Introduction to Quantum Computation and Information Theory - week 1

Michał Studziński, Bianka Woloncewicz

Gdańsk, Poland, 11-15 July 2022

Abstract

This is a summary of lectures given during the first week of the summer school entitled "Next generation of quantum information scientists. Series of international schools for students in Gdansk". Presented notes are suitable for students who think about doing their master's in quantum computation and information from the perspective of theoretical computer science.

Contents

1 Introduction **2**

2 Introduction to the formalism of quantum information theory **2**
2.1 Quantum state in Hilbert space 3
2.1.1 Quantum state 3
2.1.2 Scalar product of wave functions in $\mathcal{L}^2$ 3
2.2 Dirac notation and some properties of Hilbert space 3
2.2.1 Dirac notation 3
2.2.2 Scalar product and norm in Hilbert space 4
2.2.3 Completeness in Hilbert space 5
2.3 Orthonormal basis 5
2.4 Qubit 6
2.5 Quantum observables 6
2.6 Mathematical digression: trace and its properties 7
2.7 Hermitian observables 7
2.8 Special case of hermitian observable: Projector 7
2.9 Spectral theorem 7
2.10 Postulates of quantum mechanics 8

3 Framework of quantum mechanics and quantum information **9**
3.1 Pure and mixed states 9
3.1.1 Properties of density matrix 10
3.1.2 Bloch sphere representation 11

3.2 The description of composed system 11
3.3 Partial trace 12
3.4 Purification 13
3.5 Fidelity between quantum sates 14
3.6 Quantum entanglement and entanglement criteria 15
3.6.1 Entanglement of pure states 15
3.6.2 Entanglement of mixed states 16
3.7 Quantum channel 16

4 Quantum Teleportation **18**

5 Quantum superdense coding **20**

6 No-cloning theorem **21**

7 BB84 protocol **23**

8 E91 protocol **24**

1 Introduction

Quantum mechanical processes can be exploited to provide new modes of information processing that are beyond the capabilities of any classical computer. This leads to remarkable new kinds of information-theoretic protocols which were previously deemed impossible as well as algorithms (so-called quantum algorithms) that can offer a dramatically increased efficiency for the execution of some computational tasks. In addition to such potential practical benefits, the study of quantum information and computation has great theoretical interest, combining concepts from information theory, computational complexity theory and quantum physics to provide striking fundamental insights into the nature of these disciplines.

2 Introduction to the formalism of quantum information theory

Quantum theory is an ensemble of tools that enable the mathematical description of Nature. We concentrate on the three most essential notions with which we associate physical objects and situations i.e. states, observables and the theory of measurement.

2.1 Quantum state in Hilbert space

2.1.1 Quantum state

In the formalism of quantum mechanics we describe physical systems using quantum states. Quantum state, denoted with a wave function procures a complete description of a such a system. E.g. a spinless particle is described with a wave function $\psi(\vec{r}, t)$ where $\vec{r}$ can denote any parameter that changes in the given time t. The choice of parameter $\vec{r}$ depends on the phenomena that we aim to describe. The wave function "symbolises" the wave-particle duality of physical objects and it encodes the amplitude of probability density of the particle being in the range $(\vec{r}, \vec{r} + \delta\vec{r})$ in the time $(t, t + \delta t)$. Thus, the description of a state with the wave function has fully probabilistic character. Such a interpretation imposes the following:

- p(wherever, whenever) $= 1$,
- If $r \to \infty$ then $\psi(\vec{r}, t) \to 0$,
- $|\psi(\vec{r}, t)|^2 < \infty$ and
- as probabilities sum up to unity: $\int dp = 1$ and $\int dp = \int_{\mathbf{R}^3} d^3r|\psi|^2$ we have $\int_{\mathbf{R}^3} d^3r|\psi|^2 = 1$ what means that ψ is normalised.

For simplicity from now on we will simplify the notation and denote $\psi(\vec{r}, t)$ as ψ. The analysis of ψ is strictly related to the linear space $\mathcal{L}^2$, in which ψ has properties listed above. The linearity of implies that the $\mathcal{L}^2$ superposition principle applies: if ϕ_1 and $\phi_2 \in \mathcal{L}^2$ their superposition (up to the normalisation constant) reads

$$\phi_1 + \phi_2 = \phi_3 \in \mathcal{L}^2.$$

2.1.2 Scalar product of wave functions in $\mathcal{L}^2$

In $\mathcal{L}^2$ we introduce the scalar product $(.,.)$ such that $\forall\ \psi$ and $\phi \in \mathcal{L}^2$ we have

$$(\phi, \psi) = \int_{\mathbf{R}^3} d^3r \quad \phi^*\psi \in \mathbf{C}, \tag{1}$$

where the subscript *denotes the complex conjugate. The scalar product is

2.2 Dirac notation and some properties of Hilbert space

2.2.1 Dirac notation

You cannot deduce it from the previous sections but quantum mechanical mathematical expressions are, indeed, quite complex In order to simplify the notation from now on we will use "bra-ket" notation introduced by Dirac that nowadays is commonly used in quantum optics and quantum information theory. The basic idea is as follows: for any quantum state $\psi(\vec{r}, t)$ we assign a ray, that i.e.:

an equivalence class of vectors that differ by multiplication by a complex scalar. In Dirac notation a vector is denoted by a "ket" $|.\rangle$. We have:

$$\mathcal{L}^2 \ni \psi(\vec{r},t) \rightarrow |\psi\rangle \in \mathcal{H}. \tag{2}$$

Note that $|\psi\rangle$ does not depend anymore of any specific parameter. Also according to the definition of a state given above $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are equivalent. Here we call θ a global phase that is irrelevant. Hilbert space is of $\mathcal{L}^2$ type so the superposition principle applies i.e. if $|\psi_1\rangle$ and $|\psi_2\rangle \in \mathcal{H}$ than

$$|\psi_1\rangle + |\psi_2\rangle = |\psi_3\rangle \in \mathcal{H}$$

.

The complex conjugate of a "ket" is called "bra". We have:

$$|\psi\rangle^* = \langle\psi| \in \mathcal{H}^*, \tag{3}$$

where $\mathcal{H}^*$ is the dual Hilbert space of linear functionals.

