Week 6

Announcements:

- HW2 solns posted.
- More practice problems for Test 2 posted
- Test 2: Next Friday Oct 23 (~50 mins)

Today: Randomized Algorithms cont'd
and review for Test 2

Review Last Week - Probability Inequalities

① Markov Inequality Let $X : S \to \mathbb{R}^+$, $\mathcal{D}$ distrib over S.

$$\forall K \geq 1 : \quad \Pr_{\mathcal{D}}[X \geq K \cdot E[X]] \leq \frac{1}{K}$$

② Chebyshev's Inequality: $\Pr[|X - \mu| \geq a] \leq \frac{\text{Var}[X]}{a^2}$

$$\mu = \mathbb{E}[X], \quad \text{Var}[X] = \mathbb{E}[(X - \mu)^2]$$

(3) Chernoff / Hoeffding Inequalities

* requires $X = X_1 + \ldots + X_m$, $X_i \in \{0,1\}$ indep rv's

Chernoff Ineq Let $X = X_1 + \ldots + X_m$, each X_i indep 0/1 random vars, $\mathbb{E}[X] = \mu$

Then $\forall\ 0 \le \delta \le 1$:

$$\Pr[X < (1-\delta)\mu] \le e^{-\frac{1}{2}\delta^2\mu} \quad \text{and}$$

$$\Pr[X \ge (1+\delta)\mu] \le e^{-\frac{1}{3}\delta^2\mu}$$

} multiplicative form

Hoeffding Ineq Let $X = X_1 + \ldots + X_m$, each X_i indep 0/1 rv's, $\mathbb{E}[X] = \mu$

Then for all $a > 0$: $\Pr[|X - \mu| \ge a] \le 2e^{-2a^2/m}$

} additive form

Randomized Complexity Classes

Defn (RP) $L \in RP$ if $\exists$ polytime TM $M(x,r)$ [polytime in $|x|=n$]

s.t. $\forall x$:

$x \in L \Rightarrow \Pr_r[M(x,r) \text{ accepts}] \geq 2/3$

$x \notin L \Rightarrow \Pr_r[M(x,r) \text{ accepts}] = 0$

one-sided error!

Defn (coRP) $L \in RP$ if $\exists$ polytime TM $M(x,r)$ [polytime in $|x|=n$]

s.t. $\forall x$:

$x \notin L \Rightarrow \Pr_r[M(x,r) \text{ rejects}] \geq 2/3$

$x \in L \Rightarrow \Pr_r[M(x,r) \text{ accepts}] = 1$

one-sided error!

equivalently $L \in coRP$ iff $\bar{L} \in RP$

Defn [BPP] $L \in BPP$ if $\exists$ polyTIME TM $M(x,r)$ [polytime in $|x|=n$]

s.t. $\forall x$:

$x \in L \Rightarrow \Pr_r[M(x,r) \text{ accepts}] \geq 2/3$

$x \notin L \Rightarrow \Pr_r[M(x,r) \text{ accepts}] \leq 1/3$

2 sided error!

BPP alg with (2-sided) error $\varepsilon = 1/3$

Error Amplification

Theorem 1 If A is an RP algorithm for L with error $\varepsilon = \frac{1}{3}$ then for all polynomials $p(n) > 0$ there is another RP algorithm A' for L with error $\left(\frac{1}{2}\right)^{p(n)}$

Proof for RP is easier

Theorem 2 Same as Theorem 1 but with RP replaced by BPP

Proof

Idea for RP: Run $A(x, *)$ on fresh random strings $r_1 \ldots r_{p(n)}$ $p(n)$ times
Accept x iff $A(x, r_i)$ accepts $\forall r_i$

Idea for BPP: Run $A(x, *)$ on fresh random strings $r_1 \ldots r_{p(n)}$
Accept x iff majority answer of $\{A(x, r_1) \ldots A(x, r_{p(n)})\}$ is 1

RP amplification:

Let $A \in RP$ accept L (with error ε : $x \in L \Rightarrow Pr[A(x,r) \text{ accepts}] \geq 1-\varepsilon$)

A' on x:

Run $A(x,\cdot)$ k times each independently. reject ↓ accept ↑

Let outcomes be $\{o_1, o_2, \ldots, o_k\}$, $o_i \in \{0, 1\}$

Accept x if $\exists o_i$ s.t. $o_i = 1$; Reject x ow.

