Lecture 5 – Quantum computing basics

Up to this point we've looked at the interference model and seen how interference can be used as a resource for efficient computation

Problem \ # queries	Classical	Interference
Deutsch–Josza	3	1
Bernstein–Vazirani	n	1
Simon	$2^{n/2}$	$O(n)$

But can we achieve interference in practice?

Yes, with quantum operations!

Building off of the linear algebra perspective from Lecture 3, we now move on to quantum computation.

Quantum computation

In the linear algebra way of representing computations, need to specify the following

States : $|\psi\rangle \in H_n$ - complex vectors in Hilbert space

Transformations : $UU^\dagger = U^\dagger U = I$ - unitary matrices

Composition : $\otimes$ tensor product

Measurement / Observation : $\Pr(x) = |\langle x|\psi\rangle|^2$

Born rule.

States

We've seen that memory states can be represented as vectors. This is true for Q.C. as well.

If our memory has size n, state is a 2^n-dimensional vector $|\psi\rangle$. Denote space of such vectors as H_n.

$\dim(\mathcal{H}_n) = 2^n$

$\mathcal{H}_n$ - Hilbert space - complex Euclidean space

$$\boxed{|\psi\rangle = \sum_{i=1}^{2^n} \psi_i |i\rangle}$$

where $\{|i\rangle\}_{i \leq 2^n}$ is a set of basis vectors for $\mathcal{H}_n$.

ψ_i - complex coefficients ($\psi_i \in \mathbb{C}$) or $\boxed{\text{amplitudes}}$

$\mathcal{H}_n$ is endowed with an inner product

$$\langle \cdot , \cdot \rangle : \mathcal{H}_n \times \mathcal{H}_n \to \mathbb{C}$$

- $\langle \psi, \phi \rangle = \langle \phi, \psi \rangle^*$ ← complex conjugation
- $\langle a\psi_1 + b\psi_2, \phi \rangle = a\langle \psi_1, \phi \rangle + b\langle \psi_2, \phi \rangle$
- $\langle \psi, \psi \rangle \geq 0, \ \forall \ \psi \in \mathcal{H}_n$

We will use the bra-ket notation for inner products

$$\langle \psi, \phi \rangle = \langle \psi | \phi \rangle = (\langle \psi |) \cdot (| \phi \rangle)$$

dual space $\to \overline{\mathcal{H}_n}$ $\qquad$ $\mathcal{H}_n$

For a given $|\psi\rangle \in H_n$ we'll think of $\langle\psi|$ as the transposed complex conjugate of $|\psi\rangle$

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_{2^n} \end{pmatrix} \qquad \langle\psi| = \left(\psi_1^* \ \psi_2^* \ \ldots \ \psi_{2^n}^* \right)$$

Memory states of q.c. = quantum states

Represent quantum states with vectors of norm 1

(norm $|\psi\rangle$ is $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$)

$$\langle\psi|\psi\rangle = \|\psi\|^2 = 1$$

We'll also ignore all global phases

$|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are the same state

We'll generally be interested in orthonormal bases (ONB)

$\{|i\rangle\}_{i\leq 2^n}$ is ONB iff. $\langle i|j\rangle = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$

$$\Rightarrow \quad |\psi\rangle = \sum_{i=1}^{2^n} \psi_i \, |i\rangle$$

$$\langle j|\psi\rangle = \sum_{i=1}^{2^n} \psi_i \langle j|i\rangle = \psi_j$$

Fix one particular ONB and label each $|i\rangle$ by its binary representation = $\boxed{\text{computational basis.}}$

$\boxed{\text{E.g.}}$ • The qubit $n=1$

Comp basis = $\{|0\rangle, |1\rangle\}$ $\rightarrow$ $\begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$

Arbitrary qubit $|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$

$\psi_0, \psi_1 \in \mathbb{C}$ $\boxed{\text{Superposition}}$

$$\langle\psi|\psi\rangle = 1 \Rightarrow \underbrace{\left(\psi_0^*\langle 0| + \psi_1^*\langle 1|\right)}_{\langle\psi|}\underbrace{\left(\psi_0|0\rangle + \psi_1|1\rangle\right)}_{|\psi\rangle} = 1$$

$$\psi_0^*\psi_0 \underbrace{\langle 0|0\rangle}_{1} + \psi_0^*\psi_1 \underbrace{\langle 0|1\rangle}_{0} + \psi_1^*\psi_0 \underbrace{\langle 1|0\rangle}_{0} + \psi_1^*\psi_1 \underbrace{\langle 1|1\rangle}_{1} = 1$$

