Minimum distance bounds for divisible codes

Iwan Duursma*

AMS/SMM - HOUSTON, May 13-15, 2004

*This work supported by NSF DMS-0099761. Slides posted at http://www.math.uiuc.edu/~duursma/pub

A linear code is **divisible** if for some $c > 1$ the Hamming distance between any two codewords is divisible by c.

The **minimum distance** d of a code is the smallest Hamming distance between any two distinct codewords.

D'03 : The Singleton bound

$$d + d^{\perp} \leq n + 2$$

generalizes to

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

With an improvement

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

for even self-complimentary binary codes.

Define the **weight enumerator** of a q-ary linear code

$$A(x,y) := \sum_{w=0}^{N} A_w \, x^{N-w} y^w,$$

where A_w is the number of words of Hamming weight w and N is the codelength.

The dual code has weight enumerator

$$A^*(x,y) = q^{-k} \sum_{w=0}^{N} A_w (x + \gamma y)^{N-w} (x-y)^w.$$

where $k = \dim_{F_q} C$ and $\gamma = q - 1$.

A linear code is divisible by c if

$$A(x,y) \in C[x^c - y^c, y^c].$$

A linear code is divisible by c and symmetric if

$$A(x,y) \in C[(x^c - y^c)^2, x^c y^c].$$

A linear code is formally self-dual if

$$A(x,y) \in C[x(x+\gamma y), y(x-y)].$$

By Gleason's Theorem a nontrivial self-dual divisible code is of one of four types. For each type, the weight enumerator belongs to a ring of invariants of the form $C[F,G]$.

Gleason'71 :

(Type I)	$(q,c) = (2,2)$	$C[F_8, G_2]$
(Type II)	$(q,c) = (2,4)$	$C[F_{24}, G_8]$
(Type III)	$(q,c) = (3,3)$	$C[F_{12}, G_4]$
(Type IV)	$(q,c) = (4,2)$	$C[F_6, G_2]$

Mallows-Sloane'73 :

(Type I)	$d \leq 2\lfloor n/8 \rfloor + 2$
(Type II)	$d \leq 4\lfloor n/24 \rfloor + 4$
(Type III)	$d \leq 3\lfloor n/12 \rfloor + 3$
(Type IV)	$d \leq 2\lfloor n/6 \rfloor + 2$

The Mallows-Sloane upper bounds are attained only by a finite number of codes.

Zhang'99 :

$$
\begin{array}{lll}
\text{(Type I)} & n \leq 24, & \text{if } 8|n. \\
\text{(Type II)} & n \leq 3672, & \text{if } 24|n. \\
\text{(Type III)} & n \leq 828, & \text{if } 12|n. \\
\text{(Type IV)} & n \leq 96, & \text{if } 6|n.
\end{array}
$$

The Mallows-Sloane upper bounds allow an asymptotic improvement.

Krasikov-Litsyn'00 (Type II), Rains'03 :

$$
\limsup d/n \leq \begin{cases} .2113 < 1/4 & \text{(Type I).} \\ .1656 < 1/6 & \text{(Type II).} \\ .2467 < 1/4 & \text{(Type III).} \\ .3170 < 1/3 & \text{(Type IV).} \end{cases}
$$

Or

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

Theorem 1 (Type III/IV) :

For $N = cn$, let

$$A(x,y) = \sum_{i=0}^{n} a_i (x^c - y^c)^{n-i} (y^c)^i$$

Then, for $n = (c+1)m$,

(Type III) :
$a_{m+1} - 270a_{m-1} - 1944a_{m-2} - 2187a_{m-3} = 0.$

(Type IV) :
$a_{m+1} - 48a_{m-1} - 128a_{m-2} = 0.$

Theorem 2 (Type I/II) :

For $N = 2cn$, let

$$A(x, y) = \sum_{i=0}^{n} a_i (x^c - y^c)^{2n-2i} (x^c y^c)^i$$

Then, for $2n = (c + 2)m$,

(Type I) :
$a_{m+1} - 16 a_{m-1} = 0.$

(Type II) :
$a_{m+1} - 768 a_{m-1} - 8192 a_{m-2} = 0.$

Let $C((t))$ be the ring of formal series in t.

For $f = \sum_{i \gg \infty} a_i t^i$,

$$\mathrm{Res}_t(f dt) := a_{-1}$$

is called the residue of the differential $f dt$.

