Binomial moments for divisible self-dual codes

Iwan Duursma*

May 31, 2009 / August 31, 2009

Abstract

For self-dual codes with all weights divisible by an integer greater than one, the minimum distance is bounded by the Mallows-Sloane upper bounds and by their improvements due to Krasikov-Litsyn and Rains. We obtain the improved upper bounds from short relations with constant coefficients on suitable binomial moments of the codes. In this approach, the Mallows-Sloane bounds are analogues of the Singleton bound and the improved bounds are analogues of the Plotkin bound.

1 Introduction

For a linear code of length n and dimension k over a finite field $\mathbb{F}$, the minimum distance d is the smallest Hamming distance between any two distinct words. A trivial upper bound for the minimum distance is given by the Singleton bound $d \leq n-k+1$. For a code with dual minimum distance $d^\perp$, it follows that

$$d + d^\perp \leq n + 2. \tag{1}$$

A code is divisible by c if the Hamming distance between any two words is a multiple of c. In [2], the author gives improvements of the Singleton bound for divisible codes. In general,

$$d + cd^\perp \leq n + c(c+1). \tag{2}$$

For binary codes that contain the all-one word,

$$2d + cd^\perp \leq n + c(c+2). \tag{3}$$

*Address: Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street, Urbana IL 61801, USA. E-mail: duursma@math.uiuc.edu.

The Mallows-Sloane upper bounds for the minimum distance of a divisible self-dual code [4] are obtained as a special case with the substitution $d^\perp = d$. The Gleason-Pierce theorem shows that divisible self-dual codes with $d > 2$ exist, over a field $\mathbb{F}$ of q elements, only if $(q, c) = (2, 2), (2, 4), (3, 3), (4, 2)$. For doubly-even binary self-dual codes, the case $(q, c) = (2, 4)$, Krasikov and Litsyn [3] obtained an asymptotic improvement of the Mallows-Sloane upper bound.

$$d/n \lesssim \frac{1}{2}\left(1 - \frac{1}{\sqrt[4]{5}}\right).$$

Rains [5] proved a generalized bound that holds for all four types of divisible self-dual codes.

$$d/n \lesssim \frac{q-1}{q}\left(1 - \frac{1}{\sqrt[c]{c+1}}\right).$$

All bounds follow from linear relations among the coefficients of the weight enumerator. The improved bounds exploit the sign pattern of the smallest possible relation among the leading coefficients in the weight enumerator. The analysis of the sign pattern requires a choice on how to represent weight enumerators and how to express MacWilliams duality for weight enumerators. Krasikov and Litsyn use Krawchouck polynomials to represent weight enumerators and find the relation with Delsarte's method. Rains uses invariant theory and Gleason's theorem to represent weight enumerators and the Bürmann-Lagrange theorem to find the relation. Both methods require a considerable amount of analysis to locate the sign changes in the sign pattern of the relation. Our approach can be seen as a two step version of the last method. Instead of using the Bürmann-Lagrange theorem to obtain relations for the coefficients of the weight enumerator we describe relations among suitable binomial moments. These relations turn out to be of finite length with coefficients that depend only on the class of the code (i.e. the values for q and c) but not on the codelength n. From these short relations a short and elementary argument gives the improved bounds. The proof using binomial moments separates the roles of q and n. The argument that gives the improved bounds by putting the two parts together is analogous to the Plotkin bound.

In the next section, we present our approach for arbitrary self-dual codes. In Section 3, we redefine binomial moments in two different ways for divisible codes. In Section 4, we determine relations among the binomial moments of a divisible self-dual code. In Section 5, we use the relations to obtain asymptotic upper bounds for the minimum distance of divisible self-dual codes.