$$\Rightarrow \quad \boxed{|\psi_0|^2 + |\psi_1|^2 = 1}$$

$$\left.\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |-\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{aligned}\right\} \text{ also forms ONB}$$

$$|\psi\rangle = \psi_+ |+\rangle + \psi_- |-\rangle$$

$$\langle +|-\rangle = \langle -|+\rangle = 0 \qquad \langle +|+\rangle = \langle -|-\rangle = 1$$

$$\boxed{|\psi_+|^2 + |\psi_-|^2 = 1}$$

$$\psi_+ = \langle +|\psi\rangle ; \quad \psi_- = \langle -|\psi\rangle$$

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

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

- $\boxed{n = 2}$

Comp. basis $= \{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$

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

$$|\psi_{00}|^2 + |\psi_{01}|^2 + |\psi_{10}|^2 + |\psi_{11}|^2 = 1$$

Transformations

We've seen that transformations are matrices.

- Deterministic – permutation matrices
- Probabilistic – doubly stochastic matrices
- Quantum – unitary matrices

a $2^n \times 2^n$ matrix U is unitary iff.

$$\boxed{U \cdot U^\dagger = U^\dagger \cdot U = I} \rightarrow 2^n \times 2^n \text{ identity matrix}$$

$U^\dagger$ – transpose complex conjugate of U

(note that $\langle\psi| = (|\psi\rangle)^\dagger$ and $|\psi\rangle = (\langle\psi|)^\dagger$)

Set of $2^n \times 2^n$ unitaries denoted U_n (also $U(2^n)$)

Important properties

- $\| |\psi\rangle \| = \| U \cdot |\psi\rangle \|$ (= 1 for unit vectors)

- For any $|\psi\rangle, |\phi\rangle \in H_n$ let

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

$$|\phi'\rangle = U|\phi\rangle$$

Then $\langle\psi'|\phi'\rangle = \langle\psi| \cdot \underbrace{U^\dagger \cdot U}_{I} |\phi\rangle = \langle\psi|\phi\rangle$

- If $\{|i\rangle\}$ is ONB then so if $\{U|i\rangle\}$

- $U(a|\psi\rangle + b|\phi\rangle) = a \cdot U|\psi\rangle + b \cdot U|\phi\rangle$

- columns of a unitary matrix form ONB (in particular they are orthogonal and of norm 1)

$\boxed{\text{E.g.}}$ $n = 1$

Not to be confused with Hilbert space

$\boxed{\text{Hadamard}}$ $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $H^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$

$$H \cdot H^\dagger = H^\dagger \cdot H = H \cdot H = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

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

$$H \cdot |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

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

But $H^\dagger = H$ so $H|+\rangle = |0\rangle$

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

$\boxed{\text{Pauli matrices}}$ $\underline{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad X = X^\dagger$

$$\underline{Y} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad Y = Y^\dagger$$

$$\underline{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Z = Z^\dagger$$

$$X^2 = Y^2 = Z^2 = \underline{I}$$

$X|0\rangle = |1\rangle$; $X|1\rangle = |0\rangle$

(bit flip operation)

$$X|+\rangle = \frac{1}{\sqrt{2}}\Big(X|0\rangle + X|1\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|1\rangle + |0\rangle\Big) = |+\rangle$$

$$X|-\rangle = \frac{1}{\sqrt{2}}\Big(X|0\rangle - X|1\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|1\rangle - |0\rangle\Big) = -|-\rangle$$

same state as $|-\rangle$

$Y|0\rangle = i\cdot|1\rangle$

↳ same state as $|1\rangle$

$Y|1\rangle = -i\cdot|0\rangle$

↳ same state as $|0\rangle$

$$Y\cdot|+\rangle = \frac{1}{\sqrt{2}}\Big(Y|0\rangle + Y|1\rangle\Big) =$$

$$= \frac{1}{\sqrt{2}}\Big(i|1\rangle - i|0\rangle\Big) = i\cdot|-\rangle$$

↳ same state as $|-\rangle$

$$Y|-\rangle = \frac{1}{\sqrt{2}}\Big(Y|0\rangle - Y|1\rangle\Big) = i|+\rangle$$

