

New Inequalities for q -ary Constant-Weight Codes

Hyun Kwang Kim*¹ Phan Thanh Toan¹

¹Department of Mathematics, POSTECH

International Workshop on Coding and Cryptography

April 15-19, 2013, Bergen (Norway)

Outline

1 Results on binary codes

- Binary codes
- A fundamental problem in coding theory
- Delsarte's linear programming bound for binary codes
- New upper bounds for binary constant-weight codes

2 Generalizations to q -ary codes

- q -ary codes
- Delsarte's linear programming bound for q -ary codes
- New inequalities for q -ary constant-weight codes
- New upper bounds for q -ary constant-weight codes

What is a code?

Binary code

- Let $\mathcal{F} = \{0, 1\}$.
- A subset \mathcal{C} of \mathcal{F}^n is called a *(binary) code* of length n .
- An element of a code \mathcal{C} is called a *codeword*.

Minimum distance of a code

- *Hamming distance* between two vectors $u, v \in \mathcal{F}^n$, denoted by $d(u, v)$, is the number of coordinates where they differ.
- *Minimum distance* of a code \mathcal{C} is defined by

$$\min\{d(u, v) \mid u, v \in \mathcal{C}, u \neq v\}.$$

Delsarte's linear programming bound

Distance distribution of a code

Let \mathcal{C} be a code of length n . The *distance distribution* $\{A_i\}_{i=0}^n$ of \mathcal{C} is defined by

$$A_i = \frac{1}{|\mathcal{C}|} |\{(u, v) \in \mathcal{C}^2 \mid d(u, v) = i\}|$$

for $i = 0, 1, \dots, n$.

Remark

- By definition, $A_0 = 1$ and $\sum_{i=0}^n A_i = |\mathcal{C}|$.

Delsarte's linear programming bound

- For upper bounds on $A(n, d)$, Delsarte's linear programming bound is a powerful bound.
- Delsarte's linear programming bound is based on the fact that the following linear combinations of the distance distribution $\{A_i\}_{i=0}^n$ are nonnegative (as follows).

Delsarte's linear programming bound for binary codes

Delsarte's linear programming bound

Theorem (Delsarte)

Let \mathcal{C} be a code with distance distribution $\{A_i\}_{i=0}^n$. For $k = 1, 2, \dots, n$,

$$\sum_{i=0}^n P_k(n; i) A_i \geq 0,$$

where $P_k(n; x)$ is the Krawtchouk polynomial given by

$$P_k(n; x) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j}.$$

Delsarte's linear programming bound

Theorem (Delsarte's linear programming bound)

$$A(n, d) \leq 1 + \lfloor \max(A_1 + A_2 + \cdots + A_n) \rfloor,$$

where the maximization is taken over all (A_1, A_2, \dots, A_n) satisfying $A_i \geq 0$ for $i = 1, 2, \dots, n$ and satisfying the above linear constraints.

Remark

- If d is even, then $A(n, d)$ is attained by a code with all vectors having even weights.
- Hence, if d is even, then we can put $A_i = 0$ if i is odd.
- Also, by definition, $A_i = 0$ if $0 < i < d$.

Delsarte's linear programming bound for binary codes

Delsarte's linear programming bound

Theorem (Delsarte's linear programming bound and its improvements)

Let \mathcal{C} be a code with distance distribution $\{A_i\}_{i=0}^n$. For $k = 1, 2, \dots, n$,

$$\sum_{i=0}^n P_k(n; i) A_i \geq 0.$$

If $M = |\mathcal{C}|$ is odd, then

$$\sum_{i=0}^n P_k(n; i) A_i \geq \frac{1}{M} \binom{n}{k}.$$

If $M = |\mathcal{C}| \equiv 2 \pmod{4}$, then there exists $t \in \{0, 1, \dots, n\}$ such that

$$\sum_{i=0}^n P_k(n; i) A_i \geq \frac{2}{M} \left[\binom{n}{k} + P_k(n; t) \right].$$

Delsarte's linear programming bound for binary codes

Counting the number of $2 \times k$ submatrices

Result 1

- We prove simultaneously Delsarte's linear programming bound and its well known improvements.
- The proof is based on counting the number of $2 \times k$ submatrices of \mathcal{C} , where \mathcal{C} is considered as a $|\mathcal{C}| \times n$ matrix (each codeword in \mathcal{C} is a row).

