# COMP6453: Week 9 Answers

## 1 Zero Knowledge Proof for Graph Isomorphism

For this exercise, review what an *isomorphism* between two graphs is.

Consider the following proof between a prover $P$ and a verifier $V$. Given two graphs $G_0$ and $G_1$, $P$ wants to convince $V$ that he knows a permutation $\pi$ such that $\pi(G_0) = G_1$. $P$ could simply send $\pi$ to $V$, but that is hardly zero-knowledge; we want to convince $V$ that $\pi$ is an isomorphism without revealing anything about it. The protocol is as follows:

$P \to V$ : P randomly chooses a permutation $\sigma$ and a bit $b \in \{0,1\}$, computes $H = \sigma(G_b)$, and sends $H$ to $V$.

$V \to P$: $V$ chooses a bit $b_0 \xleftarrow{R} \{0,1\}$ and sends it to $P$.

$P \to V$ : $P$ sends the permutation $\tau$ to $V$ , where

$$\tau = \begin{cases} \sigma & b = b' \\ \sigma\pi^{-1} & b = 0, b' = 1 \\ \sigma\pi & b = 1, b' = 0 \end{cases}$$

$V$ accepts if and only if $H = \tau(G_{b_0})$.

Show the protocol is complete and sound (it is also zero knowledge, can try to prove this as well)

**Answer:**

Completeness can be verified. For soundness, we note that when $b \neq b'$, then $\tau(G_{b'} = H$ if and only if $\pi$ is an isomorphism. If $\pi$ is not an isomorphism, then the verification check only passes when $b = b'$ and for one of the other cases. This occurs with a probability below 1. We can reduce this probability by re-running the protocol multiple times.

**Zero-knowledge.** To see this is zero knowledge, we need to show that for any (honest) verifier $V^*$, there exists an efficient simulator $S$ which can produce a transcript indistinguishable to conversation between the prover $P$ and the verifier $V^*$.

Given a verifier $V^*$, define $h^*(G_0, G_1, H)$ be the bit chosen by $V^*(G_0, G_1, z)$ at the second step of the protocol, after having received H.

The simulator works as follows: randomly choose a bit $b \in \{0,1\}$ and a permutation $\sigma$ on $G_b$. Set $H = \sigma(G_b)$ and let $b' = h^*(G_0)$. If $b' = b$, output $(b', \sigma, H)$. Otherwise, restart. Since $Pr[b = b'] = 1/2$, simulator iterates twice on average, so it is efficient.

Using $Pr[b = b'] = 1/2$ again, we see that the simulator halting on a certain $(b, \sigma)$ is independent of the choice of $(b, \sigma)$ and therefore of $H = \sigma(G_b)$. Therefore the distribution of the simulator output is the same as the distribution of a real interaction.

## 2 Interactive Proof for Quadratic Residue

Next, we describe an interactive proof, where the $P$ convinces $V$ of *knowledge* of a quadratic residue in $\mathbb{Z}_N$. Namely, for a public statement $x \in \mathbb{Z}_N$, $P$ will prove he knows $w$ such that $w^2 = x \pmod{N}$.

$P \to V$ : $P$ chooses random $u \xleftarrow{R} \mathbb{Z}_N^*$ and sends $y = u^2$ to $V$.

$V \to P$ : $V$ chooses $b \xleftarrow{R} \{0, 1\}$ and sends $b$ to $P$.

$P \to V$ : If $b = 0$, $P$ sends $u$ to $V$. If $b = 1$, $P$ sends $w \cdot u \pmod n$ to $V$.

Verification: Let $z$ denote the number sent by $P$. $V$ accepts the proof in the case $b = 0$ and $z^2 = y \pmod n$. In the case $b = 1$, $V$ accepts the proof if $z^2 = xy \pmod n$.

Show the protocol is complete and sound (it is zero knowledge as well but this is much trickier).

**Answer:**

Completeness is an easy check. For soundness, suppose $x$ is not a quadratic residue. Let $y$ be $P$'s output at the beginning of the protocol. Note that we can make $V$ reject if $y \notin Z_N^*$, so assume $y \in Z_N^*$ without loss of generality. Note that $y$ is independent of the bit $b$ which the verifier sends in the second step in the protocol. Assume $x$ is not a quadratic residue. We now have two cases:

Case 1: $y$ itself is a quadratic residue. Then $y = u^2$ for some $u \in \mathbb{Z}_N^*$. With probability 1/2 we have $b = 1$. Assume the prover accepts in this case. Let $z$ be the $P$'s message in the last step of the protocol. Since $b = 1$, the verifier only accepts when $z^2 = xy$. But this implies that $(zu^{-1})^2 = z^2u^{-2} = xyy^{-1} = x$. This implies $x$ is a quadratic residue, a contradiction. So the verifier rejects with probability $\geq 1/2$ in this case.

Case 2: y is not a quadratic residue. With probability 1/2 we have that $b = 0$. In this case, the prover must come up with $z$ such that $z^2 = y$, which is impossible. So the verifier rejects with probability $\geq 1/2$ in this case.

We showed the verifier accepts with probability less than 1/2 when $x$ is not a quadratic residue. This probability can be reduced with multiple iterations of the protocol.