J. Korean Math. Soc. **47** (2010), No. 6, pp. 1167–1182
DOI 10.4134/JKMS.2010.47.6.1167

HIGHER WEIGHTS AND GENERALIZED MDS CODES

Steven T. Dougherty and Sunghyu Han

Abstract. We study codes meeting a generalized version of the Singleton bound for higher weights. We show that some of the higher weight enumerators of these codes are uniquely determined. We give the higher weight enumerators for MDS codes, the Simplex codes, the Hamming codes, the first order Reed-Muller codes and their dual codes. For the putative $[72, 36, 16]$ code we find the i-th higher weight enumerators for $i = 12$ to 36. Additionally, we give a version of the generalized Singleton bound for non-linear codes.

1. Introduction

Maximum Distance Separable (MDS) codes are an important class of codes. They are significant since they are optimal codes for their length and dimension but also because of their relation to various combinatorial structures, see [11] for a complete description. In this paper, we study a generalization of MDS codes, namely those codes meeting a generalized Singleton bound for higher weights. We shall define higher weights and then describe some basic results of generalized MDS codes which we will generalize. We also give the higher weight enumerators for the Simplex codes, the Hamming codes, the first order Reed-Muller codes and their dual codes. We give a version of the generalized Singleton bound for non-linear codes. We use these results to find a significant number of the higher weight enumerators for the putative $[72, 36, 16]$ Type II code. We find the i-th higher weight enumerators for $i = 12$ to 34 as well using the techniques of the paper. We also use the techniques of the paper to determine some previously unknown higher weight enumerators of the codes associated with the projective plane of order 5.

We begin with some basic definitions from coding theory. For any undefined terms from coding theory see [11] or [18].

A code C of length n over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$, and if it is a vector space, then we say it is a linear code. We attach the standard inner product to the ambient space $\mathbb{F}_q^n$, that is $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \mathbf{w}_i$, and define $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{w} \in C\}$. If $C = C^\perp$, then C is said to be a self-dual code. A Type II

Received February 4, 2009.
2000 *Mathematics Subject Classification.* 94B65.
Key words and phrases. higher weight enumerators, higher weights, MDS codes.

code is a binary self-dual code where all weights in the code are a multiple of 4. A Type I code is a binary self-dual code that is not Type II. For a Type I code, let C_0 be the codimension 1 subcode of doubly-even vectors. Then the shadow code $S = C_0^\perp - C$. The Hamming weight of a vector is the number of non-zero coordinates of the vector.

1.1. Higher weights

We describe higher weights which are generalizations of Hamming weights. These were introduced by Wei in [19]. Throughout we use the notation in [17].

Let C be a code and let $D \subseteq \mathbb{F}_q^n$ be a linear subcode of C. We define

$$||D|| = |\mathrm{Supp}(D)|,$$

where

$$\mathrm{Supp}(D) = \{i \mid \exists \mathbf{v} \in D,\ \mathbf{v}_i \neq 0\}.$$

We define the r-minimum weight for a linear code C as

$$d_r = d_r(C) = \min\{||D|| \mid D \subseteq C,\ \dim(D) = r\}.$$

Then $d_1(C)$ is the minimum Hamming weight.

The weight spectrum is generalized to the higher weight spectrum as follows:

$$A_i^r = A_i^r(C) = |\{D \subseteq C \mid \dim(D) = r,\ ||D|| = i\}|.$$

Weight enumerators are generalized to the following:

$$W^r(C; y) = W^r(C) = \sum A_i^r y^i.$$

For each $r \leq \dim(C)$ there is a weight enumerator. The weight enumerator $W^1(C; y)$ is not the Hamming weight enumerator $H_C(y) = \sum \alpha_i y^i$ where there are α_i vectors of Hamming weight i in C. Rather we have $W^1(C; y) = \frac{1}{q-1}(H_C(y) - 1)$ since each multiple of a vector has the same support and the zero vector does not generate a subcode of dimension 1.

As noted, for example in [16], simply because two codes have identical Hamming weight enumerators, this does not imply that the codes have identical $W^r(C; y)$ weight enumerators for all r. For example, consider two $[16, 8, 4]$ binary extremal self-dual codes d_{16}^+ and e_8^2. Both have the same Hamming weight enumerator $(1 + 14y^4 + y^8)^2$, but from [5, Table 3], d_3 of d_{16}^+ is 8 and d_3 of e_8^2 is 7, so their higher weight enumerators are not the same.

MacWilliams identities exist for these weights (see [12] or [17]). They are:

$$(1)\quad \sum_{r=0}^{s} [s]_r W^r(C^\perp; y) = q^{-sk}(1 + (q^s - 1)y)^n \sum_{r=0}^{s} [s]_r W^r\left(C; \frac{1-y}{1 + (q^s - 1)y}\right),$$

where the code has dimension k in $\mathbb{F}_q^n$, and $[s]_r = \prod_{j=0}^{r-1}(q^s - q^j)$. To find $W^s(C^\perp; y)$ one must use $W^r(C; y)$ for all r, with $0 \leq r \leq s$. We shall drop the y from the notation when it is not necessary.

1.2. MDS codes

There are various proofs of the Singleton bound. It can be proven both combinatorially and algebraically. We describe the algebraic proof whose techniques we shall use in the paper. This proof comes from Proposition 5.4 in [18]. Namely, take a generator matrix $G = (I\ A)$ for a code equivalent to C, where I is the $k \times k$ identity matrix. The minimum weight d is less than or equal to the weight of first row of G which is less than or equal to $n - k + 1$. This gives the well known bound which we state as a theorem.

Theorem 1.1 (Singleton Bound)**.** *If C is a linear $[n, k, d]$ code over $\mathbb{F}_q$, then*

$$d \leq n - k + 1. \tag{2}$$

This leads naturally to the following definition.

