sum_{0\le i\le s,\ i\equiv 0 \pmod{p^t}} a_i \right) = p^t M$$

where M is some integer. Therefore

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

As a result

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

So the bound for $\dim C$ given in the theorem is the best possible for all $t \ge 1$, $k \ge 0$, and $e \ge 1$.

Note that when $k=0$, Theorem 2.4 coincides with Theorem 1.1. For level k divisible codes with $k \ge 1$, the bound for the dimension of C given in Theorem 2.4 is much better than that given in Theorem 1.1.

III. A Bound for Divisible Codes

In this section, we will give an upper bound for the dimension of level k divisible codes by a similar method as in the proof of Theorem 2.4. The main theorem of this section is based on the following lemma.

Lemma 3.1: Suppose $f(x) \equiv (1-x)^s g(x) \pmod{p^e}$ for some integer-coefficient polynomial g with $g(0)=1$, and s is the largest possible integer. Then

$$\sum_{i\ge 0} \binom{i-1}{j} f_i \begin{cases} \equiv 0 \pmod{p^e} & 0 \le j < s \\ \not\equiv 0 \pmod{p^e} & j = s \end{cases}$$

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

Proof: Use induction on s and first consider the base case $s=0$. As f modulo p^e has no factor of $1-x$

$$\sum_{i\ge 0} \binom{i-1}{s} f_i = \sum_{i\ge 0} f_i = f(1) \not\equiv 0 \pmod{p^e}.$$

So the statement is valid for $s=0$ case. Now assume that for some $s \ge 0$ the lemma holds and consider $s+1$ case, i.e.

$$f(x) \equiv (1-x)^{s+1} g(x) \pmod{p^e}$$

and $g(1) \not\equiv 0 \pmod{p^e}$. Let $h(x)=(1-x)^s g(x)$. By induction hypothesis

$$\sum_{i\ge 0} \binom{i-1}{j} h_i \begin{cases} \equiv 0 \pmod{p^e} & 0 \le j < s \\ \not\equiv 0 \pmod{p^e} & j = s \end{cases}$$

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

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

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

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

Therefore

$$\sum_{i\ge 0} \binom{i-1}{j} f_i$$
$$\equiv \binom{-1}{j} + \sum_{i\ge 1} \binom{i-1}{j}(h_i - h_{i-1})$$
$$= \sum_{i\ge 0} \binom{i-1}{j} h_i - \sum_{i\ge 1} \binom{i-2}{j-1} h_{i-1} - \sum_{i\ge 1} \binom{i-2}{j} h_{i-1}$$
$$= -\sum_{i\ge 0} \binom{i-1}{j-1} h_i \begin{cases} \equiv 0 \pmod{p^e} & 1 \le j < s+1 \\ \not\equiv 0 \pmod{p^e} & j = s+1. \end{cases}$$ □

Remark 3.2: Given the same assumptions as in Lemma 3.1, we also have

$$\sum_{i\ge 0} \binom{i}{j} f_i \begin{cases} \equiv 0 \pmod{p^e} & 0 \le j < s \\ \not\equiv 0 \pmod{p^e} & j = s \end{cases}$$

by a similar argument or by the fact that

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

Now we may give the main theorem of this section.

Theorem 3.3: Let p be a prime and $q=p^l$ for some integer $l \ge 1$. Let k be some nonnegative integer and C a q-ary level k divisible code. Suppose that the weight enumerator of C is $w(x^{p^k})$, and

$$w(x) \equiv (1-x)^s g(x) \pmod{p^e}$$

for some integer-coefficient polynomial g, where s is the largest possible. Then

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

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

$$f(\mathbf{c}) = \binom{wt(\mathbf{c})}{s}$$

where $wt(\mathbf{c})$ denotes the weight of $\mathbf{c}$. Then by Remark 3.2

$$\sum_{\mathbf{c}\in C} f(\mathbf{c}) \not\equiv 0 \pmod{p^e}.$$

On the other hand, 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 $w(x) = \sum_{i\geq 0} w_i x^i$ has integer coefficients if and only if

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

for $0 \leq j < \dim C$. (cf. [2, Th. 7.1].) Take $j = s$ and we have that

$$\sum_{\mathbf{c}\in C} f(\mathbf{c}) \equiv 0 \pmod{q^{\dim C - s}}.$$

Therefore $l(\dim C - s) < e$, i.e.

