Computational Complexity Theory

Lecture 22: Sipser-Gacs-Lautemann theorem; Classes RP and ZPP

Department of Computer Science,
Indian Institute of Science

Recap: Probabilistic Turing Machines

- Definition. A *probabilistic Turing machine* (PTM) M has two transition functions δ_0 and δ_1. At each step of computation on input $x \in \{0,1\}^*$, M applies one of δ_0 and δ_1 uniformly at random (independent of the previous steps). M outputs either 1 (accept) or 0 (reject). M runs in $T(n)$ time if M always halts within $T(|x|)$ steps *regardless of its random choices*.

- Note. PTMs and NTMs are syntatically similar – both have two transition functions. But, semantically, they are quite different

Recap: Probabilistic Turing Machines

- Definition. A *probabilistic Turing machine* (PTM) M has <u>two</u> transition functions δ_0 and δ_1. At each step of computation on input $x \in \{0,1\}^*$, M applies one of δ_0 and δ_1 uniformly at random (independent of the previous steps). M outputs either 1 (accept) or 0 (reject). M runs in $T(n)$ time if M always halts within $T(|x|)$ steps *regardless of its random choices*.

- Note. The above definition allows a PTM M to <u>not</u> halt on some computation paths defined by its random choices (unless we explicitly say that M runs in $T(n)$ time). More on this later when we define ZPP.

Recap: Class BPP

- **Definition.** A PTM M *decides* a language L in time $T(n)$ if M runs in $T(n)$ time, and for every $x \in \{0,1\}^*$,

$$\underbrace{\Pr[M(x) = L(x)]}_{\text{Success probability}} \geq 2/3.$$

- **Definition.** A language L is in $\mathrm{BPTIME}(T(n))$ if there's PTM that decides L in $O(T(n))$ time.

- **Definition.** $\mathrm{BPP} = \bigcup_{c > 0} \mathrm{BPTIME}(n^c)$.

- Clearly, $\mathrm{P} \subseteq \mathrm{BPP}$.

Recap: Class BPP

- Definition. A PTM M *decides* a language L in time $T(n)$ if M runs in $T(n)$ time, and for every $x \in \{0,1\}^*$,
$$\Pr[M(x) = L(x)] \geq 2/3.$$

- Definition. A language L is in $\mathrm{BPTIME}(T(n))$ if there's PTM that decides L in $O(T(n))$ time.

- Definition. $\mathrm{BPP} = \bigcup_{c>0} \mathrm{BPTIME}(n^c)$.

  Bounded-error **P**robabilistic **P**olynomial-time

- Clearly, $P \subseteq \mathrm{BPP}$.

Remark. The defn of class BPP is robust. The class remains unaltered if we replace 2/3 by any constant ***strictly greater*** than (i.e., ***bounded away*** from) ½. We'll discuss this next.

Recap: Error reduction for BPP

- Lemma. Let $c > 0$ be a constant. Suppose L is decided by a poly-time PTM M s.t. $\Pr[M(x) = L(x)] \geq ½ + |x|^{-c}$. Then, for every constant $d > 0$, L is decided by a poly-time PTM M' s.t. $\Pr[M'(x) = L(x)] \geq 1 - \exp(-|x|^d)$.

Recap: Alternative definition of BPP

- Definition. A language L in BPP if there's a poly-time DTM $M(.\ ,\ .)$ and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 2/3.$$

- $2/3$ can be replaced by $1 - \exp(-|x|^d)$ as before.

Recap: Alternative definition of BPP

- Definition. A language L in BPP if there's a poly-time DTM $M(.\,,\,.)$ and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 2/3.$$

- Hence, $P \subseteq BPP \subseteq EXP$.
- Sipser-Gacs-Lautemann. $BPP \subseteq \Sigma_2$. (We'll prove this)
- How large is BPP? Is $NP \subseteq BPP$? i.e., is $SAT \in BPP$?
- Theorem. (*Adleman 1978*) $BPP \subseteq P/poly$.
- So, if $NP \subseteq BPP$ then $PH = \Sigma_2$. (*Karp-Lipton*)

Recap: Alternative definition of BPP

- Definition. A language L in BPP if there's a poly-time DTM $M(. , .)$ and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 2/3.$$

- Hence, $P \subseteq BPP \subseteq EXP$.
- Sipser-Gacs-Lautemann. $BPP \subseteq \Sigma_2$. (We'll prove this)

- Most complexity theorist believe that $P = BPP$! (More on this later.)