2 Self-dual codes

In this section, we illustrate our approach by proving the asymptotic upper bound $d/n \lesssim (1-1/q)/2$ for the relative distance of a general self-dual code. The bound is the special case $c = 1$ of the Rains bound and the special case $k/n = 1/2$ of the asymptotic Plotkin bound $d/n \lesssim (1-1/q)(1-k/n)$. In the next sections we refine the arguments in the proof in order to obtain bounds for divisible self-dual codes. Let C be a linear code of length n over the field of q elements, and let A_w denote the number of words of weight w in C. The weight enumerator of C is the polynomial

$$A(X,Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

The weight enumerator of the dual code is obtained with the MacWilliams transform

$$A^{\perp}(X,Y) = \frac{1}{|C|} A(X+\gamma Y, X-Y), \qquad \gamma = q-1.$$

The binomial moments of the code are defined as

$$B_i = \sum_{w=0}^{i} \binom{n-w}{n-i} A_w, \qquad i = 0,1,\ldots,n. \tag{4}$$

The binomial moments appear as coefficients of the weight enumerator when it is written out on a different basis.

$$A(X,Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w = \sum_{i=0}^{n} B_i (X-Y)^{n-i} Y^i.$$

The moment enumerator of C is the polynomial $B(X,Y) = \sum_{i=0}^{n} B_i X^{n-i} Y^i$. The transform for the dual moment enumerator is

$$B^{\perp}(X,Y) = A^{\perp}(X+Y,Y) = \frac{1}{|C|} A(X+qY,X) = \frac{1}{|C|} B(qY,X).$$

For a self-dual code of length $n = 2m$, the transform amounts to the $m+1$ identities

$$B_{m+r} = q^r B_{m-r}, \qquad r = 0,1,\ldots,m. \tag{5}$$

The term $A_0 = 1$ appears with multiplicity $\binom{n}{i}$ in the binomial moment B_i. After dividing both sides by $\binom{n}{i}$, Equation (4) becomes

$$\frac{B_i}{\binom{n}{i}} = \sum_{w=0}^{i} \binom{i}{w} \frac{A_w}{\binom{n}{w}}.$$

With (5), for $r = 0, 1, \ldots, m$,

$$0 = \frac{B_{m+r}}{\binom{n}{m+r}} - q^r \frac{B_{m-r}}{\binom{n}{m-r}} = \sum_{w=0}^{m+r} \frac{A_w}{\binom{n}{w}} \left(\binom{m+r}{w} - q^r \binom{m-r}{w} \right).$$

Combination of the identities for $r = 1$ and $r = 2$ yields a relation among $A_1, A_2, \ldots, A_{m+2}$,

$$\begin{aligned} 0 &= \frac{B_{m+2}}{\binom{n}{m+2}} - q^2 \frac{B_{m-2}}{\binom{n}{m-2}} - (q+1)\left(\frac{B_{m+1}}{\binom{n}{m+1}} - q \frac{B_{m-1}}{\binom{n}{m-1}} \right) \\ &= \sum_{w=1}^{m+2} \frac{A_w}{\binom{n}{w}} \left[\left(\binom{m+2}{w} - q^2 \binom{m-2}{w} \right) - (q+1)\left(\binom{m+1}{w} - q \binom{m-1}{w} \right) \right]. \end{aligned}$$

For $0 \le s \le 4$, we use the approximation

$$\binom{m+2-s}{w} = \binom{m+2}{w} \cdot \left[\left(\frac{m-w}{m} \right)^s + O(m^{-1}) \right], \quad \text{as } m \longrightarrow \infty.$$

For $T = (m-w)/m$,

$$\begin{aligned} 0 &= \sum_{w=1}^{m+2} A_w \frac{\binom{m+2}{w}}{\binom{n}{w}} \left[(1 - q^2 T^4) - (q+1)(T - qT^3) + O(m^{-1}) \right]. \\ &= \sum_{w=1}^{m+2} A_w \frac{\binom{m+2}{w}}{\binom{n}{w}} \left[(1-T)(1-qT)(1-qT^2) + O(m^{-1}) \right]. \end{aligned} \tag{6}$$

Equation (6) shows that, as $m \longrightarrow \infty$, the contribution of A_w to the right side is negative for w/m in the range $w/m \in (1 - 1/\sqrt{q}, 1 - 1/q)$ and positive for w/m outside that range. It follows that, as $n \longrightarrow \infty$, $A_w \neq 0$ for some $w/m \le 1 - 1/q$, and $d/n \lesssim (1 - 1/q)/2$.

