

Probabilistic Computation

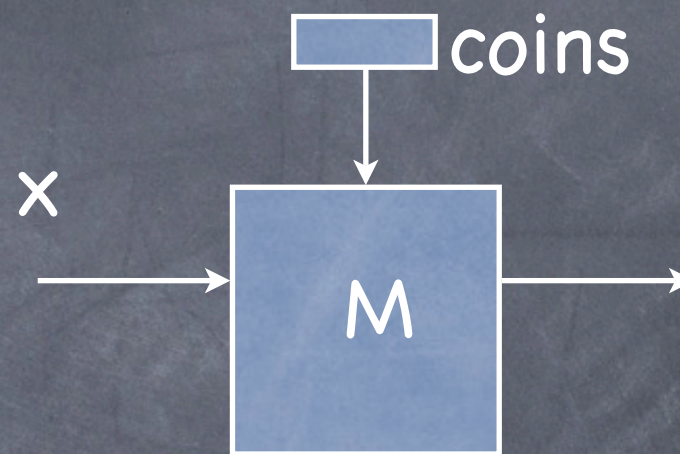
Lecture 12

Flipping coins, taking chances

PP, BPP

Probabilistic Computation

- Output depends not only on x , but also on random “coin flips”
- M, x define a probability distribution over outcomes
- If **for all x** , $M(x)$ equals $f(x)$ with very high probability, could be used as $f(x)$

