11/6/23

Lecture 17: Statistical Query Model (Basics)

Parity w/ noise (LPN):

- Unknown $S \subseteq [n]$
- Given examples $(x_1, y_1), \ldots, (x_N, y_N)$ s.t.

$$x_i \sim \mathrm{Unif}(\{\pm 1\}^d)$$

$$y_i = \begin{cases} x_S & \text{w.p. } 1-\eta \\ -x_S & \text{o.w.} \end{cases}$$

Thm [Kearns et al. '98]: Even when $\eta = 0$, any SQ algorithm for LPN requires tolerance $2^{-\Omega(d)}$ or must make $2^{\Omega(d)}$ queries.

Pf: Consider any CSQ $\phi : \{\pm 1\}^d \to [-1, 1]$

Define $\phi_S \triangleq \mathbb{E}_x [x_S \cdot \phi(x)]$.

Claim: For uniformly random S,

$$\mathrm{Var}_S[\phi_S] \leq 2^{-\Omega(n)}$$

Pf: $\operatorname{Var}_S[\phi_S] =$ $\qquad 1$ $\quad -1$

$$\mathbb{E}_S[\phi_S^2] - \mathbb{E}_S[\phi_S]^2$$

$$= \mathbb{E}_S \mathbb{E}_{x,x'}[x_S x'_S \, \phi(x)\phi(x')]$$

$$- \mathbb{E}_{S,S'} \mathbb{E}_{x,x'}[x_S x'_{S'} \, \phi(x)\phi(x')]$$

$$= \mathbb{E}_{x,x'}\Big[\phi(x)\phi(x') \underbrace{\mathbb{E}_{S,S'}[x_S x'_S - x_S x'_{S'}]}\Big]$$

Claim: $= 0$ if $x \neq x'$

Pf: For $z \neq \vec{1}$, $\mathbb{E}_S[z_S] = 0$

So if $x \neq x'$, $\mathbb{E}_S[x_S x'_S] = \mathbb{E}[z_S] = 0$

and $\mathbb{E}_{S,S'}[x_S x'_{S'}] = \mathbb{E}_S[x_S]\,\mathbb{E}_{S'}[x'_{S'}] = 0$

b/c at most one of $x, x' = \vec{1}$.

"parity function is pairwise-independent hash function."

$$= \mathbb{E}_{x,x'}\left[\phi(x)\,\phi(x') \cdot \mathbb{1}[x = x'] \right]$$

$$= \frac{1}{2^n} \mathbb{E}_{x}\left[\phi(x)^2 \right] \leq \frac{1}{2^n}.$$

So by Chebyshev's,

$$\Pr_S\left[\left| \phi_S - \mathbb{E}_S[\phi_S] \right| \geq \tau \right] \leq \frac{\mathrm{Var}_S(\phi_S)}{\tau^2}$$

$$\leq \frac{1}{2^n \tau^2}.$$

i.e. to answer CSQ ϕ, just output $\mathbb{E}_S[\phi_S]$. If tolerance $= \tau$, this is accurate for $\frac{1}{2^n \tau^2}$ fraction of parity functions. i.e. each CSQ only rules out at most $\frac{1}{\tau^2}$ many S's, so we need $2^n/\tau^2$ queries. Taking $\tau = 2^{-n/3}$ completes the proof. $\square$