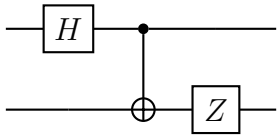
- Each student should provide and come up with their solutions independently.
- You are allowed to use any literature/source you want, but don't forget to add references when required.
- There are 5 problems in total.

Problem 1. (*Basic math & circuit evaluation*).

1. Consider the following two qubit quantum circuit.



   (a) Compute the matrix corresponding to the above circuit.

   (b) Compute the output state of the circuit on input $|01\rangle$.

   (c) Compute the probability of measuring $|00\rangle$ from the circuit, given input $|10\rangle$.

2. Recall that $|u\rangle \in \mathbb{C}^n$ is an eigenvector of a unitary U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U|u\rangle = \omega_u |u\rangle .$$

   (a) Consider the unitary $CNOT \cdot (H \otimes Z) \cdot CNOT$. Compute the eigenvectors and eigenvalues.

   Remark. *By noting that $CNOT = CNOT^{-1}$, you may simplify your life a lot..*

   (b) (H) Consider the unitary $H \cdot Z_{\pi/2} \cdot H \cdot Z$, where

$$Z_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{1}$$

   Compute the eigenvectors and eigenvalues of the corresponding unitary.

3. Consider the following basis

$$\left\{ |a\rangle = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix}, |b\rangle = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{3}} \\ \frac{-1}{\sqrt{3}} \end{pmatrix} \right\}.$$

   (a) Show that it is an *orthonormal* basis.

   (b) Compute the probabilities of all possible outcomes when measuring the state

$$|\psi\rangle = \left(H \cdot Z_{\pi/2} \cdot H\right)|0\rangle$$

   in the computational basis $\{|0\rangle, |1\rangle\}$ (see Equation 1 for definition of $Z_{\pi/2}$).

   (c) Compute the probabilities of all possible outcomes when measuring this same state $|\psi\rangle$, but this time in the basis given by $\{|a\rangle, |b\rangle\}$.

Problem 2. (*Relative phase vs. Global phase*).
Write down any circuit on 2 qubits that only involves CNOTs, Hadamards and other single qubit gates. Use 3-5 gates in total and use at least 2 distinct gates. Let U be the unitary corresponding to this circuit.

Next, choose a measurement basis $M = \{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle\}$ (any basis works; the computational basis is fine), and an arbitrary outcome $i \in \{1, 2, 3, 4\}$ associated with one of the previously chosen basis vectors $|\phi_i\rangle$.

Global phase:

1. Compute the probability of seeing outcome i if you measure the state $U|11\rangle$ in the basis given by M.

Now consider the unitary U' obtained by exchanging any single qubit gate V that appears in your chosen U, by the gate $e^{i\theta}V$, with $\theta \in (0, 2\pi)$.

2. Compute the probability of seeing outcome i if you measure the state $U'|11\rangle$ in the basis given by M.

Remark. *If you have done the exercise correctly, you will note that the choice of the angle θ never influences the measurement outcomes – no matter what measurement you chose.*

Consider the unitary $\widetilde{U}$ obtained by exchanging the single qubit gate V in your previously chosen U with a "controlled-V". The matrix of a controlled-W, for *any* single qubit gate W is given by the block matrix

$$\begin{pmatrix} I_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & W \end{pmatrix},$$

where I_2 denotes the 2×2 identity matrix and $\mathbf{0}_2$ denotes the 2×2 matrix with zero entries.

Relative phase:

1. Compute the probability of seeing outcome i if you measure the state $\widetilde{U}|11\rangle$ in the basis given by M.

Now consider the unitary $\widetilde{U}'$ obtained by exchanging the controlled-V in the circuit $\widetilde{U}$ by a "controlled-$[e^{i\theta}V]$".

2. Compute the probability of seeing outcome i if you measure the state $\widetilde{U}'|11\rangle$ in the basis given by M.