Error prob of A' on x:

1. $x \in L$: $\text{Prob}[A'(x) \text{ rejects}] \leq \varepsilon^k$ (all o_i's must be 0 to reject)

2. $x \notin L$: $\text{Prob}[A'(x) \text{ accepts}] = 0$ so A' still never errs on x's not in L

RP amplification contd

So if $x \in L$ A' accepts x wp $\geq (1 - \varepsilon^k)$

$\varepsilon = \frac{1}{3} \Rightarrow 1 - \left(\frac{1}{3}\right)^k$

Runtime of A' on $x \approx$ [Runtime of $A(x, \cdot)$] $\times k$.

$\therefore$ can drive error on yes inputs to be exponentially small in $|x|$ (pick $k = n = |x|$) and still run in polytime

BPP amplification

$A'(x)$: Run $A(x,*)$ k times each independently. reject ↓ accept ↓

Let outcomes be $\{X_1, \ldots, X_k\}$ $X_i \in \{0, 1\}$

If $\underbrace{X_1 + \ldots + X_k}_{\text{counts \# of accepts}} \geq \frac{k}{2} \Rightarrow$ accept

ow fail

Analysis : use Chernoff / Hoeffding:

2 cases (1) $x \in L$

(2) $x \notin L$

Case 1 Fix $x \in L$.

Let $X = X_1 + \dots + X_K$

$$X_i = \begin{cases} 1 & \text{if } i^{th} \text{ run } A(x,r) = 1 \\ 0 & \text{ow} \end{cases}$$

$$\Pr[X_i = 1] = \Pr_r[A(x,r) = 1] = p_{yes} \geq 2/3$$

$\mu = \mathbb{E}[X]$

$= K \cdot \mathbb{E}[X_i]$

$= K \cdot p \geq \frac{2K}{3}$

$\forall\ 0 \leq \delta \leq 1$:

$\Pr[X < (1-\delta)\mu] \leq e^{-\frac{1}{2}\delta^2\mu}$

$\Pr[X \geq (1+\delta)\mu] \leq e^{-\frac{1}{3}\delta^2\mu}$

$x \in L$: Want to show $\Pr[X < \frac{K}{2}] \leq \left(\frac{1}{e}\right)^{\frac{K}{48}}$ ☺

$\Pr[X \leq (1-(1-\frac{1}{2p}))pK]$ set $K/2 = (1-\delta)\mu = (1-\delta)pK \Rightarrow \delta = 1 - \frac{1}{2p}$

$\leq \Pr[X \leq (1-\frac{1}{4})K \cdot \frac{2}{3}]$ set $p = 2/3$

$\leq \exp\left(-\delta^2 \frac{\mu}{2}\right)$ chernoff with $\delta = \frac{1}{4}$ $\mu = \frac{2}{3}K$

$\leq \left[\frac{1}{e}\right]^{\mu/32}$

$= \left[\frac{1}{e}\right]^{K/48}$

* Do other case (ii) $x \notin L$

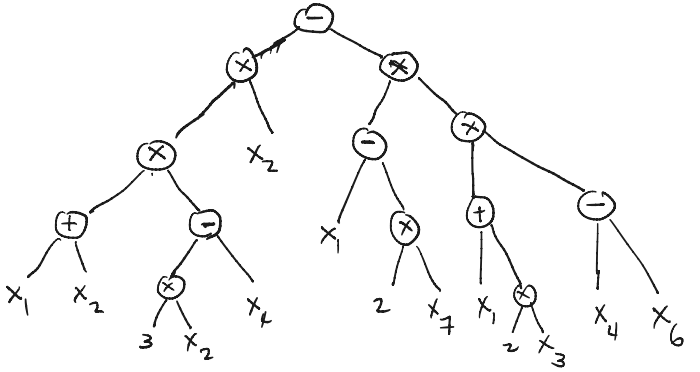
An example where Randomness seems to help:

Polynomial Identity Testing ("PIT"):

Input is an n-variable algebraic formula/expression $p(x_1 \ldots x_n)$

Example $p(x_1 \ldots x_n) = \left[(x_1 + x_2)(3x_2 - x_4)\right]x_2 - \left[x_1 - 2x_7\right]\cdot\left[(x_1 + 2x_3)(x_4 - x_6)\right]$

$p(x_1 \ldots x_n) =$



accept iff $p(x_1, \ldots, x_n) \equiv 0$ ← as a formal polynomial after cancellation