3 Binomial moments

For a divisible code of length $N = cn$, let A_w denote the number of words of weight cw, for $w = 0, 1, \ldots, n$. The weight enumerator of the code is the polynomial

$$A(X, Y) = \sum_{w=0}^{n} A_w (X^c)^{n-w} (Y^c)^w.$$

Define binomial moments B_i, for $i = 0, 1, \ldots, n$, by

$$B_i = \sum_{w=0}^{i} A_w \binom{n-w}{n-i}. \tag{7}$$

The moments satisfy the transformation

$$\sum_{w=0}^{n} A_w (X^c)^{n-w} (Y^c)^w = \sum_{i=0}^{n} B_i (X^c - Y^c)^{n-i} (Y^c)^i, \tag{8}$$

Or, for $\eta = Y^c/X^c$,

$$\sum_{w=0}^{n} A_w \eta^w = \sum_{i=0}^{n} B_i \eta^i (1-\eta)^{n-i}. \tag{9}$$

For a binary divisible code of length $N = cn$, with n even such that $A_{n-w} = A_w$ for $w = 0, 1, \ldots, n$, we define binomial moments B_i differently. For $i = 0, 1, \ldots, n/2$, let

$$B_i = \sum_{w=0}^{i} A_w \binom{n-i-w}{n-2i} \frac{n-2w}{n-i-w}. \tag{10}$$

The definition corresponds to the transformation

$$\sum_{w=0}^{n} A_w (X^c)^{n-w} (Y^c)^w = \sum_{i=0}^{n/2} B_i (X^c - Y^c)^{n-2i} (X^c Y^c)^i. \tag{11}$$

Or, for $\eta = Y^c/X^c$,

$$\sum_{w=0}^{n} A_w \eta^w = \sum_{i=0}^{n/2} B_i \eta^i (1-\eta)^{2(n/2-i)}. \tag{12}$$

The correspondence between (10) and (11) is based on the identity, for n even,

$$(x^n + y^n) = \sum_{i=0}^{n/2} \frac{n}{n-i} \binom{n-i}{n-2i} (xy)^i (x-y)^{n-2i}.$$

Another approach is given by Lemma 4.1 in the next section. Applied to (12), with $g(t) = (1-t)^2$, it yields

$$B_i \;=\; [t^i]\,(g(t) - tg'(t)) g(t)^{i-m-1} \,(\sum_{w=0}^{2m} A_w t^w).$$

From this one easily obtains (10).

4 Divisible self-dual codes

By the Gleason-Pierce theorem the nontrivial self-dual divisible codes are of four types. For each type, the ring of invariants generated by the weight enumerators is of the form $\mathbb{C}[F, G]$.

$$\begin{array}{lllll} (q,c) = & (2,2) & F = & X^2Y^2(X^2-Y^2)^2 & G = & X^2+Y^2 \\ & (2,4) & & X^4Y^4(X^4-Y^4)^4 & & X^8+14X^4Y^4+Y^8 \\ & (3,3) & & Y^3(X^3-Y^3)^3 & & X^4+8XY^3 \\ & (4,2) & & Y^2(X^2-Y^2)^2 & & X^2+3Y^2 \end{array}$$

For each of the four types, we express the weight enumerator $A(X, Y)$ as a polynomial in the invariants F and G and we compare this with an expression in terms of binomial moments.