The residue of a differential does not depend on the choice of local parameter:

For a different local parameter u and for $g(u)du = f(t)dt$,

$$\mathrm{Res}_u(g(u)du) = \mathrm{Res}_t(f(t)dt).$$

Lemma: Let

$$\sum_{i\geq 0} a_i u^{i-m} = \sum_{j=0}^{m} c_j v^{j-m},$$

for local parameters u and v in $C((t))$, and let

$$v^{-2}dv = h(u)u^{-2}du,$$

for $h(u) = \sum h_i u^i$. Then

$$\sum_{i=0}^{m+1} h_i a_{m+1-i} = 0.$$

Proof:

$$\begin{aligned} 0 &= \mathrm{Res}_v(\sum_{j=0}^{m} c_j v^{j-m-2} dv) \\ &= \mathrm{Res}_u(\sum_{i\geq 0} a_i u^{i-m-2} h(u) du) \\ &= \sum_{i=0}^{m+1} h_i a_{m+1-i}. \end{aligned}$$

Proof Thm 1 (Type III, $N = 12m$) :

$$\begin{aligned} A(x,y) &= \sum_{i=0}^{4m} a_i (x^3 - y^3)^{4m-i} (y^3)^i \\ &= \sum_{j=0}^{m} c_j F^j G^{3m-3j} \end{aligned}$$

for $F = y^3(x^3 - y^3)^3, G = (x^4 + 8xy^3)$.

Let $t = y^3/x^3$,

$$u = \frac{t}{1-t}, \quad v = \frac{t(1-t)^3}{(1+8t)^3}.$$

Then

$$\sum_{i=0}^{4m} a_i u^{i-m} = \sum_{j=0}^{m} c_j v^{j-m}.$$

$$v^{-2} dv = \underline{(1+9u)^2(1-18u-27u^2)}\, u^{-2} du.$$

Proof Thm 1 (Type IV, $N = 6m$) :

$$\begin{aligned} A(x,y) &= \sum_{i=0}^{3m} a_i (x^2 - y^2)^{3m-i} (y^2)^i \\ &= \sum_{j=0}^{m} c_j F^j G^{3m-3j} \end{aligned}$$

for $F = y^2(x^2 - y^2)^2, G = (x^2 + 3y^2)$.

Let $t = y^2/x^2$,

$$u = \frac{t}{1-t}, \quad v = \frac{t(1-t)^2}{(1+3t)^3}.$$

Then

$$\sum_{i=0}^{3m} a_i u^{i-m} = \sum_{j=0}^{m} c_j v^{j-m}.$$

$$v^{-2} dv = \underline{(1+4u)^2(1-8u)}\, u^{-2} du.$$

Proof Thm 2 (Type I, $N = 8m$) :

$$
\begin{aligned}
A(x,y) &= \sum_{i=0}^{2m} a_i (x^2 - y^2)^{4m-2i} (xy)^{2i} \\
&= \sum_{j=0}^{m} c_j F^j G^{4m-4j}
\end{aligned}
$$

for $F = x^2 y^2 (x^2 - y^2)^2, G = (x^2 + y^2)$.

Let $t = y^2/x^2$,

$$
u = \frac{t}{(1-t)^2}, \quad v = \frac{t(1-t)^2}{(1+t)^4}.
$$

Then

$$
\sum_{i=0}^{4m} a_i u^{i-m} = \sum_{j=0}^{m} c_j v^{j-m}.
$$

$$
v^{-2} dv = \underline{(1+4u)(1-4u)}\, u^{-2} du.
$$

Proof Thm 2 (Type II, $N = 24m$) :

$$A(x,y) = \sum_{i=0}^{3m} a_i (x^4 - y^4)^{6m-2i}(xy)^{4i}$$
$$= \sum_{j=0}^{m} c_j F^j G^{3m-3j}$$

for $F = x^4y^4(x^4-y^4)^4, G = (x^8+14x^4y^4+y^8)$.

Let $t = y^4/x^4$,

$$u = \frac{t}{(1-t)^2}, \quad v = \frac{t(1-t)^4}{((1+14t+t^2)^3}.$$

Then

$$\sum_{i=0}^{3m} a_i u^{i-m} = \sum_{j=0}^{m} c_j v^{j-m}.$$

$$v^{-2} dv = \underline{(1+16u)^2(1-32u)}\, u^{-2} du.$$

Proof KLR (Type III, $N = 3n = 12m$) :

For $A(x,y)$ of Type III and for

$$\Delta = y(y^3 - x^3)\frac{\partial}{\partial y}(\frac{\partial^3}{\partial^3 y} - 8\frac{\partial^3}{\partial^3 x})$$

$\Delta A(x,y)$ is again of Type III.

We apply Theorem 1 to $\underline{\Delta A(x,y)}$.

