Last time: • outlined pf of

> **Theorem ★**: Let $\mathcal{C}$ be a concept class that's efficiently SQ-learnable.
> Then $\mathcal{C}$ is eff. PAC learnable in presence of RCN.
> → $\forall\ 0 \le \eta < \frac{1}{2}$, time $\text{poly}(\ldots, \frac{1}{1-2\eta})$

• Recalled that $\mathcal{C} = \{\text{all } 2^n \text{ PAR functions over } \{0,1\}^n\}$ is efficiently PAC learnable.

$n^{w(1)}$

Today: - Sketch pf that if $\mathcal{C}, \mathcal{D}$ is s.t. $\mathcal{C}$ contains many functions that are all pairwise uncorrelated under $\mathcal{D}$, then no SQ alg. can eff. learn $\mathcal{C}$ when dist. is $\mathcal{D}$.

- HW problem 5: no eff. SQ alg. exists for parities, DNFs, DTs.
- Start unit on crypto. hardness of learning "rich" concept classes.

Questions?

Def: Let $\mathcal{D}$ be dist. over $\{0,1\}^n$.
We say two concepts $c_1, c_2 : \{0,1\}^n \to \{0,1\}$ are "ε-uncorrelated" under $\mathcal{D}$ if

$$\Pr_{x \sim \mathcal{D}}[c_1(x) = c_2(x)] \in \left[\tfrac{1}{2} - \varepsilon,\ \tfrac{1}{2} + \varepsilon\right]$$

$$\to = 1 - \Pr_{x \sim \mathcal{D}}[c_1(x) \neq c_2(x)]$$

H/w: any 2 dist. PAR_{S_1}, PAR_{S_2} are perfectly uncorr.

($\varepsilon = 0$: perfectly uncorr.)

↳ under $\mathcal{D}$ = uniform.

Fact ["SQ alg's can't learn uncorr. fns"]:

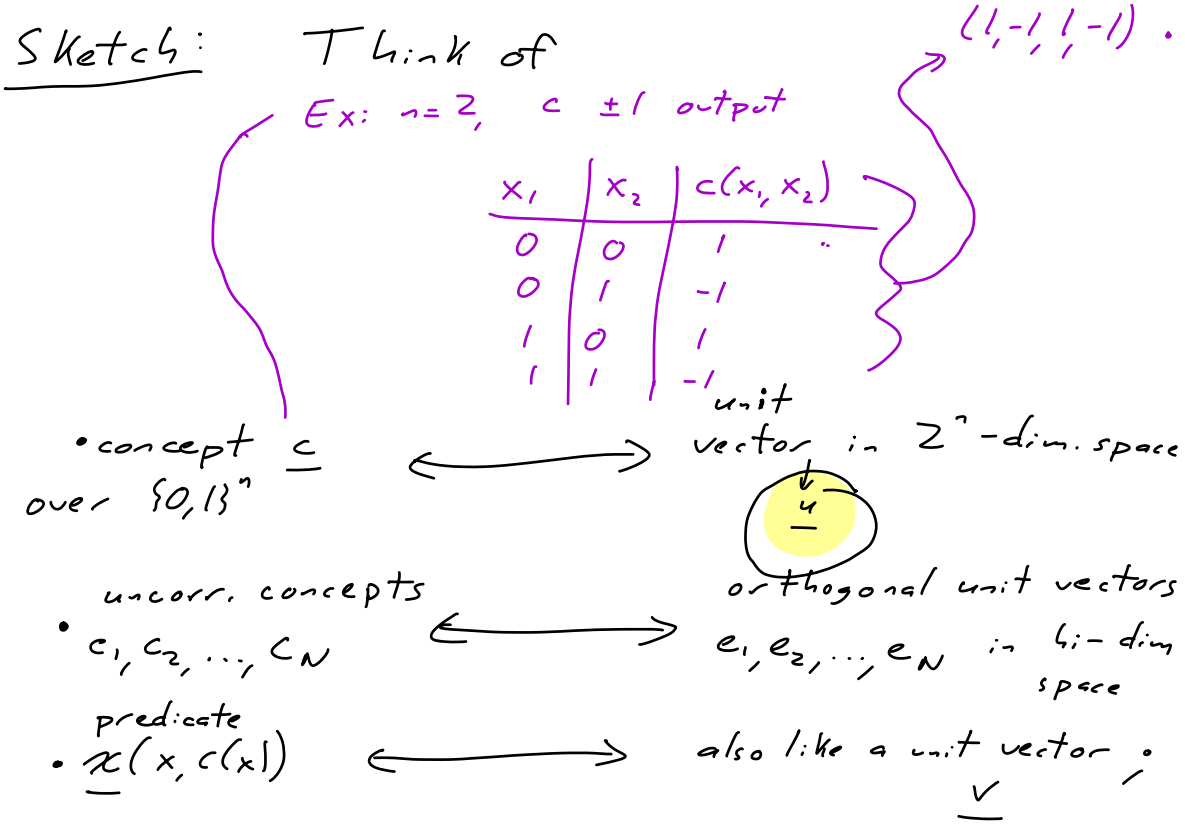
Let $\mathcal{C}$ be a concept class over $\{0,1\}^n$; let $\mathcal{D}$ be a dist. over $\{0,1\}^n$ s.t. $\mathcal{C}$ contains N concepts $c_1, \dots, c_N$ s.t. $\forall\ 1 \le i < j \le N$, c_i & c_j are perfectly $1/N^{1/3}$-uncorrelated under $\mathcal{D}$.

