1. Let \( f \) be a family of one-way permutations, and let \( b = \{b_n\} \) be a hard bit for \( f^{-1} \). Use \( f \) and \( b \) to describe a language \( L \) for which \( L \in (\text{NP} \cap \text{coNP}) - \text{BPP} \).

The moral of this problem is: the assumption we used to construct the BMY pseudo-random generator placed a priori bounds on the power of \( \text{BPP} \) – it presumed that \( \text{BPP} \) was not powerful enough to simulate \( \text{NP} \cap \text{coNP} \) – and this is one reason to prefer the NW construction, which is based on an assumption that does not place such bounds on the power of \( \text{BPP} \).

2. **Minimum Truth Table Circuit (MTTC)** is the language of pairs \((x, k)\) for which (1) \( |x| \) is a power of 2, and (2) there exists a Boolean circuit of size at most \( k \) computing the function whose truth table is \( x \). Observe that MTTC is in \( \text{NP} \).

   (a) Show that \( \text{MTTC} \in \text{P} \) implies \( \text{BPP} = \text{ZPP} \).

   (b) Show that \( \text{NP} \cap \text{BPP} \subseteq \text{ZPP} \cap \text{NP} \).

Hint: for both parts you may want to refer to Shannon’s theorem from Lecture 5.

3. **CNFs and DNFs.** Recall that a Boolean formula is said to be in \( 3\text{-CNF} \) form if it is the conjunction of clauses, with each clause being the disjunction of at most 3 literals. A Boolean formula is said to be in \( 3\text{-DNF} \) form if it is the disjunction of terms, with each term being the conjunction of at most 3 literals.

   (a) Two useful transformations: describe a polynomial-time computable function that is given as input a fan-in two \((\land, \lor, \neg)\)-circuit \( C(x_1, x_2, \ldots, x_n) \), and produces a 3-CNF Boolean formula \( \phi \) on variables \( x_1, x_2, \ldots, x_n \) and additional variables \( z_1, z_2, \ldots, z_m \) for which

   \[
   \exists z_1, z_2, \ldots, z_m \, \phi(x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_m) = 1 \Leftrightarrow C(x_1, x_2, \ldots, x_n) = 1.
   \]

   Also, describe a polynomial-time computable function that is given as input a fan-in two \((\land, \lor, \neg)\)-circuit \( C(x_1, x_2, \ldots, x_n) \), and produces a 3-DNF Boolean formula \( \phi \) on variables \( x_1, x_2, \ldots, x_n \) and additional variables \( z_1, z_2, \ldots, z_m \) for which

   \[
   \forall z_1, z_2, \ldots, z_m \, \phi(x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_m) = 1 \Leftrightarrow C(x_1, x_2, \ldots, x_n) = 1.
   \]
(b) The definition of QSAT\textsubscript{i} is delicate: recall the definition of QSAT\textsubscript{i} (below each \(x_j\) refers to a vector of variables):

\[
\text{QSAT}_i \text{ (i odd)} = \{3\text{-CNFs } \phi(x_1, x_2, \ldots, x_i) : \exists x_1 \forall x_2 \exists x_3, \ldots \exists x_i \phi(x_1, x_2, \ldots, x_i) = 1\} \\
\text{QSAT}_i \text{ (i even)} = \{3\text{-DNFs } \phi(x_1, x_2, \ldots, x_i) : \exists x_1 \forall x_2 \exists x_3, \ldots \forall x_i \phi(x_1, x_2, \ldots, x_i) = 1\}
\]

We saw that QSAT\textsubscript{i} is \(\Sigma^P_i\)-complete. Argue that if the “CNF” and “DNF” in the above definitions were exchanged, then QSAT\textsubscript{i} would be in \(\Sigma^P_{i-1}\).