Definition

For each $k = 1, 2, \dots, n$, we introduce polynomials

$$P_k^-(n; x) = \sum_{\substack{j=0 \\ j \text{ odd}}}^k \binom{x}{j} \binom{n-x}{k-j} \quad \text{and} \quad P_k^+(n; x) = \sum_{\substack{j=0 \\ j \text{ even}}}^k \binom{x}{j} \binom{n-x}{k-j}.$$

Remark

It follows that $P_k^+(n; x) + P_k^-(n; x) = \binom{n}{k}$. The polynomial $P_k(n; x) := P_k^+(n; x) - P_k^-(n; x)$ is called the *Krawtchouk polynomial*.

Counting the number of $2 \times k$ submatrices

The proof immediately follows from the following lemma.

Lemma

Let \mathcal{C} be a code with size M and distance distribution $\{A_i\}_{i=0}^n$ and let t be the number of columns of \mathcal{C} containing an odd number of ones. For each $k = 1, 2, \dots, n$,

$$\sum_{i=1}^n P_k^-(n; i) A_i \leq \frac{2}{M} \left[N \binom{n}{k} - \delta P_k^+(n; t) \right] \quad (1)$$

and

$$-\sum_{i=1}^n P_k^+(n; i) A_i \leq -(M-1) \binom{n}{k} + \frac{2}{M} \left[N \binom{n}{k} - \delta P_k^+(n; t) \right], \quad (2)$$

where N and δ are given by

$$N = \begin{cases} \frac{M^2}{4} & \text{if } M \text{ is even} \\ \frac{M^2-1}{4} & \text{if } M \text{ is odd} \end{cases} \quad \text{and} \quad \delta = \begin{cases} 1 & \text{if } M \equiv 2 \pmod{4} \\ 0 & \text{otherwise} \end{cases} .$$

Counting the number of $2 \times k$ submatrices

Proof of Lemma

- Write $\mathcal{C} = (c_{mi})$, $1 \leq m \leq |\mathcal{C}|$, $1 \leq i \leq n$. Let $S_1(k)$ be the number of $2 \times k$ matrices

$$A = \begin{pmatrix} c_{mi_1} & c_{mi_2} & \cdots & c_{mi_k} \\ c_{li_1} & c_{li_2} & \cdots & c_{li_k} \end{pmatrix}$$

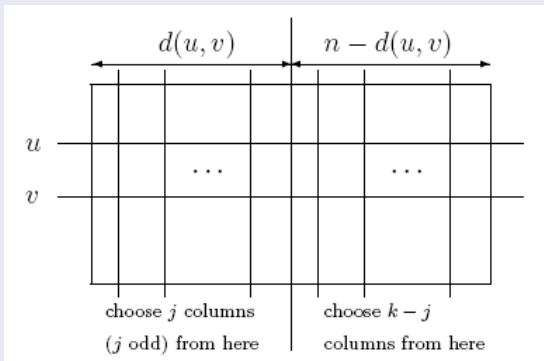
such that $m \neq l$, $i_1 < i_2 < \cdots < i_k$, and A contains an odd number of 1's.

- The entries of A are on the intersection of two rows and k columns of \mathcal{C} .

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- For an ordered pair (u, v) of different rows of \mathcal{C} , to get such a matrix A choose j coordinates (j odd) where u and v differ and choose $k - j$ coordinates where u and v are the same.



Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- Hence, an ordered pair (u, v) will contribute

$$\sum_{\substack{j=0 \\ j \text{ odd}}}^n \binom{d(u, v)}{j} \binom{n - d(u, v)}{k - j} = P_k^-(n; d(u, v))$$

