define@key

Lectures on Quantum Computing and Completely Positive Maps

Vern Paulsen
Notes by Brandon Lee

December 16, 2011

Contents

1 Preface

These are an unedited transcription of lectures I gave at the University of Houston in the Fall of 2011 and should not be circulated widely. This was my first time teaching this material and there are a number of mistakes, etc., that need to be corrected before I show them to a broader audience. The attendees at the IMSC short course on QC in Chennai are welcome to read these, but I ask that they not post them to any other websites.

My only hope is that they will give the attendees some supplementary material that will inform more than they misinform!

Vern Paulsen, Houston

2 Day - 22/Aug/11

2.1 Computing Overview

Classical (binary)	Quantum
Bit - $\{0,1\} = \mathbb{Z}_2$; "on/off"	*Qubit* - unit vector in $\mathbb{C}^2$; electron/photon; $\uparrow = (1,0)$, $\rightarrow = (0,1)$, $\circlearrowleft = \frac{1}{\sqrt{2}}(1,i)$
N *bits* - element of $\mathbb{Z}_2^N$	N *qubit* - unit vector in $\mathbb{C}^{2^N} \cong \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ (N times)
Operations - flip, register shifts	*Operations* - completely positive maps on M_{2^N}
Information Theory - 2^N states; $(P_1, \ldots, P_N)$, $P_i \geq 0$, $P_1 + \ldots + P_{2^N} = 1$	*Information Theory* - P $2^N \times 2^N$ positive; semidefinition matrices with $tr(P) = 1$

2.2 Course Overview

I. Basic Math

- Hilbert spaces, matrices, and linear maps
- Positive definite matrices
- Tensor products

II. Introduction to Quantum Computing

- Axioms of quantum mechanics
- Classical vs. quantum gates
- Quantum algorithms
- Introduction to entanglement

III. Theory of Completely Positive Maps

IV. Entanglement

- Entanglement witnesses

V. Topics

- Quantum error correction
- Quantum coding
- Quanum cryptography

2.3 References

1. Michael Nielsen/Isaac Chuang - "Quantum Computation and Quantum Information" (Cambridge University Press)
2. S.J Lomonaco (editor) - "Quantum Computation, A Grand Mathematical Challenge for the 21st Century" (AMS)
3. John Preskill - "Quantum Computation" (Online lecture notes at http://www.theory.caltech.edu/people/preskill/ph229)
4. P. Kaya, R. Laflamme, M. Mosca - "An Introduction to Quantum Computing" (Oxford University Press)

2.4 Basic Math I

Note. We adopt the notation of physicists.

Example. Let $\mathbb{C}^n$ be the space of complex n-tuples; i.e.,

$$\mathbb{C}^n = \{x = (x_1, \ldots, x_n) \,:\, x_i \in \mathbb{C}\}$$

and define

$$\alpha x = (\alpha x_1, \ldots, \alpha x_n),$$

for any $\alpha \in \mathbb{C}$, $x \in \mathbb{C}^n$. $\mathbb{C}^n$ has an inner product defined by

$$\langle y|x\rangle = \sum_{i=1}^{n} \overline{y}_i x_i.$$

$\langle \cdot|\cdot \rangle$ has the following properties:

- Linear in RHS: $\langle y|x + x'\rangle = \langle y|x\rangle + \langle y|x'\rangle$ and $\langle y|\alpha x\rangle = \alpha\langle y|x\rangle$;
- Conjugate linear in LHS (called "sesquilinear"): $\langle y + y'|x\rangle = \langle y|x\rangle + \langle y'|x\rangle$ and $\langle \alpha y|x\rangle = \overline{\alpha}\langle y|x\rangle$;
- Positive definite : $\langle x|x\rangle \geq 0$ and $\langle x|x\rangle = 0 \Leftrightarrow x = 0$;

- Euclidean length: Define $||x|| = \sqrt{\langle x|x\rangle}$ for all $x \in \mathbb{C}^n$. Then $||\cdot||$ is a norm satisfying $||x+y|| \leq ||x|| + ||y||$, $||\alpha x|| = |\alpha|||x||$ for all $\alpha \in \mathbb{C}$, $x, y \in \mathbb{C}^n$.

Definition. A *Hilbert space* is a complex vector space $\mathcal{H}$ equipped with a map

$$\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

that is sesquilinear, positive definite, and $\mathcal{H}$ is complete with respect to the norm $||x|| = \sqrt{\langle x|x\rangle}$.

Examples. (1) $\mathbb{C}^n$, as above.

(2) The space of matrices $M_{n,k} = \{(t_{ij}) : t_{ij} \in \mathbb{C}, 1 \leq i \leq n, 1 \leq j \leq k\}$, where n is the number of rows and k is the number of columns. $M_{n,k}$ is equipped with the inner product defined by

$$\langle (y_{ij})|(x_{ij})\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{y}_{ij}x_{ij}.$$

We note that $M_{n,k} \cong \mathbb{C}^{nk}$.