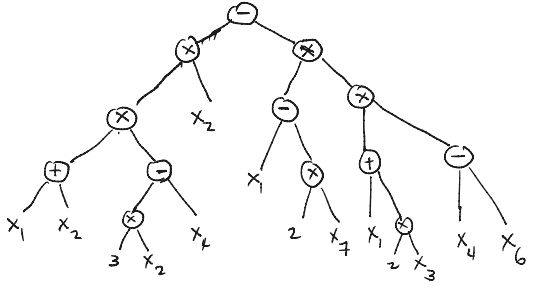
Polynomial Identity Testing ("PIT")

Example $p(x_1 \ldots x_n) = \left[(x_1+x_2)(3x_2-x_4)\right]x_2 - \left[x_1-2x_7\right]\cdot\left[(x_1+2x_3)(x_4-x_6)\right]$

operations:
binary $+, -, \times$

Input: vars x_i or an integer

$p(x_1 \ldots x_n) =$



accept iff $p(x_1, \ldots, x_n) \equiv 0$ ← as a formal polynomial after cancellation

Obvious algorithm: Expand $p(x_1 \ldots x_n)$ to write as sum of monomials, and check if $\equiv 0$

Ex. $q(x_1, x_2) = -x_1^2 + x_2(4x_2 + 2) + (x_1 - 2x_2)(x_1 + 2x_2 + 1) - x_1 \equiv 0$

PIT is in coRP

Idea: on input algebraic ckt $p(x_1 .. x_n)$:

Plug in random values $a_1, \ldots, a_n$ for input vars and check if $p(a_1 .. a_n) = 0$

Note: can't just try one deterministically chosen value

Instead we will pick random values for each x_i in some range $[1, \ldots, M]$, $M = 2^{|p|}$ $|p|$ = algebraic formula/ckt size of input

and argue whp $p(a_1 .. a_n) = 0 \Leftrightarrow p \equiv 0$

PIT is in coRP

Alg A on input $p(x_1 \ldots x_n)$:

Let $m = |p|$, $M = 2^m$

Pick n random integers $a_1 \ldots a_n$ from $\{1, \ldots, M\}$

Evaluate $p(a_1 \ldots a_n)$. Accept iff $p(a_1 \ldots a_n) = 0$

← coRP algorithm
r = random integers $a_1, \ldots, a_n \in [M]$

Claim 0 Alg runs in polytime in $|p|$

Claim 1 $\forall p$, if $p \equiv 0$, alg accepts with probability 1

Claim 2 $\forall p$, if $p \not\equiv 0$, $\Pr[A(p, r) \text{ accepts}] \leq \frac{m}{M} = \frac{m}{2^m}$

PIT - Better Randomized Algorithm

Alg A on input $p(x_1 \ldots x_n)$: $|p|$ = # operations = size of algebraic formula p

Let $m = 2^{|p|}$, $M = 2^m$

Pick n random integers $a_1 \ldots a_n$ from $\{1, \ldots, M\}$

Evaluate $p(a_1 \ldots a_n)$. Accept iff $p(a_1 \ldots a_n) = 0$

Claim 0 Alg runs in polytime in $|p|$ ✓

Claim 1 $\forall p$, if $p \equiv 0$, alg accepts with probability 1 ✓

Claim 2 $\forall p$, if $p \not\equiv 0$, $\Pr[A(p, r) \text{ accepts}] \leq \frac{m}{M} = \frac{m}{2^m}$

Proof of Claim 2 $\left[\forall p,\ \text{if } p \not\equiv 0,\ \Pr[A(p,r) \text{ accepts}] \le \frac{m}{M} = \frac{m}{2^m}\right]$

Fact 1 If p is an algebraic formula then $\text{degree}(p) \le |p|$

Lemma [Schwartz-Zippel Lemma]
Let S be any finite set of numbers, and let $p(x_1 \ldots x_n) \not\equiv 0$
Then $\Pr_{a_1,\ldots,a_n \in S}[p(a_1 \ldots a_n) = 0] \le \frac{\text{degree}(p)}{|S|}$

(We will pick $S = \{1, \ldots, 2^m\}$)

Proof of Claim 2

Assume $p(x_1 \ldots x_n) \not\equiv 0$. Pick $S = \{1, 2, \ldots, M\}$, $M = 2^m = 2^{|p|}$