↳ same state as $|+\rangle$

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

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

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

Some useful relations

$$XZ = iY; \quad ZX = -iY \qquad (XZ = -ZX)$$

(similar relations hold for other products)

$$HXH = Z \qquad HZH = X$$

- $\boxed{n = 2}$

$$\boxed{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$CNOT|00\rangle = |00\rangle \qquad CNOT|10\rangle = |11\rangle$$

$$CNOT|01\rangle = |01\rangle \qquad CNOT|11\rangle = |10\rangle$$

$$CNOT\,|x,y\rangle = |x, x\oplus y\rangle$$

$$(x, y \in \{0,1\})$$

CNOT - controlled NOT (also known as CX)

- flips second qubit controlled on the value of the first

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$CZ\,|00\rangle = |00\rangle$ $\quad$ $CZ\,|10\rangle = |10\rangle$

$CZ\,|01\rangle = |01\rangle$ $\quad$ $CZ\,|11\rangle = -|11\rangle$

$$\boxed{CZ\,|x,y\rangle = (-1)^{x\cdot y}\,|x,y\rangle}$$

- controlled on first qubit apply Z to second.
- operation is symmetric $CZ\,|x,y\rangle = CZ\,|y,x\rangle$

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\boxed{U}} \\ 0 & 0 & & \end{pmatrix}$$

where U is a 2x2 unitary

Controlled on first qubit applies U to second qubit.

Composition

States and transformations compose via tensor product.

$|\psi\rangle \in H_n$, $|\phi\rangle \in H_m$

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle \in H_{n+m}$$

note $\dim(H_{n+m}) = 2^{n+m}$

Similarly $U_1 \in U_n$, $U_2 \in U_m$

$$U_1 \otimes U_2 \in U_{n+m}$$

$\hookrightarrow$ $2^{n+m} \times 2^{n+m}$ unitary

Some properties

- associativity $U_1 \otimes (U_2 \otimes U_3) = (U_1 \otimes U_2) \otimes U_3$

$$|\psi_1\rangle \otimes (|\psi_2\rangle \otimes |\psi_3\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) \otimes |\psi_3\rangle$$

- distributivity with addition

$$U_1 \otimes (a U_2 + b U_3) = a\, U_1 \otimes U_2 + b\, U_1 \otimes U_3$$

$$|\psi_1\rangle \otimes (a|\psi_2\rangle + b|\psi_3\rangle) = a|\psi_1\rangle|\psi_2\rangle + b|\psi_1\rangle|\psi_3\rangle$$

- matrix product of tensor products

$$(U_1 \otimes U_2) \cdot (U_3 \otimes U_4) = (U_1 \cdot U_3) \otimes (U_2 \cdot U_4)$$

$$(U_1 \otimes U_2) \cdot (|\psi_1\rangle \otimes |\psi_2\rangle) = U_1|\psi_1\rangle \otimes U_2|\psi_2\rangle$$

- relation to dagger

$$(U_1 \otimes U_2)^\dagger = U_1^\dagger \otimes U_2^\dagger$$

$$(|\psi_1\rangle \otimes |\psi_2\rangle)^\dagger = \langle\psi_1| \otimes \langle\psi_2|$$

(but note that for ordinary product the relation is different $(U_1 \cdot U_2)^{\dagger} = U_2^{\dagger} \cdot U_1^{\dagger}$)

- generally not commutative

$$U_1 \otimes U_2 \neq U_2 \otimes U_1$$

$$|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle$$

- $\{|i\rangle\}_{i \leq 2^n}$ ONB for H_n and $\{|j\rangle\}_{j \leq 2^m}$ ONB for H_m, then $\{|i\rangle \otimes |j\rangle\}_{\substack{i \leq 2^n \\ j \leq 2^m}}$ is an ONB for H_{n+m} (and so is $\{|j\rangle \otimes |i\rangle\}$ though not necessarily the same basis)

$\boxed{\text{E.g.}}$ $|01\rangle = |0\rangle \otimes |1\rangle$

$$|x\rangle = |x^1\rangle|x^2\rangle \dots |x^n\rangle, \text{ for } x \in \{0,1\}^n$$

$\{|+\rangle, |-\rangle\}$ basis for H_1 so $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ is a basis for H_2

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

$$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$|\psi\rangle^{\otimes n} = \underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \dots \otimes |\psi\rangle}_{n \text{ times}}$$

$$U^{\otimes n} = \underbrace{U \otimes U \otimes \dots \otimes U}_{n \text{ times}}$$

