Problem 1: Aborting simulators

Let $R, P, V$ be as in the lecture in the description of the graph isomorphism protocol.

In the classical case, we used the following two properties of the “aborting simulator” $S_1$ (described in the lecture):

Claim 1: If $(x, w) \in R$, then $\Pr[S_1(x, z) \text{ aborts}] = \frac{1}{2}$.

Claim 2: Assume that $(x, w) \in R$. Let $S_1(x, z)$ denote the distribution of the output of $S_1$ on inputs $x, z$. (Assume a special output symbol $\bot$ for abort.) Let $S_1(x, z)|\text{success}$ denote that distribution under the condition that $S_1(x, z) \neq \bot$. Then $S_1(x, z)|\text{success}$ has the same distribution as $(P(x, w), V(x, z))$.

These two claims can be shown as follows:

Consider the following games. In each game, we assume that $V^*$ runs on input $(x, z)$, and the notation $\alpha \leftarrow V^*[\beta]$ means that we send $\beta$ to $V^*$ and let $\alpha$ denote the answer/output. We write $\alpha \overset{\$}{\leftarrow} M$ for uniformly chosen $\alpha \in M$. $\text{perm}$ denotes the set of permutations on the set of vertices of $G_1$. We assume $x = (G_1, G_2)$ and $w = \phi$, and that $V^*$ never chooses an $i \notin \{1, 2\}$. 
This shows Claim 2.

\[ \langle \perp \rangle \]

(a) Understand the proof in the classical case. In particular, understand why all the outputs of the last game, conditioned on not being \( \perp \), is the same as \( \langle \perp \rangle \).

Since the outputs of the first and the last game have the same distribution, it follows that \( \rho \) and returns the quantum state

\[ \rho \]

For simplicity, assume a state \( \langle \perp \rangle \) is constructed like \( \perp \). This gives no points, but is helpful for the next problem. You don’t need to write anything up for this problem.
(b) Show: If \((x, w) \in R\), then \(\text{tr}(P \cdot S^Q_1(x, \rho)) = \frac{1}{2}\). (I.e., \(S^Q_1\) aborts with probability exactly \(\frac{1}{2}\).)

(c) Show: If \((x, w) \in R\), then
\[
\frac{\bar{P} \cdot S^Q_1(x, \rho) \cdot \bar{P}}{\text{tr}(\bar{P} \cdot S^Q_1(x, \rho) \cdot \bar{P})} = \langle P(x, w), V^*(z, \rho) \rangle.
\]
(I.e., conditioned on not aborting, \(S^Q_1(x, \rho)\) outputs \(\langle P(x, w), V^*(z, \rho) \rangle\).)

(d) Show: If \(\frac{\bar{P} \cdot S(x, \rho) \cdot \bar{P}}{\text{tr}(\bar{P} \cdot S(x, \rho) \cdot \bar{P})} = \langle P(x, w), V^*(z, \rho) \rangle\) for some simulator \(S\) and \(\text{tr}(P \cdot S(x, \rho)) \leq \varepsilon\), then \(\text{TD}(S(x, \rho), \langle P(x, w), V^*(z, \rho) \rangle) \in O(\sqrt{\varepsilon})\).

(This shows that if we manage to construct a simulator \(S\) that aborts rarely and, conditioned on not aborting, has the right distribution, then we have statistical zero-knowledge.)

Hint: Apply Lemma 8 in the lecture notes to \(S(x, \rho)\) to get a state \(\tilde{\rho}\) with \(\bar{P} \cdot \tilde{\rho} \cdot \bar{P} = \tilde{\rho}\) and \(\text{TD}(\tilde{\rho}, \rho) \leq \sqrt{\varepsilon}\) where \(\rho \equiv S(x, \rho)\). Then find upper bounds for \(\text{TD}(\bar{P} \cdot \rho S \cdot \bar{P}, \bar{P} \cdot \tilde{\rho} \cdot \bar{P})\), for \(\text{TD}(\tilde{\rho}, t_S \rho V)\) where \(\rho V \equiv \langle P(x, w), V^*(z, \rho) \rangle\) and \(t_S \equiv \text{tr}(\bar{P} \cdot \rho S \cdot \bar{P})\), for \(\text{TD}(\rho V, t_S \rho V)\), and for \(\text{TD}(\rho S, \rho V)\) (in that order).

Problem 2: Quantum proofs

Show that if \((P, V)\) is a proof system (Definition 59 in the lecture notes), then it also is a quantum proof system as in the following definition:

**Definition 1 (Quantum proof systems)** We call a pair \((P, V)\) of interactive machines a quantum proof system for the relation \(R\) with soundness-error \(\varepsilon\) iff the following two conditions are fulfilled:

- Completeness: For any \((x, w) \in R\), we have that \(\text{Pr}[\langle P(x, w), V(x) \rangle = 1] = 1\).
- Soundness: For any (potentially computationally unlimited) quantum machine \(P^*\), and for any \(x \notin L_R\), we have \(\text{Pr}[\langle P^*(x), V(x) \rangle = 1] \leq \varepsilon\).

Notice that the only difference to Definition 59 in the lecture notes is the additional word quantum.

Problem 3: Zero-knowledge and discrete logarithm (bonus problem)

This problem is optional. But you can gain 8 extra points from it. This can help if you are below the 50% required for participating in the exam.
Fix a group $G$ of prime order $q$ with generator $g$. ($G$, $q$, and $g$ may depend on some implicit security parameter but are considered publicly known.) Let $R := \{(x, w) : g^w = x, w \in \{0, \ldots, q-1\}\}$.

Consider the following proof system for $R$ (Schnorr’s proof system for discrete logarithms):

- The prover $P$ gets input $(x, w) \in R$.
- The verifier $V$ gets input $x \in R$.
- The prover $P$ chooses $b \overset{\$}{\leftarrow} \{0, \ldots, q-1\}$ and sends $a := g^b$ to the verifier $V$.
- The verifier chooses $r \overset{\$}{\leftarrow} \{0, \ldots, q-1\}$ and sends $r$ to the prover $P$.
- The prover $P$ computes $s := b + rw \mod q$ and sends $s$ to the verifier $V$.
- The verifier $V$ checks whether $x, a \in G$ and $g^s = ax^r$.

This proof system is well-known to be a proof system. However, in the classical setting, it is unknown whether this proof system is zero-knowledge!

(a) Show that $(P, V)$ is a proof system with soundness-error $1/q$.

(b) Show that $(P, V)$ is statistical quantum zero-knowledge.

**Hint:** This has nothing to do with rewinding!

---

It is however “honest-verifier zero-knowledge”. This is a weaker notion where the verifier is considered to behave honestly.