Introduction to Quantum Computing

Javier Orduz
CSI 5V93

August 11, 2021

Contents

Part I

Quantum Circuits & Quantum Algorithms (Basic Qiskit)

In this chapter, we talk about ...

1. Modern Physics: Quantum (Go to previous slides)
2. Quantum Computing

   qbits

   Gates

   single qbits state and Multistates
3. Bell states:

   Entanglement

   Superposition

   measure

I need to cre
the slides an
take materia

Chapter 1

Objectives

The chapter's objective is

General objective

Describe the behavior of basic elements and the inner working of algorithms, and use Dirac's notations.

Chapter 2

Activities, materials and more

In this chapter you will use:

- Computer
- Mobile phone
- tablet

In activities section, we will use:

- Kahoot
- Padlet
- GForms
- etc.

Chapter 3

Gates

We will use next gates,

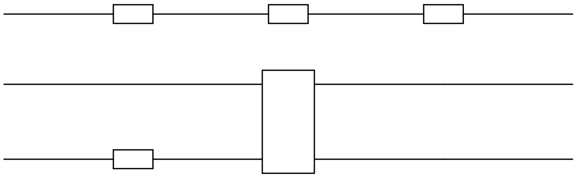


Figure 3.1: Sample of the circut: lines are quantum wires, and rectangles represent the gates.

Figure 3.1 shows a circuit of depth three (3), space (width) four (4), and having five (5) gates.
More gates,

3.1 Hadamard

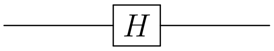


Figure 3.2: Hadamard gate

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.1}$$

The Hadamard operator on one qubit may be written as

$$H = \frac{1}{\sqrt{2}}\Big(\left(|0\rangle + |1\rangle \right) \langle 0| + \left(|0\rangle - |1\rangle \right) \langle 1| \Big) \tag{3.2}$$

Exercise 1 *Write out the eq.* (3.1) *and figure out the eq.* (3.2)*.*

Example 1 *Obtain*

- $H\,|0\rangle$
- $H\,|1\rangle$

3.2 Pauli X

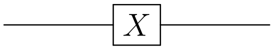


Figure 3.3: Pauli X gate

$$X = \text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.3}$$

3.3 Pauli Y

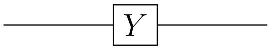


Figure 3.4: Pauli Y gate

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3.4}$$

3.4 Pauli Z

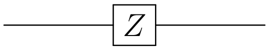


Figure 3.5: Pauli Z gate

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.5}$$

Exercise 2 *You must compute the eigenvectors of the Pauli matrices.*

The Pauli matrices can be represented as,

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{3.6}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{3.7}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \tag{3.8}$$

Those the rotation operators about the $\hat{x}, \hat{y}$, and $\hat{z}$ axes. If we define $\hat{n} = (n_x, n_y, n_z)$, then we have,

$$R_{\hat{n}}(\theta) \equiv e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\Big(n_xX + n_yY + n_zZ\Big) \tag{3.9}$$

Example 2 *Show*

$$\sigma_X\sigma_Y\sigma_X = -\sigma_Y \tag{3.10}$$

Solution:

$$\begin{aligned}
\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&-i\\i&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} &= \left(\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&-i\\i&0\end{pmatrix}\right)\begin{pmatrix}0&1\\1&0\end{pmatrix}\\
&= \begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\\
&= \begin{pmatrix}0&i\\-i&0\end{pmatrix}\\
&= -\begin{pmatrix}0&-i\\i&0\end{pmatrix} \qquad (3.11)
\end{aligned}$$

If we use

$$\sigma_X = |0\rangle\langle 1| + |1\rangle\langle 0| \qquad (3.12)$$

$$\sigma_Y = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0| \qquad (3.13)$$

$$\sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1| \qquad (3.14)$$

then eq. (3.10) can be written

$$\big(\,|0\rangle\langle 1| + |1\rangle\langle 0|\,\big)\big(-i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|\,\big)\big(\,|0\rangle\langle 1| + |1\rangle\langle 0|\,\big) = -\sigma_Y \qquad (3.15)$$

Exercise 3 *Prove that $\sigma_X R_Y(\theta)\sigma_X = R_Y(-\theta)$*

Exercise 4 *Use definition for $X = \sigma_X = \sigma_1 = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ to obtain equations (3.6)-(3.8)*

Exercise 5 *Express the Hadamard gate H as a product of R_X and R_Z rotations and $e^{i\phi}$ for some ϕ.*

Exercise 6 *Show:*

- $\sigma_i = \sigma_i^\dagger$ *where* $i = 1, 2, 3$.
- $\sigma_X^2 = \sigma_Y^2 = \sigma_Z^2 = I$ *where* I *identity matrix.*
- *Show (the next three cyclic permutations):*

$$[\sigma_X, \sigma_Y] = 2i\sigma_Z$$

$$[\sigma_Z, \sigma_X] = 2i\sigma_Y$$

$$[\sigma_Y, \sigma_Z] = 2i\sigma_X$$

3.5 Phase

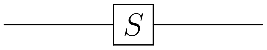


Figure 3.6: Phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{3.16}$$

We can express any arbitrary single qubit operator as

$$U = e^{i\alpha} R_{\hat{n}}(\theta) \tag{3.17}$$

and any operator in this way will be unitary.

