On the Linear Programming Bounds for Constant Dimension Codes

Zong-Ying Zhang Yong Jiang Shu-Tao Xia

Graduate School at Shenzhen, Tsinghua University

July 26, 2011

Introduction

Constant Dimension Code (CDC) is employed to correct errors and/or erasures over the operator channel.

- $\mathbb{F}_q$: finite field with q elements (q is a prime power).
- W: n-dimensional vector space over $\mathbb{F}_q$.
- $\mathcal{P}(W)$: the set of all subspaces of W.
- For any $A, B \in \mathcal{P}(W)$, the dimension distance [3] between A and B:

$$d(A,B) == \dim(A) + \dim(B) - 2\dim(A \cap B). \qquad (1)$$

- q-ary (n, M, D) or $(n, M, D)_q$ code $\mathcal{C}$: subset of P(W) with size M and minimum dimension distance D which is defined by

$$D = D(\mathcal{C}) = \min_{X \neq Y \in \mathcal{C}} d(X,Y) \qquad (2)$$

Constraint Dimension Code

- $\mathcal{P}(W,l)$: the set of all l dimensional of W.
- *Gaussian binomial coefficient*:

$$\begin{bmatrix} n \\ m \end{bmatrix} \triangleq \begin{bmatrix} n \\ m \end{bmatrix}_q = \prod_{i=0}^{m-1} \frac{q^{n-i}-1}{q^{m-i}-1}. \tag{3}$$

- $$|\mathcal{P}(W,l)| = \begin{bmatrix} n \\ m \end{bmatrix}; \tag{4}$$
- A q-ary $(n, M, 2\delta, l)$ or $(n, M, 2\delta, l)_q$ constant dimension code is simply a subset of $\mathcal{P}(W,l)$ with size M and minimum dimension distance 2δ.

Maximum Number of Codewords

Proposition

Compact Johnson Bound

$$A_q[n, 2\delta, l] \leq \frac{\begin{bmatrix} n \\ l-\delta+1 \end{bmatrix}}{\begin{bmatrix} l \\ l-\delta+1 \end{bmatrix}}. \quad (5)$$

Proposition

Johnson Bound

$$A[n, 2\delta, l] \leq \left\lfloor \frac{q^n - 1}{q^l - 1} \left\lfloor \frac{q^{n-1} - 1}{q^{l-1} - 1} \left\lfloor \cdots \left\lfloor \frac{q^{n-l+\delta} - 1}{q^\delta - 1} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor.$$

Our work

Linear programming (LP) bounds of $A[n, 2\delta, l]$ are given and then it is shown that the *Compact Johnson Bound* is a special case of the proposed LP bounds.

Gaussian binomial coefficients

$$\begin{bmatrix} x \\ l \end{bmatrix}_b = \begin{cases} 1 & l = 0 \\ \prod_{i=0}^{l-1} \frac{b^{x-i}-1}{b^{l-i}-1}, & l = 1, 2, \ldots \end{cases} \tag{6}$$

- Properties

$$\lim_{b \to 1} \begin{bmatrix} x \\ l \end{bmatrix}_b = \binom{x}{l}, \tag{7}$$

$$\begin{bmatrix} n \\ l \end{bmatrix}_b = \begin{bmatrix} n \\ n-l \end{bmatrix}_b, \tag{8}$$

$$\begin{bmatrix} n \\ l \end{bmatrix}_b \begin{bmatrix} l \\ r \end{bmatrix}_b = \begin{bmatrix} n \\ r \end{bmatrix}_b \begin{bmatrix} n-r \\ l-r \end{bmatrix}_b. \tag{9}$$

Gaussian binomial coefficients

Cauchy Binomial Theorem

$$\prod_{i=1}^{m}(1+q^i x) = \sum_{i=0}^{m} \begin{bmatrix} m \\ i \end{bmatrix} q^{i(i+1)/2} x^i.$$

Let $x = -1/q$, we have that

$$\sum_{i=0}^{m} \begin{bmatrix} m \\ i \end{bmatrix} q^{i(i-1)/2} (-1)^i = \delta_{m,0}, \quad (10)$$

where

$$\delta_{m,n} = \begin{cases} 1 & \text{if } m = n, \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

Grassmannian/q-Johnson scheme

The Grassmannian or q-Johnson scheme is an association scheme where $\mathcal{P}(W, l)$ is the set of points.