By Swartz-Zippel Lemma: $\Pr_{a_1 \ldots a_n \in S}[p(a_1 \ldots a_n) \text{ accepts}] \le \frac{\deg(p)}{M} \le \frac{m}{M} \le \frac{1}{m}$

By Fact $\deg(p) \le |p| = m$

Fact 1 If p is an algebraic formula, then $\text{degree}(p) \leq |p|$

Proof by Induction on $|p|$

Base case: $|p| = 1$ so p is either a variable or constant
so $\deg(p) \leq 1$

Induction step

$$p = p_1 \cdot p_2 \quad : \quad \deg(p) \leq \deg(p_1) + \deg(p_2)$$
$$\leq |p_1| + |p_2| \leq |p|$$

$$p = p_1 + p_2 \quad : \quad \deg(p) \leq \max\{\deg(p_1), \deg(p_2)\}$$
$$\leq |p_1| + |p_2| \leq |p|$$

Lemma ["Schwartz-Zippel" Lemma]

Let S be any finite set of numbers, and let $p(x_1 \ldots x_n) \not\equiv 0$.

Then $\Pr_{a_1,\ldots,a_n \in S} [p(a_1 \ldots a_n) = 0] \leq \frac{\text{degree}(p)}{|S|}$

Proof By induction on # vars in p $(= n)$

$n = 1$: $p(x)$ is univariate polynomial

Use fact that every degree-d univ poly has $\leq d$ roots

$\therefore \Pr_{a \in S} [p(a) = 1] \leq \deg(p)/|S|$

Lemma [Schwartz-Zippel Lemma]

Let S be any finite set of numbers, and let $p(x_1 \ldots x_n) \not\equiv 0$.

Then $\Pr_{a_1,\ldots,a_n \in S} [p(a_1 \ldots a_n) = 0] \leq \frac{\text{degree}(p)}{|S|}$

Proof By induction on # vars in p $(= n)$

$n = 1$: $p(x)$ is univariate polynomial

Use fact that every degree-d univ poly has $\leq d$ roots

$\therefore \Pr_{a \in S} [p(a) = 1] \leq \deg(p)/|S|$

Induction step:

Write $p(x_1 \ldots x_n) = \sum_{i=0}^{k} P_i(x_1 \ldots x_{n-1}) \, x_n^k$ where k = max degree of x_n in p

$$\Pr_{a_1 \ldots a_n \in S}[p(a_1 \ldots a_n) = 0] \leq \Pr[P_k(a_1 \ldots a_{n-1}) = 0] + \Pr[p(a_1 \ldots a_n) = 0 \mid P_k(a_1 \ldots a_{n-1}) \neq 0]$$

since $\Pr(A) = \Pr[A \wedge B] + \Pr[A \wedge \bar{B}] \leq \Pr[B] + \Pr[A \wedge \bar{B}]$

$= \Pr[B] + \Pr[\bar{B}] \cdot \Pr[A \mid \bar{B}]$

$\leq \Pr[B] + \Pr[A \mid \bar{B}]$

Lemma [Schwartz-Zippel Lemma]

Let S be any finite set of numbers, and let $p(x_1 \ldots x_n) \not\equiv 0$.

Then $\Pr_{a_1, \ldots, a_n \in S} [p(a_1 \ldots a_n) = 0] \leq \frac{\text{degree}(p)}{|S|}$

Induction step:

Write $p(x_1 \ldots x_n) = \sum_{i=0}^{k} P_i(x_1 \ldots x_{n-1}) x_n^k$ where k = max degree of x_n in p

Then: $\Pr_{a_1 \ldots a_n \in S} [p(a_1 \ldots a_n) = 0] \leq \Pr[P_k(a_1 \ldots a_{n-1}) = 0] + \Pr[p(a_1 \ldots a_n) = 0 \mid P_k(a_1 \ldots a_{n-1}) \neq 0]$

First term: By I.H. $\therefore \Pr[P_k(a_1 \ldots a_{n-1}) = 0] \leq \frac{\deg(P_k)}{|S|}$

Second term: given values $a_1 \ldots a_{n-1}$ p is a degree k poly in one variable x_n

$\therefore \Pr_{a_1 \ldots a_n \in S} [p(a_1 \ldots a_n) = 0] \leq \frac{\deg(P_k)}{|S|} + \frac{k}{|S|} \leq \frac{\deg(p)}{|S|}$ ✓

