2.1 Definition of Interactive Proofs

An interactive proof of membership in some language $L$ is a protocol $(P, V)$ between a probabilistic prover $P$ and a probabilistic verifier $V$ and satisfies the following properties:

(i) **Completeness:** If $x \in L$, then (honest) prover $P$ makes verifier $V$ accept with probability at least $p = 3/4$.

(ii) **Soundness:** If $x \notin L$, then every (even dishonest) prover $P'$ makes verifier $V$ accept with probability at most $q = 1/2$.

The class of all languages $L$ for which there exists an interactive proof $(P, V)$ with a polynomially bounded verifier $V$ is denoted by $\text{IP}$. Note that the prover $P$ is assumed to be unbounded, i.e., there are no restrictions on her computing power.

a) $(\star)$ Name a language that is not in $\text{IP}$.

b) $(\star)$ Show that a deterministic prover $P$ is as powerful as a probabilistic one, i.e., prove that for every interactive proof $(P, V)$, there exists an interactive proof $(\tilde{P}, V)$ with deterministic $P'$ that accepts the same language.

c) $(\star)$ Show that a language $L$ for which there exists an interactive proof $(P, V)$ with a deterministic verifier $V$ is in $\text{NP}$.

d) $(\star)$ Show that a language $L$ for which there exists an interactive proof with $q = 0$ is in $\text{NP}$.

e) $(\star\star)$ Argue that the definition of $\text{IP}$ is independent of the actual choice of $p,q > 0$. More precisely, let $p = p' + \varepsilon$ and $q = p' - \varepsilon$ for $\varepsilon > 0$ and $p' \in (\varepsilon, 1 - \varepsilon]$. Given an interactive proof $(P, V)$ with parameters $p,q$, construct an interactive proof $(P', V')$ with parameters $p',q'$ for $1 > p' > q' > 0$.

**Hint:** Use Hoeffding’s inequality. Let $\varepsilon > 0$ and let $X_1, \ldots, X_n$ be i.i.d. Bernoulli random variables where $X = \frac{1}{n} \sum X_i$ and $E[X] = \mu$. Then it holds that:

$$P[X - \mu \leq -\varepsilon] \leq e^{-2n\varepsilon^2}$$
$$P[X - \mu \geq \varepsilon] \leq e^{-2n\varepsilon^2}$$
2.2 Discrete Logarithms and Interactive Proofs (⋆⋆)
Consider a cyclic group $G$ of prime order $p$, two generators $g$ and $h$, and two arbitrary group elements $z_1, z_2 \in G$.

a) Construct an interactive protocol that allows a prover $P$ to prove to a verifier $V$ that
\[
\log_g z_1 = \log_h z_2,
\]
where $\log(\cdot)$ is the discrete logarithm in $G$.

Hint: Base your protocol on Schnorr’s. Note that (1) is equivalent to the existence of an $x$ such that $z_1 = g^x$ and $z_2 = h^x$.

b) Analyze your protocol w.r.t. the completeness, soundness, proof-of-knowledge (informally), and zero-knowledge (for the honest verifier) properties. Is your protocol a proof of a statement or of knowledge (or both)?

c) Compare your protocol from a) to Schnorr’s protocol and find a unified view on both protocols.

2.3 The “Complement” of Fiat-Shamir: Proof of Quadratic Non-Residuosity (⋆⋆)
The Fiat-Shamir protocol allows Peggy to prove to Vic that some given number $z \in \mathbb{Z}_m^*$ ($m = p \cdot q$) is a quadratic residue.

a) Describe an interactive protocol $(P, V)$ that allows Peggy to prove to Vic that a given number $a \in \mathbb{Z}_m^*$ is not a quadratic residue. You may assume that Peggy is computationally unbounded.

b) Argue that your protocol is complete and sound. Is your protocol a proof of a statement, or is it a proof of knowledge (or both)?

c) Argue that your protocol leaks no information to the honest verifier $V$, who follows the protocol instructions.

d) Does this hold for a cheating verifier $V'$ as well?