Quantum Information   Spring 2023   Problem Set 3

Solutions are due on Sunday May 8, 23:59.

1. **Quantum teleportation (programming)**
   In this problem you will implement the quantum teleportation protocol using Qiskit. You can use the template notebook “teleportation.ipynb” which you can find on the MyCourses page. Follow the notebook and fill in the missing parts. I recommend using `jupyter.cs.aalto.fi`. Return your answer as a .ipynb-notebook (you can download the notebook from JupyterHub if you used the department cloud installation.)
   Solution.
   See “teleportation_solution.ipynb”.

2. **Grover search on two qubits (programming)**
   This time you will implement the Grover search algorithm. Use the template “grover.ipynb” and fill in the missing parts which are:

   - Implementation of the oracle
   - Implementation of the phase flip
   - The correct number of Grover iterations

   Solution.
   See “grover_solution.ipynb”.

3. **Grover iteration**
   Recall the definitions

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle \tag{1}$$

$$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle \ , \tag{2}$$

   where $\sum_x{}'$ is a sum over all solutions to the search problem and $\sum_x{}''$ is a sum over x which are not solutions. Show that in the $|\alpha\rangle$, $|\beta\rangle$ basis, we may write the Grover iteration as

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ , \tag{3}$$

   where θ is a real number in the range 0 to $\pi/2$ chosen so that

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N} \ . \tag{4}$$

You can assume for simplicity that $M \leq N/2$.
Solution.
The equally weighted superposition over the search space can be written as a linear combination of $|\alpha\rangle$ and $|\beta\rangle$.

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} {\sum_x}' |x\rangle + \frac{1}{\sqrt{N}} {\sum_x}'' |x\rangle \tag{5}$$

$$= \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \ . \tag{6}$$

In this basis, the oracle can be written as

$$O = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta| \ , \tag{7}$$

since this marks the solutions $|\beta\rangle$ and leaves non-solutions $|\alpha\rangle$ invariant. The Grover iteration is therefore

$$G = (2|\psi\rangle\langle\psi| - \mathbb{I})O \tag{8}$$

$$= \left[2\left(\sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle\right)\left(\sqrt{\frac{N-M}{N}} \langle\alpha| + \sqrt{\frac{M}{N}} \langle\beta|\right) - \mathbb{I}\right] O \tag{9}$$

$$= \frac{N-2M}{N} |\alpha\rangle\langle\alpha| - \frac{2\sqrt{M(N-M)}}{N} |\alpha\rangle\langle\beta| \tag{10}$$

$$+ \frac{2\sqrt{M(N-M)}}{N} |\beta\rangle\langle\alpha| + \frac{N-2M}{N} |\beta\rangle\langle\beta| \tag{11}$$

$$= \begin{pmatrix} \frac{N-2M}{N} & -\frac{2\sqrt{M(N-M)}}{N} \\ \frac{2\sqrt{M(N-M)}}{N} & \frac{N-2M}{N} \end{pmatrix} \ . \tag{12}$$

Now since we may assume $M \leq N/2$, then for some real number $\theta \in [0, \pi/2]$

$$\frac{N-2M}{N} = \cos\theta \qquad \frac{2\sqrt{M(N-M)}}{N} = \sin\theta \ . \tag{13}$$

This means that we can write the Grover iteration as

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ . \tag{14}$$

4. **Circuit identities**
Show that the following circuit identities hold. Subscripts denote on which qubit a gate acts and C denotes the CNOT-gate with the first qubit as control and the second qubit as target.

(a) $CX_1C = X_1X_2$

Solution.

Since the controls are on the first qubit, it is useful to study the action of the LHS on states $|0\rangle |\psi\rangle$ and $|1\rangle |\psi\rangle$ for some arbitrary state $|\psi\rangle$ on the second qubit.

$$\begin{aligned} CX_1C\,|0\rangle \otimes |\psi\rangle &= CX_1\,|0\rangle \otimes |\psi\rangle = C\,|1\rangle \otimes |\psi\rangle = |1\rangle \otimes X\,|\psi\rangle && (15)\\ &= (X \otimes X)\,|0\rangle \otimes |\psi\rangle = X_1X_2\,|0\rangle \otimes |\psi\rangle && (16)\\ CX_1C\,|1\rangle \otimes |\psi\rangle &= CX_1\,|1\rangle \otimes X\,|\psi\rangle = C\,|0\rangle \otimes X\,|\psi\rangle && (17)\\ &= |0\rangle \otimes X\,|\psi\rangle = (X \otimes X)\,|1\rangle \otimes |\psi\rangle && (18)\\ &= X_1X_2\,|1\rangle \otimes |\psi\rangle \ . && (19) \end{aligned}$$

Since any state can be written as a linear combination of $|0\rangle \otimes |\psi\rangle$ and $|1\rangle \otimes |\psi\rangle$, it follows that $CX_1C = X_1X_2$.