Inclusions : $P \subseteq \begin{matrix} RP \\ coRP \end{matrix} \subseteq BPP \subseteq EXP$

$E = 2^{O(n)}$

$EXP = 2^{n^{O(1)}} = 2^{poly(n)}$

OPEN 1 Is $P = BPP$? Conjectured to be true.

what's known

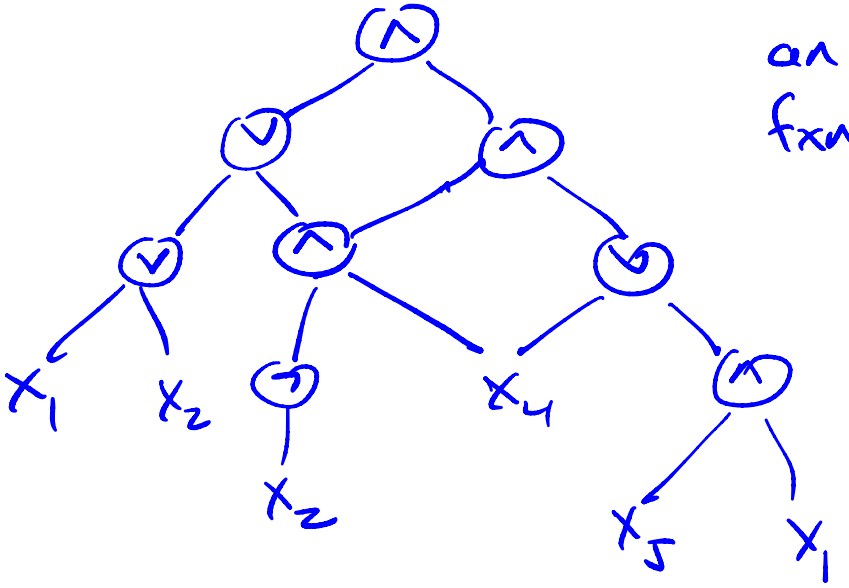
① Conjecture is true, assuming a believable complexity assumption:

Thm (IW) $\exists L \in E = DTIME(2^{O(n)})$ such that L requires circuits of size $2^{\Omega(n)} \Rightarrow P = BPP$

$\approx$ L requires time $2^{\Omega(n)}$

Circuit complexity (More later in course)

Circuit over $\wedge, \vee, \neg$:



← C computes ~~an~~ an associated fxn $f: \{0,1\}^n \to \{0,1\}$

Size = # of "gates" ($\wedge, \vee, \neg$'s in C)

Inputs: $x_1 \cdots$ ~~x_n~~

Say a language $L \subseteq \{0,1\}^*$

has polysize circuits if $\exists$

$C_0\ C_1\ C_2 \ldots$

s.t. ① $\forall n$ C_n is a Boolean circuit on

inputs $x_1 \ldots x_n$

and $\forall x \in \{0,1\}^n$ $C(x) = 1$ iff $x \in L$

② $\exists$ poly $p(n)$ s.t.

$\forall C_n$ $|C_n| = \text{poly}(n)$

"P/poly" is the class of languages L that can be recognized by a family $C = \{C_0, C_1, \ldots\}$ of poly size.

Lemma

If $L \in P$ then $L \in P/poly$

Conjecture $P = BPP$.

What's known

① Conjecture is true, assuming a believable complexity assumption:

Thm (IW) $\mathbf{E} \not\subseteq P/poly \Rightarrow P = BPP$

② Conversely, $P = BPP \Rightarrow$ circuit lower Bounds:

Thm (IKW): $P = BPP \Rightarrow$ Either ① Circuit LBs for permanent
or
② $NEXP \not\subseteq P/poly$

Thus resolving $P \stackrel{?}{=} BPP$ is essentially equivalent to proving circuit lower bounds for some $L \in NEXP$

How Powerful is Randomness ?

Second Open Question : $BPP \subseteq NP$?

What's known

1. If $P = BPP$ then $BPP \subseteq NP$.
2. Can we show $BPP \subseteq NP$ without assuming $P = BPP$?

Theorem $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

(so every $L \in BPP$ also lies in 2nd level of polytime hierarchy)

HW2, Test 2, Practice Probs

Problems using Additive + Multip Chernoff

RP, coRP, BPP, error ampl

Williams Time → Space

PSPACE, NL, coNL