Lecture & Proseminar 250120/250122
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2020/21

— Exercise Sheet #9 —

Problem 1: Circuits for one-qubit unitaries and controlled unitaries.

Let $R_\alpha(\phi) = e^{i\phi/2\,\sigma_\alpha}$, $\alpha = x, y, z$.

1. Show that for any H with $H^2 = I$, $e^{i\vartheta H} = \cos(\vartheta)\, I + i\, \sin(\vartheta)\, H$. (Recall that exponentials of operators are defined through the Taylor series.)

2. Show that any one-qubit unitary U can be written as
$$U = e^{i\phi} R_z(\alpha) R_x(\beta) R_z(\gamma) \ .$$
Construct the angles α, β, γ, and ϕ explicitly in terms of U. (It can be helpful to start by choosing a suitable parametrization of the entries of U.)

3. Show that also such a decomposition of the form
$$U = e^{i\phi'} R_x(\alpha') R_z(\beta') R_x(\gamma') \tag{1}$$
(i.e. with the position of the x and z swapped) exists.

4. Use (1) to show that for a special unitary 2×2 matrix $U \in \mathrm{SU}(2)$ (i.e. $\det(U) = 1$), there exist matrices $A, B, C \in \mathrm{SU}(2)$ such that $ABC = I$ and $AXBXC = U$, where X is the Pauli x matrix.

5. Use this to construct a circuit which implements a controlled-U gate (for any unitary U), which uses the matrices A, B, and C, CNOT gates, and an additional one-qubit gate E that which adjusts relative phases.

Problem 2: 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).

Problem 3: 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 which beyond using it as a control qubit?