2.2.2 Scalar product and norm in Hilbert space

Hilbert space is an abstract vectorial space over complex numbers ($\mathbf{C}$). It is equipped with the scalar product : $\forall\ |\psi\rangle, |\phi\rangle \in \mathcal{H}$ the scalar product $\langle.|.\rangle$ of two vectors reads

$$\langle\psi|\phi\rangle \in \mathbf{C}.$$

It has the following properties:

- positive: $\langle\psi|\psi\rangle > 0$ if $|\psi\rangle \neq 0$.
- linear: $\langle\lambda_1\phi_1 + \lambda_2\phi_2|\psi\rangle = \lambda_1^* \langle\phi_1|\psi\rangle + \lambda_2^* \langle\phi_2|\psi\rangle$,
- skew-symmetric: $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

Also in Hilbert the space scalar product encodes the norm of $|\psi\rangle$

$$||\,|\psi\rangle\,|| = \sqrt{\langle\psi|\psi|\psi|\psi\rangle}. \tag{4}$$

This norm shares similar properties as well-known Euclidian norm in $\mathbf{R}^3$ i.e.:

- positivity $||\,|\psi\rangle\,|| > 0$ if $\psi \neq 0$
- linearity:$\forall\lambda \in \mathbf{C}$ we have $|\lambda_1\,|\phi_1\rangle\,|| + \lambda_2\,|\phi_2\rangle\,|| = |\lambda_1|\,||\,|\phi_1\rangle\,|| + |\lambda_2|\,||\,|\phi_2\rangle\,||$
- and the triangle inequality is fulfilled:$|||\phi+\psi\rangle|| \leq ||\,|\phi\rangle\,|| + ||\,|\psi\rangle\,||$

Obviously, due to the probabilistic character of quantum state $|\psi\rangle$ we have: $||\,|\psi\rangle\,|| = 1$ Also in Hilbert space Cauchy-Schwartz inequality holds:

$$|\,\langle\phi|\psi|\phi|\psi\rangle\,| \leq ||\,|\phi\rangle\,||||\,|\psi\rangle\,||. \tag{5}$$

2.2.3 Completeness in Hilbert space

We specify that we are going to consider only finite-dimensional Hilbert space that is enough for our use. Quantum information happens in the $d \times d$ dimensional space. The Hilbert space of the dimension d will be denoted as $\mathcal{H}^d$ or $dim\mathcal{H} = d$.

Still,it is important to remember that phenomena described with quantum physics in general require infinite dimensional Hilbert space. It is then of key importance to insure that we are able to reach any point in Hilbert space, e.g. perform any measurement on any quantum state from this space. Such a property is guaranteed by the completeness of Hilbert space. A linear space is called complete if each Cauchy series $\{|x_i\rangle\}_{i=1}^{\infty}$ it is convergent in this space i.e.

$$\forall\ \{|x_i\rangle\}_{i=1}^{\infty}\ \in\ \mathcal{H},\ \text{if for subscripts } m \text{ and } n \lim_{n,m\to\infty} \text{and}\ \langle x_n - x_m | x_n - x_m\rangle = 0$$

$$\text{then}\ \exists\ \ |x\rangle \in \mathcal{H}\ \ \text{such that} \lim_{n\to\infty} \langle x - x_n | x - x_n\rangle = 0$$

.

2.3 Orthonormal basis

Let us recap the properties of $|\psi\rangle$ in Dirac notation:

- $|\psi\rangle \in \mathcal{H}$,
- $||\,|\psi\rangle\,|| = 1 = \sqrt{\langle\psi|\psi\rangle}$,
- $|\psi\rangle$ and $\phi \in \mathcal{H}$ also $|\psi\rangle + |\phi\rangle \in \mathcal{H}$.

In Hilbert $\mathcal{H}^d$ space we define an orthogonal basis $\{|x_i\rangle\}_{i=1}^{d} \in \mathcal{H}$ such that $\langle x_i|x_j\rangle = \delta_{ij}$ and $||\,|x_i\rangle\,|| = 1$.

Any state $|\psi\rangle$ can be decomposed in any orthonormal basis:

$$|\psi\rangle = \sum_{i=1}^{d} c_i\,|x_i\rangle\,, \tag{6}$$

where $c_i \in \mathbf{C}$ are complex coefficients given by: $c_i = \langle x_i|\psi\rangle$. These coefficients are uniquely defined by the basis $\{|x_i\rangle\}_{i=1}^{d}$ i.e.: the basis is complete. Let us check the completeness of the orthonormal basis in $\mathcal{H}^d$:

$$|\psi\rangle = \sum_{i=1}^{d} c_i\,|x_i\rangle = \sum_{i=1}^{d} \langle x_i|\psi\rangle\,|x_i\rangle = \sum_{i=1}^{d} \left\langle x_i \middle| \sum_{j=1}^{d} d_j x_j \right\rangle |x_i\rangle$$

$$= \sum_{i=1}^{d}\sum_{j=1}^{d} d_j\,\langle x_i|x_j\rangle\,|x_i\rangle = \sum_{j=1}^{\infty} d_j\delta_{ji}\,|x_i\rangle = \sum_{i=1}^{d} d_i\,|x_i\rangle\,.$$

Thus an orthonormal basis $\{|x_i\rangle\}_{i=1}^{d}$ is complete and an arbitrary quantum $|\psi\rangle$ has a unique representation in $\{|x_i\rangle\}_{i=1}^{d}$ in $\mathcal{H}^d$.

2.4 Qubit

From now we concentrate on 2-dimensional Hilbert space $\mathcal{H}^2$. This a handy tool that allows us to build models with two-level systems e.g. two-level atoms, polarised photons, ions traps, spin $\frac{1}{2}$ particles etc.

In this space we define a qubit:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{7}$$

where $\{|0\rangle\,, |1\rangle\}$ is an orthonormal basis called computational (or standard) basis and α and $\beta \in \mathbf{C}$ are coefficient such that satisfy the normalization condition of ψ i.e. $|\alpha|^2+|\beta|^2 = 1$. The physical meaning of computational basis is determined by the situation that we want to describe: it can be either the basis of spin up and spin down $|0\rangle := |\uparrow\rangle$ and $|1\rangle := |\downarrow\rangle$ for ion trap models, or polarisation basis e.g. $|0\rangle := |H\rangle$ and $|1\rangle := |V\rangle$ for photons.

2.5 Quantum observables

An observable is a property of a state that can be (at least in theory) observed. Examples of observables are position and momentum. In quantum theory an observable is represented with an operator denoted e.g. by $\hat{A}$ that is a linear map such that:

$$\mathcal{H} \ni |\psi\rangle \to \hat{A}\,|\psi\rangle = |\psi'\rangle \in \mathcal{H}.$$

We shall assume that observables are square matrices so they have their eigenvectors $|v\rangle$ and eiegenvalues λ:

$$\hat{A}\,|v\rangle = \lambda\,|v\rangle\,.$$

Apart from that we need another reasonable assumption. In quantum theory, observables are represented with normal operators i.e. $\hat{A}\hat{A}^\dagger = \hat{A}^\dagger\hat{A}$, where $\dagger$ denotes Hermitian conjugate. For normal operators the set of eigenvectors is complete - what has a very precise physical meaning. It ensures that sure that the experiment (represented with $\hat{A}$) can be modelled consistently;

The operators that we will be dealing with have some inner structure and are constructed out of "smaller" objects.

In the further sections we discuss examples the decomposition of linear operators useful in quantum information theory in order to understand its inner structure and physical meaning.

Having observable defined we can calculate its expectation value denoted by $\langle . \rangle$ for an arbitrary quantum state $|\psi\rangle$

$$\left\langle \hat{A} \right\rangle_{\psi} = \langle\psi|\hat{A}|\psi\rangle = \mathrm{Tr}\Big[\hat{A}\,|\psi\rangle\langle\psi|\Big],$$

where $|\psi\rangle\langle\psi|$ is a matrix representation of $|\psi\rangle$ and Tr[.] denotes trace. We will discuss the trace operation in further sections.