Sipser-Gacs-Lautemann theorem

BPP is in PH

- We saw that $P \subseteq BPP \subseteq EXP$. But, is $BPP \subseteq NP$? Not known! (Yes, people still believe BPP = P.)

- Sipser showed $BPP \subseteq PH$, Gacs strengthened it to $BPP \subseteq \Sigma_2 \cap \Pi_2$, Lautemann gave a simpler proof.

- Theorem. *(Sipser-Gacs-Lautemann '83)* $BPP \subseteq \Sigma_2 \cap \Pi_2$.

BPP is in PH

- We saw that $\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{EXP}$. But, is $\mathsf{BPP} \subseteq \mathsf{NP}$? Not known! (Yes, people still believe BPP = P.)

- Sipser showed $\mathsf{BPP} \subseteq \mathsf{PH}$, Gacs strengthened it to $\mathsf{BPP} \subseteq \Sigma_2 \cap \Pi_2$, Lautemann gave a simpler proof.

- Theorem. *(Sipser-Gacs-Lautemann '83)* $\mathsf{BPP} \subseteq \Sigma_2 \cap \Pi_2$.
- *Proof.* Observe that BPP = co-BPP *(homework)*. So, it is sufficient to show $\mathsf{BPP} \subseteq \Sigma_2$.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* Let $L \in$ BPP. Then, there's a poly-time <u>DTM</u> M and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

  $$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 1 - 2^{-|x|} .$$
- Let $n = |x|$ and $m = q(n)$.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* $BPP \subseteq \Sigma_2$.
- *Proof.* Let $L \in BPP$. Then, there's a poly-time <u>DTM</u> M and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 1 - 2^{-|x|} .$$

- Let $n = |x|$ and $m = q(n)$. Let $A_x \subseteq \{0,1\}^m$ such that $r \in A_x$ iff $M(x, r) = 1$. Observe that

$$x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* Let $L \in$ BPP. Then, there's a poly-time DTM M and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 1 - 2^{-|x|} .$$

- Let $n = |x|$ and $m = q(n)$. Let $A_x \subseteq \{0,1\}^m$ such that $r \in A_x$ iff $M(x, r) = 1$. Observe that

$$x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

- Idea. If A_x is large then there exists a "small" collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.

bit-wise Xor

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* Let $L \in$ BPP. Then, there's a poly-time DTM M and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 1 - 2^{-|x|} .$$

- Let $n = |x|$ and $m = q(n)$. Let $A_x \subseteq \{0,1\}^m$ such that $r \in A_x$ iff $M(x, r) = 1$. Observe that

$$x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

- Idea. If A_x is large then there exists a "small" collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$. No such collection exists if $|A_x|$ is small.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* Let $L \in$ BPP. Then, there's a poly-time DTM M and a polynomial function $q(.)$ s.t. for every $x \in \{0,1\}^*$,

$$\Pr_{r \in_R \{0,1\}^{q(|x|)}} [M(x, r) = L(x)] \geq 1 - 2^{-|x|} .$$

- Let $n = |x|$ and $m = q(n)$. Let $A_x \subseteq \{0,1\}^m$ such that $r \in A_x$ iff $M(x, r) = 1$. Observe that

$$x \in L \;\Rightarrow\; |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \;\Rightarrow\; |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

- Idea. If A_x is large then there exists a "small" collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$. Capture this property with a Σ_2 statement.

BPP is in PH

- **Theorem.** *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Then

$$x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

- Set $\boxed{k = m/n + 1}$.
- **Obs.** If $|A_x| \leq 2^{-n}.2^m$ then for *every* collection $u_1, \ldots, u_k \in \{0,1\}^m$, $\bigcup_{i\in[k]} (A_x \oplus u_i) \subsetneq \{0,1\}^m$.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Then

  $x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m$ (A_x is large)

  $x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m$ (A_x is small).
- Set $k = m/n + 1$.
- Obs. If $|A_x| \leq 2^{-n}.2^m$ then for *every* collection $u_1, \ldots, u_k \in \{0,1\}^m$, $\bigcup_{i\in[k]} (A_x \oplus u_i) \subsetneq \{0,1\}^m$.
- *Proof.* As $|A_x| \leq 2^{-n}.2^m$, $|\bigcup_{i\in[k]} (A_x \oplus u_i)| \leq k.2^{m-n} < 2^m$ for sufficiently large n.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* $\mathrm{BPP} \subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Then

  $x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m$ (A_x is large)

  $x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m$ (A_x is small).
- Set $k = m/n + 1$.
- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there <u>*exists*</u> a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.

