Quantum computation and information - Indranil Chakravarty

Siddharth Bhat

Contents

Chapter 1

Lecture 1: Introduction

Taught in collaboration with MSR Redmond for the Q# bits.

Topics:

- Intro: Transition from Classical to Quantum: Stern Gerlash, Sequential Stern Gerlash, Rise of randomness.
- Foundations of Quantum Theory: States, Ensembles, Qubits, Pure and Mixed states, Multi qubit states, Tensor products, Unitary transforms, Spectral decomposition, SVD, Generalized measurements, Projective measurements, POVM, Evolution of quantum state, Krauss Representation.
- Quantum Entropy: Subadditivity of Entropy, Avani-Licb(?) Inequality, Quantum channel, Quantum channel capacity, Data compression, Benjamin Schumahur(?) theorem.
- Quantum Entanglement: EPR paradox, Schmidt decomposition, Purification of entanglement, Entanglement separability problem, Pure and mixed entangled states, Measures of Entanglement.
- Quantum information processing protocols: Teleportation, Superdense coding, Entanglement swapping.
- Impossible operations in quantum information theory: No cloning, No deleting, No partial erasure.
- Quantum Computation: Introduction to Quantum Computating, Pauli gates, Hadamard gates, Universal gates, Quantum algorithms (Shor, Grover search, machine learning and optimisation).
- Quantum programming: Programming quantum algorithms, Q# progtramming language, quantum subroutines.

Books:

- Quantum computation and Quantum information — Nielsen and Chuang.

- Preskill lecture notes.

Grading:

- Possibility of open book take-home open ended exam for the finals.
- Mid 1: 15%
- Mid 2: 15%
- End sem (open book?) : 30%
- Assignments: 15%
- Projects: 25%

1.1 Stern-Gerlach: A brief, morally correct construction of qubits

```
light rays ---> [z] ---> (z+, z-) --block (z-) --> [x] --- (x+, x-) -- block (x-) --> [z] ---> (z+, z-?!)
```

[z] represents a polarizer along that axis.

- Since we first polarized along z, how did we manage to get out light rays in the x direction? The polarization should have killed everything.
- Since we blocked $z-$, How did we get back $z-$ after passing stuff through [x]? Something has changed drastically from our classical picture.

We can consider $|z+\rangle$ to be something like:

$$|z+\rangle \equiv_? \frac{1}{2}|x+\rangle + \frac{1}{2}|x-\rangle$$

Where $|x+\rangle$ and $|x-\rangle$ are basis vectors for some vector space over $\mathbb{R}$.

If we were to pass the $z+$ light rays through [y], then we would get $|y+\rangle, |y-\rangle$. So, $|z+\rangle$ is also:

$$|z+\rangle \equiv_? \frac{1}{2}|y+\rangle + \frac{1}{2}|y-\rangle$$

1.1.1 Analogy with polarization of light

Consider a monochromatic light wave in the z direction. A linearly polarized light with polarization in the x direction which we call x polarized light is given by:

$$E_x = E_0 \hat{x} \cos(kz - \omega t)$$

$\omega \equiv$ frequency $\equiv ck$, $c \equiv$ speed of light, $k \equiv$ wave number.

Similarly, y polarized light is given by:

$$E_y = E_0 \hat{y} \cos(kz - \omega t)$$

Consider the case where we have x filters along direction -, x' filter along direction /, y filters along direction |. In this case, we can have x, x', y filters arranged sequentially give us non-zero output (contrast with just having x, y).

We can express the x' polarization as:

$$E_0 \hat{x}' \cos(kz - \omega t) = \frac{E_0}{\sqrt{2}} \hat{x} \cos(kz - \omega t) + \frac{E_0}{\sqrt{2}} \hat{y} \cos(kz - \omega t)$$

By analogy, we write:

$$|z_+\rangle \equiv \frac{1}{\sqrt{2}} |x_+\rangle + \frac{1}{\sqrt{2}} |x_-\rangle$$

However, we now have probability $\frac{1}{\sqrt{2}}$, but we want $\frac{1}{2}$. So, we define the probability as:

$$\langle x + |x_-\rangle^2 = \frac{1}{2}$$

$$\begin{aligned}
z_+ &\equiv x \text{ polarization} \\
z_- &\equiv y \text{ polarization} \\
x_+ &\equiv x' \text{ polarization} \\
x_- &\equiv y' \text{ polarization}
\end{aligned}$$

This problem can be solved again by polarization of light. This time, we consider circularly polarized light which can be obtained by letting linearl polarized light passing through a quarter wave plate (?)

When we pass such circularly polarized light through an x or y filter, we again obtain either an x polarized beam, or a y polarized beam of equal intensity. Yet, everybody knows that circularly polarized light is totally different from 45° linearly polarized light.

A right circularly polarized light is a linear combination of x polarized light and y polarized light, where the oscillation of the electric field for the y component is 90° out of phase with the x polarized component.

$$\begin{aligned}
E &= \frac{E_0}{\sqrt{2}} \hat{x} \cos(kz - \omega t) + \frac{E_0}{\sqrt{2}} \hat{y} \cos\left(kz - \omega t + \frac{n}{2}\right) \\
\frac{E}{E_0} &= \frac{1}{\sqrt{2}} \hat{x} e^{i(kz - \omega t)} + \frac{i}{\sqrt{2}} \hat{y} e^{i(kz - \omega t)}
\end{aligned}$$

Similarly, left circularly polarized light is:

$$E = \frac{E_0}{\sqrt{2}} \hat{x} \cos(kz - \omega t) - \frac{E_0}{\sqrt{2}} \hat{y} \cos\left(kz - \omega t + \frac{n}{2}\right)$$

1.2 Observable

An observable is something that we observe.

$$Z\,|z+\rangle = \frac{\mathrm{hbar}}{\sqrt{2}}\,|z+\rangle \qquad Z\,|z-\rangle = \frac{\mathrm{hbar}}{\sqrt{2}}\,|z-\rangle$$

TODO: try to construct an operator that takes a vector $|v\rangle$ to a vector that is orthogonal to it.

1.3 Operators

1.3.1 Projectors — P

Suppose W is a k-dimensional vector subspace of the d-dimensional vector space V.

Using Gram-Schmidt, it is possible to construct an orthonormal basis $|1\rangle, |2\rangle, \ldots |d\rangle$ for V such that $|1\rangle \ldots |k\rangle$ is an orthonormal basis for W. Then the projector P is defined as:

$$P_W \equiv \sum_{i=1}^{k} |i\rangle\langle i|$$

- $P^\dagger = P$ (Immediate from writing in $|i\rangle$ basis)
- $P^2 = P$ (Immediate from writing in $|i\rangle$ basis)

$Q = I - P$ is the projector onto orthogonal complement of the subspace that P. projects into. This projects onto the $|k+1\rangle \ldots |d\rangle$ basis.

1.3.2 Normal operator

$$AA^\dagger = A^\dagger A$$

Theorem 1 *Spectral theorem for normal operators: Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V.*

Proof. Let λ be an eigenvalue of M. P_λ is the projector onto λ's eigenvector. $Q_\lambda = P_\lambda^\perp$ is the orthogonal complement projector of P.

We first establish a fact about PMQ:

$$MM^\dagger |\lambda\rangle = M^\dagger(M|\lambda\rangle) = \lambda M^\dagger \lambda$$
Hence, $M^\dagger v \in P$.
$$Q(M^\dagger P) = 0 \implies (PMQ)^\dagger = 0 \implies PMQ = 0$$

Next, we prove some properties of QM and $QM^\dagger$

$$QM = QM(P+Q) = QMP + QMQ = QMQ$$
$$QM^\dagger = QM^\dagger(P+Q) = QM^\dagger P + QM^\dagger Q = (PMQ)^\dagger + QM^\dagger Q$$

QMQ is normal:

$(QMQ)^\dagger(QMQ) = Q^\dagger M^\dagger Q^\dagger QMQ = QM^\dagger QMQ = QM^\dagger MQ$

$(QMQ)(QMQ)^\dagger = (QMQ)(Q^\dagger M^\dagger Q^\dagger) = QMQM^\dagger Q = QMM^\dagger Q = QM^\dagger MQ = (QMQ)^\dagger QMQ$

$$M = (P+Q)M(P+Q)$$
$$M = PMP + PMQ + QMP + QMQ$$
$$M = PMP + QMQ$$
$$M = \lambda_i |i\rangle\langle i| + QMQ$$
Since QMQ is normal, and we are performing induction on dimension, and $P \perp Q$,
$$M = \lambda_i |i\rangle\langle i| + \sum_k \lambda_k |k\rangle\langle k|$$
Hence M is normal

Theorem 2 *Any diagonalizable operator is normal*

Proof. Let M be diagonal with respect to basis $|i\rangle$. Then, $M \equiv \sum_i \lambda_i |i\rangle\langle i|$. Now, $M^\dagger = \sum_i \lambda_i^* |i\rangle\langle i|$.

$$MM^\dagger = \left(\sum_i \lambda_i |i\rangle\langle i|\right)\left(\sum_j \lambda_j^* |j\rangle\langle j|\right)$$
$$MM^\dagger = \sum_i \lambda_i^* \lambda_i |i\rangle\langle i|$$
$$\text{Similarly,} \quad M^\dagger M = (\sum_i \lambda_i^* \lambda_i |i\rangle\langle i|)$$

1.3.3 Unitary operator

$$UU^\dagger = U^\dagger U = I$$

- unitary operator is normal.
- unitary operator preserves inner products.

$$\langle b' | |a'\rangle = \langle b| U^\dagger U |a\rangle = \langle b| I |a\rangle$$

1.3.4 Positive operator

Special class of Hermitian operator.

$$\forall v \in V, \langle v| A |v\rangle \geqslant 0$$

If the inner product is strictly greater than zero, then such an operator is called as *positive definite*. If it is greater than or equal to zero, it is called *positive semidefinite*.

Theorem 3 *A positive operator is Hermitian*

Proof. **TODO**. Proof most likely follows real case, where we use cholesky to write it as $A^T A$ and then show that it is normal. We then use the fact that its eigenvalues are greater than or equal to zero to establish that it is Hermitian.

Chapter 2

Tensor product states

2.1 Postulates of QM

- Associated to any isolated physical system is a complex vector space with inner product. This space is called as the state space of the system. This system is completely described by its state vector which is a unit vector in the state space.

2.2 Tensor product

Let A and B be vector spaces with bases A_{basis}, B_{basis}. $A \otimes B$ is a *new vector space*, whose basis vectors are $a_i \otimes b_j$ where $a_i \in A_{basis}, b_i \in B_{basis}$.

Properties of the tensor product:

- For any arbitrary scalar z and element $v \in H_a$, $w \in H_b$, $z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$
- $(|v\rangle_1 + |v\rangle_2) \otimes |w\rangle = |v\rangle_1 \otimes |w\rangle + |v\rangle_2 \otimes |w\rangle$
- $|w\rangle \otimes (|v\rangle_1 + |v\rangle_2) = |w\rangle \otimes |v\rangle_1 + |w\rangle \otimes |v\rangle_2$ **TODO: what is an easy way to get correctly sized brackets?**
- Suppose $|v\rangle \in H_a, |w\rangle \in H_b$, and A and B are linear operators on H_a and H_b respectively. $(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv (A|v\rangle) \otimes (B|w\rangle)$.
- Let $C = \sum_i c_i A_i \otimes B_i$, where A_i, B_i are linear operators on H_a, H_b. Now, $C(|v\rangle \otimes |w\rangle) = \sum_i c_i((A_i|v\rangle) \otimes (B_i|w\rangle))$
- $|x\rangle = \sum_i a_i |v\rangle_i \otimes |w\rangle_i$. $|y\rangle = \sum_j b_j |v\rangle_j \otimes |w\rangle_j$. Now, $\langle x|y\rangle = (\sum_i a_i^* \langle v|_i \otimes \langle w|_i)(\sum_j b_j |v\rangle_j \otimes |w\rangle_j)$, which is equal to $\sum_i \sum_i a_i^* b_j \left\langle v_i \middle| v_j' \right\rangle \left\langle w_i \middle| w_j' \right\rangle$

This is way too redundant, **TODO:** write down the slick definition of tensor product spaces seen in John Lee's intro to smooth manifolds, or the definition seen in Tensor Geometry: The Geometric Viewpoint and its uses.

$$\text{tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle i| A|\psi\rangle\langle\psi|i\rangle = \sum_i (\langle\psi|i\rangle)\cdot(\langle i| A|\psi\rangle) = \sum_i \langle\psi|(|i\rangle\langle i|)A|\psi\rangle = \langle\psi| A|\psi\rangle$$

Theorem 4 *Two operators* A, B *are simeltanelously diagonalizable iff* $[A, B] = 0$, *where* $[A, B] = AB - BA$. *That is, there exists a basis where both* A *and* B *are diagonal matrices.*

Proof. One direction of the proof is easy. If two operators are simeltanelously diagonalizable, then we can simply write both operators in this common basis. Diagonal matrices commute, hence $[A, B] = 0$.

Let $|a, j\rangle$ be an orthonormal basis for the eigenspace V_a of A with eigenvalue a and index j to label repeated eigenvalues.

$AB|a, j\rangle = BA|a, j\rangle = aB|a, j\rangle$. Hence, $A(B|a, j\rangle = a(B|a, j\rangle$. Hence, $B|a, j\rangle$ is an eigenvector of A. Therefore, $B|a, j\rangle \in V_a$.

Define projector P_a onto V_a. Now, define $B_a \equiv P_aBP_a$. This is hermitian on V_a, since

$$(P_aBP_a)^\dagger = P_a^\dagger B^\dagger P_a^\dagger = P_aBP_a$$

.

Let us call the eigenvalues of B_a as $|a, b, k\rangle$ where a, b are the eigenvalues of A and B, and K is the degeneracy index.

$P_aB|a, b, k\rangle = b|a, b, k\rangle$, since $B|a, b, k\rangle \in V_a$. **TODO: complete proof**

Lemma 1 $[A, B]^\dagger = [B^\dagger, A^\dagger]$

Proof. $[A, B]^\dagger = (AB - BA)^\dagger = (B^\dagger A^\dagger - A^\dagger B^\dagger) = [B^\dagger, A^\dagger]$

$$\begin{aligned}
&[A, B]^\dagger \\
&= (AB - BA)^\dagger \\
&= (B^\dagger A^\dagger - A^\dagger B^\dagger) \\
&= [B^\dagger, A^\dagger]
\end{aligned}$$

2.3 Postulate 2 of QM: Unitary time evolution

The evolution of a closed quantum system is described by unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to a state $|\psi'\rangle$ at a time t_2 by unitary operator U which depends only on time t_1 and t_2. That is, $|\psi'\rangle = U(t_1, t_2)|\psi\rangle$. We usually suppress t_1, t_2 to write $|\psi'\rangle = U|\psi\rangle$.

Schrodinger equation:

$$i\hbar\frac{\partial\psi}{\partial t} = H|\psi\rangle$$

Homework: Show that the Schrodinger equation implies unitary evolution

2.4 Postulate 3 of QM: Measurement postulate

Quantum measurements are described by a collection $\{M_i\}$ of measurement operators. These operators are acting on the state space of the system which is measured. The index i refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ before the measurement, the probability that the result i occurs is given by:

$$p(i) \equiv \langle\psi| M_i^\dagger M_i |\psi\rangle$$

The state if result i occurs is:

$$|\psi'\rangle = \frac{M_i |\psi\rangle}{\sqrt{p(i)}}$$

We normalize the state $|\psi'\rangle$ to ensure that we evolve Unitarily.
Also, notice that since $\sum_m p(m) = 1$, since $p(m)$ represents probabilities, we can write:

$$\sum_m p(m) = 1 \qquad \langle\psi| \sum_m M_m^\dagger M_m |\psi\rangle = 1 \qquad \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1$$

Since $|\psi\rangle$ is a normalized state, we must have:

$$\sum_m M_m^\dagger M_m = I$$

2.4.1 Projective measurements

A projective measurement is described by an observable M, a hermitian operator on the state space of the system being observed.

Let the observable M have spectral decomposition:

$$M \equiv \sum_m m P_m$$

$$p(m) = \langle\psi| P_m^\dagger P_m |\psi\rangle = \langle\psi| P_m |\psi\rangle$$

$$\mathbb{E}[M] = \sum_m m p(m) = \sum_m m \langle\psi| P_m |\psi\rangle = \langle\psi| \sum_m m P_m |\psi\rangle = \langle\psi| M |\psi\rangle$$

$$\mathbb{E}\left[M^2\right] = \langle\psi| M^2 |\psi\rangle$$

$$V(M) = \mathbb{E}\left[M^2\right] - \mathbb{E}[M]^2 = \langle\psi| M^2 |\psi\rangle - (\langle\psi| M |\psi\rangle)^2$$

2.4.2 Quantum sharing experiment

$$\text{Alice: } \{|\psi_1\rangle, |\psi_2\rangle, \dots\} \xrightarrow{|\psi_i\rangle} \text{Bob: } |\psi_i\rangle$$

Bob has to correctly guess the i that was sent to him. We have two cases: One where $\{|\psi_i\rangle\}$ are orthonormal, the other where they are not.

If the states $\{|\psi_i\rangle\}$ are not orthogonal, then we can prove that there is no quantum measurement that is capable of distinguishing the states.

The idea is that bob will make a measurement M_j with outcome j. Depending on the outcomes of the measurement, bob tries to guess the index i by some rule.

Proof. Consider two non-orthogonal states $|\psi\rangle_1, |\psi\rangle_2$. Assume a measurement is possible by which we can distinguish these two. In other words, if the state $|\psi\rangle_1$ is prepared, then the probability of measuring k such that (????) $f(j) = 1$ (f is our guessing function)

Define some measurement operator $E_i \equiv \sum_{j,\ f(j)=i} M_j^\dagger M_j$

Chapter 3

Quantum deletion

$$\psi = \alpha |0\rangle + \beta |1\rangle$$
$$|\psi\rangle |0\rangle |M\rangle \to |\psi\rangle |\psi\rangle |M\rangle_{\psi}$$
$$(\alpha |0\rangle + \beta |1\rangle) |0\rangle |M\rangle = (\alpha |00\rangle + \beta |10\rangle) |M\rangle$$

Cloning is possible upto fidelity 0.83. We get a similar theorem for quantum deletion — in that, we can perform approximate deletion.

If ψ_1, ψ_2 are two non-orthogonal states, then there is no deletion machine by which we can delete one copy from two cpies of of ψ_1 and ψ_2

$$\psi_1\psi_1 \to \psi_1\Sigma$$
$$\psi_2\psi_2 \to \psi_2\Sigma$$
$$\langle\psi_1|\psi_2\rangle^2 = \langle\psi_1|\psi_2\rangle \langle\Sigma|\Sigma\rangle$$
$$(\langle\psi_1|\psi_2\rangle - 1) \langle\psi_1|\psi_2\rangle = 0$$

Hence $\langle\psi_1|\psi_2\rangle = 0 \vee 1$

3.1 No flipping

One of the strongest impossible operations. Given a state $|\psi\rangle$, we cannot make a state that takes it to an orthogonal state $|\overline{\psi}\rangle$.

(Take a state $a0 + b1$ to $-b0 + a1$?)

3.2 No partial erasure

$|\psi(\theta, \phi)\rangle \to |\psi'(\theta)\rangle |\Sigma\rangle$ is impossible, where $\psi(\theta, \phi)$ is the parametrisation of a 2 qubit state on a bloch sphere.

3.3 No splitting

We cannot split quantum information. $|\psi(\theta, \phi)\rangle \rightarrow |\psi'(\theta)\rangle |\Sigma'(\phi)\rangle$ is impossible. That is, we cannot split the combined information in (θ, ϕ) into two separate pieces of data.

Chapter 4

Clasical information theory

Book recommendation: Elements of Information theory — JJ Thomas and Thomas Cover.

4.1 What is information

Entropy Blah blah blah, define surprisal of a probability

$$I : [0, 1] \to \mathbb{R} \quad I(p) = -\log p$$

Now, entropy of a random variable X is:

$$\mathbb{H} : \text{Random variable} \to \mathbb{R} \quad \mathbb{H}(X) \equiv \sum_{x \in X} p(x) I\left(p(x)\right)$$

Conditional entropy

$$\mathbb{H} : \text{Random variable} \times \text{Random variable} \to \mathbb{R} \quad \mathbb{H}(Y|X) \equiv \sum_{x \in X} p(x) H(Y|X = x)$$

It can be shown that $\mathbb{H}(X, Y) = \mathbb{H}(X) + \mathbb{H}(Y|X)$

Mutual information

$$\begin{aligned} I(X; Y) &\equiv H(X) - H(X|Y) \\ &= H(X) - [H(X, Y) - H(Y)] \\ &= H(X) + H(Y) - H(X, Y) \end{aligned}$$

It is a measure of the reduction of uncertainty in X upon knowing Y.

Relative entropy / K-L divergence Suppose there are two probability distributions $P(x)$ and $Q(x)$. The relative entropy is:

$$H\left(p(x)\|q(x)\right) \equiv \sum_{x\in X} p(x)\log\frac{p(x)}{q(x)}$$

Theorem 5 *K-L divergence is always positive. That is,* $H(p(x)\|q(x)) \geqslant 0$*, with* $H(p(x)\|q(x)) = 0 \iff p(x) = q(x)$

Proof.

$$\begin{aligned} H(p(x)\|q(x)) &= \sum_{x\in X} p(x)\log\left(\frac{p(x)}{q(x)}\right) \\ &= -\sum_{x\in X} p(x)\log\left(\frac{q(x)}{p(x)}\right) \end{aligned}$$

We know that $\log x \leqslant \frac{x-1}{\ln 2}$. Hence, $-\log x \geqslant \frac{1-x}{\ln 2}$.

$$\begin{aligned} H(p(x)\|q(x)) &= -\sum_{x\in X} p(x)\log\left(\frac{q(x)}{p(x)}\right) \\ &\geqslant \frac{1}{\ln 2}\sum_{x\in X} p(x)\left(1-\frac{q(x)}{p(x)}\right) \\ &\geqslant \frac{1}{\ln 2}\sum_{x\in X} (p(x)-q(x)) \\ &\geqslant \frac{1}{\ln 2}(1-1) = 0 \end{aligned}$$

Chapter 5

Quantum Entropy

5.1 Quantum relative entropy

$$S(\rho||\sigma) \equiv \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$$

This is a meaausre of entanglement.

$$\varepsilon(\rho) = \min_{delta} S(\rho||\delta)$$

We will now prove that this value is always non negative. $S(\rho||\sigma) \geqslant 0$.

$$\rho = \sum_i p_i |i\rangle \langle i| \quad \sigma = \sum_j q_j |j\rangle \langle j|$$

$$S(\rho||\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma) = \sum_i p_i \log p_i - \sum_i \langle i| \rho \log \sigma |i\rangle$$

Notice that $\langle i| \rho = p_i \langle i|$. Substituting,

$$\langle i| \log \sigma |i\rangle = p_i \langle i| \log \sigma |i\rangle = \langle i| \left(\sum_j \log(q_j) |j\rangle \langle j| \right) |i\rangle = \sum_j \log q_j \langle i|j\rangle \langle j|i\rangle$$

Let $P_{ij} \equiv \langle i|j\rangle \langle j|i\rangle$

$$S(\rho||\sigma) = \sum_i p_i \log p_i - \sum_i p_i \langle i| \rho \log \sigma |i\rangle = \sum_i p_i \left(\log p_i - \sum_j \log q_j P_{ij} \right)$$

Since $\log(\cdot)$ is a concave function,

$$-\sum_j P_{ij} \log q_j \geqslant -\log r_i \quad \text{where } r_i \equiv \sum_j P_{ij} q_j$$

$$S(\rho||\sigma) = \sum p_i \left(\log p_i - \sum_j P_{ij} \log q_j \right) \geqslant \sum_i p_i (\log p_i - \log r_i) = H(p_i||r_i)$$

Note that $H(p_i||r_i) = 0 \iff \forall i,\ p_i = r_i$

- The entropy is non-negative. It is 0 iff the state is pure.
- In a d dimensional hilbert space, the entropy is at most $\log d$
- The entropy is $\log d$ when the system is completely mixed. That is, I/d. (*white noise*)
- For a composite system AB, $S(A) = S(B)$
- $S(\sum_i p_i \rho_i) = H(p_i) = \sum_i p_i S(rho_i)$
- Suppose p_i are the probabilities for $\{|i\rangle\}$, and ρ_i are any density operators of system B. $S(\sum_i p_i |i\rangle \langle i| \otimes \rho_i) = H(p_i) + \sum_i p_i S(\rho_i)$

$$
\begin{aligned}
&S(\rho || I/d) = -S(\rho) - \mathrm{tr}(\rho \log(I/d)) \geqslant 0 \\
&-S\rho - \log(1/d) \,\mathrm{tr}\, \rho \geqslant 0 \\
&-S(\rho) + \log d \geqslant 0 \\
&S(\rho) \leqslant \log(d)
\end{aligned}
$$

Let λ_i^d and $|e_i^d\rangle$ be the eigenvalues and eigenvectors of ρ_i. Observe that $p_i \lambda_i^j$ and $\left|e_i^j\right\rangle$ are eigenvalues and eigenvectors of $\sum_i p_i \rho_i$.

$$
\begin{aligned}
S\left(\sum_i p_i \rho_i\right) &= \sum_{ij} p_i \lambda_i^j \log\left(p_i \lambda_i^j\right) \\
&= -\sum_i p_i \log p_i + \sum p_i (-sum_j \lambda_i^j log \lambda_i^j \\
&= H(p_i) + \sum p_i S(\rho_i)
\end{aligned}
$$

Chapter 6

Locality

$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - \mathrm{ket}10_{AB}\right)$

Ontological model: Something in the background which is controlling stuff that goes on in the foreground. Einstein was convinced that there are some hidden variables in the ontological model which give rise to quantum weirdness. Particularly, there is a *hidden variable* λ. It is an unknown variable that is present to describe ψ, but we are unable to measure / access it. That is, our state is $|\psi(x, \lambda)\rangle$

Any local, realistic, hidden variable model can be shown to satisfy an inequality which at first glance seems absurd. However, it was later shown experimentally that QM does not satisfy this inequality. QM can also be explained with a non-local, deterministic, hidden variable theory (pilot wave theory). (Note to self: Go read the axioms sometime).

Any local realistic model will have ($\mathrm{lhs} \leqslant 2$). Quantum mechanics can hit ($\mathrm{lhs} = 2\sqrt{2}$). The inequality by construction can go up to 4. There are stronger correlations (example, PR-box) which can hit 4.

There is a polytope (no signalling polytope) in which PR-box is a vertex.

6.1 Bell's inequality

```
A <-C-> B
```

Bell's inequality has nothing to do with QM. It is a purely mathematical construction that is *independent* of QM.

Imagine Alice recieves her particle and does a measurement on it. Imagine that she has two different measurement apparatus, and she chooses to perform one of the two different measurements (P_Q and P_R). Bob has two measurements as well, and he can perform one of the measurements (P_S and P_T). The measurements to be done are chosen with uniform probability $1/2$.

To make things simple, let the measurement outcomes be $+1, -1$.

Reality Q, R, S, T are objective values of the particle. That is, these values exist independent of measurement

Locality Any action performed by Alice cannot affect measurements performed by Bob.

The Inequality Now consider the function $QS + RS + RT - QT = (R + Q)S + (R - Q)T$. Note that each of Q, R, S, T can be ± 1. Hence, the maximum value it can reach is 2 (TODO: prove).

$P(q, r, s, t)$ is the probability of $(Q = q, R = r, S = s, T = t)$. $\mathbb{E}[QS + RS + RT - QT] = \mathbb{E}[QS] + \mathbb{E}[RS] + \mathbb{E}[RT] - \mathbb{E}[QT] \leqslant 2$.

Now, for the QM side of the story.

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad Q = Z_1 \quad R = X_1 \quad S = \frac{-Z_2 - X_2}{\sqrt{2}} \quad T = \frac{Z_2 - X_2}{\sqrt{2}}$$
$$\mathbb{E}[QS + RS + RT - QT] = 2\sqrt{2}$$

This clearly violates bell's inequality. So, we ned to lose either reality or locality in QM (and understand which one is lost).

6.2 Measures of Entangelement

Consider a state in superposition $(\alpha|0\rangle + \beta|1\rangle)$. If a state $\psi \neq |\phi_1\rangle \otimes |\phi_2\rangle \, \forall \phi_1, \phi_2$, then ψ is entangled.

For mixed state, $\rho \geqslant 0$, $\mathrm{Tr}(r) = 1$. We have the inequality that $\mathrm{Tr}(\rho^2) = 1$ for a pure state, and $\mathrm{Tr}(\rho^2) < 1$ for a mixed state.

Let $(\rho \neq \sum_i p_i \rho_i^A \otimes \rho_i^B)$ where the ρ_i are pure states. So now the question is, how do we detect if such a ρ contain entanglement. Let the states have dimensionality d_a and d_b.

6.3 Detecting Entanglement

6.3.1 PPT criteria (Positive Partial Transposition)

$\rho_{AB} \to \rho_{AB}^{T_{A(B)}}$. $T_{A(B)}(|pq\rangle\langle xy|) \equiv |xq\rangle\langle py|$. If it remains a density matrix which is positive, then it is called PPT. If it is not positive, then it is called NPT, and is known to be entangled (sufficient). The condition is necessary and sufficient for dimensions $2 \otimes 2$, $2 \otimes 3$. The intuition is that when we perform transposition for these dimensions, we will always get negative eigenvalues.

Note that this is not physically realisable. It is physically realised by adding white noise. This is called structural physical approximation. It then becomes a complete positive map. (TODO: what are the definitions of these words?)

6.3.2 Entanglement Witness

The Hahn-banach theorem states that for any convex, compact set and a given point, either the point lies within the set, or one can construct a hyperplane which separates the set from the point. (We only need to invoke Hahn banach in the infinite dimensional case. For the finite dimensional case, Farkas lemma works)

6.4 Quantification of Entanglement

A function $Q : M(\mathbb{C}) \to \mathbb{R}$ is said to be an entanglement quantifier iff:

- For separable states ρ, $Q(\rho) = 0$.
- Constant under local unitary: $Q(LU(\rho)) = Q(\rho)$
- Under LOCC, $Q(LOCC(\rho)) \leqslant Q(\rho)$
- (Desirable) Convex under classical mixing: $Q\left(\sum_i p_i \rho_i\right) \leqslant \sum_i p_i Q(\rho_i)$. That is, states can lose entanglement under classical mixing.
- (Desirable) Additive: $Q(\rho \otimes \sigma) = Q(\rho) + Q(\sigma)$
- (Desirable) Continuity: $\lim_{n\to\infty} \left\langle \psi^{\otimes n} \right| \rho^{\otimes n} \left| \psi^{\otimes n} \right\rangle \to 1$

Chapter 7

Quantum Computing: Simon's Problem

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$. There exists an (unknown to us) $s \in \{0,1\}^n$.

We are promised that:

- $\forall x \in \{0,1\}^n,\ f(x \oplus s) = f(x)$.
- $f(y) = f(x) \iff [y = x \oplus s] \vee [y = x]$.

Goal is to find s.

$$f(y \oplus x) = f((y \oplus s) \oplus (x \oplus s))$$

Supppose we have checked f for $y_1, y_2, \ldots y_k$. For each pair, have a trial $s_{i,j} = y_i \oplus y_j$. If $y_i = y_j$, then $s = s_{i,j}$.

What's the runtime? We can find a lower bound. There are $\frac{k(k-1)}{2}$ pairs, but some $s_{i,j}$ may be the same.

$$\frac{k^2}{2} > \frac{k(k-1)}{2} > 2^n > \frac{2^n}{2} \qquad k > \sqrt{2^n}$$

Classically, we will need to perform at least $\sqrt{2^n}$ tests.

7.1 Quantum solution

We will create a linear algorithm.

$$\begin{aligned}
|\psi_1\rangle &\equiv |0\rangle^{\otimes n} |0\rangle^{\otimes n} \\
|\psi_2\rangle &\equiv \mathbb{H}^{\otimes n} \otimes I^{\otimes n}(\psi_1) = 2^{\frac{-n}{2}} \sum_{y \in 0,1^n} |y\rangle |0\rangle^{\otimes n} \\
|\psi_3\rangle &\equiv U_f(\psi_2) = 2^{\frac{-n}{2}} \sum_{y \in \{0,1\}^n} |y\rangle |f(y)\rangle
\end{aligned}$$

Notice that since f is two-to-one, for every component $|f(y)\rangle$ of the second qubit, we will have first qubits: $|y\rangle, |y \oplus s\rangle$.

$$|\psi_3\rangle \equiv 2^{\frac{-n}{2}} \sum_{y \in \{0,1\}^n} \frac{(|y\rangle + |y \oplus s\rangle)\,|f(y)\rangle}{2}$$

We divide by two since we are double counting the pair $(y, y \oplus s)$, since later we will hit $(y' \equiv y \oplus s, y' \oplus s = y \oplus s \oplus s = y)$.

We now measure the second qubit:

$$|\psi_4\rangle \equiv M(\psi_3) = \frac{|y\rangle + |y \oplus s\rangle}{\sqrt{2}} \qquad \text{(for some } y \text{ with prob. } 2^{-(n-1)}\text{)}$$

We next apply hadamard to $|\psi_4\rangle$, which we will write using the identity:

$$H^{\otimes n}|x\rangle \equiv 2^{\frac{-n}{2}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z}|z\rangle$$

Here, $x \cdot y \equiv$ inner product over $\mathbb{Z}/2\mathbb{Z}$.

$$|\psi_5\rangle \equiv H^{\otimes n}(\psi_4) = \frac{\sum_{z \in \{0,1\}^n}\left((-1)^{y \cdot z} + (-1)^{(y \oplus s) \cdot z}\right)|z\rangle}{2^{-\frac{n-1}{2}}}$$
$$= \frac{\sum_{z \in \{0,1\}^n}\left((-1)^{y \cdot z}\left[1 + (-1)^{(s \cdot z)}\right]\right)|z\rangle}{2^{-\frac{n-1}{2}}}$$

If $(s.z = 1)$, then the coefficient $1 + (-1)^{s \cdot z} = 1 - 1 = 0$. So, we will only get $|z\rangle$ which have $(s.z = 0)$.

Using this, we can get z's such that $(s.z) = 0$.We can gather $(n-1)$ of these and solve the system $(s.z_i) = 0$ for s.

7.2 Probability computation

Next, we perform some probability computations to check how many of the vectors will be linearly independent. The number of matrices is $2^{n \times (n-1)}$.

Now, we need to check that this matrix is invertible for the system of linear equations to be solvable. Note that for the first vector z_1, only the zero vector is not allowed. So, the number of z_1's is $(2^n - 1)$. Now, the second vector z_2 must be linearly independent of the first vector z_1, for which we have $(2^n - 2)$ choices, since we must remove the 2 vectors that are linearly dependent on z_1. For z_3, we need to eliminate the 4 vectors that are combinations of z_1, z_2. So, number of choices for z_3 will be $(2^n - 2^2)$. For z_i, we will have $(2^n - 2^{i-1})$.

Total:

$$\frac{\prod_{i=1}^{n}(2^n - 2^{i-1})}{2^{n \times (n-1)}} > \frac{1}{4}$$