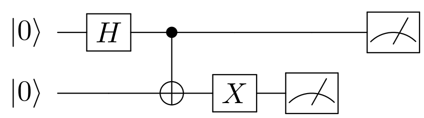
COMS 4281 - Introduction to Quantum Computing Fall 2024

Practice Worksheet 4

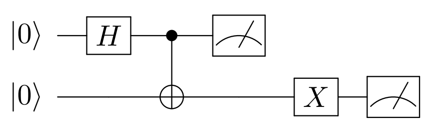
This practice worksheet is intended to act as a review sheet for the midterm as well as give some practice for the more recently covered material. The midterm and final exam will have questions inspired by the worksheets.

Problem 1: Quantum Information

(a) Consider the following two circuits. Assume all measurements take place in the standard basis.



What are the measurement probabilities if the first qubit is measured as the final operation in the circuit? Find the post-measurement state after the second qubit is measured, and then calculate the first qubit's measurement probabilities.



In the above circuit, the first qubit's measurement occurs before the X gate and the second qubit's measurement, so logically the first measurement cannot depend on those operations at all. Show that first qubit's measurement statistics in this circuit are the same as before.

(b) Alice has a quantum state $|\psi\rangle$. She measures $|\psi\rangle$ in the standard basis and gets $|0\rangle$. If she immediately makes another measurement in the Hadamard basis, what are her measurement probabilities? What if she first measured in the Hadamard basis, got $|+\rangle$, and then measured in the standard basis? Relate these results to the Uncertainty Principle.

Problem 2: Basic Circuits

(a) Draw a circuit that takes in three qubits in the $|000\rangle$ state and outputs the equal superposition given by

$$|\psi\rangle = \frac{1}{2^{3/2}} \sum_{x=0}^{2^3-1} |x\rangle \, .$$

(b) Draw a circuit that takes in three qubits in the $|000\rangle$ state and outputs the so-called GHZ state given by

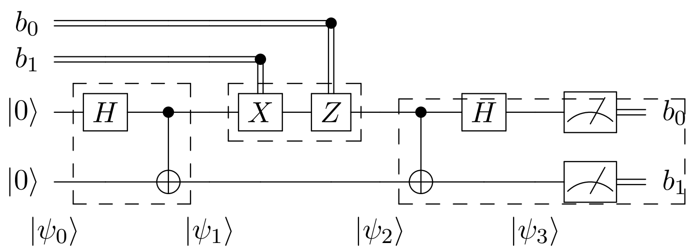
$$|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

(c) For the above two states, what are the measurement probabilities if measuring in the standard basis? What about the Hadamard basis?

Problem 3: Superdense. Supersecret.

In the superdense coding protocol (pictured below), Alice is trying to communicate two classical bits to Bob. Alice and Bob each have half of a pre-shared engtangled pair, together in the state $(|00\rangle + |11\rangle)/\sqrt{2}$. Alice applies one of four operations to her qubit (I, X, Z, XZ) depending on the 2-bit string she wants to send, and then sends her half of the entangled pair to Bob. Bob receives her qubit, applies a fixed circuit, and can recover the bits she sent.

In the below circuit depicting the superdense coding protocol, the first group of operations represents generating the pre-shared entangled pair. The second group represents Alice's operations on her qubit. Then she sends her half of the entangled pair (still entangled even after her operations) to Bob, and the final group of operations represents his circuit to recover the classical bits Alice sent.



Now suppose an eavesdropper Eve intercepts Alice's qubit on its way to Bob (when the pair of qubits is collectively in state $|\psi_2\rangle$). What information can Eve recover about the bits b_0, b_1?

(a) To begin, show that Alice is sending one of the four Bell states $|\beta(b_0, b_1)\rangle$ defined as follows. (Note that this is a slightly unconventional definition of the Bell states; usually the two bits are swapped.)

$$|\beta(b_0, b_1)\rangle := \frac{1}{\sqrt{2}}\Big(|b_1, 0\rangle + (-1)^{b_0}\,|\overline{b_1}, 1\rangle\Big)$$

(b) Assume Eve may perform some unitary operation E on Alice's qubit in state $|\beta(b_0, b_1)\rangle$, and then will measure the qubit after her operation. Show that Eve's measurement probabilities are not dependent on b_0, b_1.