Definition 1. A linear $[n, k, d]$ code over $\mathbb{F}_q$ with $d = n - k + 1$ is called a Maximum Distance Separable (MDS) code.

The combinatorial proof of the Singleton bound in Equation 2 holds for codes over any alphabet, namely $d \leq n - \log_q(|C|) + 1$, where q is the size of the alphabet. The algebraic version has been generalized to a variety of rings, for example codes meeting the generalized algebraic Singleton bound for linear codes are called MDR codes, see [7] for a description of these codes over $\mathbb{Z}_k$. The most general version is given in [10] and is proven for codes over quasi-Frobenius rings.

A well known theorem relates MDS codes and their duals. It can be found in Theorem 2.4.3 in [11] and Theorem 9.2 in [18] for example.

Theorem 1.2. *If a linear $[n, k, d]$ code C is MDS, then so is its dual $C^\perp$.*

Later we shall give a proof of this theorem which will follow from results about higher weights.

The following is given in Theorem 7.4.1 in [11]. Let C be an $[n, k, d]$ MDS code over $\mathbb{F}_q$. The weight distribution of C is given by $A_0 = 1$, $A_i = 0$ for $1 \leq i < d$, and

$$A_i = \binom{n}{i} \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} (q^{i+1-d-j} - 1) \tag{3}$$

for $d \leq i \leq n$, where $d = n - k + 1$. As a corollary we then have that if C is an $[n, k, d]$ MDS code over $\mathbb{F}_q$, then

$$A_d = (q - 1)\binom{n}{d}. \tag{4}$$

See page 330 of [13] for a complete description.

1.3. r-MDS codes

In this section we shall define codes meeting a generalized Singleton bound for higher weights. We shall describe some results that we will use throughout the paper. We begin with a result that will be used to give a generalized Singleton bound. The following result can be found in [19]. If C is a linear $[n, k, d]$ code over $\mathbb{F}_q$, then

$$d = d_1(C) < d_2(C) < \cdots < d_k(C) \leq n. \tag{5}$$

This leads to the following result known as the generalized Singleton bound. Namely, if C is a linear $[n, k, d]$ code over $\mathbb{F}_q$, then

$$d_r \leq n - k + r \tag{6}$$

for $1 \leq r \leq k$. The proof can be found in Theorem 7.10.6 in [11].

As before this bound leads naturally to the following definition [17], [19].

Definition 2. A linear $[n, k, d]$ code over $\mathbb{F}_q$ with $d_r(C) = n - k + r$ is called an r-th maximum distance separable (r-MDS) code.

By this definition an MDS code is a 1-MDS code.

The following result is Theorem 7.10.7 in [11] and the proof follows from the proof of Equation 6. Namely, if C is an MDS code over $\mathbb{F}_q$, then C is an r-MDS code for all $1 \leq r \leq k$. Additionally, we have the following result which is Corollary 3.2 in [17]. It follows from the proof of Equation 6. Namely, if C is an r-MDS code over $\mathbb{F}_q$, then C is an r_1-MDS code for all $r \leq r_1 \leq k$.

This leads to the following definition.

Definition 3. If C is not an $(r-1)$-MDS code but it is an r-MDS code over $\mathbb{F}_q$, then C is called a proper r-MDS (P_r-MDS) code.

By this definition a non-trivial MDS code is a P_1-MDS code.

Example 1. Let C be the $[7, 4, 3]$ binary Hamming code. Then $C^\perp$ is the $[7, 3, 4]$ binary Simplex code. We can easily calculate the following:

$$d_1(C) = 3, d_2(C) = 5, d_3(C) = 6, d_4(C) = 7;$$
$$d_1(C^\perp) = 4, d_2(C^\perp) = 6, d_3(C^\perp) = 7.$$

This gives that both C and $C^\perp$ are P_2-MDS codes.

The following can be found in [19]. Namely, let C be an $[n, k]$ code over $\mathbb{F}_q$. Then

$$\{d_r(C) | 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \backslash \{n + 1 - d_r(C^\perp) \mid 1 \leq r \leq n - k\}. \tag{7}$$

2. r-MDS codes

We shall now investigate the properties of P_r-MDS codes. Using Equation 7, we have the following (Note: Similar statements to Theorem 2.1 are in Corollary 4.1 in [17]).

Theorem 2.1. *Let C be an $[n, k, d]$ code and let $C^\perp$ be an $[n, n-k, d^\perp]$ code.*

(1) *If $d^\perp = 1$, then C is not a P_r-MDS code for any $1 \le r \le k$.*

(2) *If $d^\perp > 1$, then C is a $P_{k-d^\perp+2}$-MDS code.*

Proof. Suppose $d^\perp = 1$. Since $1 \in \{d_r(C^\perp) \mid 1 \le r \le n-k\}$, we have $n \notin \{d_r(C) \mid 1 \le r \le k\}$. Therefore C is not a P_k-MDS code and C is not a P_r-MDS code for any $1 \le r \le k$. Suppose $d^\perp > 1$. By the Singleton bound, $d^\perp \le k+1$. Then we have that $1 \le k - d^\perp + 2 \le k$. Since $1, 2, \dots, d^\perp - 1 \notin \{d_r(C^\perp) \mid 1 \le r \le n-k\}$, we have $n-d^\perp+2, n-d^\perp+3, \dots, n \in \{d_r(C) \mid 1 \le r \le k\}$. Then since $d^\perp \in \{d_r(C^\perp) \mid 1 \le r \le n-k\}$, we have $n - d^\perp + 1 \notin \{d_r(C) \mid 1 \le r \le k\}$. Therefore, we have $d_{k-d^\perp+1} < n - d^\perp + 1$ and $d_{k-d^\perp+2} = n - d^\perp + 2$. We conclude that C is a $P_{k-d^\perp+2}$-MDS code. □

Corollary 2.2. *If C is an $[n, \frac{n}{2}, d]$ self-dual code over $\mathbb{F}_q$, then C is a $P_{\frac{n}{2}-d+2}$-MDS code.*

Proof. It follows from Theorem 2.1 noting that $d = d^\perp$ and $k = n - k$. □

While non-trivial binary MDS codes do not exist, by the previous corollary it is easy to see that non-trivial binary r-MDS codes are easily found.