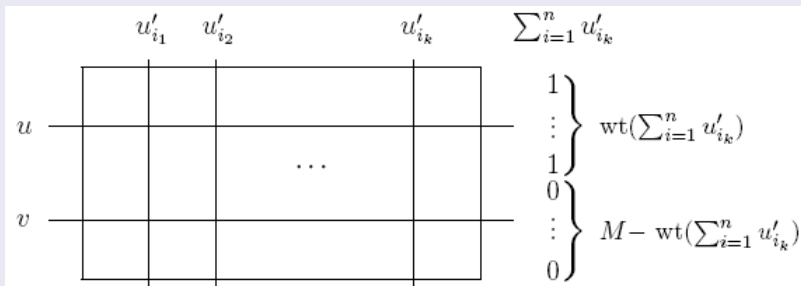
to $S_1(k)$. Therefore,

$$\begin{aligned} S_1(k) &= \sum_{\substack{u, v \in C \\ u \neq v}} P_k^-(n; d(u, v)) = \sum_{i=1}^n \sum_{\substack{u, v \in C \\ d(u, v)=i}} P_k^-(n; i) \\ &= \sum_{i=1}^n P_k^-(n; i) \sum_{\substack{u, v \in C \\ d(u, v)=i}} 1 \\ &= M \sum_{i=1}^n P_k^-(n; i) A_i. \end{aligned}$$

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- Let u'_1, u'_2, \dots, u'_n be the n columns of \mathcal{C} .



- For k columns $u'_{i_1}, u'_{i_2}, \dots, u'_{i_k}$, to get such a matrix A choose one row such that the intersection of this row with the k columns has an odd number of 1's and choose another row such that the intersection of that row with the k columns has an even number of 1's.

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- Hence,

$$S_1(k) = 2 \sum_{i_1 < i_2 < \dots < i_k} wt(u'_{i_1} + \dots + u'_{i_k}) [M - wt(u'_{i_1} + \dots + u'_{i_k})].$$

- If M is odd, then $\delta = 0$ by definition. For all $i_1 < i_2 < \dots < i_k$,

$$wt(u'_{i_1} + \dots + u'_{i_k}) [M - wt(u'_{i_1} + \dots + u'_{i_k})] \leq \frac{M-1}{2} \frac{M+1}{2} = \frac{M^2 - 1}{4} = N.$$

- So

$$S_1(k) \leq 2 \sum_{i_1 < i_2 < \dots < i_k} N = 2N \binom{n}{k} = 2 \left[N \binom{n}{k} - \delta P_k^+(n; t) \right].$$

- Therefore, (1) is proved if M is odd.

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- If $M \equiv 0 \pmod{4}$, then $\delta = 0$ by definition. For all $i_1 < i_2 < \dots < i_k$,

$$wt(u'_{i_1} + \dots + u'_{i_k})[M - wt(u'_{i_1} + \dots + u'_{i_k})] \leq \frac{M}{2} \frac{M}{2} = \frac{M^2}{4} = N.$$

- So

$$S_1(k) \leq 2N \binom{n}{k} = 2 \left[N \binom{n}{k} - \delta P_k^+(n; t) \right].$$

- Therefore, (1) is proved if $M \equiv 0 \pmod{4}$.

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- If $M \equiv 2 \pmod{4}$, then $\delta = 1$ by definition.
- Let I be the collection of coordinates i such that the column u'_i contains an odd number of 1's.
- If $|\{i_1, i_2, \dots, i_k\} \cap I|$ is odd, then

$$\text{wt}(u'_{i_1} + \dots + u'_{i_k})[M - \text{wt}(u'_{i_1} + \dots + u'_{i_k})] \leq \frac{M}{2} \frac{M}{2} = \frac{M^2}{4} = N.$$

- However, if $|\{i_1, i_2, \dots, i_k\} \cap I|$ is even, then

$$\text{wt}(u'_{i_1} + \dots + u'_{i_k})[M - \text{wt}(u'_{i_1} + \dots + u'_{i_k})] \leq \frac{M-2}{2} \frac{M+2}{2} = N-1.$$

$$\begin{aligned} S_1(k) &\leq 2 \left(\sum_{|\{i_1, i_2, \dots, i_k\} \cap I| \text{ odd}} N + \sum_{|\{i_1, i_2, \dots, i_k\} \cap I| \text{ even}} N-1 \right) \\ &= 2 \left[N \binom{n}{k} - \delta P_k^+(n; t) \right]. \end{aligned}$$

- Hence, (1) is proved if $M \equiv 2 \pmod{4}$.

