26 Feb LP Bound for Codes

Code:

$$C \subseteq \{0,1\}^n \quad (\subseteq [q]^n)$$

$$d(C) = \min_{c \neq c' \in C} d(c,c') \qquad d(x,y) = \#\{i \mid x_i \neq y_i\}$$

Qn: Given n & d, what is the size of the largest set $C \subseteq \{0,1\}^n$ s.t. $d(C) \geq d$?

$A_2(n,d) := \max\{|C| \mid C \subseteq \{0,1\}^n$ w/ distance $d\}$

GV Bound: $A_q(n,d) \geq \dfrac{2^n}{\mathrm{Vol}_2(n,d-1)} = \dfrac{2^n}{\sum_{j=0}^{d-1}\binom{n}{j}}$

Asymptotic form: $R \geq 1 - h_2(\delta) - o(1)$

$R = k/n$. $\delta = d/n$.

Other directions:

Singleton Bd: $A_2(n,d) \leq 2^{n-d+1}$ $(R \leq 1 - \delta + o(1))$

Plotkin Bd: (binary code) $R \leq 1 - 2\delta + o(1)$

Johnson & Elias-Bassalygo Bound:

$$R \leq 1 - h\left(\frac{1-\sqrt{1-2\delta}}{2}\right) + o(1)$$

Delsarte · LP Bound.

MRRW. $R \leq h\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) + o(1)$ (best for $\delta > 0.273$)

MRRW second bound.

Delsarte LP Bound

Key Observation: Independent Set Problem

$G_d^{(n)} \left(V = \{0,1\}^n, E_{\le d}\right)$

$E(G) = \{(x,y) \mid \Delta(x,y) \le d\}$.

$A(n,d) = \alpha\left(G_d^{(n)}\right)$.

Hoffman Bound

$\alpha(G) \le \Theta_H(G) = \dfrac{-\lambda_{min}}{1-\lambda_{min}} |V|$

① $M(x,y) = 0$ if $(x,y) \notin E$

② $M\mathbb{1} = \mathbb{1}$

(G - regular)

Lovász Bound

$\alpha(G) \le \Theta(G) = \min \lambda$

$\begin{cases} M(x,y) = 1 & (x,y) \notin E \\ M \le \lambda I \end{cases}$

Schrijver Bound:

$M(x,y) \ge 1$. in above

History: Delsarte (LP formulation for Codes) '73

Hoffman '76

Lovász '79

Schrijver (Hamming Schemes $\Theta_G = \Theta_{LP}$) '79

Delsarte: Hamming Association Scheme

SDP $\longrightarrow$ LP bound.

MRRW '77
(McEliece, Rodemich, Rumsey, Welch
(dual witness for LP)

Today: Alternate proof of Delsarte's LP via MacWilliam Identities

Next lecture: Navon + Samorodnitsky's proof of MRRW first bound. (Friedman + Tillich)

$\mathcal{F} = \{f : \{0,1\}^n \to \mathbb{R}\}$.

2^n-dim vector space

Inner product $\langle f, g \rangle = \mathbb{E}[fg]$

$\chi_\alpha(x) := (-1)^{\sum x_i \alpha_i} = (-1)^{\langle x, \alpha \rangle}$

C - linear code. $C^\perp$ - dual

$C^\perp = \{y \in \{0,1\}^n \mid \sum x_i y_i = 0, \ \forall x \in C\}$

$\dim(C) + \dim(C^\perp) = n$

Prop: For any binary linear code C

$$\sum_{c \in C} \chi_\alpha(c) = \begin{cases} |C| & \text{if } \alpha \in C^\perp \\ 0 & \text{o.w.} \end{cases}$$

χ_α - orthonormal basis under above inner product

$\langle \chi_\alpha, \chi_\beta \rangle = \delta_{\alpha=\beta}$

$f = \sum \hat{f}(\alpha) \chi_\alpha$

$\hat{f}(\alpha) = \langle f, \chi_\alpha \rangle$

$\langle f, g \rangle = \sum \hat{f}(\alpha) \hat{g}(\alpha)$

$\hat{f}(0) = \mathbb{E}[f(x)]$

S. $\mathbb{1}_S(x)$ - characteristic fn.

Claim: For any linear $C \subseteq \{0,1\}^n$

$$\hat{\mathbb{1}}_C = \frac{|C|}{2^n} \mathbb{1}_{C^\perp}$$

Pf: $\hat{\mathbb{1}}_C(\alpha) = \mathop{\mathbb{E}}_x[\mathbb{1}_C(x)\chi_\alpha(x)] = \mathop{\mathbb{E}}_x[\mathbb{1}_C(x)\chi_\alpha(x)]$

$$= \frac{1}{2^n}\sum_{c\in C}\chi_\alpha(c) = \begin{cases} |C|/2^n & \text{if } \alpha \in C^\perp \\ 0 & \text{otherwise} \end{cases}$$