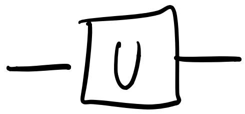
$$H^{\otimes 2} = H \otimes H$$

$$H^{\otimes 2} \cdot |00\rangle = |++\rangle$$

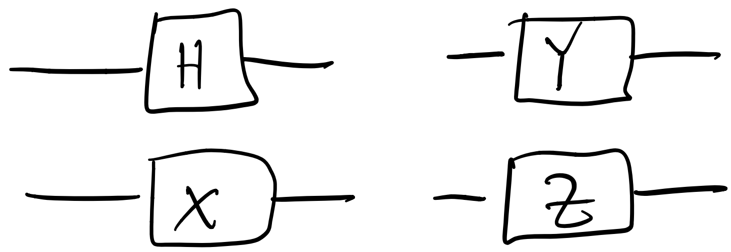
$$H^{\otimes n} \cdot |0^n\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

The circuit picture

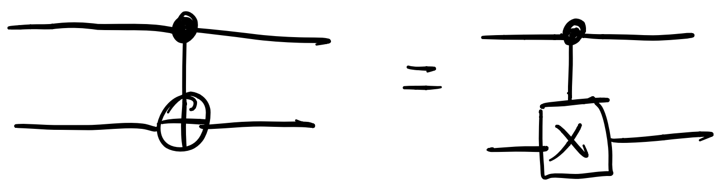
Wires —— qubits

Boxes  unitaries

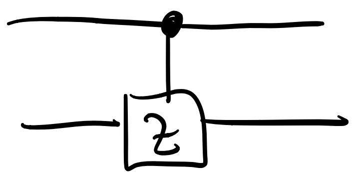
H, X, Y, Z →



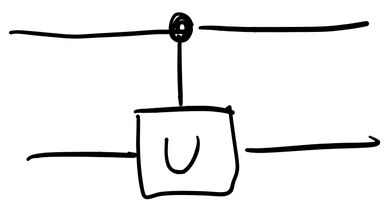
CNOT →



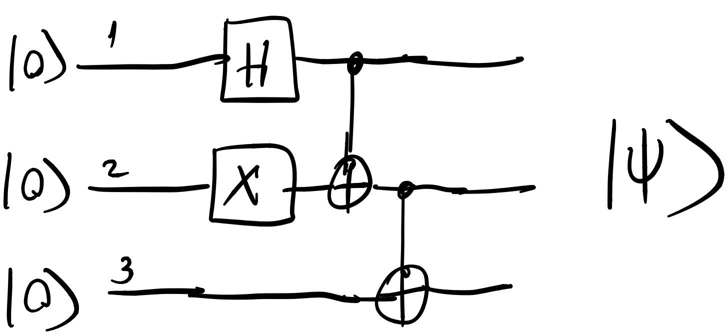
CZ →



CU →



E.g.



$$|\psi\rangle = \left(I \otimes CNOT_{23}\right)\left(CNOT_{12} \otimes I\right)\left(H \otimes X \otimes I\right)|000\rangle_{123}$$

$$H \otimes X \otimes I\,|000\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \cdot |1\rangle \cdot |0\rangle =$$

$$= \frac{1}{\sqrt{2}}\left(|010\rangle_{123} + |110\rangle_{123}\right)$$

Applying $CNOT_{12}$ we get

$$\frac{1}{\sqrt{2}}\, CNOT_{12}\left(|010\rangle_{123} + |110\rangle_{123}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|010\rangle + |100\rangle\right) = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \cdot |0\rangle$$

Applying $CNOT_{23}$ we get

$$\frac{1}{\sqrt{2}}\, CNOT_{23}\left(|010\rangle_{123} + |100\rangle_{123}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|011\rangle + |100\rangle\right)$$

Can we write this as a tensor product of states?

No!

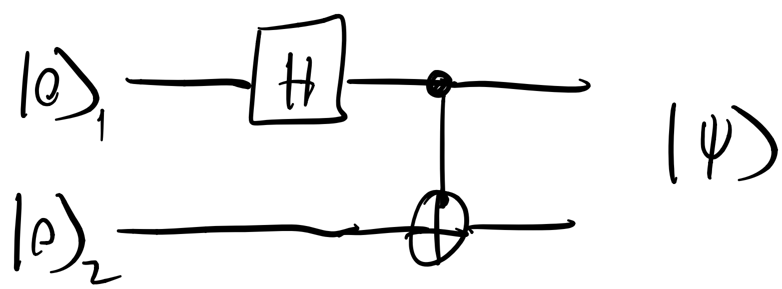
Entanglement.