Using Theorem 2.1, we can reprove Theorem 1.2.

Corollary 2.3. *If a linear $[n, k, d]$ code C is MDS, then so is its dual $C^\perp$.*

Proof. Since C is a P_1-MDS code, $k - d^\perp + 2 = 1$, and it follows that $d^\perp = k + 1$. □

Example 2. Let $H_{q,r}$ be the $[(q^r-1)/(q-1), (q^r-1)/(q-1)-r, 3]$ Hamming code over $\mathbb{F}_q$. Then its dual $S_{q,r}$ is the $[(q^r-1)/(q-1), r, q^{r-1}]$ Simplex code. By Theorem 2.1, $H_{q,r}$ is a $P_{(q^r-1)/(q-1)-r-q^{r-1}+2}$-MDS code and $S_{q,r}$ is a P_{r-1}-MDS code.

Theorem 2.4. *There exist P_r-MDS codes for all $r \ge 1$.*

Proof. The theorem follows from the fact that $S_{q,r}$ is a P_{r-1}-MDS code. □

We shall give a generalization of the result in Equation 3 for P_r-MDS codes. First we need the following notation and the following result. Recall the definition of the Gaussian binomial:

$$\begin{bmatrix} k \\ r \end{bmatrix} = \frac{(q^k-1)(q^k-q)\cdots(q^k-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})},$$

which is the number of subspaces of dimension r in a k dimensional space over $\mathbb{F}_q$.

The following result is Theorem 2 in [15].

Let C be an $[n, k, d]$ code and let $C^\perp$ be an $[n, n-k, d^\perp]$ code. If $k+1-d^\perp < r \le k$, then

$$A_i^r(C) = \binom{n}{n-i} \sum_{j=0}^{k+i-r-n} (-1)^j \begin{bmatrix} k-n+i-j \\ k-r-n+i-j \end{bmatrix} \binom{i}{j}. \tag{8}$$

Furthermore, if we know $W^1(C^\perp)$, then for $k+2-d_2(C^\perp) < r \le k+1-d^\perp$, we have that

$$A_i^r(C) = U_{n-i}^{k-1-r}(II) + U_{n-i}^{k-1-r}(I), \tag{9}$$

where $U_{n-i}^{k-1-r}(II)$ and $U_{n-i}^{k-1-r}(I)$ are given in [15].

Remark 1. In Equation 9, $U_{n-i}^{k-1-r}(II)$ and $U_{n-i}^{k-1-r}(I)$ are complex formulas. In [15], it is remarked that it will be possible to compute $A_i^r(C)$ for

$$k+3-\min\{d_3(C^\perp), 2d^\perp\} < r \le k - d_2(C^\perp) + 2$$

provided $W^2(C^\perp)$ is known.

Now we give a generalization of the result in Equation 3 for P_r-MDS codes. For a similar result see Theorem 8.1 in [9].

Theorem 2.5. *Let C be an $[n,k]$ P_r-MDS code over $\mathbb{F}_q$. Then, for $r \le i \le k$, the higher weight spectrum of $W^i(C;y)$ is determined by the parameters n, k, and q. In fact, it is given by $A_j^i(C) = 0$ for $0 \le j < d_i$, and*

$$A_j^i(C) = \binom{n}{j} \sum_{t=0}^{j-d_i} (-1)^t \binom{j}{t} \begin{bmatrix} j+i-d_i-t \\ i \end{bmatrix}$$

for $d_i \le j \le n$, where $d_i = d_i(C) = n-k+i$.

Proof. By Theorem 2.1, $r = k-d^\perp+2$. Now the theorem is an easy consequence of Equation 8. □

The following corollary is a generalization of Equation 4.

Corollary 2.6. *If C is an $[n,k]$ P_r-MDS code over $\mathbb{F}_q$ with $d_i = n-k+i$ $(r \le i \le k)$, then $A_{d_i}^i = \binom{n}{d_i}$.*

Proof. It follows from Theorem 2.5. □

Example 3. Using Theorem 2.5, we can calculate all higher weight spectrums for MDS codes. For example, consider a $[6,4,3]$ Reed-Solomon code C over $\mathbb{F}_7$. Then the weight spectrums are given by the following:

$$\begin{aligned} W^0 &= 1, \\ W^1 &= 20y^3 + 60y^4 + 162y^5 + 158y^6, \\ W^2 &= 15y^4 + 312y^5 + 2523y^6, \\ W^3 &= 6y^5 + 394y^6, \\ W^4 &= y^6. \end{aligned}$$

Example 4. Using Theorem 2.5, we can calculate some higher weight spectrums for self-dual codes. For the $[24,12,8]$ Golay Type II code, we can determine $W^i(C;y)$ for $6 \le i \le 12$. For the unique $[48,24,12]$ Type II code, we can determine $W^i(C;y)$ for $14 \le i \le 24$. These weight enumerators were done in their entirety in [3]. For the putative $[72,36,16]$ Type II code, we can determine $W^i(C;y)$ for $22 \leq i \leq 36$. Later we shall find even more of these weight enumerators.

The higher weight spectrums of the Simplex codes $S_{q,r}$ were stated in [12]. In the following we provide an alternate proof.