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

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

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

Let $\mathbf{c}^*$ be as defined in Lemma 2.1. By Lemma 3.1

$$\sum_{\mathbf{c}\in C} f(\mathbf{c}^*) = \sum_{i\geq 0} \binom{i-1}{s} w_i \not\equiv 0 \pmod{p^e} \qquad (1)$$

where w_i denotes the coefficient of x^i in w.

On the other hand

$$f(\mathbf{x}) = \frac{1}{s!p^{ks}}(x_1 + \cdots + x_n - p^k)\ldots(x_1 + \cdots + x_n - sp^k).$$

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

$$\frac{1}{s!p^{ks}}(-1)^j \frac{(s-j)!}{a_1!\ldots a_r!} W_s(j) p^{kj}$$

where $j = s - (a_1 + \cdots + a_r)$ and $W_s(j)$ is as defined in Lemma 2.3. Then the p-adic valuation of the coefficient is at least

$$-(k + \frac{1}{p-1})s + \frac{r}{p-1}$$

by a similar argument as in the proof of Theorem 2.4. So by Lemma 2.1

$$\sum_{\mathbf{c}\in C} f(\mathbf{c}^*) \equiv 0 \pmod{p^{l(\dim C - r) - \left(k + \frac{1}{p-1}\right)s + \frac{r}{p-1}}}$$

when $r = s$, i.e., when

$$l(\dim C - r) - \left(k + \frac{1}{p-1}\right)s + \frac{r}{p-1}$$

attains its minimum for $0 \leq r \leq s$.

Therefore

$$\sum_{\mathbf{c}\in C} f(\mathbf{c}^*) \equiv 0 \pmod{p^{l\dim C - (k+l)s}}.$$

Comparing this with (1),

$$\dim C < \left(\frac{k}{l} + 1\right)s + \frac{e}{l}. \qquad \square$$

Remark 3.4: We highly suspect that the result in Lemma 2.3 can be improved to

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

so that we need not deal with $k = 0$ case separately in both proofs of Theorem 2.4 and Theorem 3.3.

Remark 3.5: Theorem 3.3 says that if the weight enumerator $w(x^{p^k})$ of a q-ary, $q = p^l$, level k code C satisfies that $w(x) \equiv (1-x)^s g(x) \pmod{p^e}$, where s is the largest possible, then

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

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

$$w(x^{p^k}) \equiv (1 - x^{p^k})^{[\frac{l\dim C - e}{k+l}]+1} g(x^{p^k}) \pmod{p^e}$$

for some integer-coefficient polynomial g.

Remark 3.6: Suppose C is a q-ary linear code of divisibility level k. Then we have

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

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, $w(x^{p^k})$ denotes the weight enumerator of C, and g is some integer-coefficient polynomial. So Theorem 2.4 (when $e = 1$) is just a special case of Theorem 3.3, by taking $s = p^t - 1$ and $e = 1$.

Anyway, Theorem 2.4 is not simply covered by Theorem 3.3 when $e > 1$. [2, Formula (2.9)] says that

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

for all integers j. So

$$(1-x)^{(e(p-1)+1)p^{t-1}} \equiv (1 - x^{p^t})h(x) \pmod{p^e}$$

for some integer-coefficient polynomial h. Note that the above power $(e(p-1)+1)p^{t-1}$ is the smallest one we can employ here to make the congruence hold. As a result, we need assume that

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

which is a little stronger than assuming, as in Theorem 2.4, that

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

Then Theorem 3.3 asserts that

$$w(x) \equiv (1-x)^{(e(p-1)+1)p^{t-1}} g(x) \pmod{p^e}$$

for some integer-coefficient polynomial g. Therefore

$$w(x) \equiv (1 - x^{p^t})h(x)g(x) \pmod{p^e}$$

which is equivalent to

$$N(jp^k, p^{k+t}) \equiv 0 \pmod{p^e}$$

for all integers j.

