

Programming Quantum Computers

Prof. Balwinder Singh Sodhi
Dept of Computer Science and Engineering,
IIT Ropar

Credits/acknowledgement

- Some of the slides have content adapted from following publicly available documents:
 - https://en.wikipedia.org/wiki/Quantum_information_science
 - <https://docs.microsoft.com/en-us/quantum>
 - <https://quantumexperience.ng.bluemix.net/qx/user-guide>
 - <http://pyquil.readthedocs.io/en/latest/>
 - <https://www.quantiki.org>

Why learn quantum programming?

- Technology that promises to solve hard computing problems
 - Quantum supremacy: Speedups over the best known classical algorithms
- Still in its infancy, but quickly evolving
 - **Opportunities for early adopters**
- Quantum programming is a distinct art from classical programming
 - Requires very different tools to understand and express quantum algorithmic thinking

Major player in quantum computing

<https://docs.microsoft.com/en-us/quantum>



<https://quantumexperience.ng.bluemix.net/qx/experience>

rigetti

<https://www.rigetti.com/forest>

<https://www.dwavesys.com/>

D:WAVE
The Quantum Computing Company™

Few prerequisites in maths

- A vector v of dimension n is a collection of n complex numbers (v_1, v_2, \dots, v_n) arranged as a column

$$v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

- Norm of the vector v is: $\sqrt{\sum_i |v_i|^2}$

- A unit vector has norm 1

- Adjoint of vector v is denoted as v^\dagger and is defined as:

*Here * denotes
complex conjugate*

$$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}^\dagger = [v_1^* \quad \dots \quad v_n^*]$$

Vectors

- Two vectors multiply via the inner or dot product
 - **express one vector as a sum of other simpler vectors**
- The inner product between u and v , denoted $\langle u, v \rangle$ is defined as: $\langle u, v \rangle = u^\dagger v = u_1^* v_1 + \dots + u_n^* v_n$.

$$\text{If } u = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \text{ and } v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \text{ then } au + bv = \begin{bmatrix} au_1 + bv_1 \\ au_2 + bv_2 \\ \vdots \\ au_n + bv_n \end{bmatrix}$$

Matrices and tensors


- A matrix of size $m \times n$ is a collection of mn complex numbers arranged in m rows and n columns as shown

below:

- Matrix M of dimension $m \times n$ and

N of dimension $n \times p$ multiply

to give $m \times p$ matrix P : $P_{ik} = \sum_j M_{ij} N_{jk}$


$$M = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ & & \ddots & \\ M_{m1} & M_{m2} & \cdots & M_{mn} \end{bmatrix}$$

$$\begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ & & \ddots & \\ M_{m1} & M_{m2} & \cdots & M_{mn} \end{bmatrix} \begin{bmatrix} N_{11} & N_{12} & \cdots & N_{1p} \\ N_{21} & N_{22} & \cdots & N_{2p} \\ & & \ddots & \\ N_{n1} & N_{n2} & \cdots & N_{np} \end{bmatrix} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1p} \\ P_{21} & P_{22} & \cdots & P_{2p} \\ & & \ddots & \\ P_{m1} & P_{m2} & \cdots & P_{mp} \end{bmatrix}$$

Tensor product

- Tensor product of two matrices $M_{m \times n}$ and $N_{p \times q}$ is a larger matrix $P = M \otimes N$ of size $mp \times nq$, and is obtained from M and N as follows:

$$\begin{aligned}
 M \otimes N &= \begin{bmatrix} M_{11} & \cdots & M_{1n} \\ & \ddots & \\ M_{m1} & \cdots & M_{mn} \end{bmatrix} \otimes \begin{bmatrix} N_{11} & \cdots & N_{1q} \\ & \ddots & \\ N_{p1} & \cdots & N_{pq} \end{bmatrix} \\
 &= \begin{bmatrix} M_{11} \begin{bmatrix} N_{11} & \cdots & N_{1q} \\ & \ddots & \\ N_{p1} & \cdots & N_{pq} \end{bmatrix} & \cdots & M_{1n} \begin{bmatrix} N_{11} & \cdots & N_{1q} \\ & \ddots & \\ N_{p1} & \cdots & N_{pq} \end{bmatrix} \\ & \vdots & \\ M_{m1} \begin{bmatrix} N_{11} & \cdots & N_{1q} \\ & \ddots & \\ N_{p1} & \cdots & N_{pq} \end{bmatrix} & \cdots & M_{mn} \begin{bmatrix} N_{11} & \cdots & N_{1q} \\ & \ddots & \\ N_{p1} & \cdots & N_{pq} \end{bmatrix} \end{bmatrix}
 \end{aligned}$$

