

# Quantum computation and information - Indranil Chakravarty

Siddharth Bhat



# Contents

<b>1</b>	<b>Lecture 1: Introduction</b>	<b>5</b>
1.1	Stern-Gerlach: A brief, morally correct construction of qubits . . . . .	6
1.1.1	Analogy with polarization of light . . . . .	6
1.2	Observable . . . . .	8
1.3	Operators . . . . .	9
1.3.1	Projectors — $P$ . . . . .	9
1.3.2	Normal operator . . . . .	9
1.3.3	Unitary operator . . . . .	10
1.3.4	Positive operator . . . . .	10
<b>2</b>	<b>Tensor product states</b>	<b>11</b>
2.1	Postulates of QM . . . . .	11
2.2	Tensor product . . . . .	11
2.3	Postulate 2 of QM: Unitary time evolution . . . . .	12
2.4	Postulate 3 of QM: Measurement postulate . . . . .	13
2.4.1	Projective measurements . . . . .	13
2.4.2	Quantum sharing experiment . . . . .	13



# Chapter 1

## Lecture 1: Introduction

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

Topics:

- Intro: Transition from Classical to Quantum: Stern Gerlach, Sequential Stern Gerlach, 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 Schumahir(?) 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 Computing, Pauli gates, Hadamard gates, Universal gates, Quantum algorithms (Shor, Grover search, machine learning and optimisation).
- Quantum programming: Programming quantum algorithms, Q# programming 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  $\rightarrow [z] \rightarrow (z+, z-) \rightarrow \text{block } (z-) \rightarrow [x] \rightarrow (x+, x-) \rightarrow \text{block } (x-) \rightarrow [z] \rightarrow (z+, z-?)$

$[z]$  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:

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

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

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:

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

$z_+ \equiv x$  polarization

$z_- \equiv y$  polarization

$x_+ \equiv x'$  polarization

$x_- \equiv y'$  polarization

This problem can be solved again by polarization of light. This time, we consider circularly polarized light which can be obtained by letting linearly 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  $45^\circ$  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  $90^\circ$  out of phase with the  $x$  polarized component.

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

$$\frac{E}{E_0} = \frac{1}{\sqrt{2}} \hat{x} e^{i(kz - \omega t)} + \frac{i}{\sqrt{2}} \hat{y} e^{i(kz - \omega t)}$$

Similarly, left circularly polarized light is:

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

## 1.2 Observable

An observable is something that we observe.

$$Z|z+\rangle = \frac{\hbar}{\sqrt{2}}|z+\rangle \quad Z|z-\rangle = \frac{\hbar}{\sqrt{2}}|z-\rangle$$

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  $|1\rangle, |2\rangle, \dots, |d\rangle$  for  $V$  such that  $|1\rangle \dots |k\rangle$  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  $|k+1\rangle \dots |d\rangle$  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  $\lambda$  be an eigenvalue of  $M$ .  $P_\lambda$  is the projector onto  $\lambda$ 's eigenvector.  $Q_\lambda = P_\lambda^\perp$  is the orthogonal complement projector of  $P$ .

We first establish a fact about  $PMQ$ :

$$MM^\dagger |\lambda\rangle = M^\dagger (M |\lambda\rangle) = \lambda M^\dagger |\lambda\rangle$$

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  $QM^\dagger$

$$\begin{aligned} QM &= QM(P + Q) = QMP + QMQ = QMQ \\ QM^\dagger &= QM^\dagger(P + Q) = QM^\dagger P + QM^\dagger Q = (PMQ)^\dagger + QM^\dagger Q \end{aligned}$$

$QMQ$  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,  $M^\dagger = \sum_i \lambda_i^* |i\rangle\langle i|$ .

$$MM^\dagger = \left( \sum_i \lambda_i |i\rangle\langle i| \right) \left( \sum_j \lambda_j^* |j\rangle\langle j| \right)$$

$$MM^\dagger = \sum_i \lambda_i^* \lambda_i |i\rangle\langle i|$$

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

### 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.

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

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  $A_{\text{basis}}, B_{\text{basis}}$ .  $A(X)B$  is a *new vector space*, whose basis vectors are  $a_i(X)b_j$  where  $a_i \in A_{\text{basis}}, b_i \in B_{\text{basis}}$ .

Properties of the tensor product:

- For any arbitrary scalar  $z$  and element  $v \in H_a, w \in H_b$ ,  $z(|v\rangle(X)|w\rangle) = (z|v\rangle)(X)|w\rangle = |v\rangle(X)(z|w\rangle)$
- $(|v\rangle_1 + |v\rangle_2)(X)|w\rangle = |v\rangle_1(X)|w\rangle + |v\rangle_2(X)|w\rangle$
- $|w\rangle(X)(|v\rangle_1 + |v\rangle_2) = |w\rangle(X)|v\rangle_1 + |w\rangle(X)|v\rangle_2$  **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.  $(A(X)B)(|v\rangle(X)|w\rangle) \equiv (A|v\rangle)(X)(B|w\rangle)$ .
- Let  $C = \sum_i c_i A_i(X)B_i$ , where  $A_i, B_i$  are linear operators on  $H_a, H_b$ . Now,  $C(|v\rangle(X)|w\rangle) = \sum_i c_i((A_i|v\rangle)(X)(B_i|w\rangle))$
- $|x\rangle = \sum_i a_i |v\rangle_i(X)|w\rangle_i, |y\rangle = \sum_j b_j |v\rangle_j(X)|w\rangle_j$ . Now,  $\langle x|y\rangle = (\sum_i a_i^* \langle v|_i(X)\langle w|_i)(\sum_j b_j |v\rangle_j(X)|w\rangle_j)$ , which is equal to  $\sum_i \sum_j a_i^* b_j \langle v_i|v'_j\rangle \langle w_i|w'_j\rangle$

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 simultaneously 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 simultaneously 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  $B_a \equiv P_a B P_a$ . This is hermitian on  $V_a$ , since

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

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.

$P_a B|a, b, k\rangle = b|a, b, k\rangle$ , 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:

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

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:

$$M \equiv \sum_m m P_m$$

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

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

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

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

### 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.