Delsarte's linear programming bound for binary codes

Counting the number of $2 \times k$ submatrices

Proof of Lemma (continued)

- For (2), one can count (two times of) the number of $2 \times k$ submatrices A such that A contains an even number of 1's or just use the equality

$$\sum_{i=1}^n P^-(n; i)A_i + \sum_{i=1}^n P^+(n; i)A_i = (M - 1) \binom{n}{k}.$$

Counting the number of $2 \times k$ submatrices

Theorem (Delsarte's linear programming bound and its improvements)

Let \mathcal{C} be a code with distance distribution $\{A_i\}_{i=0}^n$. For $k = 1, 2, \dots, n$,

$$\sum_{i=1}^n P_k(n; i) A_i \geq -\binom{n}{k}.$$

If $M = |\mathcal{C}|$ is odd, then

$$\sum_{i=1}^n P_k(n; i) A_i \geq -\binom{n}{k} + \frac{1}{M} \binom{n}{k}.$$

If $M = |\mathcal{C}| \equiv 2 \pmod{4}$, then there exists $t \in \{0, 1, \dots, n\}$ such that

$$\sum_{i=1}^n P_k(n; i) A_i \geq -\binom{n}{k} + \frac{2}{M} \left[\binom{n}{k} + P_k(n; t) \right].$$

Proof of Theorem

Take sum of inequalities (1) and (2) in the above lemma.

New upper bounds for binary constant-weight codes

Upper bounds for $A(n, d, w)$

Definition

Given n , d , and w , define

$A(n, d, w)$ = maximum number of codewords
in any code of length n and
minimum distance $\geq d$ such that
each codeword has exactly w ones.

Counting the number of $1 \times k$ submatrices

Proposition (1-row k -column formula)

Let \mathcal{C} be a code of length n and constant-weight w . For each $k = 1, 2, \dots, n$,

$$\sum_{i_1 < \dots < i_k} wt(u'_{i_1} + \dots + u'_{i_k}) = MP_k^-(n; w),$$

where the sum is taken over all (i_1, i_2, \dots, i_k) such that $i_1 < i_2 < \dots < i_k$.

Sketch of proof

Count the number of $1 \times k$ submatrices of \mathcal{C} containing an odd number of 1's.

Counting the number of $2 \times k$ submatrices

Result 2 (2-row k -column formula)

Let \mathcal{C} be a code of length n and constant-weight w . For each $k = 1, 2, \dots, n$,

$$\sum_{i=d/2}^w P_k^-(n; 2i) A_{2i} \leq \frac{2}{M} \left[\left(\binom{n}{k} - r_k \right) q_k (M - q_k) \right. \\ \left. + r_k (q_k + 1) (M - q_k - 1) \right]$$

and

$$- \sum_{i=d/2}^w P_k^+(n; 2i) A_{2i} \leq \frac{2}{M} \left[\left(\binom{n}{k} - r_k \right) q_k (M - q_k) \right. \\ \left. + r_k (q_k + 1) (M - q_k - 1) \right] - (M - 1) \binom{n}{k},$$

where q_k and r_k are the quotient and the remainder, respectively, when dividing $MP_k^-(n; w)$ by $\binom{n}{k}$, i.e., $MP_k^-(n; w) = q_k \binom{n}{k} + r_k$, with $0 \leq r_k < \binom{n}{k}$.

New upper bounds on $A(n, d, w)$

Sketch of proof

Count (two times of) the number of $2 \times k$ submatrices of \mathcal{C} containing an odd (even) number of 1's.

Result 2 gives the following new upper bounds for $A(n, d, w)$, $n \leq 28$.

- $A(18, 6, 8) \leq 427 \quad (428)$
- $A(18, 6, 9) \leq 424 \quad (425)$
- $A(20, 6, 10) \leq 1420 \quad (1421)$
- $A(27, 6, 11) \leq 66078 \quad (66079)$
- $A(27, 6, 12) \leq 84573 \quad (84574)$
- $A(27, 6, 13) \leq 91079 \quad (91080)$
- $A(28, 6, 11) \leq 104230 \quad (104231)$
- $A(28, 6, 13) \leq 164219 \quad (164220)$
- $A(28, 6, 14) \leq 169739 \quad (169740)$