Tensor product examples

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \\ e \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} c \\ d \\ e \end{bmatrix} \\ b \begin{bmatrix} c \\ d \\ e \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ ae \\ bc \\ bd \\ be \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} e & f \\ g & h \end{bmatrix} & b \begin{bmatrix} e & f \\ g & h \end{bmatrix} \\ c \begin{bmatrix} e & f \\ g & h \end{bmatrix} & d \begin{bmatrix} e & f \\ g & h \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{bmatrix}$$

A convention about notation

For a vector v or matrix M , $v^{\otimes n}$ or $M^{\otimes n}$ is shorthand for an n -fold repeated tensor product

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{\otimes 1} &= \begin{bmatrix} 1 \\ 0 \end{bmatrix}, & \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{\otimes 2} &= \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, & \begin{bmatrix} 1 \\ -1 \end{bmatrix}^{\otimes 2} &= \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}, \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes 1} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes 2} &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

Eigenvalues and Eigenvectors

- Let \mathbf{M} be a square matrix and \mathbf{v} be a vector that is not having all entries equal to 0.
- We say \mathbf{v} is an eigenvector of \mathbf{M} if:
 - $\mathbf{M}\mathbf{v} = c\mathbf{v}$ for some number c
- In that case, c is the eigenvalue corresponding to the eigenvector \mathbf{v} .
- In general a matrix \mathbf{M} may transform a vector into any other vector, but an eigenvector is special because it is left unchanged except for being multiplied by a number.

Unitary matrix

A complex square matrix U is unitary if its conjugate transpose U^* is also its inverse.

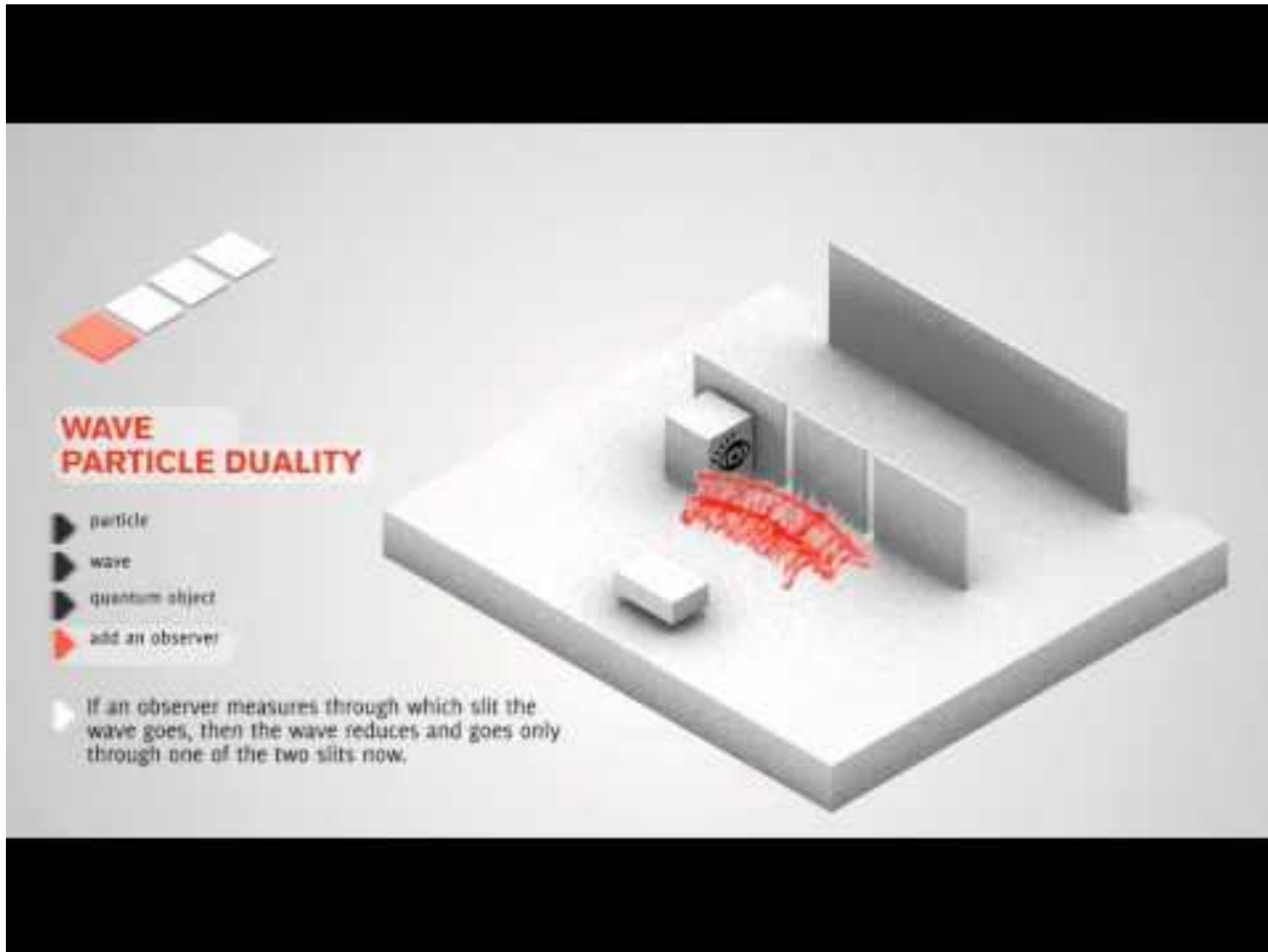
That is, if:

