Postulates of Quantum Mechanics I

Postulate 1 (state space): Associated to any *isolated* system is a complex vector space (i.e. Hilbert space) called the *state space*. The system is completely described by its *state vector*, which is a *unit vector* in the state space.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, |-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix},$$

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

BRICS

Postulates of Quantum Mechanics II

Postulate 2 (composite systems): The state space of a composite system is the *tensor product* of the components. If we have n systems $|\psi_1\rangle, \ldots, |\psi_n\rangle$ then the joint state is

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle.$$

The tensor product is the following operation on vectors,

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_m \\ \vdots \\ a_n b_m \end{pmatrix}.$$

BRICS

More States

Let us define a few states in the 4-dimensional Hilbert space $\mathcal{H}_4$:

$$|0+\rangle = |0\rangle \otimes |+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix}.$$

The following is a basis for $\mathcal{H}_4$:

$$\begin{aligned} |\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned}$$

BRICS

A Little More on Bras and Kets

Let $|\phi\rangle$ and $|\psi\rangle$ be two unit vectors then:

- $|\phi\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ then $\langle\phi| = (a_1^*, \ldots, a_n^*)$.
- $\langle\phi|\psi\rangle$ denotes the inner product between $|\phi\rangle$ and $|\psi\rangle$.
- $|\phi\rangle\langle\psi|$ is an operator that maps $|\psi\rangle \mapsto |\phi\rangle$. In general, an arbitrary state $|\lambda\rangle$ (belonging to the same space) is mapped to:

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

- $|\phi\rangle\langle\phi|$ is the projector operator along the state $|\phi\rangle$.

BRICS

Postulates of Quantum Mechanics III

Postulate 3 (evolution): The evolution of a *closed* system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ at time t_1 is related to the state $|\psi'\rangle$ at time t_2 by a unitary transform U,

$$|\psi'\rangle = U|\psi\rangle.$$

NOTE 1: Operator U (square matrix over the complex) is unitary if all columns (and rows) are orthonormal. Such transformation maps a basis into another one:

$$U : |e_i\rangle \mapsto |f_i\rangle,$$

where $\langle e_i|e_j\rangle = \langle f_i|f_j\rangle = \delta_{i,j}$.

NOTE 2: The complex conjuguate $U^\dagger$ for unitary U is always such that $U^\dagger U = \mathbb{I}$.

BRICS

A Little More on Unitary Transforms

When $U : |e_i\rangle \mapsto |f_i\rangle$ then U can be written as

$$U = \sum_i |f_i\rangle\langle e_i|$$

$$U^\dagger = \sum_i |e_i\rangle\langle f_i|$$

We easily see that $U^\dagger$ is the inverse of U:

$$\begin{aligned} UU^\dagger &= (\sum_i |f_i\rangle\langle e_i|)(\sum_j |e_j\rangle\langle f_j|) \\ &= \sum_{i,j} |f_i\rangle\langle e_i|\ |e_j\rangle\langle f_j| \\ &= \sum_i |f_i\rangle\langle f_i| = \mathbb{I}. \end{aligned}$$

BRICS

Complete Set of Unitary Evolutions

Any function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ can be computed by an unitary transform U_f as follows:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

Fact: If f is computable efficiencly by some algorithm then U_f can be implemented perfectly by an efficient quantum circuit.

Thm: *The set of unitary transforms,*

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \text{ and } \texttt{CNOT} = \begin{array}{ccc} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

is universal for quantum computation.

BRICS

Hadamard Transform

The Hadamard transform is extremly important. It works as follows:

$$H : \begin{bmatrix} |0\rangle & \mapsto & |+\rangle \\ |1\rangle & \mapsto & |-\rangle \end{bmatrix} = \begin{bmatrix} |+\rangle & \mapsto & |0\rangle \\ |-\rangle & \mapsto & |1\rangle \end{bmatrix}$$

In general, for $x \in \{0,1\}^n$:

$$H^{\otimes n}|x\rangle = 2^{-n/2} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle.$$

BRICS

More Useful Transformations

$$X = \begin{cases} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{cases}, Z = \begin{cases} |+\rangle & \mapsto & |-\rangle \\ |-\rangle & \mapsto & |+\rangle \end{cases}, Y = \begin{cases} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & -|0\rangle \end{cases},$$

are called:

- X is the **bit flip** operator,
- Z is the **phase flip** operator,
- $Y = XZ$ is the **bit-phase flip** operator.