- valency:

$$v_i = q^{i^2} \begin{bmatrix} l \\ i \end{bmatrix} \begin{bmatrix} n-l \\ i \end{bmatrix} \tag{12}$$

- multiplicity:

$$\tilde{\mu}_j = \binom{n}{j} - \binom{n}{j-1}, \tag{13}$$

Grassmannian/q-Johnson scheme

- the first eigenvalue:

$$E_i(j) = \sum_{m=0}^{i} (-1)^{i-m} q^{\binom{i-m}{2}+jm} \begin{bmatrix} l-m \\ l-i \end{bmatrix} \begin{bmatrix} l-j \\ m \end{bmatrix} \begin{bmatrix} n-l-j+m \\ m \end{bmatrix}. \quad (14)$$

- the second eigenvalue:

$$Q_j(i) = \frac{\mu_j}{v_i} E_i(j). \quad (15)$$

- Orthogonality:

$$\sum_{k=0}^{l} Q_k(i) E_j(k) = \begin{bmatrix} n \\ l \end{bmatrix} \delta_{i,j}, \quad (16)$$

$$\sum_{k=0}^{l} E_k(i) Q_j(k) = \begin{bmatrix} n \\ l \end{bmatrix} \delta_{i,j}. \quad (17)$$

Distance Distribution of CDC

Let $\mathcal{C} \subset \mathcal{P}(W,l)$ be an $(n,M,2\delta,l)_q$ constant dimension code.

- The *distance distribution* of $\mathcal{C}$ is defined by

$$A_i = \frac{1}{M}|\{(X,Y) : X,Y \in C, d(X,Y) = 2i\}|, i = 0,1,\ldots,l. \quad (18)$$

Clearly,

$$A_0 = 1, \quad A_i \geq 0, \quad 1 + \sum_{i=\delta}^{l} A_i = M. \quad (19)$$

- Since $\mathcal{P}(W,l)$ forms an association scheme, it is from Delsarte's theory that

$$\sum_{i=0}^{l} Q_j(i)A_i \geq 0, j = 1,2,\ldots,l, \quad (20)$$

or

$$\sum_{i=\delta} lQ_j(i)A_i \geq -\mu_j, j = 1,2,\ldots,l, \quad (21)$$

LP Bounds of CDC

Similar to LP Bounds in binary constant weight codes, we have the following LP problem:

LP-I

Choose the real variables $x_\delta, x_\delta + 1, \ldots, x_l$ so as to

$$maximize\ 1 + \sum_{i=\delta}^{l} x_i \tag{22}$$

subject to the inequalities

$$\begin{aligned} & x_i \geq 0,\ i = \delta, \delta+1, \ldots, l, \\ & \sum_{i=\delta}^{l} Q_j(i) x_i \geq -\mu_j,\ j = 1, 2, \ldots, l. \end{aligned} \tag{23}$$

the optional solution of (LP-I) has to be an upper bound of M.

LP Bounds of CDC

The dual problem of (LP-I) is given as follows:

LP-II

Choose the real variables $y_1, y_2, \ldots, y_l$ so as to

$$minimize\ 1 + \sum_{j=1}^{l} y_j \mu_j \tag{24}$$

subject to the inequalities

$$\begin{aligned} & y_j \geq 0,\ \ j = 1, 2, \ldots, l, \\ & \sum_{j=1}^{l} y_j Q_j(i) \leq -1,\ \ i = \delta, \delta+1, \ldots, l. \end{aligned} \tag{25}$$

LP Bounds of CDC

The duality theory

Proposition

Let

$$Y(x) = \sum_{k=0}^{l} y_k Q_k(x) \tag{26}$$

such that

$$y_0 = 1, y_k \geq 0, k = 1, 2, \ldots, l, \quad Y(i) \leq 0, i = \delta, \delta + 1, \ldots, l. \tag{27}$$

then

$$A_q[n, 2\delta, l] \leq Y(0). \tag{28}$$

Polynomial $Y(x)$ is said to be *feasible* if conditions above are satisfied, any feasible polynomial $Y(x)$ leads to an upper bound of $A_q[n, 2\delta, l]$.

