**Quantum Cryptography (spring 2023)** Dominique Unruh

# Exercise Sheet 12

Out: 2023-05-08 Due: 2023-05-15

## 1 Quantum proofs

| | |
|---|---|
| **Knowlets:** | ProofSys ProblemID: QProofs |
| **Time:** | |
| **Difficulty:** | |

Show that if $(P, V)$ is a proof system (Definition 56 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* $\Pr[\langle P(x, w), V(x)\rangle = 1] = 1$.
- Soundness: *For any (potentially computationally unlimited)* ***quantum*** *machine $P^*$, and for any $x \notin L_R$, we have* $\Pr[\langle P^*(), V(x)\rangle = 1] \leq \varepsilon$.

Notice that the only difference to Definition 56 in the lecture notes is the additional word **quantum**.

**Hint:** You will crucially use the fact that it is possible for a classical algorithm to simulate the output of a quantum algorithm (as long as the quantum algorithm does not output quantum information, and as long as we don't hcare about the runtime).