

**Problem 26: 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  $\alpha$ ,  $\beta$ ,  $\gamma$ , and  $\phi$  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  $2 \times 2$  matrix  $U \in \text{SU}(2)$  (i.e.  $\det(U) = 1$ ), there exist matrices  $A, B, C \in \text{SU}(2)$  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 27:  $n$ -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 all initialized in the state  $|0\rangle$ .
- Second, the ancillas are in some unknown state  $|\phi\rangle$  (this can be a different state for each ancilla – note that by linearity, this implies that the ancillas can be part of a complicated entangled state including other qubits).

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.

- 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?)
- 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 28: 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 29: Reversible classical 2-bit gates.**

- Show that all reversible classical 2-bit gates  $G(x_1, x_2) = (y_1, y_2)$  can be written as an affine linear map over  $\mathbb{Z}_2$ , i.e.,

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \pmod{2}$$

(where  $x_i, y_i \in \{0, 1\}$ , and  $M$  has entries 0 and 1).

- Show that all those gates can be decomposed into only NOT and CNOT gates. (A useful identity can be that three consecutive CNOTs with opposite alignment swap the input bits.) Of course, you can solve this question before question 1, and then just show that CNOT and NOT are affine linear maps over  $\mathbb{Z}_2$ .
- Show that this implies that any classical circuit consisting only of reversible 2-bit gates can be written as an affine linear transformation over  $\mathbb{Z}_2$ .
- Show that the Toffoli gate is not of this form – that is, reversible classical two-bit gates are not universal for classical computation.

(*Note:* The class of problems which can be solved this way in time  $\text{poly}(n)$ , with  $n$  the number of bits, defines the complexity class  $\oplus\text{L}$  (pronounced “Parity-L”).  $\oplus\text{L}$  can be simulated in time  $\log(n)^2$  by a general classical circuit, and is thus indeed much more restricted than general efficient classical computations, which can have a runtime  $\text{poly}(n)$ .)

**Problem 30: The Bernstein-Vazirani algorithm.**

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

Suppose that we are given an oracle

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

where  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , 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 unknown  $a \in \{0, 1\}^n$ . 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 31: The original Deutsch algorithm.**

In the original version of his algorithm (found under this link with univie-Login), Deutsch does not use the phase kick-back technique. Instead, he applies  $U_f$  to  $|+\rangle|0\rangle$ , and thus obtain the state

$$|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle) .$$

1. Write down explicitly the output states  $|\psi_{\text{out}}\rangle$  obtained for an  $f$  which is (i) constant (i.e.,  $f(0) = f(1)$ ), and (ii) balanced (i.e.,  $f(0) \neq f(1)$ ).
2. Devise a measurement (projective or POVM) which has three outcomes, where outcome 1 allows to conclude with certainty that  $f$  is constant, outcome 2 allows to conclude with certainty that  $f$  is balanced, and the third outcome does not allow for any definite conclusion about  $f$ .
3. Try to find a measurement which give a conclusive result with an as high as possible probability. What is the best you can achieve? (*Hint*:  $\frac{1}{2}$  is possible.) Can you achieve this with a projective measurement?

*Feel free to check the paper (linked above) – the solution can be found there quite explicitly, and checking papers can be very instructive.*