The contribution of

$$\Delta A_{3w}(x^3)^{n-w}(y^3)^w$$

to a_i, for $i = m + o(1)$ as $n \to \infty$, is a positive multiple of

$$\begin{aligned} & 12(w^3 - 8(m-w)(n-w)^2) \\ = \; & \underline{(2n)^3 - 4(2n-3w)^3}. \end{aligned}$$

The RHS changes sign once for $w/n \in [0, 1/4]$.

Proof KLR (Type IV, $N = 2n = 6m$) :

For $A(x,y)$ of Type IV and for

$$\Delta = y(y^2 - x^2)\frac{\partial}{\partial y}(\frac{\partial^2}{\partial^2 y} - 9\frac{\partial^2}{\partial^2 x})$$

$\Delta A(x,y)$ is again of Type IV.

We apply Theorem 1 to $\underline{\Delta A(x,y)}$.

The contribution of

$$\Delta A_{2w}(x^2)^{n-w}(y^2)^w$$

to a_i, for $i = m + o(1)$ as $n \to \infty$, is a positive multiple of

$$\begin{aligned} & 6(w^2 - 9(m-w)(n-w)) \\ = \ & \underline{(3n)^2 - 3(3n-4w)^2}. \end{aligned}$$

The RHS changes sign once for $w/n \in [0, 1/3]$.

Proof KLR (Type I, $N = 4n = 8m$) :

For $A(x,y)$ of Type I and for

$$\Delta = xy(y^2 - x^2)\frac{\partial^2}{\partial x \partial y}(\frac{\partial^2}{\partial^2 y} - \frac{\partial^2}{\partial^2 x})$$

$\Delta A(x,y)$ is again of Type I.

We apply Theorem 2 to $\underline{\Delta A(x,y)}$.

The contribution of

$$\Delta A_{2w}((x^2)^{2n-w}(y^2)^w + (x^2)^w(y^2)^{2n-w})$$

to a_i, for $i = m + o(1)$ as $n \to \infty$, is a positive multiple of

$$\begin{aligned} & 8(w^2(2n-m-w) - (m-w)(2n-w)^2) \\ = \ & n(\underline{n^2 - 3(n-2w)^2}). \end{aligned}$$

The RHS changes sign once for $w/n \in [0, 1/4]$.

Proof KLR (Type II, $N = 8n = 24m$) :

For $A(x, y)$ of Type II and for

$$\Delta = xy(y^4 - x^4)\frac{\partial^4}{\partial x \partial y}(\frac{\partial^4}{\partial^4 y} - \frac{\partial^4}{\partial^4 x})$$

$\Delta A(x, y)$ is again of Type II.

We apply Theorem 2 to $\underline{\Delta A(x, y)}$.

The contribution of

$$\Delta A_{4w}((x^4)^{2n-w}(y^4)^w + (x^4)^w(y^4)^{2n-w})$$

to a_i, for $i = m + o(1)$ as $n \to \infty$, is a positive multiple of

$$\begin{aligned} & 24(w^4(2n - m - w) - (m - w)(2n - w)^4) \\ = \; & n\,(\underline{n^4 - 5(n - 2w)^4}). \end{aligned}$$

The RHS changes sign once for $w/n \in [0, 1/6]$.

Our proof of the KLR bound applies to divisible codes (not necessarily self-dual) with

$$d^{\perp} \geq N/(c+1)+c$$

and to even self-complimentary binary codes with

$$d^{\perp} \geq N/(c+2)+c$$

Namely, such codes have $a_{m+1}=0$ in $\Delta A(x,y)$.

Differential operators and bounds

For a divisible code :

$$y^{d-c}(x^c - y^c)^{d^\perp - c} \mid \Delta A(x,y)$$

For an even self-complimentary binary code :

$$(xy)^{d-c}(x^c - y^c)^{d^\perp - c} \mid \Delta A(x,y)$$

Differential operators and Gleason's Theorem

The subring of $C[\partial x, \partial y]$ of differential operators that preserve the invariant ring $C[F, G]$ is of the form $C[\mathcal{F}, \mathcal{G}]$ for each of the types I, II, III, IV.

Differential operators and zeta functions

For a given weight enumerator $A(x,y)$ there exists a unique MDS code, with weight enumerator $M(x,y)$, and a unique differential operator $\Delta \in C[\partial x, \partial y]$ such that

$$A(x,y) = \Delta M(x,y).$$

For $\mathcal{P} = \partial x + \partial y$ and $\mathcal{S} = \partial x$,

$$\frac{\partial}{\partial y}(\frac{\partial}{\partial y} - \gamma\frac{\partial}{\partial x}) = (\mathcal{P} - \mathcal{S})(\mathcal{P} - q\mathcal{S}).$$