We say a state $|\psi\rangle \in H_A \otimes H_B$ is **entangled**
if $\nexists$ $|\psi\rangle_A \in H_A$ and $|\psi\rangle_B \in H_B$ s.t.

$$|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$$

E.g. **Bell states**

Consider the circuit



$$|\psi\rangle = CNOT_{12} \cdot (H \otimes I)\,|00\rangle$$

$$= CNOT\ \frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big) = \overbrace{\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)}^{\text{Bell state}}$$

Suppose there existed $|\psi_1\rangle = a|0\rangle + b|1\rangle$

$$|\psi_2\rangle = c|0\rangle + d|1\rangle$$

s.t $|\psi_1\rangle \otimes |\psi_2\rangle = |\psi\rangle$

$$\Rightarrow \Big(a|0\rangle + b|1\rangle\Big)\Big(c|0\rangle + d|1\rangle\Big) =$$

$$= ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle$$

$$= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$

$$\Rightarrow \quad a \cdot c = \frac{1}{\sqrt{2}} \qquad b \cdot d = \frac{1}{\sqrt{2}}$$

$$a \cdot d = 0 \qquad b \cdot c = 0$$

Not possible!

Usually denote $\frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$ as $|\phi^+\rangle$

3 other Bell states

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big)$$

Can be obtained by applying $CNOT \cdot (H \otimes I)$ to $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$\Rightarrow \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ is an ONB

Measurement

As we said, amplitudes translate to probabilities. In the quantum case, the translation is given by the square (of the absolute values) of the amplitudes.

Of course, as we've seen, amplitudes depend on the basis we choose to represent the state in. So

$$\text{ONB } \{|i\rangle\} \rightarrow \text{measurement}$$

$$|\psi\rangle = \sum_i \psi_i |i\rangle$$

if we measure in this basis we get outcome with prob $|\psi_i|^2$

$$\sum_i |\psi_i|^2 = 1$$

$\boxed{\text{E.g.}}$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Measure in computational basis $\{|0\rangle, |1\rangle\}$

We see $|0\rangle$ with prob $|a|^2$

$|1\rangle$ with prob $|b|^2$

Measure in $\{|+\rangle, |-\rangle\}$ basis

We see $|+\rangle$ with prob $|\langle + | \psi\rangle|^2 = |a\langle +|0\rangle + b\langle +|1\rangle|^2$

$$= \left|a \cdot \frac{1}{\sqrt{2}} + b\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}|a+b|^2$$

We see $|-\rangle$ with prob $|\langle - | \psi\rangle|^2 = |a\langle -|0\rangle + b\langle -|1\rangle|^2$

$$= \left|a \cdot \frac{1}{\sqrt{2}} - b\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}|a-b|^2$$

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Measure in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis

Outcome
$|00\rangle$ with prob $|a|^2$
$|01\rangle$ with prob $|b|^2$
$|10\rangle$ with prob $|c|^2$
$|11\rangle$ with prob $|d|^2$

What if we only measure one of the 2 qubits?

Projective measurement (PVM)

To each possible measurement outcome we associate a projector - an operator P (not unitary) satisfying $P^2 = P^\dagger = P$, $P \geq 0$ (P has positive eigenvalues)

Suppose we have a k-outcome measurement $\{P_i\}_{i \leq k}$

Outcome i occurs with prob $\langle\psi| P_i |\psi\rangle$

State after meas is $\dfrac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$

It should also be the case that $\boxed{\sum_i P_i = I}$

(equivalently, $\forall\, |\psi\rangle$, $\sum_i \langle\psi|P_i|\psi\rangle = 1$)

For an ONB $\{|i\rangle\}$, corresponding PVM is given by $\{|i\rangle\langle i|\}$, i.e. $P_i = |i\rangle\langle i|$

Prob of outcome i $\quad \langle\psi|\,|i\rangle\langle i|\,|\psi\rangle = \underbrace{\langle\psi|i\rangle}_{\psi_i^*}\underbrace{\langle i|\psi\rangle}_{\psi_i} = |\psi_i|^2$

State after measurement $\quad \dfrac{|i\rangle\langle i|\psi\rangle}{\sqrt{|\psi_i|^2}} = \dfrac{\psi_i}{|\psi_i|}|i\rangle$

Note: if $\psi_i = 0$ state becomes the 0 vector (not to be confused with $|0\rangle$). In general we'll only consider outcomes for which $\psi_i \neq 0$.