3 Day - 24/Aug/11

3.1 Examples of Hilbert Spaces

Example. $\mathbb{C}^n$ is a Hilbert space with inner product

$$\langle y|x\rangle = \sum_{i=1}^{n} \overline{y}_i x_i,$$

where $y = (y_1, \ldots, y_n), x = (x_1, \ldots, x_n) \in \mathbb{C}^n$. $\mathbb{C}^n$ has an orthonormal basis defined by

$$e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1),$$

and for all $x \in \mathbb{C}^n$,

$$x = \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} \langle e_i|x\rangle e_i.$$

Example. The $n \times m$ matrices, $M_{n,m}$, is a Hilbert space with inner product

$$\langle (y_{ij})|(x_{ij})\rangle = \sum_{i,j} \overline{y}_{ij}x_{ij}.$$

$M_{n,m}$ has as an orthonormal basis the set of matrix units defined by

$$E_{ij} = \begin{cases} 1, & (i,j)^{th}\ entry, \\ 0, & otherwise. \end{cases}$$

For all $X \in M_{n,m}$,

$$X = \sum_{i,j} X_{ij}E_{ij} = \sum_{i,j} \langle E_{ij}|X\rangle E_{ij}.$$

3.2 Matrices

Definition. Let $X = (x_{ij}) \in M_{n,m}$. We define the following:

1. *Conjugate* matrix: $\overline{X} = (\overline{x}_{ij})$.
2. *Transpose* matrix: $X^t = (x_{ij})^t = (x_{ji})$.
3. *Conjugate Transpose* or *Adjoint* matrix: $X^* = \overline{X}^t = (\overline{x}_{ij})^t$. (Note that physicist denote this by $X^\dagger = X^*$.)

Matrix Multiplication. Let $X = (x_{ij}) \in M_{n,m}$ and $Y = (y_{ij}) \in M_{m,p}$. Then,

$$XY = \left(\sum_k x_{ik} y_{kj} \right) \in M_{n,p}.$$

If we write

$$X = \begin{pmatrix} R_1 \\ \cdots \\ \vdots \\ \cdots \\ R_n \end{pmatrix}, Y = (C_1 \vdots \ldots \vdots C_p),$$

as matrices of row and column vectors, then

$$XY = (R_i \cdot C_j),$$

where "$\cdot$" is the usual dot product.

Definition. Define the mapping $Tr : M_{n,n} \to \mathbb{C}$ by $Tr(X) = \sum_{i=1}^n x_{ii}$. Tr is called the *trace* of X. We sometimes write Tr_n for the trace of $M_{n,n}$.

3.3 Physicists Bra-Ket Notation

Notation. Let $x, y \in \mathbb{C}^n$. Define

$$|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and

$$\langle y| = |y\rangle^* = (\overline{y}_1, \ldots, \overline{y}_n).$$

Then,

$$\langle y|x\rangle = (\overline{y}_1, \ldots, \overline{y}_n) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and

$$|x\rangle \langle y| = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot (\overline{y}_1, \ldots, \overline{y}_n) = (x_i \overline{y}_j) \in M_{n,n}.$$

In addition, physicists prefer to number by $0, 1, \ldots, n-1$ instead of $1, 2, \ldots, n$. In this numbering scheme, the canonical orthonormal basis of $\mathbb{C}^n$ is $e_0, \ldots, e_{n-1}$. We can also write this bases by

$$|e_j\rangle = |j\rangle ,$$

for all j. So, the canonical orthonormal basis is $|0\rangle , \ldots , |n-1\rangle$.

Note also that

$$\begin{aligned} |x\rangle &= \sum_{i=0}^{n-1} \langle e_i|x\rangle \cdot |e_i\rangle \\ &= \left[\sum_{i=0}^{n-1} |e_i\rangle \langle e_i| \right] |x\rangle \\ &= I_n |x\rangle . \end{aligned}$$

3.4 Matrices and Linear Maps

Definition. $T : \mathbb{C}^k \to \mathbb{C}^n$ is *linear* if

$$T(x+y) = T(x) + T(y)$$

and

$$T(\alpha x) = \alpha T(x).$$

We denote by $\mathcal{L}(\mathbb{C}^k, \mathbb{C}^n)$ to be the space of all linear maps from $\mathbb{C}^k$ to $\mathbb{C}^n$.

