IT41: Classical and Quantum Algorithms
Exam

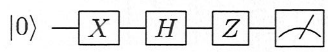
June 23, 2021, 2 hours

All documents are authorized as well as a calculator. The exam is made of 3 independent exercises. The grading will take into account the length of the subject.

Exercise 1: General questions (5 points)

The following questions are independent.

1. What will be the outcomes of the following circuit (measurement in the standard basis):



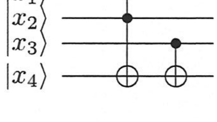
2. Is the quantum state $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ entangled or not ?

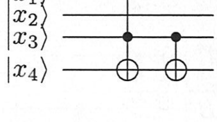
3. Is the following matrix unitary ?

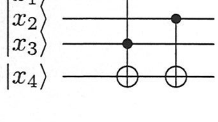
$$U = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

4. Provide a circuit that corresponds to the matrix U.

5. Let us consider the classical boolean function $f(x_1, x_2, x_3) = (x_1.x_2) \oplus x_3$ (where . is the logical operation "AND"). Which of the following circuit implements $U_f |x_1x_2x_3\rangle |x_4\rangle = |x_1x_2x_3\rangle |x_4 \oplus f(x_1, x_2, x_3)\rangle$?







6. Why is Shor's algorithm interesting ?

7. What does the quantum part of Shor's algorithm do ?

Exercise 2: Hadamard gates, Control-Z gates and Graph states (10 points)

1. Calculate the 4×4 matrix $H \otimes H$ and the 8×8 matrix $H \otimes H \otimes H$ where H is the Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

2. Check that the image of $|3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ by $H^{\otimes 3}$ satisfies the relation $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle$.

3. A control-Z gate (CZ-gate) is given by the following circuit:

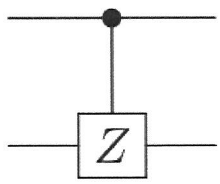


Figure 1: Control-Z gate

The action of the CZ-gate reads as follows, if the control qubit is $|1\rangle$ then one applies a $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ gate on the target qubit, if the control qubit is $|0\rangle$ nothing happens on the target qubit.

   (a) Explain how the CZ-gate acts on the standard basis $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$.

   (b) Provide the corresponding 4×4 unitary matrix in the standard basis.

   (c) For a CZ-gate does it really matter which qubit is the control qubit and which one is the target ? Explain.

4. Let us consider the following quantum circuit:

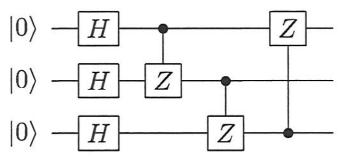


Figure 2: A quantum circuit based on Hadamard gates and CZ-gates.

(a) Express, in the binary basis, the quantum state $|\psi\rangle$ that one obtains at the end of the circuit provided by Figure 2.

(b) What is the probability of measuring $|1\rangle$ on the last qubit of $|\psi\rangle$? What is the corresponding state after measurement ? Let us denote $|\psi'\rangle$ the state after the measurement.

(c) Suppose you measure the first qubit of $|\psi'\rangle$ in the standard basis. What is the state of the second qubit if you obtained $|0\rangle$? Same question if you obtained $|1\rangle$? Conclude that the quantum state $|\psi\rangle$ generated by the circuit of Figure 2 was entangled.

5. A graph state is a quantum state generated by a quantum circuit made of Hadamard gates on each wire and a distribution CZ-gates between the wires. The position of the CZ-gates are provided by a graph. Each node of the graph represents a wire and each edge corresponds to a CZ-gate between the wire. For instance consider the following graph:

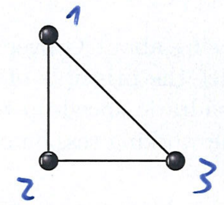


Figure 3: An example of graph G made of three nodes and three edges. The corresponding quantum state is $|\psi\rangle$.

To the graph of Figure 3 one associates the circuit of Figure 2: To each node corresponds a wire with a Hadamard gate and to each edge corresponds a CZ-gate between the associated node/wire. Note that the order of the wires and the order of the CZ-gates do not matter.

(a) Provide the quantum circuit of the graph states corresponding to the graph of Figure 4.

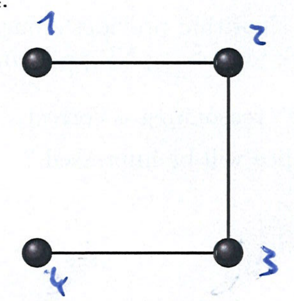


Figure 4: A four-qubit graph states.

(b) What is the corresponding graph states ?

Exercise 3: Grover's algorithm (7 points)

1. In this exercise one applies Grover's algorithm on a four-qubit Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Suppose you are given an Oracle which signs the elements $|0000\rangle$ and $|1111\rangle$, i.e. the Oracle $\mathcal{O}_f$ comes from a classical function f such that $f(0000) = f(1111) = 1$ and $f(x) = 0$ for all $x \notin \{0000, 1111\}$ (in decimal notation $f(0) = f(15) = 1$ and $f(x) = 0$ for all $0 < x < 15$).

   (a) Describe the quantum state after one run of Grover's algorithm (you can use either the binary or decimal basis $|0\rangle = |0000\rangle, |1\rangle = |0001\rangle, |2\rangle = |0010\rangle \dots, |15\rangle = |1111\rangle$).

   (b) What is the probability of measuring one of the two elements marked after one run of the algorithm ?

   (c) (difficult) What would be the optimal number of iterations in that case ?

2. Alice and Bob are discussing about Grover's algorithm. Bob is very excited after explaining Alice the principle of this beautiful quantum algorithm that provides a quadratic speed-up to find an element recognized by a function f. After the working session comes an intersting discussion among both of them:

   - Alice "But Bob what is Grover's algorithm good for ?"
   - Bob "Well, it helps finding an element in an unsorted database with a quadractic speed-up compare to all other classical algorithms !"
   - Alice "Yes but what is it good for ? What is it useful for ?"
   - Bob "Aren't you imprest ?"
   - Alice "Not really"

   Bob feels very sorry to not be able to share the beauty of this algorithm with his friend. Then some light shows up in Bob's eyes !

   - Bob: "Grover's algorithm provides a quadratic speed-up on all algorithms that work for solving NP problem !!"

   (a) Explain why Bob reasonning is correct.

   (b) Do you think Alice will be impressed ?