# Quantum Information Theory and the No-Cloning Theorem

Alex Zhang

May 2021

## 1 Introduction

For the past half a century, classical computers and their operations have been primarily developed through studies on classical information theory, where information is fundamentally built from units that take either the value of 0 or 1, more formally known as classical bits. However more recently, there has been increased attention towards the application of quantum-effects and concepts to store and transmit information. This field, known as quantum information theory, is an extension of classical information theory that uses a different fundamental unit, the *qubit*, to store information. While a classical bit can only be two possible states, the state of a qubit is the superposition of two states, and therefore can theoretically encode an infinite number of classical bits. Additionally, it is possible for information between multiple qubits to be correlated in a way that is fundamentally impossible for classical bits to achieve through a phenomenon known as *quantum entanglement*. Nevertheless, there are certain limitations within quantum information theory such as the no-cloning theorem that was proved in 1982 by Wootters and Zurek [9] that lead to interesting discussions on the formulation of quantum algorithms and their implications.

## 2 Background

In the study of physics, a physical system is generally described by its state; that is, what is going on in the system itself. An isolated system is one in which energy does not flow in or out of the system, and there are no external forces on the system. For the rest of the paper, we consider any defined system to be isolated, although in practice this is not technically the case unless we consider everything to be one giant isolated system. We begin with four major postulates surrounding quantum mechanics stated from [1], then move onto a discussion of classical versus the more recent quantum information theory, and finally conclude with a proof and discussion on the no-cloning theorem that develops the relationship between classical and quantum information theory.

## Postulate I: The Hilbert Space

In quantum mechanics, an isolated physical system has an associated inner product space $H$ such that the state of the physical system is described by a unit vector $u \in H$. $H$ is generally described to be a *Hilbert Space*, whose properties are described below:

A Hilbert space $H$ is a vector space with an inner product such that the norm is described by

$$\text{Given } u \in H, \quad ||u|| = \sqrt{\langle u, u \rangle}$$

with the property that the metric defined by the norm is complete. In other words, every Cauchy sequence of elements converges to an element in the space.

Examples of a complete metric space would be $\mathbb{R}^k$ for positive $k$, as proved in intro to analysis. It should be noted that Hilbert spaces are generally defined to be infinite-dimensional [3]. However, more recently finite-dimensional inner product spaces with the properties above have also been defined to be Hilbert spaces.

**Proposition:** The complex vector space $\mathbb{C}^n$ with the Euclidean inner product is a Hilbert space.
**Proof:** Clearly $\mathbb{C}^n$ is a vector space. Using the norm described for $\mathbb{C}^n$ with the Euclidean inner product,

$$\text{Let } u = (x_1 + iy_1, x_2 + iy_2, ..., x_n + iy_n) \in \mathbb{C} \text{ for } x_1, ..., x_n, y_1, ..., y_n \in \mathbb{R}$$

$$||u|| = \sqrt{x_1^2 + y_1^2 + ... + x_n^2 + y_n^2}$$

Notice that the metric on $\mathbb{C}^n$ induced by the norm above is same as the Euclidean metric on $\mathbb{R}^{2n}$ induced by the Euclidean norm, where we describe $u = (x_1, y_1, x_2, y_2, ..., x_n, y_n) \in \mathbb{R}^{2n}$. Therefore, because the Euclidean space $\mathbb{R}^k$ for positive $k$ is known to have a metric that is complete[6], it follows that $\mathbb{C}^n$ also has a metric that is complete. Thus, $\mathbb{C}^n$ with the Euclidean inner product is a Hilbert space. $\square$

For simplicity, we will work on a 2-dimensional Hilbert space $\mathbb{C}^2$ with a canonical basis $\{|0\rangle, |1\rangle\}$. Note that describing a vector in the form $|\cdot\rangle$ is called Dirac notation, where its corresponding dual vector is denoted as $\langle\cdot|$. We can also define function composition from a linear operator $A$ and $\langle\varphi|A$ as [1]

$$(\langle\varphi|A)|\psi\rangle = \langle\varphi|(A|\psi\rangle) \tag{1}$$

As mentioned earlier, the state of our physical system is described a unit vector $|\varphi\rangle$, which can be written as a linear combination of our canonical basis:

$$|\varphi\rangle = a|0\rangle + b|1\rangle \text{ where } |a|^2 + |b|^2 = 1$$

Compared to the case of classical bits which can be represented as either 0 or 1, we note that our unit vector $|\,\varphi\rangle$ is represented as a superposition of $|0\rangle$ and $|1\rangle$. We call this system a *qubit*, which is the quantum analog to the classical bit in information theory. We will further discuss the significance of working with qubits in **section 3**.