2.6 Mathematical digression: trace and its properties

2.7 Hermitian observables

The most intuitive observables in quantum theory are considered to be hermitian i.e. $\hat{A}$ is such that $\hat{A} = \hat{A}^\dagger$. The hermitianity of $\hat{A}$ ensures that eingenvalues $\lambda \in \mathbf{R}$. Even more, the hermitianity ensures that the expectation value $\hat{A}$ for a given quantum state $|\psi\rangle$ is also a real number

$$\left\langle \hat{A} \right\rangle_\psi = \langle\psi|\hat{A}|\psi\rangle = r \in \mathbf{R}.$$

Thus hermitian operator $\hat{A}$ is an intuitive mathematical tool to describe an observable that is supposed to represent a measurable, physical quantity. All experimental equipment have scales in real numbers!

2.8 Special case of hermitian observable: Projector

Here we discuss the special observables that are projectors i.e.

$$\hat{P} = \hat{P}^\dagger = \hat{P}\hat{P}^\dagger = \hat{P}^2$$

Note that every quantum state given by $|\psi\rangle$ has its projector . It is easy to check that $|\psi\rangle\langle\psi|$ is in fact a projector

$$|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| \left(|\psi\rangle\langle\psi|\right)^\dagger = |\psi\rangle\langle\psi| \, |\psi\rangle\langle\psi| \quad \text{because} \quad \langle\psi|\psi\rangle = 1.$$

This fact has the following consequence

$$\forall \, |\psi\rangle \in \mathcal{H} \; \exists \; \hat{P}_\psi = |\psi\rangle\langle\psi| \;\; : \;\; \hat{P}_\psi \, |\psi\rangle = |\psi\rangle$$

Thus, every $|\psi\rangle$ from $\mathcal{H}$ there exist at last in its theoretical description such a projector $\hat{P}_\psi$ that acting on $|\psi\rangle$ gives a certain result with probability equal to unity. i.e $\langle\hat{P}_\psi\rangle_\psi = \langle\psi|\hat{P}_\psi|\psi\rangle = 1$:

2.9 Spectral theorem

As mentioned before linear operators have their inner structure. Spectral theorem determines the structure of a normal operators. Here we present the version of spectral theorem for finite dimensional Hilbert spaces. Let $dim\mathcal{H}$ be the dimension of Hilbert space. Let n be the number of eigenvalues of considered operator $\hat{A}$ i.e. $\{\lambda_i\}_{i=1}^n$ and subscripts $i = 1, 2, ...n \leq dim\mathcal{H}$. Operator $\hat{A}$ has the following spectral representation:

$$\hat{A} = \sum_i^n \lambda_i \hat{P}_{\lambda_i}, \tag{8}$$

where $\hat{P}_{\lambda_i}$ are projectors on the particular subspaces $\mathcal{H}_{\lambda_i}$ the form $\mathcal{H}$ and they are uniquely related with λ_i. The set of eigenvalues $\{\lambda_i\}_{i=1}^n$ is called the spectrum of $\hat{A}$.

2.10 Postulates of quantum mechanics

Quantum mechanics, also known as quantum physics or quantum theory, is a fundamental theory in physics that describes the behavior of matter and energy at the smallest scales. It is formulated based on a set of postulates or principles that lay the foundation for understanding quantum systems. These postulates are the fundamental rules or axioms of quantum mechanics. Here are the key postulates of quantum mechanics:

1. State Space: Quantum systems are described by state vectors, also known as wave functions, denoted by the symbol $|\psi\rangle$. These state vectors exist in a complex vector space known as a Hilbert space, typically denoted as $\mathcal{H}$.

2. Superposition Principle: The superposition principle states that a quantum system can exist in a linear combination of multiple states, and each state contributes with a certain probability amplitude. Mathematically, if $|\psi_1\rangle$ and $|\psi_2\rangle$ are valid states, then $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$ is also a valid state, where α and β are complex numbers.

3. Quantization of Observables: Physical observables in quantum mechanics, such as position, momentum, energy, and angular momentum, are represented by operators. These operators act on the state vectors, and their eigenvalues correspond to possible measurement outcomes.

4. Measurement Postulate: When a quantum system is measured, the measurement process "collapses" the state vector to one of its eigenstates, with probabilities determined by the squared magnitudes of the probability amplitudes associated with the eigenstates.

5. Time Evolution: The time evolution of a quantum system is described by the Schrödinger equation, which governs how the state vector $|\psi\rangle$ changes over time. The Schrödinger equation is typically written as

$$\hat{H}|\psi\rangle = i\hbar \frac{\mathrm{d}\,|\psi\rangle}{\mathrm{d}\,t}, \tag{9}$$

   where $\hat{H}$ is the Hamiltonian operator, and $\hbar$ (h-bar) is the reduced Planck constant.

6. Quantum Entanglement: Quantum entanglement is a fundamental property where the quantum states of two or more particles become correlated in such a way that the measurement of one particle instantaneously determines the state of the others, even if they are physically separated.

7. Postulate of Quantum Measurement (Alternative to 4): This postulate specifies that measurement operators corresponding to observables are Hermitian (self-adjoint) operators. Upon measurement, the system's state collapses to one of the eigenstates of the measurement operator.

8. Projection Postulate: After measurement, if a system is found to be in an eigenstate $|\Phi\rangle$ of an observable, the post-measurement state is the projection of the original state onto $|\Phi\rangle$.

3 Framework of quantum mechanics and quantum information

3.1 Pure and mixed states

In quantum mechanics, states of a quantum system are categorized into two main types: pure states and mixed states. These two types of states represent different levels of knowledge and information about the system.

Definition 1. *(Pure States) A pure quantum state is a state for which you have complete and definite information. Mathematically, a pure state is represented by a ket vector $|\psi\rangle$ in a Hilbert space.*

Pure states are described by a single ket vector $|\psi\rangle$, and all measurements performed on the system will yield the same outcome, given by the eigenvalues of the corresponding observables. The probability distribution for measurement outcomes is deterministic for pure states, meaning that the outcome of a measurement is known with certainty. Pure states are often used to describe idealized or well-prepared quantum systems.

Definition 2. *(Mixed States) A mixed quantum state is a statistical ensemble or a probabilistic combination of pure states. It represents a situation where you don't have complete knowledge of the system, and you need to describe it statistically.*

Mixed states are described by a density operator (also called a density matrix) ρ, which is a Hermitian, positive-semidefinite matrix that represents the statistical mixture of pure states. Measurements performed on a system in a mixed state yield probabilistic outcomes. The probabilities of obtaining specific measurement results are given by the trace of the product of the density operator and the corresponding observable operator. Mixed states are used to describe situations where you have incomplete information about the system, such as when the system is in a statistical ensemble of different pure states with associated probabilities. The mathematical tool that allows us to represent mixed states is a density matrix given by

$$\rho = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i| \,, \tag{10}$$

where $|\psi_i\rangle\langle\psi_i|$ are (pure states) projectors and the coefficients p_i denote the probabilities that given $|\psi_i\rangle\langle\psi_i|$ appears in the mixture ρ. The probabilistic interpretation of quantum state imposes the normalisation condition so $\sum_{i=1}^{n} p_i = 1$. In reference to the definition of a mixed state (10) we can say that pure state

$|\psi\rangle$ is such a state that cannot be decomposable as a convex combination of projectors i.e. $|\psi\rangle \neq \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|$. Still, $|\psi\rangle$ can be a superposition of other pure states i.e $|\psi\rangle = \sum_{i=1}^{n} \sqrt{p_i} |\psi\rangle$ and then $\sum_{i=1}^{n} \sqrt{p_i} = 1$.