$$U^*U = UU^* = I, U^*U = UU^* = I,$$

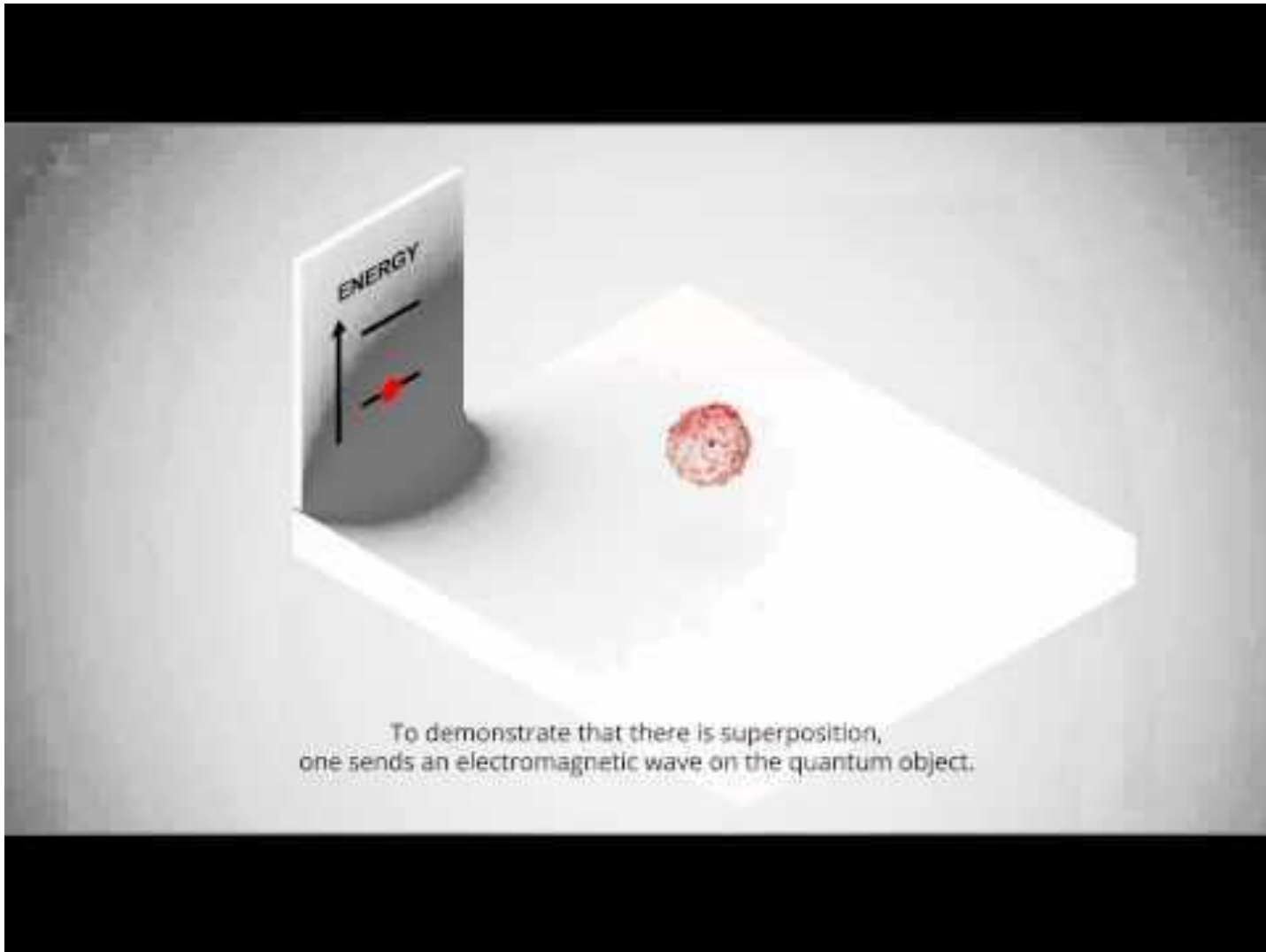
where I is the identity matrix

- Given two complex vectors x and y , multiplication by U preserves their inner product; that is, $\langle Ux, Uy \rangle = \langle x, y \rangle$.

Wave-particle-quantum



Quantum superposition



Classical bits

- Bits (0 and 1) are fundamental objects of information on classical computer
- At any given time
 - A single bit can be either 0 or 1
 - N bits taken together can be in only one of 2^N states
- Classical CPU processes information using basic digital circuits:
 - Logic gates such as AND, OR, NOT, NAND etc.
 - Flip-flops or latches for storing information

Qubits and their basis states

- A qubit or quantum bit or qbit is the fundamental object of information on a quantum computer