New upper bounds on $A(n, d, w)$

New upper bounds

•	$A(24, 10, 10)$	\leq	170	(171)
•	$A(24, 10, 11)$	\leq	222	(223)
•	$A(24, 10, 12)$	\leq	246	(247)
•	$A(26, 10, 9)$	\leq	213	(214)
•	$A(27, 10, 9)$	\leq	298	(299)
•	$A(28, 10, 14)$	\leq	2628	(2629)
<hr/>				
•	$A(26, 12, 10)$	\leq	47	(48)
•	$A(27, 12, 12)$	\leq	139	(140)
•	$A(27, 12, 13)$	\leq	155	(156)
•	$A(28, 12, 11)$	\leq	148	(149)
•	$A(28, 12, 12)$	\leq	198	(199)
•	$A(28, 12, 13)$	\leq	244	(245)
•	$A(28, 12, 14)$	\leq	264	(265)

q -ary codes

Generalizations to q -ary codes

- Results 1 and 2 appeared in [B. G. Kang, H. K. Kim, and P. T. Toan, "Delsarte's linear programming bound for constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5956–5962, Sep. 2012].
- In the remaining, we generalize Results 1 and 2 to q -ary codes.

Definition

Definition

Let \mathbb{F}_q be a finite field with q elements. A subset \mathcal{C} of \mathbb{F}_q^n is called a q -ary code of length n .

Definition

Given n and d , define

$$A_q(n, d) = \text{maximum number of codewords in any } q\text{-ary code of length } n \text{ and minimum distance } \geq d.$$

Definition

Given n , d , and w , define

$$A_q(n, d, w) = \text{maximum number of codewords in any } q\text{-ary code of length } n \text{ and minimum distance } \geq d \text{ such that each codeword has weight } w.$$

Delsarte's linear programming bound for q -ary codes

Result 3

We prove simultaneously Delsarte's linear programming bound and its well known improvements for q -ary codes.

Theorem (Delsarte's linear programming bound and its improvements)

Let \mathcal{C} be a q -ary code with distance distribution $\{A_i\}_{i=0}^n$. Let $M = |\mathcal{C}|$. For $k = 1, 2, \dots, n$,

$$\sum_{i=0}^n P_k(n; i) A_i \geq \frac{1}{M} r (q - r) (q - 1)^{k-1} \binom{n}{k},$$

where r is the remainder when dividing M by q and

$$P_k(n; x) = \sum_{j=0}^k (-1)^j (q - 1)^{k-j} \binom{i}{j} \binom{n-i}{k-j}$$

is the Krawtchouk polynomial.

Delsarte's linear programming bound for q -ary codes

Idea of proof

- Write $\mathcal{C} = (c_{mi})$, $1 \leq m \leq |\mathcal{C}|$, $1 \leq i \leq n$.
- Consider all $2 \times k$ matrices

$$A = \begin{pmatrix} c_{mi_1} & c_{mi_2} & \cdots & c_{mi_k} \\ c_{li_1} & c_{li_2} & \cdots & c_{li_k} \end{pmatrix}$$

such that $m \neq l$, $i_1 < i_2 < \cdots < i_k$ and all vectors

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k) \in (\mathbb{F}_q^*)^k,$$

where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

- Count the number of pairs (A, α) such that

$$\alpha_1 c_{mi_1} + \cdots + \alpha_k c_{mi_k} \neq \alpha_1 c_{li_1} + \cdots + \alpha_k c_{li_k}.$$

Inequalities for q -ary constant-weight codes

Result 4

Using the same idea in the proof, we get the following new inequalities for q -ary constant-weight codes.

Theorem

Suppose that $\{A_i\}_{i=0}^n$ is the distance distribution of a q -ary constant-weight code \mathcal{C} of length n and constant-weight w . Let $M = |\mathcal{C}|$. Then for each $k = 1, 2, \dots, n$,

$$\sum_{i=1}^n P_k(n; i) A_i \geq (M-1)(q-1)^k \binom{n}{k} - \frac{2q}{(q-1)M} T(k),$$

where $T(k) = T_1(k) + T_2(k) + T_3(k)$.

Inequalities for q -ary constant-weight codes

Notations

$$T_1(k) = \left[(q-1)^k \binom{n}{k} - r_k \right] (M - q_k)q_k + r_k(M - q_k - 1)(q_k + 1),$$

$$T_2(k) = \left[(q-1)^k \binom{n}{k} - r_k \right] \left[\binom{q-1-t_k}{2} s_k^2 + (q-1-t_k)t_k s_k(s_k+1) + \binom{t_k}{2} (s_k+1)^2 \right],$$

$$T_3(k) = r_k \left[\binom{q-1-t'_k}{2} s_k'^2 + (q-1-t'_k)t'_k s_k'(s_k'+1) + \binom{t'_k}{2} (s_k'+1)^2 \right],$$

where

- q_k and r_k are the quotient and the remainder, respectively, when dividing $\frac{2(q-1)M}{q} P_k^-(n; w)$ by $(q-1)^k \binom{n}{k}$,
- s_k and t_k are the quotient and the remainder, respectively, when dividing q_k by $(q-1)$,
- s'_k and t'_k are the quotient and the remainder, respectively, when dividing $q_k + 1$ by $(q-1)$.

