CS355: Applied Zero Knowledge Proofs **Spring 2025**

Assignment #1

Due: 11:59pm on Wed, Apr. 16, 2025, on Gradescope (each answer on a separate page)

Problem 1. (*ZK proof variants*) In Lecture 2 we saw a classic zero-knowledge interactive proof for the 3-coloring relation. For a graph $G = (V, E)$, in every iteration, the verifier chose a uniform random edge $e = (i, j)$ in E. We explained in the lecture that if the verifier instead chose a random pair $(i, j) \in V^2$ then the proof system would not be zero knowledge. Suppose that the verifier always chose its query as a random edge $e = (i, j)$ in E', where E' is a proper subset of E (i.e., $E' \subset E$ but $E' \neq E$). The rest of the protocol is unchanged. You can assume that the set E' is part of the statement, that is the prover and verifier are given (G, E').

a. Is the resulting proof system HVZK? If so, show a simulator.

b. Is the resulting (repeated) proof system sound? If so explain why. If not, show a statement (G, E') where G is not 3-colorable, but the verifier always accepts.

Problem 2. (*Sigma protocols*) Let G be a cyclic group of prime order q with generator $g \in G$. Consider the following relation

$$R := \left\{ \big((u, v, w \in G), (\alpha \in \mathbb{Z}_q)\big) \ : \ u = g^{\alpha},\ v = g^{(\alpha^2)},\ w = g^{(\alpha^3)} \right\}$$

a. Use the generalized Schnorr protocol to write out an explicit HVZK proof system for R. Hint: consider the homomorphism $\varphi(\gamma) := (g^{\gamma}, u^{\gamma}, v^{\gamma})$ from $\mathbb{Z}_q$ to G^3.

b. What is the transcript of this protocol?

c. Show that your proof system from part (a) is complete.

d. Give an explicit proof that your proof system from part (a) is HVZK. That is, construct a simulator $S(u, v, w)$ that simulates the transcript whenever $(u, v, w) \in L(R)$.

e. Prove that your proof system from part (a) is knowledge sound. It suffices to show that your proof system from part (a) is 2-special sound.