- One qubit can represent following values:
 - One of the two *basis states* (Something corresponding to one classical bit i.e. 1 or 0)
 - A quantum superposition of the two basis states
- The two states in which a qubit may be measured are known as basis states (or basis vectors)

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



“Ket 0”



“Ket 1”

Dirac or
“Bra-Ket”
notation

Qubit system

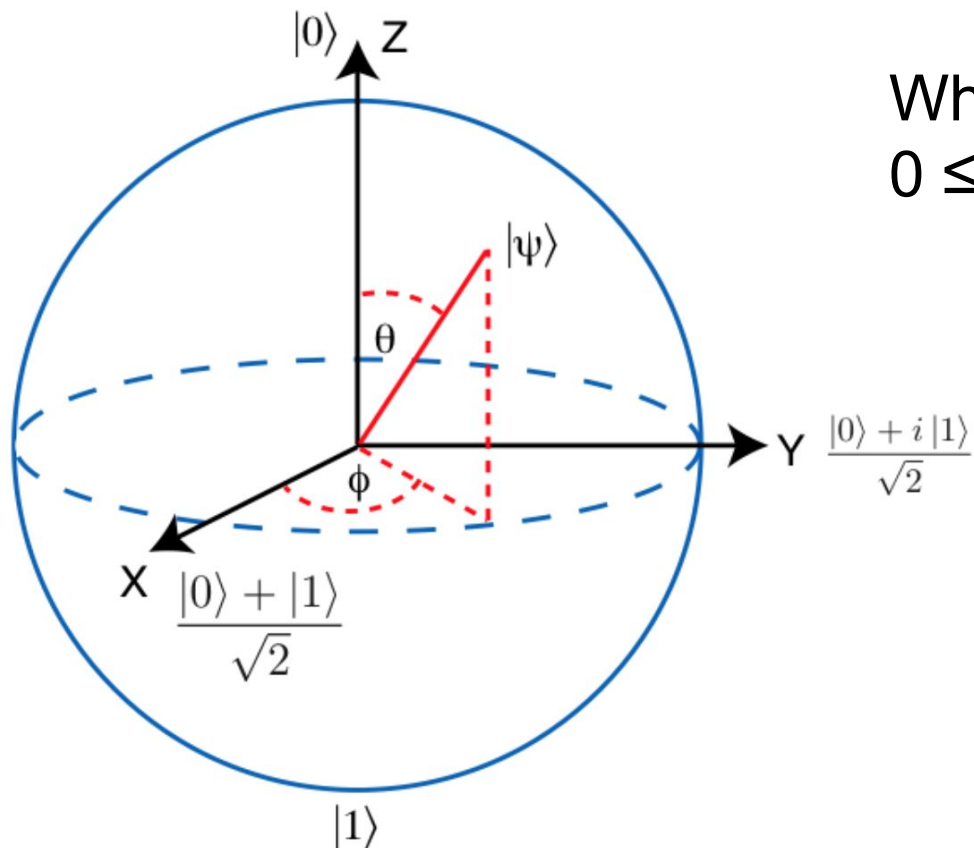
- It is a two-dimensional complex vector space, and
- State of a qubit is a complex vector in that space
- A pure qubit can be represented as a *superposition* (i.e. linear combination) of basis states $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ such that } |\alpha|^2 + |\beta|^2 = 1$$

