gic <i>mputational</i>	Outline
Complexity Theory Georg Moser Institute of Computer Science @ UIBK Summer 2008	 Summary of Last Lecture: Probabilistic Turing Machines Project Assignment Probabilistic Turing Machines (Proof)
Summary of Last Lecture	GM (Institute of Computer Science @ UIBK) Complexity Theory 8/14 Summary of Last Lecture
 Probabilistic Turing Machines Definition a probabilistic Turing machine <i>M</i> is a TM and ∃ extra read-only tape containing random bits random bits may be consulted to decide on the next step outcome <i>M</i>(<i>x</i>, <i>y</i>) for input <i>x</i> and random bits <i>y</i> <i>M</i> is <i>T</i>(<i>n</i>) time bounded if ∀ input <i>x</i> it runs in <i>T</i>(<i>n</i>) steps is <i>S</i>(<i>n</i>) space bounded if ∀ input <i>x</i> it needs <i>S</i>(<i>n</i>) space for any random bits <i>y</i> probability of accept for <i>T</i>(<i>n</i>) time bounded <i>M</i>: 	DefinitionRPa set A is in RP if \exists probabilitic TM M with polytime bound n^c such that1 if $x \in A$, then $\Pr_y(M(x, y) accepts) \ge \frac{3}{4}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) accepts) = 0$ Fact $P \subseteq RP \subseteq NP$ DefinitionBPPa set A is in BPP if \exists probabilitic TM M with polytime bound n^c such that1 if $x \in A$, then $\Pr_y(M(x, y) accepts) \ge \frac{3}{4}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) accepts) \ge \frac{3}{4}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) accepts) \le \frac{1}{4}$
$\Pr_{y}(M(x,y) \text{ accepts}) = \frac{ \{y \in \{0,1\}^{k} \mid M(x,y) \text{ accepts}\} }{2^{k}}$ for $k \ge T(x)$ GM (Institute of Computer Science @ UIBK)	Fact $RP \subseteq BPP$ and BPP is closed under complement GM (Institute of Computer Science @ UIBK) Complexity Theory 10/14

HomeworkAmplification• Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC.Lemma if $A \in RP$, then Y polynomials n^d B probabilistic polytime TM M such that on input x $(n = x)$: if $x \in A$, then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $A \in BPP$, then \forall polynomials n^d B probabilistic polytime TM M such that on input x $(n = x)$: if $x \in A$, then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $A \in BPP$, then \forall polynomials n^d BPP $\subseteq \Sigma_2^0 \cap \Pi_2^0$ Corollary let $A \in BPP$ • if $x \in A$, then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ • if $x \in A$, then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n^d}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then $Pr_y(M(x, y)$ accepts) $\geq 1 - 2^{-n}$ if $x \in A$ then Pr_y	Homework	Amplification
• Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC. • Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC. • Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC. • If $A \in BP$, then V polynomials n^d $\exists r A \in BP$, then V polynomials n^d $\exists r A \in BP$, then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. Then V polynomials n^d $\exists r A \in BP$. The V polynomials n^d $\exists r A \in BP$. The V polynomials n^d $\exists r A \in BP$. The V polynomials n^d $\exists r A \in BP$. The V polynomials n^d $\exists r A \in BP$. The V polynomials n^d $\forall r A = A \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\exists f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \geq 1 - 2^{-n^d}$ $\forall f X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \equiv 1 - 2^{-n^d}$ $f x \notin X \notin A, \text{ then } Pr_r(M(x, y) \text{ accepts}) \equiv 1 - 2^{-n$	Homework	Amplification