Remark 3.7: For divisible codes over prime fields, the bound given in Theorem 3.3 is sharp for all integers k, $s \geq 0$ when $e = 1$. To see this, we consider the concatenation C of s $(k+1)$-dimensional dual Hamming codes. The dimension of C is $(k+1)s$, and the weight enumerator $w(x^{p^k})$ of C satisfies

$$w(x) \equiv (1 - x)^s \pmod{p}.$$

In addition, we also have Ward's bound [3] that gives upper bound on the dimension of divisible codes.

Theorem 3.8: Ward's Bound. Let p be a prime and $q = p^l$ for some integer $l \geq 1$. Let C be a q-ary level k 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 $\Delta = p^k$. Then

$$\dim C \leq m\left(\frac{k}{l} + 1\right) + \frac{1}{l} v_p\left(\binom{b}{m}\right).$$

Comparing this with our bound given in Theorem 3.3, we see that our bound is better than Ward's bound. In other words, we may deduce Ward's bound from Theorem 3.3, but not vice versa. In this section we will just show that Theorem 3.3 implies Theorem 3.8. In the next section we will give some examples in which the bound in Theorem 3.3 is indeed better than Ward's bound.

Proposition 3.9: 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

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

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

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 $f(x) \equiv (1 - x)^{m+1} g(x) \pmod{p^e}$ for some g. Let g_i, $i \geq 0$, denote the coefficient of x^i in $g(x)$. Then as $\deg(f) \leq b$, g_i must vanish modulo p^e for all $i \geq b - m$. On the other hand, we claim that

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

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

$$\sum_{j=0}^{k} (-1)^j \binom{m+1}{j} g_{k-j} \equiv 0 \pmod{p^e} \tag{2}$$

for all $1 \leq k \leq b - m$.

Now we will prove our claim by induction on i. Base case $i = 0$

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

arises directly from $f(x) \equiv (1 - x)^{m+1} g(x) \pmod{p^e}$. Assume that for some $1 \leq i \leq b - m$, our claim is true for all $0 \leq j < i$. Then the congruence in (2) with $k = i$ gives

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

Note that

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

by a well-known relation between binomial coefficients

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{m+n-j}{k-j} = \begin{cases} \binom{m}{k}, & \text{if } m \geq k \\ 0, & \text{if } m < k \end{cases}$$

which can be proved by inclusion-exclusion. Therefore

$$g_i \equiv (-1)^0 \binom{m+1}{0} \binom{m+i-0}{i-0} = \binom{m+i}{i} \pmod{p^e}.$$

In particular

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

which gives a contradiction! □

We see that Ward's bound can be directly derived from Theorem 3.3 by applying Proposition 3.9. Moreover, from the proof of Proposition 3.9 we see that when Ward's bound is attained, one can completely determine the weight enumerator modulo p^e, where $e = v_p\left(\binom{b}{m}\right) + k + l$. So 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.

IV. Some Applications of the Bound

We have shown in the previous section that our 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^e. So in some certain cases, our bound gives better results.

For example, let us consider the q-ary, $q = p^l$, level k divisible codes whose nonzero weights are among

$$rp^k, (r+p)p^k, (r+2p)p^k, \ldots, (r+mp)p^k$$

where r is some integer such that $0 < r < p$. Ward's bound says that the dimension of such codes cannot exceed

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

By applying Theorem 3.3, we see that no matter how large is m, the dimension is always at most $\frac{k}{l}+1$, which is quite an improvement. Actually, this is the same as the bound for constant weight codes of the same divisibility level.

Theorem 4.1: Suppose p is a prime and $q = p^l$. Suppose C is a q-ary linear code of level k. If there exists some integer r with $0 < r < p$ such that all codewords in C have weights congruent to rp^k modulo p^{k+1}, then

$$\dim C \le \frac{k}{l} + 1.$$

Proof: Let $w(x^{p^k})$ 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 $p \ge 2$, the power of $1-x$ in $w(x)$ modulo p is at most 1. So by Theorem 3.3

$$\dim C \le \frac{k}{l} + 1. \qquad \square$$

Generally, if we assume that C is a q-ary, $q = p^l$, level k code without nonzero weights divisible by p^{k+1}, then Theorem 2.4 asserts that

$$\dim C \le (\frac{k}{l}+1)(p-1).$$

Furthermore, suppose there are t, $t < p$, series of nonzero weights in a q-ary, $q = p^l$, level k code C