The distinction between pure and mixed states in quantum mechanics is based on the level of information and certainty you have about a quantum system. Pure states represent situations where you have complete knowledge and deterministic outcomes, while mixed states represent situations where you have incomplete knowledge and probabilistic outcomes due to a statistical mixture of pure states. Mixed states are often encountered in real-world quantum systems, especially when dealing with systems that are not perfectly isolated or prepared.

Such a description of a physical object is very idealised, because we assume that we have e.g. isolated ideally prepared atom or photon. We call $|\psi\rangle$ a pure state. However, in more realistic physical situations we deal not with perfect copies of one isolated atoms (pure states) but with the ensemble of atoms or photons that correspond to the statistical mixture of not necessarily perfect copies of the state $|\psi\rangle$ and even some additional occasionally measuremd states (e.g. the environment, because the state is not perfectly isolated). Then noise and losses shall be take under consideration. Such a ensemble is called mixed state and it is given with the convex combination (not superposition!!!) of pure states (that can be in superposition).

Here already arises the great difference between the superposition (pure state) and mixed states (convex combination of pure states). Firstly, let us distinguish here the two different levels of lack of the knowledge regarding the quantum state. Consider a (pure) qubit: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Before taking a measurement our lack of the knowledge whether $|\psi\rangle$ is in $|\psi_1\rangle$ or $|\psi_2\rangle$ is fundamental i.e. we do not have information whether $|\psi\rangle$ is in $|0\rangle$ or $|1\rangle$. This is the most intrinsic level of "not-knowing" about the state. But that is also another "statistical lack of knowledge" of quantum ensemble, that less fundamental that lack of knowing resulting from superposition. But on the less fundamental level we still have another lack of knowledge that refers to the probabilistic character of the mixture ρ. These two kinds of lack of knowledge occur independently to each other.

Moreover, the density matrix formalism comes in handy for the description of interactions between the state and environment (bath) including noise and losses - we will study theses cases in the following sections.

3.1.1 Properties of density matrix

The density matrix ρ can be used for the description of pure and mixed states. It enable more general description of the state than the vector $|\psi\rangle$ that can be used only for pure states. Still, ρ and $|\psi\rangle$ share the following properties:

- $\rho \geq 0$,
- $\rho = \rho^{\dagger}$,
- $\mathrm{Tr}\,\rho = 1$.

Also, the spectral decomposition (8) can be applied for ρ :

$$\rho = \sum_{i=1}^{n} \lambda_i \left| x_i \right\rangle \left\langle x_i \right|, \tag{11}$$

where $sum_{i=1}^{n} \lambda_i = 1$ because $\operatorname{Tr} \rho = 1$ and $\lambda_i \geq 0$because $\rho \geq 0$. The set of vectors $\{|x_i\rangle\}_{i=1}^{n}$ is orthonormal.

Note that every pure state $|\psi\rangle$ in the matrix representation is a projector itself $|\psi\rangle\langle\psi|$, but a mixed state ρ is not. We use this observation to distinguish pure from mixed states by calculating $\operatorname{Tr} \rho^2$. For every pure states we have $\operatorname{Tr}(|\psi\rangle\langle\psi|)^2$ as $|\psi\rangle\langle\psi|$ is a projector while for a mixed state $\operatorname{Tr} \rho^2 < 1$.

3.1.2 Bloch sphere representation

Let us introduce Pauli operators:

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

They are 2×2 Hermitian operators $\det \sigma_i = -1$ and $\operatorname{Tr} \sigma_i$ for $i = 1, 2, 3$.

Pauli operators σ_i together with the unity matrix denoted as $\sigma_0 = \mathbf{1}$ span a subspace for all 2×2 Hermitian operators. Every 2×2 self-adjoint operator $(\hat{A})$ can be decomposed as follows:

$$\hat{A} = \sum_{i=0}^{4} c_i \sigma_i, \tag{12}$$

where $c_i \in \mathbf{C}$.

Let us introduce $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$. Formula (12) can be put as:

$$\hat{A} = c_0 \sigma_0 + \vec{n}\vec{\sigma}, \tag{13}$$

where $\vec{n}$ is a 3-dimensional unit vector. Obviously the same representation applies to the 2×2 density matrix:

3.2 The description of composed system

Till now we were considering a system descring one physical object e.g.: a spinless particle, or a photon. Nevertheless, it is time to stress that the correlations and interactions between systems are of great importance for quantum mechanics, quantum information theories and its applications. In order to merge two systems together we introduce a tensor product and denote it as $\otimes$. Let A and B be two (sub)systems, the complex system $(A + B)$ is geven by:

$$(A + B) = A \otimes B. \tag{14}$$

3.3 Partial trace

The partial trace is a mathematical operation commonly used in quantum mechanics to extract information about a subsystem of a composite quantum system. When you have a composite quantum system consisting of multiple subsystems, the partial trace allows you to describe the state of one subsystem while ignoring the other subsystems. This operation is particularly useful in quantum information theory, quantum entanglement, and studying the reduced density matrix of a subsystem.

The partial trace is defined as follows:

Given a composite quantum system with a joint or global density operator ρ that describes the entire system, and each subsystem is associated with a Hilbert space $\mathcal{H}_i$, the partial trace over a particular subsystem (let's say subsystem i) is denoted as Tr_i and is defined as follows:

$$\mathrm{Tr}_i(\rho) = \sum_j \langle .j|\rho|i\rangle. \tag{15}$$

Here, $|i\rangle$ and $\jmath\rangle$ are basis states of the Hilbert space $\mathcal{H}_i$ for subsystem i. The partial trace operation involves taking the inner product of the basis states $|i\rangle$ and $\jmath\rangle$ and summing over all possible values of j.

The result of the partial trace is a density operator that describes the reduced state of the subsystem i, effectively "tracing out" the degrees of freedom associated with the other subsystems. This reduced density operator is often denoted as ρ_i and represents the state of subsystem i when the entire system is in state ρ.

Mathematically, the reduced density operator for subsystem i is given by:

$$\rho_i = \mathrm{Tr}_i(\rho). \tag{16}$$

Properties and Applications of the Partial Trace:

Reduced Density Matrix: The partial trace operation allows you to find the reduced density matrix of a subsystem, which can be used to calculate observables and properties of that subsystem independently of the rest of the system.

Entanglement: It is crucial for studying entanglement in composite systems. The reduced density matrix can help determine whether subsystems are entangled or separable.

Mixed States: When dealing with mixed states (statistical ensembles), the partial trace is used to find the reduced density matrix for each subsystem.

Quantum Channels: In the context of quantum channels, the partial trace is used to describe the evolution of a subsystem when only partial information is available.