Remark. Each $n \times k$ matrix $A = (a_{ij})$ defines a linear map from $\mathbb{C}^k$ to $\mathbb{C}^n$ by matrix multiplication:

$$\begin{aligned} A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} &= \begin{pmatrix} \sum_{i=1}^k a_{1i} x_i \\ \vdots \\ \sum_{i=1}^k a_{n_i} x_i \end{pmatrix} \\ &= \begin{pmatrix} R_1 \cdot x \\ \vdots \\ R_n \cdot x \end{pmatrix}. \end{aligned}$$

Every linear map T is multiplication by the matrix

$$\langle e_i | T e_j \rangle = \langle i | T | j \rangle .$$

3.5 Matrix Theory

Orthogonal Projections. Let $V \subseteq \mathbb{C}^n$ be a subspace with $dim(V) = k < n$. Pick an orthonormal basis $\{v_1, \ldots, v_k\}$ for V. Let $P = \sum_{i=1}^{k} |v_i\rangle \langle v_i|$. Then,

$$Px = \sum_{i=1}^{k} \langle v_i|x\rangle v_i \in V.$$

Also,

$$\begin{aligned} \langle v_j|x - Px\rangle &= \langle v_j|x\rangle - \left\langle v_j| \sum_{i=1}^{k} \langle v_i|x\rangle v_i \right\rangle \\ &= \langle v_j|x\rangle - \sum_{i=1}^{k} \langle v_i|x\rangle \langle v_j|v_i\rangle \\ &= \langle v_j|x\rangle - \langle v_j|x\rangle \\ &= 0. \end{aligned}$$

So, $v_j \perp (x - Px)$ for all j. This implies that $(x - Px) \perp V$. Therefore, $x = Px + (x - Px)$, where $Px \in V$ and $(x - Px) \in V^{\perp}$. Hence, we have shown that any $x \in \mathbb{C}^n$ can be written as $x = v + w$, where $v \in V$ and $w \in V^{\perp}$.

We claim that this decomposition is unique. Suppose x can also be written as $x = v_1 + w_1$, where $v_1 \in V$ and $w_1 \in V^{\perp}$. Then,

$$\begin{aligned} v + w = v_1 + w_1 &\Rightarrow v - v_1 = w_1 - w \\ &\Rightarrow v - v_1 = w_1 - w = 0 \\ &\Rightarrow v = v_1, w = w_1. \end{aligned}$$

Thus, Px and $x - Px$ is the unique decomposition of writing x.

Now, suppose we picked a different orthonormal basis for V, say $\{\tilde{v}_1, \ldots, \tilde{v}_k\}$ and formed

$$\tilde{P} = \sum_{i=1}^{k} |\tilde{v}_i\rangle \langle \tilde{v}_i| .$$

By uniqueness, $\tilde{P} = P$. Note also that if $v \in V$, then by uniqueness, $Pv = v$.

We summarize: Given $V \subseteq \mathbb{C}^n$, pick any orthonormal basis. Then

$$Px = \sum_{i=1}^{k} |v_i\rangle \langle v_i| x$$

is the unique orthonormal projection onto V.

Parseval. If $v \in V$ and $\{v_1, \ldots, v_k\}$ is an orthonormal basis, then $v = \sum_{i=1}^{k} \langle v_i|v\rangle v_i$. Then,

$$||v||^2 = \left|\left| \sum_{i=1}^{k} \langle v_i|v\rangle v_i \right|\right|^2 = \sum_{i=1}^{k} |\langle v_i|v\rangle|^2.$$

If we take $V = \mathbb{C}^n$, this says that if $\{v_1, \ldots, v_n\}$ is any orthonormal basis, then

$$||v||^2 = \sum_{i=1}^{n} |\langle v_i|v\rangle|^2.$$

Other Properties of P.

1. $P^2 = P$.
2. $P = P^*$. This is because $P = \sum_{i=1}^{k} |v_i\rangle \langle v_i|$ and, for any vector x,

$$|x\rangle \langle x| = (x_i \overline{x}_j) = (x_i \overline{x}_j)^*.$$

Theorem. If $P \in M_n$ such that $P^2 = P$ and $P = P^*$, and if we let $V = range(P)$, then P is the orthogonal projection onto V.

Proof. For $v \in V$, then $v = Px$. So, $Pv = P(Px) = P^2x = Px = v$. If $w \perp V$, then

$$\begin{aligned} ||Pw||^2 &= \langle Pw|Pw\rangle \\ &= \langle w|P^*Pw\rangle \\ &= \langle w|Pw\rangle \\ &= 0. \end{aligned}$$

Therefore, P is the orthogonal projection onto V.

4 Day - 31/Aug/11

4.1 Unitary Matrices

Definition. $U \in M_n$ is *unitary* if $U^*U = I$.

Theorem. For $U \in M_n$, the following are equivalent:

(a) U is unitary.

(b) U is invertible and $U^{-1} = U^*$.

(c) $UU^* = I$.

(d) U^* is unitary.

(e) The columns of U are orthonormal.

(f) The rows of U are orthonormal.

(g) (*Isometry*) $||Ux|| = ||x||$ for all $x \in \mathbb{C}^n$.

(h) (*Inner product preserving*) $\langle Ux|Uy\rangle = \langle x|y\rangle$ for all $x, y \in \mathbb{C}^n$.

