Christian B. Mendl, Pedro Hack, Irene López Gutiérrez, Keefe Huang due: 05 Dec 2022, 08:00 on Moodle

Tutorial 6 (The no-cloning theorem[1])

The *no-cloning theorem* states that, surprisingly, one cannot make a copy of an unknown quantum state. In more detail, we consider a system of two qubits (source and target): the first qubit is the source state $|\psi\rangle$, and the second qubit starts out in some standard state $|s\rangle$, for example $|s\rangle = |0\rangle$. Thus the initial state is $|\psi\rangle \otimes |s\rangle \equiv |\psi\rangle\,|s\rangle$. One would like to copy $|\psi\rangle$ into $|s\rangle$, that is, find some unitary transformation $U \in \mathbb{C}^{4\times 4}$ such that

$$|\psi\rangle \otimes |s\rangle \mapsto U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,.$$

Show that such a copying procedure is impossible: the equation cannot hold for arbitrary source qubits $|\psi\rangle$.

Exercise 6.1 (Heisenberg uncertainty principle for a single qubit)

Imagine we prepare multiple copies of an arbitrary single-qubit state $|\psi\rangle$, described by the Bloch vector (r_x, r_y, r_z). Some of these copies are measured using the observable Z, and the remaining copies using the observable X.

(a) Compute the expectation values of both measurements.
Hint: These two measurements are projective measurements and have a geometric interpretation on the Bloch sphere. You can use without proof the identities $\cos(\alpha/2)^2 - \sin(\alpha/2)^2 = \cos(\alpha)$ and $2\cos(\alpha/2)\sin(\alpha/2) = \sin(\alpha)$ for any $\alpha \in \mathbb{R}$.

(b) What will be their corresponding standard deviations? Recall from the lecture that the standard deviation of an observable M is defined as $\Delta M = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$, with $\langle A\rangle \equiv \langle\psi|\,A\,|\psi\rangle$ for any observable A.

(c) Evaluate the commutator $[Z, X]$ and its expectation value $\langle\psi|\,[Z, X]\,|\psi\rangle$.

(d) Insert your results and explicitly verify that the Heisenberg uncertainty principle is satisfied.

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] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), page 532

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

6-1) a-) Measuring Z means that

in Bloch sphere we projecting Z to z axis which can be represented by r_z

Also measuring X is projecting into x axis represented by r_x

$$\boxed{\langle Z \rangle = r_z} \qquad \boxed{\langle X \rangle = r_x}$$

b-)

$$\Delta Z = \sqrt{\langle Z^2 \rangle - \langle Z \rangle^2}, \quad Z^2 = I, \quad \langle Z \rangle = r_z$$

$$\Delta Z = \boxed{\sqrt{1 - r_z^2}}$$

similarly,

$$\Delta X = \boxed{\sqrt{1 - r_x^2}}, \quad X^2 = I, \quad \langle X \rangle = r_x$$

c-)

$$[Z,X] = ZX - XZ$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} = 2iY$$

Expectation values of X, Z $\langle \psi | [Z,X] | \psi \rangle$

$$= \langle \psi | 2iY | \psi \rangle = \boxed{2i r_y}$$

d-) Heisenberg uncertainty can be written as follows,

$$\Delta(Z) \, \Delta(X) \geq \frac{|\langle \psi | [Z,X] | \psi \rangle|}{2}$$

$$= \sqrt{1 - r_z^2} \cdot \sqrt{1 - r_x^2} \geq \frac{|\cancel{2} i r_y|}{\cancel{2}}$$