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

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

$$\dim C \le t(\frac{k}{l}+1).$$

Theorem 4.2: Suppose p is an odd prime and $q = p^l$. Suppose C is a q-ary linear code of level k. 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_jp^k, $1 \le j \le t$, modulo p^{k+1}, then

$$\dim C \le t(\frac{k}{l}+1).$$

Proof: Let $w(x^{p^k})$ 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, $1 \le j \le t$

$$x^{r_j} - x^{r_j+ip} \equiv x^{r_j}(1-x)^p(1+x+\cdots+x^{i-1})^p \pmod p.$$

So

$$w(x) \equiv 1 + c_1x^{r_1} + \cdots + c_tx^{r_t} + (1-x)^p g(x) \pmod p$$

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 power 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 jth derivative of $f(x)$ satisfies that

$$f^{(j)}(x) \equiv (1-x)^{t+1-j}h_j(x) \pmod p, \quad 0 \le j \le t,$$

for some integer-coefficient polynomials h_j. So

$$f^{(j)}(1) \equiv 0 \pmod p, \quad 0 \le j \le t.$$

Therefore

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

which is impossible. Hence, the power of $1-x$ in $w(x)$ modulo p is at most t and by Theorem 3.3

$$\dim C \le t(\frac{k}{l}+1). \qquad \square$$

For a level k code that does have some nonzero weights divisible by p^{k+1}, we cannot draw any remarkable conclusion by Theorem 3.3. Yet as a first step, we may examine binary codes with exactly two nonzero weights.

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

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

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

Note that $1+x+\cdots+x^{m-1}$ modulo 2^{e+1} has no more factor of $1-x$. So by Theorem 3.3, $\dim C < (k+1)+(e+1)$, i.e.

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

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

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

where $f(x)$ is an integer-coefficient polynomial with $f(1) \equiv 1 \pmod 2$. So $1+x+\cdots+x^{m-1}+2^d f(x)$ modulo 2^{d+1} has no more factor of $1-x$. Hence by Theorem 3.3, $\dim C < (k+1)+(d+1)$. Therefore

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

Case 3: $v_2(N) = e$.

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

As $1+2x+\cdots+(m-1)x^{m-2}$ modulo 2^e has no more factor of $1-x$, again by Theorem 3.3, $\dim C < 2(k+1)+e$, i.e.

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

As a conclusion, we always have $\dim C \leq 2k + v_2(m) + 1$ as a bound.

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

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

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

Since in this case, all codewords of weight $2^k m$ (plus the zero word) form a subcode C_1. Write $C = C_1 \bigoplus C_2$, where C_2 has constant nonzero weight $2^k n$. 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, $\dim C \leq k + v_2(m) + 1$; if $\dim C_1 \leq v_2(m)$, note that $\dim C_2 \leq k+1$, so we still have $\dim C \leq k + v_2(m) + 1$.

To see this bound is sharp for any k, m, and $n > 2m$, we may let C be generated by $(\mathbf{G} \quad \mathbf{1})$, where $\mathbf{G}$ is the generating matrix of the t-fold, $t = m/2^{v_2(m)}$, replicated $(k + v_2(m) + 1)$-dimensional dual Hamming code, and $\mathbf{1}$ is the $k + v_2(m) + 1$ by $2^k(n-m)$ all one matrix. Then C has nonzero weights $2^k m$ and $2^k n$, and dimension $k + v_2(m) + 1$. Note that the construction requires $n > m$.

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

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

Since in this case, all codewords of weight $2^k n$ (plus the zero word) form a subcode C_1. So $N \equiv 1 \pmod 2$, and hence Theorem 2.4 gives that $\dim C \leq k+1$. Moreover, this bound can be attained by letting C be generated by $(\mathbf{G} \quad \mathbf{1})$, where $\mathbf{G}$ is the generating matrix of the n-fold replicated $(k+1)$-dimensional dual Hamming code, and $\mathbf{1}$ is the $k+1$ by $(m-n)2^k$ all one matrix. Note that this construction requires $m > n$.

