1 (20 p) Let \( S \subseteq \{0, 1\}^n \) be a set of strings that can be recognized in polynomial time. For concreteness let us say that \( S \) is the set of satisfying assignment for a Boolean formula \( \phi \). Let us consider an interactive proof where an all powerful prover, \( P \) wants to convince a polynomial time verifier, \( V \), that the size of \( S \) is at least \( 2^s \) for some parameter \( s \). Let \( H_\alpha : \{0, 1\}^n \rightarrow \{0, 1\}^s \) be a family of pairwise independent hash functions. Consider the following protocol:

1. \( V \) chooses a random \( \alpha_0 \) and a random value \( z \in \{0, 1\}^s \) and sends \( \alpha_0 \) and \( z \) to \( P \).
2. \( P \) responds with \( x \).
3. \( V \) accepts if \( x \in S \) and \( H_{\alpha_0}(x) = z \) and rejects otherwise.

Analyze this protocol! Show that if the size of \( S \) is significantly larger than \( 2^s \) then an optimal \( P \) can make \( V \) accept with high probability while if \( |S| \) is significantly smaller than \( 2^s \) then this probability is small. Try to get good bounds for both probabilities as a function of the size \( |S| \).

2 (20 p) Let \( S \subseteq \{0, 1\}^n \) be a set of strings that can be recognized in polynomial time. For concreteness let us say that \( S \) is the set of all \( x \) such that \( f(x) = y \) for some given value of \( y \) and a one-way function \( f \). Assume that \( V \) holds a random element \( x_0 \in S \). This could have been achieved by a procedure where \( V \) actually defined \( S \) by picking a random \( x \) and then computing \( y = f(x) \). Let us consider an interactive proof where an all powerful prover, \( P \) wants to convince the polynomial time verifier \( V \), that the size of \( S \) is at most \( 2^s \) for some parameter \( s \). Let \( H_\alpha : \{0, 1\}^n \rightarrow \{0, 1\}^s \) be a family of pairwise independent hash functions. Consider the following protocol:

1. \( V \) chooses a random \( \alpha_0 \) and computes \( z = H_{\alpha_0}(x_0) \) and sends \( \alpha_0 \) and \( z \) to \( P \).
2. \( P \) responds with \( x \).
3. \( V \) accepts if \( x = x_0 \) and rejects otherwise.

Analyze this protocol! Show that if the size of \( S \) is significantly smaller than \( 2^s \) then an optimal \( P \) can make \( V \) accept with high probability while if \( |S| \) is significantly larger than \( 2^s \) then this probability is small. Try to get good bounds for both probabilities as a function of the size \( |S| \).