The case $(q, c) = (3, 3)$**.** Let $A(X, Y)$ be a weight enumerator of degree $N = 3n = 12m$. Let $U = X^3 - Y^3, V = Y^3$, so that $F = U^3V$ and $G^3 = (U+V)(U+9V)^3$. There exist $C_j, j = 0, 1, \ldots, m$ such that

$$A(X,Y) = \sum_{i=0}^{n} B_i U^{n-i} V^i = \sum_{j=0}^{m} C_j F^j G^{3m-3j}.$$

The binomial moments B_i are defined as in (7). For $t = V/U$,

$$\sum_{i=0}^{n} B_i t^i = \sum_{j=0}^{m} C_j t^j g(t)^{m-j}, \qquad g(t) = (1+t)(1+9t)^3. \tag{13}$$

The case $(q, c) = (4, 2)$**.** Let $A(X, Y)$ be a weight enumerator of degree $N = 2n = 6m$. Let $U = X^2 - Y^2, V = Y^2$, so that $F = U^2V$ and $G^3 = (U + 4V)^3$. There exist $C_j, j = 0, 1, \ldots, m$ such that

$$A(X,Y) = \sum_{i=0}^{n} B_i U^{n-i} V^i = \sum_{j=0}^{m} C_j F^j G^{3m-3j}.$$

The binomial moments B_i are defined as in (7). For $t = V/U$,

$$\sum_{i=0}^{n} B_i t^i = \sum_{j=0}^{m} C_j t^j g(t)^{m-j}, \qquad g(t) = (1+4t)^3. \tag{14}$$

The case $(q,c) = (2,2)$**.** Let $A(X,Y)$ be the weight enumerator of a code of length $N = 2n = 8m$. Let $U = (X^2 - Y^2)^2, V = X^2Y^2$, so that $F = UV$ and $G^4 = (U + 4V)^2$. There exist $C_j, j = 0, 1, \ldots, m$ such that

$$A(X,Y) = \sum_{i=0}^{n/2} B_i U^{n/2-i} V^i = \sum_{j=0}^{m} C_j F^j G^{4m-4j}.$$

The binomial moments B_i are defined as in (10). For $t = V/U$,

$$\sum_{i=0}^{n/2} B_i t^i = \sum_{j=0}^{m} C_j t^j g(t)^{m-j}, \qquad g(t) = (1+4t)^2. \tag{15}$$

The case $(q,c) = (2,4)$**.** Let $A(X,Y)$ be the weight enumerator of a code of length $N = 4n = 24m$. Let $U = (X^4 - Y^4)^2, V = X^4Y^4$, so that $F = U^2V$ and $G^3 = (U + 16V)^3$. There exist $C_j, j = 0, 1, \ldots, m$ such that

$$A(X,Y) = \sum_{i=0}^{n/2} B_i U^{n/2-i} V^i = \sum_{j=0}^{m} C_j F^j G^{3m-3j}.$$

The binomial moments B_i are defined as in (10). For $t = V/U$,

$$\sum_{i=0}^{n/2} B_i t^i = \sum_{j=0}^{m} C_j t^j g(t)^{m-j}, \qquad g(t) = (1+16t)^3. \tag{16}$$

Equations (13), (14), (15), (16) imply relations among the binomial moments. The relations are given in Proposition 4.3. The general procedure to obtain the relation is to use the Bürmann-Lagrange theorem, for example in the form of Lemma 3.1 and Corollary 3.2 in [5]. The special case that we need is a direct consequence of the following lemma.

Lemma 4.1. *Let $g(t)$ be a polynomial with $g(0) = 1$. For $r \in \mathbb{Z}$,*

$$[t^r]\ (g(t) - tg'(t))g(t)^{r-1} = \begin{cases} 1 & \text{if } r = 0. \\ 0 & \text{if } r \neq 0. \end{cases}$$

Proof. The cases $r = 0$ and $r < 0$ are immediate. For $r > 0$,

$$\begin{aligned} [t^r]g(t)^r &= \frac{1}{r!}\left(\frac{\partial^r g(t)^r}{\partial t^r}\right)_{t=0} \\ &= \frac{1}{(r-1)!}\left(\frac{\partial^{r-1} g'(t)g(t)^{r-1}}{\partial t^{r-1}}\right)_{t=0} = [t^{r-1}]g'(t)g(t)^{r-1}. \end{aligned}$$