If $n < 2m$ and $m < 2n$, we cannot decide whether the bound $2k + v_2(m) + 1$ is sharp or not. The following examples show that either case may occur depending on the value of m, n, and k.

Example 4.3: $(k = 1, m = 2, n = 3.)$

The bound 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 4.4: $(k = 1, m = 4, n = 7.)$

The bound gives that $\dim C \leq 5$, where the nonzero weights of C are 8 and 14. Suppose $\mathbf{c} \in C$ has weight 14. Let I be the complement of the support of $\mathbf{c}$. Let C_I denote the projection code of C on I. Then C_I has no nonzero weights other than 1, 4, 7. The weight 1 can also be eliminated as C_I is linear. So $\dim C_I \leq 2\times 0 + v_2(4) + 1 = 3$. Note that $\mathbf{c}$ 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 $k + v_2(m) + 1$.

Inspired by this example we see that generally if $m < n < 2m$ and $2(2m-n) < n - m$, i.e., $\frac{5}{3}m < n < 2m$, then the bound can be improved to $\dim C \leq k + v_2(m) + 1$ by an induction proof on k: We use a similar method as described in the previous example to reduce to cases with smaller k, i.e., take $\mathbf{c} \in C$ with weight $2^k n$ and consider the projection C_I of C on the complement I of the support of $\mathbf{c}$. Then C_I has nonzero weights $2^{k-1}m$ and $2^{k-1}n$. Moreover, the bound is sharp because the same construction as before in the $n > 2m$ case still works here.

Similarly if $\frac{5}{3}n < m < 2n$, the bound can be improved to $\dim C \leq k + 2$ by an induction proof on k: The method of reducing to cases with smaller k is similar as above, where in this situation, we take a codeword $\mathbf{c}$ of weight $2^k m$. Note that the base case says that if C has nonzero weights m and n, with

m even, n odd, and $\frac{5}{3}n < m < 2n$, then $\dim C = 2$. We see that the bound is sharp by the following inductive construction. Let C_0 be the two-dimensional code with one codeword of weight m, and two codewords of weight n, and $\mathbf{G}_0$ be the generating matrix of C_0. Then for any $k \geq 1$, let C_k be generated by

$$\mathbf{G}_k = \begin{pmatrix} \mathbf{G}_{k-1} & \mathbf{G}_{k-1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

where $(\mathbf{1} \quad \mathbf{0} \quad \mathbf{1})$ represents a codeword of weight $2^k m$. Note that by this construction, each C_k has nonzero weights $2^k m$ and $2^k n$, and dimension $k+2$.

Example 4.5: ($k = 1$, $m = 4$, $n = 3$.)

The bound gives that $\dim C \leq 5$, where the nonzero weights of C are 8 and 6. Suppose $\mathbf{c} \in C$ has weight 8. Let I be the complement of the support of $\mathbf{c}$. 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 $2, 4$ is missing, then $\dim C_I \leq 3$. If 3 is missing and $2, 4$ are not, let C_I' denote the projection code of C on the support of $\mathbf{c}$. Then $\dim C_I = \dim C_I' - 1$. However, C_I' has nonzero weights $4, 8$, thus $\dim C_I' \leq 4$, and so $\dim C_I \leq 3$. 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 $\mathbf{c}$ is the only nontrivial word in C that vanishes on I, $\dim C = 1 + \dim C_I \leq 4$. Therefore, the bound $2k + v_2(m) + 1$ cannot be attained. Moreover, dimension 4 can be attained by letting C be generated by

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

ACKNOWLEDGMENT

The author thanks R. M. Wilson for his interest and support.

REFERENCES

[1] H. N. Ward, "Divisible codes," *Arch. Math.*, vol. 36, pp. 485–499, 1981.
[2] R. M. Wilson, "A lemma on polynomials modulo p^m and applications to coding theory," in *Proc. Int. Workshop Comb., Linear Algebra, and Graph Coloring*, 2003.
[3] H. N. Ward, "A bound for divisible codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 1, pp. 191–194, Jan. 1992.