Theorem 2.7. *Recall that $S_{q,r}$ is the $[(q^r-1)/(q-1), r, q^{r-1}]$ Simplex code. Then the higher weight spectrums of $S_{q,r}$ are given by the following. For $1 \leq i \leq r$,*

j	$A_j^i(S_{q,r})$
$q^{r-i}\frac{q^i-1}{q-1}$	$\begin{bmatrix} r \\ i \end{bmatrix}$
otherwise	0

Proof. The following simple property of $||D||$ is known [17]. If $\dim D = r$, we have

$$||D|| = \frac{1}{q^r - q^{r-1}} \sum_{v \in D} ||\mathbf{v}||.$$

Note that all nonzero codewords have Hamming weight q^{r-1}. Let $\dim D = i$ and $D \subseteq S_{q,r}$. Then

$$\begin{aligned} ||D|| &= \frac{1}{q^i - q^{i-1}} \sum_{v \in D} ||\mathbf{v}|| \\ &= \frac{1}{q^i - q^{i-1}} \cdot (q^i - 1) q^{r-1} \\ &= q^{r-i} \frac{q^i - 1}{q - 1}. \end{aligned}$$

□

From Equation 1, if we know $W^r(C;y)$, $(0 \leq r \leq s)$, then we can calculate $W^s(C^\perp;y)$. But there is also an explicit expression for $W^s(C^\perp;y)$ in [12, Theorem 2], namely the following.

Theorem 2.8. *For all $s \geq 0$ we have*

$$\begin{aligned} W^s(C^\perp;y) &= \sum_{i=0}^{s} \sum_{r=0}^{i} (-1)^{s-i} \frac{q^{((s-i)(s-i-1)/2)-i(s-i)-r(i-r)-ik}}{[s-i]_{s-i}[i-r]_{i-r}} \\ &\quad \times (1 + (q^i - 1)y)^n W^r\Big(C; \frac{1-y}{1+(q^i-1)y}\Big). \end{aligned}$$

Using Theorem 2.7 and Theorem 2.8, we calculated the higher weight spectrums of $S_{2,j}$ and $H_{2,j}$ for $j = 2, 3, 4$, and $S_{3,j}$ and $H_{3,j}$ for $j = 2, 3$ and present them in Tables 1 to 12 which can be found in [2].

In the following, we give the higher weight spectrums of the first order Reed-Muller codes and their dual codes. We start with the following notation. For $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$,

$$|\mathbf{u} \vee \mathbf{v}| = |\mathrm{Supp}(\mathbf{u}) \cup \mathrm{Supp}(\mathbf{v})|, \;\; |\mathbf{u} \wedge \mathbf{v}| = |\mathrm{Supp}(\mathbf{u}) \cap \mathrm{Supp}(\mathbf{v})|.$$

Theorem 2.9. *Let $R(1,r)$ be the $[2^r, r+1, 2^{r-1}]$ first order Reed-Muller code. Then the higher weight spectrums of $R(1,r)$ are given by the following. If $1 \leq i \leq r$, then*

j	$A_j^i(R(1,r))$
$2^r - 2^{r-i}$	$\begin{bmatrix} r+1 \\ i \end{bmatrix} - \begin{bmatrix} r \\ i-1 \end{bmatrix}$
2^r	$\begin{bmatrix} r \\ i-1 \end{bmatrix}$
otherwise	0

If $i = r+1$, then $W^i(R(1,r);y) = y^{2^r}$.

Proof. If $i = 1$ or $i = r+1$, then the theorem is true. Assume that $2 \leq i \leq r$. Let G_2 be the matrix

$$G_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

For $r \geq 3$, define G_r inductively by

$$G_r = \left[\begin{array}{c|c|c} 0\cdots0 & 1 & 1\cdots1 \\ \hline & 0 & \\ G_{r-1} & \vdots & G_{r-1} \\ & 0 & \end{array}\right].$$

Then G_r is a generator matrix for the binary Simplex code $S_{2,r}$, $(r \geq 2)$ [11, p. 30]. Define $G(1,r)$ to be the following $(r+1) \times 2^r$ matrix:

$$G(1,r) = \left[\begin{array}{c|c} 1 & 1\cdots1 \\ \hline 0 & \\ \vdots & G_r \\ 0 & \end{array}\right].$$

Then $G(1,r)$ is a generator matrix for $R(1,r)$ [11, p. 36].

We can think of an i dimensional subspace for $R(1,r)$ in three ways.

(1) The i dimensional subspace is generated by the rows of $G(1,r)$ except the first row. Then every vector in the subspace is of the form $(0, \mathbf{a})$, where $\mathbf{a}$ is a vector in an i dimensional subspace for $S_{2,r}$. Therefore the size of the support of the i dimensional subspace is $2^r - 2^{r-i}$.

(2) First we make an $i-1$ dimensional subspace which is generated by the rows of $G(1,r)$ except the first row. Then by adding the first row, we make an i dimensional subspace. Therefore, in this case, the weight spectrum is given by the following:

$$\begin{bmatrix} r \\ i-1 \end{bmatrix} y^{2^r}.$$

(3) The i dimensional subspace is generated by the following vectors:

$$(\delta_1, \mathbf{a}_1 + \delta_1 \mathbf{1}), (\delta_2, \mathbf{a}_2 + \delta_2 \mathbf{1}), \ldots, (\delta_i, \mathbf{a}_i + \delta_i \mathbf{1}),$$

where $\mathbf{a}_j$ is a codeword in $S_{2,r}$ and $\delta_j = 0, 1$ for $1 \leq j \leq i$ (at least one δ_j is 1) and $\mathbf{1}$ is the all 1 vector of length $2^r - 1$. Without loss of generality, we may assume that the generating vectors can be changed to the following vectors.

$$(0, \mathbf{a}_1), (0, \mathbf{a}_2), \ldots, (0, \mathbf{a}_{i-1}), (1, \mathbf{a}_i + \mathbf{1}).$$

