Problem Set 7

Due: Never.

In all problems the languages are over the alphabet Σ = {0, 1}.

Problem 1. [50 points] Let P be a prover and V a verifier. We say that (P, V) is an interactive proof with perfect completeness for language L if:

- **Perfect completeness**: For all \( x \in L \) : \( \text{AccPr}_P(x) = 1 \)
- **Soundness** with error 1/2: For all \( \hat{P} \) and all \( x \notin L \) : \( \text{AccPr}_{\hat{V}}(\hat{P}, x) \leq 1/2 \)

Consider the protocols \((P_1, V_1)\) and \((P_2, V_2)\) shown in Figure 1 and Figure 2 respectively. For each, say whether or not it is an interactive proof with perfect completeness for the language

\[
\text{GRAPH-ISOMORPHISM} = \{ \langle G_0, G_1 \rangle : G_0 \cong G_1 \}
\]

and prove your answer correct.

In both protocols, the common input is \( \langle G_0, G_1 \rangle \) where \( G_0 = ([k], E_0) \) and \( G_1 = ([k], E_1) \) are graphs. In the case \( G_0 \cong G_1 \), the prover is assumed to know (or have computed) a permutation \( \pi \in \text{Perm}(k) \) such that \( \pi(G_1) = G_0 \). If \( \alpha, \beta \in \text{Perm}(k) \) then \( \alpha \beta \in \text{Perm}(k) \) denotes the permutation defined for all \( i \in [k] \) by \( (\alpha \beta)(i) = \alpha(\beta(i)) \).
Figure 1: Specification of $P_1$ and $V_1$, interacting on common input $\langle G_0, G_1 \rangle$.

Figure 2: Specification of $P_2$ and $V_2$, interacting on common input $\langle G_0, G_1 \rangle$. 