□

Lemma 4.2. *Let $g(t)$ be a polynomial of degree $\ell \geq 1$ with $g(0) = 1$, and let*

$$\sum_{i=0}^{\ell m} B_i t^i = \sum_{j=0}^{m} C_j t^j g(t)^{m-j}.$$

Then, for $r \geq 1$,

$$[t^{m+r}](g(t) - tg'(t))g(t)^{r-1} \sum_{i=m+r-\ell r}^{m+r} B_i t^i = 0$$

Proof. Use the previous lemma. For $0 \leq j \leq m < m + r$,

$$[t^{m+r}](g(t) - tg'(t))g(t)^{r-1} t^j g(t)^{m-j} \;=\; [t^{m+r-j}](g(t) - tg'(t))g(t)^{m+r-j-1} \;=\; 0.$$

□

Proposition 4.3. *For codes of types $(q, c) = (3, 3), (4, 2)$, let*

$$B_i = \sum_{w=0}^{i} A_w \binom{n-w}{n-i}, \quad g(t) = \begin{cases} (1+t)(1+9t)^3 & \text{if } (q,c) = (3,3). \\ (1+4t)^3 & \text{if } (q,c) = (4,2). \end{cases}$$

For codes of types $(q, c) = (2, 2), (2, 4)$, let

$$B_i = \sum_{w=0}^{i} A_w \binom{n-i-w}{n-2i} \frac{n-2w}{n-i-w}, \quad g(t) = \begin{cases} (1+4t)^2 & \text{if } (q,c) = (2,2). \\ (1+16t)^3 & \text{if } (q,c) = (2,4). \end{cases}$$

The binomial moments B_i satisfy, for any real number α,

$$[t^{m+2}](g(t) - tg'(t))(g(t) - \alpha t) \sum_{i=m+2-2\ell}^{m+2} B_i t^i = 0. \tag{17}$$

Proof. Apply the lemma to Equations (13), (14), (15), (16). □

5 Asymptotic bounds

Using Proposition 4.3 we obtain relations among the leading coefficients $A_1, A_2, \ldots, A_{m+2}$ of the weight enumerator of a divisible self-dual code. To obtain relations we first substitute in (17) the expressions for the binomial moments B_i.

Recall that for a divisible self-dual code we use the following notation. Codes are of length $N = cn$ and minimum distance d. For $w = 0, 1, \ldots, n$, the coefficient A_w in the weight enumerator gives the number of words of weight cw. For the cases $(q, c) = (3, 3), (4, 2)$, $n = \ell m$, $\ell = c + 1$, and for the cases $(q, c) = (2, 2), (2, 4)$, $n/2 = \ell m$, $2\ell = c + 2$.

The cases $(q, c) = (3, 3), (4, 2)$**.**

$$B_i = \sum_{w=0}^{i} \beta_{i,w} A_w, \qquad \beta_{i,w} = \binom{n-w}{n-i}.$$

For the binomial moments in the finite interval $B_{m+2}, B_{m+1}, \ldots, B_{m+2-2\ell}$, where ℓ is the degree of the polynomial $g(t)$, we use the approximation, as $m \longrightarrow \infty$,

$$\beta_{m+2-s,w} = \beta_{m+2,w}(t_w^s + O(m^{-1})), \qquad t_w = (m-w)/(n-m).$$

The cases $(q, c) = (2, 2), (2, 4)$**.**

$$B_i = \sum_{w=0}^{i} \beta_{i,w} A_w, \qquad \beta_{i,w} = \frac{n-2w}{n-2w-i}\binom{n-i-w}{n-2i}.$$

For the binomial moments in the finite interval $B_{m+2}, B_{m+1}, \ldots, B_{m+2-2\ell}$, where ℓ is the degree of the polynomial $g(t)$, we use the approximation, as $m \longrightarrow \infty$,

$$\beta_{m+2-s,w} = \beta_{m+2,w}(t_w^s + O(m^{-1})), \qquad t_w = (m-w)(n-m-w)/n^2.$$

