MULT20015 Elements of Quantum Computing

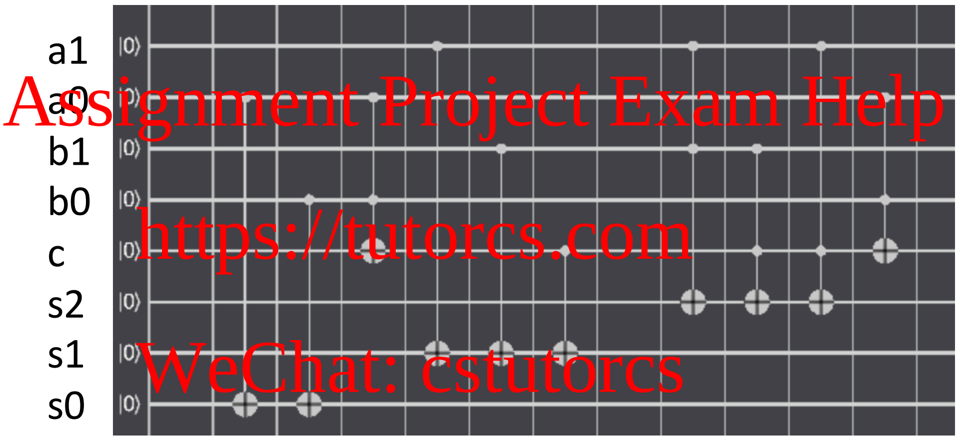
Assignment 2

Due: 5pm Thursday 14th October, 2021

Instructions: Work on your own, attempt all questions. Submit your completed written work electronically as a pdf file (no other formats accepted) to LMS, with name and student number on the front, on or before the due date. You may submit a scanned or photographed copy of a hand-written assignment as long as your submission is clear and legible. Only electronic submissions of PDF files are accepted.

Total marks = 30

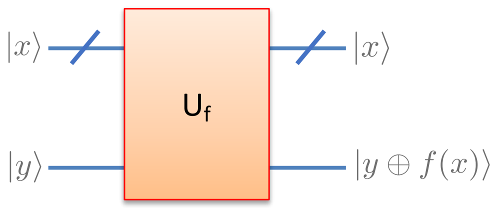
Question 1 [2.0 + 2.0 = 4.0 marks]
The circuit (below left) carries out two-bit addition S = A + B with an addition carry bit (c), where A = a0 + 2a1, B = b0 + 2b1 (ordering is a0 = least significant bit, a1 = most significant bit etc) and the sum S is represented using 3 bits, i.e. S = s0 + 2s1 + 4s2:



(a) Explain how the circuit works by considering the system at each time-step for the case: A = 3, B = 3 (decimal notation).

(b) Show how you would modify the circuit so that the bit ordering of A, B and S are reversed (i.e. most significant bit last).

Question 2 [2.0 + (1.0 + 3.0 + 1.0) = 7.0 marks]
Consider the Deutsch-Josza algorithm for the case where the function $f(x)$ is defined over 2-bit numbers, x. In Lectures, the general circuit for function evaluation was given by:



(a) Find circuits that correspond to each of the four function cases for the two-bit case (tabulated below). Program these in the QUI (four separate instances) to verify. Supply screen shots for each of the four cases.

CONSTANT	$f_1(00) = 0$ $f_1(01) = 0$ $f_1(10) = 0$ $f_1(11) = 0$ $f_2(00) = 1$ $f_2(01) = 1$ $f_2(10) = 1$ $f_2(11) = 1$	BALANCED	$f_3(00) = 0$ $f_3(01) = 1$ $f_3(10) = 0$ $f_3(11) = 1$ $f_4(00) = 1$ $f_4(01) = 0$ $f_4(10) = 0$ $f_4(11) = 1$

(b) Now consider a different set of functions f_i defined over two-qubit (n=2) inputs as:

$f_1(00) = 0$	$f_2(00) = 0$	$f_3(00) = 0$	$f_4(00) = 1$
$f_1(01) = 0$	$f_2(01) = 0$	$f_3(01) = 1$	$f_4(01) = 0$
$f_1(10) = 0$	$f_2(10) = 1$	$f_3(10) = 0$	$f_4(10) = 0$
$f_1(11) = 1$	$f_2(11) = 0$	$f_3(11) = 0$	$f_4(11) = 0$

Each function f_i returns '1' for only one of the possible two-bit/qubit inputs and '0' for all other input strings.

Consider you are provided an implementation (i.e. a program in either the classical or quantum sense) for one of the functions f_i where i is one of the 4 values from the set {1, 2, 3, 4}, the problem is to develop a classical and a quantum algorithm to determine i, i.e. which of the functions is being evaluated.

(i) Describe a classical algorithm to solve the above problem. What is the elementary step? What is the cost function (under worst-case scenario) as a function of input size n? Find Big-O class from the cost function.

(ii) Devise a quantum algorithm to solve the above problem for n=2. Determine the quantum circuit for each f_i and explain carefully how they work. Implement the quantum circuits on QUI and verify their working for all four functions f_i tabulated above (include screen shots).

