

Quantum computing

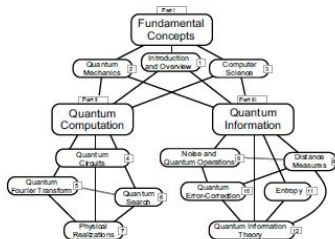
Abhik

CST Dept, IEST Shibpur

21. Januar 2025

- 1 Fundamental concepts
 - Basic notations of linear algebra
 - Basic concepts of quantum mechanics
 - Basic concepts of qubits and gates
 - Important quantum concepts
 - Some quantum algorithms
 - Quantum communication

What we intend to cover



Bases

- Consider $|v_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|v_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- Then $|v\rangle = a_1 |v_1\rangle + a_2 |v_2\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$
- Then $|v_1\rangle$ and $|v_2\rangle$ span the vector space C^2 .
- Similarly, $|v_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $|v_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$ also spans C^2 .
- In this case, $|v\rangle = \frac{a_1+a_2}{\sqrt{2}} |v_1\rangle + \frac{a_1-a_2}{\sqrt{2}} |v_2\rangle$ represents the linear combination.

Linear independence

- Linearly dependent when $a_1 |v_1\rangle + a_2 |v_2\rangle + \dots + a_n |v_n\rangle = 0$ with at least for one $i, a_i \neq 0$ and a_1, a_2, \dots, a_n are complex.
- The set of linearly independent vectors that span the vector space contains same number of elements.
- Such set is called the basis, always exists.
- Number of elements in the basis is called the dimension.

Linear operators and matrices

- Take a function $A : V \rightarrow W$.
- Note $A(\sum_i a_i |v_i\rangle) = \sum_i a_i A(|v_i\rangle) = A|v\rangle$
- Identity operator $I_v |v\rangle = v$ for all vectors v
- Zero operator $0 |v\rangle = 0$.
- Composition like $(BA)(|v\rangle) = B(A(|v\rangle))$

Inner product

- Inner product of two vectors denoted as $(|v\rangle, |w\rangle)$ or use notation $\langle v | w \rangle$
- C_n has inner product defined by

$$((y_1, \dots, y_n), (z_1, \dots, z_n)) = \sum_i y_i^* z_i = [y_1^* \dots y_n^*] \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

- Linear in second argument $(|v\rangle, \sum_i \lambda_i |w_i\rangle) = \sum_i \lambda_i (|v\rangle, |w_i\rangle)$
- Also $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$
- $(|v\rangle, |v\rangle) \geq 0$ with equality only for zero vector.
- Dual of the vector $|v\rangle$ will be denoted as $\langle v|$.
- The inner product space is called Hilbert space.

Orthogonality and norm

- Two vectors are orthogonal if Inner product of the two vectors is zero ($|v\rangle, |w\rangle$)
- For ($|v\rangle = (0, 1), |w\rangle = (1, 0)$) the inner product is zero.
- The norm of vector $\| |v\rangle \|$ is expressed as $\sqrt{\langle v | v \rangle}$ For unit vector, norm is one.
- When $\| |v\rangle \| = 1$ the vector is normalized in the form $\frac{|v\rangle}{\| |v\rangle \|}$
- Set $|i\rangle$ of vectors is orthonormal if each vector is unit vector and distinct vectors in the set are orthogonal i.e. $\langle i | j \rangle = \delta_{ij}$

Hilbert space and outer product

- Consider $|w\rangle = \sum_i w_i |i\rangle$ and $|v\rangle = \sum_j v_j |j\rangle$ as vectors represented in their orthonormal basis.
- Since $\langle i | j \rangle = \delta_{ij}$, we have

$$\langle v | w \rangle = \sum_i v_i \langle i | \sum_j w_j | j \rangle = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i$$
- In other words, $\langle v | w \rangle = [v_1^* \dots v_n^*][w_1 \dots w_n]^T$
- This further implies that dual $\langle v |$ of $|v\rangle$ is row vector of complex conjugates.
- Outer product representation $|w\rangle \langle v|$ is an operator $(|w\rangle \langle v|)(|v'\rangle) = |w\rangle \langle v | v' \rangle = \langle v | v' \rangle |w\rangle$ which converts the said operation to a known multiplication.

Completeness relation

- Consider $|i\rangle$ as vectors represented in any orthonormal basis for V .
- Hence there is some $|v\rangle = \sum_i v_i |i\rangle$ for a set of complex numbers v_i .
- Since $\langle i | v \rangle = v_i$, hence

$$(\sum_i \langle i | |i\rangle) |v\rangle = \sum_i |i\rangle \langle i | v \rangle = \sum_i v_i |i\rangle = |v\rangle$$
- Therefore, we have $\sum_i |i\rangle \langle i| = I$ which is called the completeness relation.
- Suppose $A : V \rightarrow W$ we have

$$A = I_W A I_V = \sum_{ij} |w_j\rangle \langle w_j| A |v_i\rangle \langle v_i| = \sum \langle w_j| A |v_i\rangle |w_j\rangle \langle v_i|$$
- Then elements of A matrix are $\langle w_j| A |v_i\rangle$ where input basis is column, output basis is row.

Cauchy Schwartz inequality

- Suppose $A : V \rightarrow W$ we have

$$A = I_W A I_V = \sum_{ij} |w_j\rangle \langle w_j| A |v_i\rangle \langle v_i| = \sum \langle w_j| A |v_i\rangle |w_j\rangle \langle v_i|$$
- Then elements of A matrix are $\langle w_j| A |v_i\rangle$ where input basis is column, output basis is row.
- For two vectors $|v\rangle, |w\rangle$ the $|\langle v | w \rangle|^2 \leq \langle v | v \rangle \langle w | w \rangle$ with equality when $|v\rangle = Z |w\rangle$ or $|w\rangle = Z |v\rangle$ i.e. linearly related vectors.

Adjoint and Hermitian

- A is any linear operation on Hilbert space.
- Then $(|v\rangle, A|w\rangle) = (A^\dagger |v\rangle, |w\rangle)$
- So $(AB)^\dagger = A^\dagger B^\dagger$
- By convention, $|v\rangle^\dagger = \langle v|$ Hence $(A|v\rangle)^\dagger = \langle v| A^\dagger$
- It can be shown that $(|w\rangle \langle v|)^\dagger = |v\rangle \langle w|$ and $(A^\dagger)^\dagger = A$
- In matrix terms, $A^\dagger = (A^*)^T$ first conjugate then transpose.
- Example: $\begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}^\dagger = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix}$
- When $A^\dagger = A$ matrix is Hermitian.

Projector onto subspace

- Take $P = \sum_{i=1}^k |i\rangle \langle i|$
- Since $|v\rangle \langle v|$ is Hermitian for any $|v\rangle$ $P^\dagger = P$ (Hermitian)
- Orthogonal complement of P is $Q = I - P$.
- Here Q is the projector onto the vector space $|k+1\rangle, \dots, |d\rangle$ the orthogonal complement of the orthonormal basis $|1\rangle, \dots, |k\rangle$
- When $A^\dagger A = A A^\dagger$ operator is normal, Hermitian is also normal.

Unitary matrix properties

- Unitary operator is normal since $U^\dagger U = I = UU^\dagger$
- Hence U has a spectral decomposition, which implies U can be diagonalized.
- Unitary operators preserve inner products between vectors.

$$(U|v\rangle, U|w\rangle) = \langle v| U^\dagger U |w\rangle = \langle v| I |w\rangle = \langle v | w \rangle$$
- Hence U can have outer product representation. Define $|w_i\rangle = U|v_i\rangle$ so if $|v_i\rangle$ is orthonormal basis set, so is $|w_i\rangle$. Then $U = \sum_i |w_i\rangle \langle v_i|$
 This implies that the outer product is unitary.
- Eigenvalues of U has modulus 1 hence of the form $e^{i\theta}$.
- Pauli matrices are Hermitian and unitary.

Positive operator

- Special class of Hermitian operator.
- Operator A for $(|v\rangle, A|v\rangle)$ is real non negative number.
- A is positive definite when $(|v\rangle, A|v\rangle) > 0$ for all $|v\rangle \neq 0$
- Any positive operator is Hermitian and by spectral decomposition has diagonal representation $\sum_i \lambda_i |i\rangle \langle i|$ with non negative eigenvalues λ_i

Tensor product

- Way to form large vector spaces

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

- Several important operator functions may be defined.
- square root of positive operator, logarithm of positive definite operator, exponential of normal operator

Trace of matrix

- Trace is sum of diagonal elements. $tr(A) = \sum_i A_{ii}$
- Then we have $tr(UAU^\dagger) = tr(U^\dagger UA) = tr(A)$
- For linearity $tr(A|\psi\rangle\langle\psi|) = \sum_i \langle i|A|\psi\rangle\langle\psi|i\rangle = \langle\psi|A|\psi\rangle$

Commutator and anti commutator

- $[A, B] = AB - BA$ Then if $[A, B] = 0$ implies $AB = BA$ then A commutes with B .
- Similarly $A, B = AB + BA$ and if $A, B = 0$ then A anti-commutes B .
- Example:

$$[X, Y] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} - \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = 2i \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = 2iZ$$

- Hence X, Y does not commute, no common eigenvectors.
- A, B are simultaneously diagonalizable iff $[A, B] = 0$
- For other Pauli matrices, $[Y, Z] = 2iX$ and $[Z, X] = 2iY$.

Polar and singular value decomposition

- A is any linear operation on vector space V .
- Then we have some U along with positive operators J, K such that $A = UJ$ (left polar) $= KU$ (right polar decomposition where $J = \sqrt{A^\dagger A}$ and $K = \sqrt{AA^\dagger}$
- If A is invertible, U is unique.

Postulates of quantum mechanics - state space

- Associated to any isolated physical system is a complex vector space with inner product (i.e. Hilbert space) known as state space of the system.
- The system is completely described by its state vector which is a unit vector in the system's state space.
- For the arbitrary state vector $|\psi\rangle = a|0\rangle + b|1\rangle$ to be unit vector we require the inner product $\langle\psi|\psi\rangle = 1$ which is equivalent to the condition $|a|^2 + |b|^2 = 1$. This is known as the normalization condition.
- Any linear combination $\sum_i \alpha_i |\psi_i\rangle$ is a superposition of the states $|\psi_i\rangle$ with amplitudes α_i .

Postulates of quantum mechanics - evolution

- Evolution of the state space of a system is described by a unitary transformation.
- For the arbitrary state vector $|\psi\rangle$ at time t_1 relates with $|\psi'\rangle$ at time t_2 by the unitary operator U so that $|\psi'\rangle = U|\psi\rangle$
- In case of single qubits any U can be realized realistically!
- Pauli X (Quantum NOT), Pauli Z (phase flip), Hadamard gates are all such transformations.
- Continuous time evolution is based on differential equations, not discrete t_1, t_2 . Like $i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$ describes Schrödinger equation. Here H is Hamiltonian of the closed system.

Postulates of quantum mechanics - measurement

- Quantum measurements can be described in terms of collection $\{M_m\}$ of measurement operators. These operators act on the state space of the system being measured.
- Here m is the count on measurement outcomes. Result occurs with probability $p_m = \langle \psi | M_m^\dagger M_m | \psi \rangle$
- State of the system after measurement will be $\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$
- Here completeness equation $\sum_m M_m^\dagger M_m = I$
- This implies $\sum_m p_m = 1 = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle$

Qubit measurement

- Take $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$
- These are Hermitian $M_0^2 = M_0$ and $M_1^2 = M_1$
- Hence completeness gives $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$
- Now suppose $|\psi\rangle = a|0\rangle + b|1\rangle$. Then
 $p_0 = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2$. Similarly, $p_1 = |b|^2$.
- States after measurement are $\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$ and $\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle$

Distinguishing quantum states

- Only orthogonal states can be distinguished.
- Suppose $|\psi_i\rangle$ are orthonormal. Given a state, how to identify index i .
- Define measurement operators $M_i = |\psi_i\rangle \langle \psi_i|$ and one more M_0 taken as positive square root of $I - \sum_{i \neq 0} |\psi_i\rangle \langle \psi_i|$ so that the operators together satisfy the completeness relation.
- If the state $|\psi_i\rangle$ is prepared, then $p_i = \langle \psi_i | M_i | \psi_i \rangle = 1$
- Thus it is reliably possible to distinguish orthonormal states.
- For two non-orthonormal states, $|\psi_1\rangle$ and $|\psi_2\rangle$, $|\psi_2\rangle$ can be decomposed into a component parallel to $|\psi_1\rangle$ and a component perpendicular to $|\psi_1\rangle$. Now because of the parallel component, there is non-zero probability of getting same outcome for $|\psi_2\rangle$.

Notation for qubit

- Quantum mechanics uses Dirac notation $\langle\psi|\psi\rangle$
- Consider that $|0\rangle$ and $|1\rangle$ are two possible states
- Linear combination of states $\alpha|0\rangle + \beta|1\rangle$
- Here α and β can be complex, may also consider real
- State of qubit is a vector in two dimensional vector space.
- Then $|0\rangle$ and $|1\rangle$ are special states that form the orthonormal basis for this vector space.
- Notations used in this study material has been prepared following the book **Quantum computation and quantum information by Michael A. Nielsen and Isaac L. Chuang**

Observation of qubit

- It is not possible to retrieve α or β through measurement
- Measurement results in 0 with probability $|\alpha|^2$ and in 1 with probability $|\beta|^2$.
- Since these two (0 and 1) are exhaustive, $|\alpha|^2 + |\beta|^2 = 1$
- This implies the state of a qubit is a unit vector in the 2D vector space.
- This dichotomy between the unobservable state of the qubit and the observations possible is where the quantum computing thrives.
- Ex. The state $|+\rangle$ is defined as $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Here the probability of measuring 0 and 1 are equiprobable.

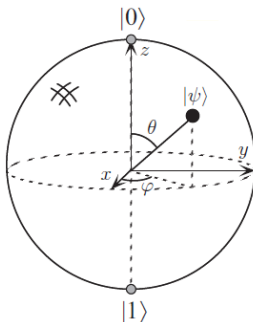
Quick look at binary implementations

- Two different polarizations of a photon particle
- Alignment of nuclear spin in a uniform magnetic field
- Two states, ground or excited, of an electron orbiting a single atom
- By shifting light on atom to adjust time, energy can change a $|0\rangle$ to $|1\rangle$ or vice versa.
- Similar adjustment can bring $|0\rangle$ to a state $|+\rangle$.

Geometric interpretation of qubit state

- $|\psi\rangle = e^{i\gamma}(\cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle)$
- Here the front term γ has no observational effects and hence may be ignored. The terms θ and ϕ define points on a unit 3D Bloch sphere. The concept is not easily extendable to multiple qubits.

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



Geometric interpretation explained

- $|\psi\rangle = r_\alpha e^{i\theta_\alpha} |0\rangle + r_\beta e^{i\theta_\beta} |1\rangle$
- A global phase concept in quantum mechanics says difference of $e^{i\theta}$ is indistinguishable.
- So consider new state $|\psi'\rangle = e^{-i\theta_\alpha} |\psi\rangle$ to eliminate θ_α
- Now substitute $\theta = \theta_\beta - \theta_\alpha$ to get $|\psi'\rangle = r_\alpha |0\rangle + r_\beta e^{i\theta} |1\rangle$
- Applying the modulus sum, $|r_\alpha|^2 + |x + iy|^2 = 1$ which gives the 3D sphere equation $|r_\alpha|^2 + x^2 + y^2 = 1$ in real space.
- Spherical coordinates are $x = r\sin\theta\cos\phi$, $y = r\sin\theta\sin\phi$, $z = r\cos\theta$.
- Take $z = r_\alpha$ so that $|\psi'\rangle = \cos\theta |0\rangle + e^{i\phi}\sin\theta |1\rangle$
- For full sphere, use half angles, since $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$

Where is my qubit?

- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix}$
- This implies, $\frac{\theta}{2} = \frac{\pi}{2}$ or $\theta = \pi$
- From the second row, $e^{i\phi}\sin\frac{\theta}{2} = 1$ implies $\phi = 0$.
- Likewise for the state $|0\rangle$, $\cos\frac{\theta}{2} = 1$ giving $\theta = 0$.

Quantum NOT gate

- input: $\alpha |0\rangle + \beta |1\rangle$
- output: $\alpha |1\rangle + \beta |0\rangle$
- linear behaviour is framework of quantum mechanics
- nonlinearity leads to paradox like time travel or faster than light
- may also lead to violations of second law of thermodynamics

Matrix representation of QNOT

- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $\alpha |0\rangle + \beta |1\rangle$ written as $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- so that $X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$
- Transformation like $|\psi'\rangle = \alpha' |0\rangle + \beta' |1\rangle$
- For this $|\alpha|^2 + |\beta|^2 = 1 = |\alpha'|^2 + |\beta'|^2$
- Condition for single qubit gate is that the 2×2 matrix describing the transformation must be unitary matrix.

Unitary matrix

- By definition, any unitary matrix produces valid quantum gate.
- For this unitary matrix product with its adjoint is identity matrix
 $U^\dagger U = I$
- Adjoint means first take transpose, then take complex conjugate.
- For the CNOT gate described earlier, $X^\dagger X = I$
- Another example unitary matrix is $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- For this case $|0\rangle$ leaves unchanged, $|1\rangle$ flips to $-|1\rangle$

Hadamard gate

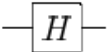
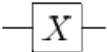
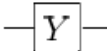
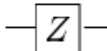
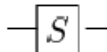
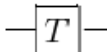
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- This resembles square root of NOT gate.
- The state $|0\rangle$ transforms to $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$
- The state $|1\rangle$ transforms to $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$
- Both of these states lie halfway between $|0\rangle$ and $|1\rangle$.
- Note that H^2 is not the NOT gate since $H^2 = I$.
- This means applying Hadamard gate twice leaves the state unchanged.

Hadamard operation

- Rotation - rotate the sphere about Y axis by 90°
- Reflection - rotate about X axis by 180° .
- X changes $\alpha |0\rangle + \beta |1\rangle$ to $\beta |0\rangle + \alpha |1\rangle$
- Z changes $\alpha |0\rangle + \beta |1\rangle$ to $\alpha |0\rangle - \beta |1\rangle$
- H changes $\alpha |0\rangle + \beta |1\rangle$ to $\alpha \frac{(|0\rangle+|1\rangle)}{\sqrt{2}} + \beta \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$

Common quantum gates

Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Product of rotation operations

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos \gamma/2 & -\sin \gamma/2 \\ \sin \gamma/2 & \cos \gamma/2 \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

- phase shift by α
- plane rotation by $\beta/2$
- ordinary rotation by $\gamma/2$
- plane rotation by $\delta/2$

Multiple qubit gates

- Rotation - rotate the sphere about Y axis by 90°
- Reflection - rotate about X axis by 180° .
- X changes $\alpha |0\rangle + \beta |1\rangle$ to $\beta |0\rangle + \alpha |1\rangle$
- Z changes $\alpha |0\rangle + \beta |1\rangle$ to $\alpha |0\rangle - \beta |1\rangle$
- H changes $\alpha |0\rangle + \beta |1\rangle$ to $\alpha \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} + \beta \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$

Multi qubit quantum gates

controlled-NOT



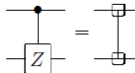
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

controlled-Z



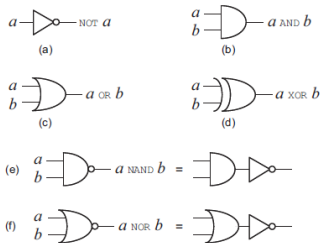
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

controlled-phase

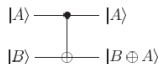


$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

Classical vs quantum gate

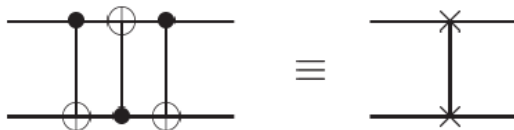


controlled-NOT



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Swap quantum gate explained



$$\begin{aligned}
 |a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\
 &\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
 &\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle,
 \end{aligned}$$

Controlled NOT gate explained

- Universality - input and output preserve same parity, restricting the class of functions that may be computed.
- If control qubit is set to zero, no change. $|00\rangle$ and $|01\rangle$ remain unchanged.
- But if set to 1, target qubit gets flipped. $|10\rangle$ changes to $|11\rangle$ and $|11\rangle$ changes to $|10\rangle$.

Computational basis states

- Consider $|+\rangle = \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$
- Consider $|-\rangle = \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$
- Then $|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$ gives

$$|\psi\rangle = \alpha \frac{(|+\rangle+|-\rangle)}{\sqrt{2}} + \beta \frac{(|+\rangle+|-\rangle)}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}} |+\rangle + \frac{\alpha-\beta}{\sqrt{2}} |-\rangle$$
- Now probabilities of post measurement are
 $(|\alpha + \beta|^2)/2 + (|\alpha - \beta|^2)/2$ read with $|\alpha|^2 + |\beta|^2 = 1$.
- Now generalize to any $|a\rangle$ and $|b\rangle$.

Reversibility of qubit gates

- CNOT is basically generalization of classical XOR gate since $|A, B\rangle$ transforms to $|A, B \oplus A\rangle$ being the modulo-2 addition.
- Also note U_{CN} is unitary since $U_{CN}^\dagger U_{CN} = I$.
- Classical XOR, NAND gates are irreversible and noninvertible. From output $A \oplus B$ A, B are not retrievable. Irretrievable loss of information at the gate.
- Since inverse of unitary matrix is also unitary, quantum gates are always invertible. This reversibility is crucial for quantum computation.

Universality of CNOT gates

- Any multiple qubit logic gate can be composed from CNOT and single qubit gates only.
- Swap gate follows as an example of this.
- This parallels the classical sense of universal gate.
- Also note U_{CN} is unitary since $U_{CN}^\dagger U_{CN} = I$.
- Classical XOR, NAND gates are irreversible and non-invertible. From output $A \oplus B$ the A, B are not retrievable. Irretrievable loss of information at the gate.
- Since inverse of unitary matrix is also unitary, quantum gates are always invertible. This reversibility is crucial for quantum computation.

Few points on quantum circuits

- No loops allowed, quantum circuits are acyclic
- FANIN not allowed, since bitwise OR is irreversible.
- FANOUT not allowed since qubit cannot be copied.
- Wire is not necessarily physical wire, it could be passage of time or a photon particle moving from one location to another through space.

What we need for quantum computing

- A register or a set of registers,
- A unitary matrix U , tailored to execute a given quantum algorithm,
- Measurements to extract information that is needed

So quantum computation is the set $\{H, U, \{M_m\}\}$ where H is the Hilbert space C^{2^n} for n -qubit register with $U \in U(2^n)$ represents the algorithm and M_m set of measurement operators.

Register is set to initial state $|\psi_{in}\rangle$ and some unitary transformation U_{alg} yields output $|\psi_{out}\rangle = U_{alg} |\psi_{in}\rangle$. The transformation here implies external fields, such as oscillating magnetic fields, electric fields or laser beams are applied to produce gate operations on the register.

Classical computation vs Quantum computation

- The former is based upon digital processing and the latter upon hybrid (digital + analogue) processing.
- A qubit may take an arbitrary superposition of $|0\rangle$ and $|1\rangle$, and hence their coefficients are continuous complex numbers.
- A gate is also an element of a relevant unitary group, which contains continuous parameters.
- An operation such as rotate a specified spin around the x-axis by an angle π is implemented by applying a particular pulse of specified amplitude, angle and duration.
- These parameters are continuous numbers and always contain errors.
- These aspects might cause challenging difficulties in a physical realization of a quantum computer.

Unitary matrix single qubit gate explanation

- Identity I keeps the states $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow |1\rangle$ Hence it can be expressed as $|0\rangle\langle 0| + |1\rangle\langle 1|$ hence $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- NOT X changes the states $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$ Hence it can be expressed as $|1\rangle\langle 0| + |0\rangle\langle 1|$ hence $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Phase shift Z changes the states $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow -|1\rangle$ Hence it can be expressed as $|0\rangle\langle 0| - |1\rangle\langle 1|$ hence $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- Combination Y changes the states $|0\rangle \rightarrow -|1\rangle$ and $|1\rangle \rightarrow |0\rangle$ Hence it can be expressed as $|0\rangle\langle 1| - |1\rangle\langle 0|$ hence $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

Unitary matrix CNOT gate explanation

- Basis for two qubit system $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

- Transformations are

$$|00\rangle \rightarrow |00\rangle,$$

$$|01\rangle \rightarrow |01\rangle,$$

$$|10\rangle \rightarrow |11\rangle,$$

$$|11\rangle \rightarrow |10\rangle$$

- Hence CNOT can be expressed as

$$|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

- Another way to express it is $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

- Vectors are

$$|00\rangle = (1000)^T; |01\rangle = (0100)^T; |10\rangle = (0010)^T; |11\rangle = (0001)^T$$

- Hence the matrix for CNOT is
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Unitary matrix for SWAP gate

- Transformations are

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |10\rangle, |10\rangle \rightarrow |01\rangle, |11\rangle \rightarrow |11\rangle$$

- Hence CNOT can be expressed as

$$|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

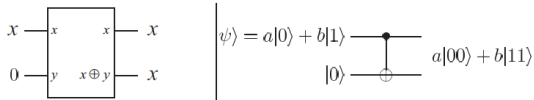
- Hence the matrix for SWAP is
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Note that the SWAP gate is a special gate which maps an arbitrary tensor product state to a tensor product state. In contrast, most two-qubit gates map a tensor product state to an entangled state.
- Controlled SWAP gate is Fredkin gate $|0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes U_{SWAP}$

Copying of qubits and no cloning

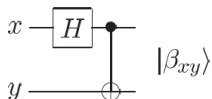
- Classical CNOT gate would copy bits from input side to output side. Take input $x, y = 0$ then output is $x, x \oplus y = x$.
- Take input $|\psi\rangle = a|0\rangle + b|1\rangle$ together with $|0\rangle$. Then at output we get $[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle$.
- If $|\psi\rangle = |0\rangle$ or $|1\rangle$ copying is possible. But not so for arbitrary states.
- For example,
$$(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$
- Thus it is impossible to copy unknown state - no cloning
- Since measurement of one qubit fully determines the other one, the hidden information gets lost. Copying would have allowed retention of information.

Circuit for copying



Circuit for copying

In	Out
$ 00\rangle$	$(00\rangle + 11\rangle)/\sqrt{2} \equiv \beta_{00}\rangle$
$ 01\rangle$	$(01\rangle + 10\rangle)/\sqrt{2} \equiv \beta_{01}\rangle$
$ 10\rangle$	$(00\rangle - 11\rangle)/\sqrt{2} \equiv \beta_{10}\rangle$
$ 11\rangle$	$(01\rangle - 10\rangle)/\sqrt{2} \equiv \beta_{11}\rangle$



Bell states

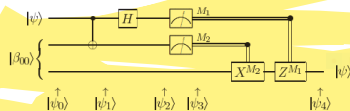
- Bell states can be generalized as $|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}$
- Take input $|\psi\rangle = a|0\rangle + b|1\rangle$ together with $|0\rangle$. Then at output we get $[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle$.
- If $|\psi\rangle = |0\rangle$ or $|1\rangle$ copying is possible. But not so for arbitrary states.
- For example,

$$(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$
- Thus it is impossible to copy unknown state - no cloning
- Since measurement of one qubit fully determines the other one, the hidden information gets lost. Copying would have allowed retention of information.
- These are called EPR (Einstein Podolski Rosen) qubit pairs since they explored strange properties.

Teleportation

- Alice wants to deliver a qubit $|\psi\rangle$ to Bob. Earlier, they generated an EPR pair and are in possession of one qubit out of the pair.
- State to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with α, β unknown amplitudes.
- Now after first stage, $|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle$ using Bell state.
- Using XOR logic, $|\psi_0\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$.
- Here there are three qubits, first two are at the end of Alice and third one is at the end of Bob.
- First one is sent through H gate and second one through CNOT gate.

Teleportation explained



$$00 \mapsto |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle]$$

$$01 \mapsto |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle]$$

$$10 \mapsto |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle]$$

$$11 \mapsto |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle] .$$

Teleportation continued

- For CNOT, $|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$.
- For H, $|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$.
- Regrouping terms, $|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$
- Now when Alice measures outcome, Bob is able to get back $|\psi\rangle$ by applying appropriate gate.
- When Alice measures $|00\rangle$ Bob gets to know α, β straight away.
- For $|01\rangle$ fix up the state applying gate X . For $|10\rangle$ fix up the state applying gate Z . For $|11\rangle$ fix up the state applying first gate X followed by Z .

Does Teleportation really succeed?

- Bob needs to know the measurement outcome of Alice to proceed. This requires communication over the classical channel. Hence teleportation fails.
- Further, copying is also ruled out since the original qubit is measured and thereby collapses.

Superdense coding

- Alice and Bob share one half of an entangled pair of qubits with $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Two classical bits can be transmitted using only a single qubit of communication and the preshared entanglement.
- To send 00 apply I to get outcome $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- To send 01 apply phase flip Z to get outcome $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$
- To send 10 apply CNOT X to get outcome $\frac{|10\rangle + |01\rangle}{\sqrt{2}}$
- To send 11 apply iY to get outcome $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$

Superdense coding

- These are the Bell basis or Bell states or EPR pairs, which are orthonormal hence distinguishable through measurement.
- Alice sends to Bob this qubit, Bob measures to get the 2 classical bits. The other half of the pair is with Bob.
- Alice has interacted with single qubit. Some third party has prepared the entangled state and predistributed the two qubits.
- Information is physical and this capability is significant. Physical experiments have been conducted and it actually works!
- Eavesdropper cannot infer about classical bits by tapping the qubit.

The possibilities

- What are the computations to be performed?
- Is it possible to better what can be done with the classical computer?
- Can quantum computers do classical computation?

Unitary matrix CCNOT - Toffoli gate

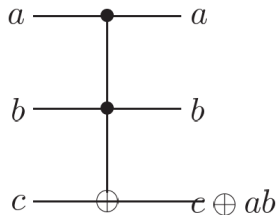
- Basis for three qubit system
 $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$
- Transformations only when first two bits are 1, third bit inverts.
 $|110\rangle \rightarrow |111\rangle$ and $|111\rangle \rightarrow |110\rangle$
- Hence CCNOT can be expressed as
 $(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X$
- This is the Toffoli gate

Classical computation using Toffoli gate

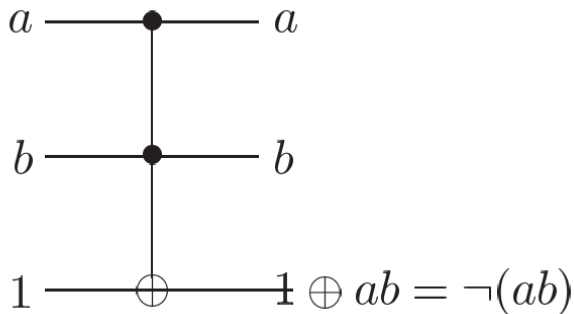
- When both a and b are 1, c flips.
- Reversibility is ensured since $(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$
- Now $c = 1$ implements NAND gate.
- Toffoli gate resembles 8×8 unitary matrix, hence it is valid quantum gate.
- Since NAND can be simulated, this is classical computation using quantum circuits.

Toffoli gate truth table

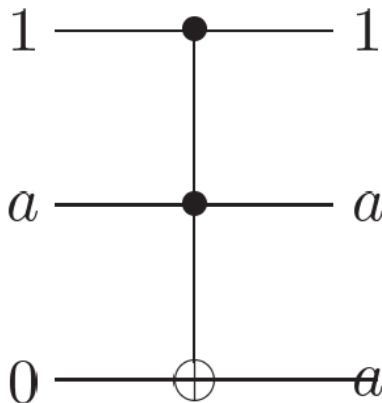
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Classical computation - NAND using Toffoli gate



Classical computation - Toffoli gate FANOUT



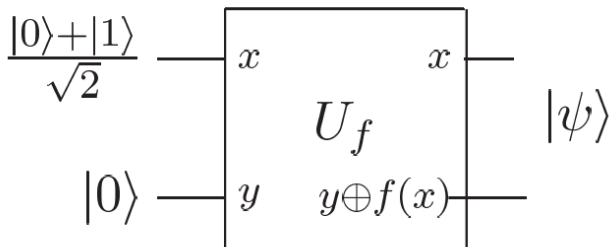
Non-deterministic Classical computation

- Classical computers that are able to generate random bits for computation.
- Prepare qubit in state $|0\rangle$ then pass it through Hadamard gate to produce $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$
- Now if state is measured, outcome is $|0\rangle$ or $|1\rangle$ with probability 0.5 each.

Quantum parallelism

- Unitary matrix U_f transforms from $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$
- When $y = 0$ final state is $f(x)$.
- When state $|0\rangle$ is passed through Hadamard gate to produce $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ the resulting state is $\frac{|0, f(0)\rangle+|1, f(1)\rangle}{\sqrt{2}}$
- This implies that $f(0)$ and $f(1)$ are computed simultaneously, unlike classical computation.
- The concept extends to multiple qubits by applying n Hadamard gates in parallel. $H^{\otimes 2}$ means $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}} \frac{(|0\rangle+|1\rangle)}{\sqrt{2}} = \frac{(|00\rangle+|01\rangle+|10\rangle+|11\rangle)}{2}$ so that for n gates $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$ may be obtained.

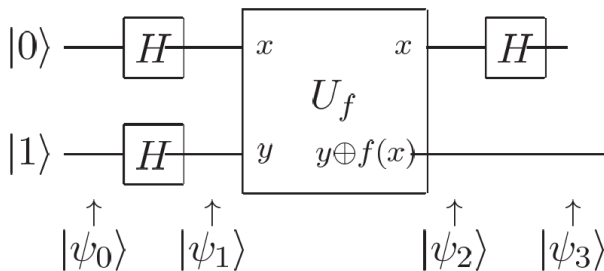
Finding f_0, f_1 in parallel



Deutsch algorithm explanation

- Exploit quantum parallelism and interference. Apply H on both $|0\rangle$ and $|1\rangle$ states, then pass through U_f transformation. Now property of $f(0) \oplus f(1)$ gets revealed.
- Stage 1: Feed 0 and 1 states: $|\psi_0\rangle = |01\rangle$
- Stage 2: Apply H gate: $|\psi_1\rangle = \left[\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}\right]\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]$
- Stage 3: Apply U_f : $|\psi_2\rangle = \pm\left[\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}\right]\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]$ when $f_0 = f_1$
 $|\psi_2\rangle = \pm\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]$ when $f_0 \neq f_1$
- Note $U_f(|x\rangle\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]) = (-1)^{f(x)} |x\rangle\left[\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\right]$

Deutsch algorithm



Deutsch algorithm - final stage

- Finally apply H on first qubit which becomes $\pm|0\rangle$ if $f(0) = f(1)$ and $\pm|1\rangle$ if $f(0) \neq f(1)$
- Note that $f(0) \oplus f(1) = 0$ if $f(0) = f(1)$ and $f(0) \oplus f(1) = 1$ if $f(0) \neq f(1)$
- Using above, rewrite $|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
- By measuring first qubit, a property involving both $f(0)$ and $f(1)$ is thus found in single evaluation, while in classical case two evaluations are required.

Deutsch Jozsa algorithm - motivation

- To check whether a Boolean function of n variables is balanced or constant. Balanced Boolean function is very important for cryptography.
- Alice selects x in the range 0 to $2^n - 1$ and sends n bits to Bob. This is n -bit query register.
- Bob computes $f(x)$ and replies to Alice - 0 or 1 in the form of 1-bit answer register.
- In classical computing, Alice needs $\frac{2^n}{2} + 1$ tries before being able to comment on $f(x)$ since first half may all return zero before getting a one.
- But if allowed to exchange qubits and calculate $f(x)$ using a unitary transform U_f a single query is enough. Alice interferes states in the superposition using H on the query register and then apply suitable measurement.

How the function gets incorporated

- Consider the initial state prepared as $|\psi_0\rangle = |x, 1\rangle$
- Now transform the second qubit $|\psi_1\rangle = |x, H.1\rangle = \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$
- Now apply the function Oracle $|\psi_2\rangle = \frac{|x,0 \oplus f(x)\rangle - |x,1 \oplus f(x)\rangle}{\sqrt{2}}$
- When $f(x) = 0$ we get $|\psi_2\rangle = \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$
- When $f(x) = 1$ we get $|\psi_2\rangle = \frac{|x,1\rangle - |x,0\rangle}{\sqrt{2}}$
- Combining, we get $|\psi_2\rangle = (-1)^{f(x)} \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}}$

How the inner product gets incorporated

- Consider the Hadamard transform $H|x\rangle$. This can be either $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ or $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Let us rewrite numerator as $(-1)^{x \cdot 0} |0\rangle + (-1)^{x \cdot 1} |1\rangle$ so that when $x = 0$ it resembles $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and when $x = 1$ it becomes $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
- Introduce now the variable $|z\rangle$ in states $|0\rangle$ and $|1\rangle$ alongside to write the above as $(-1)^{xz} |z\rangle$ with z assuming the two states and x remaining variable as usual.
- Now extend this concept to $H^{\otimes n} |x_1, \dots, x_n\rangle$ along with the function $f(x)$ to get $\sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}} \right]$
- When $|x_1, \dots, x_n\rangle = |0, \dots, 0\rangle$ this simplifies to $(-1)^{f(x)} |z\rangle$

Deutsch Jozsa algorithm explanation

- Apply H on n -qubit query register and 1-qubit answer register.
- Stage 1: Feed n qubits and 1 qubit: $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$
- Stage 2: Apply H gate: $|\psi_1\rangle = \sum \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ summed over $x \in \{0, 1\}^n$
- Stage 3: Apply U_f : $|\psi_2\rangle = \sum \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$
- Here result of function evaluation is stored in the qubit superposition state. It is alike the Deutsch algorithm.
- Next interfere the terms in superposition using H

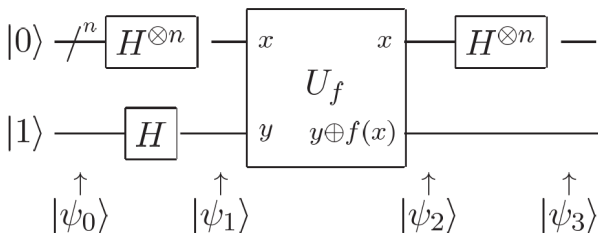
Deutsch Jozsa algorithm final step

- For single qubit $|x\rangle$ applying H check the cases $x = 0$ and $x = 1$ separately.
- Then $H|x\rangle = \sum_z (-1)^{xz} |z\rangle / \sqrt{2}$
- Hence $H^{\otimes n} |x_1, \dots, x_n\rangle = [\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle] / \sqrt{2^n}$
- Here $x.z$ is the inner product (bitwise, using modulo-2) for vectors x and z .
- Now using $|\psi_2\rangle$, we get $|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x.z + f(x)} |z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$
- For state $|0\rangle^{\otimes n}$ of query register, amplitude is $\sum_x (-1)^{f(x)} / 2^n$

Deutsch Jozsa algorithm inference

- When $f(x)$ is constant, amplitude of $|0\rangle^{\otimes n}$ will be $+1$ or -1 . All other amplitudes must be zero, observation yields only $|0\rangle$ s for all the qubits in query register.
- When $f(x)$ is balanced, positive and negative contributions of $|0\rangle^{\otimes n}$ cancels out, leaving zero amplitude. Measurement yields non-zero (other than $|0\rangle$) on at least one qubit in the query register.
- Measure all $|0\rangle$ states implies constant f and measure some non-zero state implies balanced.
- Importance and applications of the problem is limited. Probabilistic answer with classical approach is quite fast. Method seems quite different and not realistic.
- Useful algorithms are based on FFT, quantum search, quantum simulation.

Circuit for Deutsch Jozsa algorithm



Deutsch Jozsa algorithm

Algorithm: Deutsch-Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \dots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$. It is promised that $f(x)$ is either *constant* for all values of x , or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x , and 0 for the other half.

Outputs: 0 if and only if f is constant.

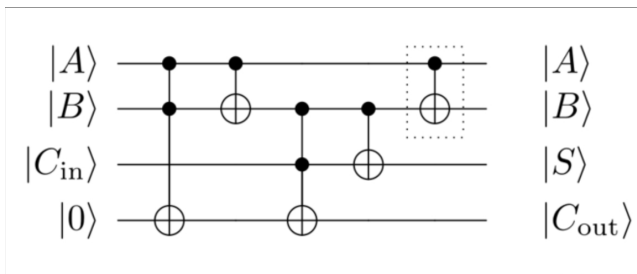
Runtime: One evaluation of U_f . Always succeeds.

Procedure:

1. $|0\rangle^{\otimes n}|1\rangle$ initialize state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ create superposition using Hadamard gates
3. $\rightarrow \sum_x (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ calculate function f using U_f
4. $\rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ perform Hadamard transform
5. $\rightarrow z$ measure to obtain final output z

Feynman full adder circuit

- First line $|A\rangle \rightarrow |A\rangle$
- Second line $|B\rangle \rightarrow |B\rangle$ EX-ORed twice with $|A\rangle$ cancelling it out.
- Third line: $|S\rangle = |A \oplus B \oplus C_{in}\rangle$
- Fourth line: $|C_{out}\rangle = |(A \wedge B) \oplus |0\rangle\rangle \oplus |(A \oplus B) \wedge C_{in}\rangle$



Quantum Fourier transform

- Fourier transform evaluations $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j$
- Now imagine transformations $|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$ for computational basis $|j\rangle$ with $0 \leq j \leq 2^n - 1$.
- This is unitary due to the group formed by roots of unity. This can therefore be realized using quantum circuits.
- Now apply superposition

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle$$

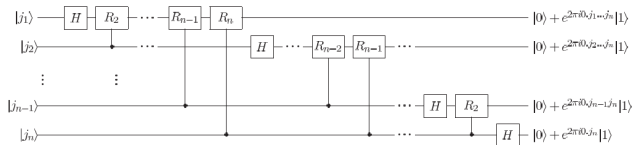
Quantum Fourier transform

- Here $|0\rangle, \dots, |N-1\rangle$ form orthonormal basis states with linear operator $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$
- Hence $\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$ with amplitudes $y_k = DFT(x_j)$
- Taking $N = 2^n$ computational basis in the range $|0\rangle, \dots, |2^n - 1\rangle$ for n -qubit quantum computer. Here $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$ using binary representation.
- $|j_1, \dots, j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i \cdot 0 \cdot j_n} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0 \cdot j_{n-1}} |1\rangle) \dots (|0\rangle + e^{2\pi i \cdot 0 \cdot j_1} |1\rangle)}{2^{n/2}}$

Quantum Fourier transform

- Start from $|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle$
- Then split the sum $\frac{1}{2^{n/2}} \sum_{k_l=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{-l}) / 2^n} |k_1 \dots k_n\rangle$
- which is
$$\frac{1}{2^{n/2}} \sum_{k_l=0}^1 \dots \sum_{k_n=0}^1 \otimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle = \frac{1}{2^{n/2}} \otimes_{l=1}^n \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$
- simplifies to $\frac{1}{2^{n/2}} \otimes_{l=1}^n [|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle]$
- yields finally
$$\frac{(|0\rangle + e^{2\pi i \cdot 0 \cdot j_n} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0 \cdot j_{n-1} \cdot j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle)}{2^{n/2}}.$$

Circuit for quantum Fourier transform



Implementing QFT for small qubits

- Consider QFT_2 . Here $\omega = e^{\pi i} = -1$ so that

$$QFT_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & \omega \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ Here } QFT_2 = H^{\otimes 2}$$

- Now we get to QFT_4 . Primitive fourth root of unity is i so that

$$QFT_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

- Now take $|f\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ The QFT on $|f\rangle$ gives

$$\frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Implementing QFT for small qubits

- For $|g\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ Applying QFT gives $\frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$
- For $|h\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ Applying QFT gives $\frac{1}{2} \begin{bmatrix} 1 \\ i \\ -1 \\ -i \end{bmatrix}$

Implementing QFT

- 2×2 unitary Gate $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$
- Start with $|j_1 \dots j_n\rangle$ as input. Then perform H on $|j_1\rangle$ to get $\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1} |j_2 \dots j_n\rangle)$
- Now $e^{2\pi i \cdot 0 \cdot j_1} = +1$ for $j_1 = 0$ and it is -1 for $j_1 = 1$.
- Next gates are controlled- R_2 , controlled- R_3 and so on. For R_2 gate, $\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \cdot j_2} |1\rangle) |j_2 \dots j_n\rangle)$
- Finally the state of $|j_1\rangle$ becomes $\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle) |j_2 \dots j_n\rangle)$

Implementing QFT

- Similar operation on second qubit gives

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0 \cdot j_2} |1\rangle) |j_3 \dots j_n\rangle$$

- followed by controlled gate gives

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0 \cdot j_2 \dots j_n} |1\rangle) |j_3 \dots j_n\rangle$$

- Continuing this way for each qubit, final state becomes

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle)(|0\rangle + e^{2\pi i \cdot 0 \cdot j_2 \dots j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i \cdot 0 \cdot j_n} |1\rangle)$$

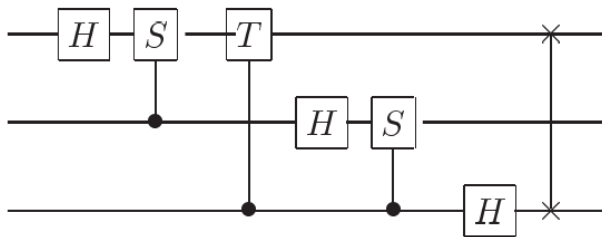
- Next swap operation is used to reverse the order, giving

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i \cdot 0 \cdot j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i \cdot 0 \cdot j_1 \dots j_n} |1\rangle)$$

Implementing QFT

- No of gates for first qubit is one H and $(n - 1)$ conditional rotations.
- For second qubit, one Hadamard and $(n - 2)$ conditional rotations.
- Continuing this way, total number of gates would be
$$n + (n - 1) + \dots + 1 = \frac{n(n+1)}{2}$$
- Next $n/2$ swaps are needed, with 3 CNOT gates per swap.
- Overall gates required is thus $O(n^2)$.
- On 2^n elements, classical FFT algorithm needs $O(n2^n)$ gates.
- These amplitudes cannot however be accessed by measurement.
- There is no way to prepare original state to be Fourier transformed.

Quantum Fourier transform - 3 qubits



Implementing QFT for 3 qubits

- Here $\omega = e^{2\pi i/8} = \sqrt{i}$
- Use phase gate for $k = 2$ i.e. $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- Use T gate for $k = 3$ i.e. $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

- Overall transform is
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

QFT is unitary

- QFT generalizes Hadamard transform, introduces phase.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2N-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3N-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{N-1} & \omega^{2N-2} & \omega^{3N-3} & \dots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

- The i^{th} column and j^{th} column has terms that are orthonormal. Their inner product will be zero. $\langle F_i | F_j \rangle = \frac{1}{N} \sum_{n=0}^{N-1} (\omega^{i-j})^n$
- Hence for $i = j$, we have $\langle F_i | F_j \rangle = 1$. For $i \neq j$, we have a GP series and the sum becomes $\frac{1}{N} \frac{\omega^{N(i-j)} - 1}{\omega^{i-j} - 1} = 0$ since $\omega^{N(i-j)} = 1$ with ω being the N^{th} root of unity.

First Stage for phase estimation

- Prepare state $|u\rangle$ with eigenvalue $e^{2\pi i\psi}$ as unitary transform. Then apply controlled U^{2^j} operations.
- First register contains t qubits in state $|0\rangle$ where t is chosen as number of digits of accuracy and probability of success in phase estimation.
- Second register begins in state $|u\rangle$ and contains as many qubits needed to store $|u\rangle$.
- Now apply H to first register. Apply controlled U to second register with successive powers of 2 upto 2^{t-1} .

Second Stage for phase estimation

- Final state of first register would be

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 2^{t-1}\psi} |1\rangle) \dots (|0\rangle + e^{2\pi i 2^0\psi} |1\rangle) \text{ which is}$$

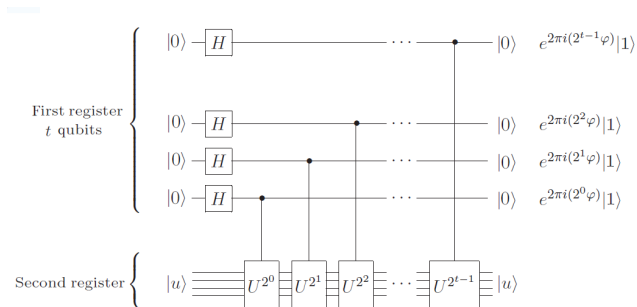
$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \psi_k} |k\rangle$$

- Second register does not change, remains $|u\rangle$.
- In second stage, apply inverse QFT. This gives back $|\psi_1, \dots, \psi_t\rangle$ since

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \psi_j} |j\rangle |u\rangle \rightarrow |\tilde{\psi}\rangle |u\rangle.$$

- Hence when measured $|\tilde{\psi}\rangle$ gives good estimation of phase.

Stages for phase estimation



Quantum phase estimation algorithm

Algorithm: Quantum phase estimation

Inputs: (1) A black box which performs a controlled- U^j operation, for integer j , (2) an eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i\varphi_u}$, and (3) $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ qubits initialized to $|0\rangle$.

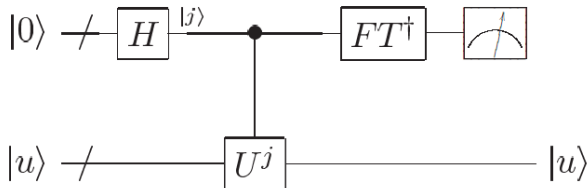
Outputs: An n -bit approximation $\tilde{\varphi}_u$ to φ_u .

Runtime: $O(t^2)$ operations and one call to controlled- U^j black box. Succeeds with probability at least $1 - \epsilon$.

Procedure:

1. $|0\rangle|u\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ create superposition
3. $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j |u\rangle$ apply black box
 $= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \varphi_u} |j\rangle |u\rangle$ result of black box
4. $\rightarrow |\varphi_u\rangle|u\rangle$ apply inverse Fourier transform
5. $\rightarrow \tilde{\varphi}_u$ measure first register

Schematic for overall phase estimation



Order finding

- Order of 5 mod 21 is 6 means $5^6 \bmod 21 = 1$
- Apply phase estimation to $U|y\rangle = |xy \bmod N\rangle$
- Here $y \in \{0, 1\}^L$ with range split from 0, $N - 1$ where U acts non-trivially and $N, 2^L - 1$ where $xy \bmod N = y$ only so that U has no role.
- Take the basis $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle$
- Then $U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle$

Order finding

- Consider eigenvalues of $|v\rangle$ an eigenvector of U . Then $U^k |v\rangle = \lambda^k |v\rangle$ or, $U^k |y\rangle = |x^k y \pmod N\rangle$ for computational basis state $|y\rangle$ encoding y as coprime to N .
- Let r be the order of x modulo N so that $x^r = 1 \pmod N$
- Then $\lambda^r |v\rangle = U^r |v\rangle = |v\rangle$ So we have $\lambda^r = 1$ or in other words the eigenvalues are simply the roots of unity. Hence $\lambda = \exp\left[\frac{2\pi i s}{r}\right]$ for $s = 0, \dots, r-1$. Hence order finding gets somehow connected with Fourier transform and phase estimation.
- Here U permutes the states $|x^0 \pmod N\rangle, \dots, |x^{r-1} \pmod N\rangle$ results in uniform superposition.
- Now $|v_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \pmod N\rangle$ is eigenvector associated with eigenvalue of 1.

Order finding

- Then $|v_{a_0, \dots, a_{r-1}}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a_k |x^k \pmod N\rangle$ where a_k are complex numbers and $|v_a\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a^k |x^k \pmod N\rangle$
- Then $U|v_{a_0, \dots, a_{r-1}}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a_k |x^{k+1} \pmod N\rangle$ This shifts the kets by one position cyclically relative to the coefficients a_k .
- Now $a_k = a^k$ is required to take a constant out of the sum.

$$U|v_a\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a^k |x^{k+1} \pmod N\rangle = a^{-1} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a^{k+1} |x^{k+1} \pmod N\rangle$$
- So if $a^r = 1$ then $U|v_a\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} a^k |x^{k+1} \pmod N\rangle = a^{-1} |v_a\rangle$
 implies v_a is eigenvector associated with $\lambda = a^{-1}$.

Order finding

- Since $a^r = 1$ to generate roots of unity $a = \exp(\frac{-2\pi is}{r})$
- Hence $|u_s\rangle = |v_{e^{-2\pi is/r}}\rangle = \sum_{k=0}^{r-1} \exp(\frac{-2\pi isk}{r}) |x^k(\text{mod } N)\rangle$ is eigenvalue of U associated with eigenvalue $\exp(\frac{2\pi is}{r})$.
- Hence phase estimation gives approximate value of $\frac{s}{r}$. Here $|\frac{s}{r} - \psi| \leq \frac{1}{2r^2}$

Phase estimation to integer order

- Now apply continuous fractions algorithm to get integers s and r .
- Example: $\frac{31}{13} = 2 + \frac{5}{13} = 2 + \frac{1}{\frac{13}{5}} = 2 + \frac{1}{2+\frac{3}{5}} = 2 + \frac{1}{2+\frac{1}{\frac{5}{3}}} =$
 $2 + \frac{1}{2+\frac{1}{1+\frac{2}{3}}} = 2 + \frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}}$
- Algorithm terminates after few split and invert steps.
- When s, r are L bit integers, the algorithm uses $O(L^3)$ operations. This part is run on classical computer, once the real number resembling phase estimate becomes available through quantum computing.

Factoring from order finding

- When x is non-trivial solution to $x^2 = 1 \pmod{N}$ then at least one of $\gcd(x - 1, N)$ or $\gcd(x + 1, N)$ is a non-trivial factor of N .
- Let $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ be prime factorization of an odd positive integer. Choose x coprime to N with r being order of $x \pmod{N}$. Then $\text{prob}(\text{risevenand} x^{r/2} \neq -1 \pmod{N}) \geq 1 - \frac{1}{2^n}$
- Example: $N = 91$. Choose $x = 4$. Then $r = 6$. Now $4^{6/2} - 1 = 63$ and $4^{6/2} + 1 = 65$. Now $\gcd(63, 91) = 7$ and $\gcd(65, 91) = 13$ which indeed are the factors of 91.

Factoring from order finding

- Input: Composite N Output: non-trivial factor of N .
- If N even, return 2 as factor,
- Check whether $N = a^b$ then return a as factor,
- Choose $x \leq N - 1$ if $\gcd(x, N) > 1$ return \gcd ,
- Find order r of $x(\text{mod } N)$,
- if r is even, $x^{r/2} \not\equiv -1(\text{mod } N)$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$ and test if the gcd divides N . Then return this as factor.
- Some steps involve classical number theoretic algorithms. But major step of order finding is based on quantum computing.

Factoring 15 quantum mechanically

- To factor $N = 15$ First choose $x = 7$ having no common factor with N , Next compute order r of x wrt N using Quantum order finding
- Create the state $\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |0\rangle = \frac{1}{\sqrt{2^t}} [|0\rangle + |1\rangle + \dots |2^t - 1\rangle] |0\rangle$ by applying $t = 11$ Hadamard transforms to first register. This value ensures error probability of at most $1/4$.
- Next compute $f(k) = x^k \bmod N$ leaving result in second register.

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |x^k \bmod N\rangle =$$

$$\frac{1}{\sqrt{2^t}} [|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle + |4\rangle |1\rangle + |5\rangle |7\rangle + |6\rangle |4\rangle + \dots]$$

Factoring 15 quantum mechanically

- Now apply inverse Fourier transform to first register and measure it. So a random result from 1,7,4,13 is obtained. Suppose 4 is obtained. The state input to FT^\dagger is $\frac{4}{\sqrt{2^t}}[|2\rangle + |6\rangle + |10\rangle + |14\rangle + \dots]$
- After applying inverse Fourier transform, we obtain $\sum_l \alpha_l |l\rangle$ with $2^t = 2048$ peaks at 0,512,1024,1536 with probability $1/4$ each.
- Suppose $l = 1536$ is obtained from measurement. Then $1536/2048 = 1/(1 + (1/3))$ so $3/4$ giving $r = 4$ as the order of $x = 7$
- Here r is even, $x^{r/2} \bmod N = 7^2 \bmod 15 = 4 \neq -1 \bmod 15$ so algorithm works.
- Henceforth $Gcd(x^2 - 1, 15) = 3$ and $Gcd(x^2 + 1, 15) = 5$ means $3 \times 5 = 15$

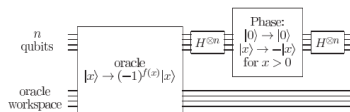
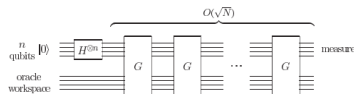
Quantum search algorithm

- By definition, $f(x) = 1$ if x is a solution to the search algorithm and $f(x) = 0$ otherwise.
- The oracle is unitary operator $|x\rangle |q\rangle \rightarrow |x\rangle |q \oplus f(x)\rangle$.
- So the oracle qubit $|q\rangle$ is flipped if $f(x) = 1$, so prepare $|x\rangle |0\rangle$, apply oracle, check to see if the oracle qubit has flipped to $|1\rangle$.
- Take the oracle qubit initially in the state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. If x is not a solution of the search problem, applying oracle to the state $|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ does not change the state. Else $|0\rangle$ and $|1\rangle$ get interchanged.

Quantum search algorithm

- Final state is then $-\lvert x \rangle \frac{\lvert 0 \rangle - \lvert 1 \rangle}{\sqrt{2}}$.
- This is like Deutsch Jozsa algorithm. $\lvert x \rangle \frac{\lvert 0 \rangle - \lvert 1 \rangle}{\sqrt{2}} \rightarrow (-1)^{f(x)} \lvert x \rangle \frac{\lvert 0 \rangle - \lvert 1 \rangle}{\sqrt{2}}$.
- Here action of oracle is like $\lvert x \rangle \rightarrow (-1)^{f(x)} \lvert x \rangle$. The solutions are marked by shifting the phase of the solution.
- For an N element search problem, with M solutions, search oracle needs to be applied $O(\sqrt{N/M})$ times only.
- This can be explained geometrically as Grover iterations can be interpreted as rotations, those interested may see the book for details.
- Quantum search has various applications, like simulation, counting, speeding up NP complete problems like Hamiltonian cycle, searching through an unstructured database.

Grover Search algorithm explained



Distance between quantum states

- Trace distance between probability distributions

$$D(p_x, q_x) = \frac{1}{2} \sum_x |p_x - q_x| \text{ Also called Kolmogorov distance.}$$

- Fidelity of probability distributions $F(p_x, q_x) = \sum_x \sqrt{p_x q_x}$

- Closeness of two quantum states is $D(\rho, \sigma) = \frac{1}{2} \text{tr}|\rho - \sigma|$

- When ρ and σ commute, then $\rho = \sum_i r_i |i\rangle \langle i|$ and $\sigma = \sum_i s_i |i\rangle \langle i|$ so that $D(\rho, \sigma) = D(r_i, s_i)$.

Fidelity metric

- For fidelity also $F(\rho, \sigma) = F(r_i, s_i)$.
- The two measures are related $D(|a\rangle, |b\rangle) = \sqrt{1 - F(|a\rangle, |b\rangle)^2}$
- Can be shown taking $|a\rangle = |0\rangle$ and $|b\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle$ so that $F(|a\rangle, |b\rangle) = |\cos\theta|$ and $D(|a\rangle, |b\rangle) = \frac{1}{2} \left| \begin{bmatrix} 1 - \cos^2\theta & -\cos\theta\sin\theta \\ -\cos\theta\sin\theta & -\sin^2\theta \end{bmatrix} \right|$
- Fidelity tells us how well a quantum channel preserves the information. Fidelity can also be expressed through chaining or cascading of unitary transforms that affect the quantum states in the quantum channels.

Von Neumann entropy

- For quantum state ρ formula is $S(\rho) = -\sum_x \text{tr}(\rho \log \rho)$ and with eigenvalues of ρ $S(\rho) = -\sum_x \lambda_x \log \lambda_x$

Information Theory	
Classical	Quantum
Shannon entropy	von Neumann entropy
$H(X) = -\sum_x p(x) \log p(x)$	$S(\rho) = -\text{tr}(\rho \log \rho)$
Distinguishability and accessible information	
Letters always distinguishable	Holevo bound
$N = X $	$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$ $\rho = \sum_x p_x \rho_x$
Noiseless channel coding	
Shannon's theorem	Schumacher's theorem
$n_{\text{bits}} = H(X)$	$n_{\text{qubits}} = S\left(\sum_x p_x \rho_x\right)$
Capacity of noisy channels for classical information	
Shannon's noisy coding theorem	Holevo-Schumacher-Westmoreland theorem
$C(N) = \max_{p(x)} H(X:Y)$	$C^{(1)}(\mathcal{E}) = \max_{\{p_x, \rho'_x\}} \left[S(\rho') - \sum_x p_x S(\rho'_x) \right]$ $\rho'_x = \mathcal{E}(\rho_x), \quad \rho' = \sum_x p_x \rho'_x$

Accessible information and Holevo bound

- How much information can be gained about X based on measurement result Y is the accessible information, how well can one infer about the prepared state.
- Accessible information is the maximum of mutual information $H(X : Y) \leq H(X)$ over all possible measurement schemes.
- Suppose Alice prepares state ρ_X where $X = 0, \dots, n$ with probabilities p_0, \dots, p_n . Bob performs a measurement $\{E_Y\} = \{E_0, \dots, E_m\}$ on that state, with measurement outcome Y . Holevo bound states that for any of Bob measurement $H(X; Y) \leq S(\rho) - \sum_x \lambda_x p_x S(\rho_x)$ where $\rho = \sum_x p_x \rho_x$. Holevo bound is thus an upper bound on accessible information.

Example of Holevo bound

- Alice is preparing single qubit in one of two quantum states as per outcome of fair coin toss. For heads, state is $|0\rangle$ and for tails, $\cos\theta|0\rangle + \sin\theta|1\rangle$.
- Hence in $|0\rangle, |1\rangle$ basis, $\rho = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}$
- Clearly, eigenvalues of ρ are $(1 \pm \cos\theta)/2$ so that Holevo bound is given by binary entropy $H_2((1 + \cos\theta)/2)$ so that Holevo bound maximizes for $\theta = \pi/2$, attaining 1 bit of information.
- This is the case where Alice has prepared from orthogonal set. For other values of θ Holevo bound gives strictly less than one bit, so for Bob it is impossible to determine which state Alice has prepared.

Data compression

- Schumacher noiseless channel coding theorem - For a quantum information source H, ρ any compression scheme with rate $R < S(\rho)$ is not reliable.

Information-theoretic relations

Fano inequality	Quantum Fano inequality
$H(p_e) + p_e \log(X - 1)$ $\geq H(X Y)$	$H(F(\rho, \mathcal{E})) + (1 - F(\rho, \mathcal{E})) \log(d^2 - 1)$ $\geq S(\rho, \mathcal{E})$
Mutual information	Coherent information
$H(X:Y) = H(Y) - H(Y X)$	$I(\rho, \mathcal{E}) = S(\mathcal{E}(\rho)) - S(\rho, \mathcal{E})$
Data processing inequality	Quantum data processing inequality
$X \rightarrow Y \rightarrow Z$	$\rho \rightarrow \mathcal{E}_1(\rho) \rightarrow (\mathcal{E}_2 \circ \mathcal{E}_1)(\rho)$
$H(X) \geq H(X:Y) \geq H(X:Z)$	$S(\rho) \geq I(\rho, \mathcal{E}_1) \geq I(\rho, \mathcal{E}_2 \circ \mathcal{E}_1)$

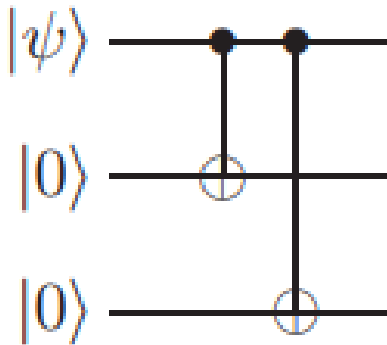
Difficulties of implementing codes

- Due to no cloning, repeating code is not possible. Also, measuring and comparing three quantum states at output from channel is not possible.
- Unlike discrete error in classical channel, continuum of different errors occur on single qubit. It is not possible to trace and requires infinite precision and resources.
- Measurement destroys quantum information. Hence unlike in classical decoding, it is not possible to observe first and then decide on decoding strategy. No recovery is possible after observing quantum state.

