COMS 6998: Unconditional Lower Bounds & Derandomization

Overview of today:

- introductions (me, you, topic of course)
- administrative / logistical overview (web page)
- more detailed overview of course topic
- start unit on Boolean formulas

(Scribe: Ashvin & Sam)

General topic: cxity thy

why are some functions hard to compute?

→ 2 strands:

1) Hi-level cxity: P, NP, BPP, PSPACE

Deep questions:

(Conditional)

Ⅰ: Are there natural problems that have no efficient algs? (P=NP ?)

Ⅱ: Is randomness helpful for efficient computation (P= BPP ?)

2) Low-level complexity: unconditional results!

But... about restricted models of comput.

We'll look at

diff. restricted models

- Boolean formulas
- shallow Bool. ckts
- DNF/CNF formulas
- decision trees
- branching programs
- polynomial models
- communic. protocols
- ⋮

diff. research goals

(A) • Worst-case lb's

(B) • average-case lb's

(C) • PRGs (pseudorandom generators)

(D) • Deterministic approximate counting algs.

More detailed overview:

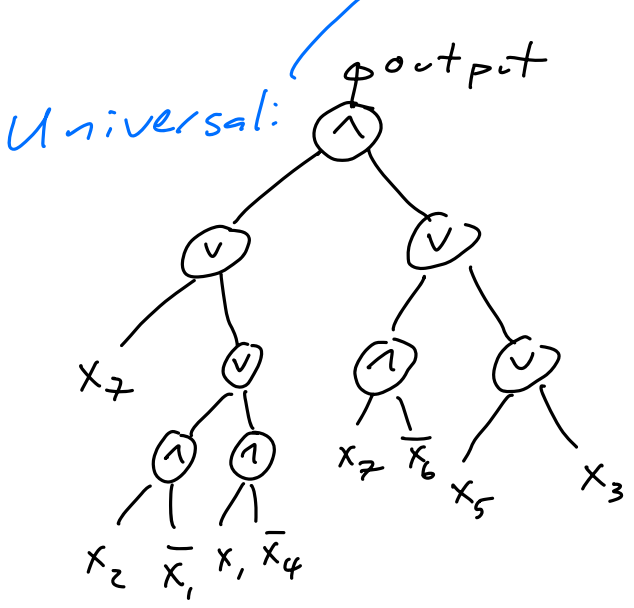
Readings: HH survey Chap 1, Chap. 4.1

Some comput. models we'll consider:

(Each one: way of computing $f: \{0,1\}^n \to \{0,1\}$)

- Boolean formulas:

→ every $f \in FORM_{2^n}$



Universal:

$1 \wedge 1 = 1$

$1 \wedge 0 = 0$

$1 \vee 0 = 1$

etc.

size = # leaves

depth = depth

$FORM_s = FORM_{s(n)}$

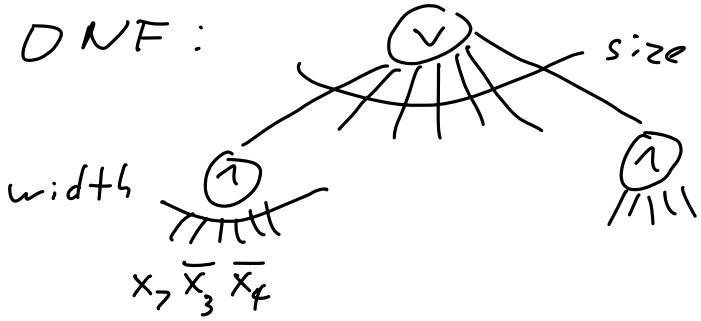
= class of all $f: \{0,1\}^n \to \{0,1\}$ computable by form. of size $\leq s$.

(Today: $\sum_{i=1}^{n} x_i \bmod 2 \notin FORM_{n^{1.49}}$.)

- DNFs, CNFs:

OR-of-AND

DNF:



size-s DNFs: univ. if $s \geq 2^{n-1}$

size = # $\wedge$-gates

width = max # lits in any term

univ. only if $k = n-1$

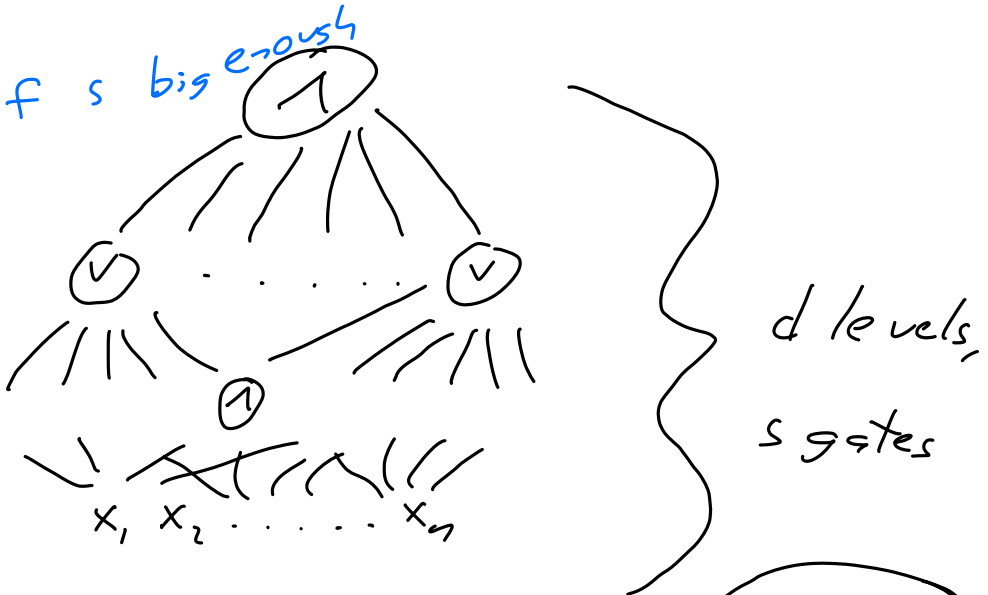
k-DNF = all $f: \{0,1\}^n \to \{0,1\}$ comput. by width-k DNFs.

size-s-DNF = all $f: \{0,1\}^n \to \{0,1\}$ comput. by size-s DNFs.

CNF: $\wedge$ of $\vee$'s.

- $AC^0_{d,s}$ = depth-d, size-s $\wedge/\vee/\neg$ ckts

univ. $d \geq 2$ if s big enough



Last one: $\mathbb{F}_2$-polynomials. (Everything mod 2)

. .

$x_1x_2x_4 + x_1x_4x_5x_6 + \ldots$

$x_1x_2\ldots x_n = AND(x_1,\ldots,x_n)$

sparsity = # monom.

degree = max deg any monomial.

DEG_d = all $f: \{0,1\}^n \to \{0,1\}$ comput. by deg-d $\mathbb{F}_2$-polynomial.

univ. if $d=n$

---

n: asymptotic parameter. $DEG_d = \{n \geq 1\}$

Goals:

(1) Establishing Hardness.

Dream: $P \neq NP$. We think it's true. little progress towards pf "

How might you try to prove $P \neq NP$?

Known:

$P \neq NP$ if bad (worst-case) lb's on Bool. ckts computing $f \leftrightarrow L \in NP$.

If knew

(★) "Any family $(C_n)_{n \geq 1}$ of ckts (unrestricted ckts) solving HAM-CYCLE on n-node graphs must have size $\geq n^{\omega(1)}$"

then get $P \neq NP$.

Don't know how to prove this! (★)

So we replace unrestricted ckts

with restricted models.

Ⓐ

Def ("worst-case hardness"):
Let $\mathcal{C}$ be a class of fns $f: \{0,1\}^* \to \{0,1\}$
(e.g. $\mathcal{C} = FORM_{n^{1.49}}$)

We say $h: \{0,1\}^* \to \{0,1\}$ is worst-case hard for $\mathcal{C}$ if $h \notin \mathcal{C}$.

"Worst-case": b/c on "worst" input, h is wrong.

Stronger notion (l.b.): avg-case hardness

Def: Let $f, g: \{0,1\}^* \to \{0,1\}$,
let $\mathcal{D}$ be some distrib. on $\{0,1\}^*$.

Define

$$Cor_{\mathcal{D}}[f,g] = \left| \Pr_{x\sim\mathcal{D}}[f(x)=g(x)] - \Pr_{x\sim\mathcal{D}}[f(x)\neq g(x)] \right|$$

($1-p$ and p)

$$= 2 \cdot \left| \frac{1}{2} - \Pr_{x\sim\mathcal{D}}[f(x)\neq g(x)] \right| \in [0,1]$$

(correl! f,g under $\mathcal{D}$)

For $\mathcal{C}$ a class of fns f, say g a fixed fn,

$$\mathrm{Cor}_{\mathcal{D}}[g, \mathcal{C}] = \max_{f \in \mathcal{C}} \mathrm{Cor}_{\mathcal{D}}[f, g]$$

If $\mathcal{D}$ = unif dist $\mathcal{U} = \mathcal{U}_n$ over $\{0,1\}^n$: just write

$$\mathrm{Cor}[f, g] \quad \text{or} \quad \mathrm{Cor}[g, \mathcal{C}].$$

Obs: • $f \equiv g$ or $f \equiv \bar{g}$, $\mathrm{Cor} = 1$.