3.6 $\pi/8$

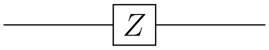


Figure 3.7: $\pi/8$ gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \tag{3.18}$$

Analogously to the eq. (3.10), we can give next theorem

Theorem 1 *$Z-Y$ Decomposition Let U be a unitary operator applied on a single qbit, then there exist real numbers α, β and δ such that*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \tag{3.19}$$

Exercise 7 *Suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Use Theorem 4.1 to show that an arbitrary single qubit unitary U may be written*

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$$

for appropriate choices of α, β, γ and δ.

Let $\{A, B, C\}$ which a set of operators acting on single qbit, such as $ABC = I$ and $U = e^{i\alpha} AXBXC$, where $X = \sigma_X$ and α is a overall phase factor.

Example 3 *Consider*

$$\begin{aligned} A &\equiv R_z(\beta) R_y(\gamma/2) \quad (3.20) \\ B &\equiv R_y(-\gamma/2) R_z\big(-(\delta+\beta)/2\big) \quad (3.21) \\ C &\equiv R_z\big((\delta-\beta)/2\big) \quad (3.22) \end{aligned}$$

. Note that

$$ABC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(-\frac{\gamma}{2}\right) R_z\left(\frac{-\delta-\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right) = I \tag{3.23}$$

Since $\sigma_X^2 = X = I$, and using Exercise 3, we express

$$XR_y\left(-\frac{\gamma}{2}\right) XXR_z\left(-\frac{\delta+\beta}{2}\right) X = XBX = R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta+\beta}{2}\right).$$

Thus

$$\begin{aligned} AXBXC &= R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \\ &= R_z(\beta)R_y(\gamma)R_z(\delta) \end{aligned}$$

Thus $U = e^{i\alpha}AXBXC$ *and* $ABC = I$*, as it required.*

Exercise 8 *Propose* A, B, C *and* α *for the Hadamard gate.*

Example 4 *Obtain (with Dirac and Matrices notation)*

- *Rotation around* X *by* π. $\sigma_X |0\rangle$ *and* $\sigma_X |1\rangle$
- *Rotation around* Y *and phase flip.* $\sigma_Y |0\rangle$ *and* $\sigma_Y |1\rangle$
- *Rotation around* Z *by* π. $\sigma_Z |0\rangle$ *and* $\sigma_Z |1\rangle$
- *Hadamard (Superposition and change basis* $X \rightarrow Z$*)* $H|+\rangle$ *and* $H|-\rangle$
- S *(phase) (change basis)* $S|+\rangle = |+i\rangle$ *and* $S|-\rangle = |-i\rangle$
- SH *(change basis)* $Z \rightarrow Y$. $SH|0\rangle$ *and* $SH|1\rangle$

3.7 Controlled-NOT

We have the CNOT gate in the quantum context and it has two input qbits:

- Control qbit •
- target qbit ⊕

This gate act as

$$|c\rangle |t\rangle \rightarrow |c\rangle |t \oplus c\rangle \tag{3.24}$$

where ⊕ denotes the modulo-2 addition.

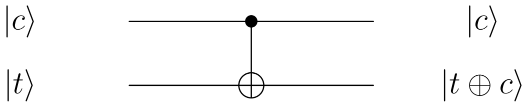


Figure 3.8: Controlled-NOT gate

$$CNOT = \neg X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.25}$$

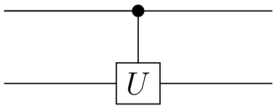
$$\neg X = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \tag{3.26}$$

Consider $|c\rangle = |1\rangle$, what do you think it is happening?

Definition 1 *Let U be is a two qbit operation with a control and target qbit. This operation has set the control qbit in order U is applied to the target qbit, otherwise the target qbit is left alone.*

$$|c\rangle\,|t\rangle \rightarrow |c\rangle\, U^c\,|t \oplus c\rangle \tag{3.27}$$

This operation is called controlled-U operation as is represented by



Exercise 9 *Build the truth table for the eq. (3.24) with $|c\rangle \rightarrow |1\rangle$*

Example 5 *We can propose the XOR gate in quantum computing context as a XOR reversible. Quantum Computing gates are reversible, at least, $\neg X$.*

$$\begin{aligned}
\langle 00|10\rangle &= \langle 0|1\rangle\,\langle 0|0\rangle = 0\\
\langle 01|10\rangle &= \langle 0|1\rangle\,\langle 1|0\rangle = 0\\
\langle 11|10\rangle &= \langle 1|1\rangle\,\langle 1|0\rangle = 0\\
\langle 10|10\rangle &= \langle 1|1\rangle\,\langle 0|0\rangle = 1
\end{aligned}$$

