Lecture & Proseminar 250078/250042
"Quantum Information, Quantum Computation, and Quantum Algorithms" WS 2024/25

— Exercise Sheet #7 —

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

$$U = e^{i\phi'} R_z(\alpha') R_y(\beta') R_z(\gamma') \tag{1}$$

   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. (*Hint:* Try to split up the individual rotations in (1) into several rotations, e.g. $R_z(\alpha') = R_z(\alpha' + \delta)R_z(-\delta)$, and use the fact that commutation with X changes the rotation direction of y and z rotations, e.g. $XR_z(\delta) = R_z(-\delta)X$.)

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 which adjusts relative phases.

Problem 2: n-qubit Toffoli gates.

An n-qubit Toffoli gate is a Toffoli gate with $n-1$ controls; i.e., it flips the n'th bit if and only if the other $n-1$ bits are all one. The goal of this problem is to see how n-qubit Toffolis can be built up from simpler gates, most importantly normal 3-qubit Toffolis.
The subsequent constructions rely on using ancilla qubits. For all problems below, **consider two cases**:

- First, the ancillas are initialized in the state $|0\rangle$.
- Second, the ancillas are in some unknown state $|\phi\rangle$.

In both cases, we want to return the ancilla qubits in the state in which they were initially. While the first case is of course covered by the second case, you should also consider whether there is a simpler realization in the first case.
(Being able to realize the gate using an unknown ancilla which is returned in the same state is very useful, since then any qubit on which the gate to be constructed does not act can serve as a "temporary" ancilla.)

1. Show that the n-qubit Toffoli gate can be implemented using two $n-1$-qubit Toffoli gates and two regular 3-qubit Toffoli gates using one ancillary qubit.

2. Using the previous procedure to recursively decompose every gate into 3-qubit Toffoli gates, how many 3-qubit Toffoli gates do you need to construct the n-qubit Toffoli gate? How many ancillas are needed? (Are there ways to save ancillas?)

3. Find a construction which is more efficient in terms of the scaling of the number 3-qubit Toffoli gates used, at the cost of using more ancillas. (You should get a circuit which requires a number of 3-fold Toffoli gates which scales linearly with n.)

(*Hint:* Remember that the Toffoli gate can be used to build a logical AND gate using ancillas.)

Problem 3: 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)?