Last time:

computational hardness of learning

$\mathcal{C}$ = all poly(n)-size Boolean circuits

can learn with poly(n) many examples, in exp(poly(n)) time

based on existence of pseudorandom function families

- mapping the boundary of efficient learnability
- start hardness of learning based on public-key cryptography (trapdoor 1-way permutations)

Today:

- hardness of learning based on trapdoor 1-way permutations (public-key cryptography)
  - specific (conjectured) trapdoor 1-way perm.: "discrete cube roots"
    - Hardness assump. about ⇒ certain "simple" Bool. functions (that have poly(n) size circuits) are hard to learn
      - In fact, even poly(n) size Bool. formulas.

alternative:

- Ask Me Anything review session for exam

Reminder: Closed-book, closed-note assessment this Thurs 12/04 (be on time!)

Questions?

We understand

- permut.
- one-way perm.
- trapdoor one-way perm. (TOWP)

PKC

Public-Key Cryptosystem: scheme allowing Bob

to send an (encrypted) msg to Alice in such a way that an eavesdropper Eve can't infer the underlying msg even seeing everything B sends to A (but A can decrypt the encrypted msg).

These follows directly from TOPW. Here's how:

"trapdoor" — A keeps this info secret!

Setup: • A creates a TOWP (chooses primes p, q; mult. $pq = N$)
"encryp. fn": f, the
"decryp. fn": f^{-1}.
A knows trapdoor info $(p \& q)$, so can eff. compute f^{-1} on any point
• A publishes alg. for computing f. (Publishes N.)

To send a secure msg z to A, Bob:

• computes $f(z)$
• sends $f(z)$ to A.
→ A applies her alg for computing f^{-1} to $f(y)$, & gets $f^{-1}(f(y)) = y$. :)
• What about Eve? She sees $f(z)$, but lacks trapdoor info, so can't compute f^{-1} on $f(z)$ & can't recover y.

RSA

(TOWP)

Key conn. between PKC & learning: if scheme is secure, the decryption fns f^{-1} are hard to learn.

Why? Sps there's an eff. learning alg. A to learn decryp. fns.

Crypto/eavesdrop. world:

E gets some $f(z)$, wants to invert f & get z i.e. compute f^{-1} on $f(z)$.

Key point: Eve can generate data set needed by A!

Does this by drawing $y^1, y^2, \ldots, y^m$ & computing $f(y^1), \ldots, f(y^m)$, & using

$(f(y^1), y^1)$
$(f(y^2), y^2)$
$\vdots$
$(f(y^m), y^m)$

} distrib. is identical to dist. of.

Learning world:

learning alg. A gets labeled ex's

$(x^1, f^{-1}(x^1))$
$(x^2, f^{-1}(x^2))$
$\vdots$
$(x^m, f^{-1}(x^m))$

} x^i's unif rand.

computes, outputs hi-acc. hyp. h (so on fresh ex. y, whp $h(y) = f^{-1}(y)$).

PKC

So, if TOWP exist, the decryp. fns (f^{-1}'s) are a hard-to-learn class of fns.

$X = [0,1]$

$\mathcal{C}$ = intervals like $[.38, .417]$

$|\mathcal{C}| =$ infinite

$VCDIM(\mathcal{C}) \leq 2$:

$\cdot \quad \cdot \quad \cdot$

$+ \quad - \quad +$ no interval lab. 3 pts this way.

$\mathcal{C} =$ {1}, {2}, ⋮ is ∞ "☺" (1)

$h_1 = \{1\}$ adv: $x' = 1$ $h_1(x') = 1 +$ Yes

adv: no, sorry, $c(x') = c(1) = 0$ WRONG

(2) too "☺"

Def of "A has MB M for $\mathcal{C}$": (OCMB alg)

∀ seq of ex $x^1, x^2, \ldots \in X$

∀ target conc. $c \in \mathcal{C}$,

if c is target conc. ∀ is seq of ex, alg makes $\leq M$ mist.

$\mathcal{C} = \{ \{1\}, \{2\}, \{3\}, \ldots \}$

$|\mathcal{C}| = \infty$

VCOIM(e) = 1

3, 5, 1, 4, 9

$\frac{3}{22}, \frac{5}{22}, \frac{1}{22}, \frac{4}{22}, \frac{9}{22}$

$$Z_t = \sum_{i=1}^{m} \vartheta_t(i) \exp(-\alpha_t y_i h_t(x^i))$$

---

hyp h error $\mathrm{err}_\vartheta(h, c)$

"adv of h" $= \frac{1}{2} - \mathrm{err}_\vartheta(h, c)$

$\mathrm{err} \in (0, \frac{1}{2})$: $0 < \gamma < \frac{1}{2}$

#1 PS 5:

(i) argued for ± 1 valued hyp's h

target c:

can view adv. either in terms of

$\frac{1}{2} - \mathrm{err}_\vartheta(h, c)$, or in terms of

$\frac{1}{2} \cdot \mathbb{E}_{x \sim \vartheta}[h(x) c(x)]$

- h perfect: $= 1$. adv. $\frac{1}{2}$
- h 50% error: adv. $= 0$, $\not\equiv$ adv. 0

(ii) : if f is a low-wt LTF over $\{\pm 1\}^n$, $f = \mathrm{sign}\left(\sum_{i=1}^{n} w_i x_i\right)$

$w_i \in \mathbb{Z}$, $\sum_{i=1}^{n} |w_i| = W$ odd,

for any dist $\mathcal{D}$, $\exists\ i \in [n]$ s.t.

either $\mathbb{E}[f(x) x_i] \geq \frac{1}{W}$ or

$\mathbb{E}[f(x) \cdot (-x_i)] \geq \frac{1}{W}$.