

# Mathematics of Quantum Computing

(Tentative Title)

A report submitted in partial fulfillment  
of the requirement for the degree of

**MASTER OF SCIENCE  
IN  
MATHEMATICS**

by

**Pranay Raja Krishnan**

22MMT002

Under the guidance of

**Dr. Trivedi Harsh Chandrakant**



**Department of Mathematics  
The LNM Institute of Information Technology,  
Rupa ki Nangal, Post-Sumel, Via-Jamdoli, Jaipur,  
Rajasthan 302031 (INDIA).**

# Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

# Certificate

This is to certify that the dissertation entitled **Mathematics of Quantum Computing (Tentative Title)** submitted by **Pranay Raja Krishnan** (22MMT002) towards the partial fulfillment of the requirement for the degree of Master of Science (M.Sc) is a bonafide record of work carried out by him at the Department of Mathematics, The LNM Institute of Information Technology, Jaipur, (Rajasthan) India, during the academic session 2023-2024 under my supervision and guidance.

**Dr. Trivedi Harsh Chandrakant**  
**Assistant Professor**  
**Department of Mathematics**  
**The LNM Institute of Information**  
**Technology, Jaipur**

# Acknowledgements

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Date: September 4, 2023

Pranay Raja Krishnan

# List of Notations

Unless explicitly defined the following notations are used.

**TODO:** Add Required Notation

Symbol	Meaning
$\subseteq$	subset or equal to
$\not\subseteq$	not subset
$\supseteq$	superset or equal to
$\emptyset$	empty set
$\in$	belongs to
$\notin$	does not belong to
$\prod_{i \in I}$	product over index set $I$
$\mathbb{C}$	the set of complex numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{N}$	the set of natural numbers

# Contents

<b>Abstract</b>	<b>i</b>
<b>Certificate</b>	<b>ii</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>List of Notations</b>	<b>iv</b>
<b>1 Qubits</b>	<b>1</b>
1.1 Superposition . . . . .	2
1.2 Measurement . . . . .	3
1.3 Entanglement . . . . .	6
1.4 Transformation . . . . .	7
<b>2 Gates</b>	<b>8</b>
2.1 Gates on a single Qubit . . . . .	9
2.2 Gates on Multiple Qubits . . . . .	10
<b>Bibliography</b>	<b>11</b>

# Chapter 1

## Qubits

---

The computers we use today rely on classical information theory, which are based on **bits** (binary digits) which can represent a 0 or 1 state. These **classical computers** are equivalent to a Turing Machine in computational efficiency.

On a quantum computer the **qubit** (quantum bit) is the basic unit of information.

In labs, qubits have been implemented using photon polarization, electron spin, the ground/excited state of an atom in a cavity, and even defect centers in a diamond. In this paper, we will define a qubit as an abstracted mathematical object and expect that every real-world implementation follow the same rules.

**Definition 1.0.1** (Qubit): A **qubit** is any quantum mechanical system which is associated with 2-dimensional complex Hilbert space  $\mathcal{H}$  (known as the **state space** and follows the below principles:

- Principle of Superposition
- Principle of Measurement
- Principle of Entanglement
- Principle of Transformation

A given state of the system is completely described by a *unit vector*  $|\psi\rangle$ , which is called the **state vector** (or wave function) on the Hilbert Space

The principles in the above definition will be elaborated on in the upcoming sections.

**Notation 1.0.2:** Observe above that we have written the vector  $\vec{\psi} \in \mathcal{H}$  as  $|\psi\rangle$ . This is the notation for a vector in Dirac's bra/ket notation, and is read **ket psi**

## 1.1 Superposition

**Lemma 1.1.1** (Principle of Superposition): Suppose  $|\psi\rangle$  and  $|\sigma\rangle$  are two perfectly distinguishable quantum states of a quantum system, and  $\alpha, \beta \in \mathbb{C}$  with  $\alpha^2 + \beta^2 = 1$ . Then  $\alpha|\psi\rangle + \beta|\sigma\rangle$  is a valid state of the quantum system.

The principle of superposition says that any linear combination of two orthogonal states is a valid state of the qubit. This leads to qubits being referred to as **two-state** quantum systems. These orthogonal states act as the basis elements of the Hilbert space  $\mathcal{H}$  modelling the qubit.

When working with Hilbert spaces associated with quantum systems, we normally use *orthonormal bases*.

**Definition 1.1.2:** The **computational basis** for the two dimensional complex vector space  $\mathcal{H}$  is  $\{|0\rangle, |1\rangle\}$  where  $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

With respect to the computational basis  $\{|0\rangle, |1\rangle\}$ , the state of the qubit can be described as

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \text{ where } a, b \in \mathbb{C} \text{ and } a^2 + b^2 = 1.$$

Another commonly used orthonormal basis for the Hilbert space  $\mathcal{H}$  modelling a qubit is the Hadamard Basis.