Then the size of the support of the i dimensional subspace is

$$1 + |\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1} \vee (\mathbf{a}_i + \mathbf{1})|.$$

Note that

$$\begin{aligned} & |\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1} \vee (\mathbf{a}_i + \mathbf{1})| \\ = & |\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}| + |(\mathbf{a}_i + \mathbf{1})| - |(\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}) \wedge (\mathbf{a}_i + \mathbf{1})|. \end{aligned}$$

Note that $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1}$ are linearly independent. If $\mathbf{a}_i$ is a linear combination of $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{i-1}$, then we can reduce this case to the above case. We can then assume that $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_i$ are linearly independent. Since

$$\begin{aligned} & |(\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}) \wedge \mathbf{a}_i| \\ &= |\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}| + |\mathbf{a}_i| - |\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_i| \\ &= (2^r - 2^{r-i+1}) + 2^{r-1} - (2^r - 2^{r-i}) \\ &= 2^{r-1} - 2^{r-i}, \end{aligned}$$

we have

$$\begin{aligned} & |(\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}) \wedge (\mathbf{a}_i + \mathbf{1})| \\ &= |(\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1})| - |(\mathbf{a}_1 \vee \mathbf{a}_2 \vee \cdots \vee \mathbf{a}_{i-1}) \wedge \mathbf{a}_i| \\ &= (2^r - 2^{r-i+1}) - (2^{r-1} - 2^{r-i}) \\ &= 2^{r-1} - 2^{r-i}. \end{aligned}$$

From the above values, the size of the support of the i dimensional subspace is

$$\begin{aligned} & 1 + (2^r - 2^{r-i+1}) + (2^r - 1 - 2^{r-1}) - (2^{r-1} - 2^{r-i}) \\ = \; & 2^r - 2^{r-i}. \end{aligned}$$

From the above arguments, we complete the proof. □

In the Reed-Muller codes, there are the following dual relations [11, Theorem 1.10.1]:

$$R(r, r) = \{\mathbf{0}\}^{\perp}, R(r-1, r) = R(0, r)^{\perp}, R(r-2, r) = R(1, r)^{\perp}.$$

Since we already know $W^0(\{\mathbf{0}\}; y) = 1$ and $W^1(R(0, r); y) = y^{2^r}$, using Theorem 2.9 and Theorem 2.8, we can easily calculate the higher weight spectrums of $R(r-2,r)$, $R(r-1,r)$ and $R(r,r)$ (Note that $R(r,r)$ is the entire space $\mathbb{F}_2^{2^r}$). We give the computational results for $R(1,r)$ and $R(r-2,r)$ for $r=2,3,4$ in Tables 13 to 18 which can be found in [2] (Note that $R(1,3)$ is the $[8,4,4]$ extended Hamming self-dual code).

2.1. Higher weight distributions of codes from projective planes

We can examine some of the higher weight enumerators which were not found for the projective plane of order 5 in [6]. Let Π be the projective plane of order n and let $C_p(\Pi)$ be the code from the projective plane of order n. The Hull of the plane Π is defined as $\mathrm{Hull}_p(\Pi) = C_p(\Pi) \cap C_p(\Pi)^\perp$ and is a self-orthogonal code.

We know from [6] that $\mathrm{Hull}_p(\Pi)$ is of codimension 1 in $C_p(\Pi)$ and $C_p(\Pi) = \langle \mathrm{Hull}_p(\Pi), \mathbf{1}\rangle$. If p sharply divides n, then $\mathrm{Hull}_p(\Pi) = C_p(\Pi)^\perp$. Additionally we know that for $1 \le k \le \dim(C_p(\Pi))$, we have

$$d_k(C_p(\Pi)) \ge d_{k-1}(\mathrm{Hull}_p(\Pi)).$$

For more details, refer to [6].

We shall calculate some of the higher weight distributions of the code and the Hull of the projective plane of order 5.

We know that $C_5(\Pi)$ is a $[31,16]$ code over $\mathbb{F}_5$ and that $\mathrm{Hull}_5(\Pi)$ is a $[31,15]$ code over $\mathbb{F}_5$. We use the known weight enumerator $W^1(C_5(\Pi))$ [14] to obtain by Equation 1 the weight enumerator $W^1(\mathrm{Hull}_5(\Pi))$. Then we have that $d_1(C_5(\Pi)) = 6$ and $d_1(\mathrm{Hull}_5(\Pi)) = 10$. Let

$$\begin{aligned} W^i(C_5(\Pi)) &= a_{i+8}y^{i+8} + a_{i+9}y^{i+9} + \cdots + a_{31}y^{31}, \\ W^i(\mathrm{Hull}_5(\Pi)) &= b_{i+9}y^{i+9} + b_{i+10}y^{i+10} + \cdots + b_{31}y^{31}, \end{aligned}$$

where $2 \le i \le 16$.

We apply the MacWilliams relations to

$$W^0(C_5(\Pi)), W^1(C_5(\Pi)), \ldots, W^i(C_5(\Pi))$$

and

$$W^0(\mathrm{Hull}_5(\Pi)), W^1(\mathrm{Hull}_5(\Pi)), \ldots, W^i(\mathrm{Hull}_5(\Pi))$$

for $2 \le i \le 16$, sequentially. By a Maple calculation, we determined $W^i(C_5(\Pi))$ for $8 \le i \le 16$ and $W^i(\mathrm{Hull}_5(\Pi))$ for $8 \le i \le 15$. But the others remain undetermined. The weight enumerators can be found in [1].

