Randomization in Algorithms

Complexity Viewpoint

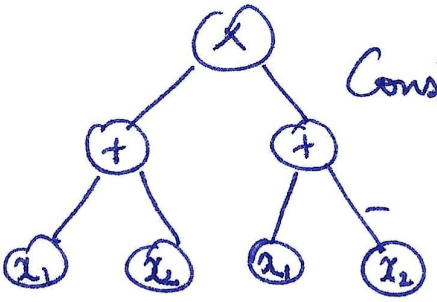
$$\prod_{i,j} (x_i - x_j)$$

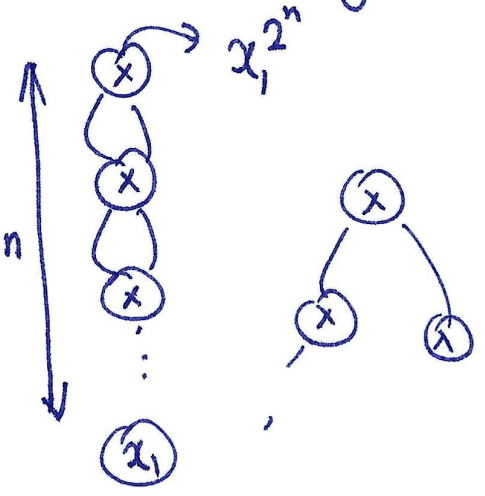
$$(x_1 - x_2)(x_1 + x_2) = x_1^2 - x_2^2$$ Polynomial Identity

Format $x^p \equiv x \pmod p$ (p is prime)

Polynomial Identity Testing

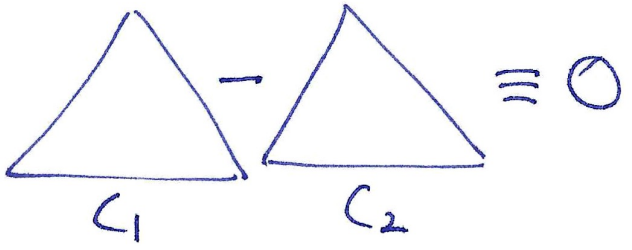
Polynomial as a circuit with $\oplus$ and $\otimes$ gates

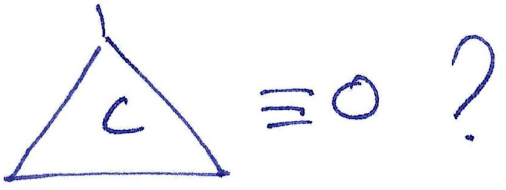




identically equal

Qn: Is $C_1 \equiv C_2$





Idea: Evaluate C at some points.

Thm [~~Schwartzstein~~ Schwartz – Zippel – DeMillo–Lipton 79]

Consider non-zero polynomial $p(x_1, \ldots, x_n)$ over $\mathbb{N}$, of total degree $\leq d$. Consider $S \subseteq \mathbb{N}$

$$\Pr_{\substack{s_i \in_R S \\ \text{independently}}} [\, p(s_1, \ldots, s_n) = 0 \,] \leq \frac{d}{|S|}$$

PIT(C):

(1) Determine upper bound d on degree of polynomial computed by C

(2) Pick $S = [1, 2d]$

(3) Evaluate C at uniform random integers from S

(4) If evaluation is zero, ACCEPT, else REJECT.

$$\mathcal{L} = \{ \langle C \rangle \mid C \equiv 0 \}$$

If $\langle C \rangle \in \mathcal{L}$, algorithm always accepts.

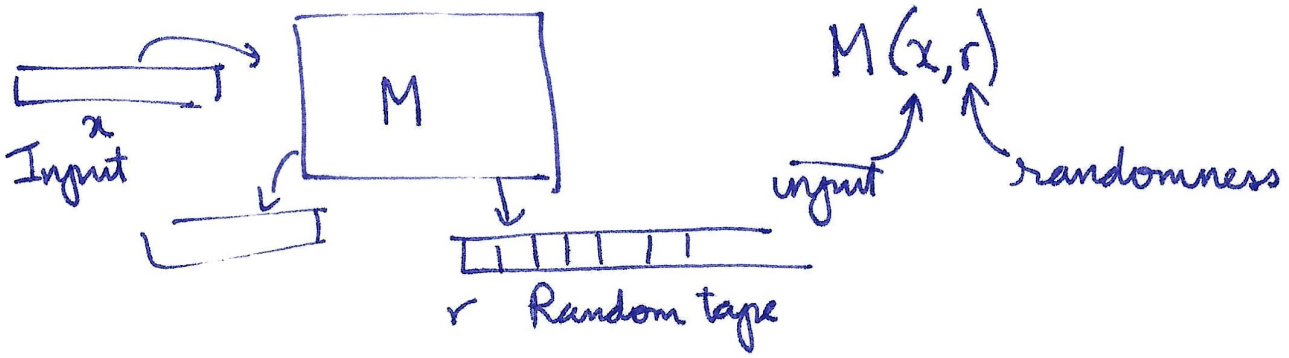
If $\langle C \rangle \notin \mathcal{L}$, algorithm accepts with prob. $\leq 1/2$

