Linalg

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

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
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:

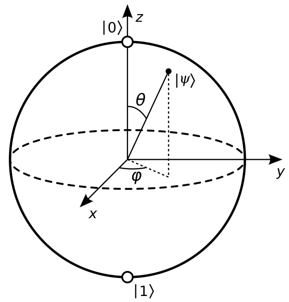
On average, we need at least $\frac{N_0}{1-H(q)}$ bits to encode one of 2^{N_0} equally probable messages (N_0 is the original message length) where $H(q) = -[q\log q + (1-q)\log(1-q)]$ is the entropy associated with single bit error q.
Efficient Coding: Plot $N/N_0 - 1$ vs q to see when overhead becomes 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	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$



$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$
$+x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad +y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
$-x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ $\quad -y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

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 and use probability and regression to reconstruct the state

Operators

Operators produce another ket

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

$[\hat{\sigma}_x, \hat{\sigma}_y] = 2i\hat{\sigma}_z$ $\quad \{\hat{\sigma}_x, \hat{\sigma}_y\} = 0$
$[\hat{\sigma}_y, \hat{\sigma}_z] = 2i\hat{\sigma}_x$ $\quad \{\hat{\sigma}_y, \hat{\sigma}_z\} = 0$
$[\hat{\sigma}_z, \hat{\sigma}_x] = 2i\hat{\sigma}_y$ $\quad \{\hat{\sigma}_z, \hat{\sigma}_x\} = 0$
$[\hat{\sigma}_a, \hat{\sigma}_b] = 2i\epsilon_{abc}\hat{\sigma}_c$
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,

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

Common Gates

Hadamard gate:
$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}(\hat{\sigma_z} + \hat{\sigma_x})$ **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, $\vec{J} = \frac{1}{2}\vec{\sigma}$

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.

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 $\Psi^- = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) =$
$\frac{1}{\sqrt{2}}(|\theta, \theta+\pi/2\rangle - |\theta+\pi/2, \theta\rangle)$

Examples of entangled states ($|\psi^-\rangle$)

EPR Pair: $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
GHZ State: $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$
W State: $|\psi^-\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$

Density matrix formalism

Density Operator: Represents a mixture of states $\hat{\rho} = \sum_n p_n|\phi_n\rangle\langle\phi_n|$
Expectation Value: $\langle A\rangle = Tr(\hat{\rho}\hat{A})$
Purity: $Tr(\hat{\rho}^2) = \sum_m \rho_m^2$ is the purity of a state Essentially how separable / correlated the two states are.

Reduced density matrices

For a two-bit state that can be factored,

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

We can use the reduced density matrix to describe the state of one of the qubits.
$Tr_B\rho_{AB} \equiv |\psi_A\rangle\langle\psi_A|Tr|\psi_B\rangle\langle\psi_B| = |\psi_A\rangle\langle\psi_A| = \rho_A$

Von Neumann entropy

$S_A = -Tr(\hat{\rho_A}\log\hat{\rho_A} = -\sum_i p_i^A \ln p_i^A = -\sum_i |a_i|^2\ln|a_i|^2 \neq 0)$ and $S_A \equiv S_B$ (Characterizes how strongly A and B are entangled)
Local Measurements:
Generalized Born Rule: We can extend the Born rule to density matrices:

$$p(a) = Tr(\hat{\rho}\hat{\Pi}_a)$$

Where $\hat{\Pi}_a$ is the projector onto the eigenspace of $\hat{A}$ with eigenvalue a, e.g. $\hat{\Pi}_a = \sum_i |a_i\rangle\langle a_i|$

Bell's Inequalities

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: For any local hidden variable theory, the following inequality holds:

$$| < M_A M_B - M_A N_B + N_A M_B + N_A N_B > | \leq 2$$

Where M_A, M_B, N_A, N_B are the results of measurements on two entangled particles.
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.