# Delsarte's bounds for codes

def: $C \subseteq \{0,1\}^n$ is a code of min. dist. $\geq d$ if $\text{dist}(x,y) \geq d$ $\forall$ $x \neq y \in C$

[error correcting codes, tol. $\frac{d}{2}$ errors]

[major open] Q: What is Opt := max poss. $|C|$? [want "rate" as high as poss.]

"Gilbert-Varshamov bound": Opt $\geq$ naive (vol.-based) analysis of greedy. $\frac{2^n}{\sum_{j<d} \binom{n}{j}}$

Opt $\leq$ ? Q. is an instance of Max-Indep-Set!

$V = \{0,1\}^n$, $(x,y) \in E$ iff $0 < \text{dist}(x,y) < d$.

[LP blows for Indep-Set, but SDP good]

$\to$ SDPOpt [for what SDP?]

ex: Lovasz $\theta$ SDP $\equiv$ Canonical CSP SDP relax

$\equiv$ SDP: (idea: $J_x \equiv \begin{cases} \frac{1}{\sqrt{\alpha}} & \text{if } x \in \text{I.S.} \\ 0 & \text{if } x \notin \text{I.S.,} \end{cases}$ ($\alpha$ = max I.S.))

$$\max \ \mathbb{E}\left[\left(\sum_{x \in \{0,1\}^n} J_x\right)^2\right] = \sum_{x,y} \mathbb{E}[J_x J_y]$$

$\left(\alpha \cdot \frac{1}{\sqrt{\alpha}}\right)^2 = \alpha$ ✓

s.t. • $(J_x)_{x \in \{0,1\}^n}$ joint r.v.'s

$\alpha \left(\frac{1}{\sqrt{\alpha}}\right)^2 = 1$ ✓

• $\sum_x \mathbb{E}[J_x^2] = 1$

• $\mathbb{E}[J_x J_y] = 0$ if $0 < \text{dist}(x,y) < d$

$\boxed{\text{[Schrijver 79]}}$: Throw in $\mathbb{E}[J_x J_y] \geq 0$ $\forall x,y$.

[Why not?]

ex: $\equiv$ matching 2nd moment condits $\forall x,y$. [in constr. or not]

[← the strengthened SDP]

$\text{Opt} \le \text{SDP}'\text{Opt}$ [Seems a tad crazy to analyze: "size" $2^n$, and an SDP! But it simplifies....]

"symmetrization": Define joint r.v.s $(J'_x)_{x \in \{0,1\}^n}$:

- Draw $z \sim \{0,1\}^n$ rand.
- Draw $(J_x)_x$ [once]
- Output $J'_x = J_{x+z \pmod 2}$

Claim 1: ~~[illegible]~~ $(J'_x)_x$ valid SDP sol$^n$ w/ same obj.

pf: $\cdot \sum_x E[J'^2_x] = \sum_x \underset{z}{E}\, E[J^2_{x+z}] = \underset{z}{E}\left[\sum_x E[J^2_{x+z}]\right] = \underset{z}{E}\left[\sum_y E[J_y^2]\right]$ $=1$ $=1$ ✓

$\cdot\ E[J'_x J'_y] = \underset{z}{E}\left[\underbrace{E[J_{x+z} J_{y+z}]}\right]$

$\ge 0$ always, $= 0$ if $0 < \text{dist}(x+z, y+z) < d$

$\iff 0 < \text{dist}(x,y) < d$. ✓

$\cdot\ \sum_{x,y} E[J'_x J'_y] = \sum_{x,y} \underset{z}{E}\, E[J_{x+z} J_{y+z}] = \underset{z}{E}\left[\sum_{x,y} E[J_{x+z} J_{y+z}]\right] = \underset{z}{E}\left[\sum_{x,y} E[J_x J_y]\right]$
$= \underset{z}{E}[\text{SDP}'\text{Opt}]$ ✓

□

Claim 2: $\forall z \in \{0,1\}^n$, $(J'_x)_x$ has same joint distrib. as $(J'_{x+z})_x$. ✓ [Pf obvious]

$\Rightarrow E[J'_{x+z} J'_{y+z}] = E[J'_x J'_y]\ \forall z$; i.e., $E[J'_x J'_y]$ only deps. on $x - y = x+y$.

[So we can WOLOG insist on this symmetry.]

[well-def'd]
def: $\sigma(z) = E[J'_x J'_y]$ for any/all $x, y$ with $x - y = z$.

i.e., $SDP'Opt$ = $LPOpt$ of $\left(\tilde\sigma(z) = 2^n\sigma(z)\right)$

$$\max \sum_z \tilde\sigma(z)$$

$$\text{s.t.}\quad \tilde\sigma(0,\dots,0) = 1$$

$$\tilde\sigma(z) = 0, \qquad 0 < |z| < d$$

$$\tilde\sigma(z) \geq 0.$$

$$\left[\hat{\sigma}(\gamma) = \tfrac{1}{2^n}\right] \sum_z (-1)^{\gamma\cdot z}\tilde\sigma(z) \geq 0 \qquad \forall \gamma \in \{0,1\}^n$$

[[This looks fairly awesomely simple, tho. still $2^n$ vbls]]

symmetrize again! Let $\sigma'(z) = \underset{\substack{\text{perms}\\ \pi \text{ on } [n]}}{\text{avg}} \tilde\sigma(\pi(z))$.

Claim 1: $\sigma'$ valid for LP, same obj.

Pf: · $\sigma'(0) = \tilde\sigma(0) = 1.$ ✓

· If $0<|z|<d$, $\tilde\sigma(\pi(z)) = 0$ $\forall\pi$ $\because |\pi(z)| = |z|$.