By repeating k times independently:

If $\langle C \rangle \notin \mathcal{L}$, algorithm accepts w.p. $\leq 1/2^k$ all runs

What is a probabilistic TM?

It has an extra "random" tape that contains uniform random bits



For input x : $\Pr_r[M(x,r) \text{ accepts}]$

Def: $\mathcal{L} \in BPTIME(t(n))$

↖ Bounded Polynomial

if $\exists$ a probabilistic TM M that runs in $t(n)$ time and satisfies the following:

$\forall\ x \in \{0,1\}^*$

Two-Sided Error

$$x \in \mathcal{L} \Rightarrow \Pr_{r \in \{0,1\}^{t(n)}}[M(x,r) \text{ accepts}] \geq 2/3$$

$$x \notin \mathcal{L} \Rightarrow \Pr_{r \in \{0,1\}^{t(n)}}[M(x,r) \text{ accepts}] \leq 1/3$$

↕ Gap

For all inputs, Prob of accepts $\geq 2/3$ or $\leq 1/3$

$$BPP = \bigcup_{c \in \mathbb{N}} BPTIME(n^c)$$

RP

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

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

↖ Cert. of acceptance

$RP \subseteq NP$

co-RP $\quad x \in L \Rightarrow - - = 1$

$x \notin L \Rightarrow - - \leq 1/3$ ← Certificate of rejection

$$P \subseteq RP \subseteq NP \cap co\text{-}RP \subseteq BPP \subseteq co\text{-}NP \subseteq PSPACE$$

ZPP "zero-error" probabilistic polynomial

$M(x,r)$ always outputs the correct answer.

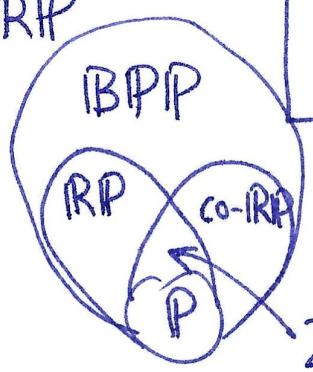
But its running time is unbounded.

Expected running time is polynomial

Thm: $ZPP = RP \cap co\text{-}RP$

[Nisan-Wigderson 90s]

If $NP \not\subseteq P/poly$, then $P = BPP$



The robustness of BPP wrt gap

$\mathcal{L} \in$ BPP

For convenience, $\mathcal{L}(x) = \begin{cases} 1 & x \in \mathcal{L} \\ 0 & x \notin \mathcal{L} \end{cases}$

BPP $\forall x: \Pr_r[M(x,r) = \mathcal{L}(x)] \geq 2/3 = 1/2 + \underbrace{\text{gap}}_{\varepsilon}$

BPP(gap) BPP(ε)

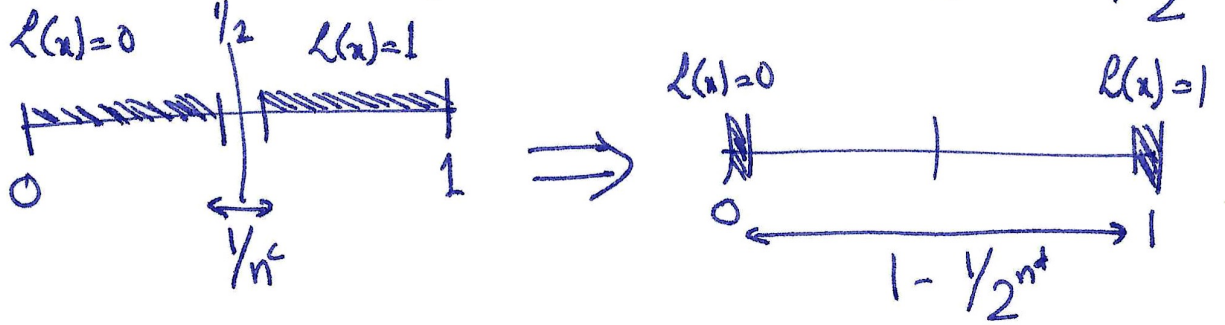
Our BPP is BPP(1/6)