Remark 2. Note that $C_5(\Pi)$ is a P_8-MDS code and that $\mathrm{Hull}_5(\Pi)$ is a P_{11}-MDS code. Compared to what follows from Theorem 2.5, we have obtained additional results for

$$W^8(\mathrm{Hull}_5(\Pi)), W^9(\mathrm{Hull}_5(\Pi)), \text{ and } W^{10}(\mathrm{Hull}_5(\Pi))$$

by the above calculation.

Remark 3. If we use the fact that $d_2(C_5(\Pi)) \ge 10$, then the weight enumerators $W^i(\mathrm{Hull}_5(\Pi))$ $(i \ge 8)$ can be calculated using Equation 9.

3. A non-linear version of the generalized Singleton bound

The Singleton bound applies to either linear or non-linear codes. For non-linear codes it applies to the distance between vectors rather than the weight of vectors, where the distance between two vectors is the number of coordinates in which they differ. Specifically, if d is the minimum distance of a length n code C (linear or not) over an alphabet of size q with $|C| = M$, then

$$M \leq q^{n-d+1}.$$

This immediately gives the usual form of the Singleton bound:

$$\log_q(M) \leq n - d + 1.$$

We shall generalize this to higher weights. We begin with a definition.

Let C be a length n code over an alphabet of size q. Let $D \subseteq C$. Note that we are not assuming that either C or D is linear. Define

$$||D|| = |\{i \mid \text{ there exist } v, w \in D \text{ with } v_i \neq w_i\}|$$

(cf. This definition is the same as the definition of the support of a non-linear code given in [17]). That is, it is the number of coordinates where there are at least two vectors that differ there. If D is linear, then $||D||$ is the size of the support of D since the zero vector is present. Therefore, this definition coincides with our previous definition for linear codes.

Define

$$d_r = d_r(C) = \min\{||D|| \mid D \subseteq C, q^{r-1} < |D| \leq q^r\}. \tag{10}$$

Again, if C and D are linear, then this coincides with the usual definition.

Lemma 3.1. *Let C be a length n code over an alphabet of size q with $|C| = M$ and $q^{k-1} < M \leq q^k$ for some k. Then*

$$1 \leq d_1(C) < d_2(C) < d_3(C) < \cdots < d_k(C) \leq n.$$

Proof. Let D be a code of size $|D| > q^{r-1}$ with $||D|| = d_r$. Pick a coordinate i where there exist $\mathbf{v}, \mathbf{w} \in D$ with $\mathbf{v}_i \neq \mathbf{w}_i$. Let α be the element that appears the most in that coordinate. Let $D' = \{\mathbf{v} \mid \mathbf{v}_i = \alpha\}$. The pigeon hole principle gives that $|D'| \geq \frac{1}{q}|D|$, with equality when dealing with linear codes. Remove elements of D' to form D'' so that $q^{r-2} < |D''| \leq q^{r-1}$. Then $||D''|| < d_r$, since the number of coordinates in D'' where there are vectors that differ is strictly less than that of D. This gives that $d_r > d_{r-1}$. □

Theorem 3.2. *Let C be a length n code over an alphabet of size q with $|C| = M$ and $q^{k-1} < M \leq q^k$ for some k. Then for $1 \leq r \leq k$,*

$$\log_q(M) \leq n - d_r + r.$$

Proof. We shall prove the result by induction. Let $r = k$. Using $M \leq q^k$, we have $\log_q(M) \leq k$. Then we have that $n \leq n - \log_q(M) + k$ and clearly $d_k \leq n$. Therefore $d_k \leq n - \log_q(M) + k$ and the theorem holds for $r = k$.

Assume $d_r \leq n - \log_q(M) + r$. By Lemma 3.1, $d_{r-1} \leq d_r - 1$, which gives that $d_{r-1} \leq n - \log_q(M) + (r-1)$. Then we have the result. □

If $M = q^k$ this gives the usual

$$k \leq n - d_r + r.$$

Rearranging we have

$$d_r \leq n - k + r.$$

Theorem 3.3. *Let C be an $[n,k]$ linear code over $\mathbb{F}_q$ and $E = \mathbf{a} + C$ for some $\mathbf{a} \in \mathbb{F}_q^n$. Then the value $d_r(C)$ as a linear code is equal to the value $d_r(E)$ as a non-linear code.*

Proof. Let $D' \subseteq C$ with $\dim(D') = r$ and $||D'|| = d_r(C)$. Let $D'' = \mathbf{a} + D'$. Note that $||D''|| = ||D'||$ and

$$||D''|| \in \{||D|| \mid D \subseteq E, q^{r-1} < |D| \leq q^r\}.$$

This gives that $||D'|| \geq d_r(E)$ and $d_r(C) \geq d_r(E)$. For the other inequality, let $D' \subseteq E$ with $q^{r-1} < |D'| \leq q^r$ and $||D'|| = d_r(E)$. Fix an element $\mathbf{v} \in D'$. Define $D'' = \langle\{\mathbf{v} - \mathbf{w} | \mathbf{w} \in D'\}\rangle$. Note that $||D''|| = ||D'||$ and $\dim(D'') \geq r$. So, $||D''|| \geq d_r(C)$ and $d_r(C) \leq d_r(E)$. □

Example 5. Let C be a Type I binary self-dual code and S be the shadow code of C. From Theorem 3.3, the value $d_r(S)$ as a non-linear code is equal to the value $d_r(C)$ as a linear code. Note that this does not imply that the minimum weight of the shadow and the code is the same but rather that their minimum distances are the same.