Quantum Information: The partial trace is a fundamental tool in quantum information theory for analyzing quantum states, quantum operations, and quantum channels in multipartite systems.

In summary, the partial trace is a mathematical operation that plays a crucial role in quantum mechanics and quantum information theory, allowing physicists

and researchers to focus on specific subsystems within a composite quantum system.

3.4 Purification

Purification is a concept in quantum mechanics used to represent a composite quantum system in a way that emphasizes its entanglement structure and allows for a more complete description of the system. The purification process involves introducing an auxiliary quantum system (usually called a "purifying system" or "ancilla") in such a way that, when combined with the system of interest, it results in a pure quantum state. This is particularly useful for understanding entanglement properties, performing quantum operations, or studying the environment's effects on a quantum system.

Here's a mathematical description of the purification process. Let's start with a mixed state represented by a density operator ρ, which acts on a finite-dimensional Hilbert space $\mathcal{H}$. The density operator ρ is Hermitian (self-adjoint) and positive semidefinite, and it describes a quantum system in a mixed state. Mathematically, it can be expressed as:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{17}$$

where $|\psi_i\rangle$ represents pure states of the system, p_i are the corresponding probabilities, and $\sum_i p_i = 1$ to ensure trace normalization. Now, to perform purification, you introduce an auxiliary system, often referred to as an ancillary system or purifying system. This auxiliary system resides in a Hilbert space $\mathcal{H}'$ such that the composite system $\mathcal{H} \oplus \mathcal{H}'$ is in a pure state. The composite pure state is represented as:

$$|\Psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle \otimes |\phi_i\rangle, \tag{18}$$

where $|\phi_i\rangle$ are orthonormal states in $\mathcal{H}'$. The crucial idea here is that $|\Psi$ is a pure state, and it contains the information about ρ. The original mixed state ρ can be obtained by taking the partial trace over the ancillary system $\mathcal{H}'$:

$$\rho = \mathrm{Tr}_{\mathcal{H}'}(|\Psi\rangle\langle\Psi|) = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{19}$$

In this expression, $\mathrm{Tr}_{\mathcal{H}'}$ represents the partial trace operation over the ancillary system $\mathcal{H}'$.

The purification process involves introducing an ancillary system and creating a composite pure state $|\Psi\rangle$ that contains the same information as the original mixed state ρ. The purification allows for a more complete and elegant description of the quantum system, and it is particularly useful for understanding entanglement properties and performing various quantum operations.

In summary, purification is a powerful concept in quantum information theory and quantum mechanics because it allows for a more elegant and unified treatment of quantum systems. It simplifies the description of entanglement,

quantum operations, and various quantum protocols. Additionally, it provides a theoretical framework for understanding quantum correlations and the nature of quantum entanglement.

3.5 Fidelity between quantum sates

Quantum fidelity, often denoted as $F(\rho, \sigma)$, is a mathematical measure of the similarity or closeness between two quantum states, ρ and σ. It quantifies how "close" or "similar" the two quantum states are in terms of their quantum properties. High fidelity indicates a high degree of similarity, while low fidelity indicates dissimilarity between the states.

The quantum fidelity $F(\rho, \sigma)$ between two quantum states, ρ and σ, is defined as follows:

$$F(\rho, \sigma) = \mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]^2, \tag{20}$$

where Tr denotes the trace (the sum of the diagonal elements) of the matrix. $\sqrt{\rho}$ denotes the square root of a state ρ. The square roots in this expression are well-defined because ρ and $\sqrt{\rho}\sigma\sqrt{\rho}$ are for positive semidefinite matrices, and the square root of a positive semidefinite matrix is defined via the spectral theorem. Properties and Interpretation of Quantum Fidelity:

1. **Range:** Quantum fidelity values range from 0 to 1, with 0 indicating complete dissimilarity (orthogonal states) and 1 indicating perfect similarity (identical states).

2. **Maximal Fidelity:** The fidelity is maximized when ρ and σ are identical states, resulting in $F(\rho, \sigma) = 1$.

3. **Minimizing Fidelity:** Fidelity is minimized when ρ and σ are orthogonal states, resulting in $F(\rho, \sigma) = 0$.

4. **Triangle Inequality:** Fidelity satisfies the triangle inequality, meaning that for any three quantum states ρ, σ, and τ, $F(\rho, \tau) \leq F(\rho, \sigma) + F(\sigma, \tau)$.

5. **Physical Interpretation:** Fidelity can be thought of as a measure of the overlap or similarity between the wavefunctions of the two quantum states. In quantum information theory, it is often used to quantify the quality of quantum operations, quantum channels, or quantum measurements.

6. **Quantum Information Applications:** Quantum fidelity plays a critical role in quantum information theory, quantum error correction, quantum state discrimination, and quantum communication protocols. For example, it is used to measure how well a quantum channel preserves quantum states or to quantify the performance of quantum gates in quantum computing.

In summary, quantum fidelity is a mathematical tool for quantifying the similarity or closeness between two quantum states. It is an essential concept in

quantum information theory and quantum technologies, providing a way to assess the quality of quantum processes and operations.

3.6 Quantum entanglement and entanglement criteria

3.6.1 Entanglement of pure states

Entanglement is a fundamental and intriguing feature of quantum mechanics that arises when two or more quantum systems are described by a composite pure state that cannot be factorized into individual states for each subsystem. In other words, entanglement is a phenomenon where the properties of one quantum system become correlated with the properties of another, even when the systems are spatially separated. Here's an explanation of entanglement in the context of a pure state:

1. **Composite Pure State:**

   Consider a composite quantum system composed of two or more subsystems. Mathematically, this can be represented as $|\psi\rangle$, where $|\psi\rangle$ is a pure state in a joint Hilbert space H that describes the entire system.

2. **Factorization:**

   If the pure state $|\psi\rangle$ can be expressed as a simple tensor product of individual states, $|\psi\rangle = |A\rangle \otimes |B\rangle$, then the system is not entangled, and it can be described independently as the product of the states for each subsystem. Such states are called separable states.

3. **Entangled States:**

   If, however, $|\psi\rangle$ cannot be expressed as a simple tensor product of individual states, $|\psi\rangle \neq |A\rangle \otimes |B\rangle$, then the system is entangled. In this case, the properties of one subsystem cannot be described independently of the other subsystem(s). Entangled states exhibit non-classical correlations that go beyond classical physics. Entanglement is characterized by the presence of quantum correlations between the subsystems. When measurements are performed on one subsystem, the outcomes are correlated with the measurements on the other subsystem(s) in a way that cannot be explained by classical physics. These correlations can be stronger than any correlations achievable classically.

4. **Bell States:**

   A famous example of an entangled state is the Bell state, which is maximally entangled. One of the Bell states is:

   $$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{21}$$

   If you measure one qubit of an entangled Bell state and find it in the $|0\rangle$ state, you instantly know that the other qubit is in the $|0\rangle$ state as well, no matter how far apart the two qubits are.

Entanglement is a resource in quantum information processing and quantum computing and is crucial for many quantum protocols, such as quantum teleportation, quantum cryptography, and quantum entanglement swapping. Understanding and harnessing entanglement is a key element of the power of quantum mechanics in processing information and performing quantum operations that have no classical analogs.

