Lecture "Quantum Information" WS 19/20 — Exercise Sheet #5

Problem 1: One-qubit unitaries.

1. Show that for any U such that $U^2 = I$, it holds that $\exp[i\phi U] = \cos\phi\,\mathbb{1} + i\sin\phi\,U$.
2. Verify that $R_z(\phi)$ rotates a state about the z-axis by angle ϕ. This is, given a state ρ with Bloch vector $\hat{r} = (r_x, r_y, r_z)$, show that the Bloch vector of $\rho' = R_z(\phi)\rho R_z(\phi)^\dagger$ is $\hat{r}$ rotated by ϕ about z.
3. Show that up to a global phase, any unitary one-qubit transformation U can be implemented with three rotations about the x and z-axes, i.e. find angles α, β, γ and α', β', γ' such that $U = R_x(\alpha)R_z(\beta)R_x(\gamma)$ and $U = R_z(\alpha')R_x(\beta')R_z(\gamma')$. (*Hint:* Up to a global phase factor, any unitary transformation on a single qubit is a rotation $U = R_{\hat{n}}(\phi)$ by an angle ϕ about axis $\hat{n} = (n_x, n_y, n_z)$.)

(*Note:* There is nothing specific about the choice of x and z axes, one may e.g. choose y and z instead, such that for some angles α, β, γ it e.g. also holds that $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ for any U.)

Problem 2: Controlled-U gate.
In this exercise, we will show that for any unitary matrix U, the controlled-U gate can be realized using only one-qubit and CNOT gates.

1. Use the previous exercise to show that for a special unitary matrix $U \in SU(2)$ (i.e. $\det(U) = 1$), there exist matrices $A, B, C \in SU(2)$ such that $ABC = I$ and $AXBXC = U$, where X is one of the Pauli matrices.
2. Based on this, find a realization of the controlled-U gate (for any unitary U) that uses only the matrices A, B, and C, CNOT gates, and an additional one-qubit gate E that is used to adjust the global phase.

Problem 3: Gate identities.
Verify the following gate identities given in the lecture:

1. Verify the identities for the behavior of the CNOT gate when conjugating it with Hadamard gates.
2. Verify the construction for the Toffoli gate using controlled-V gates.

(*Note:* While both of these identities can be verified by multiplying out the matrices, it is more instructive to treat the control qubits as "classical", i.e., consider each of their values in the computational basis.)

Problem 4: n-qubit Toffoli gate.
An n-qubit Toffoli gate is a Toffoli gate with $n-1$ controls; i.e., it flips the nth bit if and only if the other $n-1$ bits are all one.

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. Decomposing every gate into 3-qubit Toffoli gates, how many 3-qubit Toffoli gates do you need to construct the n-qubit Toffoli gate?
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. (A linear number of 3-fold Toffoli gates should suffice.)

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

Problem 5: The Bernstein-Vazirani algorithm.
This is a variation of the Deutsch-Jozsa problem. Suppose that the quantum black box computes one of the functions f_a, where $f_a(x) = a \cdot x$ and a is an n-bit string. In the quantum circuit formalism, this corresponds to a unitary U_a s.t. $U_a|x\rangle = (-1)^{a\cdot x}|x\rangle$. In other words, the unitary applies the Z gate to

the kth qubit, iff the string a has 1 on the kth position (for all $k \in \{1, 2, ..., n\}$). The task is to determine a. Show that this problem can be solved by the Deutsch-Jozsa algorithm. That means that we use the same quantum circuit, just with a different oracle (and a different interpretation of the measurement result).