2 Complexity Theory (tg508)

Let GI be the language

$$\mathsf{GI} = \{(G_1, G_2) : G_1 \cong G_2\},$$

where G_1, G_2 are simple graphs on the same number of vertices.

Consider the following protocol for GI. On common input (G_1, G_2), the prover P (who knows an isomorphism $\varphi : G_1 \to G_2$ if one exists) does the following:

- P chooses a uniformly random permutation π of the vertices and sends $H = \pi(G_1)$.
- V chooses a uniformly random bit $b \in \{1, 2\}$ and sends b.
- P sends an isomorphism $\sigma : G_b \to H$ (if $b = 1$, $\sigma = \pi$; if $b = 2$, $\sigma = \pi \circ \varphi^{-1}$). V accepts iff $\sigma(G_b) = H$.

Answer the following questions, providing complete definitions and proofs.

(*a*) Define the notion of *statistical zero knowledge proofs*, and explain how the notion of a simulator helps capture the zero knowledge property. [5 marks]

(*b*) Define *honest-verifier* zero knowledge (HVZK) and explain briefly why it is a weaker notion than full zero knowledge. [3 marks]

(*c*) Prove completeness and soundness of the protocol for GI stated above. [6 marks]

(*d*) Show that the protocol is HVZK by describing a simulator, and then show that it produces the same distribution as the honest verifier's view. [6 marks]