- $|\beta|^2$ is the probability of finding the qubit in $|1\rangle$
- $|\alpha|^2$ is the probability of finding the qubit in $|0\rangle$
- Any two-dimensional column vector of real or complex numbers with norm 1 represents a possible quantum state held by a qubit

Representation of qubit vectors

$$\begin{aligned} |\psi\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \\ &= \cos\left(\frac{\theta}{2}\right)|0\rangle + (\cos\phi + i\sin\phi)\sin\left(\frac{\theta}{2}\right)|1\rangle \end{aligned}$$



Where, $0 \leq \theta \leq \pi$
 $0 \leq \phi \leq 2\pi$

Examples of valid qubit superposition

$$\underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{\text{Basis states}}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}, \text{ and } \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$$

Basis states

- Any quantum state vector can be written as a sum of these basis vectors

$$\begin{bmatrix} x \\ y \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Two basis quantum states correspond to classical bits 0 and 1, normally as:

$$0 \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad 1 \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Operations on qubit states

$$\Psi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

- “Measuring” the state of a qubit
 - “Collapses” the qubit to one of the classical states
 - Measuring a qubit ψ gives 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$, s.t $|\alpha|^2 + |\beta|^2 = 1$
- “Transforming” a qubit state by applying quantum gate
 - Quantum gates can emulate any rotation of the quantum state vector
 - Mathematically speaking, the qubit undergoes a unitary transformation
 - Unitary transformation preserves the inner product of two vectors

Quantum gates

- Mathematically, are matrices with two properties
 - Operations that they represent are reversible
 - When applied to a state vector on the Bloch sphere, the resulting vector is also on the Bloch sphere
- Matrices that satisfy these two properties are called unitary matrices
- Applying a gate to a quantum state is the same as multiplying a vector by one of these matrices

Multi-qubits states

- Qubit base states can also be combined
 - **2 qubits have the following base states**

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \text{ and } |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

- Basis for two-qubit states is formed by the tensor products of one-qubit states

$$\begin{aligned} 00 &\equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, & 01 &\equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \\ 10 &\equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, & 11 &\equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \end{aligned}$$

Entangled states

- Not all two-qubit quantum states can be written as the tensor product of two single-qubit states
 - E.g. there are no states ψ and ϕ such that their tensor product is the state $\psi \otimes \phi$ as expressed below:

$$\psi \otimes \phi = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$$

- Such two qubits are said to be *entangled*

Entanglement implications

- The information that an entangled 2 qubit state holds is not confined to either of the qubits individually
- Rather, the information is stored non-locally in the correlations between the states of two qubits
- This non-locality of information is one of the major distinguishing features of quantum computing

Related interesting reading:

- https://en.wikipedia.org/wiki/Bell_state
- https://en.wikipedia.org/wiki/EPR_paradox

Simple description of entanglement

“two systems that appear too far apart to influence each other can nevertheless behave in ways that, though individually random, are too strongly correlated to be described by any classical local theory”