3.6.2 Entanglement of mixed states

Entanglement is not limited to pure states in quantum mechanics; it can also exist in mixed states. Mixed states represent situations where a quantum system is in a statistical mixture of pure states. In the context of mixed states, entanglement describes the presence of quantum correlations between subsystems that cannot be explained classically. Here's how entanglement works in mixed states.

As we said earlier a mixed state ρ is represented by a density operator rather than a pure state ket vector. Mathematically, it can be expressed as a convex combination of pure states: $\rho = \sum_{i=1}^{n} p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|$, where $\left|\psi_i\right\rangle\!\left\langle\psi_i\right|$ are pure states (possibly entangled), and p_i are probabilities such that $\sum_i p_i = 1$. Entanglement can still exist in mixed states when the density operator ρ cannot be expressed as a convex combination of product states. In other words, if there is no way to write ρ as $\rho = \sum_i p_i \rho_i \otimes \sigma_i$, where ρ_i and σ_i are density operators for the individual subsystems, then the mixed state ρ is entangled.

Measuring the degree of entanglement in a mixed state is more challenging than in pure states. Various measures and entanglement criteria have been developed to quantify entanglement in mixed states, such as entanglement entropy, concurrence, and negativity.

Entanglement in mixed states is a valuable resource for quantum technologies and quantum information processing, similar to pure state entanglement. Mixed states often arise in realistic scenarios, such as due to decoherence and interactions with the environment. Understanding and characterizing entanglement in mixed states is crucial for the design and analysis of quantum protocols, quantum error correction, and quantum communication in real-world applications. It's important to note that the study of entanglement in mixed states is more complex than in pure states because mixed states can exhibit a broader range of behaviors, including classical correlations and noise. Detecting and quantifying entanglement in mixed states is an active area of research in quantum information theory. Various tools and techniques have been developed to address this complexity and exploit entanglement for practical quantum technologies.

3.7 Quantum channel

The quantum channel formalism is a mathematical framework used in quantum mechanics and quantum information theory to describe the evolution of quantum states and operations on quantum systems. Quantum channels are used to model various physical processes, such as quantum measurements, quantum

communication, and the effects of noise and decoherence on quantum systems. They provide a way to mathematically represent how a quantum state transforms under the influence of these processes.

Quantum channels are often described using superoperators, which are linear maps Φ that act on density operators (also called density matrices). A density operator represents the quantum state of a system. A density operator ρ is a Hermitian, positive-semidefinite matrix that describes a quantum state. It can be written as $\rho = |\psi\rangle\langle\psi|$ for pure states and as a convex combination of pure states for mixed states. Quantum channels represent quantum operations or transformations that take an input quantum state ρ and produce an output quantum state $\rho' = \Phi(\rho)$. Mathematically, a quantum channel Φ can be represented as a superoperator that acts on the density operator ρ as $\Phi(\rho)$. Quantum channels are required to be trace-preserving (TP), which means that they preserve the trace (the sum of the diagonal elements) of the density operator. This ensures that probabilities are conserved. Quantum channels should also be completely positive (CP), which is a condition that ensures the positivity of the density operator remains intact.

We have many ways of describing quantum channels. For example, quantum channels can be expressed in terms of Kraus operators. A quantum channel Φ can be written in the Kraus representation as follows:

$$\Phi(\rho) = \sum_i K_i \rho K_i^\dagger, \tag{22}$$

where K_i are the Kraus operators satysfying relation $\sum_i K_i^\dagger K_i = \mathbf{1}$, and $\dagger$ denotes the conjugate transpose.

Different approach for describing quantum channels is the Stinespring dilation theorem. It is a mathematical theorem that provides a way to represent certain types of quantum operations as unitary operations on a larger Hilbert space, including the introduction of an auxiliary system. This theorem is particularly relevant in the study of quantum channels and quantum operations.

The Stinespring dilation theorem can be formally stated as follows:

Theorem 1. *(Stinespring Dilation) Given a completely positive trace-preserving (CPTP) linear map Φ, which represents a quantum channel, there exists a larger Hilbert space $\mathcal{H}_E$ and a unitary operator U on $\mathcal{H} \oplus \mathcal{H}_E$ such that, for any input state ρ on $\mathcal{H}$, the action of Φ on ρ can be represented as:*

$$\Phi(\rho) = \mathrm{Tr}_E \left[U(\rho \oplus |0\rangle_E\langle 0|) U^\dagger \right], \tag{23}$$

where $\Phi(\rho)$ is the output state after the application of the quantum channel. $\mathcal{H}$ is the original Hilbert space. $\mathcal{H}_E$is an auxiliary Hilbert space. U is a unitary operator on the combined Hilbert space $\mathcal{H} \oplus \mathcal{H}_E$. $|0\rangle_E$ is the initial state of the auxiliary system $\mathcal{H}_E$. Tr_E represents the partial trace over the auxiliary system $\mathcal{H}_E$.

In other words, the Stinespring dilation theorem tells us that any quantum channel Φ can be represented as the action of a unitary operator on a larger composite system that includes both the original quantum system and an auxiliary

system (usually referred to as an "ancilla" or "environment"). The unitary operator U allows the quantum channel to be realized as a unitary transformation on this composite system.

The Stinespring dilation theorem is a fundamental tool in the study of quantum channels and quantum operations, and it has applications in quantum information theory, quantum error correction, and quantum communication. It provides a way to understand and analyze the behavior of quantum channels in a broader context and is a key result in the mathematical framework of quantum mechanics.

Examples of Quantum Channels:

1. **Unitary Evolution:** A unitary quantum channel represents a reversible transformation and is described by a unitary operator U. It can be written as $\Phi(\rho) = U\rho U^\dagger$.

2. **Depolarizing Channel:** This channel models the effect of noise and randomizing quantum states. It acts on a quantum state by the following way:
$$\Phi_p(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z). \tag{24}$$
Alternatively, $\Phi_p(\rho)$ replaces p replaces the input with the completely mixed state $\mathbf{1}/2$ with probability $q = 4p/3$:
$$\Phi_p(\rho) = (1-q)\rho + q\frac{\mathbf{1}}{2}. \tag{25}$$

3. **Quantum Measurement:** A quantum measurement can be described as a quantum channel that maps the input state to a set of possible outcomes with associated probabilities.

Quantum channels can be experimentally characterized through quantum process tomography, which involves applying known input states to the channel and measuring the corresponding output states to reconstruct the action of the channel.

Quantum channels play a crucial role in quantum information processing tasks, such as quantum teleportation, quantum error correction, and quantum key distribution. In summary, the quantum channel formalism provides a powerful framework for describing and analyzing the evolution of quantum states under various physical processes and operations. It is a fundamental tool in quantum information theory and quantum technologies.

4 Quantum Teleportation

Quantum teleportation is a remarkable quantum information protocol that allows the transfer of the quantum state of one system (usually a qubit) to another, distant system, while destroying the original state in the process. This

transfer occurs without the physical transfer of particles, making it fundamentally different from classical information transfer. Quantum teleportation is a crucial component of many quantum communication and quantum computing protocols.

