Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2023/24

— Exercise Sheet #8 —

Problem 21: Ordering of controlled gates and measurements.

Consider $n+1$ qubits, split into one qubit labeled A and n qubits B, and consider a controlled-U gate which is controlled by A and where U acts on B, and which acts on some initial state $|\psi\rangle$ (e.g. because it is part of a larger circuit). After applying the controlled-U gate, the control qubit A is measured in the computational basis.

Show that we can replace this circuit acting on $|\psi\rangle$ by one where we *first* measure the qubit A, and then apply U conditioned on the measurement outcome – i.e., we apply U only if the outcome was $|1\rangle$. (Differently speaking, we control the application of U by the *classical* measurement outcome.)

Explain how this can be generalized to circuits containing several controlled gates controlled by A. How early can we measure A? What happens when the circuit also contains gates which act on A in a way where it is used other than as a control qubit (i.e. where the state of A in the computational basis is changed)?

Problem 22: The Bernstein-Vazirani algorithm.

The Bernstein-Vazirani algorithm is a variation of the Deutsch-Jozsa problem.

Suppose that we are given an oracle

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle \ ,$$

where $f : \{0,1\}^n \to \{0,1\}$, i.e. x is an n-qubit state and y a single qubit, and where we have the promise that $f = a \cdot x$ for some unkown $a \in \{0,1\}^n$. The task is to determine a.

Show that the same circuit used for the Deutsch-Jozsa algorithm can also solve this problem, i.e., it can be used to find a with unit probability in one iteration.

Compare this to the number of classical calls to the function f required to determine a (either deterministically or with high probability).