Notice that the **Hadamard** transform can be written as,

$$H = \frac{1}{\sqrt{2}}(X + Z).$$

This is not surprising since X, Y, Z, and $\mathbb{I}$ form a basis for all 1-qubit operators.

BRICS

Postulates of Quantum Mechanics IV

Postulate 4 (measurement): Quantum measurements are described by a collection $\{M_m\}_m$ of *measurement operators*. These operators act on the *state space* of the system being measured. The index m is the meaurement outcomes. If the state before the mesurement is $|\psi\rangle$ then the probability $p(m)$ to observe outcome m is given by,

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \mathrm{tr}\left(M_m^\dagger M_m|\psi\rangle\langle\psi|\right) \quad \text{and,}$$
$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}.$$

The measurement operators must satisfy the *completeness equation*:

$$\sum_m M_m^\dagger M_m = \mathbb{I}.$$

This ensures that,

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

BRICS

Projective Measurements

A *projective* or *Von Neumann* measurement is defined by operators $\{P_m\}_m$ where

- for all m, P_m is a projection (i.e. $P_m^2 = P_m$),
- $P_m \perp P_{m'}$ for $m \neq m'$,

Equivalently to $\{P_m\}_m$ the *observable* $M = \sum_m mP_m$ describes the measurement (we'll see later why). From **Postulate IV**, when $|\psi\rangle$ is measured:

- $p(m) = \langle\psi|P_m^\dagger P_m|\psi\rangle = \langle\psi|P_m P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle = \||P_m|\psi\rangle\|^2$,
- $|\psi_m\rangle = P_m|\psi\rangle/\sqrt{p(m)}$.

Examples:

- $Z = |0\rangle\langle 0| - |1\rangle\langle 1| \equiv \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$,
  $X = |+\rangle\langle +| - |-\rangle\langle -| \equiv \{|+\rangle\langle +|, |-\rangle\langle -|\}$ are measurements in the "+" and "×" basis respectively.

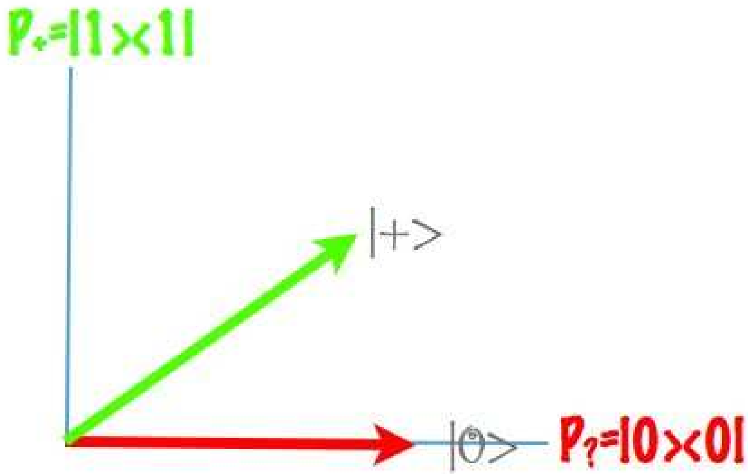
BRICS

Using Projective Measurements

Setting: Suppose a source is sending a qubit in state $|0\rangle$ or $|+\rangle$ each with probability $\frac{1}{2}$.

Problem: Find the best projective measurement that either:

- Identifies the state received perfectly or,
- Outputs "I don't know".



The probability p_{id} to identify the state is $p_{id} = \frac{1}{4}$. This is the best over all projective measurements.