We conclude that

$$\neg X\,|10\rangle = CNOT|10\rangle = |11\rangle$$

When the target qubit is $|1\rangle$, we have

$$\begin{aligned}
\neg X\,|11\rangle &= \big(\,|00\rangle\,\langle 00| + |01\rangle\,\langle 01| + |10\rangle\,\langle 11| + |11\rangle\,\langle 10|\,\big)\,|11\rangle\\
&= |00\rangle\,\langle 00|11\rangle + |01\rangle\,\langle 01|11\rangle + |10\rangle\,\langle 11|11\rangle + |11\rangle\,\langle 10|11\rangle\\
&= |10\rangle
\end{aligned}$$

So we've confirmed that the controlled NOT gate flips the target qubit when the control bit is $|1\rangle$. Now we can use what we've learned to find the action on the target qubit when it's in the state $\alpha\,|0\rangle + \beta\,|1\rangle$. In this case

$$CN(\alpha|10\rangle + \beta|11\rangle) = \alpha CN|10\rangle + \beta CN|11\rangle = \alpha|11\rangle + \beta|10\rangle$$

Therefore the CN takes $\alpha\,|0\rangle + \beta\,|1\rangle$ to $\beta\,|0\rangle + \alpha\,|1\rangle$ when the control bit is $|1\rangle$.

Exercise 10 *Applied the $CNOT$ to the state $\alpha\,|10\rangle + \beta\,|11\rangle$*

3.8 Controlled-Z

The unitary matrix in the computational basis is,

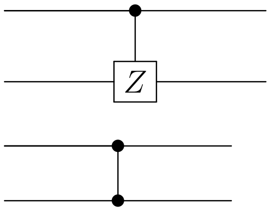


Figure 3.9: CZSWAP gate

$$\mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{3.28}$$

3.9 Swap

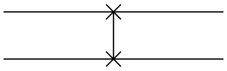


Figure 3.10: Swap gate

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.29}$$

3.10 Controlled-phase gate

This gate...

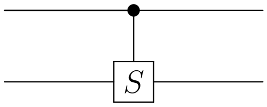
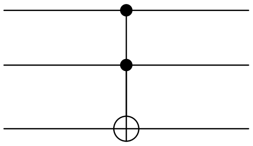


Figure 3.11: Controlled-phase gate

$$\mathrm{CPhase} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \tag{3.30}$$

3.11 Toffoli (CCNOT, CCX, TOFF) gate

This gate...



$$\mathrm{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.31}$$

Toffoli gate flips the third qubit, the target qubit, conditioned on the first two qubits, the control qubits, being set to one.

Exercise 11 *Check the exercise 4.20 in ref.[3, pag.179]*

3.11.1 Controlled-U operator for a single qbit

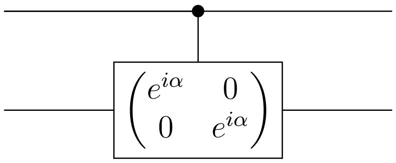
If we want to implement a controlled-U operation for arbitrary single qbit U, with a single qbit operations and CNOT gate, we will follow next strategy to respect the theorem 1.
We are going to use a CNOT operation and qbits.

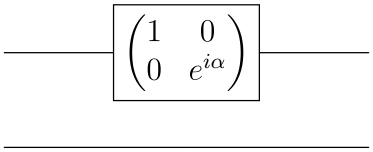
- Apply a phase shift: $e^{i\alpha}$ on the $\langle t|$ (target qbit). If $|1\rangle \to |c\rangle$, there will be a phase shift ($e^{i\alpha}$). Otherwise $|c\rangle$ will be left alone.
- We use $U = e^{i\alpha}AXBXC$ and $ABC = I$.

  If $|1\rangle \to |c\rangle$, then $|t\rangle \to e^{i\alpha}AXBXC\,|t\rangle$

  If $|0\rangle \to |c\rangle$, then $|t\rangle \to ABC\,|t\rangle$

Next two circuits show the previous discussion.

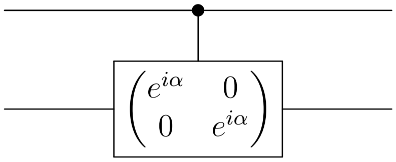

$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$

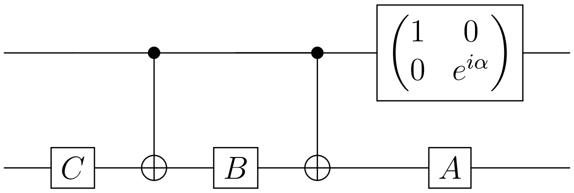


Are those circuits equivalents? Ans: yes!

$$\begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to e^{i\alpha}\,|10\rangle \\ |11\rangle &\to e^{i\alpha}\,|11\rangle \end{aligned} \tag{3.32}$$

Consider check the subsection3.11.2 for multiple qbits and come this section back.


$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$



3.11.2 Conditioning on multiple qbits

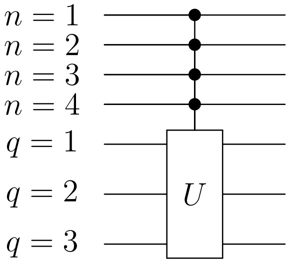
In general, we can rewrite conditions, considering any U operator. We have

- $n + k$ qubits, and
- U is a k qubit unitary operator.

