The $\text{BP} \cdot C$ complexity class operator is defined as follows; $L \in \text{BP} \cdot C$ if there is a language $L_V \in C$ ("$V$" for "verifier") and a polynomial $p$ such that for all strings $x$,

\[
x \in L \Rightarrow \Pr_{r \in \{0,1\}^p(n)}[(x, r) \in L_V] \geq 3/4
\]
\[
x \notin L \Rightarrow \Pr_{r \in \{0,1\}^p(n)}[(x, r) \in L_V] \leq 1/4
\]

Reading before class on Thursday Nov 9

- Köbler, Schöning, and Torán pp. 68–71 on probability amplification.

In-Class Exercises Tuesday

1. Define $\text{BPP} = \text{BP} \cdot \text{P}$.
   (a) Show that $\text{co} \cdot \text{BP} \cdot C = \text{BP} \cdot \text{co}C$ for any class $C$. (Recall: $L^c = \{x \in \Sigma^* : x \notin L\}$ and $\text{co} \cdot C = \{L : L^c \in C\}$.)
   (b) Use the preceding to conclude that $\text{BPP}$ is closed under complement, that is, $\text{BPP} = \text{coBPP}$.

2. We say that a decision problem $A$ is (polynomial-time) majority reducible to a decision problem $B$, denoted $A \leq_{\text{maj}}^P B$, if there is a polynomial-time function $r \in \text{FP}$ such that, for each input $x$, $r(x)$ outputs a tuple of strings, $r(x) = (y_1, \ldots, y_{\text{poly}(|x|)})$, and for all strings $x$,

\[
x \in A \iff \text{More than half of the } y_i \text{ are in } B.
\]

A class $C$ is closed under majority reductions if $B \in C$ and $A \leq_{\text{maj}}^P B$ implies $A \in C$.
   (a) Show that $\text{P}$ is closed under majority reductions.
   (b) Show that $\text{NP}$ is closed under majority reductions.

In-Class Exercises Thursday

3. Show that if $C$ is a class that is closed under majority reductions, then $\text{BP} \cdot \text{BP} \cdot C = \text{BP} \cdot C$.

4. (This one is important! Gets used all over the place.) Show that if $C$ is closed under majority reductions, then $\exists \cdot \text{BP} \cdot C \subseteq \text{BP} \cdot \exists \cdot C$. 
(b) We define the classes $MA = \exists \cdot BPP$ and $AM = BP \cdot NP$. Show that $MA \subseteq AM$.
(c) Show that $NP \cup BPP \subseteq MA$.
(d) Using complexity class operators and previous parts, show that if $C$ is closed under majority reductions, then $\forall \cdot BP \cdot C \subseteq BP \cdot \forall \cdot C$. (That is: don’t re-do a similar proof to part (a), instead use part (a) directly and some things you know about complexity class operators to prove this result.)

5. Define the “Arthur–Merlin hierarchy” by extending the above, e.g.

$$AMA = BP \cdot MA$$
$$MAM = \exists \cdot AM,$$

and similarly for more letters. That is, define

$$AM[k] = BP \cdot MA[k - 1]$$
$$MA[k] = \exists \cdot AM[k - 1],$$

Show that this hierarchy collapses: for all constant $k$ (independent of input size), $AM[k] \cup MA[k] \subseteq AM$. (Food for thought: what happens if we allow a number of alternations between strong majority and $\exists$ quantifiers that depends on the input size? The answer may surprise you!)

Next week’s exercises

6. (a) Show that $AM \subseteq \Pi_2 P$.
(b) Show that $MA \subseteq \Sigma_2 P \cap \Pi_2 P$. (Note how much stronger this is than merely $BPP \subseteq \Sigma_2 P \cap \Pi_2 P$!)

7. (a) Show that if $NP \subseteq BPP$, then $PH = BPP$. Hint: Use induction, Exercise 4(a), and Exercise 3 to show that $NP \subseteq BPP \Rightarrow PH \subseteq BPP$.
(b) Show that if $NP \subseteq \text{coAM}$, then $PH = AM$. Hint: Similar to previous part, playing around with complexity class operators to show that $NP \subseteq \text{coAM} \Rightarrow PH \subseteq \text{coAM}$.

8. Prove that if Graph Isomorphism is $NP$-complete, then $PH$ collapses to the second level.

Optional Homework Exercises (Side Quest): BPP and oracles

9. (a) Show that $BPP$ is closed under $\leq_p^P$ reductions, that is, that $P^{BPP} = BPP$.
(b) Show that $BPP$ is self-low, that is, $BPP^{BPP} = BPP$.

10. Show that for all classes $C$, we have $BP \cdot C \subseteq BPP^C$.

11. Show that $NP^X$ is closed under majority reductions for any oracle $X$. Use the oracle characterization of $PH$ to show immediately that $\Sigma_k P$ (for all $k$) and $PH$ are all closed under majority reductions.

12. (a) If $L$ is in $BPP$, and $p$ is a polynomial, show that $L' = \{(1^n, x_1, \ldots, x_{p(n)}) : x_i \in L \text{ for all } i\}$ is also in $BPP$. 

(b) Show that $\text{NP}^{\text{BPP}} = \text{NP}[\text{BPP}]$, where the latter means $\text{NP}$ with a $\text{BPP}$ oracle, but it only queries the oracle once. **Hint:** Use nondeterminism to guess the oracle answers, and use the one query at the end to verify all the guesses at once, using part (a).

(c) Show that $\text{NP}^{\text{BPP}} \subseteq \text{BPP}^{\text{NP}}$. **Hint:** With the previous part of this exercise, this part becomes closely related to Exercise 4.

(d) Use the previous part and the oracle characterization of $\text{PH}$ to give an alternative proof that if $\text{NP} \subseteq \text{BPP}$ then $\text{PH} \subseteq \text{BPP}$.

Resources

- Our approach to this material is closest to that in Chapter 2 of Köbler, Schöning, and Torán.

- Arora & Barak Section 8.4.3 covers the result about $\text{NP}$-completeness of GI implying collapse of $\text{PH}$. The rest of their Chapter 8 covers interactive proofs more generally. (Note: they have an exercise to show that $\text{AM} \subseteq \Sigma_3^P$, but in fact we will see it is contained in $\Sigma_2^P$.)

- The result about GI is also covered in Homer & Selman Section 10.5. The rest of Chapter 10 covers probabilistic classes such as $\text{BPP}$ (and friends); their Section 12.3 covers Arthur–Merlin games, while the rest of their Chapter 12 covers more general interactive proofs.


- **Warning!** There is another class called “$\exists^{\text{BPP}}$”, but it is not the same as $\exists^{\cdot \text{BPP}} = \text{MA}$. See the Complexity Zoo entry for the difference (it has to do with how the randomized machines behave on all witnesses vs how they behave only on the one accepted witness).