Prerequisites:

1. Alice (the sender) has a quantum state $|\psi\rangle$ that she wants to teleport to Bob (the receiver).
2. Alice and Bob share an entangled pair of qubits, typically prepared in one of the Bell states:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}, \tag{26}$$

$$|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}, \tag{27}$$

$$|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}, \tag{28}$$

$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}. \tag{29}$$

Quantum Teleportation Steps:

1. **Entanglement Measurement:**
   - Alice performs a Bell measurement on her quantum state $\Psi\rangle$ and her part of the entangled pair (let's call it qubit A). The Bell measurement consists of applying a set of quantum operations.
   - The result of the Bell measurement is two classical bits, which we'll denote as a and b.
2. **Classical Communication:** Alice sends the two classical bits (a and b) to Bob through a classical communication channel.
3. **Conditional Operations:**
   - Based on the values of the received classical bits (a and b), Bob performs one of four possible quantum operations on his part of the entangled pair (let's call it qubit B):
     - If $(a, b) = (0, 0)$, Bob applies the identity operation (do nothing).
     - If $(a, b) = (0, 1)$, Bob applies the X gate (bit-flip).
     - If $(a, b) = (1, 0)$, Bob applies the Z gate (phase-flip).
     - If $(a, b) = (1, 1)$, Bob applies both the X and Z gates.
   - This operation effectively transforms Bob's qubit B into the state $|\Psi\rangle$, which was originally held by Alice.

Quantum teleportation depends on the prior existence of an entangled pair of particles. It is a probabilistic process; successful teleportation relies on the outcome of the Bell measurement. Quantum teleportation is a fundamental building block for quantum communication and quantum computing, as it allows for the transmission of quantum information over long distances, overcoming some of the limitations of classical communication.

5 Quantum superdense coding

Quantum superdense coding is a quantum communication protocol that allows two parties, traditionally referred to as Alice and Bob, to send two classical bits of information using only one qubit and a pre-shared entangled pair of qubits. It's a fascinating example of how quantum entanglement can be used to enhance communication efficiency. Here's a step-by-step explanation of quantum superdense coding.

1. **Preparation of an Entangled Pair:**

   Alice and Bob share an entangled pair of qubits. This entangled pair can be created using a process such as generating entangled photons. The entangled pair is typically in one of the four Bell states:

$$\begin{aligned} |\Phi^+\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\ |\Phi^-\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} \\ |\Psi^+\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} \\ |\Psi^-\rangle &= (|01\rangle - |10\rangle)/\sqrt{2} \end{aligned} \tag{30}$$

2. **Encoding Alice's Message:**

   Alice wants to send a two-bit classical message to Bob. Let's say she wants to send the message "10." To encode her message, Alice performs one of four possible operations (Pauli operators) on her qubit based on her message:

   - If she wants to send "00," she does nothing (identity operator).
   - If she wants to send "01," she applies the X gate (bit-flip).
   - If she wants to send "10," she applies the Z gate (phase-flip).
   - If she wants to send "11," she applies both X and Z gates (bit-flip followed by phase-flip). This operation transforms Alice's qubit into one of the four Bell states, depending on her message.

3. **Transmission:** Alice sends her qubit to Bob, who now holds both Alice's qubit and his own entangled qubit.

4. **Decoding by Bob:** To decode Alice's message, Bob performs a Bell measurement on the two qubits he holds. This measurement distinguishes between the four possible Bell states. The outcome of the Bell measurement directly reveals Alice's message:

   - If the measurement result is $|\Phi^+\rangle$, Bob knows that Alice's message was "00."
   - If the measurement result is $|\Phi^-$, Bob knows that Alice's message was "01."

- If the measurement result is $|\Psi^+\rangle$, Bob knows that Alice's message was "10."
- If the measurement result is $|\Psi^-\rangle$, Bob knows that Alice's message was "11."

And that's it! Using just one qubit and an entangled pair of qubits, Alice is able to convey two classical bits of information to Bob, thanks to the principles of quantum entanglement and quantum superposition. This protocol demonstrates the advantage of quantum communication over classical communication for certain tasks.

6 No-cloning theorem

The no-cloning theorem is a fundamental result in quantum mechanics that states it is impossible to create an exact copy of an arbitrary unknown quantum state. This theorem is a consequence of the principles of quantum superposition and the linearity of quantum mechanics. The theorem has important implications for quantum information theory and quantum computing.

The no-cloning theorem can be formally stated as follows:

Theorem 2. *(No-Cloning Theorem) Given an arbitrary unknown quantum state $|\psi\rangle$, it is impossible to create a quantum process or device that can produce an independent, identical copy of $|\psi\rangle$, resulting in two identical quantum states, $|\psi\rangle$ and $|\psi\rangle$, unless $|\psi\rangle$ is a member of a specific set of orthogonal states, such as the computational basis states in a qubit system.*

Proof. The proof follows from linearity of quantum mechanics and it can be divided in six steps:

1. **Assume Cloning is Possible:** Let's start by assuming that it is possible to clone an arbitrary unknown quantum state $|\psi\rangle$, meaning we can create two identical copies of $|\psi\rangle$, resulting in states $|\psi\rangle$ and $|\phi\rangle$, where $|\psi\rangle = |\phi\rangle$.

2. **Use Linearity of Quantum Mechanics:** Since quantum mechanics is a linear theory, the cloned state can be represented as a linear combination of $|\psi\rangle$ and $|\phi\rangle$: $|\phi\rangle = \alpha|\psi\rangle + \beta|\psi\rangle$ where α and β are complex coefficients.

3. **Normalization Condition:** For the cloned state $|\phi\rangle$ to be normalized (i.e., to have a probability amplitude sum of 1), we must have $|\alpha|^2 + |\beta|^2 = 1$.

4. **Measurement of the Cloned State:** Now, let's consider the measurement of the cloned state $|\phi\rangle$ in the computational basis, which consists of the states $|0\rangle$ and $|1\rangle$:

   - If $|\phi\rangle = |0\rangle$, the measurement outcome is $|0\rangle$ with probability $|\alpha|^2$.
   - If $|\phi\rangle = |1\rangle$, the measurement outcome is $|1\rangle$ with probability $|\beta|^2$.

5. **Measurement of the Original State:** At the same time, let's consider measuring the original state $|\psi\rangle$ in the computational basis:
   - If $|\psi\rangle = |0\rangle$, the measurement outcome is $|0\rangle$ with probability 1 (certainty).
   - If $|\psi\rangle = |1\rangle$, the measurement outcome is $|1\rangle$ with probability 1 (certainty).
6. **Contradiction:** Now, here's where the contradiction arises. If we clone the original state $|\psi\rangle$ to obtain $|\psi\rangle$ and then measure $|\phi\rangle$, the probabilities of the measurement outcomes must match the probabilities of measuring the original state $|\psi\rangle$. However, we have:
   - For the cloned state $|\psi\rangle$, the measurement outcome probabilities depend on α and β.
   - For the original state $|\psi\rangle$, the measurement outcome probabilities are always 1 with certainty.

