CSE 468T Introduction to Quantum Computing **Spring 2023**

Exam II

Given: 26 April 2023 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.

   - 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**
   - 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**
   - Shor's algorithm provides exponential speedup over the best-known approach for factoring large integers. ☐ **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**
   - Deutsch–Jozsa solves a problem in polynomial time on a quantum computer that takes worst-case exponential time on a classical computer. ☐ **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**
   - Grover's algorithm provides exponential speedup over classical algorithms that solve the same problem. ☐ **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**
   - 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 9. ☐ **true** ☐ **false**

2. **(10 points)** Using the circuit diagram below, create a 3-bit oracle of your choice, and answer the following questions. To receive credit, your oracle must use at least one quantum gate. In other words, don't provide $f(x) = 0$. Any other function is acceptable.

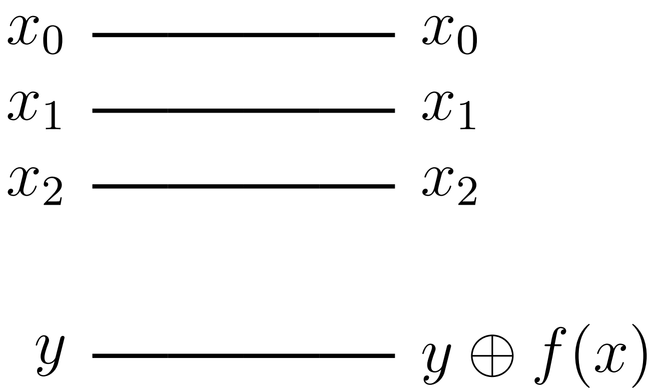
   (a) My oracle implements

   $f(x) =$ ____________________

   or, if easier, describe your function in prose:

   (b) My oracle is suitable for use in at least the following algorithms we have studied this semester: ____________________

   (c) And, at last, my oracle is:



Rubric:

- Full credit if all parts agree, no matter how simple the oracle, providing you used at least one gate.
- Partial credit available based on how closely your answers correspond with each other.

3. (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	$\overline{\mathbf{Z} \otimes \mathbf{X}}$	$\overline{\mathbf{X} \otimes \mathbf{Z}}$	$\mathbf{Y} \otimes \mathbf{Y}$

Alice, having traveled to Israel, decides to compute her squares' results **right to left**, while Bob, still in St. Louis (he turned down a trip to Australia), reports his results top to bottom, as usual.

(a) (2 points) With this change to Mermin–Peres, answer the following questions, assuming error-free quantum computations:

- For any of her three rows, Alice *always* reports values whose products are +1 as required. □ **true** □ **false**
- Alice and Bob *always* agree on a value in their common square. □ **true** □ **false**

(b) (4 points) Below, explain your answers to part (a), by providing an example that makes a statement false, or by explaining why the statement is true.

(c) (4 points) Alice and Bob are assigned row 2 and column 2, respectively. Suppose Alice happens to measure first, measuring $|{+}{+}\rangle$ for her (first and rightmost) $\mathbf{X} \otimes \mathbf{X}$ square.

Fill in the blanks below showing *all possible values* that could be reported by Alice and Bob, as they examine their squares in the order below, following Alice's initial measurement of the rightmost square in row 2.

Alice row 2

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

Bob column 2

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

4. (15 points)

Consider a qubit in state $|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}$

(a) (3 points) We wish to measure this state in the **X** basis, but alas we can only perform measurements on quantum computers in the computational (**Z**) basis. Put the following operations in the correct order (1, 2, 3) by writing the appropriate numerals in the blanks provided:

- ________ We map the **X** basis to the **Z** basis using an **H** gate.
- ________ We map the **Z** basis to the **X** basis using an **H** gate.
- ________ We measure in the computational basis.

(b) (8 points) For a nice change, suppose we want to measure state $|\psi\rangle$ in the **Y** basis. Recall that the **Y** basis is spanned by

$$|{+y}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \text{ and } |{-y}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$

in the same way **Z** is spanned by $|0\rangle$ and $|1\rangle$, and **X** is spanned by $|+\rangle$ and $|-\rangle$. Here we want to measure in the **Y** basis.

The matrix that transforms state from the **Z** basis to **Y**, mapping $|0\rangle$ to $|{+y}\rangle$ and $|1\rangle$ to $|{-y}\rangle$ is (use the blank to the left of the matrix for a common fraction, if you like):

$$\underline{\hspace{2em}}\begin{pmatrix} \underline{\hspace{2em}} & \underline{\hspace{2em}} \\ \underline{\hspace{2em}} & \underline{\hspace{2em}} \end{pmatrix}$$

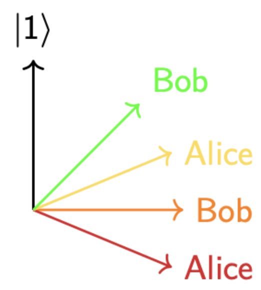
and its inverse is (be sure to conjugate as needed):

$$\underline{\hspace{2em}}\begin{pmatrix} \underline{\hspace{2em}} & \underline{\hspace{2em}} \\ \underline{\hspace{2em}} & \underline{\hspace{2em}} \end{pmatrix}$$

(c) (4 points) Measuring $|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}$ in the **Y** basis yields ________.

Hint: You can find this particular answer easily, without performing any matrix multiplication. Hint: the trick rhymes with phrobal glaze.

5. (10 points)



- Recall that in the CHSH solution, the angle between adjacent rays in the picture above is $\pi/8$, so that the probability of agreement where it should happen is $\cos^2(\pi/8)$, which is approximately 85%. In this solution, that same probability holds in the one case where (red) Alice and (green) Bob should disagree.
- Suppose the angle between each adjacent pair of rays is changed to $\pi/16$, so that when they should agree, their probability of agreement is now

  $$\cos^2(\pi/16) \approx 96\%$$

  Here are similar computations, some of which you may find useful:

  $$\begin{array}{ll} \cos^2(2\pi/16) \approx 85\% & \cos^2(3\pi/16) \approx 70\% \\ \cos^2(4\pi/16) \approx 50\% & \cos^2(5\pi/16) \approx 37\% \\ \cos^2(6\pi/16) \approx 15\% & \cos^2(7\pi/16) \approx 04\% \end{array}$$

All other aspects of the game are unchanged:

- Alice and Bob are provided colors that are chosen randomly and uniformly.
- The metric for *success* of the game is the *average* rate at which Alice and Bob agree when they should, and disagree when they should, over all 4 possible combinations of colors they can be provided.
- In the game's solution using the above diagram, as taught, the *success* metric is approximately 85%.

Answer the following:

- (1 points) This change improves the *success* of the game. □ **true** □ **false**.
- (5 points) What is the approximate success metric of the game with this change?

  (provide a numeric answer, such as "85" for "85%") ____________%
- (3 points) Show the math supporting your answers below:

6. (10 points) During an iteration of Grover, and after the first step (reflection) but before the second step (diffusion), we have obtained the following state:

$$|\psi_f\rangle = \begin{pmatrix} 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ -0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \\ 0.25 \end{pmatrix}$$

Important: The column's first index (top) is 0; its last index is 15.

(a) This is an instance of Grover for a function, where the input values are ______ bits wide.

(b) From $|\psi_f\rangle$ shown above, what is the secret $|w\rangle$ (the input value that Grover is trying to find)? ____________

(c) This is the first step of the ____________ iteration of the algorithm.

(d) When we complete this iteration by performing diffusion, the amplitude on $|w\rangle$ will be approximately ____________, because it increases each iteration on a problem of this size by approximately ____________.

7. **(15 points)** You are at a party where everybody is talking about quantum computing. You overhear somebody pontificating about Bernstein–Vazirani problems of n bits, namely functions of the form $f(x) = x \bullet s$, where x and s are each n bits wide.

   (a) **(6 points)** After one too many Negronis, the person claims that *all* values of s lead to balanced functions for the Deutsch–Jozsa problem.

   "Not so fast!" you say. That is almost true. Yes, in terms of n, it is true that there are $\Theta\left(\underline{\qquad}\right)$ such functions, but for one value of s, namely $s =$ ______, $f(x) = x \bullet s$ is not a balanced function; it is, in fact, constant.

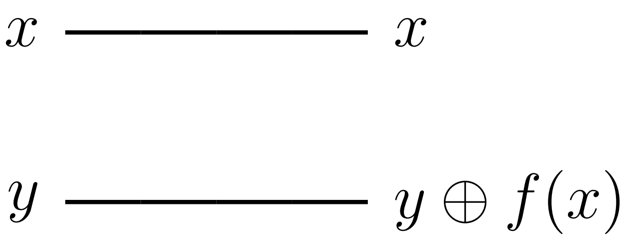
   (b) **(6 points)** OK the pontificator concedes, you are right[1], but for all other values of s, Bernstein–Vazirani functions provide *all* oracles that are balanced to Deutsch–Jozsa: there are absolutely no others.

   "Thundering superpositions!" you exclaim, that cannot be the case. And you continue by providing a single-qubit counterexample[2] of a function that is balanced, but not of the form $f(x) = x \bullet s$ for any s:

   $f(0) =$ ______

   $f(1) =$ ______

   (c) **(3 points)** You then draw the oracle for this function on a conveniently provided party napkin (just draw gates as needed over what you see below):



   Be certain your oracle provides both of the outputs, as required and shown above.

[1] At least, Ron Cytron hopes you got this right; sadly, he was not invited to this party

[2] the crowd gasping in awe at the elegance and simplicity of your counterexample

8. (10 points) Using Shor's algorithm, let's try to factor the number 35 using the following table of values for

$$2^i \bmod 35$$

i	2^i mod 35
0	1
1	2
2	4
3	8
4	16
5	32
6	29
7	23
8	11
9	22
10	9
11	18
12	1

(a) (2 points) What is the period of this function?__________

(b) (2 points) 2 is a suitable base for using Shor's algorithm to factor 35 because the period of 2^i mod 35 is even □ **true** □ **false**.

(c) (6 points) To find the factors of 35 we would perform the following computations:

- GCD(_____,35) = _____
- GCD(_____,35) = _____