## Postulate II: Evolution of the State of a System

In quantum mechanics, the time evolution of the state $|\,\varphi_t\rangle$ of a closed quantum system is described using Schrödinger's Equation,

$$i\hbar\frac{d|\,\varphi_t\rangle}{dt} = U|\,\varphi_t\rangle$$

where $\hbar$ is Planck's constant and $U$ is an isometry called the Hamiltonian of the system. The analog below follows from the above postulate:

Suppose we can describe the system at time $t_1$ as $|\,\varphi_{t_1}\rangle$ and the system at time $t_2 > t_1$ as $|\,\varphi_{t_2}\rangle$. Then there exists an isometry $U \in \mathcal{L}(H)$ such that

$$|\,\varphi_{t_2}\rangle = U|\,\varphi_{t_1}\rangle$$

Part of Postulate II is that any isometry describes a certain evolution on the state of a physical system. In the case of *qubits*, there are several common isometries called the *Pauli Matrices* that are used as logical gates in quantum circuits. These isometries often have classical gate analogs.

**Example I:**
Below are a few examples of matrices of isometries with respect to the computational basis:

$$\mathbf{1} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \sigma_x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$
$$\sigma_y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \quad \sigma_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

## Postulate III: Measurement Operators

While a quantum state is in constant superposition with probabilities determined by the amplitudes of the state, we ultimately need a way to measure the state. Postulate III states that there exists a collection of operators $\{M_n\}_n$ that describe a measurement on a quantum state in a Hilbert space $H$ such that given a state $|\,\varphi\rangle$ prior to measurement, the probability that the outcome $S$ of measuring the state $M(|\,\varphi\rangle)$ is $n$ is

$$\mathbb{P}(S = n) = \langle\varphi\,|M_n^* M_n|\,\varphi\rangle$$

and the state after measurement is

$$\frac{M_n|\,\varphi\rangle}{\sqrt{\mathbb{P}(S=n)}}$$

The above probabilities also satisfy the laws of probability, so

$$\sum_n M_n^* M_n = I$$

**Example II**
Considering $H = \mathbb{C}^2$, the collection of measurement operators is defined as

$$M_0 = |0\rangle\langle 0| \quad \text{and } M_1 = |1\rangle\langle 1|$$

Notice that these operators are projections that sum to **1**. We also see that for an arbitrary state $|\,\varphi\rangle = a|0\rangle + b|1\rangle$,

$$\mathbb{P}(S = 0) = |a|^2 \text{ and } \mathbb{P}(S = 1) = |b|^2$$

as expected from our discussion of superposition and amplitudes in the section on **Postulate I**.

In the above example the measurement operators were projections, although this is not always necessarily true. There are a class of measurements known as **projective measurements** that consist of orthogonal projections that are extremely useful for computations. Measurement operators on quantum systems are a very important topic with a rich set of research attached; while they will not be discussed much further in this write-up, they are relevant for most quantum information theory topics.

## Postulate IV: State of Composite Quantum Systems

We can often model quantum systems by composing them into a larger, composite quantum system. Postulate IV states that we can represent the state of this composition system as a tensor product of the states of the individual systems,

$$|\,\varphi_1\rangle \otimes ... \otimes |\,\varphi_m\rangle$$

An intuitive explanation for why this representation is a tensor product rather than a Cartesian product is that when describing general probability distributions for an $m$-composite system with $n$ unique states, it is easier to deal with a vector space with $mn$ dimensions, where each basis vector corresponds to a unique system and state pair [6].

An important part of postulate IV is that there exists non-elementary tensor products in the tensor product of several Hilbert spaces, which allow for a special property known as *quantum entanglement* where the quantum states of multiple particles cannot be described independently of each other (section 3.1) [10].

**Example III**
A common example of such a tensor product is the Bell state $|\,\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|\Phi^+\rangle = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$$

# 3 Representation of Information

In the previous section, we discussed the representation of quantum bits and their relation to physical systems. We now focus more on the computational aspect of quantum information and stray away from the influence of physical factors. In 1948, Claude Shannon published a revolutionary paper on information theory [4] that led to advances in data compression, communication, and error correction systems. The basic unit of information in classical information theory, which we know as the **bit**, takes on states in $\{0, 1\}$, and is what we use to store information in our modern computing devices. The qubit introduced in Postulate I is the quantum analog to the bit, which can take a superposition of the classical bit states until it is measured. In the following example, we show why qubits are of interest in information theory as a new basic unit of information:

**Example IV: Superdense Coding**
Suppose Noah wants to send two classical bits of information $d \in \{00, 01, 10, 11\}$ to his friend Areeq. We consider a Bell state qubit pair, where the first qubit is shared between Noah and Areeq beforehand. Noah can actually send a single qubit (the other Bell state qubit) to Areeq to transmit two classical bits of information. The importance of such a system is that the first qubit can be shared/sent at any time in the past independent of the time that the second qubit is send any two bits of information [11].