Example of entangled state

- Bell state, denoted as: $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$
 - Subscript A means qubit held by Alice and B held by Bob
- Qubit held by Alice can be 0 as well as 1
- If Alice measured her qubit in the standard basis
 - the outcome would be perfectly random
 - either possibility $|0\rangle$ and $|1\rangle$ having probability $\frac{1}{2}$
- Now if Bob measured his qubit, due to entanglement of qubits, outcome will be same as Alice's
- So, individually Alice and Bob see random outcomes but seen together outcomes are correlated

Quantum logic gates

- Represented by unitary matrices
- Operate on spaces of one or two qubits
 - Just like classical logic gates operate on one or two bits
- Can be described by $2^n \times 2^n$ sized unitary matrices, where n is the number of qubits that the gate act on
- Act upon variables that are vectors of 2^n complex dimensions
 - n is the number of qubits of the variable
 - Measurement outcomes are the base vectors, and a quantum state is a linear combination of these outcomes

Quantum logic gates

- The number of qubits in the input and output of the gate have to be equal
- To find the action of a gate on a specific quantum state:
 - Multiply the vector which represents the state by the matrix representing the gate

Grover's algorithm

- Typically described as “database/list search” algorithm
 - Finds an item in a given list/database
- If we have a function $y = f(x)$ that can be evaluated on a quantum computer, Grover's algorithm allows us to calculate x when given y
- Finds with high probability the unique input to a function that produces a given output value
 - Uses just $O(\sqrt{N})$ evaluations of the function, where N is the size of the function's domain
- It was devised by Lov Grover in 1996.

Algorithm outline

1. Choose suitable encoding of list for representing it in qubits
2. Initialize the qubits to a uniform superposition $|s\rangle$ over all qubit states
3. Perform the following "Grover iteration" $r(N)$ times. The function $r(N)$ is $O(N^{1/2})$
 - a. Apply the operator U_f (Described shortly)
 - b. Apply the operator U_s
4. Perform the measurement on qubits state

Providing input list to the quantum computer

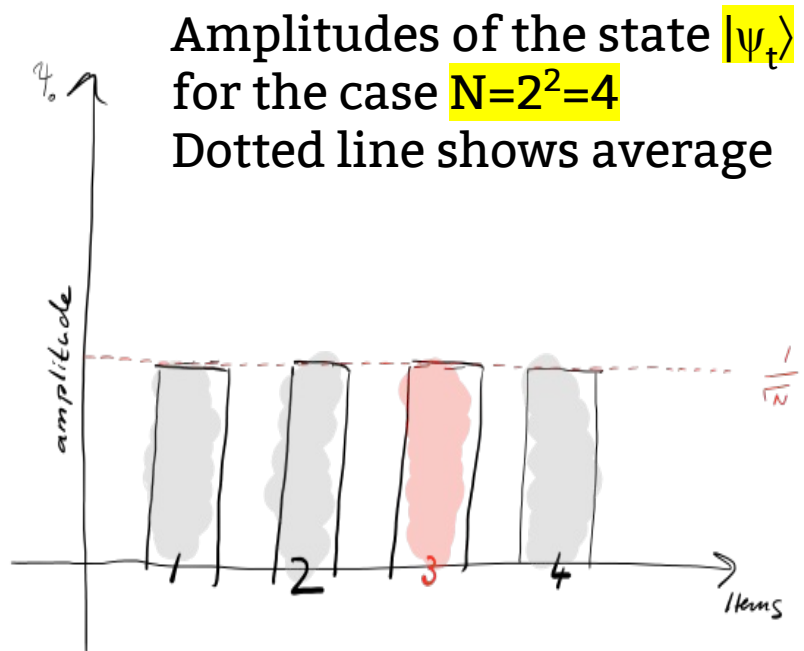
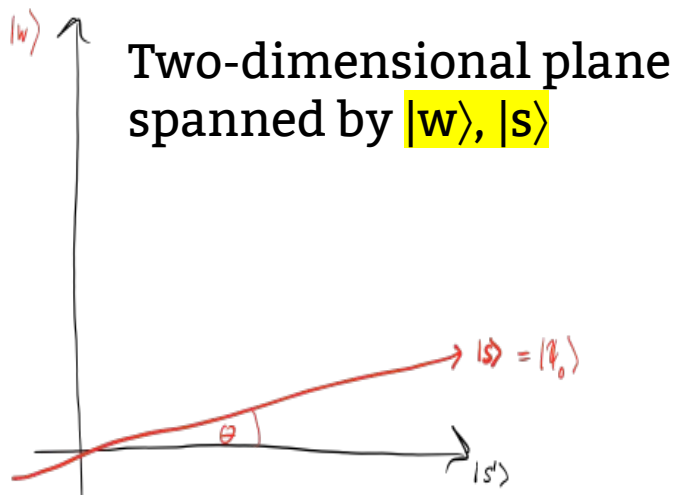
- Consider an unsorted list with N entries.
- Encode the list in terms of a function f such that:
 - $f(x)=1$ for the searched item and 0 for the rest
- Choose a binary encoding of items $x, w \in \{0,1\}^n$ s.t $N=2^n$
 - Can be represented by $n = \log_2 N$ qubits.
- Define the oracle matrix U_f to act on any of the simple, standard basis states $|x\rangle$ by $U_f|x\rangle = (-1)^{f(x)}|x\rangle$
 - It maps $U_f|w\rangle$ to $-|w\rangle$
 - A reflection about origin for the marked item in an $N=2^n$ dimensional vector space.