Proof. $((a) \Rightarrow (b))$: U^* is a left inverse implies U is one-to-one. So, $dim(rg(U)) = n$, and so, U is onto. Hence, U is invertible and U^* is the inverse.

$((b) \Rightarrow (c))$: Obvious.

$((c) \Rightarrow (d))$: $(U^*)^* = U$. So, $(U^*)^* U^* = I$. Hence, U^* is unitary.

$((d) \Rightarrow (a))$: Since U^* is unitary and $(U^*)^* = U$, we have that $(U^*)^* = U$ is unitary.

$((a) \Rightarrow (e))$: Recall that if

$$A = \begin{bmatrix} r_1 \\ \cdots \\ \vdots \\ \cdots \\ r_n \end{bmatrix}, B = [c_1 \vdots \ldots \vdots c_n],$$

then $A \cdot B = (r_i \cdot c_j)$. So, if $U = [c_1 \vdots \ldots \vdots c_n]$, then

$$U^* = \begin{bmatrix} c_1^* \\ \cdots \\ \vdots \\ \cdots \\ c_n^* \end{bmatrix}$$

and $I = U^* U = (c_i^* \cdot c_j)$. However,

$$c_i^* \cdot c_j = \langle c_i | c_j \rangle = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Hence, $c_1, \ldots, c_n$ are orthonormal.

$((e) \Rightarrow (a))$: Since the columns are orthonormal, we have that $U^* U = (c_i^* \cdot c_j) = I$.

$((d) \Rightarrow (f))$: Let

$$U = \begin{bmatrix} r_1 \\ \cdots \\ \vdots \\ \cdots \\ r_n \end{bmatrix}, U^* = [r_1^* \vdots \ldots \vdots r_n^*].$$

Since U^* is unitary, we know that $r_1^*, \ldots, r_n^*$ are orthonormal. Hence, $r_1, \ldots, r_n$ are orthonormal.

$((f) \Rightarrow (d))$: Similar to $((d) \Rightarrow (f))$.

$((a) \Rightarrow (g))$: $||Ux||^2 = \langle Ux | Ux \rangle = \langle x | U^* U x \rangle = \langle x | x \rangle ||x||^2$.

$((g) \Rightarrow (e))$: this implies that $||Ue_i|| = ||e_i|| = 1$. However, Ue_i is the i^{th} column. Therefore, the columns all have length one. Let $Ue_i = c_i$. For $i \neq j$,

$$||\alpha e_i + \beta e_j||^2 = |\alpha|^2 + |\beta|^2$$

and

$$||U(\alpha e_i + \beta e_j)||^2 = |\alpha|^2 + |\beta|^2.$$

However,

$$\begin{aligned} ||U(\alpha e_i + \beta e_j)||^2 &= \langle U(\alpha e_i + \beta e_j)|U(\alpha e_i + \beta e_j)\rangle \\ &= \langle \alpha e_i + \beta e_j|\alpha e_i + \beta e_j\rangle \\ &= |\alpha|^2\langle c_i|c_i\rangle + \overline{\alpha}\beta\langle c_i|c_j\rangle \\ &\quad +\alpha\overline{\beta}\langle c_j|c_i\rangle + |\beta|^2\langle c_j|c_j\rangle \\ &= |\alpha|^2 + |\beta|^2 + 2Re(\overline{\alpha}\beta\langle c_i|c_j\rangle). \end{aligned}$$

This implies $2Re(\overline{\alpha}\beta\langle c_i|c_j\rangle) = 0$ for all α, β. Hence,

$$\langle c_i|c_j\rangle = 0.$$

Therefore, the columns are orthonormal.

$((a) \Rightarrow (h))$: $\langle Ux|Uy\rangle = \langle x|U^*Uy\rangle = \langle x|y\rangle$.

$((h) \Rightarrow (g))$: $\langle Ux|Ux\rangle = \langle x|x\rangle$ implies $||Ux||^2 = ||x||^2$ implies $||Ux|| = ||x||$.

⊠

4.2 Householder Unitaries

Definition. Given $w \in \mathbb{C}^n$ with $||w|| = 1$, recall that $|w\rangle\langle w| = (w_i\overline{w}_j) = P_w$-projection onto $span\{w\}$. Set $U_w = I - 2P_w$. Then,

$$\begin{aligned} U_w^*U_w &= (I - 2P_w)^*(I - 2P_w) \\ &= (I - 2P_w)(I - 2P_w) \\ &= I - 2P_w - 2P_w + 4P_w \\ &= I. \end{aligned}$$

So, U_w is unitary. We call U_w the *Householder unitary given by* w.

Remark. Geometrically, U_w is equal to the reflection through the hyperplane $\{w\}^\perp$.

Lemma (Schur). Given $x, y \in \mathbb{C}^n$ with $||x|| = ||y||$, there exists $w \in \mathbb{C}^n$ with $||w|| = 1$ and $e^{i\theta}$ so that $U_w(x) = e^{i\theta}y$.