For clarity, the Bell state represents the state of both qubits, which are entangled as mentioned in Example III. So

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

where the first index in each tensor product represents the first qubit, and the second index in each tensor product represents the second qubit. Assume that the second qubit represents the shared qubit which is fixed, and the first qubit represents the qubit to be sent. Then we see that Noah can prepare his qubit by applying the isometries from Example I,

$$\begin{cases} \text{Applying } \mathbf{1} & \frac{|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{\sqrt{2}} \\ \text{Applying } \sigma_x & \frac{|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle}{\sqrt{2}} \\ \text{Applying } \sigma_z & \frac{|0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle}{\sqrt{2}} \\ \text{Applying } i\sigma_y & \frac{-|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle}{\sqrt{2}} \end{cases}$$

So the bell state changes accordingly. But the above set of transformations results in a basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ known as the *Bell basis*, in which by Postulate II there exists a convenient measurement so we can extract a certain 2-bit string

with probability 1:

$$\begin{cases} \frac{|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{\sqrt{2}} & \to 00 \\ \frac{|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle}{\sqrt{2}} & \to 10 \\ \frac{|0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle}{\sqrt{2}} & \to 01 \\ \frac{-|1\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle}{\sqrt{2}} & \to 11 \end{cases}$$

Since Areeq now has the entire Bell state, he can convert based using measurements based on the above basis to decode the 2-bit string that Noah sent.

From the example above it would seem as though the qubit is more efficient than the bit in terms of data movement operations. However, there are a few limitations to qubit computation, especially in data manipulation, that make working with quantum information more difficult. The next section describes the no-cloning theorem, which implies that data copying techniques must be more complicated in quantum systems.

# The No-cloning Theorem

In classical information theory, the use of an XOR gate allows us to take an unknown bit $x$ as a control bit and clone it into a target bit $y$ [3]. The following theorem implies that the quantum analog to the XOR gate, known as the CNOT gate, does not have the same effect:

**Theorem:** It is impossible to clone an unknown pure quantum state from a unitary evolution.

**Proof:** Suppose we are given two quantum systems $A$ and $B$ on a common Hilbert space $H$ where the state of $A$, denoted as $|\,\varphi\rangle_A$, is unknown. We have some initial state of the composite system defined as

$$|\,\varphi\rangle \otimes |\sigma\rangle_B$$

where $|\,\varphi\rangle$ is the unknown state to be copied and $|\sigma\rangle$ is some state independent of state $A$ that will be replaced with a copy of state $A$. We also assume that the state of $A$ and $B$ are pure tensors; that is that they can be represented as a single elementary tensor.

We want to show that there does not exist an isometry $U$ on $H \otimes H$ such that

$$U(|\,\varphi\rangle_A \otimes |\sigma\rangle_B) = |\,\varphi\rangle_A \otimes |\,\varphi\rangle_B \tag{2}$$

For simplicity, we use the notation

$$|\,\varphi\rangle \otimes |\sigma\rangle = |\,\varphi\rangle|\sigma\rangle$$

Suppose for the sake of contradiction that (2) is true. It follows that given two arbitrary pure states $|\,\varphi\rangle$ and $|\psi\rangle$,

$$U(|\,\varphi\rangle_A \otimes |\sigma\rangle_B) = |\,\varphi\rangle_A \otimes |\,\varphi\rangle_B$$

$$U(|\psi\rangle_A \otimes |\sigma\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B$$

If we take the inner product of the two states $\varphi, \psi$ and some arbitrary basis vector $e$ with norm 1,

$$\langle\varphi\,|\psi\rangle = \langle\varphi\,|\psi\rangle\langle e|e\rangle$$

Using the function composition definition of Dirac notation in (1),

$$= \langle\varphi\,|\langle e|(e\rangle)\psi\rangle$$

Using definition 7.37 in [8], that isometries preserve norms/inner products and that an isometry composed with its adjoint is the identity operator, we see that

$$= [\langle\varphi\,|\langle e|U^*][U|\psi\rangle|e\rangle]$$

which based on the Dirac notation can be rearranged as

$$= (|\,\varphi\rangle|e\rangle, U^*U|\psi\rangle|e\rangle)$$

where $(\cdot,\cdot)$ denotes the standard inner product on $H \otimes H$. By the property of adjoints on inner products from [8],

$$= (U|\,\varphi\rangle|e\rangle, U|\psi\rangle|e\rangle)$$

Finally, using (2),

$$= (|\,\varphi\rangle|\,\varphi\rangle, |\psi\rangle|\psi\rangle)$$
$$= \langle\varphi\,|\langle\varphi\,|\psi\rangle|\psi\rangle$$
$$= |\langle\varphi\,|\,\varphi\rangle|^2$$