We define the controlled operation $C^n(U)$ as

$$C^n(U)\left|x_1 \otimes x_2 \otimes ... \otimes x_n\right\rangle|\psi\rangle = |x_1x_2...x_n\rangle\, U^{x_1 \cdot x_2 \cdot ... \cdot x_n}\,|\psi\rangle \tag{3.33}$$

This operator is applied to the last $k-$qbits if the first $|n\rangle \leftarrow |1\rangle$, otherwise, nothing is done. Therefore, we will introduce a new notation:



we have $n = 4$ and $k = 3$

3.11.3 Implementation of $C^n(U)$

We will implement $C^n(U)$ gates using our existing repertoire of gates, where U is an arbitrary single qubit unitary operation.

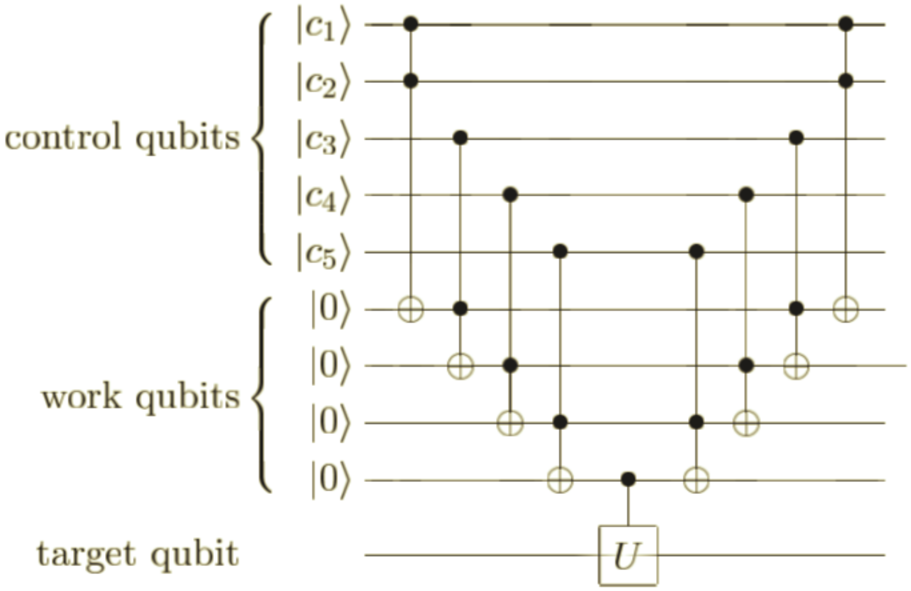


Figure 3.12: Networking implementing the $C^5(U)$ operation.

We suppose all control qbits are in the computational states, we need working qbits (*ancilla* states: $(n-1)$ all are starting and ending in $|0\rangle$). Then the circuit divides up into three stages.

1. Apply $Toff\,|c_1 \cdot c_2\rangle$. To reverse AND all the control bits $c_1, .., c_n$ to produce $c_1 \cdot .. \cdot c_n$.

2. Products

   $Toff\, |c_1 \cdot c_2 \cdot c_3\rangle$, it changes second work qbits.

   $Toff\, |c_1 \cdot c_2 \cdot c_3 \cdot c_4\rangle$, it changes third work qbits.

   $Toff\, |c_1 \cdot c_2 \cdot c_3 \cdot c_4 \cdot c_5\rangle$, it changes fourth work qbits.

3. the last part of the circuit just reverses the steps of the first stage, returning all the work qbits to their initial state, $|0\rangle$.

where $|c_i\rangle$ are $control - i \;\; qbits$.
we make use of a small number $(n-1)$ of working qubits, which all start and end in the state $|0\rangle$. Suppose the control qubits are in the computational basis state $|c_1, c_2, \ldots, c_n\rangle$. The first stage of the circuit is to reversibly AND all the control bits $c_1, \ldots, c_n$ together to produce the product $c_1 \cdot c_2 \ldots c_n$. To do this, the first gate in the circuit ANDs c_1 and c_2 together, using a Toffoli gate, changing the state of the first work qubit to $|c_1 \cdot c_2\rangle$. The next Toffoli gate ANDs c_3 with the product $c_1 \cdot c_2$, changing the state of the second work qubit to $|c_1 \cdot c_2 \cdot c_3\rangle$. We continue applying Toffoli gates in this fashion, until the final work qubit is in the state $|c_1 \cdot c_2 \ldots c_n\rangle$. Next, a U operation on the target qubit is performed, conditional on the final work qubit being set to one. That is, U is applied if and only if all of c_1 through c_n are set. Finally, the last part of the circuit just reverses the steps of the first stage, returning all the work qubits to their initial state, $|0\rangle$. The combined result, therefore, is to apply the unitary operator U to the target qubit, if and only if all the control bits c_1 through c_n are set, as desired [3, pags. 184-185].

3.12 Measurement

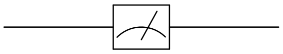


Figure 3.13: Projection onto $|0\rangle$ and $|1\rangle$

The first principle is that classically conditioned operations can be replaced by quantum conditioned operations.