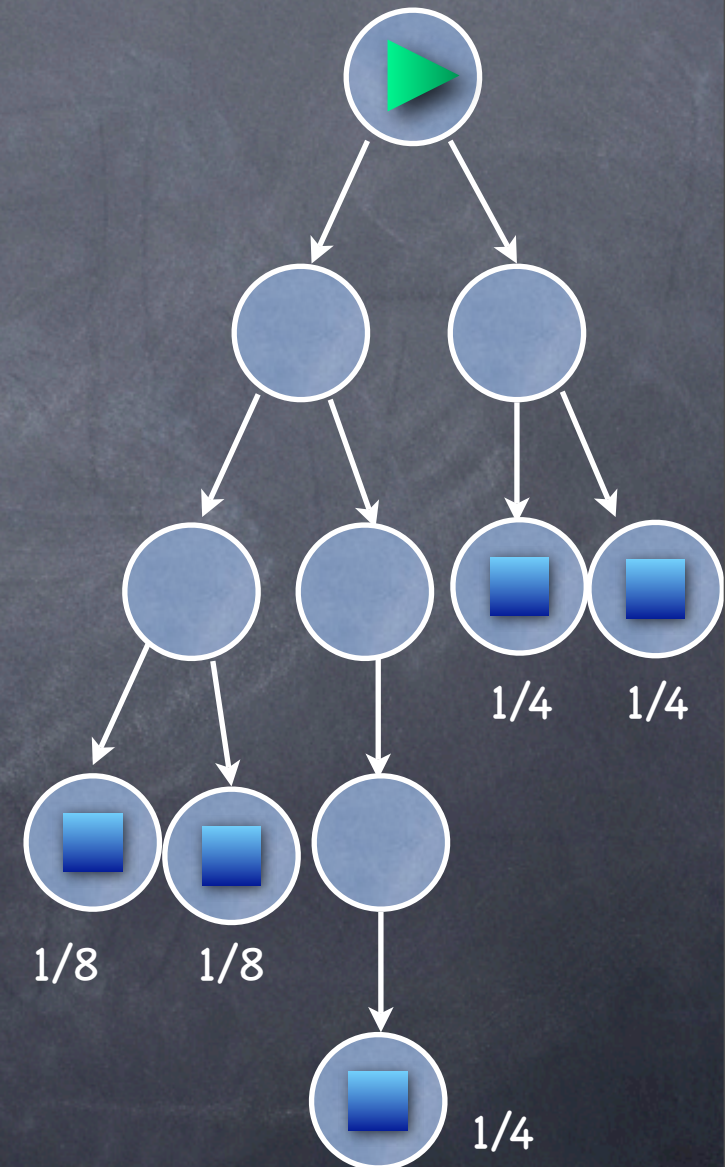


Language Decided by a Probabilistic Computation

- Different possible definitions of a prob. TM accepting input
 - M accepts x if $\text{pr}[M(x)=\text{yes}] > 0$; rejects if $\text{pr}[M(x)=\text{yes}] = 0$
 - M accepts x if $\text{pr}[M(x)=\text{yes}] > 1/2$; rejects if $\text{pr}[M(x)=\text{yes}] \leq 1/2$
 - M accepts x if $\text{pr}[M(x)=\text{yes}] > 2/3$; rejects if $\text{pr}[M(x)=\text{yes}] < 1/3$
 - M accepts x if $\text{pr}[M(x)=\text{yes}] > 2/3$; rejects if $\text{pr}[M(x)=\text{yes}] = 0$
 - Last two: If on any x neither, M doesn't decide a language!
 - When M does decide, much better than random guess

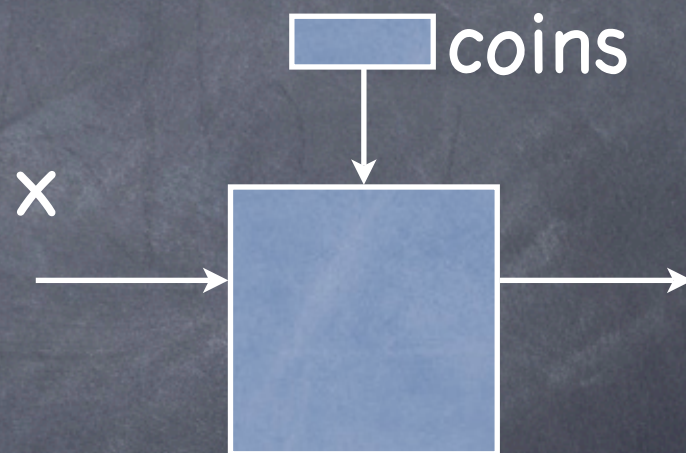
Probabilistic TM

- Like an NTM, but the two possible transitions are considered to be taken with equal probability
- Defines a probability with which an input is accepted or rejected



Random Tape

- Random choice: flipping a fair coin
 - Coin flip is written on a read-once "random tape"
 - Enough coin flips made and written on the tape first, then start execution
 - When considering bounded time TMs length of random tape (max coins used) also bounded



