General

$\sin^2\theta + \cos^2\theta = 1 \qquad 2\sin\theta = 2\sin\theta\cos\theta$
$2\cos\theta = \cos^2\theta - \sin^2\theta$
$\log_b(x) = \log_c(x)/\log_c(b)$

Linalg

Matrix Multiplication: $\begin{pmatrix}a & b\end{pmatrix}\cdot\begin{pmatrix}c\\d\end{pmatrix} = (ac+bd)$

$\begin{pmatrix}a\\b\end{pmatrix}\cdot\begin{pmatrix}c & d\end{pmatrix} = \begin{pmatrix}ac & ad\\bd & bd\end{pmatrix}$

$\begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}e & f\\g & h\end{pmatrix} = \begin{pmatrix}ae+bg & af+bh\\ce+dg & cf+dh\end{pmatrix}$

Diagonalization Given X, $\det|X-\lambda\mathbb{I}|=0$, solve for values of λ (eigenvalues) $Xv=\lambda v$ (substitute in λ, solve for v (eigenvector))

Determinant $\begin{pmatrix}a & b\\c & d\end{pmatrix} = ad-cb$

$\begin{pmatrix}a & b & c\\d & e & f\\g & h & i\end{pmatrix} =$
$a\det(e,h,f,i) - b\det(d,g,f,i) + c\det(d,g,e,h)$

Adjoint (Hermitian Conjugate): $A^\dagger = A^*$ (transpose the matrix and take the complex conjugate of each element)

Complex Conjugate: Flip the sign of the imaginary part of a complex number

Trace Sum the diagonal elements of a square matrix

Partial Trace Partial trace for B:
$Tr_B\rho_{AB} \equiv |\psi\rangle_A \langle\psi|_A\, Tr(|\psi\rangle_B \langle\psi|_A)$

Multi-bit Dirac Notation $|A\rangle|B\rangle = |AB\rangle$ The dual of this is $\langle BA|$

Properties $|A\rangle\langle A| = \hat{I}$

Probability and Bayes' Rule

Bayes' theorem formula:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Examples of calculating conditional probabilities (medical tests, particle detectors)

Poisson distribution:

$$P(n) = \frac{\lambda^n e^{-\lambda}}{n!}$$

Classical Information Theory

Shannon Entropy/Information

$H = -k\sum_i p(a_i)\log p(a_i)$ By convention, we use $k=1$ and log is base 2.

Properties of entropy

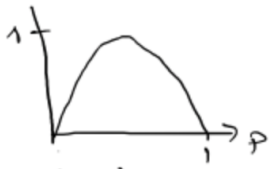
Entropy must be non-negative, and is maximized for a uniform distribution.

Thermodynamics

Gibbs Entropy: $S = -k\sum p_i \log p_i$

Communication Theory

Number of Typical Messages $W \simeq 2^{NH(p)}$ where $H(p)$ is the entropy of the message and N is the number of bits in the message.



Compression factor for different values of p. As p approaches 0.5 from either side, we can compress the message less and less, since there is more entropy we need to encode.

Shannon's Noiseless Coding Theorem:

For a given message, we only need $NH(p)$ bits to encode it (definition of $H(p)$ above)

Example: Let us have an alphabet A, B, C, D with probabilities of 1/2, 1/4, 1/8, 1/8 respectively. Entropy is $H = -(1/2\log 1/2 + 1/4\log 1/4\ldots) = 7/4$ bits Therefore, a message N characters long can be encoded in $7/4\cdot N$ bits.

Shannon's Noisy Coding Theorem:

On average, we need at least $\frac{N_0}{1-H(q)}$ bits to encode one of 2^{N_0} equally probable messages (N_0 is the original message length) where $H(q) = -[q\log q + (1-q)\log(1-q)]$ is the entropy associated with single bit error q.

Efficient Coding: Plot $N/N_0 - 1$ vs q to see when overhead becomes too "large"

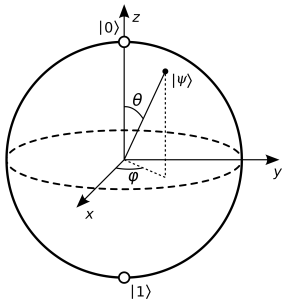
Huffman Coding

1. Sort the probabilities
2. Combine the two lowest probabilities into a tree, storing characters as branches and the sum of their probabilities as the root
3. Repeat until all probabilities are combined, and we reach a probability of 1
4. Set 0/1 to left/right (either pairing), and traverse the tree to find the encoding

Dirac Notation

$\langle\Psi| \iff |\psi\rangle^\dagger$

Ket	Matrix
$\|0\rangle$ or $\|H\rangle$	$\begin{bmatrix}1\\0\end{bmatrix}$
$\|1\rangle$ or $\|V\rangle$	$\begin{bmatrix}0\\1\end{bmatrix}$
Diagonal Up	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
Diagonal Down	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$
Left Circular	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$
Right Circular	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$
θ	$\begin{bmatrix}\cos\theta\\\sin\theta\end{bmatrix}$
$\pi/2+\theta$	$\begin{bmatrix}-\sin\theta\\\cos\theta\end{bmatrix}$



$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$

$+x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad +y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

$-x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad -y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Change of basis

Let θ be a rotation of basis vectors, counterclockwise.

$|x\rangle = \cos\theta|x'\rangle - \sin\theta|y'\rangle$ and
$|y\rangle = \sin\theta|x'\rangle + \cos\theta|y'\rangle$

where $|x'\rangle$ and $|y'\rangle$ are the new basis vectors.

Outer Product

Given that $|\psi\rangle = |\psi\rangle\langle\phi| = \begin{bmatrix}\psi_1\phi_1 & \psi_1\phi_2\\ \psi_2\phi_1 & \psi_2\phi_2\end{bmatrix}$

Quantum State Tomography

- Set a set of observables to uniquely determine a state. For a single qubit, we can use the Pauli operators.
- Prepare many copies of the state
- Measure the observables in states $\{H,V\}, \{+45,-45\}, \{LCP,RCP\}$
- Decompose state as $|\psi\rangle = r_H|H\rangle + r_V e^{i\phi}|V\rangle$ where $\phi = \phi_V - \phi_H$
- Procedure
  1. Perform measurement in {H, V} basis - Probability of detecting H is r_H^2, so $r_H = \sqrt{Pr_H}, r_V = \sqrt{1-Pr_H}$
  2. $\cos\phi = \frac{Pr_{+45}-1/2}{\sqrt{(1-Pr_H)(Pr_H)}}$
  3. $\sin_\phi = \frac{1/2-Pr_{RCP}}{\sqrt{(1-Pr_H)(Pr_H)}}$

Operators

Operators produce another ket

Spectral Decomposition

Operator A can be decomposed
$\hat{A} = \sum_i a_i |a_i\rangle\langle a_i|$

Observable

Is an operator, likely one of the Pauli operators. The measured results when observing in this "direction" will be one of its eigenvalues.

Mean value of an observable Measuring an observable $\hat{V} = \sum_i v_i |v_i\rangle\langle v_i|$ in the state $|\Psi\rangle$
Obtains result v_i with probability
$p(v_i) = |\langle v_i|\Psi\rangle|^2$
Repeating measurement many times obtains
expectation value
$\langle V\rangle = \sum_i P_i v_i = \sum_i |\langle v_i|\Psi\rangle|^2 v_i$
$\langle V\rangle_\Psi = \langle\Psi|\hat{V}|\Psi\rangle$

Uncertainty

Variance is $\Delta V^2 = \langle\Psi|(\hat{V} - \langle\Psi|\hat{V}|\Psi\rangle)^2|\Psi\rangle$
$\Delta V^2 = \langle\Psi|\hat{V}^2|\Psi\rangle - \langle\Psi|\hat{V}|\Psi\rangle^2 = \langle\hat{V}^2\rangle - \langle\hat{V}\rangle^2$

Heisenberg Uncertainty Principle

$\Delta x\Delta p \geq \frac{1}{2}|\langle\psi|[\hat{A},\hat{B}]|\psi\rangle|$ (e.g. for $[\hat{x},\hat{p}] = i\hbar$ we find $\Delta x\Delta p \geq \frac{\hbar}{2}$)

Pauli Operators

$\hat{\sigma}_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$
Eigenvectors: $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$

$\hat{\sigma}_y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix} = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$
Eigenvectors: $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$

$\hat{\sigma}_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$
Eigenvectors: $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$

$\hat{I} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$
Eigenvectors: $\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}$

(All have respective eigenvalues of +1 and -1)

Commutaton Relations

$[\hat{\sigma}_x,\hat{\sigma}_y] = 2i\hat{\sigma}_z \qquad \{\hat{\sigma}_x,\hat{\sigma}_y\} = 0$
$[\hat{\sigma}_y,\hat{\sigma}_z] = 2i\hat{\sigma}_x \qquad \{\hat{\sigma}_y,\hat{\sigma}_z\} = 0$
$[\hat{\sigma}_z,\hat{\sigma}_x] = 2i\hat{\sigma}_y \qquad \{\hat{\sigma}_z,\hat{\sigma}_x\} = 0$

$[\hat{\sigma}_a,\hat{\sigma}_b] = 2i\epsilon_{abc}\hat{\sigma}_c$

For direction $\vec{n}$, $\vec{n}\cdot\vec{\hat{\sigma}} = n_x\hat{\sigma}_x + n_y\hat{(\sigma)}y + n_z\hat{\sigma}_z$
For any operator,

$$\hat{H} = \begin{pmatrix}a & c-id\\c+id & b\end{pmatrix} = \frac{a+b}{2}\hat{\mathbb{I}} + \frac{a-b}{2}\hat{\sigma}_z + c\hat{\sigma}_x + d\hat{\sigma}_y$$

Tensor Products

Given that $|\psi\rangle = \begin{pmatrix}a\\b\end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix}c\\d\end{pmatrix}$

$$|\psi\rangle\otimes|\phi\rangle = \begin{pmatrix}a\begin{pmatrix}c\\d\end{pmatrix}\\ b\begin{pmatrix}c\\d\end{pmatrix}\end{pmatrix} = \begin{pmatrix}ac\\ad\\bc\\bd\end{pmatrix}$$

For operators,

$$\hat{A}\otimes\hat{B} = \begin{pmatrix}a & b\\c & d\end{pmatrix}\otimes\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix} = \begin{pmatrix}a\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix} & b\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix}\\ c\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix} & d\begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix}\end{pmatrix} = \begin{pmatrix}a\alpha & a\beta & b\alpha & b\beta\\ a\gamma & a\delta & b\gamma & b\delta\\ c\alpha & c\beta & d\alpha & d\beta\\ c\gamma & c\delta & d\gamma & d\delta\end{pmatrix}$$

Properties

Not commutative. Distributive:
$|\psi\rangle\otimes(|\phi\rangle + |\varphi\rangle) = |\psi\rangle\otimes|\phi\rangle + |\psi\rangle\otimes|\varphi\rangle$
$\hat{A}\otimes(\hat{B}+\hat{C}) = \hat{A}\otimes\hat{B} + \hat{A}\otimes\hat{C}$
Operators can act on one photon and not the other: Eg, let

$$\sigma_A^x = \begin{pmatrix}0 & 0 & 1 & 0\\0 & 0 & 0 & 1\\1 & 0 & 0 & 0\\0 & 1 & 0 & 0\end{pmatrix}$$

thus,

$$\begin{aligned}\sigma_A^x|HH\rangle &= \sigma_A^x\otimes\mathcal{I}(|H\rangle_A\otimes|H\rangle_B)\\ &= (\sigma_A^x|H\rangle_A)\otimes(\mathcal{I}|H\rangle_B)\\ &= |V\rangle_A\otimes|H\rangle_B\\ &= |VH\rangle\end{aligned}$$

or

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

Classical Cryptography

Criterion for Perfect Secrecy Let $\{p_i\}$ be the set of possible plaintexts, and $\{c_j\}$ be the set of possible ciphertexts. $P(p_i|C_j) = P(p_i)\forall i,j$ (discovering a ciphertext provides no information about the plaintext)

Quantum Cryptography

Based on no-cloning theorem (cannot copy an unknown quantum state)

BB84 (Quantum Key Distribution)

1. Alice sends a random sequence of bits, randomly encoded in either H/V or +45/-45 basis, to Bob
2. Bob measures each qubit in a random basis
3. Alice and Bob compare bases used
4. Alice and Bob discard qubits measured in different bases
5. Alice and Bob compare a subset of their qubits to check for eavesdropping
6. Alice and Bob use the remaining qubits as a shared key
7. Alice and Bob use the shared key to encrypt and decrypt messages

Errors in the key indicate eavesdropping (probability that Eve does not cause an error is $(3/4)^N$, where N is the number of qubits tested)

B92 Protocol

Non-orthogonal bases, eg $|0\rangle, |1\rangle$ and $|0'\rangle, |1'\rangle$
Alice prepares states in $|0\rangle, |1'\rangle$, associating them with 0 and 1, and sends them to Bob.
Bob measures in the two basis randomly. If he receives a $|0\rangle$, he discards it, as it could have been prepared as $|0\rangle$ or $|1'\rangle$, but if he receives a $|1\rangle$, he knows it was prepared as $|1'\rangle$. Same for $|0'\rangle, |1'\rangle$
Advantages: Only needs 2 states and 2 basis, unconditionally secure in a lossless channel, does not make use of entanglement.

Ekert's Entangled State Protocol

- $|\Psi\rangle^-$ kets, keep qubit A, send b
- Generated key is anti-correlated, Bob flips his measured result

Entanglement

Bell states

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$$
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle)$$

Ψ^- is isotropic (it remains the same no matter which axes we choose to measure it along) By decomposing it into θ basis, we can show that
$\Psi^- = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) =$
$\frac{1}{\sqrt{2}}(|\theta,\theta+\pi/2\rangle - |\theta+\pi/2,\theta\rangle)$

Density matrix formalism

Density Operator: $\hat{\rho} = \sum_n p_n|\psi_n\rangle\langle\psi_n|$
$\sum_i p_i = 1$ We can treat this as a "sum of probabilities", where p_i is the probability of a given state $|\psi_i\rangle$ appearing. The states for ψ_n need not be orthogonal.
We can rewrite it as $\hat{\rho} = \sum_m p_m|p\rangle_m\langle p|_m$
Measurement / Expectation Value / Generalized Born Rule Measuring using a Hermitian operator $M = \sum_i m_i|m_i\rangle\langle m_i|$ results in one of its eigenvalues m_i. The probability of obtaining a nondegenerate eigenvalue m_i is $p(m_i) = Tr[\rho\Pi_i]$, where $\Pi_i \equiv |m\rangle_i\langle m|_i$. If eigenvalues are degenerate, with value m, the probability of finding that value is $\sum_i Tr[\rho\Pi_i]$, where the sum is over the values of i where $m_i = m$.
Measuring GHZ State To measure only the first two qubits, measure all 3 qubits twice, performing 2 measurements for the last qubit.
Purity: $Tr(\hat{\rho}^2) = \sum_m \rho_m^2$ is the purity of a state Essentially how separable / correlated the two states are.

Properties

If $\hat{\rho}$ is diagonal and more than a single diagonal element is not 0, then it must be a mixed state. Measurements reduce a quantum state to a statistical mixture. $Tr(|0\rangle\langle 0|) = Tr(|1\rangle\langle 1|) = 1$
$Tr(|0\rangle\langle 1|) = Tr(|1\rangle\langle 0|) = 0$

Reduced density matrices

Given a state,

$$|\psi_{AB}\rangle$$

The density operator for this state can be separated

$$\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = |\psi_A\rangle\langle\psi_A|\otimes|\psi_B\rangle\langle\psi_B|$$

And satisfies the equality $\mathrm{Tr}\,\rho_{AB}^2 = 1$, since it is coherent. Therefore,

$$\mathrm{Tr}_B\,\rho_{AB} = \rho_A \qquad \mathrm{Tr}_A\,\rho_{AB} = \rho_B$$
$$\rho_A = |\psi_A\rangle\langle\psi_A| \qquad \rho_B = |\psi_B\rangle\langle\psi_B|$$

Von Neumann entropy

$S = -Tr(\rho\ln\rho) = -\sum_i p_i \ln p_i$ where p_i^A are diagonal elements in ρ_A

EPR Paradox

Say Alice and Bob share state
$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- If A is measured in Z, then B measures opposite Z
- Same for X measurement on A
- Predict either Z or X of qubit B by performing one or the other on A.
- If our choice does not disturb B, then the values for X and Z must exist simultaneously, so there must be hidden variables
- TL;DR, believed there was a theory as correct as QM that could deterministically predict results of Bob's measurements

Local Realism

Local realism is the idea that the properties of a system are determined by the properties of the system's parts. AKA, no spooky action at a distance.

Bell's Inequality:

Front-panel explanation:

- Source sends out pairs of particles, each apparatus has buttons marked M, N, Alice and Bob randomly measure in these states w/o communication.
- Each apparatus displayes a readout depending on results.
- Alice and Bob record their events.
- We assert that $\sum M_A M_B N_A N_B P(M_A, M_B, N_A, N_B) = 1$, such that all 4 quantities have well-defined values (say in a hidden variable), even though only 2 of them are displayed. (Locality)
- From this, we assert that $| < M_A M_B - M_A N_B + N_A M_B + N_A N_B > | \leq 2$ if locality holds.
- However, each expectation value is actually $\pm 1/\sqrt{2}$, leading to a final value of $< S >= -2\sqrt{2}$.
- Contradiction!

Loop Holes

Locality loophole If Alice and Bob are close, then information could be transmitted, and thus measurements are no longer "local"

Detection loophole If one or more photons are lost, then the situation is no longer consistent with the "front panel" described. Taking into account only the events that do occur doesn't refute local realism. e.g. a hidden variable that decides if it should appear "invisible", causing it to not have values for M and N at the same time

GHZ State

GHZ State can also show non-locality:

- 3 observers, each with a Bell apparatus, but buttons are for $\hat{\sigma}_x$ and $\hat{\sigma}_y$ measurements.
- Source sends out 3 particles at a time
- Note that whenever 2 are $\hat{\sigma}_y$ and 1 is $\hat{\sigma}_x$, result is -1.
- Local realism predicts that $\sigma_{xA}\sigma_{xB}\sigma_{xC} = -1$
- However, $\sigma_{xA}\sigma_{xB}\sigma_{xC} |GHZ\rangle = + |GHZ\rangle$, with an eigenvalue of $+1$. Contradiction.

CHSH Game:

We can construct a game to test Bell's inequality. Alice and Bob each have a bit, and they can choose to measure it in one of two bases. They win if the XOR of their bits is 0.

Using deterministic strategies, the maximum win rate is 75%.

However, using entangled particles, we can achieve a win rate of 85%, violating Bell's inequality.

Quantum Socks

- Generate $|\psi\rangle^-$

Quantum Dense Coding

- Start with shared qubit $|\Psi^-\rangle$
- Alice applies one of $\{\hat{I}, \hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z\}$ to just her qubit, producing the following conversions: $\hat{I} \otimes \hat{I} |\Psi^-\rangle = |\Psi^-\rangle$ $\hat{\sigma}_x \otimes \hat{I} |\Psi^-\rangle = -|\Phi^-\rangle$ $\hat{\sigma}_y \otimes \hat{I} |\Psi^-\rangle = i |\Phi^+\rangle$ $\hat{\sigma}_z \otimes \hat{I} |\Psi^-\rangle = |\Psi^+\rangle$ (we ignore global phases $-$ and i)
- Alice then sends single qubit to Bob
- Bob then measures in Bell-state basis, with a CNOT with 1 as control and 2 as target, and a Hadamard gate on 1. This maps $|\Psi^-\rangle \to |11\rangle$, $|\Psi^+\rangle \to |01\rangle$, $|\Phi^-\rangle \to |10\rangle$, $|\Phi^+\rangle \to |00\rangle$.
- Neither Bob nor Alice can recover the encoded information alone, instead the information resides in correlations between two qubits, and is non-local.

Quantum Teleportation

- Transfers unknown quantum state between 2 locations
- Uses classical communications channel
- Original state is destroyed

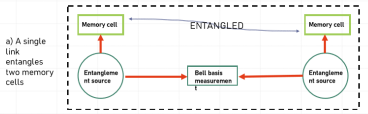
Procedure

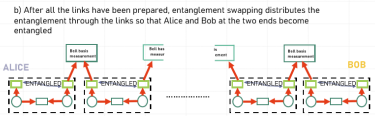
- Input state of $|\chi\rangle = \alpha |H\rangle + \beta |V\rangle$ in Hilbert space V_1
- Alice and Bob share entangled state $|\Psi^-\rangle$ in Hilbert space $V_2 \otimes V_3$
- Alice measures in $V_1 \otimes V_2$ space in the bell basis

Alice	Prob	Bob	Op
Φ^+	1/4	$-\beta |H\rangle + \alpha |V\rangle$	$\rho_z \rho_x = i\rho_y$
Φ^-	1/4	$\beta |H\rangle + \alpha |V\rangle$	ρ_x
Ψ^+	1/4	$-\alpha |H\rangle + \beta |V\rangle$	ρ_z
Ψ^-	1/4	$-(\alpha |H\rangle + \beta |V\rangle)$	none

Quantum Repeater

- Entangle each link's cells, not very likely to succeed but each link can be retried until connection is made
- Entangle link ends (that are very close and will very likely succeed) to form final long link





Quantum Gates

Properties

- Can only perform unitary operations
  - Due to all quantum operations being unitary, follows from Schrodinger's equation
  - If it were not unitary, we would be discarding data which is a "measurement"
- Any controlled-unitary gate can be made from CNOT and single qubit gates.

Necessary Conditions

- Well-defined, extendible qubit array that is stable
- Ability to prepare qubit array in suitable starting state, eg all $|0\rangle$
- Good isolation from environment (long coherence times)
- Ability to perform universal set of gate operations (e.g. single-qubit rotations, CNOT between any pair of qubits)
- Ability to perform close to ideal von Neumann measurements on each of the qubits

Unitary

Unitary if $A^\dagger A = \mathbb{I}$, where † represents conjugate transform (Hermitian Conjugate).

Common Gates

Hadamard gate:

$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$ **Rotation operator:** $\hat{R}(\vec{n}, \theta) = e^{-i\theta \vec{n} \cdot \vec{J}}$ Where $\vec{J}$ is the angular momentum operator, and $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ is a unit vector.

For spin-1/2, $\vec{J} = \frac{1}{2}\vec{\sigma}$

2-qubit Quantum Gates

$|00\rangle \Leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ $|01\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ $|10\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

$|11\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Matrix is 4 by 4, selected column(s) can be treated as "inputs", row values in said column(s) are "outputs".

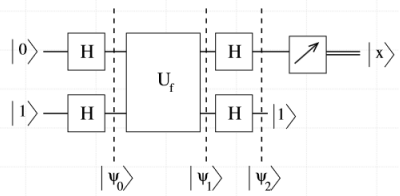
Quantum Algorithms

Deutsch-Joza Algorithm

Determine whether an unknown selection from 4 1-bit functions is constant or balanced.

Classical algorithm requires 2 evaluations for f(0) and f(1)

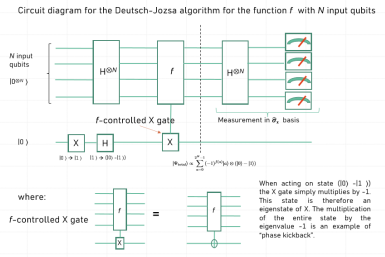
Quantum algorithm evaluates both f(0) and f(1) at the same time:



If $f(0) = f(1) = \pm |0\rangle$, else $f(0) = \pm |1\rangle \neq f(1)$.

N qubit extension

Classical has $O(2^N)$ time complexity, QM has constant time (single Oracle use).



If f is constant, amplitude is either +1 or -1, so measurement must give all 0s. Otherwise, it will not be all 0s.

Bernstein-Vazirani Algorithm

Given a function $f(x) = a \cdot x$, find a.

Classically, we would need to do n queries, one for each bit.

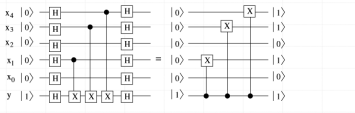


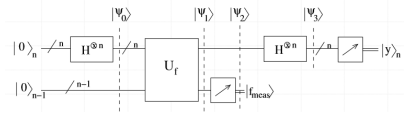
Figure B : Sandwiching the circuit for U_f in Fig. A between Hadamards, and realizing that the effect of the Hadamards is to interchange the control and target qubits in the CNOT (control-X) gates, we see immediately that the final state of the upper (input) register contains $a = 11010$.

Using QM, we can get the positisons in a that are 1 using one query.

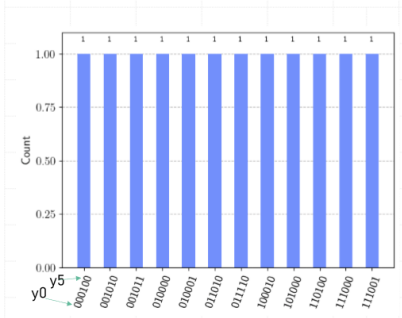
Simon's Algorithm

Given a black-box function that has the property $f(x \oplus a) = f(x)$, find a. Since $x \oplus a \oplus a = x$, $f(x) = f(x \oplus a) = f(x \oplus a \oplus a)$, therefore $f(x)$ is periodic with period a under bitwise mod 2 addition.

Classically, we evaluate functions on different inputs until we find a repetition, and then compare $m(m-1)/2$ pairs. For a good chance of success, number of pairs must be close to 2^n, so m is to the order of $2^{n/2}$.



Using the multiple measurements performed at y, the bit indicies with 1s form a linear equation, that equal 0. Combining multiple of these measurements, we can build a valid solution.



e.g. in this case, $a3 = 0$, $a2 + a4 = 0$, $a2 + a4 + a5 = 0$... and we find that $a = 010101$.

Shor's Algorithm

Given an integer N, what are its prime factors?

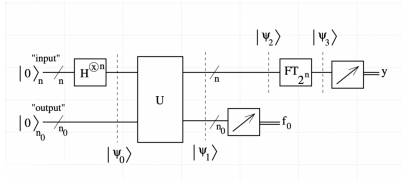
Classical algorithm: "General number field sieve", runs in exponential time w.r.t. input length.

Theory

- Let N be the product of two prime numbers p and q. Thus, the sequence $m \mod N, m^2 \mod N, m^3 \mod N, \ldots$ will repeat with a period that is a perfect divisor of $(p-1)(q-1)$
- Use Quantum Fourier Transform to find the period of this sequence

Algorithm

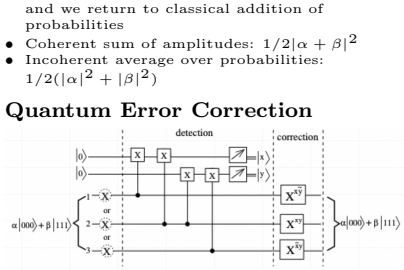
1. Pick a random integer a with no common factors with N.
2. Calculate $a, a^2, a^4 \ldots, a^{2^n} \pmod N$, where $2^n > N^2$
3. Perform modular exponentiation for all x, a.k.a $a^x = \prod_{j=0}^{n-1} (a^{2^j})^{x_j}$ (algorithm below up to Ψ_1)
4. QFT to extract the period of probabilities from upper register
5. If successful, we find y within 1/2 of $2^n m/r$, and thus $|y/2^n - m/r| < 1/2^{n+1}$.
6. Thus, m/r is one of partial sums of continued fraction expansion of $y/2^n$



Coherent Superposition

- Must be a well-defined phase between pieces in superposition
- e.g. there can eventually be interference between pieces
- If the phase is random, no interference exists, and we return to classical addition of probabilities
- Coherent sum of amplitudes: $1/2|\alpha + \beta|^2$
- Incoherent average over probabilities: $1/2(|\alpha|^2 + |\beta|^2)$

Quantum Error Correction



Measurement of Ancilla identifies and collapses the error, and applying the appropriate operator corrects the error.

Stabilizers

- Square to 1 (so eigenvalues are ± 1)
- Mutually commute, so have same eigenstates
- Syndromes are eigenstates
- Uncorrupted syndrome has eigenvalue +1 for all stabilizers
- Set of ± 1 eigenvalues of stabilizers uniquely specifies syndrome

Phase Flip Errors

Given errors of the type $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \to \alpha |0\rangle - \beta |1\rangle$

- Correct by transforming to +- basis of X operator
- Use Hadamard: $H |0\rangle = |+\rangle$, $H |1\rangle = |-\rangle$ $H |+\rangle = |0\rangle$, $H |-\rangle = |1\rangle$ (Role of X and Z are interchanged)