   Since these probabilities cannot match, we have reached a contradiction. Therefore, the assumption that cloning is possible is invalid.

The contradiction demonstrates that it is impossible to create an exact duplicate of an arbitrary unknown quantum state. This is the essence of the no-cloning theorem. □

In other words, if you have a quantum state $|\psi\rangle$ that represents some information, you cannot create a perfect copy of that state, except in special cases. Attempting to clone an arbitrary quantum state will result in an inevitable loss of information.

This no-cloning theorem has several important implications:

1. **Quantum Security:** Quantum cryptography protocols, such as quantum key distribution (e.g., BB84 or QKD), rely on the no-cloning theorem to ensure the security of information transmission. The inability to clone quantum states makes eavesdropping much more challenging.
2. **Quantum Computing:** Quantum computers are designed to manipulate quantum information in ways that classical computers cannot. The no-cloning theorem imposes constraints on quantum algorithms, as they cannot simply copy arbitrary quantum states as classical algorithms copy classical bits.
3. **Quantum Error Correction:** Quantum error correction codes are designed to protect quantum information from errors due to decoherence or other environmental factors. These codes exploit redundancy in quantum states without violating the no-cloning theorem.

4. **Quantum Teleportation:** Quantum teleportation allows the transfer of quantum information from one location to another without copying the quantum state itself. It relies on entanglement and Bell measurements to achieve this, respecting the no-cloning theorem.

5. **Quantum Cloning Approximation:** Although exact cloning is forbidden, approximate cloning can be achieved using quantum cloning machines. These machines produce clones that are close approximations to the original state, but they introduce some level of error. Various cloning strategies aim to optimize the trade-off between fidelity and the number of clones produced.

In summary, the no-cloning theorem is a fundamental concept in quantum mechanics that underscores the unique properties and limitations of quantum information. It has important implications for quantum technologies and security protocols, and it sets quantum information apart from classical information in terms of copying and cloning.

7 BB84 protocol

BB84, short for Bennett-Brassard 1984, is a quantum key distribution (QKD) protocol that allows two parties, traditionally referred to as Alice (the sender) and Bob (the receiver), to establish a secure cryptographic key over a potentially insecure quantum communication channel. The security of BB84 relies on the principles of quantum mechanics, including the no-cloning theorem and the uncertainty principle. Below is a mathematical description of the BB84 protocol:

1. **Quantum Bit Preparation:** Alice selects a random sequence of bits, which we'll denote as the "key" bits (k), and another random sequence of bits, known as the "basis" bits (b). Each basis bit (b) indicates how Alice prepares the corresponding key bit (k):

   If $b = 0$, Alice prepares the qubit in either the $|0\rangle$ state or the $|1\rangle$ state, randomly chosen. If $b = 1$, Alice prepares the qubit in either the $|+\rangle$ state (Hadamard basis) or the $|-\rangle$ state (Hadamard basis), randomly chosen. The resulting quantum state prepared by Alice can be expressed as:

   $$|\Psi_A\rangle = \sum_i |b_i\rangle \otimes |k_i\rangle. \tag{31}$$

   Here, $|b_i\rangle$ represents the basis state for the $i-$th qubit, and $|k_i\rangle$ represents the key bit for the $i-$th qubit.

2. **Quantum Transmission:**

   - Alice sends the prepared qubits to Bob over the quantum communication channel.

- Due to the properties of quantum mechanics, any eavesdropping by a third party (Eve) will disturb the qubits, potentially revealing her presence.

3. **Quantum Measurement:**
   - Upon receiving the qubits, Bob randomly selects basis bits (b') to measure each qubit, just as Alice did. This means that, for each qubit, Bob randomly chooses to measure it in either the computational basis ($b' = 0$) or the Hadamard basis ($b' = 1$).
   - Bob performs measurements on each qubit, obtaining measurement results (0 or 1) and records them.
4. **Public Announcement of Basis:** Alice and Bob publicly announce which basis bits they used (b and b', respectively), but they do not reveal the actual values of these bits.
5. **Error Estimation and Data Filtering:**
   - Alice and Bob compare the basis bits they publicly announced.
   - For matching basis bits ($b = b'$), the corresponding key bits (k and k') become part of the final secure key. For non-matching basis bits, the associated key bits are discarded.
6. **Privacy Amplification:** To enhance security, Alice and Bob perform privacy amplification on the remaining key bits to remove any residual information that might have been acquired by an eavesdropper.

BB84's security is based on the principles of quantum mechanics, which make it extremely difficult for an eavesdropper to intercept the quantum states without leaving detectable traces. Any eavesdropping attempts can be detected through the mismatch between Alice's and Bob's basis choices, leading to a reduction in the final key size and a secure key exchange.

8 E91 protocol

The E91 protocol, also known as the Ekert 91 protocol, is a quantum key distribution (QKD) protocol designed to establish a secure cryptographic key between two parties, traditionally referred to as Alice and Bob, over a potentially insecure quantum communication channel. The E91 protocol is based on the phenomenon of quantum entanglement and is one of the early protocols for quantum key distribution. Below is a mathematical description of the E91 protocol.

1. **Quantum Entanglement Preparation:**

- A third party, traditionally referred to as Charlie, generates pairs of entangled particles (qubits) in one of two Bell states (also known as EPR pairs). The Bell states are:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}, \\ |\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}. \tag{32}$$

  Charlie prepares a sequence of these Bell pairs.
- Charlie randomly measures each qubit in one of two bases: the standard basis ($Z-$basis) or the Hadamard basis ($X-$basis). The measurement basis is represented by a random sequence of bits (0 or 1) for each qubit.
- Charlie records the measurement outcomes and the basis choices for each qubit.

2. **Quantum Transmission:** Charlie sends one qubit from each entangled pair to Alice and the other qubit to Bob over the quantum communication channel. Charlie keeps the measurement outcomes and basis choices secret.

3. **Quantum Measurement by Alice and Bob:**

   - Upon receiving her qubits, Alice randomly chooses one of two measurement bases (Z or X) for each qubit and performs measurements accordingly. She records the measurement outcomes and the basis choices but does not reveal them to Bob.
   - Similarly, Bob randomly selects a measurement basis (Z or X) for each of his qubits, performs measurements, and records the results and basis choices.

4. **Public Announcement of Measurement Bases:** After the measurements are completed, Alice and Bob publicly announce which measurement bases they used for each qubit but do not reveal the measurement outcomes themselves.

5. bf Error Estimation and Data Filtering:

   - Alice and Bob compare their basis choices for each qubit. For matching basis choices, they keep the measurement outcomes as a potential part of their secure key.
   - The mismatched basis choices are discarded, and the corresponding measurement outcomes are not included in the key.

6. **Privacy Amplification:** To enhance security, Alice and Bob perform privacy amplification on the remaining measurement outcomes, typically using classical error-correcting codes and hashing functions, to obtain a shorter, secure cryptographic key.

The security of the E91 protocol relies on the properties of quantum entanglement and the no-cloning theorem, making it resistant to eavesdropping attempts. Any interference by an eavesdropper would disturb the entangled qubits, leading to detection by Alice and Bob during the basis-matching step.