Compact Johnson Bounds and LP Bounds

Remark

By (16) and (17), it's easy to see from (26) that

$$y_k = \frac{1}{\begin{bmatrix} n \\ l \end{bmatrix}} \sum_{i=0}^{l} Y(i) E_i(k), \ \ k = 0, 1, \ldots, l, \tag{29}$$

Lemma

Suppose $0 \le k, v \le l$. *Then*

$$\sum_{i=0}^{v} \begin{bmatrix} l-i \\ l-v \end{bmatrix} E_i(k) = q^{kv} \begin{bmatrix} l-k \\ v \end{bmatrix} \begin{bmatrix} n-l-k+v \\ v \end{bmatrix}. \tag{30}$$

Compact Johnson Bounds and LP Bounds

Set

$$Y^*(x) = \frac{\begin{bmatrix} n \\ l \end{bmatrix} \begin{bmatrix} l-x \\ l-\delta+1 \end{bmatrix}}{\begin{bmatrix} n-l+\delta-1 \\ \delta-1 \end{bmatrix}} \frac{}{\begin{bmatrix} l \\ l-\delta+1 \end{bmatrix}}, \qquad (31)$$

with Remark and Lemma above, it's easy to check

$$\begin{aligned} y_k^* &= \frac{1}{\begin{bmatrix} n \\ l \end{bmatrix}} \sum_{i=0}^{l} Y^*(i) E_i(k) \\ &= \frac{1}{\begin{bmatrix} n-l+\delta-1 \\ \delta-1 \end{bmatrix} \begin{bmatrix} l \\ l-\delta+1 \end{bmatrix}} \sum_{i=0}^{n} \begin{bmatrix} l-i \\ l-\delta+1 \end{bmatrix} E_i(k) \\ &= \frac{q^{k(\delta-1)} \begin{bmatrix} l-k \\ \delta-1 \end{bmatrix} \begin{bmatrix} n-l-k+\delta-1 \\ \delta-1 \end{bmatrix}}{\begin{bmatrix} n-l+\delta-1 \\ \delta-1 \end{bmatrix} \begin{bmatrix} l \\ \delta-1 \end{bmatrix}}, \end{aligned}$$

Compact Johnson Bounds and LP Bounds

so, $y_0^* = 1$ and $y_k^* \geq 0$, and also

$$Y^*(i) = 0, i = \delta, \delta+1, \ldots, l, \tag{32}$$

which means $Y^*(x)$ is *feasible*, then we have

$$A(n, 2\delta+1, l) \leq Y(0) = \frac{\begin{bmatrix} n \\ l \end{bmatrix}}{\begin{bmatrix} n-l+\delta-1 \\ \delta-1 \end{bmatrix}} = \frac{\begin{bmatrix} n \\ l-\delta+1 \end{bmatrix}}{\begin{bmatrix} l \\ l-\delta+1 \end{bmatrix}}. \tag{33}$$

which coincides with the result of compact Johnson bounds.

Concluding remarks

- LP bounds and Proposition 3 of $A_q[n, 2\delta, l]$ for constant dimension codes
- The compact Johnson bound in Proposition 1 corresponds a feasible polynomial in Proposition 3. Hence, the LP bound is at least as strong as the bound in Proposition 1.
- Future works may focus on finding more feasible polynomials, obtaining asymptotic LP bounds, or adding more restrictive inequalities to the LP problem (LP-I) for improving the LP bound.

Biblliography

- R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, No. 8, pp. 3579–3591, Aug. 2008.
- S. T. Xia and F. W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes, Cryptography*, vol. 50, pp. 163-172, Feb, 2009.
- P. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Res. Reports*, vol. 27, pp. 272-289, 1972.
- P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Reports*, Suppl. 10, 1973.

P. Delsarte, "Properties and applications of the recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) - q^kF(i,k,n)$," *SIAM Journal of Applied Mathematics*, vol. 31, no. 2, pp. 262-270, Sep. 1976.

R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory,* vol. 23, no. 2, pp. 157-166, Mar. 1977.

F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes," North-Holland, Amsterdam, 1981.

A. Schrijver, "Theory of Linear and Integer Programming," New York: Wiley, 1986.

The End!

Thanks.