• if $f, g: \{0,1\}^n \to \{-1, 1\}$,

$$\mathrm{Cor}_{\mathcal{D}}[f, g] = \left| \mathop{\mathbb{E}}_{x \sim \mathcal{D}} [f(x) \cdot g(x)] \right|$$

Rephrase:

(B)

Def: (Avg-case hardness)

Let $\mathcal{C}$ be a class of fns $f: \{0,1\}^n \to \{0,1\}$
Let $\mathcal{D}$ be dist over $\{0,1\}^n$
Let $\varepsilon > 0$.
We say $h: \{0,1\}^n \to \{0,1\}$ is ε-hard for $\mathcal{C}$ with respect to $\mathcal{D}$ if $\forall f \in \mathcal{C}$, have

$$\left| \Pr_{x \sim \mathcal{D}} [f(x) = h(x)] - \frac{1}{2} \right| \leq \varepsilon$$

i.e. $\mathrm{Cor}_{\mathcal{D}}[f, \mathcal{C}] \leq 2\varepsilon$.

Smaller ε : 4 harder.

(B): Stronger than (A).

After break: (C), (D) randomness

Second Goal:

(2) Getting Rid of Randomness

Rand. algs: alg can toss coins.

↳ often either simplest or only eff algs we know!

Ex1) Graph reachability: G = n-node undir. graph

s, t nodes. Is t reachable from s?

Here's a rand alg:

- start at s
- walk randomly

↳ Can show: $100n^2$ steps:

if t is reach. from s, $\Pr[\text{hit } t] \geq 0.99$.

↳ $O(\log n)$ space!

Ex 2) Polynomial Identity Testing.

Input: $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ algebraic formulas $+, \times$, coefficient

$$(x_1 + x_2) \cdot (3x_2^4 - x_3^5) + 5(x_1 - x_3 x_4)(x_6 x_7^7 + x_8^3)$$

Q: is $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ $\forall x$?

Only known eff alg: randomized! Let $m = |p| + |q|$ (length of input)

Pick $x = (x_1, \ldots, x_n)$ unif. from $\{1, 2, \ldots, 3m\}^n$

Check if $p(x) = q(x)$

If $p \not\equiv q$, $\Pr[p(x) = q(x)] \leq \frac{\deg(p-q)}{3m} \leq \frac{1}{3}$

P = BPP question:

does every poly-time rand alg. have an eff. det. analogue?

Maybe so...? Long history of rand. alg. getting derand.

Ex 1) rand walk alg for Graph Reach: 1979

25 years later: derand. (Reingold,

$O(\log n)$-space det alg. for —.)

Diff. ex: primality testing.

early 1970's : poly(n)-time rand alg for n-bit primality testing

" 2000's : poly(n)-time det alg for n-bit primality testing.

How could you show $P = BPP$

One way: giving explicit PRG for $\mathcal{C} = \{\text{all poly}(n)\text{-size Bool ckts}\}$

Def: (Fooling) Let $f: \{0,1\}^n \to \{0,1\}$, let X be a rand. variable over $\{0,1\}^n$.

X ε-fools f if $\left| \mathbb{E}[f(X)] - \mathbb{E}[f(U_n)] \right| \leq \varepsilon$.

(X ε-fool $\mathcal{C}$: X ε-fools all $f \in \mathcal{C}$)

Def (PRG for $\mathcal{C}$): Let $f: \{0,1\}^n \to \mathbb{R}$,

Let $G: \{0,1\}^s \to \{0,1\}^n$, let $\varepsilon > 0$.

G is an ε-PRG for f (G fools f with error ε)

if $G(\mathcal{U}_s)$ fools f with error ε.

G is an ε-PRG for $\mathcal{C}$ if G is an ε-PRG for all $f \in \mathcal{C}$.

Idea: $s \ll n$; toss s coins, not n, & $\mathcal{U}_s$ $\mathcal{U}_n$

$s =$ "seed length" of PRG

that's good enough for f.

Lemma (Nonexplicit PRGs are easy!) exist/

Let $\mathcal{C}$ be any class of fns $f: \{0,1\}^n \to \{0,1\}$

Let $\varepsilon > 0$.

There's an ε-PRG for $\mathcal{C}$ with seed length

$$\log\log|\mathcal{C}| + 2\log\frac{1}{\varepsilon} + O(1).$$

Pf: Let $G: \{0,1\}^s \to \{0,1\}^n$ be uniform rand:

$G(y)$ unif. rand. $\in \{0,1\}^n$ $\forall y$.

