Introduction to Quantum Computation (67596) 2021
Final Project

Submit your work by uploading it via the submission link on the course Moodle website.
Please direct any questions or requests for clarifications directly to me at benor@cs.huji.ac.il.
The strict submission deadline is **December 1, 2021**, but the suggested deadline is early **September 2021**.
Please provide exact references to whatever you submit that is not strictly yours [e.g. Section 2.1 of Reference1, or if you used someone's help then state "Solution suggested by X", or "joint work with Y"]. In any case the submitted work should be written solely by you, and you should be able and ready to explain whatever you submit.

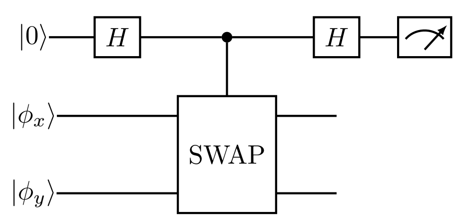
1. **Quantum Communication Complexity of Disjointness:** Consider the following communication problem. As inputs Alice gets an x and Bob get a y, where $x, y \in \{0,1\}^n$, and by exchanging information they what to determine if there is an index k with $x_k = y_k = 1$ or not. In other words, if x encodes the set $A = \{k \mid x_k = 1\}$, and y encodes $B = \{k \mid y_k = 1\}$, then Alice and Bob want to determine whether $A \cap B$ is empty or not. The classical randomized communication complexity of this problem is $\Theta(n)$.

   Assuming Alice and Bob can exchange quantum messages, show how Alice and bob can solve the task correctly with probability greater than 2/3 by exchanging at most $O(\sqrt{n}\log n)$ qubits.

   Hint: Show that Alice and Bob can implement the oracle $O\,|k\rangle = (-1)^{x_k \cdot y_k}\,|k\rangle$ exchanging $O(\log n)$ qubits, and use Grover's search.

2. **Quantum Fingerprinting:** First some preliminaries:

   (P1) Consider the following "Swap Test": Given two states $|\phi_x\rangle, |\phi_y\rangle$ in some Hilbert space $\mathcal{H}$, show that the probability of measuring a 0 outcome in the following quantum circuit is $(1 + |\langle\phi_x|\phi_y\rangle|^2)/2$.

   where $\text{SWAP}\,|\phi_x\rangle|\phi_y\rangle = |\phi_y\rangle|\phi_x\rangle$.

   (P2) Let $\mathcal{H}$ be a Hilbert space of dimension m. Show that one find exponentially many "almost orthogonal" states in $\mathcal{H}$. Namely, for any $\epsilon > 0$ there is a constant $c = c(\epsilon) > 0$, and states $|\phi_k\rangle$, $k = 1, \ldots, 2^{cm}$, such that for all $k \neq j$ we have $|\langle\phi_k|\phi_j\rangle| < \epsilon$. Hint: Pick $|\phi_k\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m} X_i\,|i\rangle$ where the X_i are independent random variables with $\text{Prob}(X_i = \pm 1) = 1/2$, and use the Chernoff bound.

   Now consider the following simultaneous communication problem. Alice and Bob do not share any entanglement or any common randomness, and cannot communicate directly with each other. As inputs, x is given to Alice, and y is given to Bob, where $x, y \in \{0,1\}^n$. Based on their inputs Alice and Bob can each send a single message to a referee R that has to decide whether $x = y$ or not.

   (a) Give a quantum protocol where Alice and Bob each send to R a quantum state on $O(\log n)$ qubits and the error probability of R is at most 1/100. Hint: Fix $\epsilon = 1/2$ and use (P1) with the states from (P2) for $m = n/c(\epsilon)$.

   (b) What is the complexity of the quantum circuits that are needed for Alice, Bob and referee R, to implement the protocol suggested in (a)? Explain/Prove why.

(c) (Optional) Describe an efficient (polynomial time complexity) protocol with $O(\log n)$ qubits messages from Alice and Bob to R. Hint: You can use a simple classical code (not necessarily binary) with 2^n codewords, that has a good distance (and a reasonable, even if not optimal, rate).

Note: There is a classical randomized algorithm where Alice and Bob each send to R a message of size $O(\sqrt{n})$ and R's error probability is at most $1/100$ (This is known to be optimal).

3. **Pick a Paper:** Select a paper that was presented at one of the recent Quantum Information Processing workshops (see QIP-2021, QIP-2020, and QIP-2019), or quantum computation related talks presented at recent STOC or FOCS (see STOC-2021, STOC-2020, STOC-2019, FOCS-2020, FOCS-2019), or a recent quantum computation related Science or Nature journal paper. Please send your selection to me by email at benor@cs.huji.ac.il for approval (on a first come basis). Many of those papers are quite long and selecting parts of a paper to review may be reasonable. Write a short summary that explains the main results of the paper emphasizing why this is interesting, what are the proof techniques, and if applicable what is left open. Limit your review to at most 4 pages. You can also prepare and submit just a public link to a short (up to 15min) video presentation of the paper if you wish to do so.

   Note: A list of the approved papers will be updated on the course Moodle website. Please consult that list before sending your selected paper for approval to verify that the paper hasn't been already selected by another student.