In other words,

$$|\langle\varphi\,|\psi\rangle| = |\langle\varphi\,|\psi\rangle|^2$$

Because quantum states are described using vectors with norm 1, we see that the above expression implies that either

$$\langle\varphi\,|\psi\rangle = 0 \quad \text{or} \quad \langle\varphi\,|\psi\rangle = 1$$

which we know from 6.23 in [8] implies that either $\varphi$ and $\psi$ are equal or orthonormal. But we assumed $\varphi$ and $\psi$ to be arbitrary unit vectors, in which there exists infinitely many vectors that are non-equal and not orthogonal in $H$. Thus, we have a contradiction, and (2) must not be true, so it must be the case that we cannot clone an unknown pure quantum state from a unitary evolution, and therefore the no-cloning theorem is proved. □

### Generalizing the No-cloning Theorem

The no-cloning theorem makes an assumption that the state being copied is a pure tensor. This assumption is valid because of the Schrödinger–HJW theorem, which proves that mixed states can be "purified" into pure states [12].

### Implications

There are several consequences of the no-cloning theorem. Firstly, classical error correction techniques such as using backup copies of states during computation are impossible [8]. Error correction in quantum systems is already a large problem and the no-cloning theorem forces the development of less intuitive techniques to minimize error.

In quantum cryptography paradigms, the no-cloning theorem actually ensures copies of transmitted keys cannot be made, and is thus important for preventing eavesdroppers from stealing information [8]. Note however that the no-cloning theorem makes no implications on approximate cloning; it only proves that perfect copies of a quantum state cannot be made. Thus, in quantum cryptography there are still probabilistic techniques that can be used to estimate approximate copies of a state.

Finally, there are several corollaries to the no-cloning theorem that fall under the more general family of no-go theorems. For example, the reversed dual of the no-cloning theorem, known as the *no-deleting* theorem, states that given two copies of an arbitrary state, it is impossible to fully delete one of them [13]. A corollary of the no-cloning theorem, known as the *no-broadcasting* theorem, states that it is impossible to broadcast a state to multiple recipients such that each receive their own copy [5]. Each of the theorems impose certain restrictions on quantum computations and have led to the development of numerous quantum algorithms designed to exploit their properties or work-around them.

## 4 Acknowledgements

I would like to thank Professor Yarmola and Professor Ascher for providing some resources and a direction with this project, as well Areeq Hasan from MAT 204 for exploring this topic with me. This topic was very interesting to read into, and I discovered that looking at quantum computing through a primarily linear algebra-based lens has helped me understand a lot of these topics on a more fundamental level.

# References


[1] "Introduction to QIT." [Online]. Available: https://www.icmat.es/miembros/cpalazuelos/Introduction_to_QIT-FInal_versionII.pdf

[2] Weisstein, Eric W. "Hilbert Space." From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/HilbertSpace.html

[3] R. B. Griffiths, "Hilbert Space Quantum Mechanics," p. 13. Available: https://quantum.phys.cmu.edu/QCQI/qitd114.pdf

[4] M. Wilde, "From Classical to Quantum Shannon Theory," arXiv:1106.1445 [quant-ph], 2017, doi: 10.1017/9781316809976.001.

[5] A. Kalev and I. Hen, "The No-Broadcasting Theorem and its Classical Counterpart," Phys. Rev. Lett., vol. 100, no. 21, p. 210502, May 2008, doi: 10.1103/PhysRevLett.100.210502.

[6] "Complete Metric Spaces and Function Spaces" Accessed: May 05, 2021. [Online]. Available: https://faculty.etsu.edu/gardnerr/5357/notes/Munkres-43.pdf.

[7] S. Axler, Linear Algebra Done Right.

[8] "The no-cloning theorem — Quantiki." https://www.quantiki.org/wiki/no-cloning-theorem.

[9] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, p. 802, Oct. 1982, doi: 10.1038/299802a0.

[10] J. M. Landsberg, "A Very Brief Introduction to Quantum Computing and Quantum Information Theory for Mathematicians," in Quantum Physics and Geometry, vol. 25, E. Ballico, A. Bernardi, I. Carusotto, S. Mazzucchi, and V. Moretti, Eds. Cham: Springer International Publishing, 2019, pp. 5–41.

[11] Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S., & Long, G. L. (2005). Quantum secure direct communication with high-dimension quantum superdense coding. Physical Review A, 71(4).

[12] K. A. Kirkpatrick, "The Schrodinger-HJW Theorem," arXiv:quant-ph/0305068, Nov. 2005, [Online]. Available: http://arxiv.org/abs/quant-ph/0305068.pdf

[13] M. Horodecki, R. Horodecki, A. S. De, and U. Sen, "No-deleting and no-cloning principles as consequences of conservation of quantum information," arXiv:quant-ph/0306044, Jun. 2003, [Online]. Available: http://arxiv.org/abs/quant-ph/0306044.