Theorem (Schur). Let $A \in M_n$. Then there exists a unitary U so that U^*AU is upper triangular.

Proof. Pick an eigenvector x_1 with $||x_1|| = 1$ and eigenvalue λ_1 of A; i.e., $Ax_1 = \lambda_1 x_1$. (We can always normalize x_1, so we may assume $||x_1||_1$.) By *Schur's lemma*, there exists $w, e^{i\theta}$ such that $U_w(x_1) = e^{i\theta}e_1$. Then,

$$\begin{aligned} (U_wAU_w^*)(e_1) &= U_wA(e^{-i\theta}x_1) \\ &= e^{i\theta}U_w\lambda_1 x_1 \\ &= \lambda_1 e^{-i\theta}e^{i\theta} \\ &= \lambda e_1. \end{aligned}$$

. This implies

$$U_w A U_w^* = \begin{bmatrix} \lambda_1 & * \\ 0 & A_1 \end{bmatrix},$$

where A_1 is $(n-1) \times (n-1)$.

Pick $x_2 \in \mathbb{C}^{n-1}$ with $||x_2|| = 1$ and λ_2 such that $A_1 x_1 = \lambda_2 x_2$. By *Schur's lemma*, there exists w_1 with

$$U_{w_1} A_1 U_{w_1}^* = \begin{bmatrix} \lambda_2 & * \\ 0 & A_2 \end{bmatrix},$$

where A_2 is $(n-2) \times (n-2)$.

Now consider

$$\tilde{U}_{w_1} = \begin{bmatrix} 1 & 0 \\ 0 & U_{w_1} \end{bmatrix}.$$

Then

$$(\tilde{U}_{w_1} U_w) A (U_w \tilde{U}_{w_1})^* = \begin{bmatrix} \lambda_1 & * & * & * \\ 0 & \lambda_2 & * & * \\ 0 & 0 & A_2 & \end{bmatrix}.$$

Now proceed by induction.

⊠

Recall. The characteristic polynomial of A is defined by $p_a(t) = det(tI - A) = n^{\text{th}}$ degree polynomial.

Corollary. $Tr(A) = \lambda_1 + \ldots + \lambda_n$, where the λ_j are the eigenvalues of A.

Proof. Apply *Schur's theorem* to $U^* A U = T$, where

$$T = \begin{pmatrix} t_{11} & * & & \\ 0 & t_{22} & & \\ & & \ddots & * \\ 0 & & & t_{nn} \end{pmatrix}.$$

Then, $t_{11} + \ldots + t_{nn} = Tr(T) = Tr(U^* A U) = Tr(AUU^*) = Tr(A)$. Since $p_T(t) = det(tI - T) = (t - t_{11}) \ldots (t - t_{nn})$, the roots are $t_{11}, \ldots, t_{nn}$. Since

$$\begin{aligned} det(tI - U^* A U) &= det(U^*(tI - a)U) \\ &= det(tI - A) \\ &= p_A(t), \end{aligned}$$

we have that $p_A(t) = p_T(t)$.

⊠

5 Day 4 - 2/Sep/11

5.1 Hermitian Matrices

Definition. $H \in M_n$ is *Hermitian*, or *self-adjoint*, if $H = H^*$.

Theorem. The following are equivalent:

(a) H is Hermitian.

(b) There exists a unitary U such that $U^*HU = D$, where D is a diagonal matrix with real entries.

(c) H has an orthonormal basis with real eigenvectors.

(d) $\langle x|Xx\rangle$ is real for all $x \in \mathbb{C}^n$.

Proof. We need a lemma:
Lemma. For $T \in M_n$, if $\langle x|Tx\rangle = 0$ for all $x \in \mathbb{C}^n$, then $T = 0$.
Remark. Let

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

and $x \in \mathbb{R}^2$. Write $x = (x_1 x_2)^t$. Then,

$$\begin{aligned} \langle x|Tx\rangle &= \langle (x_1 x_2)^t | (x_2 - x_1)^t \rangle \\ &= x_1 x_2 - x_2 x_1 \\ &= 0 \end{aligned}$$

but $T \neq 0$.

Proof of Lemma. Given $x, y \in \mathbb{C}^n$, we have

$$\begin{aligned} 0 &= \langle x + y|T(x + y)\rangle \\ &= \langle x|Tx\rangle + \langle y|Tx\rangle + \langle x|Ty\rangle + \langle y|Ty\rangle \\ &= \langle y|Tx\rangle + \langle x|Ty\rangle. \end{aligned}$$

and

$$\begin{aligned} 0 &= \langle x + iy|T(x + iy)\rangle \\ &= \langle iy|Tx\rangle + \langle x|Tiy\rangle \\ &= -i\langle y|Tx\rangle + i\langle x|Ty\rangle. \end{aligned}$$

Hence, $\langle y|Tx\rangle = \langle x|Ty\rangle$ and $\langle y|Tx\rangle = -\langle x|Ty\rangle$. So, $\langle y|Tx\rangle = 0$ for all $x, y \in \mathbb{C}^n$. Take $x = e_j$ and $y = e_i$. This implies $t_{ij} = 0$, and so, $T = 0$.