Thm: [The Boosting Thm] Suppose M is a prob. poly time TM s.t. $\exists$ constant c

$\forall x \quad \Pr_r[M(x,r) = \mathcal{L}(x)] \geq 1/2 + 1/|x|^c$

Then $\forall d \in \mathbb{N}$, there is a prob poly time TM s.t.

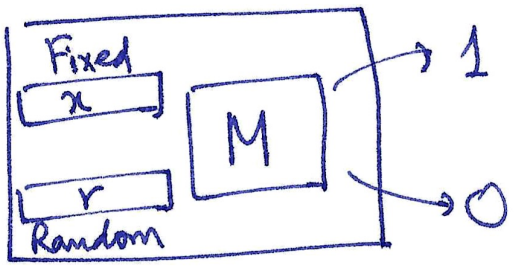
$\forall x \quad \Pr_r[M(x,r) = \mathcal{L}(x)] \geq 1 - 1/2^{|x|^d}$



Proof: Consider machine M' that runs k independent invocations of M, and outputs majority vote.

How large should k be so that

$\Pr$ [~~$M(x,r)$~~ the majority vote of these invocations = $\mathcal{L}(x)$] $\geq 1 - 1/2^{n^d}$?
over k invocations



If $x \in \mathcal{L}$, $\Pr[\text{seeing } 1] \geq \frac{1}{2} + \frac{1}{n^c}$

If $x \notin \mathcal{L}$, $\Pr[\text{seeing } 1] \leq \frac{1}{2} - \frac{1}{n^c}$

Pick uar r (uniform at random)

Expectation

If $x \in \mathcal{L}$, $\mathbb{E}[\#\text{accepts in } k \text{ runs}] \geq \frac{k}{2} + \frac{k}{n^c}$

$x \notin \mathcal{L}$, $\mathbb{E}[\#\text{accepts in } k \text{ runs}] \leq \frac{k}{2} - \frac{k}{n^c}$

[Chernoff - Hoeffding 50's] There is a random variable
Bernstein 30s

$X \in \{0,1\}$ $\Pr[X=1] = p$

$X_1, \ldots, X_k$ are iid as X

$\mathbb{E}\left[\sum_{i \leq k} X_i\right] = pk$

deviation

$\Pr\left[\left|\sum_{i \leq k} X_i - pk\right| \geq t\right] \leq 2\exp\left(\frac{-t^2}{2k}\right)$

$t = \varepsilon k$ $\qquad 2\exp\left(-\frac{\varepsilon^2 k^2}{2k}\right) = 2\exp\left(-\frac{\varepsilon^2 k}{2}\right)$

~~$p = 1/2$~~ $\qquad \varepsilon = 1/n^c \qquad \Pr\left[\#\text{accepts} > \frac{k}{2}\right]$

$p = \left(\frac{1}{2} + \frac{1}{n^c}\right)$

$x \in L$

~~$\leq \Pr$ $\Pr$~~

$$\Pr\left[\#\text{accepts} > \left(\tfrac{1}{2} + \tfrac{1}{n^c}\right)k - \frac{k}{n^c}\right]$$

$$= \Pr\left[\#\text{accepts} - \left(\tfrac{1}{2} + \tfrac{1}{n^c}\right)k > \frac{k}{n^c}\right]$$

Bound $\Pr\left[\#\text{accepts} \leq \frac{k}{2}\right]$

$$= \Pr\left[\#\text{accepts} \leq \left(\tfrac{1}{2} + \tfrac{1}{n^c}\right)k - \frac{k}{n^c}\right]$$

$$\leq \Pr\left[\left|\#\text{accepts} - \left(\tfrac{1}{2} + \tfrac{1}{n^c}\right)k\right| > \frac{k}{n^c}\right]$$

$$\leq 2\exp\left(-\frac{k}{2n^{2c}}\right) \qquad \varepsilon = \frac{1}{n^c} \quad \exp\left(-\varepsilon^2 \frac{k}{2}\right)$$

$k = n^{2c+d+1} \rightarrow \leq \exp(-n^d)$