Inequalities for q -ary constant-weight codes

Notations

For each $k = 1, 2, \dots, n$,

$$P_k^-(n; x) = \frac{1}{2} \sum_{j=0}^k [(q-1)^j - (-1)^j] (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j} \quad (3)$$

and

$$P_k^+(n; x) = (q-1)^k \binom{n}{k} - P_k^-(n; x). \quad (4)$$

Inequalities for q -ary constant-weight codes

For $k = 1$, the new inequalities give the following corollary, which was shown by P. R. J. Östergård and M. Svanström in [Ternary constant weight codes, *Electron. J. Combin.*, vol. 9, no. 1, 2002].

Corollary

If there exists a q -ary code of length n , constant-weight w , and minimum distance $\geq d$, then

$$M(M-1)d \leq 2t \sum_{i=0}^{q-2} \sum_{j=i+1}^{q-1} M_i M_j + 2(n-t) \sum_{i=0}^{q-2} \sum_{j=i+1}^{q-1} M'_i M'_j, \quad (5)$$

where

- k and t are the quotient and the remainder, respectively, when dividing Mw by n ,
- $M_0 = M - k - 1$, $M'_0 = M - k$, $M_i = \lfloor (k+i)/(q-1) \rfloor$, and $M'_i = \lfloor (k+i-1)/(q-1) \rfloor$.

New upper bounds for q -ary constant-weight codes

Example

- Suppose that $q = 3$ and $(n, d, w) = (9, 3, 7)$.
- The best known upper bound for $A_3(9, 3, 7)$ is $A_3(9, 3, 7) \leq 576$.
- Suppose that $A_3(9, 3, 7) = 576$. Let \mathcal{C} be a code whose size attains the upper bound and let $\{A_i\}_{i=0}^n$ be the distance distribution of \mathcal{C} .
- The above theorem gives the following inequalities.

$$9A_3 + 6A_4 + 3A_5 - 3A_7 - 6A_8 - 9A_9 \geq 270$$

$$27A_3 + 6A_4 - 6A_5 - 9A_6 - 3A_7 + 12A_8 + 36A_9 \geq -108$$

$$15A_3 - 24A_4 - 18A_5 + 6A_6 + 21A_7 - 84A_9 \geq -294$$

$$-72A_3 - 39A_4 + 21A_5 + 27A_6 - 21A_7 - 42A_8 + 126A_9 \geq -1890$$

$$-108A_3 + 42A_4 + 39A_5 - 36A_6 - 21A_7 + 84A_8 - 126A_9 \geq -3969$$

$$48A_3 + 72A_4 - 48A_5 - 15A_6 + 63A_7 - 84A_8 + 84A_9 \geq -4942$$

$$144A_3 - 48A_4 - 24A_5 + 54A_6 - 57A_7 + 48A_8 - 36A_9 \geq -4194$$

$$-48A_4 + 48A_5 - 36A_6 + 24A_7 - 15A_8 + 9A_9 \geq -2160$$

$$-64A_3 + 32A_4 - 16A_5 + 8A_6 - 4A_7 + 2A_8 - A_9 \geq -1480/3$$

New upper bounds for q -ary constant-weight codes

Example (continued)

- Since $A_0 = 1$ and $A_1 = A_2 = 0$,

$$1 + \sum_{i=3}^9 A_i = \sum_{i=0}^9 A_i = |\mathcal{C}| = 576.$$

- Consider the following linear programming (where the A_i are considered as variables)

$$\max \left(1 + \sum_{i=3}^9 A_i \right)$$

subject to $A_i \geq 0$, $i = 3, 4, \dots, 9$ and subject to the above inequalities.

- Solving this linear programming, we get the maximum value of $1 + \sum_{i=3}^9 A_i$ is $12094/21$, which is less than 576.
- This contradiction shows that such a code \mathcal{C} does not exist. Therefore,

$$A_3(9, 3, 7) \leq 575.$$

Thank you!