1. Prove that \( P \neq \text{SPACE}(n) \).

2. Prove the following version of the Schwarz-Zippel lemma. Let \( F \) be any field (finite or infinite) and let \( Q(x_1, x_2, \ldots, x_m) \in F[x_1, x_2, \ldots, x_m] \) be a non-zero \( m \)-variate polynomial over \( F \) of total degree \( d \). Fix any finite set \( S \subseteq F \). Prove that

\[
\text{Prob}[Q(r_1, r_2, \ldots, r_m) = 0] \leq \frac{d}{|S|}
\]

where the probability is taken over \( r_1, r_2, \ldots, r_m \) that are chosen independently and uniformly at random from \( S \).

3. Prove that if \( \text{NEXPTIME} \neq \text{EXPTIME} \), then \( P \neq \text{NP} \). (Problem 9.19, Sipser’s book)

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

5. (30 points) In this exercise, by circuits we imply Boolean circuits with NOT, AND, and OR gates of fan-in 2, and we measure the size of a circuit by the number of gates in it.

   (a) Prove that there exists a Boolean function \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) which cannot be computed by any circuit of size less than \( \frac{2^n}{8n} \). (Hint: Use a circuit counting argument.)

   (b) Let \( s: \mathbb{N} \rightarrow \mathbb{N} \) be a function such that \( n \leq s(n) < \frac{2^n}{8n} \) for \( n \geq 10 \). Prove that for all large enough \( n \), there exists a function \( g: \{0, 1\}^n \rightarrow \{0, 1\} \) that can be computed by a circuit of size \( 2 \cdot s(n) + O(1) \) but not by a circuit of size \( s(n) \).

   (c) Prove that for every \( k \geq 1 \), \( \text{EXPTIME} \not\subseteq \text{SIZE}(n^k) \), in other words there is a language that can decided in exponential time but cannot be decided by a circuit family of size \( O(n^k) \). (Hint: Use Part (b) above.)

   (d) Prove that \( \text{EXPSPACE} \not\subseteq \bigcup_{k \geq 1} \text{SIZE}(n^k) \). In other words, show that some language in \( \text{EXPSPACE} \) does not have a polynomial sized circuit family deciding it.

   (e) (Extra Credit) Strengthen the result of Part (b) above by proving that there is a function \( g: \{0, 1\}^n \rightarrow \{0, 1\} \) that can be computed by a circuit of size \( s(n) + n + O(1) \) but not by a circuit of size \( s(n) \).