Definition 2 (Principle of deferred measurement) *Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations [3, pag. 186].*

In quantum computing we can measure as an intermediate step in a quantum circuit, and the results can be used to conditionally control subsequent quantum gates. But we can perform a measure at the end of the circuit.

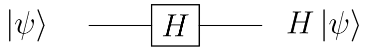
Definition 3 (Principle of implicit measurement) *Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.*

During a measurement onto the basis $\{|0\rangle, |1\rangle\}$, the state will collapse into either state $|0\rangle$ or $|1\rangle$ and we call this a Z-emasurement, since we work on the eigenstates of σ_Z.

Example 6 (Transformation and Quantum Gates) *A transformation is unitary if its inverse is equal to its adjoint. Such transformations preserve inner products and are reversibles and continuous.*
In quantum computing:

- *Algorithms are represented by circuits. The information flows from left to right.*
- *Quantum gates represent unitary transformations applied to qubits in such a circuit.*

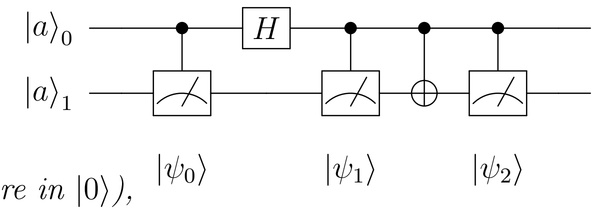
Consider the Hadamart gate:



where is,

$$H = \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \Big)$$

Let the quantum circuit,

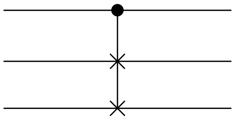


where (initial state are in $|0\rangle$),

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle \otimes |0\rangle = |00\rangle \\
|\psi_1\rangle &= \Big(H \otimes I\Big)\Big(|\psi_0\rangle\Big) = \Big(H \otimes I\Big)\Big(|0\rangle \otimes |0\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|0\rangle|0\rangle + |1\rangle|0\rangle\Big) \\
|\psi_2\rangle &= CNOT\,|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)
\end{aligned}$$

3.13 Fredkin (Controlled-swap) gate

This gate...



$$\text{Fredkin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.34}$$

Exercise 12

- *Calculate*

  $\sigma_i \otimes \sigma_i$, *where* $i = X, Y, Z$

- *Prove the following circuit identities:*

$$\begin{aligned}
CX_1C &= X_1X_2 && (3.35)\\
CY_1C &= Y_1X_2 && (3.36)\\
CZ_1C &= Z_1 && (3.37)\\
CX_2C &= X_2 && (3.38)\\
CY_2C &= Z_1Y_2 && (3.39)\\
CZ_2C &= Z_1Z_2 && (3.40)\\
R_{z,1}(\theta)C &= CR_{z,1}(\theta) && (3.41)\\
R_{x,2}(\theta)C &= CR_{x,2}(\theta) && (3.42)
\end{aligned}$$

Let subscripts denote which qubit an operator acts on, and let C be a CNOT with qubit 1 the control qubit and qubit 2 the target qubit [3, Pag. 185, exercise 4.31].

Chapter 4

Multistates

We already defined the tensor product

$$|a\rangle \otimes |b\rangle = |a\rangle\,|b\rangle = |ab\rangle \tag{4.1}$$

and those states can be in different space vector $(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} = \mathcal{H}_{\mathcal{AB}}) \otimes \mathcal{H}$, where is the $\mathcal{H}$ is a biggest Hilbert space. We use tensor product to describe multiple states. We also discussed some two-qbit gates.
Recall some definition:

Definition 4 *Uncorrelated are those we can write such as a tensor product.*

$$|a\rangle_A \otimes |b\rangle_B = |a\rangle_A\,|b\rangle_B = |ab\rangle_{AB} \tag{4.2}$$

Definition 5 *Inner product for two tensor product:*

$$\langle\psi_A|\psi_B\rangle = \Big(\,\langle a_A| \otimes \langle b_A|\,\Big)\Big(\,|a_B\rangle \otimes |b_B\rangle\,\Big) = \langle a_A|a_B\rangle\,\langle b_A|b_B\rangle \tag{4.3}$$

Definition 6 *Bell or entangled states are whose we cannot write as a tensor product.*

4.0.1 Bell States

We have

$$\left|\psi^{00}\right\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \tag{4.4}$$

$$\left|\psi^{10}\right\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big) \tag{4.5}$$

$$\left|\psi^{01}\right\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big) \tag{4.6}$$

$$\left|\psi^{11}\right\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big) \tag{4.7}$$

or, in general,

$$\left|\psi^{ij}\right\rangle = (I \otimes \sigma_x^j \sigma_z^i)\left|\psi^{00}\right\rangle \tag{4.8}$$

are not separable states (in terms of tensor product) and they are a basis, sometimes those are called EPR (Einstein-Podolski-Rosen) states/pairs. Fig. 4.1 represents a basis change from computation basis to Bell basis.