Condition of Complexity Science 0 UBNComplexity Theory12/14Complexity Complexity Theory12/14UPE < 2 < 1 < 12UPE < 2 < 1 < < 12UPE < 2 < 12UPE <	• Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC.	Lemma if $A \in \text{RP}$, then \forall polynomials n^d \exists probabilistic polytime TM M such that on input x $(n = x)$: 1 if $x \in A$, then $\Pr_y(M(x, y) \text{ accepts}) \ge 1 - 2^{-n^d}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) \text{ accepts}) = 0$ Lemma if $A \in \text{BPP}$, then \forall polynomials n^d \exists probabilistic polytime TM M such that on input x $(n = x)$: 1 if $x \in A$, then $\Pr_y(M(x, y) \text{ accepts}) \ge 1 - 2^{-n^d}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) \text{ accepts}) \ge 1 - 2^{-n^d}$ 2 if $x \notin A$, then $\Pr_y(M(x, y) \text{ accepts}) \le 2^{-n^d}$ Theorem $\text{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$
$\begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} $	GM (Institute of Computer Science @ UIBK) Complexity Theory 11/14	GM (Institute of Computer Science @ UIBK) Complexity Theory 12/14
$\begin{array}{l} BPP \subseteq \sum_{j=1}^{p} \cap \prod_{j=2}^{p} \\ Corollary \\ let A \in BPP \\ \bullet \exists probabilistic polytime TM M running in time n^c such that \\ \bullet \forall inputs x \\ \bullet if x \in A, then Pr_y(M(x,y) accepts) \geqslant 1 - 2^{-n} \\ \bullet if x \notin A, then Pr_y(M(x,y) accepts) \geqslant 2^{-n} \\ Definition \\ fix input x and let m = n^c \\ A_x = \{y \in \{0,1\}^m \mid M(x,y) accepts\} \\ R_x = \{y \in \{0,1\}^m \mid M(x,y) rejects\} = \{0,1\}^m - A_x \\ Fact \\ for x \in A \\ for x \notin A \\ IA_x \mid \ge 2^m - 2^{m-n} and \mid R_x \mid \le 2^{m-n} \\ for tat \\ IA_x \mid \ge 2^m - 2^{m-n} and \mid R_x \mid \le 2^{m-n} \\ for tat \\ IA_x \mid \ge 2^m - 2^{m-n} and \mid A_x \mid \le 2^{m-n} \end{array}$	$BPP \subseteq \Sigma_2^{p} \cap \Pi_2^{p}$	$BPP \subseteq \Sigma_2^{P} \cap \Pi_2^{P}$
$ R_{x} \ge 2''' - 2''''' \text{ and } A_{x} \le 2'''''$	$\begin{array}{l} BPP \subseteq \Sigma_2^p \cap \Pi_2^p \\ \begin{array}{l} Corollary \\ let \ A \in BPP \\ \bullet \exists \ probabilistic \ polytime \ TM \ M \ running \ in \ time \ n^c \ such \ that \\ \bullet \ \forall \ inputs \ x \\ \bullet \ if \ x \in A, \ then \ Pr_y(M(x, y) \ accepts) \geqslant 1 - 2^{-n} \\ \bullet \ if \ x \notin A, \ then \ Pr_y(M(x, y) \ accepts) \leqslant 2^{-n} \end{array}$ $\begin{array}{l} Definition \\ fix \ input \ x \ and \ let \ m = n^c \\ A_x = \{y \in \{0,1\}^m \mid M(x, y) \ accepts\} \\ R_x = \{y \in \{0,1\}^m \mid M(x, y) \ rejects\} = \{0,1\}^m - A_x \end{aligned}$ $\begin{array}{l} Fact \\ for \ x \in A \\ \qquad \qquad$	Claim $x \in A$ if and only if $\exists z_1,, z_m (z_i = m)$ such that $\{y \oplus z_j \mid 1 \leq j \leq m, y \in A_x\} = \{0, 1\}^m$ (\oplus is bitwise sum mod 2) Proof (of BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$) we only need to show BPP $\subseteq \Sigma_2^p$ as coBPP = BPP let $A \in BPP$, we show $A \in \Sigma_2^p$: 1 guess $z_1,, z_m$ 2 generate all w of length m 3 check $w \in \{y \oplus z_j \mid 1 \leq j \leq m, y \in A_x\}$ for that • test $\{w \oplus z_j \mid 1 \leq j \leq m\} \cap A_x \neq \emptyset$ • by running $M(x, w \oplus z_j)$ for all j
	$ \mathcal{K}_{X} \ge 2^{m} - 2^{m} \text{and} \mathcal{A}_{X} \le 2^{m} m$	CM (Institute of Computer Science @ IIIRK) Complexity Theory 14/14