**Definition 1.1.3:** The **Hadamard Basis** for the two dimensional complex vector space  $\mathcal{H}$  is  $\{|+\rangle, |-\rangle\}$  where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ and } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$



## 1.2 Measurement

The principle of superposition might indicate that we can use the continuum state of single qubit to store an infinite amount of information. However, a principal of quantum mechanics states that we cannot interact with the qubit without fundamentally altering its state. To know the state stored in a qubit, we must perform a measurement which forces the state of the qubit to "collapse" into one of two *preferred states*.

**Lemma 1.2.1** (Principle of Measurement): Any measurement device that interacts with the qubit will be calibrated with a pair of orthonormal vectors called the **preferred basis**, say  $\{|u\rangle, |v\rangle\}$ . If the state of the qubit with respect to the preferred basis is  $|\psi\rangle = a|u\rangle + b|v\rangle$ , then measurement of the qubit will yield either  $|u\rangle$  with a probability of  $|a|^2$  or  $|v\rangle$  with a probability  $|b|^2$ .

After measurement, the state of the qubit itself will be changed to the output of the measurement.

This principle can be formalised in a manner which couples the preferred basis and the result in a tighter way.

‘TODO: Add Von Neumann Projection‘ ‘TODO: Add Self Adjoint Operators formalism‘

‘TODO: Add Appendix with POVM Formalism‘ ‘TODO: Make appendix with observables type of measurement and POVM, refer shor lec04‘

‘From Scherer‘

**Definition 1.2.2:** An **observable** is a physically measurable quantity of a quantum system which is represented by a self-adjoint operator on a Hilbert space

**Lemma 1.2.3:** In a qubit represented by Hilbert space  $\mathcal{H}$ , the possible measurement values of an observable are given by the spectrum  $\sigma(A)$  of the self adjoint operator  $A$  representing the observable. The probability  $p_\psi(\lambda)$  that a quantum system in the pure state  $|\psi\rangle \in \mathcal{H}$  yields the eigenvalue  $\lambda$  of  $A$  upon measurement is given by the projection  $P_\lambda$  onto the eigenspace  $\text{Eig}(A, \lambda)$  of  $\lambda$  as  $p_\psi(\lambda) = \|P_\lambda |\psi\rangle\|^2$

**Definition 1.2.4:** Let  $\mathcal{H}$  be a Hilbert space. We call states  $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle \in \mathcal{H}$  perfectly distinguishable if there exists a measurement system  $\{M_i\}_{i=1}^m$  with  $m \geq n$  such that  $\|M_j |\psi_1\rangle\|^2 = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

Here *perfectly distinguishable* means that there is some experiment or experimental setup that can distinguish between these two states, atleast in theory.

**Result 1.2.5:** The states  $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$  are perfectly distinguishable if and only if they are orthogonal. This result is the reason we use orthogonal basis in quantum computing.

‘TODO: Refer Nielsen, Chuang

This property limits the amount of information that can be extracted from a qubit: a measurement yields atmost a single classical bit worth of information. In most cases, we also cannot make more than one measurement of original state of the qubit. On measurement, we have two possibilities, each corresponding to a probability of  $|a|^2$  and  $|b|^2$ , then the total probability of the whole space will be  $|a|^2 + |b|^2 = 1$ , which is valid for unit vectors  $|\psi\rangle = a|0\rangle + b|1\rangle$ .

**Notation 1.2.6:** When  $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ , then  $\langle\psi|$  is the conjugate transpose of  $|\psi\rangle$  and is read as **bra psi**,  $\langle\psi| = [\bar{a} \ \bar{b}]$

This lets us write the inner product for  $\mathcal{H}$  as: For any  $|v\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, |w\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \in \mathcal{H}$ , the operation  $\langle v|w\rangle = \langle v| |w\rangle = [\bar{a} \ \bar{b}] \begin{bmatrix} c \\ d \end{bmatrix} = \bar{a}c + \bar{b}d$   
We will consider the inner product as being linear in the second variable and conjugate-linear in the first variable.

**Remark 1.2.7:** If  $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ , then we can show  $\langle 0|\psi\rangle = a, \langle 1|\psi\rangle = b$ .  
Therefore we can write  $|\psi\rangle = a|0\rangle + b|1\rangle = \langle 0|\psi\rangle |0\rangle + \langle 1|\psi\rangle |1\rangle$ .

**Remark 1.2.8:** The standard inner product of the  $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$  with itself in the Hilbert space  $\mathcal{H}$  can therefore be written as  $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle = \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = |a|^2 + |b|^2 = 1$

**Lemma 1.2.9** (Principle of Measurement): Any physical observable is associated with a self-adjoint operator  $\mathcal{A}$  on the Hilbert space  $\mathcal{H}_S$ . The possible outcome of a measurement of the observable  $\mathcal{A}$  is one of the eigenvalues of the operator  $\mathcal{A}$ .

