Randomized Complexity Classes
• We allow TM to toss coins/throw dice etc. We write \( M(x,R) \) for output of \( M \) on input \( x \), coin tosses \( R \)

• Def: \( L \in \text{RP} \iff \exists \text{ poly-time randomized } M : \)
  \[
  x \in L \implies \Pr_R [M(x,R)=1] \geq 1/2 \\
  x \notin L \implies \Pr_R [M(x,R)=1] = 0
  
  \]

• Def: \( L \in \text{BPP} \iff \exists \text{ poly-time randomized } M : \)
  \[
  x \in L \implies \Pr_R [M(x,R)=1] \geq 2/3 \\
  x \notin L \implies \Pr_R [M(x,R)=1] \leq 1/3
  
  \]

• Exercise: For RP, can replace 1/2 with 1/n^c , or 1- 1/2^m for m = n^c , for any c
  
  For BPP, can replace (2/3,1/3) = (1/2 + 1/n^c , 1/2-1/n^c ) or (1-1/2^m , 1/2^m ).
Exercise: The following are equivalent:

1) \( L \in \text{RP} \cap \text{co-RP} \)

2) There is a randomized poly-time machine \( M \) for \( L \):
   \( \forall x, \forall R, M(x,R) \in \{L(x), ?\} \),
   \( \forall x, \Pr_R [M(x,R) = ?] \leq 1/2 \)

3) There is a randomized machine \( M \) for \( L \):
   \( \forall x, \forall R, M(x,R) = L(x) \)
   the expected running time of \( M \) on \( x \) is poly(n)

This class is known as ZPP.
• Claim: $P \subseteq ZPP \subseteq RP \subseteq BPP$
• Proof: By definition. ■

• Claim: $RP \subseteq NP$
Proof: ?
• Claim: \( P \subseteq ZPP \subseteq RP \subseteq BPP \)
• Proof: By definition.

• Claim: \( RP \subseteq NP \)
Proof: The witness is the random string

• Big open question, is \( P = ZPP = RP = BPP \)?
Surprisingly, this is believed to be the case
Claim: BPP ⊆ P/poly

Proof:
Let $L \in BPP$.
Let $M(x,R)$ be a randomized poly-time TM deciding $L$.

Make the error $< 2^{-n}$.

Note that for every $x$, $\Pr_R [ L(x) \neq M(x,R) ] < 2^{-n}$

So by the probabilistic method,
• **Claim:** \( \text{BPP} \subseteq \text{P/poly} \)

• **Proof:**
  Let \( L \in \text{BPP} \).
  Let \( M(x, R) \) be a randomized poly-time TM deciding \( L \).

  Make the error < \( 2^{-n} \).

  Note that for every \( x \), \( \Pr_R \left[ L(x) \neq M(x, R) \right] < 2^{-n} \)

  So by the probabilistic method, there exists some string \( R^* : L(x) = M(x, R^*) \ \forall \ x \).

  The circuit corresponding to \( M(x, R^*) \) is the desired circuit.  

  **Upshot:** Randomness is only “useful” for TM, not for circuits.
• Claim: BPP \subseteq \sum_2 P
• Claim: $\text{BPP} \subseteq \Sigma_2 \text{P}$

• Proof: Let $M(x,R)$ toss $|R| = r$ coins, and have error $< 1/r^2$

  Fix $x$ and ask: Can we cover $\{0,1\}^r$ with $r$ shifts of
  
  \[ A := \{ R \in \{0,1\}^r : M(x,R) = 1 \} \]

  For $s \in \{0,1\}^r$, the **s-shift** is $s+A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r$

  We'll show the answer to this question is equivalent to $x \in L$

  We then show this question can be asked in $\Sigma_2 \text{P}$
• Claim: \( \text{BPP} \subseteq \sum_2 \text{P} \)

• Proof: Let \( M(x,R) \) toss \(|R| = r\) coins, and have error \(< 1/r^2\)

Fix \( x \) and ask: Can we cover \( \{0,1\}^r \) with \( r \) shifts of

\[
A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}
\]

For \( s \in \{0,1\}^r \), the \( s \)-shift is \( s + A := \{ s \ \text{XOR} \ a : a \in A \} \subseteq \{0,1\}^r \)

• \( x \notin L \), we show we cannot cover. Note \(|A| \leq \?\)
• Claim: $\text{BPP} \subseteq \sum_2 \text{P}$

• Proof: Let $M(x,R)$ toss $|R| = r$ coins, and have error $< 1/r^2$

Fix $x$ and ask: Can we cover $\{0,1\}^r$ with $r$ shifts of $A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}$?