$\otimes$

We now prove the theorem.

$((a) \Rightarrow (b))$: By *Schur*, there exists a unitary U such that $U^*HU = T$, with T upper triangular. Then,

$$\begin{aligned} T^* &= (U^*HU)^* \\ &= U^*H^*U^{**} \\ &= U^*HU \\ &= T. \end{aligned}$$

This implies T is diagonal. Let $T = D$. Then $D^* = D$, which implies D has real entries.

$((b) \Rightarrow (c))$: Let $U^*HU = D$ and $De_j = \lambda_j e_j$ be the eigenvectors and eigenvalues. Then $HU = UD$, which implies

$$H(Ue_j) = UDe_j = U(\lambda_j e_j) = \lambda_j Ue_j.$$

So, Ue_j is an eigenvector of H for all j. However, Ue_j is the j^{th} column of U. Therefore, $u_j = Ue_j$ is an orthonormal basis of eigenvectors.

$((c) \Rightarrow (a))$ Let $\{u_1, \ldots, u_n\}$ be an orthonormal basis of eigenvectors with real eigenvalues; i.e., $Hu_j = \lambda_j u_j$, for all j. Let $D = diag\{\lambda_1, \ldots, \lambda_n\}$ and

$$U = [u_1 \vdots \ldots \vdots u_n].$$

Then U is unitary and

$$HUe_j = Hu_j = \lambda_j u_j = \lambda_j Ue_j = UDe_j$$

for all j. So, HU and UD agree in column j, for all j. This implies $HU = UD$ and $H = UDU^*$. Hence,

$$H^* = U^{**}D^*U^* = UDU^* = H.$$

$((a) \Rightarrow (d))$ $\langle x|Hx\rangle = \langle H^*x|x\rangle = \langle Hx|x\rangle = \overline{\langle x|Hx\rangle}$ implies $\langle x|Hx\rangle \in \mathbb{R}$ for all x.

$((d) \Rightarrow (a))$ $\langle x|Hx\rangle = \overline{\langle x|Hx\rangle} = \langle Hx|x\rangle = \langle x|H^*x\rangle$ implies $\langle x|(H - H^*)x\rangle = 0$ for all x. By the lemma, $H - H^* = 0$ implies $H = H^*$.

$\boxtimes$

5.2 Positive Definite and Semidefinite

Definition. $P \in M_n$ is *positive semidefinite*, denoted $P \geq 0$, if $\langle x|Px\rangle \geq 0$ for all $x \in \mathbb{C}^n$. It is called *positive definite*, denoted $P > 0$, if $\langle x|Px\rangle > 0$ for all $x \in \mathbb{C}^n$.

Note that, by *part (d)* above, P positive semidefinite implies $P = P^*$.

Theorem. $P \geq 0$ if and only if $P = P^*$ and all the eigenvalues are non-negative.

Proof. $(\Rightarrow)$ $\langle x|Px \rightarrow \geq 0$ implies $\langle x|Px\rangle \in \mathbb{R}$ implies $P = P^*$. Let $Px = \lambda x$. Then,

$$0 \leq \langle x|Px\rangle = \langle x|\lambda x\rangle = \lambda\langle x|x\rangle = \lambda||x||^2.$$

Hence, $0 \geq \lambda$.

$(\Leftarrow)$ Let $\{u_1, \ldots, u_n\}$ be an orthonormal basis of eigenvectors, $Pu_j = \lambda_j u_j$

with $\lambda_j \geq 0$. Given $x \in \mathbb{C}^n$, write $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$. Then,

$$\begin{aligned}
\langle x|Px\rangle &= \sum_{i,j} = 1^n \langle \alpha_i u_i | P(\alpha_j u_j)\rangle \\
&= \sum_{i,j} = 1^n \overline{\alpha}_i \alpha_j \langle u_i | P u_j\rangle \\
&= \sum_{i,j} = 1^n \overline{\alpha}_i \alpha_j \lambda_j \langle u_i | u_j\rangle \\
&= \sum_{j=1}^{n} \lambda_j |\alpha_j|^2 \\
&\geq 0.
\end{aligned}$$

$\boxtimes$

Corollary. $P > 0$ if and only if $P = P^*$ and all the eigenvalues are strictly positive.

Proof. ($\Rightarrow$) We know that $P = P^*$ has eigenvalues greater than or equal to 0. If $Pu_j = 0u_j$, then $0 = \langle u_j | P u_j\rangle$. Therefore, $\lambda_j > 0$ for all j.

($\Leftarrow$) Write $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$ as before. Then $\langle x|Px\rangle = \sum_{j=1}^{n} \lambda_j |\alpha_j|^2$. Since $x \neq 0$, some $\alpha_k \neq 0$. Hence, $\langle x|Px\rangle > 0$.

$\boxtimes$

Theorem. $P \geq 0$ if and only if $P = \sum_{i=1}^{m} |v_i\rangle\langle v_i|$ for some set of vectors.

Proof. ($\Rightarrow$) Take an orthonormal basis of eigenvectors $\{u_1, \ldots, u_n\}$ with $\lambda_j \geq 0$. If $x = \sum_{i=1}^{n} \alpha_i u_i$, then $Px = \sum_{j=1}^{n} \alpha_j P x_j = \sum_{j=1}^{n} \alpha_j \lambda_j u_j$. However,

$$(|u_j\rangle\langle u_j|)x = \langle u_j|x\rangle u_j = \alpha_j u_j.$$

Therefore, $Px = \left(\sum_{j=1}^{n} |u_j\rangle\langle u_j|\right) x$ implies

$$P = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| = \sum_{j=1}^{n} |\lambda_j^{1/2} u_j\rangle\langle \lambda_j^{1/2} u_j|.$$

($\Leftarrow$) If $P = \sum_{i=1}^{n} |v_i\rangle\langle v_i|$, then

$$Px = \sum_{i=1}^{m} \langle v_i|x\rangle v_i.$$

Therefore,

$$\langle x|Px\rangle = \langle x| \sum_{i=1}^{m} \langle v_i|x\rangle v_i\rangle = \sum_{i=1}^{m} \langle v_i|x\rangle\langle x|v_i\rangle = \sum_{i=1}^{m} |\langle v_i|x\rangle|^2 \geq 0.$$

So, $P \geq 0$.

$\boxtimes$

Key: $P = \sum_{i=1}^{m} |v_i\rangle\langle v_i|$. Then $\langle x|Px\rangle = \sum_{i=1}^{|} \langle v_i|x\rangle|^2$.

Theorem. Let $P_{n\times n} = \sum_{i=1}^{m} |v_i\rangle\langle v_i|$. Then $P > 0$ if and only if $span\{v_1, \ldots, v_m\} = \mathbb{C}^n$.

Proof. ($\Leftarrow$) If $x \neq 0$, since the v_i's span $\mathbb{C}^n$, $\langle v_i|x\rangle \neq 0$ for some i. So, $\langle x|Px\rangle = \sum_{i=1}^{|} \langle v_i|x\rangle|^2 > 0$. Hence, $P > 0$.

($\Rightarrow$) Suppose $\{v_1, \ldots, v_m\}$ do not span $\mathbb{C}^n$. Then there exists $x \neq 0$ such that $x \perp v_j$ for all j. then $\langle x|Px\rangle = \sum_{i=1}^{|} \langle v_i|x\rangle|^2 = 0$, contradicting $P > 0$. Therefore, $span\{v_1, \ldots, v_m\} = \mathbb{C}^n$.

$\boxtimes$

6 Day - 7/Sep/11

6.1 Aside

Given an $n \times n$ matrix P such that $P = P^*$, how do we tell $P \geq 0$ or $P > 0$.

Practical Tests

1. If $P = P^*$, then $P > 0$ if and only if

$$det \begin{pmatrix} p_{1,1} & \cdots & p_{1,k} \\ \vdots & & \vdots \\ p_{k,1} & \cdots & p_{k,k} \end{pmatrix} > 0$$

for $k = 1, \ldots, n$. Note that

$$det \begin{pmatrix} p_{1,1} & \cdots & p_{1,k} \\ \vdots & & \vdots \\ p_{k,1} & \cdots & p_{k,k} \end{pmatrix} \geq 0$$

for $k = 1, \ldots, n$ does not imply $P \geq 0$.

2. The best method is *Cholesky's algorithm*:

Theorem. If $P = (p_{i,j})$ is $n \times n$ and $P = P^*$, then $P \geq 0$ if and only if $P - \left(\frac{p_{i,1} \cdot p_{1,j}}{p_{1,1}}\right) \geq 0$.

Note that

$$\left(\frac{p_{i,1} \cdot p_{1,j}}{p_{1,1}}\right) = \begin{pmatrix} p_{1,1} & \vdots & p_{1,2} & \cdots & p_{1,n} \\ \cdots & \cdots & \cdots & & \\ p_{2,1} & \vdots & & & \\ \vdots & \vdots & & * & \\ p_{n,1} & \vdots & & & \end{pmatrix};$$

i.e., it is equal to P in the first row and column. Therefore, $P - \left(\frac{p_{i,1} \cdot p_{1,j}}{p_{1,1}}\right)$ is really an $(n-1) \times (n-1)$ matrix.

Then we repeat the process.

Example. Let

$$P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 7 \end{pmatrix}.$$

Then,

$$\begin{aligned} R &= \left(\frac{p_{i,1} \cdot p_{1,j}}{p_{1,1}}\right) \\ &= \frac{1}{1} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}^* \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{pmatrix}. \end{aligned}$$

Hence,

$$P - R = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -2 \end{pmatrix}.$$

So, $P \not\succeq 0$.