$$= \frac{|C|}{2^n}\mathbb{1}_{C^\perp}$$

$S \subseteq \{0,1\}^n$

$(W_0^S, W_1^S, \ldots W_n^S) \in \mathbb{R}^{n+1}$ wt. dist

$$W_i^S = \{x \in S / \text{wt}(x) = i\}$$

$$\sum_{i=0}^n W_i^S = |S|$$

$$W_\ell^{C^\perp} = \sum_{\alpha:\text{wt}(\alpha)=\ell} \mathbb{1}_{C^\perp}(\alpha) = \frac{2^n}{|C|}\sum_{\alpha:\text{wt}(\alpha)=\ell}\hat{\mathbb{1}}_C(\alpha)$$

$$= \frac{2^n}{|C|}\sum_{\alpha:\text{wt}(\alpha)=\ell}\mathop{\mathbb{E}}_x\left[\mathbb{1}_C(x)(-1)^{\langle\alpha,x\rangle}\right]$$

$$= \frac{2^n}{|C|}\mathop{\mathbb{E}}_x\left[\mathbb{1}_C(x)\cdot\underbrace{\left(\sum_{\alpha:\text{wt}(\alpha)=\ell}(-1)^{\langle\alpha,x\rangle}\right)}_{(A_x)}\right]$$

$$(*_x) = \sum_{\alpha : wt(\alpha)=\ell} (-1)^{\langle \alpha, x\rangle} \qquad \text{(depends only on } wt(x)\text{)}$$

Say $wt(x) = i$

$$= \underbrace{\sum_{j=0}^{\ell} (-1)^j \binom{i}{j}\binom{n-i}{\ell-j}}$$

$K_\ell^{(n)}(i)$ — Krawtchouk polynomial

$$K_\ell^{(n)}(x) = \sum_{j=0}^{\ell} (-1)^j \binom{x}{j}\binom{n-x}{\ell-j} \quad \therefore \deg = \ell.$$

$K_0^{(n)}(x) = 1$; $K_1^{(n)}(x) = n - 2x \ldots$,

$$W_\ell^{C^\perp} = \frac{1}{|C|} \sum_x \mathbb{1}_C(x)\, K_\ell(wt(x))$$

$$= \frac{1}{|C|} \sum_{c \in C} K_\ell(wt(c)) = \frac{1}{|C|} \sum_{i=0}^{n} K_\ell(i) \cdot W_i^C$$

$$\boxed{W_\ell^{C^\perp} = \frac{1}{|C|} \sum_{i=0}^{n} K_\ell^{(n)}(i) \cdot W_i^C}$$

MacWilliam's Identities:

$$W_\ell^{C^\perp} = \mathop{\mathbb{E}}_{c \in C} [K_\ell(wt(c))]$$

or in functional form

$$\sum_{\ell=0}^{n} W_\ell^{C^\perp} z^\ell = \frac{1}{|C|} \sum_{i=0}^{n} W_i^C (1-z)^i (1+z)^{n-i}$$

LP Bounding $A(n,d)$:

$$\theta_{Del} = \text{Max} \sum A_i \quad \text{subject} \begin{cases} A_0 = 1 \\ A_\ell \geq 0 \;;\; \ell = 1, \ldots n \\ A_i = 0 \;\cdot\; i = 1, \ldots d-1 \\ \sum_{i=0}^{n} K_\ell(i)\, A_i \geq 0 \quad \ell = 1, \ldots n \end{cases}$$

$i=0$

Clearly $Q_{DeL} \geq |C|$ for any linear code $C \subseteq \{0,1\}^n$ w/ distance $\geq d$

(since $(W_0^e\ W_1^e \ldots W_n^e)$ is a a primal feasible.

Non-linear codes:

$$A_i^C = \frac{\#\{(x,y) \in C^2 / \Delta(x,y) = i\}}{|C|}$$

Clearly $A_0^C = 1$

$A_i^C \geq 0; \quad i = 1, \ldots n$

$A_i^C = 0; \quad i = 1, \ldots d-1$

What about $\sum_{i=0}^{n} K_e(i) A_i^C \geq 0$

$$\sum_{i=0}^{n} A_i^C \cdot K_e(i) = \frac{1}{|C|} \sum_{i=0}^{n} \sum_{(x,y)\in C^2} \sum_{\Delta(x,y)=i} K_e(i)$$

$$= \frac{1}{|C|} \sum_{i=0}^{n} \left(\sum_{(x,y)\in C^2 : \Delta(x,y)=i} \left(\sum_{z : wt(z)=e} (-1)^{(x-y)\cdot z} \right) \right)$$

$$= \frac{1}{|C|} \sum_{(x,y)\in C^2} \sum_{z : wt(z)=e} (-1)^{(x-y)\cdot z}$$

$$= \frac{1}{|C|} \sum_{z : wt(z)=e} \left(\sum_{(x,y)\in C^2} (-1)^{\langle x,z\rangle} (-1)^{\langle y,z\rangle} \right)$$

$$= \frac{1}{|C|} \sum_{z : wt(z)=e} \left(\sum_{x} (-1)^{\langle x,z\rangle} \right)^2 \geq 0.$$

Thus, $A(n,d) \leq Q_{DEL}$

To bound θ_{DEL} - look at dual formulation

$$\beta(x) = 1 + \sum_{i=0}^{n} \beta_i K_i^{(n)}(x)$$

$$\theta_{DEL} = \min \beta(0)$$

$$\begin{cases} \beta_i \geq 0 & i = 1 \ldots n \\ \beta(j) \leq 0 & j = 1 \ldots n \end{cases}$$