For $s \in \{0,1\}^r$, the s-shift is $s+A := \{ s \text{ XOR } a : a \in A \} \subseteq \{0,1\}^r$

• $x \notin L$, we show we cannot cover. Note $|A| \leq 2^r / r^2$.

$\forall s_1, \ldots, s_r : |s_1+A \cup s_2+A \cup \ldots \cup s_r+A| \leq ?$
• Claim: \( \text{BPP} \subseteq \sum_2 \text{P} \)

• Proof: Let \( M(x,R) \) toss \(|R| = r\) coins, and have error < \(1/r^2\)

Fix \(x\) and ask: Can we cover \(\{0,1\}^r\) with \(r\) shifts of

\[
A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}
\]

For \(s \in \{0,1\}^r\), the \(s\)-shift is \(s + A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r\)

• \(x \notin L\), we show we cannot cover. Note \(|A| \leq 2^r / r^2\). 

\[\forall s_1, \ldots, s_r : |s_1 + A \cup s_2 + A \cup \ldots \cup s_r + A| \leq r \cdot |A| \leq ?\]
• Claim: \( \text{BPP} \subseteq \sum_2 \text{P} \)

• Proof: Let \( M(x,R) \) toss \( |R| = r \) coins, and have error \(< 1/r^2 \)

  Fix \( x \) and ask: Can we cover \( \{0,1\}^r \) with \( r \) shifts of

  \[
  A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}
  \]

  For \( s \in \{0,1\}^r \), the \( s\)-shift is \( s + A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r \)

• \( x \notin L \), we show we cannot cover. Note \( |A| \leq 2^r / r^2 \).

  \[
  \forall s_1, \ldots, s_r : |s_1 + A \cup s_2 + A \cup \ldots \cup s_r + A| \leq r |A| \leq r \frac{2^r}{r^2} < 2^r
  \]

• \( x \in L \), we show we can cover.

  Idea pick the shifts at random and show \( \Pr[\text{do not cover}] < ? \)
• Claim: $\text{BPP} \subseteq \sum_2 \text{P}$

• Proof: Let $M(x,R)$ toss $|R| = r$ coins, and have error $< 1/r^2$

  Fix $x$ and ask: Can we cover $\{0,1\}^r$ with $r$ shifts of $A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}$?

  For $s \in \{0,1\}^r$, the $s$-shift is $s+A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r$

• $x \notin L$, we show we cannot cover. Note $|A| \leq 2^r / r^2$. $\forall s_1, \ldots, s_r : |s_1+A \cup s_2+A \cup \ldots \cup s_r+A| \leq r |A| \leq r 2^r / r^2 < 2^r$

• $x \in L$, we show we can cover.

  Idea: pick the shifts at random and show $\Pr[\text{do not cover}] < 1$:

  $\Pr_{s_1, \ldots, s_r} [\exists y \in \{0,1\}^r : y \notin U_r s_r + A] \leq \ ?$
• Claim: $\text{BPP} \subseteq \sum_2 \text{P}$

• Proof: Let $M(x, R)$ toss $|R| = r$ coins, and have error $< 1/r^2$

Fix $x$ and ask: **Can we cover** $\{0,1\}^r$ with $r$ shifts of

$$A := \{ R \in \{0,1\}^r : M(x, R) = 1 \} \ ?$$

For $s \in \{0,1\}^r$, the s-shift is $s + A := \{ s \text{ XOR } a : a \in A \}$ ⊆ $\{0,1\}^r$

• $x \notin L$, we show we cannot cover. Note $|A| \leq 2^r / r^2$.

$\forall s_1, \ldots, s_r : |s_1 + A \cup s_2 + A \cup \ldots \cup s_r + A| \leq r |A| \leq r 2^r / r^2 < 2^r$

• $x \in L$, we show we can cover.

Idea: pick the shifts at random and show $\Pr[\text{do not cover}] < 1$:

$$\Pr_{s_1, \ldots, s_r} \left[ \exists y \in \{0,1\}^r : y \notin \cup_r s_r + A \right] \leq$$

$$\sum_y \Pr_{s_1, \ldots, s_r} [y \notin \cup_r s_r + A] = ?$$
• Claim: $\text{BPP} \subseteq \sum_2 \text{P}$

• Proof: Let $M(x,R)$ toss $|R| = r$ coins, and have error $< 1/r^2$

  Fix $x$ and ask: Can we cover $\{0,1\}^r$ with $r$ shifts of

  $A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}$ ?