Theorem 5.1. *For a divisible self-dual code, let $g(t)$ be defined as in Proposition 4.3 and let $\beta_{m,w}$ and t_w be defines as above. The coefficients $A_1, A_2, \ldots, A_{m+2}$ in the weight enumerator of the code satisfy*

$$\sum_{w=1}^{m+2} A_w \beta_{m+2,w}(g(t_w) - t_w g'(t_w))(g(t_w) - \frac{g(t_0)}{t_0} t_w) + O(m^{-1})) = 0. \tag{18}$$

Proof. We use Equation (17),

$$[t^{m+2}]\,(g(t) - tg'(t))(g(t) - \alpha t) \sum_{i=m+2-2\ell}^{m+2} B_i t^i = 0.$$

With $B_i = \sum_{w=0}^{i} \beta_{i,w} A_w$, the coefficient at A_w is

$$\begin{aligned}
& [t^{m+2} A_w]\,(g(t) - tg'(t))(g(t) - \alpha t) \sum_{i=m+2-2\ell}^{m+2} B_i t^i \\
= \; & [t^0 A_w]\,(g(t) - tg'(t))(g(t) - \alpha t) \sum_{s=0}^{2\ell} B_{m+2-s} t^{-s} \\
= \; & [t^0]\,(g(t) - tg'(t))(g(t) - \alpha t) \sum_{s=0}^{2\ell} \beta_{m+2-s,w} t^{-s} \\
= \; & [t^0]\,(g(t) - tg'(t))(g(t) - \alpha t) \sum_{s=0}^{2\ell} \beta_{m+2,w} ((t_w)^s + O(m^{-1})) t^{-s} \\
= \; & \beta_{m+2,w}\,((g(t_w) - t_w g'(t_w))(g(t_w) - \alpha t_w) + O(m^{-1}))
\end{aligned}$$

For $\alpha = g(t_0)/t_0$, the contribution at $w = 0$ vanishes. □

Corollary 5.2. *For a divisible self-dual code of type* $(q, c) = (2, 2), (2, 4), (3, 3), (4, 2)$,

$$d/N \lesssim \frac{q-1}{q}(1 - \frac{1}{\sqrt[c]{c+1}}).$$

Proof. For all four types, and for $w/m \in (0, 1]$,

$$g(t_w) - t_w g'(t_w) = 0 \quad \Leftrightarrow \quad w/n = (1 - \frac{1}{\sqrt{q}})/2 =: \omega.$$

$$g(t_w) - \frac{g(t_0)}{t_0} t_w = 0 \quad \Leftrightarrow \quad w/n = \frac{q-1}{q}(1 - \frac{1}{\sqrt[c]{c+1}}) := \omega'.$$

Thus, as $m \longrightarrow \infty$, the contribution of A_w to the left side of Equation (18) is negative for w/n in the range $w/n \in (\omega, \omega')$ and positive for w/n outside that range. It follows that, as $n \longrightarrow \infty$, $A_w \neq 0$ for some $w/n \leq \omega'$, and therefore $d/N \lesssim \omega'$. □

References

[1] Alexei Ashikhmin and Alexander Barg. Binomial moments of the distance distribution: bounds and applications. *IEEE Trans. Inform. Theory*, 45(2):438–452, 1999.

[2] Iwan Duursma. Extremal weight enumerators and ultraspherical polynomials. *Discrete Math.*, 268(1-3):103–127, 2003.

[3] Ilia Krasikov and Simon Litsyn. An improved upper bound on the minimum distance of doubly-even self-dual codes. *IEEE Trans. Inform. Theory*, 46(1):274–278, 2000.

[4] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Information and Control*, 22:188–200, 1973.

[5] Eric M. Rains. New asymptotic bounds for self-dual codes and lattices. *IEEE Trans. Inform. Theory*, 49(5):1261–1274, 2003.

[6] N. J. A. Sloane. Self-dual codes and lattices. In *Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978)*, pages 273–308. Amer. Math. Soc., Providence, R.I., 1979.

[7] Harold N. Ward. Divisible codes. *Arch. Math. (Basel)*, 36(6):485–494, 1981.