BRICS

POVMs formalism

If one is only interested in the probability distribution for the outcomes of a measurement $\{M_m\}_m$ then,

- $\{E_m\}_m = \{M_m^\dagger M_m\}_m$ is all what is needed,

From **Postulate IV**, we define a POVM (Positive Operator-Valued Measurement) as,

positivity: $\{E_m\}_m$ where E_m's are all positive operators,

completeness: $\sum_m E_m = \mathbb{I}$.

Suppose that $\{E_m = U_m \Sigma U_m^\dagger\}_m$ is a set of positive operators where Σ is diagonal with non-negative elements. Then

$$\{M_m\}_m = \{U_m \sqrt{\Sigma} U_m^\dagger\}_m = \{\sqrt{E_m}\}_m$$

is a set of measurement operators with POVM $\{E_m\}_m$.

BRICS

POVM's in action

Suppose you want to solve the same problem than before. You want to maximize the probability to identify with certainty the state $|0\rangle$ $|+\rangle$. Consider the POVM,

$$
\begin{aligned}
E_{+} &= \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1| \\
E_{0} &= \frac{\sqrt{2}}{1+\sqrt{2}}|-\rangle\langle -| \\
E_{?} &= \mathbb{I} - E_{+} - E_{0}.
\end{aligned}
$$

The POVM $\{E_{+}, E_{0}, E_{?}\}$ satisfies:

- $\langle 0|E_{+}|0\rangle = \frac{\sqrt{2}}{1+\sqrt{2}}\langle 0|1\rangle\langle 1|0\rangle = 0$,
- $\langle +|E_{0}|+\rangle = \frac{\sqrt{2}}{1+\sqrt{2}}\langle +|-\rangle\langle -|+\rangle = 0$,
- $\langle 0|E_{0}|0\rangle = \langle +|E_{+}|+\rangle = \frac{\sqrt{2}}{1+\sqrt{2}}\|\langle +|1\rangle\|^{2} = \frac{1}{\sqrt{2}(1+\sqrt{2})} \approx 0.2929.$

BRICS

Evaluation in Superposition

Suppose U_f satisfies for any $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$:

$$U_f|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle,$$

for some $f : \{0,1\}^n \mapsto \{0,1\}^m$. Then,

$$\begin{aligned} U_f(H^{\otimes n} \otimes \mathbb{I})|0\rangle \otimes |y\rangle &\mapsto 2^{-n/2} \sum_{x \in \{0,1\}^n} U_f|x\rangle|y\rangle \\ &\mapsto 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle|y \oplus f(x)\rangle. \end{aligned}$$

By calling U_f once, one gets $f(x)$ computed for all $z \in \{0,1\}^n$. By measuring each register in the Z basis, one get a random z with its corresponding value $f(z)$.

BRICS

Deutsch-Josza Algorithm

Suppose $f : \{0,1\}^n \rightarrow \{0,1\}$, is garanteed to be either balanced or constant, you must determine which one. How many calls to U_f are required?

The following sequence of transformations allows to answer the question after measuring the first n qubits:

$$(H^{\otimes n} \otimes \mathbb{I}) U_f (H^{\otimes n} \otimes H)|0^n\rangle|1\rangle.$$

One can check this as follows:

$$\begin{aligned}
(H^{\otimes n} \otimes \mathbb{I}) U_f (H^{\otimes n} \otimes H)|0^n\rangle|1\rangle &= (H^{\otimes n} \otimes \mathbb{I})(\sum_x \frac{U_f|x\rangle}{\sqrt{2^n}} \otimes |-\rangle) \\
&= (H^{\otimes n} \otimes \mathbb{I}) \sum_x \frac{|x\rangle}{\sqrt{2^{n+1}}}(|f(x)\rangle - \left|\overline{f(x)}\right\rangle) \\
&= (H^{\otimes n} \otimes \mathbb{I}) 2^{-n/2} \sum_x (-1)^{f(x)}|x\rangle|-\rangle \\
&= \sum_x \sum_z 2^{-n}(-1)^{x \cdot z \oplus f(x)}|z\rangle|-\rangle.
\end{aligned}$$