Then: Any SQ learning alg for $\mathcal{C}$, even only achieving weak accuracy $\frac{1}{2} + \frac{1}{N^{1/3}}$, must either

- make $\ge N^{1/3}$ SQ queries, or
- make some SQ query with tolerance $\tau \le \frac{1}{N^{1/3}}$.

$\mathcal{C}$ = all PAR's : $N = 2^n$. SQ alg's can't learn PAR.

Sketch: Think of



- value $p_x = \Pr_{x \sim \mathcal{D}}[\pi(x, c(x)) = 1]$ $\Longleftrightarrow$ value of $v \cdot u$

- Tol. param. τ $\Longleftrightarrow$ accuracy of estimate of $v \cdot u$.

- SQ learning $\Longleftrightarrow$ trying to estimate u via "what's $u \cdot v$ $\pm \tau$ to?" queries, for different unit vectors v.

Fact Let v be any unit vector $\left(v_1^2 + v_2^2 + \ldots = 1\right)$. L = large #

Can have $|v \cdot e_i| = v_i \geq \frac{1}{L}$ for $\leq L^2$ coordinates i.

Here's the lower bound for SQ learning:
Suppose every SQ is made to tol. $\tau = \frac{1}{N^{1/3}}$.

Target concept: one of $e_1, \ldots, e_N$ (= target vector u)

1st SQ: some unit vector v'.

Answer: "$v' \cdot u \approx_\tau 0$"

By FACT, v' had $\leq N^{2/3}$ coord's j s.t. $|v_j| \geq \frac{1}{N^{1/3}}$. So this means target u can't be any of those $N^{2/3}$ many j's.

2nd SQ: some unit vector v^2.

Answer: "$v^2 \cdot u \approx_\tau 0$"

Can repeat this $N^{1/3}-1$ times,

still have $N - \underline{(N^{1/3}-1)} \cdot \underline{N^{2/3}} = N - (N - N^{2/3})$

$= N^{2/3}$ poss e_i's left.

Back to HW:

(b) (c) for DNFs, DTs $N = n^{\log n}$

acc $\frac{1}{2} + \frac{1}{n^{(\log n)/3}}$: need $n^{\frac{\log n}{3}}$ SQ's

or $\tau = \frac{1}{n^{\frac{\log n}{3}}}$

SQ algs: can prove unconditional hardness.

Hardness of Learning

This course: cover 3 types of hardness of learning.

① "information-theoretic" (unconditional) hardness: hardness of learning no matter how much computation allowed.

- No PAC learning alg for mon. conj. using $\sqrt{\frac{n}{\varepsilon}}$ examples.
- No poly(n)-time SQ alg for n-term DNFs.
- Define C_{ALL} = all fns $f: \{0,1\}^n \to \{0,1\}$, $X = \{0,1\}^n$

$|C_{ALL}| = 2^{2^n}$; $VCDIM = 2^n$

No poly(n)-time/sample alg PAC learns C_{ALL}.

② "representation-dependent (HoL) hardness of learning":

↳ unsatisfying...

computationally hard to learn $\mathcal{C}$ using some particular $\mathcal{H}$

"Unless G3COL has a poly-time alg, can't learn 3-term DNF using $\mathcal{H}$ = 3-term DNFs".

(now) (3) representation-independent HoL:

"Unless (comput. problem XYZ) has an eff. alg., no eff. alg. can PAC learn $\mathcal{C}$ using any polynially evaluatable hypoth. class $\mathcal{H}$"

fns in $\mathcal{C}$ can be inherently unpredictable.

Note: (2), (3) make comput. assumptions

Seem to, for now, be stuck with ....

$P \stackrel{?}{=} NP$ Don't know...

If could show, unconditionally, that

$\mathcal{C}$ = {all n^2-term DNFs over $\{0,1\}^n$}

isn't PAC learnable in poly time:

would prove $P \neq NP$.

$P \approx$ problems where you can eff. find a solution [finding largest # in a list]

$NP \approx$ problems where you can eff. verify a solution if you're given it.
[3-coloring a graph]

Suppose showed

$C = \{$all n^2-term DNFs over $\{0,1\}^n\}$ isn't PAC learnable

If $P = NP$:

- it's poss. to verify, in poly(n, m) time, that, given
  - $S =$ data set of m lab. ex. from $\{0,1\}^n$, &
  - $g = T_1 \vee \ldots \vee T_{n^2}$ an n-term DNF,

that g is consistent with S.

If $P = NP$, there's an eff. alg. to find a (consistent n^2-term DNF for a data set lab. by an n^2-term DNF) given S.

for c using c

So have efficient CHF;

hence could PAC learn efficiently.

So we need assumptions to prove HoL

(2)

- Worst-case assumptions: no eff alg solves every instance.

"there's no poly(n)-time alg which, for EVERY n-node graph, correctly determines whether it's 3-colorable".

Stronger:

- Hard-on-average: ("average-case hardness") dist $\mathcal{D}$ on problem instances

"for suitable dist $\mathcal{D}$, no poly(n)-time alg. can succeed on 1% of instances drawn from $\mathcal{D}$"

(3)

Next time:

- HoL based on pseudorandomness
- start HoL based on public-key crypto.