Amplitude amplification

- Initially, location of target item w is unknown
 - Any guess of its location is as good as any other
 - Can be expressed in terms of a quantum state called a *uniform superposition*: $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
- Chances of guessing the right value w is 1 in 2^n
- On average we need to try $\sim N=2^n$ times to guess the correct item
- Amplitude amplification trick is used to enhance this probability

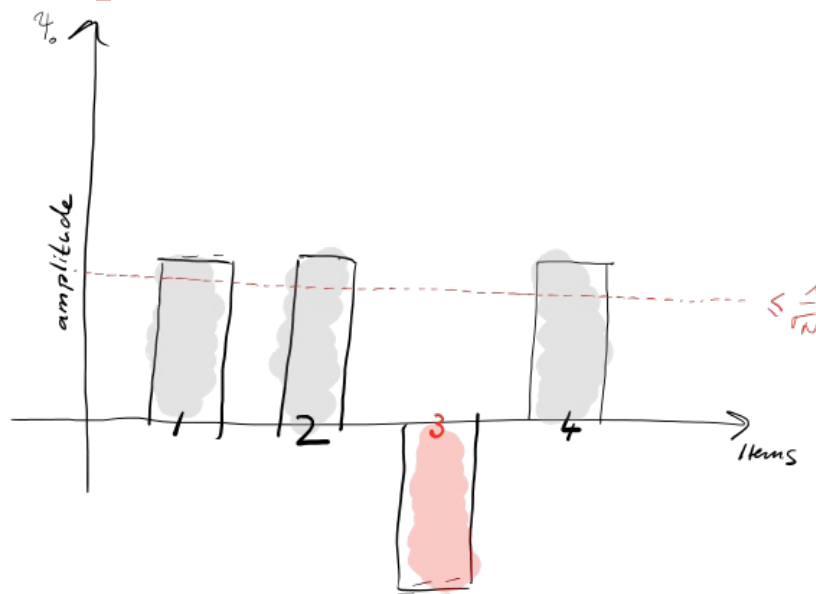
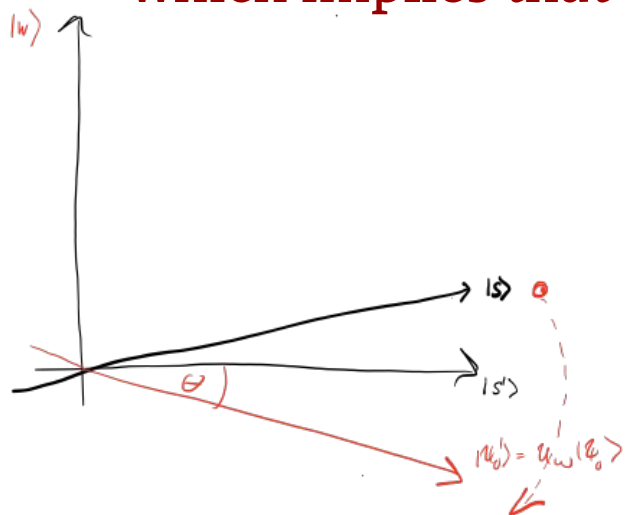
STEP-1 :: Initialize system state