Writing the eigenvalues equation,  $\mathcal{A}|i\rangle = a_i|i\rangle$  where  $|i\rangle$  is an orthonormal basis of eigenvectors of the operator  $\mathcal{A}$ , and  $|\psi\rangle = \sum_i c_i|i\rangle$ , then the probability that a measurement of the observable  $\mathcal{A}$  results in the outcome  $a_i$  is given by  $p_i = |\langle i|\psi\rangle|^2 = |c_i|^2$

‘TODO: Proof that self-adjoint matrices represent measurement operators‘

‘TODO: Relation of POVM and matrices‘

Let  $\mathcal{H}_1$  be an  $n$ -dimensional vector space with basis  $\alpha = \{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$  and  $\mathcal{H}_2$  be an  $m$ -dimensional vector space with basis  $\beta = \{|b_1\rangle, |b_2\rangle, \dots, |b_m\rangle\}$ , then the tensor product  $\mathcal{H}_1 \otimes \mathcal{H}_2$  is an  $nm$ -dimensional space with basis elements of the form  $|a_i\rangle \otimes |b_j\rangle$

**Notation 1.2.10:** In dirac’s bra/ket notation, the tensor product of  $|v\rangle \in \mathcal{H}_1, |w\rangle \in \mathcal{H}_2$  is  $|vw\rangle = |v\rangle|w\rangle = |v\rangle \otimes |w\rangle$

The tensor product is defined to satisfy the following properties:

1.  $(|v_1\rangle + |v_2\rangle)|w\rangle = |v_1\rangle|w\rangle + |v_2\rangle|w\rangle$
2.  $|v\rangle(|w_1\rangle + |w_2\rangle) = |v\rangle|w_1\rangle + |v\rangle|w_2\rangle$
3.  $(a \cdot |v\rangle)|w\rangle = |v\rangle(a \cdot |w\rangle) = a \cdot (|v\rangle|w\rangle)$

Every element  $|\sigma\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$  can be written as a superposition of elements of the basis  $\{|a_i\rangle|b_j\rangle\}$  as  $|\sigma\rangle = \alpha_{11}|a_1b_1\rangle + \alpha_{12}|a_1b_2\rangle + \dots + \alpha_{nm}|a_nb_m\rangle$ .

Most elements  $|\sigma\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$  *cannot* be decomposed to  $|\sigma\rangle = |v\rangle|w\rangle$  where  $v \in \mathcal{H}_1, w \in \mathcal{H}_2$ . ‘TODO: Check proof‘

## 1.3 Entanglement

As we have observed, a single qubit only gives us one classical bit worth of information. This equivalence diverges once we include \*multiple\* interacting qubits in the system. A system of  $n$  classical bits will have one degree of freedom for each bit, resulting in a state-space of  $n$  dimensions, i.e. classical systems are linear in  $n$ . In quantum systems, however, a system of  $n$  qubits will result in a state space of  $2^n$  dimensions. This is because of the quantum property of \*entanglement\* which describes how quantum systems interact with each other.

**Lemma 1.3.1** (Principle of Entanglement): When we have two qubits being treated as a combined system, the state space of the combined system is the tensor product  $\mathcal{H}_1 \otimes \mathcal{H}_2$  of the state spaces  $\mathcal{H}_1, \mathcal{H}_2$  of the component qubit subsystems. If the first qubit is in state  $|\psi\rangle$  and the second in state  $|\sigma\rangle$ , then the combined system of two interacting qubits is in state  $|\psi\sigma\rangle = |\psi\rangle|\sigma\rangle$ . Similarly, for a system of  $n$  qubits, the state space is the tensor product  $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_n$  of the state spaces of the  $n$  independent qubits.

The most natural basis for  $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$  is constructed from the tensor products of the basis vectors of  $\mathcal{H}_1$  (say  $\{|0\rangle_1, |1\rangle_1\}$ ) and of  $\mathcal{H}_2$  (say  $\{|0\rangle_2, |1\rangle_2\}$ ), then a basis for  $\mathcal{H}$  is given by  $\{|0\rangle_1|0\rangle_2, |0\rangle_1|1\rangle_2, |1\rangle_1|0\rangle_2, |1\rangle_1|1\rangle_2\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ .

We will often this basis as  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$  when the context is unambiguous. So an arbitrary state  $|\psi\rangle \in \mathcal{H}$  can be described as  $|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle = c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle$ .

**Definition 1.3.2:** A state  $|\psi\rangle$  is said to be **entangled** if it cannot be written as a simple tensor product of states  $|v\rangle \in \mathcal{H}_1$  and  $|w\rangle \in \mathcal{H}_2$ . If we can write  $|\psi\rangle = |v\rangle|w\rangle$ , the state is said to be **seperable**.

