COMP6453 Tutorial Week 9

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 π such that $\pi(G_0) = G_1$. P could simply send π to V, but that is hardly zero-knowledge; we want to convince V that π is an isomorphism without revealing anything about it. The protocol is as follows:

$P \to V$: P randomly chooses a permutation σ 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 τ 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 $H = \tau(G_{b_0})$ and τ is a one-to-one mapping between vertices and edges.

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

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).