- Let us complete the proof of the theorem assuming the claim – we'll proof it shortly.

BPP is in PH

- **Theorem.** *(Sipser-Gacs-Lautemann '83)* $\mathrm{BPP} \subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Then

$$x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m \quad (A_x \text{ is large})$$

$$x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m \quad (A_x \text{ is small}).$$

- Set $k = m/n + 1$.
- **Claim.** If $|A_x| \geq (1 - 2^{-n}).2^m$ then there *exists* a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- The observation and the claim imply the following:

$$x \in L \Rightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$$

$$x \notin L \Rightarrow \forall u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i\in[k]} (A_x \oplus u_i) \subsetneq \{0,1\}^m.$$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* $\text{BPP} \subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Then

  $x \in L \Rightarrow |A_x| \geq (1 - 2^{-n}).2^m$ (A_x is large)

  $x \notin L \Rightarrow |A_x| \leq 2^{-n}.2^m$ (A_x is small).
- Set $k = m/n + 1$.
- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there *exists* a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.
- The observation and the claim imply the following:

  $$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m.$$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* $BPP \subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Set $k = m/n + 1$.

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* $\mathrm{BPP} \subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Set $k = m/n + 1$.

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \quad r \in \bigcup_{i \in [k]} (A_x \oplus u_i)$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $r \in A_x$ iff $M(x, r) = 1$. Set $k = m/n + 1$.

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$$

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \;\; r \in \bigcup_{i \in [k]} (A_x \oplus u_i)$$

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \;\; \bigvee_{i \in [k]} [r \oplus u_i \in A_x]$$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $\boxed{r \in A_x \text{ iff } M(x, r) = 1.}$ Set $k = m/n + 1$.

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \;\; r \in \bigcup_{i\in[k]} (A_x \oplus u_i)$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \;\; \bigvee_{i\in[k]} [r \oplus u_i \in A_x]$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \;\; \bigvee_{i\in[k]} M(x, r \oplus u_i) = 1$

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $\boxed{r \in A_x \text{ iff } M(x, r) = 1.}$ Set $k = m/n + 1$.

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$$

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m\ \forall r \in \{0,1\}^m \quad r \in \bigcup_{i\in[k]} (A_x \oplus u_i)$$

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m\ \forall r \in \{0,1\}^m \quad \bigvee_{i\in[k]} [r \oplus u_i \in A_x]$$

$$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m\ \forall r \in \{0,1\}^m \quad \bigvee_{i\in[k]} M(x, r \oplus u_i) = 1$$

- Think of a DTM N that takes input $x, u_1, \ldots, u_m, r$, and outputs 1 iff $M(x, r\oplus u_i) = 1$ for some $i \in [k]$. Observe that N is a poly-time DTM.

BPP is in PH

- Theorem. *(Sipser-Gacs-Lautemann '83)* BPP $\subseteq \Sigma_2$.
- *Proof.* $\boxed{r \in A_x \text{ iff } M(x, r) = 1.}$ Set $k = m/n + 1$.

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \quad r \in \bigcup_{i \in [k]} (A_x \oplus u_i)$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \quad \bigvee_{i \in [k]} [r \oplus u_i \in A_x]$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \; \forall r \in \{0,1\}^m \quad N(x, \underline{\mathbf{u}}, r) = 1.$

$\underline{\mathbf{u}} = \{u_1, \ldots, u_k\}$

- Therefore, $L \in \Sigma_2$.

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there *exists* a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* The proof of this uses the probabilistic method.

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there *exists* a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

$$\Pr_{\underline{\mathbf{u}}} [\forall r \in \{0,1\}^m \;\; r \in \bigcup_{i\in[k]} (A_x \oplus u_i)] > 0 .$$

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

$$\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \;\; r \notin \bigcup_{i\in[k]} (A_x \oplus u_i)] < 1 .$$

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there <u>*exists*</u> a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

$$\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \;\; r \notin (A_x \oplus u_i) \text{ for every } i \in [k]] < 1 .$$

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

$$\Pr_{\mathbf{u}} [\exists r \in \{0,1\}^m \;\; r \oplus u_i \notin A_x \text{ for every } i \in [k]] < 1 .$$

Proof of the Claim

- Claim. If $\boxed{|A_x| \geq (1 - 2^{-n}).2^m}$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

  $$\Pr_{\underline{u}}[\exists r \in \{0,1\}^m \;\; r \oplus u_i \notin A_x \text{ for every } i \in [k]] < 1 .$$
- Fix an $r \in \{0,1\}^m$ (we'll apply a union bound later). Fix an $i \in [k]$. Then, $\Pr_{\underline{u}}[\underbrace{r \oplus u_i}_{} \notin A_x] \leq 2^{-n}$.