Random Tape

0	0	0
---	---	---

0	0	1
---	---	---

0	1
---	---

1	0
---	---

1	1
---	---

0	0	0
---	---	---

0	0	1
---	---	---

0	1	0
---	---	---

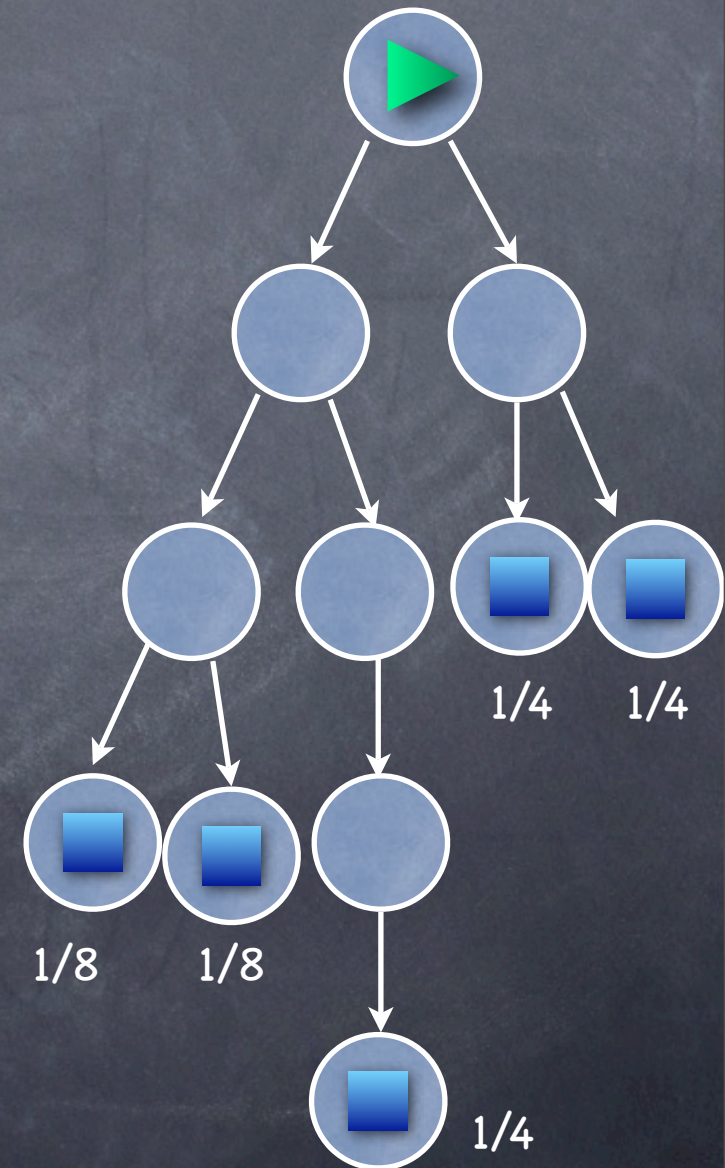
0	1	1
---	---	---

1	0	0
---	---	---

1	0	1
---	---	---

1	1	0
---	---	---

1	1	1
---	---	---



Language Decided by a Probabilistic Computation

- Different possible definitions of accepting input
 - Accept if $\text{pr}[\text{yes}] > 0$; reject if $\text{pr}[\text{yes}] = 0$ NTM
 - Accept if $\text{pr}[\text{yes}] > 1/2$; reject if $\text{pr}[\text{yes}] \leq 1/2$ PTM
 - Accept if $\text{pr}[\text{yes}] > 2/3$; reject if $\text{pr}[\text{yes}] < 1/3$ BPTM
 - Accept if $\text{pr}[\text{yes}] > 2/3$; reject if $\text{pr}[\text{yes}] = 0$ RTM
- (Not standard nomenclature!)

P_{TIME}, B_{PTIME} and R_{TIME}

- T-time probabilistic TM
 - On all inputs x , on any random tape, terminates in $T(|x|)$ time and outputs "yes" or "no."
 - Just like $\text{NTIME}(T)$
- $\text{BPTIME}(T)$ = class of languages decided by BPTMs in time T
 - Similarly $\text{P}_{\text{TIME}}(T)$ and $\text{R}_{\text{TIME}}(T)$

PP, BPP and RP

- $PP = \bigcup_{c>0} PTIME(O(n^c))$
- $BPP = \bigcup_{c>0} BPTIME(O(n^c))$
- $RP = \bigcup_{c>0} RTIME(O(n^c))$
- co-RP

co-RTM

- Accept if $\text{pr}[\text{yes}] > 0$; reject if $\text{pr}[\text{yes}] = 0$ NTM
 - Accept if $\text{pr}[\text{yes}] = 1$; reject if $\text{pr}[\text{yes}] < 1$ co-NTM
- Accept if $\text{pr}[\text{yes}] > 1/2$; reject if $\text{pr}[\text{yes}] \leq 1/2$ PTM
 - Accept if $\text{pr}[\text{yes}] \geq 1/2$; reject if $\text{pr}[\text{yes}] < 1/2$ co-PTM
- Accept if $\text{pr}[\text{yes}] > 2/3$; reject if $\text{pr}[\text{yes}] < 1/3$ BPTM
 - Accept if $\text{pr}[\text{yes}] > 2/3$; reject if $\text{pr}[\text{yes}] < 1/3$ co-BPTM
- Accept if $\text{pr}[\text{yes}] > 2/3$; reject if $\text{pr}[\text{yes}] = 0$ RTM
 - Accept if $\text{pr}[\text{yes}] = 1$; reject if $\text{pr}[\text{yes}] < 1/3$ co-RTM