Bit flip channel and encoding

- It flips the qubit with probability p . Hence it can be described as $|\psi\rangle \rightarrow X |\psi\rangle$ where X is the Pauli bit flip operator.
- Encode $a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$ with $|0\rangle \rightarrow |0_L\rangle = |000\rangle$ and $|1\rangle \rightarrow |1_L\rangle = |111\rangle$
- Begin with $|\psi\rangle$ and two $|0\rangle$'s with output being $|\psi\rangle, |\psi\rangle \oplus |0\rangle, |\psi\rangle \oplus |0\rangle$ respectively.
- When $|\psi\rangle$ is $|0\rangle$, output is $|000\rangle$. When $|\psi\rangle$ is $|1\rangle$, output is $|111\rangle$.
This encoder trick produces repeating code, without cloning of course.

Bit flip code encoder



Bit flip channel decoding

- Number of bits flipped in the channel is one or less.
- Error correction takes place in two stages. In first stage error detection or syndrome diagnosis is performed. In second stage, recovery is initiated.
- Projection operations yields error syndrome as measurement result.

$$P_0 = |000\rangle \langle 000| + |111\rangle \langle 111| - \text{no error.}$$

$$P_1 = |100\rangle \langle 000| + |011\rangle \langle 011| - \text{first qubit flipped.}$$

$$P_2 = |010\rangle \langle 010| + |101\rangle \langle 101| - \text{second qubit flipped.}$$

$$P_3 = |001\rangle \langle 001| + |110\rangle \langle 110| - \text{third qubit flipped.}$$

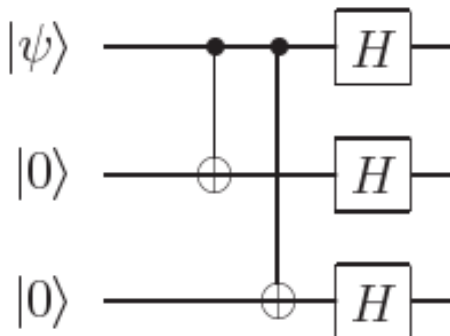
Bit flip channel decoding

- Corrupted state for first qubit in error is $|\psi\rangle = a|100\rangle + b|011\rangle$. Then measurement projection gives $\langle\psi|P_1|\psi\rangle = 1$.
Hence error syndrome = 1.
- Thus first stage ascertains which qubit is in error. The a, b information is intact.
- Recovery means just flipping once again the qubit reported to be in error.
- The error analysis is similar to the classical channel repeating code.
 $P_E = 3p^2 - 2p^3$.

Phase flip codes

- Phase flips with probability p . Uses phase flip operator Z which transforms $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$.
- This has no classical equivalent. For encoding, same as bit flip, followed by Hadamard gates.
- It is possible to interpret phase flip as bit flip using $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, so that $|0_L\rangle = |+++ \rangle$ and $|1_L\rangle = |-- - \rangle$.

Phase flip code encoder



Decoder for phase flip code

- Use conjugated Hadamard gates for projective measurements. $P_j \rightarrow P'_j = H^{\otimes 3} P_j H^{\otimes 3}$
- Syndrome measured by $H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$.
 $H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$.
- Interpret results for qubits 1, 2 or 2, 3 with the measurement giving +1 for states like $|+\rangle|+\rangle$ or $|-\rangle|-\rangle$ and -1 for states like $|+\rangle|-\rangle$ or $|-\rangle|+\rangle$.
- Now suppose first qubit flipped from $|+\rangle$ to $|-\rangle$. Then for recovery, apply $HX_1H = Z_1$.

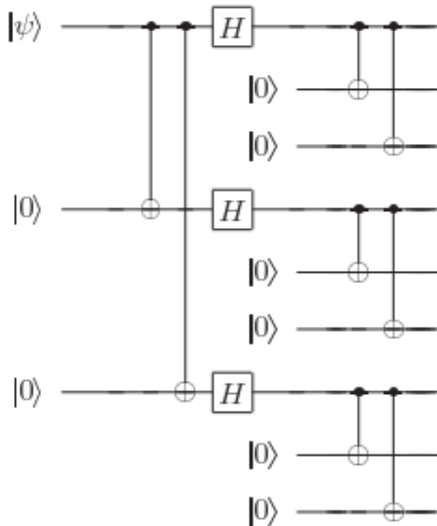
Interpretation based on two measurements

- If both X_1X_2 and X_2X_3 measure $+1$, implies no qubit flipped.
- If both X_1X_2 and X_2X_3 measure -1 , implies second qubit flipped.
- If X_1X_2 measures -1 and X_2X_3 measures $+1$, implies first qubit flipped.
- If X_1X_2 measures $+1$ and X_2X_3 measures -1 , implies third qubit flipped.

Shor code

- First encode with phase flip $|0\rangle \rightarrow |+++ \rangle$ and $|1\rangle \rightarrow |-- - \rangle$
- Next encode each with bit flip, resulting in 9– qubit code.
- $|0\rangle \rightarrow |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$
- $|1\rangle \rightarrow |1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$
- Such hierarchical encoding is called concatenation.

Shor code 9 bit encoder



How Shor code corrects bit flip

- Suppose bit flip occurs on first qubit.
- Perform measurement of $Z_1 Z_2$ to get that they are different.
- Next measure $Z_2 Z_3$ to know second and third are similar to conclude that first qubit flipped.
- Recover by flipping first qubit again.
- Bit flip error can thus be corrected for any of the nine qubits.

How Shor code corrects phase flip

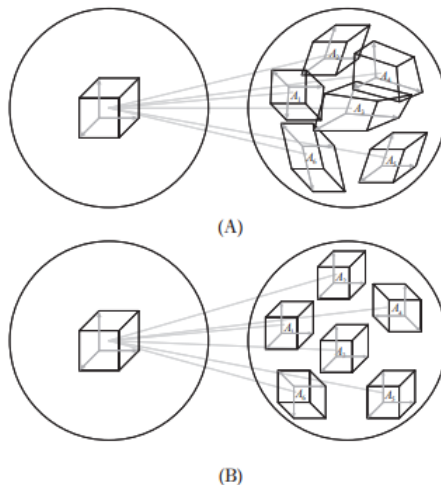
- Suppose phase flip occurs on first qubit. This flips the sign of the first block of qubits from $(|000\rangle + |111\rangle)$ to $(|000\rangle - |111\rangle)$.
- Phase flip on any of the first three qubits has this effect and the procedure works for any of these three possible errors.
- When phase flip occurs, the comparison of sign can be detected to be different. Comparison for second and third blocks yields same sign. So conclusion is that phase flip occurred for first block.
- Recovery is by flipping the phase once again.

Arbitrary error correction

- When both bit and phase flips - Suppose $Z_1 X_1$ happens on first qubit. Then both can be detected and corrected.
- Arbitrary error is like small rotation about Z axis or removal of qubits altogether. There is surprising immunity against such errors.
- Now $E_i = e_{i0}I + e_{i1}X_1 + e_{i2}Z_1 + e_{i3}X_1Z_1$ represents the overall operation for error correction on first qubit.
- Hence $E_i |\psi\rangle$ is superposition of four states $|\psi\rangle, X_1 |\psi\rangle, Z_1 |\psi\rangle, X_1 Z_1 |\psi\rangle$.
- Measurement of this error syndrome collapses into any one of these four states. Then take appropriate action to recover the state $|\psi\rangle$.

Good codes vs Bad codes

(A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.



Quantum key distribution cryptography

The BB84 QKD protocol

- 1: Alice chooses $(4 + \delta)n$ random data bits.
- 2: Alice chooses a random $(4 + \delta)n$ -bit string b . She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
- 3: Alice sends the resulting state to Bob.
- 4: Bob receives the $(4 + \delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
- 5: Alice announces b .
- 6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
- 7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
- 8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
- 9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

Implementation basics

System	τ_Q	τ_{op}	$n_{op} = \lambda^{-1}$
Nuclear spin	$10^{-2} - 10^8$	$10^{-3} - 10^{-6}$	$10^5 - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^4
Ion trap (In^+)	10^{-1}	10^{-14}	10^{13}
Electron – Au	10^{-8}	10^{-14}	10^6
Electron – GaAs	10^{-10}	10^{-13}	10^3
Quantum dot	10^{-6}	10^{-9}	10^3
Optical cavity	10^{-5}	10^{-14}	10^9
Microwave cavity	10^0	10^{-4}	10^4

Figure 7.1. Crude estimates for decoherence times τ_Q (seconds), operation times τ_{op} (seconds), and maximum number of operations $n_{op} = \lambda^{-1} = \tau_Q/\tau_{op}$ for various candidate physical realizations of interacting systems of quantum bits. Despite the number of entries in this table, only three fundamentally different qubit representations are given: spin, charge, and photon. The ion trap utilizes either fine or hyperfine transitions of a trapped atom (Section 7.6), which correspond to electron and nuclear spin flips. The estimates for electrons in gold and GaAs, and in quantum dots are given for a charge representation, with an electrode or some confined area either containing an electron or not. In optical and microwave cavities, photons (of frequencies from gigahertz to hundreds of terahertz) populating different modes of the cavities represent the qubit. Take these estimates with a grain of salt: they are only meant to give some perspective on the wide range of possibilities.