  For $s \in \{0,1\}^r$, the $s$-shift is $s+A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r$

• $x \not\in L$, we show we cannot cover. Note $|A| \leq 2^r / r^2$.

  $\forall s_1, \ldots, s_r : |s_1+A \cup s_2+A \cup \ldots \cup s_r+A| \leq r |A| \leq r 2^r / r^2 < 2^r$

• $x \in L$, we show we can cover.

  Idea: pick the shifts at random and show $\text{Pr}[\text{do not cover}] < 1$:

  $\text{Pr}_{s_1, \ldots, s_r} [\exists y \in \{0,1\}^r : y \not\in U_r s_r + A] \leq$

  $\sum_y \text{Pr}_{s_1, \ldots, s_r}[y \not\in U_r s_r + A] = \sum_y (\text{Pr}_s[y \not\in s + A])^r \leq ?$
• Claim: \( \text{BPP} \subseteq \sum_2 \text{P} \)

• Proof: Let \( M(x,R) \) toss \(|R| = r \) coins, and have error \(< 1/r^2 \)

Fix \( x \) and ask: Can we cover \( \{0,1\}^r \) with \( r \) shifts of

\[ A := \{ R \in \{0,1\}^r : M(x,R) = 1 \} \]?

For \( s \in \{0,1\}^r \), the \( s \)-shift is \( s + A := \{ s \oplus a : a \in A \} \subseteq \{0,1\}^r \)

• \( x \not\in L \), we show we cannot cover. Note \(|A| \leq 2^r / r^2 \).

\[ \forall s_1, \ldots, s_r : |s_1 + A \cup s_2 + A \cup \ldots \cup s_r + A| \leq r \cdot |A| \leq r \cdot 2^r / r^2 < 2^r \]

• \( x \in L \), we show we can cover.

Idea: pick the shifts at random and show \( \Pr[\text{do not cover}] < 1 \):

\[ \Pr_{s_1, \ldots, s_r} \left[ \exists y \in \{0,1\}^r : y \not\in U_r s_r + A \right] \leq \]

\[ \sum_y \Pr_{s_1, \ldots, s_r} [y \not\in U_r s_r + A] = \sum_y (\Pr_s [y \not\in s + A])^r \leq \sum_y (1/r^2)^r < 1 \]

So \( M(x,R) = 1 \iff ? \)
• **Claim:** \( \text{BPP} \subseteq \Sigma_2 \text{P} \)

• **Proof:** Let \( M(x,R) \) toss \(|R| = r\) coins, and have error \(< 1/r^2\)

Fix \( x \) and ask: **Can we cover \( \{0,1\}^r \) with \( r \) shifts of**

\[
A := \{ R \in \{0,1\}^r : M(x,R) = 1 \}
\]

For \( s \in \{0,1\}^r \), the **\( s \)-shift** is \( s+A := \{ s \oplus a : a \in A \} \)

• \( x \not\in L \), we show we cannot cover. Note \(|A| \leq 2^r / r^2\).

\[
\forall s_1, \ldots, s_r : |s_1+A \cup s_2+A \cup \ldots \cup s_r+A| \leq r |A| \leq r 2^r / r^2 < 2^r
\]

• \( x \in L \), we show we can cover.

Idea: pick the shifts at random and show \( \Pr[\text{do not cover}] < 1 \):

\[
\Pr_{s_1,\ldots,s_r} [\exists y \in \{0,1\}^r : y \not\in U_r s_r + A] \leq \sum_y \Pr_{s_1,\ldots,s_r}[y \not\in U_r s_r + A] = \sum_y (\Pr_s[ y \not\in s + A])^r \leq \sum_y (1/r^2)^r < 1
\]

So \( M(x,R) = 1 \iff \exists s_1, \ldots, s_r : \forall y \in \{0,1\}^r \), \( y \in U_r s_r + A \)

\[
\iff \exists s_1, \ldots, s_r : \forall y \in \{0,1\}^r , \forall_{i=1}^r M(x, y + s_i )=1
\]
• Corollary: $P = NP \Rightarrow P = BPP$.

• Proof:

  ?
Corollary: $P = NP \Rightarrow P = BPP$.

Proof:

$P = NP \Rightarrow P = PH$, and so

$P \subseteq BPP \subseteq PH = P$.