Problem 1. Define the class $\text{BPP}^A$, for any language $A$, as the class of languages $L$ for which there is a polynomial time probabilistic oracle Turing Machine $M$, such that $M^A$ accepts each $x \in L$ with probability at least $\frac{2}{3}$ and rejects each $x \notin L$ with probability at least $\frac{1}{3}$. Define $\text{BPP}^{\text{BPP}}$ as the union of all classes $\text{BPP}^A$ for $A \in \text{BPP}$.

1. Show that $\text{BPP}^{\text{BPP}} = \text{BPP}$. (20 pts)

2. $\text{RP}$ is defined similarly: $L$ is in $\text{RP}$ if there exists $A \in \text{RP}$ and a probabilistic polynomial time oracle TM such that $x \in L$ is accepted with probability at least $\frac{2}{3}$, but $x \not\in L$ is rejected with probability $1$. Show that $\text{RP}^{\text{RP}} = \text{RP}$ implies $\text{RP} = \text{co-RP}$. (10 pts)

Problem 2. Define the class $X$ as follows. $X$ consists of all languages $L$ for which there exist a pair of languages $A, B \in \text{P}$ and a polynomial $\text{poly}$ such that for each $x$ the following hold:

(a) There exists at least one $w \in \{0, 1\}^{\text{poly}(|x|)}$ such that $(x, w) \in B$.

(b) If $x \in L$, then if $w$ is drawn randomly from $\{0, 1\}^{\text{poly}(|x|)}$, $\Pr[(x, w) \in A | (x, w) \in B] \geq \frac{2}{3}$ (i.e., for at least $\frac{2}{3}$ fraction of $w$ (of length $\text{poly}(|x|)$) such that $(x, w) \in B$, we have that $(x, w) \in A$).

(c) If $x \not\in L$ then if $w$ is drawn randomly from $\{0, 1\}^{\text{poly}(|x|)}$, $\Pr[(x, w) \in A | (x, w) \in B] < \frac{1}{3}$.

1. Show that $\text{BPP} \subseteq X$. (15 pts)

2. Show that $\text{NP} \subseteq X$. (20 pts)

Problem 3. Recall that a uniform $\text{NC}^0$ circuit family consists of boolean circuits of constant depth and constant fan-in, such that the circuits in the family can be generated by a logarithmic space Turing Machine (logarithmic in the size of the input of circuit generated). Note that the output bit of an $\text{NC}^0$ circuit can depend only on a constant number of bits of the input. We consider $\text{NC}^0$ circuits which can output multiple bits. We shall say that such a circuit accepts its input if all the output bits are 1, and else rejects its input. A multi-bit output $\text{NC}^0$ circuit family is said to decide a language if for every binary string $x$, the circuit of input-size $|x|$ accepts $x$ if and only if $x$ is in the language. We define a class of languages $\text{NC}_{\text{AND}}^0$ to consist of languages that are decided (in the above sense) by uniform, multi-bit output $\text{NC}^0$ circuit families.

1. Show that $\text{NC}_{\text{AND}}^0 \subseteq \text{P}$. (10 pts)

2. Recall that $\text{NP}$ is the class of languages $L$ for which there is a language $R \in \text{P}$ and a polynomial poly such that $L = \{x | \exists w, |w| = \text{poly}(|x|), (x, w) \in R\}$. Show that instead of $R \in \text{P}$, if we use $R \in \text{NC}_{\text{AND}}^0$, the class defined is still $\text{NP}$. In other words, show that if we restricted the verifier in the definition of $\text{NP}$ to use a uniform $\text{NC}_{\text{AND}}^0$ circuit instead of polynomial time computation, the class defined remains the same. (25 pts)

[Hint: Can you think of extra information to be provided along with the witness to enable lower complexity for verification?]