Theorem 3.4. *Let C be the $(16, 256, 6)$ Nordstrom-Robinson code. Then*

$$\{d_r(C) | 1 \leq r \leq 8\} = \{6, 9, 10, 12, 13, 14, 15, 16\}.$$

Proof. By definition, $d_1 = 6$. Note that we can rewrite Equation 10 as the following:

$$d_r = d_r(C) = \min\{||D|| \mid D \subseteq C, |D| = 2^{r-1} + 1\}.$$

To show $d_2 = 9$, let $D = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} \subseteq C$ with $||D|| = d_2$. By [13, Fig. 2.18], $(\mathbf{a}_1|\mathbf{v}_1), (\mathbf{a}_2|\mathbf{v}_2), (\mathbf{a}_3|\mathbf{v}_3)$ are codewords of the Golay code of length 24, where

$$\begin{aligned} \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3 \quad \in \quad & \{(0,0,0,0,0,0,0,0), (1,0,0,0,0,0,0,1), (0,1,0,0,0,0,0,1), \\ & (0,0,1,0,0,0,0,1), \ldots, (0,0,0,0,0,0,1,1)\}. \end{aligned}$$

We know that for the Golay code d_2 is 12. Then we have

$$\begin{aligned} 12 \quad &\leq \quad ||\langle \mathbf{a}_1|\mathbf{v}_1 - \mathbf{a}_2|\mathbf{v}_2, \mathbf{a}_1|\mathbf{v}_1 - \mathbf{a}_3|\mathbf{v}_3\rangle|| \\ &= \quad ||\langle \mathbf{a}_1 - \mathbf{a}_2, \mathbf{a}_1 - \mathbf{a}_3\rangle|| + ||\langle \mathbf{v}_1 - \mathbf{v}_2, \mathbf{v}_1 - \mathbf{v}_3\rangle|| \\ &\leq \quad 3 + d_2. \end{aligned}$$

This gives that $9 \leq d_2$. By [11, Example 12.2.5], C is the Gray image of the $\mathbb{Z}_4$-linear code O_8, the octacode, with generator matrix:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{bmatrix}.$$

The set of two Gray images of the first and second rows of G and the zero codeword has support size 9. This gives that $d_2 = 9$.

By Magma [4] computation, we confirmed that $d_3 = 10$ and $d_4 = 12$. The remaining parts of the theorem follow from Lemma 3.1. □

Remark 4. By Magma computation, we calculated the following values for the Nordstrom-Robinson code.

Number of codewords	2	3	4	5	6	7	8	9
Minimum support size	6	9	10	10	10	11	11	12

4. Calculation of higher weight distributions for some Type II self-dual codes

One of the most interesting and difficult open problems in coding theory is the existence of extremal $[24k, 12k, 4k+4]$ codes. For $k = 1$ and $k = 2$ there are unique codes. For $k = 3$ the question remains open. We shall compute many of the higher weight enumerators for these codes when $1 \leq k \leq 3$.

In Example 4, we showed that we can calculate some higher weight distributions of the putative $[72, 36, 16]$ Type II codes using Theorem 2.5. In this section, we show that we can calculate these higher weight distributions with MacWilliams identities. In fact, we can calculate much more than Example 4.

We will need the following easy and well known lemma.

Lemma 4.1. *Let M be a $q^k \times n$ matrix whose rows are the codewords of an $[n, k]$ code C over $\mathbb{F}_q$. Then a column of M either consists of zeros or contains every element of $\mathbb{F}_q$ an equal number of times.*

4.1. The $[72, 36, 16]$ Type II code

Let C be the $[72, 36, 16]$ Type II code. We know W^0, W^1, and W^2 [5].

Lemma 4.2. *Let C be the* $[72, 36, 16]$ *Type II code. Then for the weight hierarchy of C, the following hold*:

$$d_1 = 16,\ d_2 = 24,\ 28 \leq d_3 \leq 33,\ 30 \leq d_4 \leq 38,\ 31 \leq d_5 \leq 39,$$
$$32 \leq d_6 \leq 40,\ 35 \leq d_7 \leq 41,\ 36 \leq d_8 \leq 42,\ 38 \leq d_9 \leq 43,\ 40 \leq d_{10} \leq 44,$$
$$41 \leq d_{11} \leq 45,\ d_{12} = 46,\ d_{13} = 47,\ d_{14} = 48,\ d_{15+i} = 50 + i\ (0 \leq i \leq 6),$$
$$d_{22+i} = 58 + i\ (0 \leq i \leq 14).$$

Proof. By definition $d_1 = 16$ and we have $d_2 = 24$ by [5].

Using Lemma 4.1, we can prove that $28 \leq d_3$ by the following argument. Suppose that D is a 3-dimensional subcode with support size 27. Let M be a 8×72 matrix whose rows are the codewords of D. By Lemma 4.1, 1 appears $4 \cdot 27 = 108$ times in M; but M has 7 rows of weight at least 16, implying that 1 appears at least 112 times in M, a contradiction. We can apply this argument to prove $30 \leq d_4$. Then we have

$$28 \leq d_3,\ 30 \leq d_4.$$

Using Equation 7, we have the following result. Since $1, 2, \ldots, 15 \notin \{d_r(C) \mid 1 \leq r \leq 36\}$, $58, 59, \ldots, 72 \in \{d_r(C^\perp) \mid 1 \leq r \leq 36\}$. Since $16 \in \{d_r(C) \mid 1 \leq r \leq 36\}$, $57 \notin \{d_r(C^\perp) \mid 1 \leq r \leq 36\}$. Since $17, 18, \ldots, 23 \notin \{d_r(C) \mid 1 \leq r \leq 36\}$, $50, 51, \ldots, 56 \in \{d_r(C^\perp) \mid 1 \leq r \leq 36\}$. Since $24 \in \{d_r(C) | 1 \leq r \leq 36\}$, $49 \notin \{d_r(C^\perp) \mid 1 \leq r \leq 36\}$. Since $25, 26, 27 \notin \{d_r(C) \mid 1 \leq r \leq 36\}$, $46, 47, 48 \in \{d_r(C^\perp) \mid 1 \leq r \leq 36\}$. In conclusion, we have the following.