Distributed uniformly inside $\{0,1\}^m$
as r is fixed and u_i is picked
uniformly at random from $\{0,1\}^m$.

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there <u>*exists*</u> a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

  $\Pr_{\underline{\mathbf{u}}} [\exists r\in\{0,1\}^m \;\; r \oplus u_i \notin A_x$ for every $i\in [k]] < 1$.
- Fix an $r\in\{0,1\}^m$ (we'll apply a union bound later). Fix an $i\in [k]$. Then, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x] \leq 2^{-n}$. As $u_1, \ldots, u_k$ are independent, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x$ for every $i\in [k]] \leq 2^{-kn}$.

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i\in[k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

  $\Pr_{\underline{u}} [\exists r \in \{0,1\}^m \ \ r \oplus u_i \notin A_x$ for every $i \in [k]] < 1$.
- Fix an $r \in \{0,1\}^m$ (we'll apply a union bound later). Fix an $i \in [k]$. Then, $\Pr_{\underline{u}} [r \oplus u_i \notin A_x] \leq 2^{-n}$. As $u_1, \ldots, u_k$ are independent, $\Pr_{\underline{u}} [r \oplus u_i \notin A_x$ for every $i \in [k]] < 2^{-m}$.

$\boxed{k = m/n + 1}$

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

  $\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \ \ r \oplus u_i \notin A_x$ for every $i \in [k]] < 1$.
- Fix an $r \in \{0,1\}^m$ (we'll apply a union bound later). Fix an $i \in [k]$. Then, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x] \leq 2^{-n}$. As $u_1, \ldots, u_k$ are independent, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x$ for every $i \in [k]] < 2^{-m}$.
- Applying union bound,

  $\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \ \ r \oplus u_i \notin A_x$ for every $i \in [k]] < 2^m 2^{-m}$

Proof of the Claim

- Claim. If $|A_x| \geq (1 - 2^{-n}).2^m$ then there ***exists*** a collection $u_1, \ldots, u_k \in \{0,1\}^m$ s.t. $\bigcup_{i \in [k]} (A_x \oplus u_i) = \{0,1\}^m$.
- *Proof.* We'll show if $u_1, \ldots, u_k$ are picked independently and uniformly at random then

  $\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \;\; r \oplus u_i \notin A_x$ for every $i \in [k]] < 1$.
- Fix an $r \in \{0,1\}^m$ (we'll apply a union bound later). Fix an $i \in [k]$. Then, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x] \leq 2^{-n}$. As $u_1, \ldots, u_k$ are independent, $\Pr_{\underline{\mathbf{u}}} [r \oplus u_i \notin A_x$ for every $i \in [k]] < 2^{-m}$.
- Applying union bound,

  $\Pr_{\underline{\mathbf{u}}} [\exists r \in \{0,1\}^m \;\; r \oplus u_i \notin A_x$ for every $i \in [k]] < 1$.

Complete derandomization of BPP ?

- Can the Sipser-Gacs-Lautemann theorem be strengthened? How low in the PH does BPP lie ?

- Theorem. *(Nisan & Wigderson 1988,…, Umans 2003)* If there's a $L \in \mathrm{DTIME}(2^{O(n)})$ and a constant $\varepsilon > 0$ such that any circuit C_n that decides $L \cap \{0,1\}^n$ requires size $2^{\varepsilon n}$, then $\mathrm{BPP} = \mathrm{P}$.

- Lower bounds $\Rightarrow$ Derandomization !

Complete derandomization of BPP ?

- Can the Sipser-Gacs-Lautemann theorem be strengthened? How low in the PH does BPP lie ?

- Theorem. *(Nisan & Wigderson 1988,…, Umans 2003)* If there's a $L \in \mathrm{DTIME}(2^{O(n)})$ and a constant $\varepsilon > 0$ such that any circuit C_n that decides $L \cap \{0,1\}^n$ requires size $2^{\varepsilon n}$, then $\mathrm{BPP} = \mathrm{P}$.

- Lower bounds ⇒ Derandomization !
- Caution: Shouldn't interpret this result as "randomness is useless".

Classes RP, co-RP and ZPP

Class RP

- Class RP is the <u>one-sided error</u> version of BPP.