≣BRICS

Conclusion

After the application fo the algorithm we get:

$$\sum_z \sum_x 2^{-n} (-1)^{x \cdot z \oplus f(x)} |z\rangle |-\rangle.$$

If $f(x)$ is constant then the state is

$$\sum_z (-1)^{f(0)} \left(\sum_x 2^{-n} (-1)^{x \cdot z} \right) |z\rangle |-\rangle$$

If $f(x)$ is balanced then the amplitude associated to $|0\rangle|-\rangle$ is:

$$\sum_x (-1)^{x \cdot 0^n} (-1)^{f(x)} |0\rangle |-\rangle = \sum_x (-1)^{f(x)} |0\rangle |-\rangle = 0 |0\rangle |-\rangle.$$

It follows that if f is balanced then $|0\rangle$ cannot be observed whereas if f is constant then $|0\rangle$ is always observed when the register is measured by $\{|z\rangle\langle z|\}_{z \in \{0,1\}^n}$. Classically, it is easy to verify that $2^{n-1} + 1$ queries are necessary in worst case.

BRICS

Conclusion

After the application fo the algorithm we get:

$$\sum_z \sum_x 2^{-n}(-1)^{x \cdot z \oplus f(x)} |z\rangle |-\rangle.$$

If $f(x)$ is constant then the state is

$$\sum_z (-1)^{f(0)} \left(\sum_x 2^{-n}(-1)^{x \cdot z} \right) |z\rangle |-\rangle = \pm |0\rangle |-\rangle.$$

If $f(x)$ is balanced then the amplitude associated to $|0\rangle|-\rangle$ is:

$$\sum_x (-1)^{x \cdot 0^n}(-1)^{f(x)} |0\rangle |-\rangle = \sum_x (-1)^{f(x)} |0\rangle |-\rangle = 0|0\rangle |-\rangle.$$

It follows that if f is balanced then $|0\rangle$ cannot be observed whereas if f is constant then $|0\rangle$ is always observed when the register is measured by $\{|z\rangle\langle z|\}_{z \in \{0,1\}^n}$. Classically, it is easy to verify that $2^{n-1} + 1$ queries are necessary in worst case.

BRICS

No Cloning

Postulates I-III imply that arbitrary quantum states cannot be cloned. Assume for a contradiction that such a cloning machine U exists. For any $|\psi\rangle$, we have

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

However, for any $|\Psi\rangle$ and $|\Phi\rangle$, unitary transforms preserve the inner product,

$$\langle\Psi|U^\dagger U|\Phi\rangle = \langle\Psi|\Phi\rangle.$$

But our *cloning machine* U satisfies:

$$\langle 0|\langle\psi|\phi\rangle|0\rangle = \langle 0| \otimes \langle\psi|U^\dagger U|\phi\rangle \otimes |0\rangle = \langle\psi| \otimes \langle\psi|\phi\rangle \otimes |\phi\rangle = \langle\psi|\phi\rangle^2,$$

which can only be satisfied for

$$\langle\psi|\phi\rangle = 0 \text{ or } \langle\psi|\phi\rangle = 1.$$

$\Rightarrow$ Such U does not exist!

Ensembles of Quantum States

Let $\{(p_i, |\psi_i\rangle)\}_i$ be an *ensemble of pure states* for $\sum_i p_i = 1$.
The *density operator* or *density matrix* for the system is,

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Unitary evolution U on a state taken from the ensemble gives,

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \overset{U}{\mapsto} \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger.$$

Measurements $\{M_m\}_m$ can be generalized the same way,

$$\begin{aligned} p(m) &= \sum_i p_i p(m \mid i) \\ &= \sum_i p_i \operatorname{tr}\left(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|\right) \\ &= \operatorname{tr}\left(M_m^\dagger M_m \rho\right). \end{aligned}$$

BRICS

Density Operators Represent States

Suppose you have only access to particle B in state,

$$|\Psi\rangle^{AB} = \frac{1}{\sqrt{2}}(|0\rangle^{A} \otimes |0\rangle^{B} + |1\rangle^{A} \otimes |1\rangle^{B}).$$

What do you get?