Remark. *If you have done the exercise correctly, you may see that now the angle θ can influence measurement outcomes – it is no longer a global phase. Global phase is an artefact of the fact that the mathematical representation using standard vector spaces is overcomplete. By overcomplete we mean that it has elements which do not correspond to physical reality. For example, the states $|\phi\rangle$ and $e^{i\theta}|\phi\rangle$ are two distinct representations of the* **same** *physical state, and the unitaries U and $e^{i\theta}U$ are two distinct representations of the* **same** *physical evolution.*

Problem 3. (*Circuit logic*).
Recall that one can construct the Toffoli gate (i.e., the control-control-NOT gate) using a couple of CNOTs and other single qubit gates – see page 183 of Nielsen & Chuang.

Using ancillary qubits (i.e., fresh qubits, that you can preset to a desired value, and afterwards discard) one can construct k-controlled-NOT gates from Toffoli gates, applying a NOT (i.e., the X-gate) only if certain k qubits are in the state $|1\rangle$.

1. Construct such a three-qubit controlled NOT, so a controlled-Toffoli gate, using one ancillary qubit.

   Remark. *This circuit will use 5 wires, 4 of which are used to implement the actual controlled-Toffoli gate.*

2. Generalize this construction to a k-controlled-NOT gate. How many ancilla qubits does your construction take? How many Toffoli gates are required?

Remark. *Interestingly we can generate the k-controlled-Toffoli* **without any ancillas**. *For the interested student see:* `https://cs.stackexchange.com/questions/40933/creating-bigger-controlled-nots-from-single-qubit-toffoli-and-cnot-gates-with`.

Problem 4. (*quantum Fourier transform & quantum phase estimation*).

1. Compute the matrix corresponding to the inverse of the 2 qubit QFT and provide the circuit. Make sure to define every gate you use.
2. Compute matrix $U = H \cdot Z_{\pi/2} \cdot H$ (see Equation 1 of Problem 1 for definition of $Z_{\pi/2}$).
3. Give the circuit that applies QPE of U using two qubits in the eigenvalue register.
4. Give the vector-representation of the output of the above circuit when applied onto the initial state $|0\rangle\,|0\rangle\,|-\rangle$.
5. Compute the same by evolving the state $|0\rangle\,|0\rangle\,|-\rangle$ in the braket-notation.

Problem 5. (*Quantum algorithms*).

1. A number $N \in \mathbb{Z}_{>0}$ is called w-smooth if all prime numbers p that divide N satisfy $p \leq w$ (i.e., N only has prime divisors less than or equal to w).

   Show how to use Grover's algorithm to find a factor of a w-smooth number N using

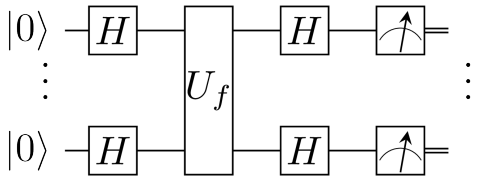
   $$O\left(\sqrt{\frac{w}{\#\{a \leq w \mid a \text{ divides } N\}}}\right) = O\left(\sqrt{\frac{w \log w}{\log N}}\right)$$

   queries to the oracle $O_N : |a\rangle \mapsto (-1)^{\delta_N(a)} |a\rangle$, where $\delta_N(a) = 1$ if a divides N and $\delta_N(a) = 0$ otherwise.

2. (H) Consider the "Bernstein-Vazirani problem" given by the following.
   Input: A function $f : \{0,1\}^n \to \{0,1\}$ with the promise that there exists some (secret) bitstring $s \in \{0,1\}^n$ such that

   $$f(a) = \left(\sum_{i=1}^{n} a_i s_i\right) \mod 2, \text{ for all } a \in \{0,1\}^n.$$

   Output: The bitstring s.
   Show how to solve the Bernstein-Vazirani problem using the following quantum circuit

   where the unitary U_f denotes the "phase-oracle" which maps $|i\rangle \mapsto (-1)^{f(i)} |i\rangle$.