

# Quantum Computing

## An Introduction

Nishanka Das    Debanjan Kola

November 2023

# Contents

- 1 Introduction
- 2 Classical Information
- 3 Dirac Notation
- 4 Multiplication of Bra and Ket
- 5 Probability Vector and Measuring Probabilistic State
- 6 Classical Operation
- 7 Quantum State Vector
- 8 Measuring Quantum States
- 9 Measuring Quantum States
- 10 Unitary Operations
- 11 Pauli Operations
- 12 Hadamard Operation
- 13 Phase Operations
- 14 Probabilistic States and Conditional Probabilities
- 15 Quantum State Representation

# Introduction

- Overview of Quantum Computing
- Basics of Quantum Systems

## Assumption

Let  $X$  be a system member defining the set of Classical States, i.e.,  $\Sigma$ .

# Dirac Notation

Ket  $|a\rangle$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Bra  $\langle a|$

$$\langle 0| = (1 \quad 0)$$

$$\langle 1| = (0 \quad 1)$$

# Multiplication of Bra and Ket

We represent the arbitrary column vector by  $|\psi\rangle$  and arbitrary row vector by  $\langle\psi|$

- Multiplication of  $|x\rangle \langle y|$  becomes a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- Multiplication of  $\langle x| |y\rangle$  becomes a number

$$(a)$$

# Probability Vector and Measuring Probabilistic State

## Probabilistic State

A probabilistic state represents the state of a quantum system where the system's state isn't determined with certainty but rather as a probability distribution over possible states.

# Classical Operation

## Deterministic Operation

Every function  $f : \Sigma \rightarrow \Sigma$  describes a deterministic operation that transforms the classical state  $a$  into  $f(a)$ ,  $\forall a \in \Sigma$

Given any function  $f : \Sigma \rightarrow \Sigma$ , there is a unique matrix  $M$  satisfying  $M|a\rangle = |f(a)\rangle \forall a \in \Sigma$

Matrix  $M$  can be got by the equation  $M(b, a) = \begin{cases} 1; b = f(a) \\ 0; b \neq f(a) \end{cases}$  In this  $M$  matrix there must be only one 1 in each column and other entries would be 0

.



## Probabilistic Operation and Composition

Probabilistic Operations are classical operations that may introduce randomness or uncertainty. It can be described by Stochastic matrix.

Where,

- 1) All entries are non-negative real numbers.
- 2) The entries in every column sum to 1.

Suppose that  $X$  is a system having classical state set  $\Sigma$  and  $M_1, \dots, M_n$  are stochastic matrices representing probabilistic operations on the system  $X$ .

If the first operation  $M_1$  is applied to the probabilistic state represented by a probability vector  $u$ , the resulting probabilistic state is represented by the vector  $M_1 u$ . If we then apply the second probabilistic operation  $M_2$  to this new probability vector, we obtain the probability vector

$$M_2(M_1 u) = (M_2 M_1)u \text{ ( by associative operation )}$$

# Quantum State Vector

A quantum state of a system is represented by a column vector, similar to probabilistic states. As before, the indices of the vector label the classical states of the system.

## Properties

- The entries of a quantum state vector are complex numbers.
- The sum of the absolute values squared of the entries of a quantum state vector is 1.

## Euclidean Norm

The Euclidean norm of a column vector  $v = \begin{pmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{pmatrix}$  is denoted and defined as follows:

$$\|v\| = \sqrt{\sum_{i=1}^n |\alpha_i|^2}$$

# Measuring Quantum States

If a quantum state is measured, each classical state of the system results with probability equal to the absolute value squared of the entry in the quantum state vector corresponding to that classical state. This is known as the Born rule in quantum mechanics. Notice that this rule is consistent with the requirement that the absolute values squared of the entries in a quantum state vector sum to 1. as it implies that the probabilities of different classical state measurement outcomes sum to 1.

For Example

$$|+\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$$

results in the two possible outcomes, 0 and 1 with probabilities as follows.

$$\Pr(\text{Outcome is 0}) = |\langle 0 | + \rangle|^2 = (1/\sqrt{2})^2 = 1/2$$

$$\Pr(\text{Outcome is 1}) = |\langle 1 | + \rangle|^2 = (1/\sqrt{2})^2 = 1/2$$

# Unitary Operations

Unitary operations are transformations applied to quantum states that preserve the inner product and maintain the normalization of quantum states. These operations are represented by unitary matrices.

# Pauli Operations

The four Pauli matrices are as follows:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$$

# Hadamard Operation

The Hadamard operation is described by this matrix:

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

# Phase Operations

A phase operation is described by the matrix:

$$P_{\theta} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$



# Relation Between Hadamard and $|+\rangle / |-\rangle$

There is a relation between  $H$  and  $|+\rangle / |-\rangle$ :

$$H|0\rangle = |+\rangle$$

$$H|1\rangle = |-\rangle$$

$$H|+\rangle = |0\rangle$$

$$H|-\rangle = |1\rangle$$

# Introduction to Classical States

- Classical States of Multiple Systems
- Compound System  $(X, Y)$
- Cartesian Product of Classical State Sets

# Cartesian Product of Classical State Sets

The set of classical states of  $(X, Y)$  is the Cartesian product of  $\Sigma$  and  $\Gamma$ , denoted as  $\Sigma \times \Gamma$ .

$$\Sigma \times \Gamma = \{(a, b) : a \in \Sigma \text{ and } b \in \Gamma\}$$

# More than Two Systems

For more than two systems  $X_1, \dots, X_n$  with classical state sets  $\Sigma_1, \dots, \Sigma_n$ :

$$\Sigma_1 \times \dots \times \Sigma_n = \{(a_1, \dots, a_n) : a_1 \in \Sigma_1, \dots, a_n \in \Sigma_n\}$$

# Example: Two Bits

If  $X_1, \dots, X_{10}$  are bits with classical state sets  $\Sigma_1 = \dots = \Sigma_{10} = \{0, 1\}$ :

$$\Sigma_1 \times \dots \times \Sigma_{10} = \{0, 1\}^{10}$$

# Probabilistic states

For example, suppose that  $X$  and  $Y$  are both bits, so that their corresponding classical state sets are  $\Sigma = \{0, 1\}$  and  $\Gamma = \{0, 1\}$ , respectively. Here is a probabilistic state of the pair  $(X, Y)$ :

$$\begin{aligned}\Pr((X, Y) = (0, 0)) &= \frac{1}{2}, \\ \Pr((X, Y) = (0, 1)) &= 0, \\ \Pr((X, Y) = (1, 0)) &= 0, \\ \Pr((X, Y) = (1, 1)) &= \frac{1}{2}.\end{aligned}$$

This probabilistic state is one in which both  $X$  and  $Y$  are random bits — each is 0 with probability  $\frac{1}{2}$  and 1 with probability  $\frac{1}{2}$  — but the classical states of the two bits always agree. This is an example of a correlation between these systems.

# Probabilistic State of Two Bits

Probabilistic state for two bits:

$\frac{\text{Probability for state 00}}{\longrightarrow}$	$\frac{1}{2}$	$\frac{\text{Probability for state 01}}{\longrightarrow}$	0
$\frac{\text{Probability for state 10}}{\longrightarrow}$	0	$\frac{\text{Probability for state 11}}{\longrightarrow}$	$\frac{1}{2}$

# Independence of Systems

Systems  $X$  and  $Y$  are independent if:

$$\Pr((X, Y) = (a, b)) = \Pr(X = a) \Pr(Y = b)$$



# Probabilistic State Independence

If  $(X, Y)$  has a probabilistic state described by:

$$\sum_{(a,b) \in \Sigma \times \Gamma} p_{ab} |ab\rangle$$

It is independent if there exist probability vectors  $|\phi\rangle$  and  $|\psi\rangle$  such that:

$$p_{ab} = q_a r_b$$

# Probabilistic States and Conditional Probabilities

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} p_{ab} |ab\rangle$$

Measuring  $X$  alone yields each possible outcome with probabilities

$$\Pr(X = a) = \sum_{b \in \Gamma} p_{ab}$$

Thus, the vector representing the probabilistic state of  $X$  alone is given by

$$\sum_{a \in \Sigma} \left( \sum_{c \in \Gamma} p_{ac} \right) |a\rangle$$

# Tensor products of vectors

The condition of independence just described can be expressed more succinctly through the notion of a tensor product. Although this is a very general notion that can be defined quite abstractly and applied to a variety of mathematical structures, in the case at hand it can be defined in simple, concrete terms. Given two vectors

$$|\phi\rangle = \sum_{a \in \Sigma} \alpha_a |a\rangle \quad \text{and} \quad |\psi\rangle = \sum_{b \in \Gamma} \beta_b |b\rangle,$$

the tensor product  $|\phi\rangle \otimes |\psi\rangle$  is a new vector over the joint state set  $\Sigma \times \Gamma$ , defined as

$$|\phi\rangle \otimes |\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} \alpha_a \beta_b |ab\rangle.$$

Equivalently, the vector  $|\pi\rangle = |\phi\rangle \otimes |\psi\rangle$  is defined by the equation

$$\langle ab | \pi \rangle = \langle a | \phi \rangle \langle b | \psi \rangle$$

# Tensor products of vectors

We can now recast the condition for independence as requiring the probability vector  $|\pi\rangle$  of the joint system  $(X, Y)$  to be representable as a tensor product

$$|\pi\rangle = |\phi\rangle \otimes |\psi\rangle$$

of probability vectors  $|\phi\rangle$  and  $|\psi\rangle$  on each of the subsystems  $X$  and  $Y$ . In this situation, it is said that  $|\pi\rangle$  is a product state or product vector.

# Tensor products of matrices

The tensor product  $M \otimes N$  of the matrices

$$M = \sum_{a,b \in \Sigma} \alpha_{ab} |a\rangle\langle b|$$

and

$$N = \sum_{c,d \in \Gamma} \beta_{cd} |c\rangle\langle d|$$

is the matrix

$$M \otimes N = \sum_{a,b \in \Sigma} \sum_{c,d \in \Gamma} \alpha_{ab} \beta_{cd} |ac\rangle\langle bd|$$

# Tensor products of matrices

Equivalently,  $M \otimes N$  is defined by the equation

$$\langle ac | M \otimes N | bd \rangle = \langle a | M | b \rangle \langle c | N | d \rangle$$

being true for every selection of  $a, b \in \Sigma$  and  $c, d \in \Gamma$ .

An alternative, but equivalent, way to describe  $M \otimes N$  is that it is the unique matrix that satisfies the equation

$$(M \otimes N)(|\phi\rangle \otimes |\psi\rangle) = (M|\phi\rangle) \otimes (N|\psi\rangle)$$

for every possible choice of vectors  $|\phi\rangle$  and  $|\psi\rangle$ . Here we are assuming that the indices of  $|\phi\rangle$  correspond to the elements of  $\Sigma$  and the indices of  $|\psi\rangle$  correspond to  $\Gamma$ .

# Probabilistic States and Conditional Probabilities

Having obtained a particular outcome  $a \in \Sigma$  of the measurement of  $X$ , the probabilistic state of  $Y$  is updated according to the formula for conditional probabilities:

$$|\pi_a\rangle = \frac{\sum_{b \in \Gamma} p_{ab} |b\rangle}{\sum_{c \in \Gamma} p_{ac}}$$

We update the probabilistic state of the joint system  $(X, Y)$  to  $|a\rangle \otimes |\pi_a\rangle$ .

# Quantum State Representation

We may use the fact that  $|ab\rangle = |a\rangle|b\rangle$  (for any classical states  $a$  and  $b$ ) to instead write

$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{6}}|0\rangle|1\rangle + \frac{i}{\sqrt{6}}|1\rangle|0\rangle + \frac{1}{\sqrt{6}}|1\rangle|1\rangle.$$

We may choose to write the tensor product symbol explicitly like this:

$$\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle - \frac{1}{\sqrt{6}}|0\rangle \otimes |1\rangle + \frac{i}{\sqrt{6}}|1\rangle \otimes |0\rangle + \frac{1}{\sqrt{6}}|1\rangle \otimes |1\rangle.$$

We may subscript the kets to indicate how they correspond to the systems being considered, like this:

$$\frac{1}{\sqrt{2}}|0\rangle_X|0\rangle_Y - \frac{1}{\sqrt{6}}|0\rangle_X|1\rangle_Y + \frac{i}{\sqrt{6}}|1\rangle_X|0\rangle_Y + \frac{1}{\sqrt{6}}|1\rangle_X|1\rangle_Y.$$



# Quantum State Representation

Of course, we may also write quantum state vectors explicitly as column vectors:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{6}} \\ \frac{i}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}.$$

# Unitary operations

We can represent operations on multiple systems as unitary matrices acting on the state vector of this larger system.

In principle, any unitary matrix whose rows and columns correspond to the classical states of whatever system we're thinking about represents a valid quantum operation—and this holds true for compound systems whose classical state sets happen to be Cartesian products of the classical state sets of the individual systems.

Focusing on two systems, if  $X$  is a system having classical state set  $\Sigma$  and  $Y$  is a system having classical state set  $\Gamma$ , then the classical state set of the joint system  $(X, Y)$  is  $\Sigma \times \Gamma$ —and therefore the set of operations that can be performed on this joint system are represented by unitary matrices whose rows and columns are placed in correspondence with the set  $\Sigma \times \Gamma$ . The ordering of the rows and columns of these matrices is the same as the ordering used for quantum state vectors of the system  $(X, Y)$ .

# The swap operation

Suppose that  $X$  and  $Y$  are systems that share the same classical state set  $\Sigma$ . The swap operation on the pair  $(X, Y)$  is the operation that exchanges the contents of the two systems but otherwise leaves the systems alone (so that  $X$  remains on the left and  $Y$  remains on the right).

We will denote this operation as SWAP. It operates like this for every choice of classical states  $a, b \in \Sigma$ :

$$\text{SWAP } |a\rangle|b\rangle = |b\rangle|a\rangle.$$

One way to write the matrix associated with this operation using the Dirac notation is as follows:

$$\text{SWAP} = \sum_{c,d \in \Sigma} |c\rangle\langle d| \otimes |d\rangle\langle c|.$$

# The swap operation

It may not be immediately clear that this matrix represents SWAP, but we can check it satisfies the condition  $\text{SWAP} |a\rangle|b\rangle = |b\rangle|a\rangle$  for every choice of classical states  $a, b \in \Sigma$ . As a simple example, when  $X$  and  $Y$  are qubits, we find that

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

# Circuits

Circuits are models of computation in which information is carried by wires through a network of gates, which represent operations that transform the information carried by the wires. Here we will discuss two types of circuits:

- Boolean Circuits

Boolean circuits involve wires carrying binary values, and the gates represent Boolean logic operations.

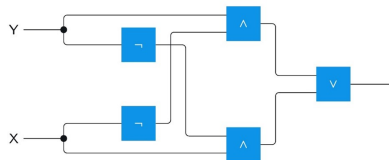


Figure: Example of a Boolean Circuit

- Quantum Circuits

Quantum circuits introduce the principles of quantum computing, where information is carried by quantum bits (qubits) and operations are represented by quantum gates. The operation is done from Left to right



Figure: Example of a Quantum Circuit

# Quantum Circuit

- Multi Qubit Quantum Circuit

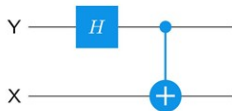


Figure: Example of a Multi Qubit Quantum Circuit

# Quantum Circuit

- Step 1: Hadamard Operation on  $Y$

The first operation is a Hadamard operation on  $Y$ :

$$H_Y = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Step 2: Controlled-NOT Operation

The second operation is the controlled-NOT operation, where  $Y$  is the control and  $X$  is the target:

$$\text{CNOT}_{YX} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



# Quantum Circuit

For reference, the Hadamard gate is represented as:

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

- Single Qubit Gates



Figure: Example of a Single Qubit Gates

# Quantum Circuit

- Multiple Qubit Gates

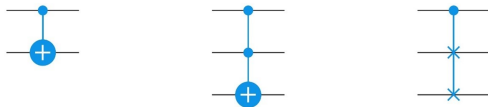


Figure: Example of a Multiple Qubit Gates

# Inner Product

If we have a column vector representing a quantum state:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

the corresponding bra vector is the conjugate transpose of this vector:

$$\langle\psi| = (|\psi\rangle)^\dagger = (\overline{\alpha_1} \quad \overline{\alpha_2} \quad \cdots \quad \overline{\alpha_n}). \quad (1)$$

Alternatively, if we express a column vector as a ket with a classical state set  $\Sigma$ :

$$|\psi\rangle = \sum_{a \in \Sigma} \alpha_a |a\rangle,$$

# Inner Product

then the corresponding row (or bra) vector is the conjugate transpose:

$$\langle\psi| = \sum_{a \in \Sigma} \overline{\alpha_a} \langle a|. \quad (2)$$

The product of a bra vector and a ket vector results in a scalar:

$$\langle\psi|\phi\rangle = \langle\psi||\phi\rangle = \sum_{a \in \Sigma} \overline{\alpha_a} \beta_a,$$

where  $|\phi\rangle = \sum_{b \in \Sigma} \beta_b |b\rangle$ .

The inner product between vectors  $|\psi\rangle$  and  $|\phi\rangle$  is given by:

$$\langle\psi|\phi\rangle = \sum_{a \in \Sigma} \overline{\alpha_a} \beta_a.$$

# Inner Product

- Relationship to the Euclidean Norm

The inner product of a vector with itself is related to the Euclidean norm:

$$\langle \psi | \psi \rangle = \sum_{a \in \Sigma} \overline{\alpha_a} \alpha_a = \sum_{a \in \Sigma} |\alpha_a|^2 = ||\psi\rangle||^2.$$

Thus, the Euclidean norm of a vector can be expressed as:

$$||\psi\rangle|| = \sqrt{\langle \psi | \psi \rangle}.$$

The Euclidean norm is always a nonnegative real number, and it is equal to zero if and only if  $|\psi\rangle = 0$ .

# Conjugate symmetry

For any two vectors

$$|\psi\rangle = \sum_{a \in \Sigma} \alpha_a |a\rangle \quad \text{and} \quad |\phi\rangle = \sum_{b \in \Sigma} \beta_b |b\rangle,$$

we have

$$\langle \psi | \phi \rangle = \sum_{a \in \Sigma} \overline{\alpha_a} \beta_a \quad \text{and} \quad \langle \phi | \psi \rangle = \sum_{a \in \Sigma} \overline{\beta_a} \alpha_a,$$

and therefore

$$\overline{\langle \psi | \phi \rangle} = \langle \phi | \psi \rangle.$$

# Linearity in the second argument

Let us suppose that  $|\psi\rangle, |\phi_1\rangle, |\phi_2\rangle$  are vectors and  $\alpha_1, \alpha_2$  are complex numbers. If we define a new vector

$$|\phi\rangle = \alpha_1|\phi_1\rangle + \alpha_2|\phi_2\rangle,$$

then

$$\langle\psi|\phi\rangle = \langle\psi|(\alpha_1|\phi_1\rangle + \alpha_2|\phi_2\rangle) = \alpha_1\langle\psi|\phi_1\rangle + \alpha_2\langle\psi|\phi_2\rangle.$$

That is to say, the inner product is linear in the second argument. This can be verified either through the formulas above or simply by noting that matrix multiplication is linear in each argument (and specifically in the second argument).

# Linearity in the second argument

Combining this fact with conjugate symmetry reveals that the inner product is conjugate linear in the first argument. That is, if  $|\psi_1\rangle, |\psi_2\rangle, |\phi\rangle$  are vectors and  $\alpha_1, \alpha_2$  are complex numbers, and we define

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle,$$

then

$$\langle\psi|\phi\rangle = (\overline{\alpha_1}\langle\psi_1| + \overline{\alpha_2}\langle\psi_2|)|\phi\rangle = \overline{\alpha_1}\langle\psi_1|\phi\rangle + \overline{\alpha_2}\langle\psi_2|\phi\rangle.$$



# The Cauchy–Schwarz inequality

For every choice of vectors  $|\phi\rangle$  and  $|\psi\rangle$  having the same number of entries, we have

$$|\langle\psi|\phi\rangle| \leq \| |\psi\rangle \| \| |\phi\rangle \|.$$

# Orthogonal and orthonormal sets

Two vectors  $|\phi\rangle$  and  $|\psi\rangle$  are said to be orthogonal if their inner product is zero:

$$\langle\psi|\phi\rangle = 0.$$

**Orthogonal Set:** A set of vectors  $\{|\psi_1\rangle, \dots, |\psi_m\rangle\}$  is called an orthonormal set if it is an orthogonal set and, in addition, every vector in the set is a unit vector. Alternatively, this set is an orthonormal set if

$$\langle\psi_j|\psi_k\rangle = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases}$$

# Orthonormal sets and unitary matrices

Orthonormal sets of vectors are closely connected with unitary matrices. One way to express this connection is to say that the following three statements are logically equivalent (meaning that they are all true or all false) for any choice of a square matrix  $U$ :

- 1 The matrix  $U$  is unitary (i.e.,  $U^\dagger U = UU^\dagger = I$ ).
- 2 The rows of  $U$  form an orthonormal set.
- 3 The columns of  $U$  form an orthonormal set.

# Projection Matrix

A square matrix  $\Pi$  is called a projection if it satisfies two properties:

- 1  $\Pi = \Pi^\dagger$ .
- 2  $\Pi^2 = \Pi$ .

# Projective measurements

Projective measurements are measurements that are described by a collection of projections whose sum is equal to the identity matrix. In symbols, a collection  $\{\Pi_1, \dots, \Pi_m\}$  of projection matrices describes a projective measurement if

$$\Pi_1 + \dots + \Pi_m = \mathbb{I}.$$

# Limitations on quantum information

1) Irrelevance of global phases: Suppose that  $|\psi\rangle$  and  $|\phi\rangle$  are unit vectors representing quantum states of some system, and assume moreover that there exists a complex number  $\alpha$  which satisfies

$$|\phi\rangle = \alpha|\psi\rangle$$

Then these two unit vectors will be called that they are differed by a global phase. It requires that  $|\alpha| = 1$  or alternatively,  $\alpha = e^{i\theta}$  for some real number  $\theta$ .

For example,  $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$  and  $-|-\rangle = -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ .

# Limitations on quantum information

2) No-cloning theorem : Let  $X$  and  $Y$  be systems sharing the same classical state set  $\Sigma$  having at least two elements. There does not exist a quantum state  $|\phi\rangle$  of  $Y$  and a unitary operation  $U$  on the pair  $(X, Y)$  such that

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

That means there is no unitary operation by which we can copy a quantum state.

# Limitations on quantum information

Proof: The vector we get after the unitary operation  $U$

$$U \left( \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |\phi\rangle \right) = \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle.$$

$$U \left( \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |\phi\rangle \right) \neq \frac{1}{\sqrt{2}}|a\rangle \otimes |a\rangle + \frac{1}{\sqrt{2}}|b\rangle \otimes |b\rangle$$



# Limitations on quantum information

Controlled-NOT gate can clone a few certain quantum state vectors, but it is inefficient for all the vectors.

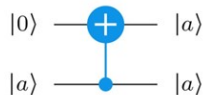


Figure: controlled-NOT operation

**3) Non-orthogonal states cannot be perfectly discriminated:** If we have two quantum states  $|\psi\rangle$  and  $|\phi\rangle$  that are not orthogonal, which means that  $\langle\phi|\psi\rangle \neq 0$ , then it's impossible to tell them apart perfectly. If we do have a way to discriminate two states perfectly, without any error, then they must be orthogonal.

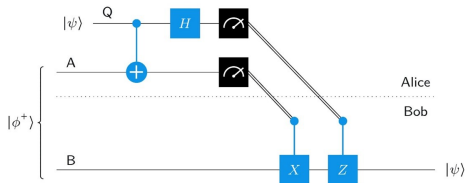
# Teleportation

## 1. Teleportation

Quantum teleportation, or just teleportation for short, is a protocol where a sender (Alice) transmits a qubit to a receiver (Bob) by making use of a shared entangled quantum state (one e-bit, to be specific) along with two bits of classical communication.

# Teleportation

## 1.1 Protocol



### 1. Alice's Operations:

- 1 Alice performs a controlled-NOT operation on the pair  $(A, Q)$ , with  $Q$  being the control and  $A$  being the target. She then performs a Hadamard operation on  $Q$ .
- 2 Alice measures both  $A$  and  $Q$  with respect to a standard basis measurement. Let  $a$  be the outcome of the measurement of  $A$ , and  $b$  be the outcome of the measurement of  $Q$ .

# Teleportation

## 2. Bob's Operations:

Bob receives  $a$  and  $b$  from Alice and performs the following conditional operations:

- If  $a = 1$ , then Bob performs a bit flip (or  $X$  gate) on his qubit  $B$ .
- If  $b = 1$ , then Bob performs a phase flip (or  $Z$  gate) on his qubit  $B$ .

That is, conditioned on  $ab$  being 00, 01, 10, or 11, Bob performs one of the operations  $I$ ,  $Z$ ,  $X$ , or  $ZX$  on the qubit  $B$ .

## 1.2 Conclusion

- 1 It is not an application of quantum information; it's a protocol for performing quantum communication.
- 2 It is reasonable to speculate that teleportation could one day become a standard way to communicate quantum information, perhaps through a process known as entanglement distillation (Process to convert large noisy e-bits into small high-quality e-bits).

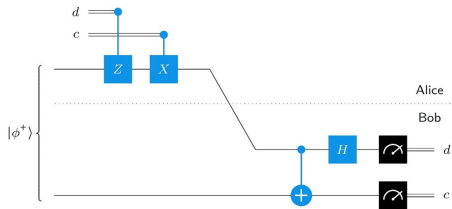
## 2. Superdense Coding

Superdense coding is a protocol that, in some sense, achieves a complementary aim to teleportation. Rather than allowing for the transmission of one qubit using two classical bits of communication (at the cost of one e-bit of entanglement), it allows for the transmission of two classical bits using one qubit of quantum communication (again, at the cost of one e-bit of entanglement).

**Note:** Holevo's theorem implies that without the use of a shared entangled state, it is impossible to communicate more than one bit of classical information by sending a single qubit.

# Superdense coding

## 2.1 Protocol



# Superdense coding

**In words, here is what Alice does:**

- ① If  $d = 1$ , Alice performs a Z gate on her qubit A (and if  $d = 0$ , she does not).
- ② If  $c = 1$ , Alice performs an X gate on her qubit A (and if  $c = 0$ , she does not).

**Now the part of Bob:** What Bob does when he receives the qubit A is to first perform a controlled-NOT gate, with A being the control and B being the target, and then he applies a Hadamard gate to A. He then measures B to obtain  $c$  and A to obtain  $d$ , with standard basis measurements in both cases.

## 2.2 Remarks

- a) Superdense coding seems unlikely to be useful in a practical sense.
- b) Together, teleportation and superdense coding establish an equivalence:

$$\frac{2 \text{ bits of classical communication}}{1e - \text{bitneededinbothcases}} = 1 \text{ bit of quantum communication}$$

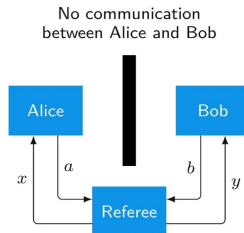
# The CHSH Game

## 3. The CHSH Game

It is not a protocol; it's a game or game theory in the sense of mathematical abstraction.

### 3.1 Nonlocal Game

- 1 Description of the nonlocal game goes here.
- 2 You can add more details as needed.





# The CHSH Game

It is a cooperative game where two players work together to achieve a particular outcome, and there is a referee who strictly follows the rules. They can prepare for the game however they choose, but once the game starts, they are forbidden from communicating. We might imagine the game taking place in a secure facility of some sort, as if the referee is playing the role of a detective, and Alice and Bob are suspects being interrogated in different rooms.

The way a nonlocal game works is that the referee first asks each of them a question. We'll use the letter  $x$  to refer to the First one's question and  $y$  to refer to the Second one's question. Here, we're thinking of  $x$  and  $y$  as being classical states, and in the CHSH game,  $x$  and  $y$  are bits. Questions are selected randomly. Alice and Bob either win or lose depending on whether or not the pair of answers  $(a, b)$  is deemed correct for the pair of questions  $(x, y)$  according to some fixed set of rules.

# The CHSH Game

## 3.2 General Description

- 1 The questions and answers are all bits:  $x, y, a, b \in \{0, 1\}$ .
- 2 The referee chooses the questions  $(x, y)$  uniformly at random. That is, each of the four possibilities,  $(0, 0)$ ,  $(0, 1)$ ,  $(1, 0)$ , and  $(1, 1)$ , is selected with probability  $1/4$ .
- 3 The answers  $(a, b)$  win for the questions  $(x, y)$  if  $a \oplus b = x \wedge y$  and lose otherwise. The following table expresses this rule by listing the winning and losing conditions on the answers  $(a, b)$  for each pair of questions  $(x, y)$ .

$(x, y)$	Win	Lose
$(0, 0)$	$a = b$	$a \neq b$
$(0, 1)$	$a = b$	$a \neq b$
$(1, 0)$	$a = b$	$a \neq b$
$(1, 1)$	$a \neq b$	$a = b$