$$\rho^{B} = \mathrm{tr}_{A}\left(|\Psi\rangle\langle\Psi|\right), |\Psi\rangle\langle\Psi| = \frac{1}{2}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|),$$

called the *partial trace* over A defined as, The partial trace is defined as follows:

$$\mathrm{tr}_{A}\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) = \mathrm{tr}\left(|a_1\rangle\langle a_2|\right)|b_1\rangle\langle b_2| = \langle a_1|a_2\rangle|b_1\rangle\langle b_2|.$$

Which results in,

$$\begin{aligned} \rho^{B} &= \frac{1}{2}(\mathrm{tr}_{A}\left(|00\rangle\langle 00|\right) + \mathrm{tr}_{A}\left(|11\rangle\langle 00|\right) + \mathrm{tr}_{A}\left(|00\rangle\langle 11|\right) + \mathrm{tr}_{A}\left(|11\rangle\langle 11|\right)) \\ &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \mathbb{I}/2 \equiv \{(1/2, |0\rangle), (1/2, |1\rangle)\}. \end{aligned}$$

BRICS

Properties of Density Operators

Theorem: *An operator ρ is the density operator associated to $\{(p_i, |\psi_i\rangle)\}_i$ if and only if*

trace condition: $\mathrm{tr}(\rho) = 1$,

positivity: ρ is a positive operator (An operator is positive if all its eigenvalues are non-negative real numbers) .

The following theorem states the *unitary freedom in the ensemble for density matrices*. We shall write ensembles in a slightly different way:

$$\{(p_i, |\psi_i\rangle)\}_i \equiv \{\sqrt{p_i}|\psi_i\rangle\}_i \equiv \{\left|\tilde{\psi}_i\right\rangle\}_i.$$

Theorem: *The ensembles $\{|\tilde{\psi}_i\rangle\}_i$ and $\{|\tilde{\phi}_i\rangle\}_i$ generate the same density matrix if and only if*

$$\left|\tilde{\psi}_i\right\rangle = \sum_j u_{i,j} \left|\tilde{\phi}_i\right\rangle$$

for some unitary matrix $\{u_{i,j}\}_{i,j}$ (where we pad the smallest ensemble with $\vec{0}$ vector).

BRICS

Unitary Freedom in Action

- Let $\{(1/2, |0\rangle), (1/2, |+\rangle)\} \equiv \{\frac{1}{\sqrt{2}}|0\rangle, \frac{1}{\sqrt{2}}|+\rangle\} \equiv \{|\tilde{0}\rangle, |\tilde{+}\rangle\}$.
- Let $\{(\cos^2\frac{\pi}{8}, |\beta_0\rangle), (\sin^2\frac{\pi}{8}, |\beta_1\rangle)\} \equiv \{\cos\frac{\pi}{8}|\beta_0\rangle, \sin\frac{\pi}{8}|\beta_1\rangle\} \equiv \{|\tilde{\beta}_0\rangle, |\tilde{\beta}_1\rangle\}$ where $\langle\beta_0|\beta_1\rangle = 0$,

$$\begin{aligned} |\beta_0\rangle &= \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle = \cos\frac{\pi}{8}|+\rangle + \sin\frac{\pi}{8}|-\rangle \\ |\beta_1\rangle &= \cos\frac{\pi}{8}|1\rangle - \sin\frac{\pi}{8}|0\rangle = -\cos\frac{\pi}{8}|-\rangle + \sin\frac{\pi}{8}|+\rangle. \end{aligned}$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \Rightarrow \begin{aligned} |\tilde{0}\rangle &= \tfrac{1}{\sqrt{2}}\left(\left|\tilde{\beta}_0\right\rangle - \left|\tilde{\beta}_1\right\rangle\right) \\ |\tilde{+}\rangle &= \tfrac{1}{\sqrt{2}}\left(\left|\tilde{\beta}_0\right\rangle + \left|\tilde{\beta}_1\right\rangle\right). \end{aligned}$$

Not surprising since:

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \cos^2\frac{\pi}{8}|\beta_0\rangle\langle\beta_0| + \sin^2\frac{\pi}{8}|\beta_1\rangle\langle\beta_1|.$$

BRICS