Quantum Circuits and Simulation Problem Set

Reminders

 $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ $-\boxed{H}- = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $-\boxed{T}- = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Problems

1. The Bell basis is

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \\ \left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right) \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle\right) \\ \left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right). \end{aligned}$$

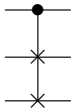
   This is an orthonormal basis for the state space of two qubits. It is named after John Bell's tests of local realism, and finds numerous applications in quantum information. Find a quantum circuit that implements the unitary change-of-basis from the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ to the Bell basis.

2. Suppose you have an efficient quantum circuit to simulate the time-evolution induced by a Hamiltonian of the form

$$H = \begin{bmatrix} 0 & U \\ U^\dagger & 0 \end{bmatrix}$$

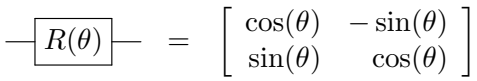
   where U is a $2^n \times 2^n$ unitary matrix. (That is, you can implement the transformation e^{-iHt} on $n+1$ qubits using $\text{poly}(n,t)$ quantum gates.) Use this primitive to construct a quantum circuit implementing U. You may ignore global phase and the action on any ancilla qubits.

3. The Fredkin gate is a controlled-SWAP.

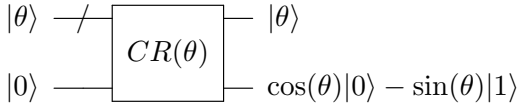
circuit symbol	truth-table
	$000 \to 000$ $001 \to 001$ $010 \to 010$ $011 \to 011$ $100 \to 100$ $101 \to 110$ $110 \to 101$ $111 \to 111$

Prove that the Fredkin gate by itself (but with access to arbitrarily initialized ancilla bits) can perform universal classical computation. *Hint:* you can do this by showing how to simulate a classical gate set that is known to be universal such as $\{\text{NOT}, \text{AND}\}$, $\{\text{NAND}\}$, or $\{\text{NOT}, \text{OR}\}$.

4. (a) Let $R(\theta)$ denote the single-qubit rotation

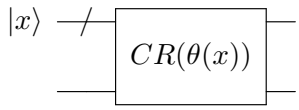


Consider the conditional-rotation unitary, which given a number θ written to n bits of precision in the control register, rotates the target qubit by angle θ.



Show how to make the conditional-rotation using $O(n)$ elementary quantum gates. You may consider your gate set to consist of all single-qubit and 2-qubit gates. (These could in turn be efficiently approximated using standard universal gate sets such as {Hadamard, CNOT, T}. However, let's not explicitly do so.)

(b) Given $x \in \{0,1\}^n$, suppose $\theta(x)$ can be computed by some efficient classical algorithm. Using reversible computing and conditional-rotations, show how to implement the following unitary. You may use polynomially many ancilla qubits to store intermediate results, but you must erase them at the end. (Otherwise, on superpositions of different inputs $\sum_x |x\rangle$ entanglement will be created with the ancilla qubits, thereby ruining the coherence.)



(c) Let $p : \{0,1\}^n \to \mathbb{R}$ be a probability distribution over the bit strings of length n. Suppose, you have an efficient classical algorithm which, for any $x_n, \ldots, x_1 \in \{0,1\}$ computes the conditional probability $p(x_n | x_{n-1} \ldots x_1)$. Using this, and the result from part b, construct an efficient quantum circuit that, given the state:

$$\sum_{x_{n-1},\ldots,x_1 \in \{0,1\}} \sqrt{p(x_{n-1},\ldots,x_1)} |x_{n-1},\ldots,x_1\rangle$$

(where $p(x_{n-1}, \ldots, x_1)$ is the marginal probability distribution induced by p) produces $\sum_{x\in\{0,1\}^n} \sqrt{p(x)}|x\rangle$.

(d) Suppose you have efficient classical algorithms to compute all of the conditional probability distributions $p(x_j|x_{j-1}\ldots x_1)$. Use this to construct an efficient quantum circuit producing $\sum_{x\in\{0,1\}^n} \sqrt{p(x)}|x\rangle$ from scratch.

5. **Fun bonus problem:** Consider the game guess-my-bitstring: an oracle contains a secret string $a \in \{0,1\}^n$. You can query the oracle with a guess $x \in \{0,1\}^n$ and the oracle will tell you how many bits you got wrong (*i.e.* the Hamming distance between a and x).

(a) Show that classically, one needs at least of order $n/\log_2 n$ queries to determine the secret string $a \in \{0,1\}^n$. Also, show that one can solve this classically using order n queries.

(b) For bitstrings $x, y \in \{0,1\}^n$ let $|x-y|$ denote the number of places they differ ("Hamming distance"). Show that

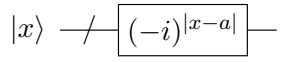
$$\sum_{x\in\{0,1\}^n} (-i)^{|a-x|}(i)^{|x-y|} = \begin{cases} 2^n & \text{if } y = a \\ 0 & \text{otherwise} \end{cases}$$

where $i = \sqrt{-1}$.

(c) Let M be the following unitary single-qubit gate

$$M = \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

Let



denote a quantum oracle that, given input $x \in \{0,1\}^n$, induces a phase $(-i)^{|x-a|}$. (If $|x-a|$ is computable by an efficient classical algorithm then such an oracle can always be built using reversible computing and phase kickback.) Using the result of part b, show that the following quantum circuit solves guess-my-bitstring using a single quantum query.