$$= (1 - r_z^2) \cdot (1 - r_x^2) \geq r_y^2$$

$$= 1 - r_x^2 - r_z^2 + r_z^2 r_x^2 \geq r_y^2$$

$$= 1 + r_z^2 r_x^2 \geq r_{x_2}^2 + r_{y_2}^2 + r_z^2 \quad \rightarrow 1$$

$$\boxed{1 + r_z^2 r_x^2 \geq 1}$$

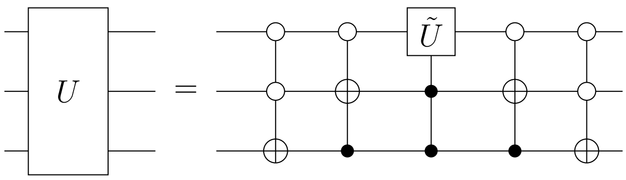
✓

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

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

Exercise 6.2

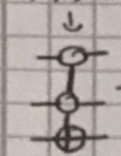
a) $U \Rightarrow \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & & & & & & \\ 0 & & 1 & & & & & \\ 0 & & & 1 & & & & \\ 0 & & & & 1 & & & \\ 0 & & & & & 1 & & \\ 0 & & & & & & 1 & \\ b & & & & & & & d \end{pmatrix}$ and $|\psi\rangle \Rightarrow$ arbitrary $\begin{pmatrix} 1 \to x_0 \\ 1 \to x_1 \\ 1 \to x_2 \\ 1 \to x_3 \\ 1 \to x_4 \\ 1 \to x_5 \\ 1 \to x_6 \\ 1 \to x_7 \end{pmatrix} =$

$$U|\psi\rangle = (ax_0 + cx_7)|000\rangle + x_1|001\rangle + x_2|010\rangle + x_3|011\rangle + x_4|100\rangle$$
$$+ x_5|101\rangle + x_6|110\rangle + (bx_0 + dx_7)|111\rangle$$

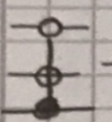
Now we can start applying the gates on the circuit to the arbitrary state and check if they're equivalent to each other.

coefficients x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7

$|\psi\rangle = |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$

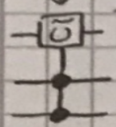


$\rightarrow |\psi_1\rangle = |001\rangle + |000\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$



$\rightarrow |\psi_2\rangle = |011\rangle + |000\rangle + |010\rangle + |001\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$

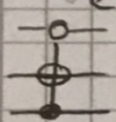
we apply $\tilde{U}$ gate if 2nd and 3rd control bits are 1, coefficients are same with the first row



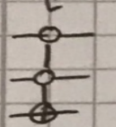
$\Rightarrow |\psi_3\rangle = \underset{x_0}{(\tilde{U}|0\rangle)|11\rangle} + |000\rangle + |010\rangle + |001\rangle + |100\rangle + |101\rangle + |110\rangle + \underset{x_7}{(\tilde{U}|1\rangle)|11\rangle}$

$(x_0 a|011\rangle + x_0 b|111\rangle)$ $(x_7 c|011\rangle + x_7 d|111\rangle)$

$|\psi_3\rangle = (ax_0 + cx_7)|011\rangle + x_1|000\rangle + x_2|010\rangle + x_3|001\rangle + x_4|100\rangle + x_5|101\rangle + x_6|110\rangle + (dx_7 + bx_0)|111\rangle$



$\Rightarrow |\psi_4\rangle = (ax_0 + cx_7)|001\rangle + x_1|000\rangle + x_2|010\rangle + x_3|011\rangle + x_4|100\rangle + x_5|101\rangle + x_6|110\rangle + (bx_0 + dx_7)|111\rangle$



$\Rightarrow |\psi_5\rangle = (ax_0 + cx_7)|000\rangle + x_1|001\rangle + x_2|010\rangle + x_3|011\rangle + x_4|100\rangle + x_5|101\rangle$
$+ x_6|110\rangle + (bx_0 + dx_7)|111\rangle.$

Then we can see the result $|\psi\rangle_5$ is same with $U|\psi\rangle$ that we found at the beginning so they are equivalent.

b-) Any unitary can be written as $U = e^{i\alpha} AXBXC$ where A, B, C are single qubit operations such that $ABC = I$

Also we know that we can write controlled flips as Toffoli gates and Pauli X gates.

c) New U is similar to the one in the problem statement only difference is that instead of $|000\rangle$, $|010\rangle$ is affected by it.

We can use a part of the first circuit and flip the gates for the 2nd and 3rd bit.