What is the measurement corresponding to measuring one qubit of a 2-qubit state in computational basis?

$P_0 = |0\rangle\langle 0| \otimes I \qquad P_1 = |1\rangle\langle 1| \otimes I$

Note that

$$P_i^{\dagger} = \left(|i\rangle\langle i| \otimes I\right)^{\dagger} = |i\rangle\langle i| \otimes I = P_i$$

$$P_i^2 = \left(|i\rangle\langle i| \otimes I\right) \cdot \left(|i\rangle\langle i| \otimes I\right) =$$

$$= |i\rangle\langle i|i\rangle\langle i| \otimes I = |i\rangle\langle i| \otimes I = P_i$$

$$P_0 + P_1 = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes I =$$

$$= \left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \otimes I = I \otimes I$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot (1\ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot (0\ 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Outcome 0 for first qubit

$$\langle\psi|P_0|\psi\rangle = \langle\psi| \cdot \left(a P_0|00\rangle + b P_0|01\rangle + c P_0|10\rangle + d P_0|11\rangle\right)$$

But now note that $(|0\rangle\langle 0|\otimes I)\,|x\rangle\otimes|y\rangle =$

$$= \underbrace{\langle 0|x\rangle}_{\substack{1 \text{ if } x=0 \\ 0 \text{ if } x=1}} \cdot\ |0\rangle|y\rangle$$

$$\Rightarrow \langle\psi|P_0|\psi\rangle = \langle\psi|\cdot\big(a|00\rangle + b|01\rangle\big) =$$

$$= \big(a^*\langle 00| + b^*\langle 01| + c^*\langle 10| + d^*\langle 11|\big)\big(a|00\rangle + b|01\rangle\big)$$

$$= |a|^2 + |b|^2$$

Similarly prob of 1 is $|c|^2 + |d|^2$

State after 0 outcome is $\dfrac{a|00\rangle + b|01\rangle}{\sqrt{|a|^2 + |b|^2}}$

State after 1 outcome is $\dfrac{c|10\rangle + d|11\rangle}{\sqrt{|c|^2 + |d|^2}}$

Suppose we meas first qubit of $|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{12} + |11\rangle_{12}\right)$ in comp basis.

$\Rightarrow$ with prob $\frac{1}{2}$ state collapses to $|00\rangle_{12}$

with prob $\frac{1}{2}$ state collapses to $|11\rangle_{12}$

What if we measure in $\{|+\rangle, |-\rangle\}$ basis?

$\boxed{\text{Useful trick:}}$ if basis is $\{U|i\rangle\}$, where $\{|i\rangle\}$ is some ONB, then measuring $|\psi\rangle$ in $\{U|i\rangle\}$ is the same as measuring $U^\dagger|\psi\rangle$ in $\{|i\rangle\}$.

So measuring in $\{|+\rangle, |-\rangle\}_1$ is the same as measuring $H\otimes I \cdot |\phi^+\rangle$ in $\{|0\rangle, |1\rangle\}_1$

$$H\otimes I = \frac{1}{\sqrt{2}}\left(|+\rangle|0\rangle + |-\rangle|1\rangle\right) =$$

$$= \frac{1}{2}\left(|00\rangle + |10\rangle + |01\rangle - |11\rangle\right)$$

Outcome 0 (or $|+\rangle$) has prob $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$

Outcome 1 (or $|-\rangle$) has prob $\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$

State after of second qubit is

for 0 outcome : $\frac{1}{\sqrt{2}}\langle 0| \otimes I \cdot \left(|00\rangle + |10\rangle + |01\rangle - |11\rangle \right)$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right)_2 = |+\rangle_2$$

for 1 outcome : $\frac{1}{\sqrt{2}}\langle 1| \otimes I \cdot \left(|00\rangle + |10\rangle + |01\rangle - |11\rangle \right)$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right)_2 = |-\rangle_2$$

So if we measure first qubit in $\{|+\rangle, |-\rangle\}$, state after measurement is

$|++\rangle$ or $|--\rangle$ with equal prob $\frac{1}{2}$

In fact this will happen in any bases we measure!

Perfect correlation accross all bases is a feature of

(maximal) entanglement.

In circuit form, what we did was