(iii) What is the elementary step in your quantum implementation? For n=2, how many elementary steps are required to find i. Plot a graph of number of function queries required as a function of n. Find the cost and complexity class.

Question 3 [1.0 + (1.0 + 1.0) = 3.0 marks]

(a) Alice chooses the two primes to construct her RSA keys:

$$p = 28813096529271137159477 11$$

and

$$q = 1432329633177924629423501 1689.$$

Determine the smallest valid RSA public key and its corresponding private key for Alice. Show your workings with an explanation justifying your answer.

(b) An experiment attempts to factor 511 using Shor's algorithm on a quantum computer. The experimenters choose a base of a = 3, and attempt to find the period, r, such that a^r = 1 mod 511. After performing Shor's algorithm, the upper control register, containing n = 18 qubits is measured and the value m = 100101010101010101_2 is obtained.

(i) Based on this measured value, use the continued fraction expansion to find candidate periods, r. For each candidate period, r, test to determine if a^r = 1 mod 511 or not. Show your working.

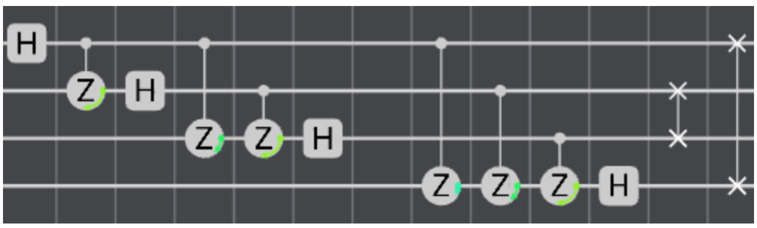
(ii) Use the period, r, obtained in part (i) to find the factors of 511. Show your working.

Question 4 [1.0 + 3.0 + 2.0 + 2.0 + 1.0 = 9.0 marks]

(a) On the QUI, program a x-rotation gate with a rotation angle of $\frac{2\pi}{3}$ and a global phase of $\frac{\pi}{3}$ directly on a $|\psi\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ state. What is the resulting state (including phase) when this rotation is applied to the $|-\rangle$ state? Show that $|-\rangle$ is an eigenstate of this rotation. Include your circuit in your answer.

(b) Construct the Quantum Phase Estimation (QPE) circuit described in the lectures, which could be used to estimate the eigenvalue of the eigenstate, $|\psi\rangle = |-\rangle$ for a x-rotation gate, with a rotation angle of $\frac{2\pi}{3}$ (with a global phase of $\frac{\pi}{3}$). Use four qubits in the control (upper) register.

You may make use of the following (inverse) quantum Fourier Transform for four qubits:



The angles of the controlled-Z rotations shown (in order, from left to right) are:

I. $-\pi/2$ (with a global phase of $-\pi/4$)
II. $-\pi/4$ (with a global phase of $-\pi/8$)
III. $-\pi/2$ (with a global phase of $-\pi/4$)
IV. $-\pi/8$ (with a global phase of $-\pi/16$)
V. $-\pi/4$ (with a global phase of $-\pi/8$)
VI. $-\pi/2$ (with a global phase of $-\pi/4$)

Include a screenshot of your circuit in your answer.

(c) Determine (using QUI) the probabilities of the resulting measurements (on the control/upper register). Recall that if

$$U|\psi\rangle = \exp(i2\pi\theta)\,|\psi\rangle,$$

then QPE allows us to estimate θ using a quantum computer. Use these measurements for the QPE circuit with $U=R_x(2\pi/3)$ (with a global phase of $\frac{\pi}{3}$) and $|\psi\rangle = |-\rangle$ to estimate θ, and briefly compare you estimates of θ with your answer in part **(a)**. Why are they not identical?

(d) Modify your circuit and repeat steps above to determine the phase angle, θ, for $U=R_x(2\pi/5)$ with a global phase of $\pi/5$ applied to the state $|\psi\rangle = |-\rangle$.

(e) Briefly explain what could you do to obtain a better estimate of θ?

Question 5 (2.0 + 2.0 + 3.0 = 7.0 marks)

The first few triangular numbers, $T_n = n(n+1)/2$, are 1, 3, 6, 10 and 15.

(a) Write out the circuit for an oracle of five qubits which marks (ie. applies a -1 phase to) each of the states if it is a triangular number. You may use multiply controlled gates. Implement the oracle on the QUI and verify its working for all triangular numbers over five qubits (include screen shots).

(b) On the QUI (set to 5 qubits), program this oracle into Grover's algorithm. Apply enough Grover iterations (consisting of oracle and inversion about the mean) to optimize the probability of measuring a triangular number. Determine the angle of rotation in the geometrical picture and show that it is consistent with the optimal number of iterations found in QUI.

(c) If you used Grover's algorithm to find a random triangular number less than or equal to 127 (commensurate with 7 qubits), approximately how many iterations (consisting of oracle and inversion about the mean) should you use to ensure a high probability of success? Show your working.