Exercise 13 *Prove that* $|\psi^{00}\rangle \neq |a\rangle \otimes |b\rangle$ *for all single qbit state* $|a\rangle$ *and* $|b\rangle$.

Next circuit is used for this

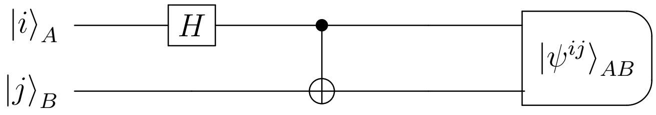


Figure 4.1: Bell state representation

Quantum entanglement is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the state of the others, including when the particles are separated by a large distance.
This is a key element in effects such as quantum teleportation, fast quantum algorithms, and quantum error-correction.

4.0.2 How many qbits must two parties exchange?

Consider

- they are to create a particular entangled state
- Alice and Bob share no prior entanglement

1. A and B share between them a Bell state, the want transform in into some other entangled state.
2. What do they need?
3. they need to be communicated (classical channel or other mean)
4. what kind of measurements we do?

Von Neumann measurements

We do this kind of measurement in quantum computing and quantum communication, and those are a projective measurements done respect to some orthonormal basis $\hat{b} = \{|\phi_j\rangle\}$.

A von Neumann measurement is such that projects the system onto the basis in which the density matrix is diagonal.
On other words, the action of the von Neumann measurement is merely to select the basis state that the system is already in.

Example 7 *Projector, operator or matrix state Given an orthonormal basis $|\varphi_j\rangle$, suppose we have a state $|\psi\rangle$, which we write in this basis:*

$$|\psi\rangle = \sum_j \alpha_j |\varphi_j\rangle$$

Recall that a Von Neumann measurement of $|\psi\rangle$ with respect to the basis $\{|\varphi_j\rangle\}$ is described by the orthogonal projectors $\{|\varphi_j\rangle\langle\varphi_j|\}$, and will output the result ' j ' with probability

$$\begin{aligned}\operatorname{Tr}\left(|\psi\rangle\langle\psi\|\varphi_j\rangle\langle\varphi_j|\right) &= \operatorname{Tr}\left(\langle\varphi_j \mid \psi\rangle\langle\psi \mid \varphi_j\rangle\right)\\ &= \langle\varphi_j \mid \psi\rangle\langle\psi \mid \varphi_j\rangle\\ &= \left|\langle\varphi_j \mid \psi\rangle\right|^2\\ &= \left|\alpha_j\right|^2\end{aligned}$$

Given a device that will measure individual qubits in the computational basis, we can use a quantum circuit to implement Von Neumann measurements of a multi-qubit register with respect to any orthonormal basis $|\varphi_j\rangle$.

We talk about orthogonal operator given by

$$\rho = |\varphi\rangle\langle\varphi| \tag{4.9}$$

this definition is relevant when one state is unknown.

Example 8 *Suppose that A is a projection operator in H_1 where $A = |0\rangle\langle 0|$ and B is a projection operator in H_2 where $B = |1\rangle\langle 1|$. Find $A \otimes B|\psi\rangle$ where[2, pag. 81]*

$$|\psi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

Using what we know about the action of tensor products of operators, we write

$$A \otimes B|\psi\rangle = A \otimes B\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left[\Big(A|0\rangle\Big)\Big(B|1\rangle\Big) + \Big(A|1\rangle\Big)\Big(B|0\rangle\Big)\right]$$

Now

$$\begin{aligned}A|0\rangle &= (|0\rangle\langle 0|)|0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle\\ A|1\rangle &= (|0\rangle\langle 0|)|1\rangle = |0\rangle\langle 0|1\rangle = 0\\ B|0\rangle &= (|1\rangle\langle 1|)|0\rangle = |0\rangle\langle 1|0\rangle = 0\\ B|1\rangle &= (|1\rangle\langle 1|)|1\rangle = |1\rangle\langle 1|1\rangle = |1\rangle\end{aligned}$$

Therefore we find that

$$A \otimes B|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle$$

Exercise 14 *Show that if A and B are Hermitian, then $A \otimes B$ is Hermitian. Hint: Use two tensor product states: $|\varphi_1\rangle = |\alpha_1\rangle \otimes |\beta_1\rangle, |\varphi_2\rangle = |\alpha_2\rangle \otimes |\beta_2\rangle$ and define the product $\langle\varphi_2| C |\varphi_1\rangle$, where $C = A \otimes B$.*

It will be handy to show

$$U \otimes I = \begin{pmatrix} U_{00}I & U_{01}I \\ U_{10}I & U_{11}I \end{pmatrix} \tag{4.10}$$

Example 9 (Density matrix) *Let us return to Alice, who controls the first qubit of the EPR pair* $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *while Bob controls the second[4, pag. 212]. The density matrix for the pure state* $|\psi\rangle \in A \otimes B$ *is*

$$\begin{aligned}\rho_\psi &= |\psi\rangle\langle\psi| \\ &= \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.\end{aligned}$$