- Definition. A language L is in RTIME(T(n)) if there's a PTM M that decides L in O(T(n)) time such that

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq 2/3$$

$$x \notin L \Rightarrow \Pr[M(x) = 0] = 1.$$

- Definition. $RP = \bigcup_{c>0} RTIME(n^c)$.

- Clearly, $RP \subseteq BPP$.

Class RP

- Class RP is the one-sided error version of BPP.

- Definition. A language L is in RTIME(T(n)) if there's a PTM M that decides L in O(T(n)) time such that

$$x \in L \quad \Rightarrow \quad \Pr[M(x) = 1] \geq 2/3$$
$$x \notin L \quad \Rightarrow \quad \Pr[M(x) = 0] = 1.$$

Remark. The defn of class RP is robust. The class remains unaltered if we replace 2/3 by $|x|^{-c}$ for any constant $c > 0$. The succ. prob. can then be amplified to $1\text{-}\exp(-|x|^d)$.

(Easy Homework)

- Definition. $RP = \bigcup_{c > 0} RTIME(n^c)$.

Randomized **P**oly-time.

- Clearly, $RP \subseteq BPP$.

Class RP

- Class RP is the <u>one-sided error</u> version of BPP.

- Definition. A language L is in $\mathrm{RTIME}(T(n))$ if there's a PTM M that decides L in $O(T(n))$ time such that

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq 2/3$$
$$x \notin L \Rightarrow \Pr[M(x) = 0] = 1.$$

- Definition. $\mathrm{RP} = \bigcup_{c>0} \mathrm{RTIME}(n^c)$.

- Clearly, $\mathrm{RP} \subseteq \mathrm{BPP}$. Obs. $\mathrm{RP} \subseteq \mathrm{NP}$. *(Easy Homework)*

Recall, we don't know whether $\mathrm{BPP} \subseteq \mathrm{NP}$.

Class co-RP

- Definition. co-RP = $\{L : \overline{L} \in \text{RP}\}$.

- Obs. A language L is in co-RP if there's a PTM M that decides L in poly-time such that

$$x \in L \;\Rightarrow\; \Pr[M(x) = 1] = 1$$
$$x \notin L \;\Rightarrow\; \Pr[M(x) = 0] \geq 2/3.$$

- Obs. co-RP $\subseteq$ BPP .

Class co-RP

- Definition. co-RP $= \{L : \overline{L} \in$ RP$\}$.

- Obs. A language L is in co-RP if there's a PTM M that decides L in poly-time such that

$$x \in L \Rightarrow \Pr[M(x) = 1] = 1$$
$$x \notin L \Rightarrow \Pr[M(x) = 0] \geq 2/3.$$

- Obs. co-RP $\subseteq$ BPP .

- Is RP$\cap$co-RP in P ? Not known!

Class ZPP

- Recall that PTMs are allowed to <u>not</u> halt on some computation paths defined by its random choices.
- We say that a PTM M has *expected running time* $T(n)$ if the expected running time of M on input x is at most $T(n)$ for all $x \in \{0,1\}^n$.

Class ZPP

- Recall that PTMs are allowed to <u>not</u> halt on some computation paths defined by its random choices.
- We say that a PTM M has *expected running time* $T(n)$ if the expected running time of M on input x is at most $T(n)$ for all $x \in \{0,1\}^n$.

- Definition. A language L is in $\mathrm{ZTIME}(T(n))$ if there's a PTM M s.t. on every input x, $M(x) = L(x)$ whenever M halts, and M has expected running time $O(T(n))$.
- Definition. $\mathrm{ZPP} = \bigcup_{c>0} \mathrm{ZTIME}(n^c)$.

Zero-error **P**robabilistic **P**oly-time.

Class ZPP

- Definition. A language L is in $\mathrm{ZTIME}(T(n))$ if there's a PTM M s.t. on every input x, $M(x) = L(x)$ whenever M halts, and M has expected running time $O(T(n))$.
- Definition. $\mathrm{ZPP} = \bigcup_{c > 0} \mathrm{ZTIME}(n^c)$.
- Problems in ZPP are said to have poly-time *Las Vegas algorithms*, whereas those in BPP are said to have poly-time *Monte-Carlo algorithms*.

- Theorem. $\mathrm{ZPP} = \mathrm{RP} \cap \text{co-}\mathrm{RP} \subseteq \mathrm{BPP}$. *(Assignment)*

- Note. If $\mathrm{P} = \mathrm{BPP}$ then $\mathrm{P} = \mathrm{ZPP} = \mathrm{BPP}$.