(b) $CZ_1C = Z_1$

Solution.

Let's use the same method again

$$\begin{aligned} CZ_1C\,|0\rangle \otimes |\psi\rangle &= CZ_1\,|0\rangle \otimes |\psi\rangle = C\,|0\rangle \otimes |\psi\rangle = |0\rangle \otimes |\psi\rangle && (20)\\ &= Z_1\,|0\rangle \otimes |\psi\rangle && (21)\\ CZ_1C\,|1\rangle \otimes |\psi\rangle &= CZ_1\,|1\rangle \otimes X\,|\psi\rangle = -C\,|1\rangle \otimes X\,|\psi\rangle && (22)\\ &= -\,|1\rangle \otimes X^2\,|\psi\rangle = -\,|1\rangle \otimes |\psi\rangle = Z_1\,|1\rangle \otimes |\psi\rangle \ . && (23) \end{aligned}$$

(c) $CY_1C = Y_1X_2$

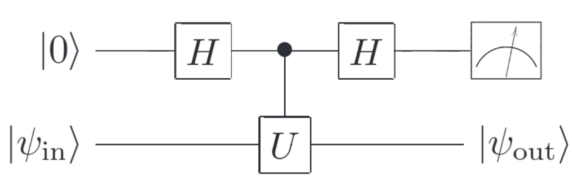
Solution.

We'll show this part by using the previous two identities, $C^2 = \mathbb{I}$, and $Y = iXZ$. Therefore,

$$CY_1C = iCX_1Z_1C = iCX_1CCZ_1C = iX_1X_2Z_1 = Y_1X_2 \ . \qquad (24)$$

5. **Measuring an operator**

Suppose we have a single qubit operator U with eigenvalues ± 1, so that U is both Hermitian and unitary, so it can be regarded both as an observable and a quantum gate. Suppose we wish to measure the observable U. That is, we desire to obtain a measurement result indicating one of the two eigenvalues, and leaving a post-measurement state which is the corresponding eigenvector. Show that the following circuit implements a measurement of U:



Solution.
The operator U has the spectral decomposition $U = |a\rangle\langle a| - |b\rangle\langle b|$, where $|a\rangle$ ($|b\rangle$) is the eigenstate with eigenvalue $+1$ (-1). Then we can express the second qubit in this basis as $|\psi_{in}\rangle = \alpha\,|a\rangle + \beta\,|b\rangle$. The initial state is then

$$|0\rangle \otimes |\psi_{in}\rangle = |0\rangle \otimes (\alpha\,|a\rangle + \beta\,|b\rangle)\ . \tag{25}$$

After the first Hadamard, the state is

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (\alpha\,|a\rangle + \beta\,|b\rangle) && (26)\\ &= \frac{1}{\sqrt{2}}\,|0\rangle \otimes (\alpha\,|a\rangle + \beta\,|b\rangle) + \frac{1}{\sqrt{2}}\,|1\rangle \otimes (\alpha\,|a\rangle + \beta\,|b\rangle)\ . && (27) \end{aligned}$$

Then we apply the controlled U

$$\begin{aligned} &\frac{1}{\sqrt{2}}\,|0\rangle \otimes (\alpha\,|a\rangle + \beta\,|b\rangle) + \frac{1}{\sqrt{2}}\,|1\rangle \otimes (\alpha U\,|a\rangle + \beta U\,|b\rangle) && (28)\\ &= \frac{1}{\sqrt{2}}\,|0\rangle \otimes (\alpha\,|a\rangle + \beta\,|b\rangle) + \frac{1}{\sqrt{2}}\,|1\rangle \otimes (\alpha\,|a\rangle - \beta\,|b\rangle) && (29)\\ &= \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |a\rangle + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |b\rangle\ . && (30) \end{aligned}$$

After the second Hadamard we have

$$\alpha\,|0\rangle \otimes |a\rangle + \beta\,|1\rangle \otimes |b\rangle\ . \tag{31}$$

Finally we measure Z on the first qubit. We can see that the measurement result is $+1$ with probability $|\alpha|^2$ leaving the second qubit in state $|a\rangle$. On the other hand the measurement result -1 occurs with probability $|\beta|^2$ and leaves the second qubit in the state $|b\rangle$. Therefore the given circuit can be used to measure U.