RP and co-RP

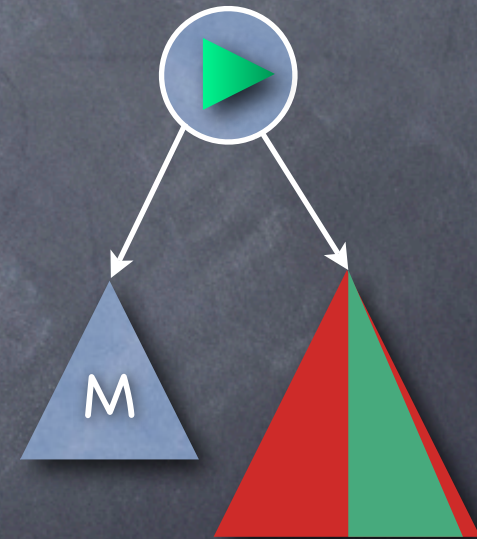
- One sided error ("bounded error" versions of NP and co-NP)
 - RP: if yes, may still say no w/p at most $1/3$
 - i.e., if RTM says no, can be wrong
 - co-RP: if no, may still say yes w/p at most $1/3$
 - i.e., if co-RTM says yes, can be wrong

co-BPP, co-PP

- $BPP = co-BPP$
 - co-BPTMs are same as BPTMs
- In fact $PP = co-PP$
 - PTMs and co-PTMs differ on accepting inputs with $\Pr[\text{yes}] = 1/2$
 - But can modify a PTM so that $\Pr[M(x)=\text{yes}] \neq 1/2$ for all x , without changing language accepted

PP = co-PP

- Modifying a PTM M to an equivalent PTM M' , so that for all x
 $\Pr[M'(x)=\text{yes}] \neq 1/2$
 - Consider $M'(x)$: w.p. $1/2$ run $M(x)$; w.p. $1/2$, ignore input and say yes w.p. $1/2 - \epsilon$, and say no w.p. $1/2 + \epsilon$
 - $\Pr[M'(x)=\text{yes}] = \Pr[M(x)=\text{yes}]/2 + (1/2 - \epsilon)/2$
 - If $\Pr[M(x)=\text{yes}] > 1/2 \Rightarrow \Pr[M(x)=\text{yes}] > 1/2 + \epsilon$
then M and M' equivalent
 - What is such an ϵ ?
 - $2^{-(m+1)}$ where no. of coins used by M is at most m
 - M' tosses at most $m+2$ coins



Bounding Probability Gap

- Gap

- $\min_{x \in L} \Pr[M(x)=\text{yes}] - \max_{x \notin L} \Pr[M(x)=\text{yes}]$
- BPP, RP, coRP require M to have gap some constant $(1/3, 2/3)$
- Setting gap = $1/n^c$ is enough
 - Can be boosted to gap = $1 - 1/2^{n^d}$ in polynomial time

Soundness Amplification for RP

- $M'(x)$: Repeat $M(x)$ t times and if any yes, say yes
 - If $x \notin L$: $\Pr[M(x)=\text{no}] = 1$. So $\Pr[M'(x)=\text{no}] = 1$
 - If $x \in L$: $\Pr[M(x)=\text{no}] \leq 1-\delta$ (when gap = δ). Then $\Pr[M'(x)=\text{no}] \leq (1-\delta)^t$
 - With $t = n^d/\delta$, $\Pr[M'(x)=\text{no}] < e^{-(n^d/\delta)}$ ($1-\delta < e^{-\delta}$)
 - For $\delta = n^{-c}$, $t = n^{d+c}$ is polynomial

Soundness Amplification for BPP

- Repeat $M(x)$ t times and **take majority**
 - i.e. estimate $\Pr[M(x)=\text{yes}]$ and check if it is $> 1/2$
 - Error only if $|\text{estimate} - \text{real}| \geq \text{gap}/2$
 - Estimation error goes down exponentially with t : Chernoff bound
 - $\Pr[|\text{estimate} - \text{real}| \geq \delta/2] \leq 2^{-\Omega(t \cdot \delta^2)}$
 - $t = O(n^d/\delta^2)$ enough for $\Pr[\text{error}] \leq 2^{-n^d}$

Today

- Probabilistic computation
- PP, RP, co-RP, BPP
 - PP too powerful: $NP \subseteq PP$
 - Constant gap: BPP, RP, co-RP
 - RP, co-RP one-sided error
 - Soundness Amplification: for RP, for BPP
 - From gap $1/\text{poly}$ to $1-1/\text{exp}$
- Next: more on BPP and relatives