Quantum Information

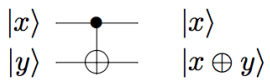
M2 Cybersecurity

December 7, 2022

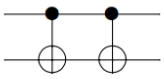
Exercise 1: CNot

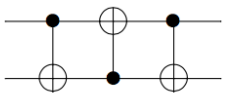
We recall that for any $x, y \in \{0,1\}$, $|x,y\rangle = |x\rangle\,|y\rangle = |x\rangle \otimes |y\rangle$.

The two qubit CNot gate $|x,y\rangle \mapsto |x, x \oplus y\rangle$ where $\oplus$ is the XOR operation (sum modulo 2) is represented as follows



1. For $a \in \{0,1\}$ what is the state CNot$|a0\rangle$
2. What are the unitary maps implemented by the following circuits?





3. Draw a circuit using H (Hadamard gate) and CNot, that maps $|00\rangle$ to $|\phi_+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

Exercise 2: No Cloning

1. Given four bits a, b, c, d when does the scalar product $\langle a, b| \, |c, d\rangle$ equals 0.

2. Given four quantum states in $\mathbb{C}^2$, $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle$, express the scalar product in $\mathbb{C}^4$, $\langle \phi_1, \phi_2| \, |\phi_3, \phi_4\rangle$ as a product of two scalar products in $\mathbb{C}^2$

3. Show that there is no unitary map $U : \mathbb{C}^4 \to \mathbb{C}^4$ s.t. $\forall \, |\phi\rangle \in \mathbb{C}^2$,

$$U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Exercise 3: Superdense Coding

Alice and Bob are sharing a pair of qubits (q_A, q_B) in the entangled state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice wants to send 2 bits of information $a, b \in \{0, 1\}$ to Bob, by sending 1 qubit only. First, if $a = 1$, Alice applies X on her qubit. Then, if $b = 1$, Alice applies Z on her qubit. Finally, she sends the qubit q_A to Bob. Show that if Bob applies CNot on (q_A, q_B) and H on q_A, then he can recover the two bits of information a and b.

Exercise 4: Teleportation

Alice and Bob are sharing a pair of qubits (q_A, q_B) in the entangled state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice has another qubit q in an unknown state $|\psi\rangle = \alpha \, |0\rangle + \beta \, |1\rangle$. Alice wants to send $|\psi\rangle$ to Bob, but they only have a classical channel to communicate. Alice proceeds as follows: she performs CNot on (q, q_A); she applies H on q; she measures q and q_A, obtaining the classical outcomes c and c_A respectively; finally, she classically sends c and c_A to Bob.

1. What is the the state of Bob's qubit after the two measurements performed by Alice?

2. Show that Bob can reconstruct the state $|\psi\rangle$.

3. Do the classical outcomes c and c_A depend on the state $|\psi\rangle$?

Exercice 5 Simon algorithm

For $N = 2^n$ we are given $x = (x_0, \dots x_{N-1})$ with $x_i \in \{0,1\}^n$ with the property that there exists an unknown $s \in \{0,1\}^n$, $s \neq 0^n$, such that $x_i = x_j$ if and only if $i = j$ or $i = j \oplus s$. The objective is to find s.

The access to x is possible through an oracle $O : |i, b\rangle \mapsto |i, b \oplus x_i\rangle$.

The quantum part of the algorithm is the following:

1. Start with $|0^n\rangle |0^n\rangle$
2. Apply Hadamard to the first n qubits
3. Apply the oracle
4. Measure the second register. Let $|x_i\rangle$ be the state of the second register after the measurement.
5. Apply Hadamard to the first register
6. Measure the first register. Let $|j\rangle$ be the state of the first register after the measurement.
7. Repeat the process until you get $n-1$ independent elements j in $\mathbb{F}_2^n$

- First we consider the particular case were $x_{000} = x_{111} = 000$, $x_{001} = x_{110} = 001$, $x_{010} = x_{101} = 010$ and $x_{100} = x_{011} = 100$.

  What is the state of the system after step 2?

  What is the state of the system after step 3?

  Suppose that the quantum state of the second register after the measurement in step 4 is $|000\rangle$ What is the state of the system after step 5, and what are the possible states of the first register after the measurement in step 6.

  Suppose that the quantum state of the second register after the measurement in step 4 is $|001\rangle$ What is the state of the system after step 5, and what are the possible states of the first register after the measurement in step 6.

- Show that in the general case for each $|j\rangle$ obtained at step 6, $j.s = 0 \bmod 2$
- Explain how to obtain the correct s at the end of the algorithm
- Describe what happens if the algorithm is applied to an x such that for all $i \neq j$, $x_i \neq x_j$. $(s = 0^n)$

Exercise 6: Eavesdropper

Alice prepares a qubit q in the state $|0\rangle$, applies H on q, and sends q to Bob through a quantum channel. Bob receives the qubit q, applies H on q, and then measures q.

1. What is the probability for Bob to obtain 0?
2. Eve is a spy. She measures the qubit q during the transmission of the qubit from Alice to Bob. In the presence of Eve, what is the probability for Bob to obtain 0?

Exercice 7 Dirac Notations

1. What is the linear map $|0\rangle\langle 0|$: how does it act on $|0\rangle$, $|1\rangle$ and on a genral state $|\phi\rangle$
2. What is the linear map $|\phi\rangle\langle\phi|$?
3. What is the map $|1\rangle\langle 0| + |0\rangle\langle 1|$?
4. Give an expression of the unitaries Z and H using Dirac notations and the states $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Exercice 8 POVM

Let

- $E_0 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|$,
- $E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|-\rangle\langle -|$
- $E_2 = I - E_0 - E_1$

Where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

1. Show that $|1\rangle + |-\rangle$ and $|1\rangle - |-\rangle$ are eigenvectors of E_2
2. Show that $\{E_0, E_1, E_2\}$ is a valid POVM
3. What happens when measuring $|0\rangle$ and $|+\rangle$?
4. What can this POVM be used for ?

Exercice 9 density matrices

What is the state of Bob state after the teleportation protocol (Exercice 4) if he does not know Alice measurements results.

To know more about quantum Computing :

- **Lecture Notes**

  Lecture Notes by Ronald de Wolf from CWI

  https://arxiv.org/pdf/1907.09415.pdf

  Lecture Notes by Vaziarni et al Berkley

  https://inst.eecs.berkeley.edu/ cs191/fa14/

  Lecture Notes by John Preskill at Caltech

  http://www.theory.caltech.edu/people/preskill/ph229/

  Lecture Notes by John Watrous et al at Waterloo

  https://cs.uwaterloo.ca/ watrous/LectureNotes/CPSC519.Winter2006/all.pdf

  Lecture Notes by Scott Aaronson (from https://www.scottaaronson.com/blog/)

  https://www.scottaaronson.com/qclec/combined.pdf

  https://www.scottaaronson.com/qisii.pdf

- **Books**

  Quantum Computation and Quantum Information by Michael Nielsen and Isaac Chuang

  Classical and Quantum Computation by A.Yu. Kitaev, A.H. Shen and M.N. Vyalyi