Christian B. Mendl, Pedro Hack, Keefe Huang, Irene López Gutiérrez

Exercise 6.2 (Universal set of quantum gates[2])
A set of quantum gates is called *universal* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit composed of only gates in this set. An example is the set of single qubit gates and the CNOT gate. In particular, this set is able to represent any two-level unitary (that is, any unitary acting non-trivially only on at most two vector components). The set of two-level unitaries is universal, and consequently so is the set of single qubit gates and CNOT.

In this exercise, you will work on representing two-level unitaries as a combination of single qubit gates and the CNOT gate.

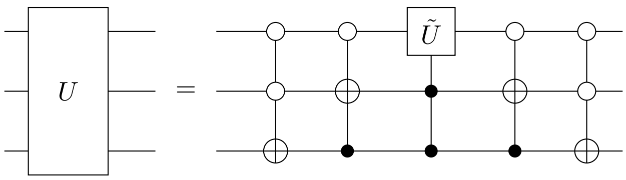
Consider a unitary U acting non-trivially only on two basis states: $|g_1\rangle$ and $|g_m\rangle$. Here, g_1 and g_m are two binary strings which differ in m bits. Flipping $m-1$ differing bits from g_1 results in g_{m-1}, which agrees with g_m except for a single bit. With this in mind, the circuit implementing U works as follows:

1. Apply controlled flips to swap the basis states $|g_1\rangle$ and $|g_{m-1}\rangle$.
2. Apply a controlled $\tilde{U}$ on the qubit in the position where $|g_m\rangle$ and $|g_{m-1}\rangle$ differ, conditional on the other qubits being in the state of the bits in both $|g_m\rangle$ and $|g_{m-1}\rangle$. Here $\tilde{U}$ is the non-trivial submatrix of U.
3. Swap back $|g_1\rangle$ and $|g_{m-1}\rangle$.

As an example, consider the following unitary operator U acting non-trivially only on $|000\rangle$ and $|111\rangle$:

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad \text{with} \quad \tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

A circuit implementation of U is:



A white dot on the control qubit means that the gate only acts if the control is $|0\rangle$. Note that the first two controlled gates on the right realize the map $|000\rangle \mapsto |011\rangle$.

(a) Show that U and the above circuit are equivalent for an arbitrary input state.

(b) Without stating the full proof, explain why the controlled flips and the controlled $\tilde{U}$ can be replaced using only single qubit gates and the CNOT gate. Hint: Section 4.3 of the Nielsen and Chuang book may be helpful.

(c) Using the procedure above, find an implementation of the two-level operation

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}.$$

[2] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 4.5.2

Solution

(a) Given an arbitrary input state

$$|\psi\rangle = x_0\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

then

$$U\,|\psi\rangle = (ax_0+bx_7)\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (cx_0+dx_7)\,|111\rangle\,.$$

Applying each gate of the circuit:

$$|\psi\rangle \mapsto |\psi_1\rangle = x_0\,|001\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

$$|\psi_1\rangle \mapsto |\psi_2\rangle = x_0\,|011\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7\,|111\rangle\,,$$

$$\begin{aligned}
|\psi_2\rangle \mapsto |\psi_3\rangle &= x_0(\tilde{U}\,|0\rangle)\,|11\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + x_7(\tilde{U}\,|1\rangle)\,|11\rangle \\
&= ax_0\,|011\rangle + bx_0\,|111\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle \\
&\quad + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + cx_7\,|011\rangle + dx_7\,|111\rangle \\
&= (ax_0 + cx_7)\,|011\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|001\rangle \\
&\quad + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (bx_0 + dx_7)\,|111\rangle\,,
\end{aligned}$$

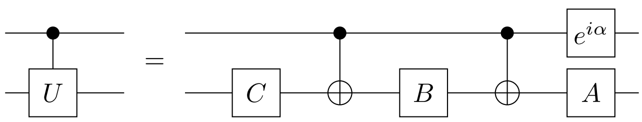
$$|\psi_3\rangle \mapsto |\psi_4\rangle = (x_0a+x_7c)\,|001\rangle + x_1\,|000\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (x_0b+x_7d)\,|111\rangle\,,$$

$$|\psi_4\rangle \mapsto |\psi_5\rangle = (x_0a+x_7c)\,|000\rangle + x_1\,|001\rangle + x_2\,|010\rangle + x_3\,|011\rangle + x_4\,|100\rangle + x_5\,|101\rangle + x_6\,|110\rangle + (x_0b+x_7d)\,|111\rangle\,,$$

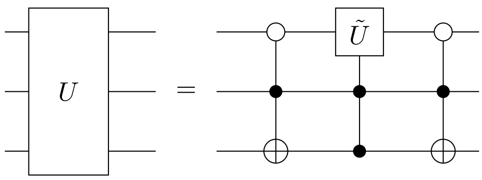
which agrees with $U\,|\psi\rangle$.

(b) All controlled flips can be written as a combination of Toffoli gates and X-Pauli gates (by simply including X gates before and after the white dots of the controlled flips). The Toffoli gate can be decomposed into single-qubit and CNOT gates, as shown in Exercise 5.2.

Any unitary can be decomposed into $e^{i\alpha}AXBXC$, where $ABC = I$. Therefore, the any controlled unitary can be decomposed into:



(c) U acts non-trivially only on $|010\rangle$ and $|111\rangle$. We first need to map $|010\rangle \mapsto |011\rangle$, and then apply a controlled-$\tilde{U}$ on the first qubit before swapping $|010\rangle$ and $|011\rangle$ again. This is realized by the circuit:



Alternatively, one can swap $|010\rangle \leftrightarrow |110\rangle$ and then apply the controlled-$\tilde{U}$ on the third qubit: