# Introductory Notes on Quantum Mechanics (plus a little bit of Quantum Information Theory)

Michael E. Cuffaro

May 23, 2014

Vector space: a nonempty set $V$ whose elements are referred to as vectors:

- ordered $n$-tuples of numbers $\psi = (z_1, z_2, \ldots, z_n)$ satisfying:
  - Vector addition: $\psi + \phi = \chi \in V$.

    E.g. $(1, 4, 3, 2) + (3, 9, 8, 4) = (4, 13, 11, 6)$
  - Scalar multiplication: $z \cdot \psi = \xi \in V$.

    E.g., $5 \cdot (3, 2, 4, 3) = (15, 10, 20, 15)$.
- zero vector: $\mathbb{0}$ s.t. $\psi + \mathbb{0} = \mathbb{0} + \psi = \psi$.

Our vector space:

$\mathbb{C}^n$: vector space of $n$-tuples of complex numbers:

$c = a + bi$, where $i = \sqrt{-1}$, $a, b \in \mathbb{R}$.

Column matrix notation for vectors:

$$(c_1, c_2, \ldots, c_n) \quad \Rightarrow \quad \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

Addition:
$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} + \begin{bmatrix} c_1' \\ c_2' \\ \vdots \\ c_n' \end{bmatrix} = \begin{bmatrix} c_1 + c_1' \\ c_2 + c_2' \\ \vdots \\ c_n + c_n' \end{bmatrix}$$

Scalar multiplication:
$$c \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} c \cdot c_1 \\ c \cdot c_2 \\ \vdots \\ c \cdot c_n \end{bmatrix}$$

Dirac notation:

"Ket"

$$|\psi\rangle \equiv \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

"Bra"

$$\langle\psi| \equiv \begin{bmatrix} c_1^* & c_2^* & \dots & c_n^* \end{bmatrix}$$

$c^*$: complex conjugation: $i \Rightarrow -i$.

$$c^* = (a + bi)^* = a - bi.$$

"Bra" and "Ket" $\Rightarrow$ "Bra-ket"

## Spanning set

A set of vectors $\{|v_1\rangle, |v_2\rangle, \ldots |v_n\rangle\}$ spans a vector space $V$ if any vector in $V$ can be expressed as a linear combination of vectors in that set.

E.g., $|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

spans $\mathbb{C}^2$, since any vector $|\psi\rangle \in \mathbb{C}^2$ can be written as:

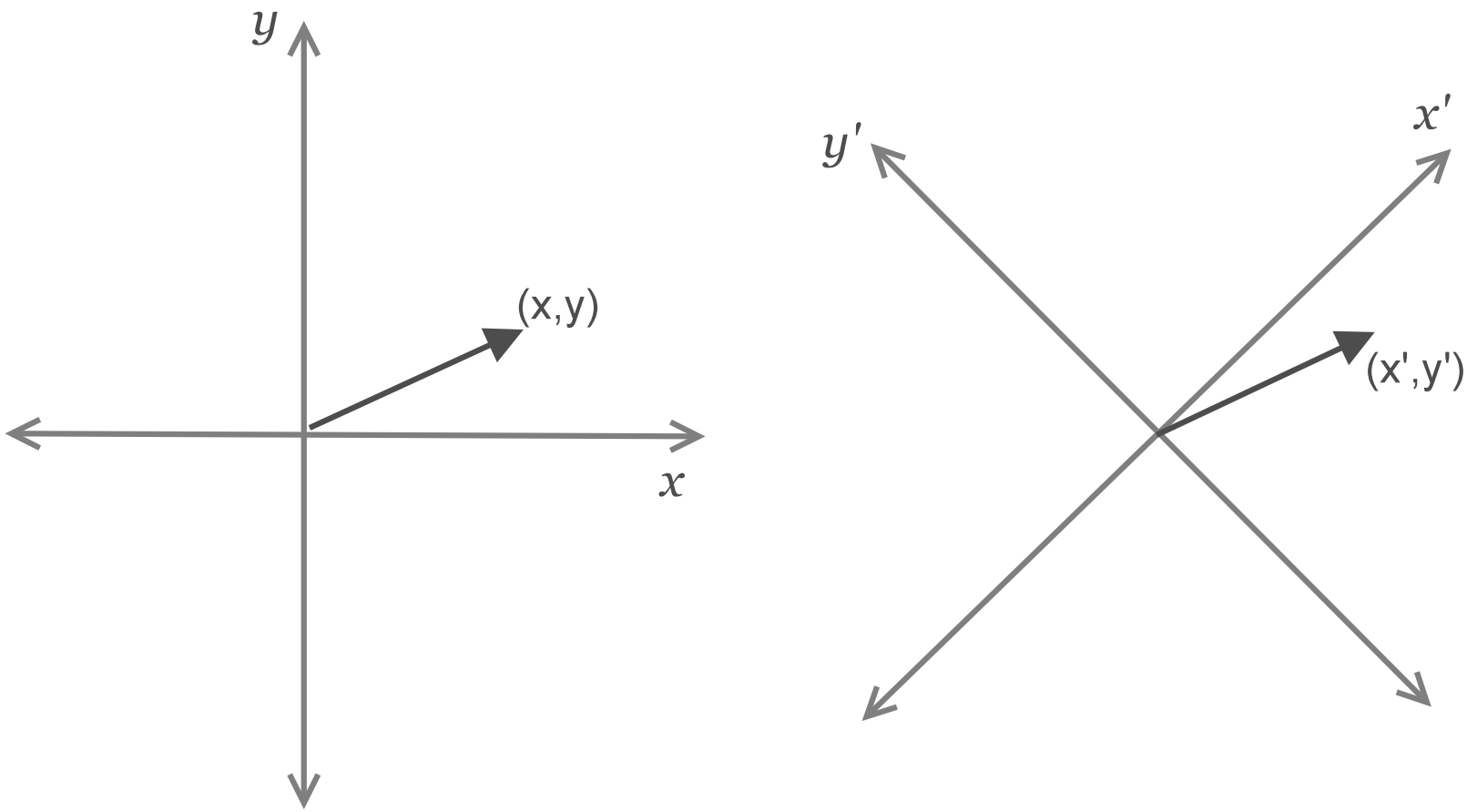
$|\psi\rangle = c_1|v_1\rangle + c_2|v_2\rangle.$

A vector space may have more than one spanning set.

E.g., $|u_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |u_2\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

also spans $\mathbb{C}^2$.

Analogy:




$x$ and $y$ span the space, and so do $x'$ and $y'$.

## Linear dependence

A set of non-zero vectors $\{|v_1\rangle, |v_2\rangle, \ldots |v_n\rangle\}$ is linearly dependent if one vector from the set can be written as a linear combination of the other vectors in the set.

E.g., $|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, and $|u_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

are linearly dependent, since $|u_1\rangle = \frac{1}{\sqrt{2}}|v_1\rangle + \frac{1}{\sqrt{2}}|v_2\rangle$

## Basis for $V$

A set of linearly independent vectors which spans the vector space $V$ is called a basis for $V$.

$|v_1\rangle \equiv |0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|v_2\rangle \equiv |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$: "computational" basis for $\mathbb{C}^2$

$|u_1\rangle \equiv |+\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $|u_2\rangle \equiv |-\rangle \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$: "+,-" basis for $\mathbb{C}^2$.

## Dimension of a vector space

Any basis of the vector space $V$ will always contain the same number of elements: $\mathrm{d}_V$. We call $\mathrm{d}_V$ the dimension of $V$.

E.g., $\mathbb{C}^2$ is a 2-dimensional space. Its bases, which include $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ have two elements each.

## Dual vector

The dual of a ket $|\psi\rangle$ is its corresponding bra $\langle\psi|$.

Calculate by taking the adjoint of the original vector:
$\langle\psi| = (|\psi\rangle)^\dagger$.

Adjoint of a matrix $M$ (recall: vectors are column matrices!):

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

I.e., turn rows into columns and take the conjugate of every entry.

Adjoint of a vector:

$$(|\psi\rangle)^\dagger = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}^\dagger = \begin{bmatrix} c_1^* & c_2^* & \dots & c_n^* \end{bmatrix} = \langle\psi|$$

## Inner product

$\langle a|b\rangle$: maps two vectors $|a\rangle, |b\rangle$ to a complex number $c$.

E.g.,

$$\langle 0|1\rangle = (|0\rangle)^\dagger |1\rangle = \begin{bmatrix}1\\0\end{bmatrix}^\dagger \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1 & 0\end{bmatrix} \begin{bmatrix}0\\1\end{bmatrix} = 0.$$

Note: when the inner product of two vectors $|a\rangle$ and $|b\rangle$ is equal to 0, we say they are orthogonal.

## Norm (a.k.a. length) of a vector:

$$\| \, |u\rangle \, \| = \sqrt{\langle u|u\rangle}$$

## Normalising a vector

To normalise a vector, divide it by its norm: $\frac{|u\rangle}{\| \, |u\rangle \, \|}$.

Result (if $|u\rangle \neq \mathbb{0}$) is always a unit vector; i.e., it has length $= 1$.

## Orthonormal basis

The members of a set $\{|v_1\rangle, \ldots, |v_n\rangle\}$ of vectors are mutually orthogonal when the inner product of any member with any other member is 0; i.e., when $\langle v_i|v_k\rangle = 0$ for all $|v_i\rangle, |v_k\rangle$ s.t. $i \neq k$.

When each member of such a set is normalised, the set is called an orthonormal set.

When the members are also linearly independent, then if the set spans the vector space $V$, the set is an orthonormal basis for $V$.

E.g., $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are both orthonormal bases of $\mathbb{C}^2$.

Any vector in $V$ can be expressed as a linear combination of elements of the orthonormal basis

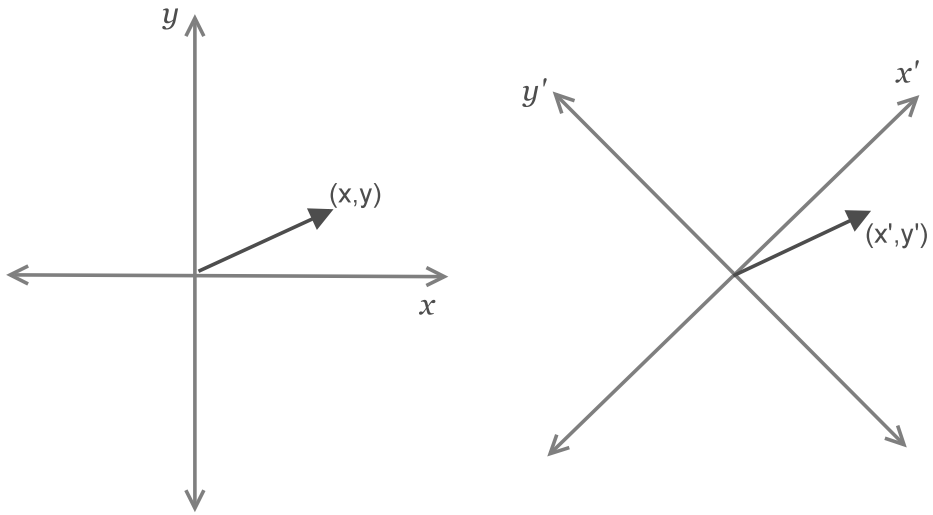
$$\forall |\psi\rangle \in \mathbb{C}^2 : \quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Similarly for any other orthonormal bases of $\mathbb{C}^2$

E.g.,

$$\forall |\psi\rangle \in \mathbb{C}^2 : \quad |\psi\rangle = \gamma|+\rangle + \delta|-\rangle$$

Note: inner products remain invariant under change of basis (so the length of a vector, $\langle v|v\rangle$, also remains invariant).



## Linear operator on a vector space $V$

Consider: a function $A$ which takes a vector $|v\rangle \in V$ to the vector $A|v\rangle = |v'\rangle \in V$.

If $A$ is "linear", i.e.: $A(\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha A|\psi\rangle + \beta A|\phi\rangle$, then $A$ is called a linear operator on $V$.

Some (trivial) examples:

- $I$ (identity operator): $I|v\rangle = |v\rangle$.
- $\emptyset$ (zero operator): $\emptyset|v\rangle = \mathbb{0}$.

Linear operators on $\mathbb{C}^2$ can be represented as $2 \times 2$ matrices.

E.g., the Pauli matrices:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Note: sometimes also referred to as $\sigma_0, \sigma_1, \sigma_2, \sigma_3$, or as $\sigma_I, \sigma_X, \sigma_Y, \sigma_Z$.

Example: $X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle.$

X is also known as the "NOT" operator.

Example: $XX|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle.$

## Outer product representation of a linear operator

$|u\rangle\langle v|$ is called an outer product.

We define it so that: $\big(|u\rangle\langle v|\big)|w\rangle = |u\rangle\langle v|w\rangle = \langle v|w\rangle|u\rangle$.

I.e., it is the operator that results in $\langle v|w\rangle|u\rangle$ when acting on $|w\rangle$.

Linear combinations of outer products are also possible, e.g.:
$c_1|\alpha\rangle\langle\beta| + c_2|\gamma\rangle\langle\delta|$.

For example, the Pauli $Z$ operator: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ can be represented as:

$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

I.e., $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

## Completeness (a.k.a closure) relation

Let $\{|u_1\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$ be an orthonormal basis for $V$.

So any $|v\rangle \in V$ can be expressed as
$|v\rangle = c_1|u_1\rangle + c_2|u_2\rangle + \cdots + c_n|u_n\rangle = \sum_i c_i|u_i\rangle$.

Now consider: $\left(\sum_i |u_i\rangle\langle u_i|\right)|v\rangle = \sum_i |u_i\rangle\langle u_i|v\rangle$.

Note that $\langle u_i|v\rangle$ is just a complex number corresponding to the length of $v$ 'in the direction of' $u_i$. So:

$\sum_i |u_i\rangle\langle u_i|v\rangle = \sum_i c_i|u_i\rangle = |v\rangle$.

Since this is true for any $|v\rangle$, it must be that $\sum_i |u_i\rangle\langle u_i| = I$

This is the completeness relation.

Converting between outer product and matrix representation.

Let $A$ be a linear operator, and apply the completeness relation twice:

$$A = IAI = \left( \sum_i |u_i\rangle\langle u_i| \right) A \left( \sum_j |u_j\rangle\langle u_j| \right) = \sum_{i,j} \langle u_i|A|u_j\rangle |u_i\rangle\langle u_j|.$$

$$A = \begin{bmatrix} \langle u_1|A|u_1\rangle & \dots & \langle u_1|A|u_n\rangle \\ \vdots & \ddots & \vdots \\ \langle u_n|A|u_1\rangle & \dots & \langle u_n|A|u_n\rangle \end{bmatrix}$$

Note that both the outer product and matrix representation are relative to a particular basis.

## Eigenvectors and eigenvalues

$|\psi\rangle$ is an eigenvector of a linear operator $A\ldots$ if applying $A$ to $|\psi\rangle$ only produces a multiple, $a|\psi\rangle$, of $|\psi\rangle, \ldots$ where $a$ is a complex number, called an eigenvalue of $A$.

I.e., whenever $A|\psi\rangle = a|\psi\rangle$, then $|\psi\rangle$ is an eigenvector of $A$ with eigenvalue $a$.

## Hermitian Adjoint (a.k.a Hermitian conjugate)

To compute the Hermitian adjoint of any expression,

- $c \Rightarrow c^*$
- $|a\rangle \Rightarrow \langle a|$
- $\langle a| \Rightarrow |a\rangle$
- order of products of operators/bras/kets is reversed.

E.g.,

$$(cA)^\dagger = c^* A^\dagger$$

$$\left(|\psi\rangle\right)^\dagger = \langle\psi|$$

$$\left(\langle\psi|\right)^\dagger = |\psi\rangle$$

$$(|\psi\rangle\langle\phi|)^\dagger = |\phi\rangle\langle\psi|$$

$$(AB)^\dagger = B^\dagger A^\dagger$$

$$\left(A|\psi\rangle\right)^\dagger = \langle\psi|A^\dagger$$

$$\left(AB|\psi\rangle\right)^\dagger = \langle\psi|B^\dagger A^\dagger$$

Note: $A^\dagger = (|\psi\rangle\langle\phi|)^\dagger = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} = |\phi\rangle\langle\psi|$

## Important types of operators

### Hermitian operator (a.k.a self-adjoint)

$A = A^\dagger$.

Examples: Pauli I, X, Y, Z

### Unitary operator

$AA^\dagger = A^\dagger A = I$

Examples: Pauli I, X, Y, Z

Pauli operators are both unitary and Hermitian (this is not typical!).

Normal operator: $AA^\dagger = A^\dagger A$.

Positive operator:

- Positive semidefinite: $\langle\psi|A|\psi\rangle \geq 0$. (a.k.a. "positive")
- Positive definite: $\langle\psi|A|\psi\rangle > 0$.

## Projection operator

Let $W$ be a k-dimensional subspace of a vector space $V$.

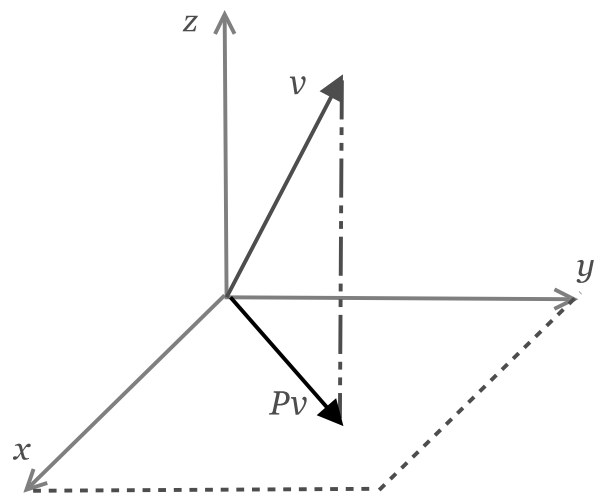
There exists an orthonormal basis $|u_1\rangle \ldots |u_d\rangle$ for $V$ such that $|u_1\rangle \ldots |u_k\rangle$ is an orthonormal basis for $W$.

Define: $P \equiv \sum_{i=1}^{k} |u_i\rangle\langle u_i|$ to be the projector onto $W$.

Properties:

Hermitian: $P = P^\dagger$

Idempotent: $PP = P^2 = P$



## Some important relationships

Positive operators are Hermitian.

Projection operators are Hermitian.

Hermitian operators are normal.

Spectral decomposition theorem: normal operators are always diagonalisable (Nielsen & Chuang, p. 72)

I.e., a normal operator $A$ acting on a vector space $V$ can always be decomposed into:

$$A = \sum_i \lambda_i |u_i\rangle\langle u_i|,$$

where the $\{|u_i\rangle\}$, which form an orthonormal basis for $V$, are eigenvectors of $A$ with eigenvalues $\lambda_i$.

## The commutator

In matrix arithmetic $AB \neq BA$ in general.

The commutator between two operators $A$ and $B$ is defined as:

$[A, B] \equiv AB - BA.$

When $[A, B] = 0$, the operators commute; i.e., when $[A, B] = 0$, $AB = BA$.

Note that:

$[A, B + C] = [A, B] + [A, C],$
$[A, BC] = [A, B]C + B[A, C].$

## Tensor product – Combining vector spaces

The tensor product $V \otimes W$ between two vector spaces $V$ and $W$ combines them into one larger vector space.

Dimensionality of the larger space is the product of the individual dimensionalities; i.e.: $d_V \cdot d_W$.

We also refer to products of elements of $V$ and $W$ as 'tensor products': $|v\rangle \otimes |w\rangle$ (where $|v\rangle \in V$ and $|w\rangle \in W$).

The elements of of the space $V \otimes W$ are just all linear combinations of these 'element tensor products'.
E.g., $\alpha|v_1\rangle \otimes |w_1\rangle + \beta|v_2\rangle \otimes |w_2\rangle$

An orthonormal basis for the space $V \otimes W$ is given by taking the tensor products of each of the elements of the orthonormal bases of $V$ and $W$.

E.g., let $V = W = \mathbb{C}^2$, then an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ is:

$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$.

Basic properties of the tensor product of vectors in $V$ and $W$

- $c\big(|v\rangle \otimes |w\rangle\big) = \big(c|v\rangle\big) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$.
- $\big(|v_1\rangle + |v_2\rangle\big) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$.
- $|v\rangle \otimes \big(|w_1\rangle + |w_2\rangle\big) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$.
- $|v\rangle \otimes |w\rangle = |w\rangle \otimes |v\rangle$

(i.e., behaves sort of like multiplication).

Inner products on tensor product spaces

Let $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle, \quad |\phi\rangle = |\gamma\rangle \otimes |\delta\rangle$.

Then $\langle\psi|\phi\rangle = \big(\langle\alpha| \otimes \langle\beta|\big)\big(|\gamma\rangle \otimes |\delta\rangle\big) = \langle\alpha|\gamma\rangle\langle\beta|\delta\rangle$.

## Linear operators on $V \otimes W$

Let $|v\rangle \in V$, $|w\rangle \in W$ and let $A$ be a linear operator on $V$ and $B$ be a linear operator on $W$.

Then the linear operator $A \otimes B$ on the vector space $V \otimes W$ is defined as:

$$\big(A \otimes B\big)\big(|v\rangle \otimes |w\rangle\big) \equiv A|v\rangle \otimes B|w\rangle.$$

In general:

$$\big(A \otimes B\big)\Big(\sum_i a_i|v_i\rangle \otimes |w_i\rangle\Big) \equiv \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$$

E.g.,

$$\big(A \otimes B\big)\big(|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle\big) = A|v_1\rangle \otimes B|w_1\rangle + A|v_2\rangle \otimes B|w_2\rangle.$$

Note: if $A$ and $B$ are Hermitian, then so is $A \otimes B$, and similarly if $A$ and $B$ are unitary, then so is $A \otimes B$.

## Tensor product of two matrices

Recall: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Example: $X \otimes Y = \begin{bmatrix} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$

Two vector matrices:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

In general: if $A$ is an $m \times n$ matrix and $B$ is $p \times q$, then $A \otimes B$ has $m \times p$ rows and $n \times q$ columns.

## Shorthand notation for tensor products

- $|\alpha\beta\rangle \equiv |\alpha\rangle|\beta\rangle \equiv |\alpha\rangle \otimes |\beta\rangle$.
- $|\alpha\rangle^{\otimes n} \equiv |\alpha\rangle^{n} \equiv |\alpha\rangle_1 \otimes |\alpha\rangle_2 \otimes ... \otimes |\alpha\rangle_n \equiv |\alpha^n\rangle$
- $A^{\otimes n} \equiv A_1 \otimes A_2 \otimes ... \otimes A_n$
- $A_1 B_2 \equiv A \otimes B$.

Note:

$$\begin{aligned} A_1 B_2 |\psi\rangle|\phi\rangle &\equiv (A \otimes B)(|\psi\rangle \otimes |\phi\rangle) \\ &\not\equiv \\ AB|\psi\rangle|\phi\rangle &\equiv (AB \otimes I)(|\psi\rangle \otimes |\phi\rangle) \end{aligned}$$

## Quantum mechanics: States and state spaces

State space, $\mathcal{H}_S$, of a system $S$: complex vector space with inner product (i.e., a "Hilbert space").

- (Note: in QIT we usually only require Hilbert spaces of finite-dimension).

The state of $S$ is completely described by a unit vector $|\psi\rangle \in \mathcal{H}_S$, called the system's "state vector".

Qubits

- Two-dimensional quantum system (live in $\mathbb{C}^2$).
- General expression in the computational basis: $|\psi\rangle = a|0\rangle + b|1\rangle$.

## Quantum mechanics: State evolution

A closed system $S$ evolves unitarily through time; i.e.:

$$|\psi^{t_1}\rangle = U|\psi^{t_0}\rangle.$$

E.g., Hadamard operator: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

## Quantum mechanics: Measurement

$\{M_m\}$: a set of measurement operators which describe a particular measurement.

Each $M_m$ describes a particular measurement outcome.

Probability of a outcome $m$ given by: $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$.

The $M_m$ satisfy the completeness relation: $\sum_m M_m^\dagger M_m = I$.

So: $\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1$.

State of the system after measurement: $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$.

## Quantum mechanics: Measurement (cont'd)

Projection operators

$$P \equiv \sum_{m=1}^{k} |u_m\rangle\langle u_m| = \sum_{m} P_m$$

is the projector onto the k-dimensional subspace $\mathcal{H}_P$ of $\mathcal{H}_S$.

Since $|u_m\rangle$ are orthogonal $\Rightarrow$ can be used to describe mutually exclusive measurement possibilities; e.g., "spin up" vs. "spin down".

Properties

Hermitian: $P = P^\dagger$
Idempotent: $PP = P^2 = P$

Completeness relation for **projectors:**

$\sum_m P_m^\dagger P_m = \sum_m P_m P_m = \sum_{\mathbf{m}} \mathbf{P_m} = \mathbf{I}.$

## Quantum mechanics: Measurement (cont'd)

E.g., qubit: $a|0\rangle + b|1\rangle$.

Complete set of projectors: $\{P_0 = |0\rangle\langle 0|,\ P_1 = |1\rangle\langle 1|\}$.

The probability of getting result $m$ is given by:

$$p(m) = \langle\psi|P_m^\dagger P_m|\psi\rangle = \langle\psi|P_m^2|\psi\rangle = \langle\psi|P_m|\psi\rangle.$$

E.g.,:

$$\begin{aligned} p(0) &= \big(a^*\langle 0| + b^*\langle 1|\big)\big(|0\rangle\langle 0|\big)\big(a|0\rangle + b|1\rangle\big) \\ &= a^*\langle 0|\big(a|0\rangle + b|1\rangle\big) \\ &= a^*a = |a|^2 \\ &\text{(Born rule).} \end{aligned}$$

$|a|^2 = a^*a$: "modulus squared".

If $a = i/\sqrt{2}$, $\quad |a|^2 = (-i/\sqrt{2})(i/\sqrt{2}) = 1/2$.

## Quantum mechanics: Measurement (cont'd)

"Measure in the basis $|m\rangle$": Perform the projective measurement $\{P_m\} = \{|m\rangle\langle m|\}$.

"Measure in the computational basis": Perform the projective measurement $\{P_m\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$.

etc.

## Quantum mechanics: Measurement (cont'd)

POVM measurements.

Recall: Probability of measurement outcome $m$ given by: $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$, with: $\sum_m M_m^\dagger M_m = I$.

Each $(M_m^\dagger M_m)$ is a positive operator (i.e., $\langle\psi|(M_m^\dagger M_m)|\psi\rangle \geq 0$.)

For any arbitrary set of positive operators $\{E_m\}$, one can always re-express these in the form $\{M_m^\dagger M_m\}$.

Positive Operator Valued Measure (POVM): any set of positive operators $\{E_m\}$ for which $\sum_m E_m = I$.

## Quantum mechanics: Composite systems

The state space associated with $n$ systems $S_1, S_2, \ldots, S_n$ is the tensor product: $\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2} \otimes \cdots \otimes \mathcal{H}_{S_n}$.

Similarly, the combined state of $S_1, S_2, \ldots, S_n$ is $|s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_n\rangle$.

## Consequences: Entanglement

One possible state of $S_1, S_2$:

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

This is a "separable state"; i.e., re-expressible as the "product state":

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

Another possible state of $S_1, S_2$:

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

One of the "Bell states" (the "singlet" state)

Not a product state!

- An entangled state.

Recall: a maximally specific description of $S$'s state is given by specifying a unit vector $|\psi\rangle \in \mathcal{H}_S$, (the state vector for the system).

$|\psi\rangle$: a "pure" state.

Alternative representation of a pure state: $\rho = |\psi\rangle\langle\psi|$.

- Called the density operator.
- Useful for representing mixed states.

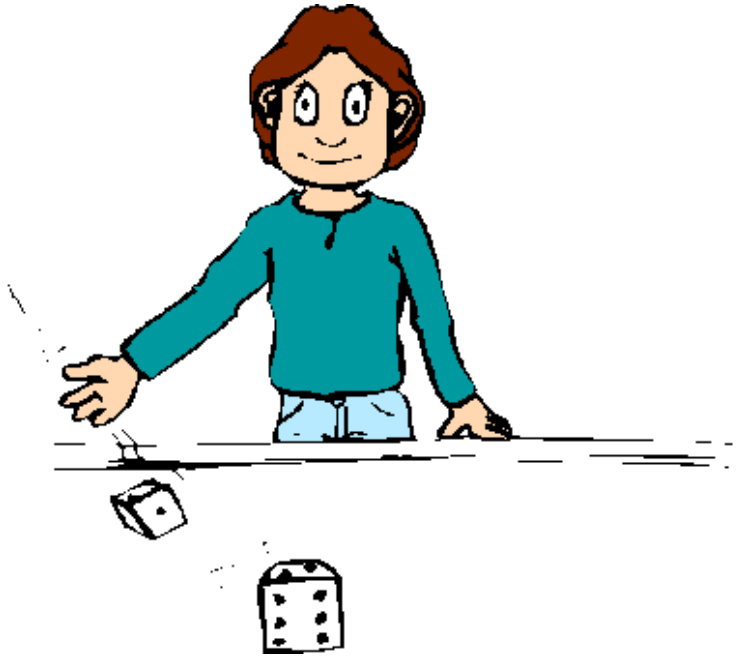
Properties of the density operator:

- $\rho$ is positive.
- has unit trace (i.e., $\mathrm{tr}(\rho) = 1$).

Trace of an operator/matrix: $\mathrm{tr}(A) \equiv \sum_i A_{ii}$

E.g., $\mathrm{tr}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = a + e + i.$

# Mixed states



$$\rho = p|\psi_1\rangle\langle\psi_1| + (1-p)|\psi_2\rangle\langle\psi_2|$$

$$\rho = p\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (1-p)\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} l & m \\ n & o \end{pmatrix}$$

$$= q\begin{pmatrix} p & q \\ r & s \end{pmatrix} + (1-q)\begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

Recall: a maximally specific description of $S$'s state is given by specifying a unit vector $|\psi\rangle \in \mathcal{H}_S$, (the state vector for the system).

$|\psi\rangle$: a "pure" state.

Alternative representation of a pure state: $\rho = |\psi\rangle\langle\psi|$.

- Called the density operator.
- Useful for representing mixed states.

Properties of the density operator:

- $\rho$ is positive.
- has unit trace (i.e., $\mathrm{tr}(\rho) = 1$).

Trace of an operator/matrix: $\mathrm{tr}(A) \equiv \sum_i A_{ii}$

E.g., $\mathrm{tr}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = a + e + i.$

Recall: positve operators (since they are normal) are subject to the spectral decomposition theorem.

$\rho$ is positive. So it is decomposable into $\rho = \sum_i \lambda_i |u_i\rangle|u_i\rangle$ (where $\{|u_i\rangle\}$ are orthogonal eigenvectors of $\rho$ with eigenvalues $\lambda_i$).

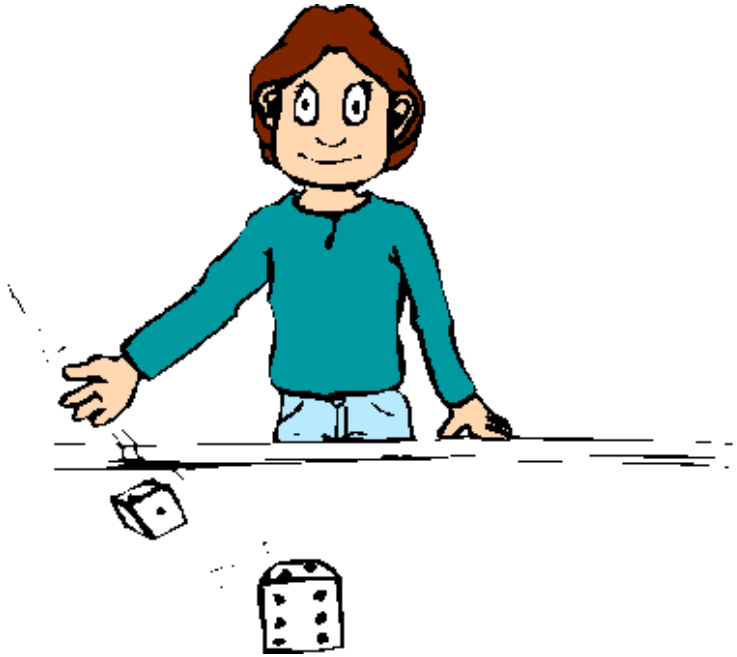
$$\text{I.e., } \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Since $\rho$ has unit trace, it follows that $\sum_i \lambda_i = 1$.

So we can use $\rho$ to describe the case in which $S$ is in the state $|u_i\rangle$ with probability $\lambda_i$.

But beware taking this too literally ...

# Mixed states



$$\rho = p|\psi_1\rangle\langle\psi_1| + (1-p)|\psi_2\rangle\langle\psi_2|$$

$$\rho = p\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (1-p)\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} l & m \\ n & o \end{pmatrix}$$

$$= q\begin{pmatrix} p & q \\ r & s \end{pmatrix} + (1-q)\begin{pmatrix} t & u \\ v & w \end{pmatrix}$$

## Unitary evolution of a density operator

Recall: a closed system $S$ evolves unitarily through time; i.e.: $|\psi'\rangle = U|\psi\rangle$.

Note: $|\psi'\rangle\langle\psi'| = U|\psi\rangle\langle\psi|U^\dagger$.

In general: $\rho' = U\rho U^\dagger$.

## Measurement in the density operator formalism

Recall: probability of a outcome $m$ given by:
$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$.

Note that: $\langle\psi|A|\psi\rangle = \mathrm{tr}(A|\psi\rangle\langle\psi|)$ (Nielsen & Chuang, p. 76).

So: $p(m) = \mathrm{tr}\big(M_m^\dagger M_m|\psi\rangle\langle\psi|\big)$

Consider:
$\rho = p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2| + \ldots p_n|\psi_n\rangle\langle\psi_n| = \sum_i p_i|\psi_i\rangle\langle\psi_i|$

$\Rightarrow p(m|i) = \mathrm{tr}\big(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|\big)$

$\Rightarrow p(m) = \sum_i p_i \mathrm{tr}\big(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|\big) = \mathrm{tr}\big(M_m^\dagger M_m \rho\big)$

State of $\rho$ after measurement (Nielsen & Chuang, p. 102:)

$$\rho' = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\big(M_m^\dagger M_m \rho\big)}$$

## Composite states in the density operator formalism

$$\rho_{ABC} = \rho_A \otimes \rho_B \otimes \rho_C.$$

## When is a state pure/mixed?

$$\begin{aligned} \text{Pure:} \quad & \mathrm{tr}(\rho^2) = 1. \\ \text{Mixed:} \quad & \mathrm{tr}(\rho^2) < 1. \end{aligned}$$

## Reduced density operator

Let $S, R$ be two systems in the joint state $\rho_{SR}$.

To find the state of $S$ alone, we "trace out", i.e. take the partial trace over $R$:

$$\rho_S = \mathrm{tr}_R(\rho_{SR}) = \sum_i \langle r_i|\rho_{SR}|r_i\rangle,$$

where $|r_i\rangle$ is an orthonormal basis for $\mathcal{H}_R$.

E.g., let $\rho_{AB} = |\Psi^-\rangle\langle\Psi^-|$.
Then:

$$\rho_B = \mathrm{tr}_A(\rho_{AB}) = \frac{|0_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|}{2} = \tfrac{1}{2}I.$$

I.e., $B$ is in the completely mixed state.

## Entropy

Recall (from last time):

$H(X) \equiv -\sum_x p_x \log(p_x)$ (Shannon entropy).

Quantifies the information gained when one comes to know the value of a random variable. (equivalently, the uncertainty associated with a random variable).

E.g., information source transmits sequences of 0s and 1s.
Probability that the next digit is 0 and 1: $p_0 = 1/3$, $p_1 = 2/3$.

$$H(X) = -(1/3 \times \log 1/3 + 2/3 \times \log 2/3) = 0.92.$$

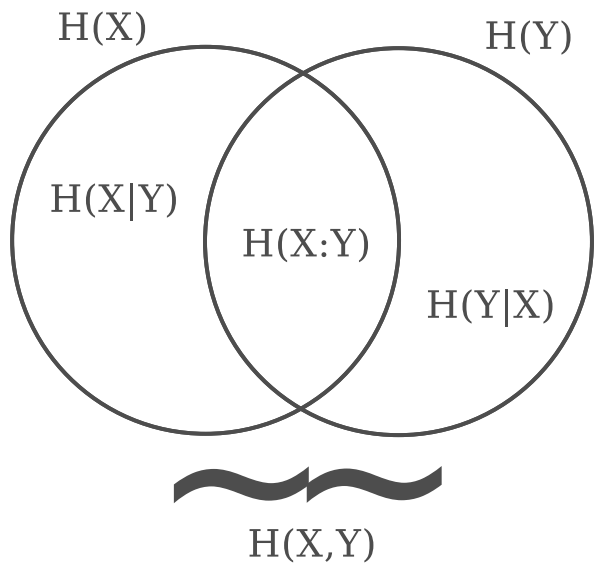
Fundamental properties:

$\mathrm{H}(\mathrm{X}) = 0$ when we are completely certain of the result.

- Intuitively: we gain no new information from any received token.

$\mathrm{H}(\mathrm{X})$ is maximum when all outcomes are equally probable.

- Intuitively: information gained on average from the tokens received is greatest.



## von Neumann entropy

$$\begin{aligned} S(\rho) &= -\mathrm{tr}(\rho \log \rho) \\ &= -\sum_i \lambda_i \log \lambda_i. \end{aligned}$$

Fundamental properties:

$S(\rho) = 0$ when $\rho$ is a pure state.

- We are completely certain of the result of a measurement.

$S(\rho)$ is maximum when $\rho$ is in the completely mixed state $I/d$ ($d$: dimension of $\mathcal{H}_S$).

- Completely uncertain what pure state the system will be in upon measuring it.

Recall: positve operators (since they are normal) are subject to the spectral decomposition theorem.

$\rho$ is positive. So it is decomposable into $\rho = \sum_i \lambda_i |u_i\rangle|u_i\rangle$ (where $\{|u_i\rangle\}$ are orthogonal eigenvectors of $\rho$ with eigenvalues $\lambda_i$).

$$\text{I.e., } \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Since $\rho$ has unit trace, it follows that $\sum_i \lambda_i = 1$.

So we can use $\rho$ to describe the case in which $S$ is in the state $|u_i\rangle$ with probability $\lambda_i$.

But beware taking this too literally ...

## von Neumann entropy

$$\begin{aligned} S(\rho) &= -\mathrm{tr}(\rho \log \rho) \\ &= -\sum_i \lambda_i \log \lambda_i. \end{aligned}$$

Fundamental properties:

$S(\rho) = 0$ when $\rho$ is a pure state.

- We are completely certain of the result of a measurement.

$S(\rho)$ is maximum when $\rho$ is in the completely mixed state $I/d$ ($d$: dimension of $\mathcal{H}_S$).

- Completely uncertain what pure state the system will be in upon measuring it.

## Disanalogies between von Neumann and Shannon Entropy

Shannon: $H(X) \leq H(X,Y)$

von Neumann: $S(A) \not\leq S(A,B)$.

Classically, we are at least as uncertain about the combined state of two random variables as we are about the state of any one of them.

Quantum mechanics:

Consider: $|\Psi^-\rangle = \frac{|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle}{\sqrt{2}}$.

- This state is pure $\Rightarrow$ maximally specified.
- So: $S(A,B) = 0$
- Joint measurement is certain to yield a 1 and a 0.

But $\rho_B = \mathrm{tr}_A(\rho_{AB}) = \frac{|0_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|}{2} = \frac{1}{2}I$.

I.e., B is in the completely mixed state $\Rightarrow S(B)$ is maximum!

Maximally entangled states:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Not all states are maximally entangled. E.g.,

$$|\phi\rangle = \sqrt{\frac{1}{3}}|01\rangle + \sqrt{\frac{2}{3}}|10\rangle$$

is entangled but not maximally entangled.

Entanglement can be useful for information processing.

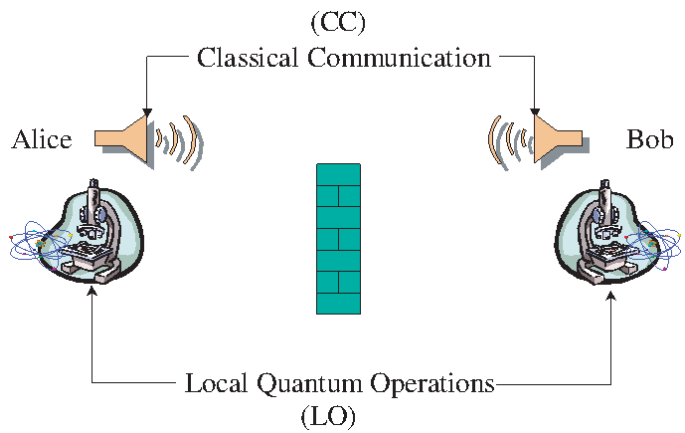
E.g., the "teleportation" protocol is more or less reliable depending on how much entanglement is present.

How to quantify? Theory of entanglement measures.

## Local operations and classical communication (LOCC)

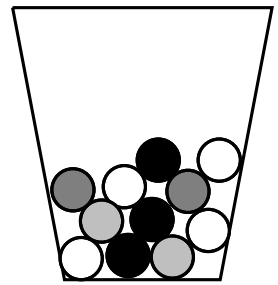
LOCC = local operations performable at sites $A$ and $B$, possibly coordinated using classical communication.

- LO on $A$ include: measurements on $A$, unitaries applied to $A$, etc.
- CC can include: telephone, laser pulse, message in a bottle, etc.




(Courtesy of: Plenio & Virmani, "An introduction to entanglement measures" (2007))

## Using LOCC to prepare a separable state:



- Probability that a ball of type $i$ is drawn is $p_i$.
- Alice chooses a ball from the urn and communicates the result to Bob, Cindy, and Dennis (in distant labs).
- Each of Alice, Bob, Cindy, and Dennis, possesses a list of which (pure) state to prepare given the drawing of a ball of type $i$.
  - Note: these lists may differ!
- Everyone forgets which ball was drawn.
- Result: $\rho^{ABCD} = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C \otimes \rho_i^D$ is prepared.

$$\rho^{ABCD\ldots} = \sum_i p_i \rho_i^A \otimes \rho_i^B \otimes \rho_i^C \otimes \rho_i^D \otimes \ldots$$

is the general form of a separable state.

- So every separable state can be generated using LOCC alone.

Correlations generable using LOCC alone are always factorisable (conditional on the classical communication).

- So a state is separable iff it can be generated using LOCC alone.

Maximally entangled states: If $|\psi\rangle$ is a maximally entangled state of $n$ qubits, it can be used to prepare (with certainty) any other $n$-qubit state.

In general, $\rho$ is more entangled than $\sigma$ if the transformation $\rho \rightarrow \sigma$ can be performed using only LOCC operations.

- Can be used to impose an ordering on entangled states.
- Any measure of entanglement should respect this ordering.

Bipartite (i.e., $n = 2$) pure-state case:

Maximally entangled states: $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$

Measure of entanglement: Entropy of entanglement:

$$\begin{aligned} E(|\psi_{AB}\rangle\langle\psi_{AB}|) &\equiv S(A) = S(B) \\ &\equiv S(\mathrm{tr}_B|\psi\rangle\langle\psi|) = S(\mathrm{tr}_A|\psi\rangle\langle\psi|), \end{aligned}$$

E.g., for $|\phi\rangle = \sqrt{\frac{1}{3}}|01\rangle + \sqrt{\frac{2}{3}}|10\rangle, \quad E(|\phi\rangle\langle\phi|) = 0.92.$

Compare with $E(|\Phi^+\rangle\langle\Phi^+|) = 1$

Gives a unique total ordering of entangled states.

Bipartite **mixed** state case

Entropy of entanglement is ambiguous in this case (b/c of non-unique decomposability of mixed states).

Finding a good entanglement measure is more difficult. Measures which satisfy all desiderata are hard to calculate. Other measures don't always generate the same orderings, etc.

Multipartite case

Don't even have an unambiguous notion of a maximally entangled state in this case.

Natual candidate:

$$|\mathrm{GHZ}\rangle = 1/\sqrt{2}\,(|000\rangle + |111\rangle)$$

Cannot generate using only LOCC:

$$|W\rangle = 1/\sqrt{3}\,(|001\rangle + |010\rangle + |100\rangle)$$

But we soldier on ...