The mixed state of Alice's qubit, which encapsulates all information that could be obtained from any sequence of measurements on Alice's qubit alone on a sequence of identical states $|\psi\rangle$*, is modeled by the density matrix* ρ^A_ψ *obtained from* ρ_ψ *by tracing over Bob's qubit,* $\rho^A_\psi = \mathrm{tr}_B\, \rho_\psi$ *The four entries* a_{00}, a_{01}, a_{10}*, and* a_{11} *for a matrix representing* ρ^A_ψ *in the standard basis can be computed separately:*
$a_{00} = \sum_{j=0}^{1} \langle 0|\langle j||\psi\rangle\langle\psi||0\rangle|j\rangle = \left(\frac{1}{2} + 0\right) = \frac{1}{2}$, $a_{01} = \sum_{j=0}^{1} \langle 0|\langle j||\psi\rangle\langle\psi||1\rangle|j\rangle = (0 + 0) = 0$, $a_{10} = \sum_{j=0}^{1} \langle 1|\langle j||\psi\rangle\langle\psi||0\rangle|j\rangle = (0 + 0) = 0$ $a_{11} = \sum_{j=0}^{1} \langle 1|\langle j||\psi\rangle\langle\psi||1\rangle|j\rangle = \left(0 + \frac{1}{2}\right) = \frac{1}{2}$ *So* $\rho^A_\psi = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$*. By symmetry, the density operator for Bob's qubit is* $\rho^B_\psi = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$*.*

4.1 Exercises

Exercise 15 *Compute* $Z \otimes I\, |\psi^{00}\rangle$

Example 10 *The density matrix of one qubit of an EPR pair,*

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4.11}$$

corresponds to the point $(0, 0, 0)$ *in the center of the sphere, farthest from the boundary. In a technical sense, this state is the least pure single-qubit mixed state possible: it is the maximally uncertain state in that no matter in what basis it is measured, it gives the two possible answers with equal probability. In contrast, for any pure state, there is a basis in which measurement gives a deterministic result. For no state, mixed or pure, do measurements in two different bases give deterministic results, so pure states are as certain as possible.*
This notion of uncertainty can be quantified for general n *-qubit states by an extension of the classical information theoretic notion of entropy. The von Neumann entropy of a mixed state with density operator* ρ *is defined to be*

$$S(\rho) = -\,\mathrm{tr}\,(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

where λ_i are the eigenvalues of ρ (with repeats). As is done for classical entropy, take $0 \log(0) = 0$. The von Neumann entropy is zero for pure states; since the density operator ρ_x for a pure state $|x\rangle$ is a projector, it has a single 1 -eigenvalue with $n - 10$ -eigenvalues, so $S\left(\rho_x\right) = 0$. Observe that the maximally uncertain single qubit mixed state ρ_{ME} has von Neumann entropy $S(\rho) = 1$. More generally, a maximally uncertain n -qubit state has a density operator that is diagonal with entries all 2^{-n}; a maximally uncertain n -qubit state ρ has von Neumann entropy $S(\rho) = n$.

Exercise 16 *Use the following examples to verify the operations,*

- $\left(\sqrt{2}-i\right)-i\left(1-\sqrt{2}i\right)=-2i$
- $\left(3,1\right)\left(3,-1\right)\left(\frac{1}{5}.\frac{1}{10}\right)=2+i$

Exercise 17 *Rewrite*

- $\frac{1+2i}{3-4i}+\frac{2-i}{5i}$
- $(1-i)^4$

Exercise 18 *Probe*

$$\left(z_1+z_2\right)^n=\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}z_1^k z_2^{n-k} \quad (4.12)$$

for $n=1,2,\ldots$ *and* $k=0,1\ldots$

Exercise 19 *Show that* $H^{\otimes n}$ *can be written as*

$$H^{\otimes n}=\frac{1}{\sqrt{2^n}}\sum_{x,y}(-1)^{x\odot y}|x\rangle\langle y|. \quad (4.13)$$

Write out matrix representation for $H^{\otimes 2}$*. In* (4.13)*, we use symbol* $\odot$ *to represent the module-2 dot product, sometimes people use:* $\cdot$ *or* $\bullet$*. Mod-2 product is defined by*

$$x\odot y=x\bullet y=x\cdot y=$$
$$x_0y_0\oplus x_1y_1\oplus x_2y_0\oplus \ldots\oplus x_{n-1}y_{n-1}$$

Chapter 5

Quantum Circuits

This model (Quantum Gates [go to slides]) is inspired by the classical gates with their truth table[1, pag. 12],

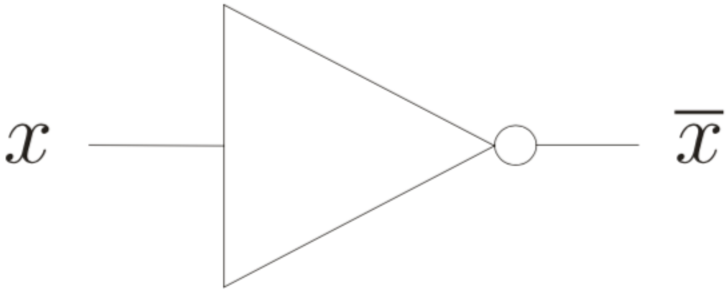


Figure 5.1: NOT logical classical gate

corresponding truth table is shown in the table (5.1)

x	y
0	1
1	0

(5.1)

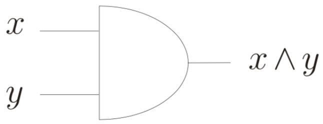


Figure 5.2: AND logical classical gate

corresponding truth table is shown in the table (5.2)

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

(5.2)

Since QC is related to a theory of reversible computing, we note that the NOT gate is reversible while the AND gate is not.

