# Quantum Computing (CS5100) : Problem Set 2

Department of Computer Science and Engineering
IIT Hyderabad

Deadline: Oct. 17, 2024 before 16:00PM

**Please read the following comments before you work on the problems.**

- Plagiarism leads to **F** grade and a meeting with disciplinary committee!
- Assignments after the deadline will not be accepted at any cost. So plan for your internet outages etc. beforehand. You may submit a hard copy as well.
- All problems builds on what has been taught in the class. Try to attempt them all.

---

1. Construct a CNOT gate from two Hadamard gates and one controlled-$Z$ gate. Recall, the controlled-$Z$ gate maps $|11\rangle \to -|11\rangle$ and acts like the identity on the other basis states. **(10 marks)**

2. A SWAP-gate interchanges two qubits, i.e., it maps basis state $|a, b\rangle$ to $|b, a\rangle$. Implement a SWAP-gate using only CNOT gates. When using a CNOT, you're allowed to use either of the 2 bits as the control, but be explicit about this. **(10 marks)**

3. Let $U$ be a 1-qubit unitary that we would like to implement in a controlled way, i.e., we want to implement the map $|c\rangle|b\rangle \mapsto |c\rangle U^c|b\rangle$ for all $c, b \in \{0, 1\}$ (here $U^0 = I$ and $U^1 = U$). Suppose there exist 1-qubit unitaries $A$, $B$, and $C$, such that $ABC = I$ and $AXBXC = U$, where $X$ is the NOT-gate. Give a circuit that acts on two qubits and implements a controlled-$U$ gate, using CNOTs and (uncontrolled) $A$, $B$, and $C$ gates. **(10 marks)**

4. Let $C$ be a given quantum circuit consisting of $T$ many gates, which may be CNOTs and single-qubit gates. Show that we can implement $C$ in a controlled way using $O(T)$ Toffoli gates, CNOTs and single-qubit gates, and no auxiliary qubits other than the controlling qubit. **(10 marks)**

5. Recall we can apply a standard query $O_x$ to bitstring $x \in \{0, 1\}^N$ in the usual form:

$$O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle.$$

Give a circuit, involving one application of $O_x$ and some other gates, to implement the following controlled-phase-query:

$$C_x\colon |c, i, 0\rangle \mapsto (-1)^{cx_i}|c, i, 0\rangle.$$

The idea here is that we implement a phase-query to $x$, but only in case the control-qubit ($c \in \{0, 1\}$) is set to 1. **(10 marks)**

6. Show that a standard query $O_x$ can be implemented using one controlled-phase-query to $x$ (which maps $|c, i\rangle \mapsto (-1)^{cx_i}|c, i\rangle$, so the phase is added only if the control bit is $c = 1$), and possibly some auxiliary qubits and other gates. **(10 marks)**

7. Give a circuit that maps $|0^n, b\rangle \mapsto |0^n, 1 \oplus b\rangle$ for $b \in \{0, 1\}$, and that maps $|i, b\rangle \mapsto |i, b\rangle$ whenever $i \in \{0, 1\}^n \setminus \{0^n\}$. You are allowed to use elementary gates, including Toffoli gates, as well as auxiliary qubits that are initially $|0\rangle$ and that should be put back to $|0\rangle$ at the end of the computation. **(10 marks)**

8. Suppose we can make queries of the type $|i, b\rangle \mapsto |i, b \oplus x_i\rangle$ to input $x \in \{0, 1\}^N$, with $N = 2^n$. Let $x'$ be the input $x$ with its first bit flipped (e.g., if $x = 0110$ then $x' = 1110$). Give a circuit that implements a query to $x'$. Your circuit may use one query to $x$. **(10 marks)**

9. Suppose our $N$-bit input $x$ satisfies the following promise: either (1) the first $N/2$ bits of $x$ are all 0 and the second $N/2$ bits are all 1; or (2) the number of 1s in the first half of $x$ plus the number of 0s in the second half, equals $N/2$. Modify the Deutsch-Jozsa algorithm to efficiently distinguish these two cases (1) and (2). **(10 marks)**

10. Consider the following generalization of Simon's problem: the input is $x = (x_0, \ldots, x_{N-1})$, with $N = 2^n$ and $x_i \in \{0, 1\}^n$ with the property that there is some unknown *subspace* $V \subseteq \{0, 1\}^n$ (where $\{0, 1\}^n$ is the vector space of $n$-bit strings with entrywise addition modulo 2) such that $x_i = x_j$ iff there exists a $v \in V$ such that $i = j \oplus v$. The usual definition of Simon's problem corresponds to the case of 1-dimensional subspace $V = \{0, s\}$.

    Show that one run of Simon's algorithm now produces a $j \in \{0, 1\}^n$ that is orthogonal to the whole subspace (i.e., $j \cdot v = 0 \bmod 2$ for every $v \in V$). **(10 marks)**