$$\{16, 24, 46, 47, 48, 50, \ldots, 56, 58, \ldots, 72\} \subset \{d_r \mid 1 \leq r \leq 36\}, \tag{11}$$

$$\{d_r \mid 1 \leq r \leq 36\} \subset (\{16, 24, 46, 47, 48, 50, \ldots, 56, 58, \ldots, 72\} \cup \{28, \ldots, 45\}). \tag{12}$$

By Equations 11, 12, and 5, the following hold:

$$d_{22+i} = 58 + i\ (0 \leq i \leq 14),\ d_{15+i} = 50 + i\ (0 \leq i \leq 6),$$
$$d_{14} = 48,\ d_{13} = 47,\ d_{12} = 46,$$

and

$$\{d_r \mid 3 \leq r \leq 11\} \subset \{28, \ldots, 45\}.$$

By the table in [8], the highest minimum distance of a $[34, 7]$ binary linear code is 15. Therefore $35 \leq d_7$. We can apply similar argument to d_9 and d_{10}. Then we have

$$35 \leq d_7,\ 38 \leq d_9,\ 40 \leq d_{10}.$$

Using the MacWilliams identities, we can check that $d_3 \leq 33$ as follows. We know W^1 and W^2 [5]. Let $W^3 = \sum_{i=28}^{72} a_i y^i$. First we have relations among the a_i by applying Equation 1 to W^0, W^1, W^2 and W^3. Then we check whether there is a possible solution for all non-negative a_i. In our Maple calculation, there is a feasible solution for $28 \leq d_3 \leq 33$. But there is no feasible solution for $34 \leq d_3$. This gives that

$$d_3 \leq 33.$$

This completes the proof of Lemma 4.2. □

Let

$$W^3 = a_{28}y^{28} + a_{29}y^{29} + \cdots + a_{72}y^{72}.$$

Apply the MacWilliams relations to W^0, W^1, W^2, W^3. We can not determine all coefficients of W^3. In a similar way we can not determine W^i for $4 \leq i \leq 11$. There remain many undetermined variables in these cases. But we do obtain the following: $39 \leq d_9 \leq 43$ and $44 \leq d_{11} \leq 45$. In other words, by a Maple calculation we checked that $d_9 \neq 38$ and $d_{11} \neq 41, 42, 43$. We continue this process for $W^{12}, \ldots, W^{36}$ sequentially and we can determine all the weight distributions for $W^i, 12 \leq i \leq 36$ sequentially. In conclusion, we know all W^i except W^i for $3 \leq i \leq 11$.

The higher weight enumerators for this code can be found at [1].

Remark 5. Equation 9 and Remark 1 indicate that $W^i(12 \leq i)$ can be calculated since $d_2 = 24$, $d_3 \geq 28$, and we know W^2 for the Type II $[72, 36, 16]$ code.

Open Problem: Determine the remaining higher weight enumerators for the extremal $[72, 36, 16]$ Type II code. That is find W^i for $3 \leq i \leq 11$.

References

[1] http://kutacc.kut.ac.kr/∼sunghyu/data/hw/HW-P5-48-72.pdf

[2] http://kutacc.kut.ac.kr/∼sunghyu/data/hw/HW-SHRM.pdf

[3] D. Britz, T. Britz, K. Shiromoto, and H. K. Sørensen, *The higher weight enumerators of the doubly-even, self-dual* $[48, 24, 12]$ *code*, IEEE Trans. Inform. Theory **53** (2007), no. 7, 2567–2571.

[4] J. Cannon and C. Playoust, *An Introduction to Magma*, University of Sydney, Sydney, Australia, 1994.

[5] S. T. Dougherty, T. A. Gulliver, and M. Oura, *Higher weights and graded rings for binary self-dual codes*, Discrete Appl. Math. **128** (2003), no. 1, 121–143.

[6] S. T. Dougherty and R. Ramadurai, *Higher weights of codes from projective planes and biplanes*, Math. J. Okayama Univ. **49** (2007), 149–161.

[7] S. T. Dougherty and K. Shiromoto, *MDR codes over* Z_k, IEEE Trans. Inform. Theory **46** (2000), no. 1, 265–269.

[8] M. Grassl, *Bounds on the minimum distance of linear codes*, online available at http://www.codetables.de. Accessed on 2008-03-09.

[9] T. Helleseth, T. Kløve, and J. Mykkeltveit, *The weight distribution of irreducible cyclic codes with block length* $n_1((q^l - 1)/N)$, Discrete Math. **18** (1977), no. 2, 179–211.

[10] H. Horimoto and K. Shiromoto, *A Singleton bound for linear codes over quasi-Frobenius rings*, Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii (USA), 51–52 (1999).

[11] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[12] T. Kløve, *Support weight distribution of linear codes*, A collection of contributions in honour of Jack van Lint. Discrete Math. **106/107** (1992), 311–316.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes I, II*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[14] G. McGuire and H. N. Ward, *The weight enumerator of the code of the projective plane of order* 5, Geom. Dedicata **73** (1998), no. 1, 63–77.

[15] H. G. Schaathun, *Duality and support weight distributions*, IEEE Trans. Inform. Theory **50** (2004), no. 5, 862–867.

[16] J. Simonis, *The effective length of subcodes*, Appl. Algebra Engrg. Comm. Comput. **5** (1994), no. 6, 371–377.

[17] M. A. Tsfasman and S. G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), no. 6, part 1, 1564–1588.

[18] L. R. Vermani, *Elements of Algebraic Coding Theory*, Chapman and Hall Mathematics Series. Chapman and Hall, Ltd., London, 1996.

[19] V. K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA
E-mail address: doughertys1@scranton.edu

Sunghyu Han
School of Liberal Arts
Korea University of Technology and Education
Cheonan 330-708, Korea
E-mail address: sunghyu@kut.ac.kr