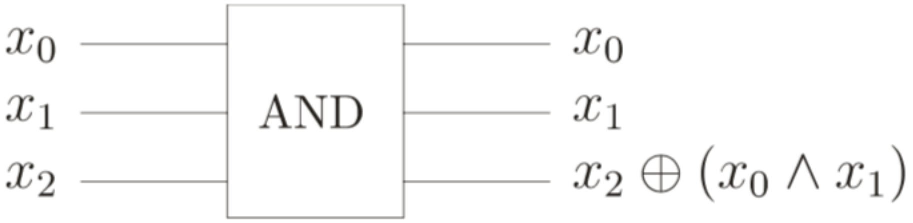


Figure 5.3: Non-reversible AND gate

Example 11 (Simulating a non-reversible AND gate)

With the circuit in the fig. 5.3, we can simulate a non-reversible gate, besides, we keep a copy of the inputs and add of the $x_0 \wedge x_1$ operation, after it adds previous result to x_2. We fix $x_2 = 0$ and obtain a non-reversible AND gate. Where $\oplus$ represents the logical exclusive-OR operation, which it is the same addition modulo two.
Then, we can obtain a reversible version of the circuit if we replace the irreversible parts with their reversible counterparts.

Example 12 (CNOT (3.25)) *Consider the gate proposed in the section Controlled-NOT, the corresponding circuit is given by,*

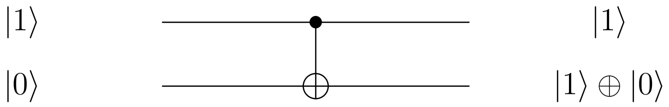


Figure 5.4: Controlled-NOT gate

Chapter 6

Advances topics: Algorithms and circuits

6.1 Why introduce density matrices?

They are very useful for situations in which one doesn't know precisely which state one is in.
Suppose our qbit could either be in the state $|\psi\rangle$, with probability P_ψ, or in the State $|\phi\rangle$, with probability P_ϕ. What is the expectation value of some observable A, e.g. I_z?
The answer should be given by: $P_\psi\times$ expectation value of A for $|\psi\rangle$ plus $P_\phi\times$ expectation value of A for $|\phi\rangle$

$$P_T = P_\psi \langle\psi| A |\psi\rangle + P_\phi \langle\phi| A |\phi\rangle .$$

Define

$$\rho = P_\psi |\psi\rangle \langle\psi| + P_\phi |\phi\rangle \langle\phi| ,$$

Expectation value $= \mathrm{tr}(\rho A)$ So ρ is a useful way of describing statistical mixtures of states: features: Hermitian. $\rho = \rho^\dagger$, and normalization: $\mathrm{tr}(\rho) = 1$.

6.2 Eigenvalues and Eigenvectors

Find the eigenvectors of $\sigma_Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$.
Suppose λ are the eigenvalues of the matrix. The characteristic equation for the matrix is $\det(\sigma_Y - \lambda I) = 0$

$$(0-\lambda)(0-\lambda) - (-i\cdot i) = 0 \quad \Rightarrow \lambda = \pm 1$$

Let the eigenvector be $\begin{pmatrix} x \\ y \end{pmatrix}$
Then the eigenvector corresponding to $\lambda = 1$ we have

$$\sigma_Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix} \quad \Rightarrow \quad \begin{matrix} -iy = x \\ ix = y \end{matrix} \quad \Rightarrow \begin{matrix} x = 1 \\ y = i \end{matrix}$$

Normalizing this eigenvector we have the normalization factor $\sqrt{1^2+1^2} = \sqrt{2}$.

So the required normalized eigenvector corresponding to $\lambda = 1$ is

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

Then the eigenvector corresponding to $\lambda = -1$ we have

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix} \quad \Rightarrow \quad \begin{aligned} -iy &= -x \\ ix &= -y \end{aligned} \Rightarrow \begin{aligned} x &= 1 \\ y &= -i \end{aligned}$$

Normalizing this eivenvector we have the normalization factor $\sqrt{1^2 + 1^2} = \sqrt{2}$. So the required normalized eigenvector corresponding to $\lambda = 1$ is

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$

So the eigenvectors corresponding to each eigenvalues are

$$\lambda = 1 \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \quad \lambda = -1 \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$$

Bibliography

[1] Phillip Kaye, Raymond Laflamme, and Michelle Mosca. *An introduction to quantum computing*. Oxford Univ. Press, 2007.

[2] David McMahon. *Quantum computing explained*. John Wiley & Sons, 2007.

[3] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[4] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Comput. Surv.*, 32(3):300–335, September 2000.