Fix an $f \in \mathcal{C}$.

For each fixed s-bit y, $f(G(y))$ is a rand. bit

with $\mathop{\mathbb{E}}_{G}[f(G(y))] = \mathop{\mathbb{E}}_{\mathcal{U}_n}[f]$

Indep. $\left(\mathbb{E}[f] \equiv \mathbb{E}_{\text{all } n}[f(\text{all } n)]\right)$

Chernoff bd $\Rightarrow$

$$\Pr_G\left[\left|\mathbb{E}[f] - \frac{1}{2^s}\sum_{y\in\{0,1\}^s} f(G(y))\right| > \varepsilon\right] \le \underbrace{2e^{-2\varepsilon^2\cdot 2^s}}_{\text{tiny!}}$$

Union bd over all $f \in \mathcal{C}$:

$$\Pr_G[G \text{ doesn't } \varepsilon\text{-fool } \mathcal{C}] \le 2|\mathcal{C}|\cdot e^{-2\varepsilon^2\cdot 2^s}$$

If $s = \log\log|\mathcal{C}| + 2\log\frac{1}{\varepsilon} + O(1)$, then < 1.

So some outcome of G fools $\mathcal{C}$. ∎

Even $\mathcal{C}$ = all poly(n)-size ckts has

$$|\mathcal{C}| = 2^{\text{poly}(n)} \quad \& \quad s = O(\log\tfrac{n}{\varepsilon})$$

"use randomness once to get G, & that's enough!" 😊

We used $ to get G 😊

Our goal: explicit PRGs.

(G is explicit: there's a det alg

that computes $G(x)$ given s-bit x, in poly(n) time.)

Derandomize, given PRG, by trying all seeds:

Lemma: Sps $G: \{0,1\}^s \to \{0,1\}^n$ is an expl. PRG that ε-fools $\mathcal{C}$.

Then there's a det alg. running in $2^s \cdot \text{poly}(n)$ time giving a value in

$$\left[\mathbb{E}[f] - \varepsilon,\ \mathbb{E}[f] + \varepsilon\right].$$

Not hard to show: (seed length $= s$)

Corollary: If had expl. PRG G for $\mathcal{C} = \overset{\text{all}}{\text{poly}}(n)$-size ckts, then get $2^s \cdot \text{poly}(n)$-time alg. for any language in BPP.

Pf sketch:

Given input x to rand alg., view C_x as ckt on rand. coins $r = (r_1, \ldots)$

Fool this C_x.

So $O(\log \frac{n}{\varepsilon})$ - s.l. PRG for poly-size ckts $\Rightarrow$ P = BPP.

↳ Motivates trying for small seed length PRG's for diff $\mathcal{C}$'s.

Hardness & PRG link:

Lemma: (PRG $\Rightarrow$ worst-case lb)

Let $\mathcal{C}$ be class of n-bit fns f s.t. $\mathcal{C}$ closed under restrictions

$f \in \mathcal{C} \Rightarrow$

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \in \mathcal{C}$$

All our classes sat. this

Let $G: \{0,1\}^s \to \{0,1\}^n$ be ε-PRG (↳ explicit) for $\mathcal{C}$, where $s < n$, $\varepsilon < 1/2$.

Define $h: \{0,1\}^{s+1} \to \{0,1\}$ as outputting 1 on x if some string in range of PRG starts with x:

$h(x) = 1$ iff $\exists\, y \in \{0,1\}^s, z \in \{0,1\}^{n-s-1}$ s.t.

$G(y) = (x, z)$ — y: s bits; x: $s+1$ bits; z: $n-s-1$ bits

Let $\mathcal{C}'$ be all restric. of fns in $\mathcal{C}$ by fixing last $n-s-1$ bits, leaving first $s+1$ alive.

Then $h \notin \mathcal{C}'$. (worst-case hardness!)

Pf: G ε-fools $\mathcal{C}$, & $\mathcal{C}$ closed under restr,

So $G(U_s)_{1,\dots,s+1}$ ε-fools $\mathcal{C}'$.

But G doesn't fool h:

$$\mathbb{E}\left[h\left(G(U_s)_{1,\dots,s+1}\right)\right] = 1, \quad \text{while} \quad \mathbb{E}_{U_{s+1}}\left[h(U_{s+1})\right] \le \frac{1}{2}$$

(def of h; b/c G's image size $\le 2^s$.)

So PRGs $\Rightarrow$ worst-case lb's.

Next time:

- PRGs $\Rightarrow$ avg-case lb's.

- det. approx. counting
- Boolean formula lb's.