- At $t=0$ the initial state is $|\psi_0\rangle = |s\rangle$
 - $|s\rangle$ is uniform superposition state made from $|s\rangle = H^{\otimes n}|0\rangle^n$



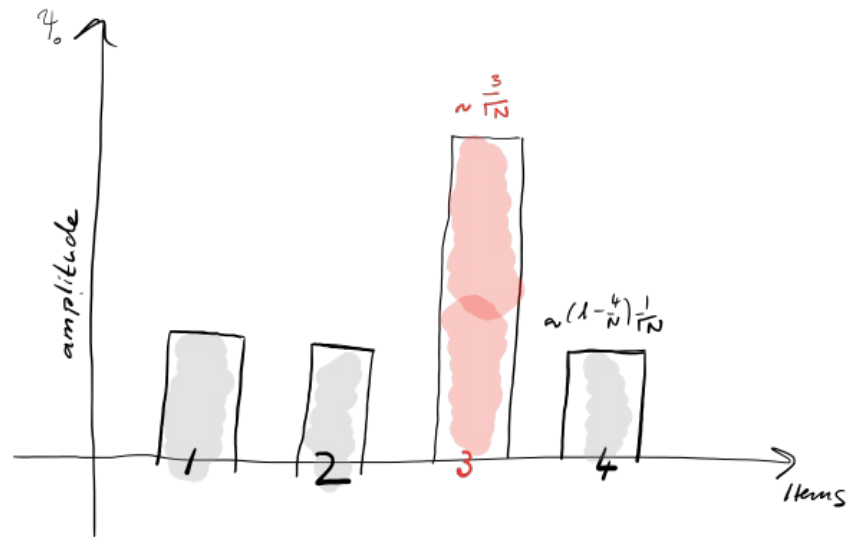
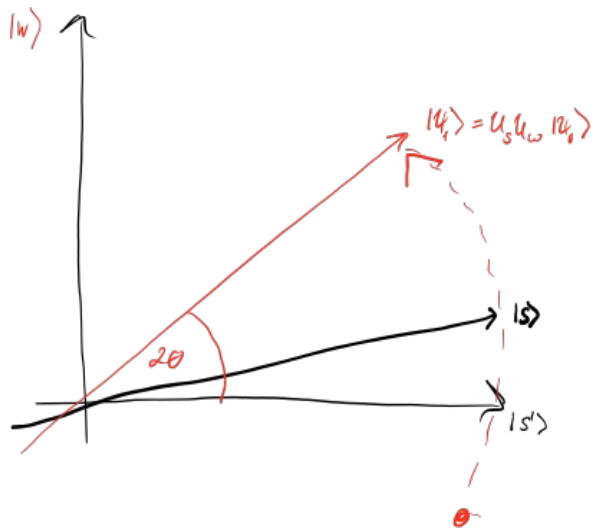
STEP 2 :: Grover iteration step-a

- Apply the oracle reflection U_f to the state $|\psi_t\rangle$ giving
 $|\psi_{t'}\rangle = U_f|\psi_t\rangle$
- Corresponds to a reflection of the state $|\psi_t\rangle$ about $-|w\rangle$
 - It means that amplitude in front of $|w\rangle$ becomes negative, which implies that average amplitude has been lowered



STEP 2 :: Grover iteration step-b

- Apply an additional reflection U_s about the state $|s\rangle$ where $U_s = 2|s\rangle\langle s| - \mathbb{1}$



STEP 2 :: Grover iteration step-b

- This transformation maps the state to $U_s|\psi_t\rangle$ and completes the transformation $|\psi_{t+1}\rangle = U_s U_f |\psi_t\rangle$
- Transformation $U_s U_f$ rotates the initial state $|s\rangle$ closer towards the winner $|w\rangle$
 - Reflection $U_s \Rightarrow$ A reflection about the average amplitude
- Boosts the negative amplitude of $|w\rangle$ to roughly 3x its original value
 - Because average amplitude was lowered by 1st reflection

STEP 2 :: Grover iteration step-b

- After t steps the state will have transformed to:

$$|\psi_t\rangle = (U_s U_f)^t |\psi_0\rangle$$

- Amplitude of $|w\rangle$ grows linearly with the number of applications $\sim tN^{-1/2}$
- Thus roughly $N^{1/2}$ rotations suffice