CSE 468T Introduction to Quantum Computing **Spring 2022**

Exam II

Given: 27 April 2022 Due: End of class

READ THIS before starting! This exam is open-book, open-notes, open-Internet, but you must do this work on your own without contact or conversations with any person. Because this exam is given in a somewhat distributed manner, no questions will be answered, and no clarifications will be given. State your assumptions and count on us to be fair and flexible, especially if we have been unclear.

Your work must be legible. Work that is difficult to read will receive no credit. There is a blank page at the end if you want to show extra work there.

There are 116 points available for this exam, but it will only be scored out of 100. Extra points earned here will count toward your total exam grade.

You must sign the pledge below for your exam to count. Any cheating will cause the students involved to receive an F for this course. Other unpleasant actions may be taken.

You must fill in your identifying information correctly.

Print clearly the following information:

Name (print clearly):

Student 6-digit ID (print *really* clearly):

Pledge: On my honor, I have neither given nor received any unauthorized aid on this exam.

Signed: ______________________________

(Be sure you filled in your information in the box above!)

1. (30 points) For the **true/false** questions below, indicate your response by marking an **x** in the appropriate box, like this: ☒ **true** ☐ **false** or ☐ **true** ☒ **false**.

   Each response is worth 3 points and there are 6 points of extra credit available here.

   - Deutsch–Jozsa solves a problem in polynomial time on a quantum computer that takes worst-case exponential time on a classical computer. ☐ **true** ☐ **false**
   - With a single query, a classical computer has at least a 50% chance of determining the correct solution to a Deutsch–Jozsa problem. ☐ **true** ☐ **false**
   - An n-bit instance of Bernstein–Vazirani can take $\Theta(2^n)$ time on a classical computer to solve exactly. ☐ **true** ☐ **false**
   - An n-bit instance of Simon's problem can take $\Theta(2^n)$ time on a classical computer to solve exactly. ☐ **true** ☐ **false**
   - If the Deutsch–Jozsa quantum algorithm is presented with an oracle from Bernstein–Vazirani with secret s, then the circuit's measurements will yield a unique result (depends only on s) in the computational basis. ☐ **true** ☐ **false**
   - If the entangled qubits for the CHSH game fail (they decohere and collapse into random values), Alice and Bob can at best win 75% of the time. ☐ **true** ☐ **false**
   - In the Mermin–Peres square, each of Alice's qubits is entangled with one of Bob's qubits. If that entanglement did not exist, the values Alice reports for her assigned rows still multiply to $+1$, as they should. ☐ **true** ☐ **false**
   - In the Mermin–Peres square, each of Alice's qubits is entangled with one of Bob's qubits. If that entanglement did not exist, Alice and Bob would still agree on the value of their shared square, as they should. ☐ **true** ☐ **false**
   - Grover's algorithm provides exponential speedup over classical algorithms that solve the same problem. ☐ **true** ☐ **false**
   - Shor's algorithm provides exponential speedup over the best-known approach for factoring large integers. ☐ **true** ☐ **false**
   - Grover's algorithm can solve the factoring problem as quickly as Shor's algorithm. ☐ **true** ☐ **false**
   - The university course evaluation for this course is worth one of the five points for participation in this class. You agree to complete the evaluation by May 11. ☐ **true** ☐ **false**

2. (10 points) Recall the Mermin–Peres square below.

↓ Bob ↓

		1	2	3
→	1	$\mathbf{Z}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{Z}$	$\mathbf{Z}\otimes\mathbf{Z}$
Alice	2	$\mathbf{I}\otimes\mathbf{X}$	$\mathbf{X}\otimes\mathbf{I}$	$\mathbf{X}\otimes\mathbf{X}$
→	3	$\overline{\mathbf{Z}\otimes\mathbf{X}}$	$\overline{\mathbf{X}\otimes\mathbf{Z}}$	$\mathbf{Y}\otimes\mathbf{Y}$

If Alice measures her qubits as $|00\rangle$ and Bob measures his qubits as $|0+\rangle$, then what results do they report for row and column 1, respectively?

Alice row 1

- Left square ________
- Center square ________
- Right square ________

Bob column 1

- Top square ________
- Middle square ________
- Bottom square ________

In the above scenario, it is possible that Alice measures $|00\rangle$ and Bob measures $|1+\rangle$ □ **true** □ **false**

3. (10 points)

For the Mermin–Peres square problem, suppose Alice and Bob agree before they separate that

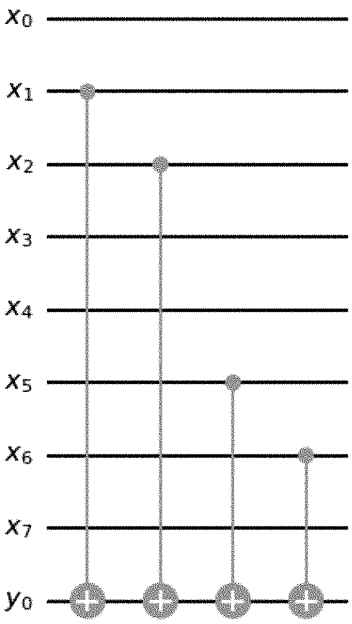
- Alice will follow the protocol exactly as taught in class.
- Bob will follow the protocol as taught in class, except that for each square in his column, he will negate the result he should have reported. Where he should report $+1$, he would report -1; where he should report -1 he will report $+1$.

With this change in protocol

- The values in Alice's assigned row will continue to multiply to $+1$. □ **true** □ **false**
- The values in Bob's assigned column will continue to multiply to -1. □ **true** □ **false**
- In the shared square for Alice and Bob, they will continue to report the same value. □ **true** □ **false**
- In the shared square for Alice and Bob, they are guaranteed to report different values. □ **true** □ **false**

4. **(10 points)** For each question below, fill in the blank. Your answer must appear in the provided blank for proper credit. Write each response in the provided blank space, fully above the dark line. For example, to express $\frac{i}{\sqrt{3}}$ you would write $i/\sqrt{3}$.

   - Consider the oracle portion of a circuit below for an 8-bit instance of the Bernstein–Vazirani problem. Recall the oracle computes $y = x \oplus s$ for a secret bit vector s.

     What is the secret s here? ______

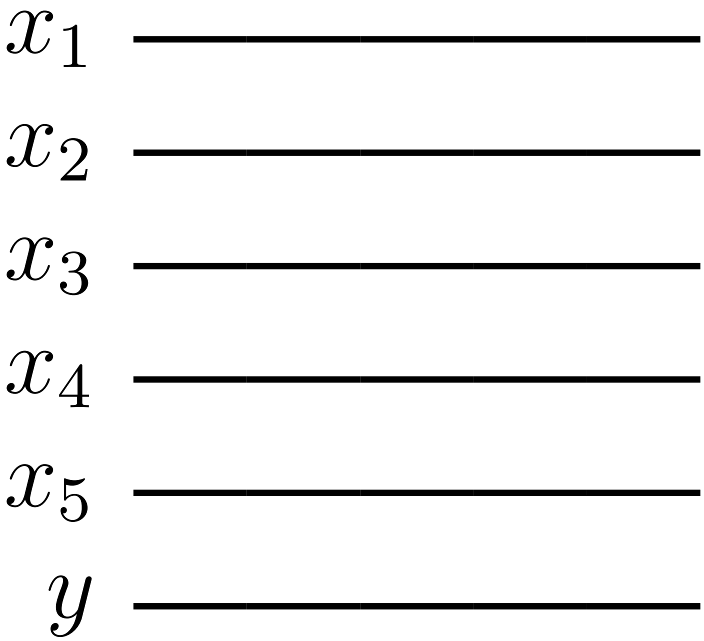
   - If this oracle is used in the Deutsch–Jozsa algorithm, what possible amplitude(s) can be measured on $|00000000\rangle$?

     ______

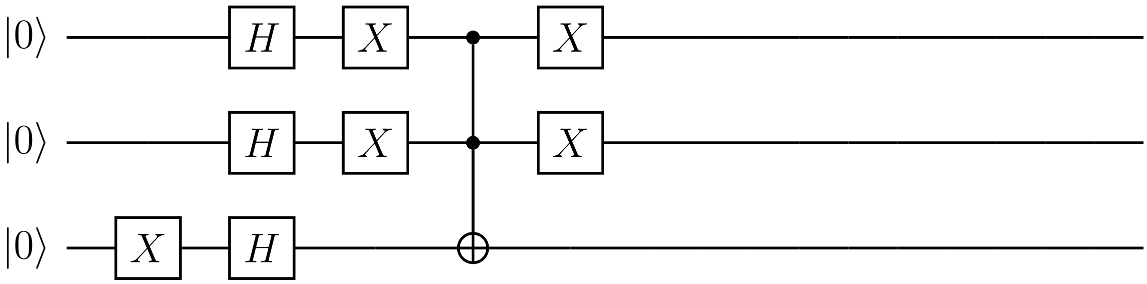
   - What other computational basis vector(s), if any, will have non-zero amplitude for Deutsch–Jozsa if the above oracle is used?

     ______

5. (10 points) Complete the circuit below so that it is an oracle for Grover's algorithm on a 5-qubit instance, sending $|xy\rangle$ to $|x \;\; y \oplus f(x)\rangle$ where the secret is 10101. Below you provide only the oracle, not any other portions of the circuit.



6. (5 points) Consider a 2-qubit instance of Grover with the secret value $|00\rangle$. The circuit up to the point of the diffusion step is specified. Complete the circuit by adding the diffusion (also called reflection about $|s\rangle$) step.



7. (10 points) (1 per blank) Recall for Grover's problem that when an oracle provided a single secret, we obtained $|w\rangle$ as a column vector of all zeros, but with a 1 in the location of the secret. For example, for a two-qubit problem ($N = 4$) with secret $|00\rangle$

$$|w\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Suppose the oracle instead provides *two* secret values, $|00\rangle$ and $|11\rangle$. If Grover's algorithm could reach $|w\rangle$ and we performed a measurement of $|w\rangle$ we would be satisfied at measuring *either* secret ($|00\rangle$ or $|11\rangle$).

We begin as before with

$$|s\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

But for this problem with the two secret values $|00\rangle$ and $|11\rangle$ (fill in the blanks):

$$|w\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} \underline{\qquad} \\ \underline{\qquad} \\ \underline{\qquad} \\ \underline{\qquad} \end{pmatrix}$$

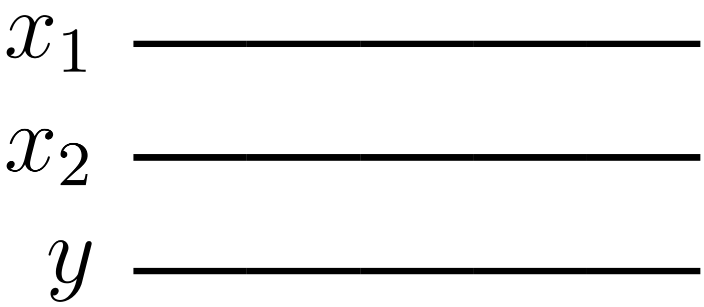
and thus $|s'\rangle$ which must be orthogonal to $|w\rangle$ is (fill in the blanks):

$$s' = \frac{1}{\sqrt{2}}\begin{pmatrix} \underline{\qquad} \\ \underline{\qquad} \\ \underline{\qquad} \\ \underline{\qquad} \end{pmatrix}$$

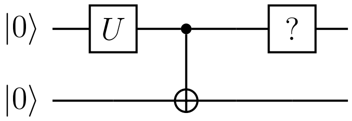
The inner product of $|s\rangle$ and $|s'\rangle$ is then $\langle s|s'\rangle = \frac{\underline{\qquad}}{\sqrt{4}}$ (fill in the numerator)

Generally, for an n qubit instance of Grover ($N = 2^n$), where $|w\rangle$ represents k acceptable secret values, what is the inner product of the resulting $|s\rangle$ and $|s'\rangle$? $\frac{\underline{\qquad}}{\sqrt{N}}$

(5 points) Complete the circuit below so that it is an oracle for Grover's algorithm on a 2-qubit instance, sending $|xy\rangle$ to $|x \quad y \oplus f(x)\rangle$ where the secret value is either 00 or 11. Below you provide only the oracle, not any other portions of the circuit.



8. Consider the circuit below where some arbitrary single-qubit gate U acts on the top qubit. Following that, a CNOT gate is applied from the top to the bottom qubit:



While we know general cloning of a quantum state is impossible, there are exactly two states resulting from $U|0\rangle$ that would be successfully cloned onto the bottom qubit using the above circuit.

(6 points) for blanks below, 2 points each.

Those states are ____________ and ____________.

If we wanted to restore the top qubit to its state prior to applying U, what gate would we place in the "?" box? ____________

The algorithm we studied for phase estimation applies gates and measures the qubits of a quantum system, thus transforming and then collapsing each qubit's state.

(4 points) Based on the above and on your knowledge of how phase estimation is performed, describe how we could perform phase estimation on an n-qubit system, but now with n ancillary (extra, additional) qubits, and now restoring the n primary bits to their state prior to the actions performed for phase estimation.

9. (10 points) Using Shor's algorithm, let's try to factor the number 24 using the following table of values for

$$17^i \bmod 24$$

i	$17^i \bmod 24$
1	17
2	1
3	17
4	1

- What is the period of this function?__________
- 17 is a suitable base for using Shor's algorithm to factor 24 because the period of 17^i mod 24 is even □ **true** □ **false**.
- To find the factors of 24 we would perform the following computations:

  GCD(_____,24) = _____
  and

  GCD(_____,24) = _____