Computational Complexity

Mohammad Mahmoody

Session 23
April 2014

Zero-Error Probabilistic Algorithms

- What if M is randomized and $M(x)$ is correct with prob. 1 ?

Definition 7.7 The class **ZTIME**$(T(n))$ contains all the languages L for which there is a machine M that runs in an expected-time $O(T(n))$ such that for every input x, whenever M halts on x, the output $M(x)$ it produces is exactly $L(x)$.

We define **ZPP** $= \cup_{c>0}$**ZTIME**(n^c). ◇

coRP $\supseteq \ldots \subseteq$ RP { if $x \in L \Rightarrow$ answer yes w.p. $\geq \frac{2}{3}$; if $x \notin L \Rightarrow$ ~ NO ~ = 1

ZPP $\subseteq$ BPP

We have M with zero err. let t_0 be s.t $E[\text{time}[M(x)]] < t_0$

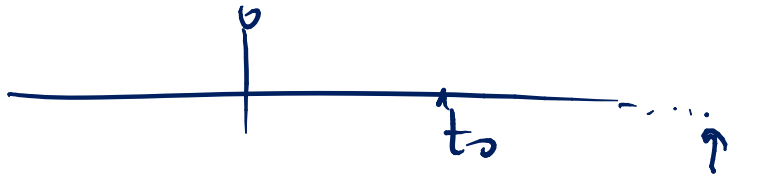
Lets run $M(x)$ for $10 t_0$ steps. { if finished in time $\Rightarrow$ output answer ; if not finished $\Rightarrow$ output random }

Markov Bound

Let T be a random variable.

$\forall\ t \leftarrow T \quad t \geq 0 \quad E[T] = t_0 \Rightarrow \Pr_{t \leftarrow T}[t \geq k t_0] \leq \frac{1}{k}$

example: { w.p $1 - \frac{1}{k}$ $T = 0$; w.p $\frac{1}{k}$ $T = t_0 \times k$ }



Proof: Assume that $\Pr[t \geq k t_0] = \alpha > \frac{1}{k}$

$\Rightarrow E[T] \geq \alpha \cdot k t_0 + (1-\alpha) \cdot 0 > \frac{1}{k} \cdot k t_0 = t_0$

$\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$

- Note $\mathbf{ZPP} \subseteq \mathbf{RP}$ implies $\mathbf{ZPP} = \mathbf{coZPP} \subseteq \mathbf{coRP}$
- So: $\mathbf{ZPP} \subseteq \mathbf{RP} \cap \mathbf{coRP}$
- Claim: $\mathbf{RP} \cap \mathbf{coRP} \subseteq \mathbf{ZPP}$

have $M_0 \in RP$ $M_1 \in coRP$. time to run $M_0/M_1 \leq t_0$

$M_0(x)$ { Yes → answer is Correct :)
No → ?

$M_1(x)$ { Yes → ?
No → sure!

M: $M_0(x)$ $M_1(x)$ $M_0(x)$ ...
ran ran ...
if yes if says Stop No Stop

Algorithm M: ① run $N_0(x)$: if says yes → stop
② run $N_1(x)$ —— N_0 → stop
③ { ⋮
④ { - - - - -

$$ZPP = RP \cap coRP$$

Suppose $x \in L$: we stop if $N_0(x)$ says yes. : $\frac{1}{2}$

Y is the output of $N_0(x)$ $\Pr[Y] = \begin{cases} 0 & : \frac{1}{2} \\ 1 & : \frac{1}{2} \end{cases}$ α

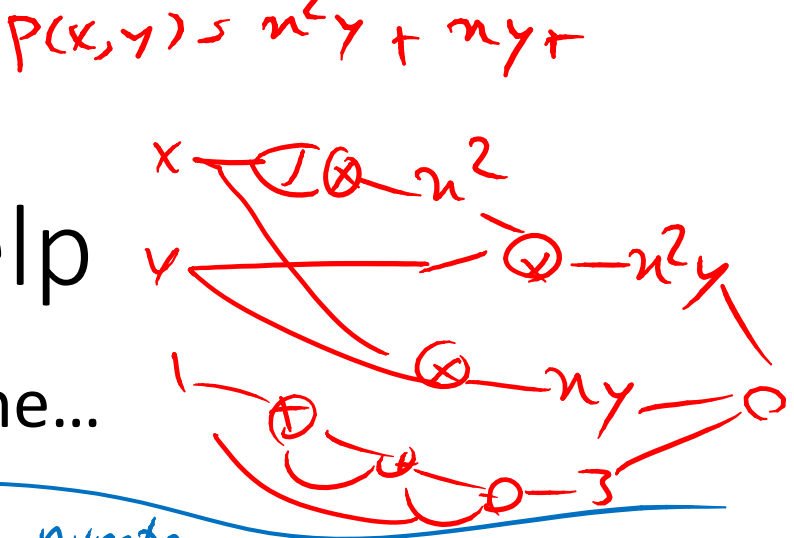
$y_1 \leftarrow Y$ $y_2 \leftarrow Y$ ... y_t ... till we get $y_t = 1$

$\Pr[\text{we go to } k \text{ steps}] = 2^{-k}$

$\mathbb{E}[\text{steps}] = 1 \cdot 2^{-1} + 2 \cdot 2^{-2} + \dots = 2$

$\mathbb{E}[\text{steps}] \le \frac{1}{\alpha}$

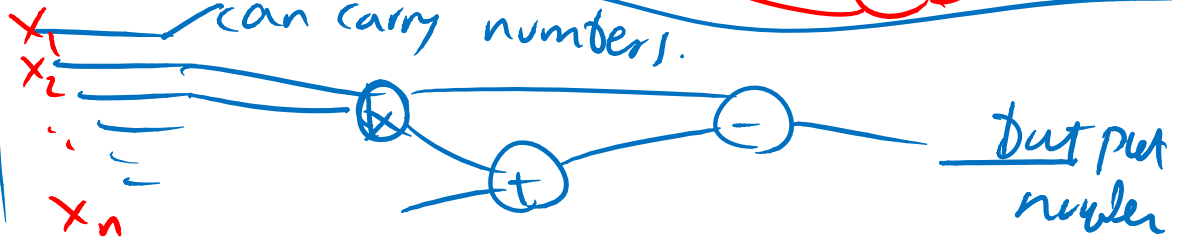
Polynomial Identity Testing: Where randomness seems to help



- Given a two polynomials, find if they are the same…

Boolean Circuit.

Algebraic circ



$\prod_{i=1}^{n}(1+x_i)$

given two circuits C_1 C_2 ; if $C_1(x) = C_2(x)$ for all x?