**Example 1.3.3:** Consider the state  $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ . We can show this is entangled. ‘TODO‘

**Example 1.3.4:** Consider the state  $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$ . We can show this is seperable since we can write  $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$

## 1.4 Transformation

**Lemma 1.4.1** (Principle of Transformation): Isolated Quantum states evolve unitarily, i.e. for an isolated system there exists a unitary matrix  $U_t$  such that  $|\psi_t\rangle = U_t |\psi_0\rangle$  where  $|\psi_0\rangle$  is the starting state and  $|\psi_t\rangle$  is the state at time  $t$ .

**Definition 1.4.2:** An observable is a physically measurable quantity of a quantum system which is represented by a self-adjoint operator on a Hilbert space.

**Definition 1.4.3:** A matrix is said to be **unitary** if and only if one of the following conditions hold:

1.  $U^\dagger U = I$
2.  $U U^\dagger = I$
3. the columns of  $U$  are orthonormal vectors
4. the rows of  $U$  are orthonormal vectors

‘Alternate from Scherer‘

**Definition 1.4.4:** An operator  $U$  on  $H$  is called **unitary** if  $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$  for all  $|\psi\rangle, |\phi\rangle \in \mathcal{H}$

# Chapter 2

## Gates

---

**Proposition 2.0.1:** Gates are described by unitary matrices.

*Proof.* Let  $M$  be a transformation of a quantum qubit state  $|\psi\rangle$ . Physics says that the evolution of an isolated quantum system is linear, so the transformation  $M$  can be described by a matrix.

For any state  $|\psi\rangle$ ,  $M|\psi\rangle$  has to be a unit vector.

If  $M|\psi\rangle$  is a unit vector, the inner product with itself is 1.

$$\implies \langle (M|\psi\rangle) | (M|\psi\rangle) \rangle = 1$$

$$\implies \langle \psi | M^\dagger M | \psi \rangle = 1$$

$$\implies M^\dagger M = I \text{ where } I \text{ is the identity matrix}$$

$$\implies M \text{ is unitary}$$

□

Since  $UU^\dagger = I$ , we can conclude that every unitary matrix is invertible. This leads to the following result:

**Result 2.0.2:** Only reversible gates can be implemented in quantum computing and any reversible gate has a quantum analog.

This shows us that the classical NOT gate has a quantum analog but NAND does not.

Any unitary  $2 \times 2$  matrix is a valid gate but only a few are used in practice.

‘TODO Notation  $|\rangle \langle|$ ‘

## 2.1 Gates on a single Qubit

**Definition 2.1.1** (Pauli Gates):  $I, X, Y, Z$  are known as the Pauli gates and are defined as:

1.  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$
2.  $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$
3.  $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1|$
4.  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

‘TODO: Effect of the Pauli Gates on the Bloch Sphere’

**Definition 2.1.2** (Hadamard Gate): The **Hadamard Gate** is the transformation  $H : \mathcal{H} \rightarrow \mathcal{H}$  such that

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$   $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$ . It is defined by the matrix  $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = |0\rangle\langle +| + |1\rangle\langle -|$

The Hadamard gate allows us to obtain a superposition state.

**Remark 2.1.3:** The Hadamard gate is its own inverse.

$$H^2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$$

**Remark 2.1.4:**  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left( \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}}(X + Z)$

**Definition 2.1.5:** The  **$z$ -Phase Gate**  $R_z$  defines a rotation about the  $z$ -axis by an angle  $\theta$  on the Bloch sphere. ‘TODO: Bloch Sphere’

It is given by  $R_z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} = |0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|$

The  **$y$ -Phase Gate** defines a rotation about the  $y$  axis and is defined by

$$\begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}$$

The  **$x$ -Phase Gate** defines a rotation about the  $x$  axis and is defined by

$$\begin{bmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}$$

## 2.2 Gates on Multiple Qubits

**Definition 2.2.1:** The **CNOT gate** is a gate that acts on 2 qubits which flips the second bit if the first bit is in the  $|1\rangle$  state.

It is defined by the matrix  $\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

The CNOT gate allows us to obtain an entangled state.

**Definition 2.2.2:** The **Toffoli gate** is a gate that acts on 3 qubits that flips the third bit if the first two are in the  $|1\rangle$  state.

Depending on the input the Toffoli gate can function as an AND, NOT and NAND gate. Since the NAND gate is universal, the Toffoli is as well. The Toffoli gate is also unitary which means it is a valid quantum gate. This shows that every classical circuit can be implemented as a quantum circuit.



# Bibliography

- [1] Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.
- [2] Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus.
- [3] Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis.
- [4] Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices.
- [5] Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl.
- [6] Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante.