1. We defined \( \Sigma^P_2 \) to be the class of languages decided by a polynomial time alternating Turing machine that has an existential quantifier followed by a universal quantifier. In other words, \( L \in \Sigma^P_2 \) iff there exists a 3-ary relation \( R(x, y, z) \) decidable in time polynomial in \( |x| \) such that
\[
x \in L \iff \exists y \forall z [R(x, y, z) = 1].
\]
Prove that \( \Sigma^P_2 \) thus defined equals \( \text{NP}^{\text{SAT}} \). (That is, prove the equivalence of the oracle and alternating views of \( \Sigma^P_2 \), which we claimed in class without proof.)

2. The Vapnik-Chervonenkis (VC) dimension is an important concept in machine learning. If \( F = \{S_1, \ldots, S_m\} \) is a family of subsets of a finite set \( U \), the VC dimension of \( F \), denoted \( \text{VC}(F) \), is the size of the largest set \( A \subseteq U \) such that for every \( A' \subseteq A \), there is an \( i \) for which \( S_i \cap A = A' \). (One says that \( A \) is shattered by \( F \).)

A boolean circuit \( C \) with two inputs \( i \in \{0, 1\}^r \) and \( x \in \{0, 1\}^n \) succinctly represents a collection \( F = \{S_1, S_2, \ldots, S_{2^r}\} \) over universe \( U = \{0, 1\}^n \) if \( S_i = \{x \in U \mid C(i, x) = 1\} \).

Define the language
\[
VCDIM = \{\langle C, k \rangle \mid C \text{ represents a collection } F \text{ s.t. } \text{VC}(F) \geq k\}.
\]
Prove that \( VCDIM \in \Sigma^P_3 \).

3. Prove that if \( \text{NP} \subseteq \text{BPP} \) then \( \text{NP} = \text{RP} \).

4. (a) Prove that \( \text{SIZE}(n^{k+1}) \neq \text{SIZE}(n^k) \) for any \( k \geq 1 \). You may assume without proof (though it is not hard to prove) that for any fixed \( k \), there are functions that are not computable by size \( O(n^k) \) circuits. (Hint: Now among those functions, consider the function with least circuit complexity.)

(b) Prove that for every fixed integer \( k \geq 1 \), \( \text{PH} \not\subseteq \text{SIZE}(n^k) \).

(c) Strengthen the above result to \( \Sigma^P_2 \cap \Pi^P_2 \not\subseteq \text{SIZE}(n^k) \) for any \( k \geq 1 \). (Hint: Make use of the Karp-Lipton collapse.)

5. Prove that if \( L \in \text{BPP} \) then there exists a 3-ary relation \( R(x, y, z) \) that is decidable in time polynomial in \( |x| \) with the following property:

- If \( x \in L \), then \( \exists y \forall z [R(x, y, z) = 1] \).
- If \( x \notin L \), then \( \exists z \forall y [R(x, y, z) = 0] \).

In what way is this a stronger inclusion than \( \text{BPP} \subseteq \Sigma^P_2 \)?

(Hint: Extend the approach behind Lauteman’s proof.)
6. Prove that if square roots modulo a prime can be found in deterministic polynomial time, then one can find a quadratic non-residue modulo a given prime in deterministic polynomial time. (As mentioned in class, the converse is also true, though you don’t have to show that for this exercise.)