(c) Having shown this, what can we state about the information Eve can extract from Alice's qubit?

Problem 4: Fourier Transform

(a) Write $F_4^\dagger$ (the complex conjugate of F_4 given below)

$$F_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

Note that this is slightly different from the matrix presented in the class slides; this is because here we're using the standard convention of ordering the columns by $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (whereas in the class slides the column ordering is $|00\rangle, |10\rangle, |01\rangle, |11\rangle$ for the sake of revealing the recursive structure of the DFT).

(b) Compute the (i, j)th entry for F_N where $i, j \in [0, N-1]$. For this problem, use the following definition of F_N: it is the unitary matrix that maps the standard basis vector $|j\rangle$ to the Fourier basis vector

$$|f_j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi i j k}{N}\right) |k\rangle \ .$$

Problem 5: Partial Measurements

Consider Alice and Bob's entangled state:

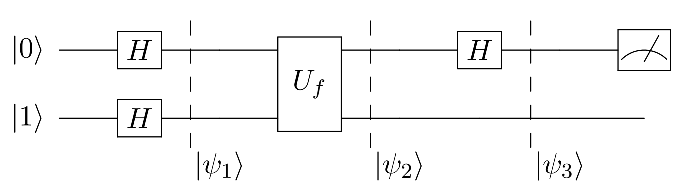
$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|10\rangle + |01\rangle \Big)$$

Suppose Alice measures her qubit using the Hadamard basis $\{|+\rangle, |-\rangle\}$.

(a) What is the distribution of Alice's measurement?

(b) What is Bob's post-measurement state when he is measuring in the computational basis conditioned on Alice getting outcome $|+\rangle$? When she gets outcome $|-\rangle$?

Problem 6: The Deutsch Algorithm



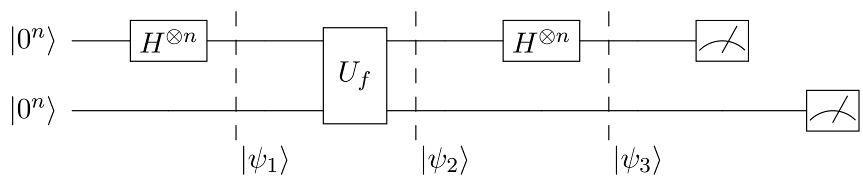
(a) Construct the unitary U_f that corresponds to the function $f : \{0, 1\} \to \{0, 1\}$ defined by $f(0) = 1,\ f(1) = 0$.

(b) Calculate $|\psi_3\rangle$ using the unitary you created. What are the measurement probabilities for the first register?

(c) Redo the previous two steps using a new unitary U_g that corresponds to the function $g : \{0,1\} \to \{0,1\}$ defined by $g(0) = 0$, $g(1) = 1$. What are the measurement probabilities for the first register now?

Problem 7: Simon's Algorithm

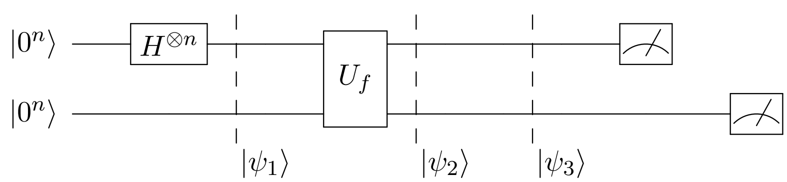
Consider the following circuit



This is different from the one shown in class in that the measurement gate for the second qubit register is delayed until after the time when the first qubit register is measured.

(a) Compute the final state $|\psi_3\rangle$ and the measurement probabilities for the first (top) n-qubit register. Does delaying when the measurement occurs affect the output of the circuit?

(b) What would the distribution of outcomes for the first qubit register be if the final n-qubit Hadamard $H^{\otimes n}$ were omitted as shown below?



(c) Does Simon's algorithm find the hidden secret with 100% probability? Why or why not?

(d) Consider the following classical algorithm for solving Simon's problem: repeatedly generate a random n-bit string x_i, query f to generate $f(x_i)$, and check if it's the same as any previous $f(x_j)$ where $x_i \neq x_j$. If it is, then $x_i \oplus x_j = s$. On average, how many queries to f would we expect to issue before finding the secret s?