$\therefore \sigma'(z) = 0.$ ✓

· $\sigma'(z) \geq 0$ ✓

· $$\widehat{\sigma'}(\gamma) = \underset{\pi}{\text{avg}}\ \widehat{\tilde\sigma\circ\pi}(\gamma) \quad \because \wedge \text{ is lin. transf.}$$

$$= \underset{\pi}{\text{avg}}\ \underbrace{\hat{\tilde\sigma}(\pi^{-1}(\gamma))}_{\geq 0\ \forall\gamma} \qquad [\text{easy}]\ ✓$$

· $$\sum_z \sigma'(z) = \sum_z \underset{\pi}{\text{avg}}\ \tilde\sigma(\pi(z)) = \underset{\pi}{\text{avg}}\left\{\sum_z \tilde\sigma(\pi(z))\right\} = \underset{\pi}{\text{avg}}\left\{\underbrace{\sum_z \tilde\sigma(z)}_{LPOpt}\right\}$$ □

Rem: $\sigma'(z)$ deps only on $k := |z|$. $\therefore$ LP $\equiv$ LP with just $n+1$ vbls, $\left(\sigma_0, \dots, \sigma_n\right.$, $\left.\sigma_k = \sum_{|z|=k} \sigma(z)\right)$

Delsarte's LP [1973] [[derived by other means]]:

$$\max\ \sigma_0 + \sigma_1 + \dots + \sigma_n$$

$$\text{s.t.}\quad \sigma_0 = 1$$

$$\sigma_1, \dots, \sigma_{d-1} = 0 \qquad \text{[can delete if you want!]}$$

$$\sigma_d, \dots, \sigma_n \geq 0 \qquad \text{[[just } n+1-d \text{ vbl(s).]]}$$

$$\sum_{k=0}^{n} K_j^{(n)}(k)\sigma_k \geq 0, \qquad \forall\, 0 \leq j \leq n$$

$\therefore$ SDP$'$ $\iff$ $\max\ 2^n \sum_z \sigma(z)$

s.t. $2^n\, \sigma(0,0,\ldots 0) = 1$.

$\sigma(z) = 0$ if $0 < |z| < d$ ← Ham. wt.

$\sigma(z) \geq 0$ $\forall z$.

$$\Sigma := \begin{array}{c|c} & y \\ \hline x \in \{0,1\}^n & \begin{pmatrix} & \vdots & \\ \cdots & \sigma(x-y) & \\ & & \end{pmatrix} \end{array}$$ is P.S.D.

$\forall\ \begin{pmatrix} f \end{pmatrix} : \{0,1\}^n \to \mathbb{R}$ $\quad f^T \Sigma f \geq 0 \iff \sum_{x,y} [f(x) f(y) \sigma(x-y)] \geq 0$

$$\| \quad \sum_{x,z} f(x) f(x+z) \sigma(z)$$

$$\| \quad \sum_z \sigma(z) \sum_x f(x) f(x+z)$$

$$\| \quad \sum_z \sigma(z)\ \text{"}f*f\text{"}(z)$$

$$\iff \quad \sum_\gamma \hat{\sigma}(\gamma)\ \widehat{f*f}(\gamma) \geq 0$$

by "Plancherel's Thm" in Bool. Fourier analysis $\|$ [Basic thm]

$$\sum_\gamma \hat{\sigma}(\gamma)\ \hat{f}(\gamma)^2 \geq 0$$

This holds $\forall f$ $\iff$ $\hat{\sigma}(\gamma) \geq 0$. $\quad \forall \gamma \in \{0,1\}^n$

[Definitions] $\|$

$$\frac{1}{2^n} \sum_z (-1)^{\gamma \cdot z} \sigma(z)$$

$\therefore$ PSD condit $\equiv$ $2^n$ <u>linear</u> condits on $\sigma(z)$'s!

$K_j(k)$ = some weird # = $j^{th}$ "Kravchuk poly. @ k"
$$= \sum_{i=0}^{j} (-1)^i \binom{k}{i} \binom{n-k}{j-k}.$$

Rem: $K_0(k) = K_j(0) = 1$. ??

Largest poss dist-d code = Opt ≤ DelsarteLPOpt ≤ ?

[[Now what?? Take the dual!!]]

[MRRW 77]

$$LP \equiv 1 + \max \; \sigma_d + \cdots + \sigma_n$$
$$\text{s.t.} \quad 1 + \sum_{k=d}^{n} K_j(k)\sigma_k \geq 0 \qquad \forall\, 1 \leq j \leq n$$
$$\sigma_d, \ldots, \sigma_n \geq 0.$$

[[ $j=0$: $\sum \sigma_k \geq 0$, redundant ]]

Dual: $1 + \min \sum_{j=1}^{n} (-c_j)$
$$\text{s.t.} \quad \sum_{j=1}^{n} K_j(k)\, c_j \geq 1, \quad k = d \ldots n$$
$$c_j \leq 0 \qquad j = 1 \ldots n.$$

[[now flip the signs, negate $c_j$]]

$$\Longleftrightarrow \quad \min \; P(0)$$
$$\text{s.t.} \quad P(k) = 1 + c_1 K_1(k) + \cdots + c_n K_n(k)$$
$$c_1, \ldots, c_n \geq 0$$
$$P(k) \leq 0, \qquad k = d, \ldots, n.$$

$\geq$ Opt

[[Now you can literally start solving it for fixed d, n with CPlex. Get actual #'s. Can try to "guess" good $c_j$'s too.]]

MRRW: Gave some explicit $c_j$'s which work, did asymptotic analysis [pain...].

[Best known (asympt.) code bds]