Example. Let

$$P = \begin{pmatrix} 4 & 2 & 3 \\ 2 & 5 & 6 \\ 3 & 6 & 8 \end{pmatrix}.$$

Then

$$\begin{aligned} R &= \left(\frac{p_{i,1} \cdot p_{1,j}}{p_{1,1}}\right) \\ &= \frac{1}{4} \begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix}^* \\ &= \frac{1}{4} \begin{pmatrix} 16 & 8 & 12 \\ 8 & 4 & 6 \\ 12 & 6 & 9 \end{pmatrix}. \end{aligned}$$

Hence,

$$P - R = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & {}^{9}/_{2} \\ 0 & {}^{9}/_{2} & {}^{23}/_{4} \end{pmatrix}.$$

Repeating, we obtain

$$\begin{pmatrix} 4 & {}^{9}/_{2} \\ {}^{9}/_{2} & {}^{23}/_{4} \end{pmatrix} - \frac{1}{4}\begin{pmatrix} 4 \\ {}^{9}/_{2} \end{pmatrix} \cdot \begin{pmatrix} 4 \\ {}^{9}/_{2} \end{pmatrix}^{*} = \begin{pmatrix} 0 & 0 \\ 0 & {}^{11}/_{16} \end{pmatrix}.$$

Therefore, P is positive semidefinite.

Remark. The other advantage of *Cholesky* is when $P \geq 0$, this writes P as a sum of rank one matrices.

6.2 Direct Sums of Vector Spaces, Partitioned Matrices

Definition. Given vector spaces V, W, their *direct sum* is defined by

$$V \oplus W = \{(v, w)\ v \in V, w \in W\}.$$

It is a vector space with operations

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2), \alpha(v, w) = (\alpha v, \alpha w).$$

It is a Hilbert space with inner product

$$\langle (v_1, w_1) | (v_2, w_2) \rangle_{V \oplus W} = \langle v_1 | v_2 \rangle_V + \langle w_1 | w_2 \rangle_W.$$

Proposition. If $v_1, \ldots, v_n$ is a basis for V and $w_1, \ldots, w_k$ is a basis for W, then $(v_1, 0), \ldots, (v_n, 0), (0, w_1), \ldots, (0, w_k)$ is a basis for $V \oplus W$.

Proof. For $v \in V$, write $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$. Similarly, for $w \in W$, write $w = \beta_1 w_1 + \ldots + \beta_k w_k$. Then,

$$\begin{aligned} (v, w) &= \alpha_1(v_1, 0) + \ldots + \beta_k(0, w_k) \\ &= (v, 0) + (0, w) \\ &= (v + 0, 0 + w) \\ &= (v, w). \end{aligned}$$

Therefore, they span $V \oplus W$. A similar calculation shows that they are linearly independent.

$\boxtimes$

Corollary. $dim(V \oplus W) = dim(V) + dim(W)$.

Note. Note that $V \cong \{(v, 0) : v \in V\} \subset V \oplus W$. Similarly for $W \cong \{(0, w) : w \in W\}$. Hence, $(v, 0) \perp (0, w)$, making V and W perpendicular to each other in $V \oplus W$.

Key Examples

1. $\mathbb{C}^{n+k} = \{(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+k}) : a_i \in \mathbb{C}\} = \{(v, w) : v \in \mathbb{C}^n, w \in \mathbb{C}^k\} = \mathbb{C}^n \oplus \mathbb{C}^k$.

2. Given $T : \mathbb{C}^{n_1+k+1} \to \mathbb{C}^{n_2+k_2}$, T can be represented by an $(n_2 + k_2) \times (n_1 + k_1)$ matrix:

$$T = \begin{pmatrix} t_{1,1} & \dots & t_{1,n_1} & t_{1,n_1+1} & \dots & t_{1,n_1+k+1} \\ \vdots & & & & & \\ t_{n_2,1} & \dots & t_{n_2,n_1} & t_{n_2,n_1+1} & \dots & t_{n_2,n_1+k_1} \\ t_{n_2+1,1} & \dots & t_{n_2+1,n_1} & t_{n_2+1,n_1+1} & \dots & t_{n_2+1,n_1+k_1} \\ \vdots & & & & & \\ t_{n_2+k_2,1} & \dots & t_{n_2+k_2,n_1} & t_{n_2+k_2,n_1+1} & \dots & t_{n_2+k_2,n_1+k_1} \end{pmatrix} = \begin{pmatrix} T_{1,1} & \vdots & T_{1,2} \\ T_{2,1} & \vdots & T_{2,2} \end{pmatrix},$$

where

$$\begin{aligned} T_{1,1} &: \mathbb{C}^{n_1} \to \mathbb{C}^{n_2}, \\ T_{1,2} &: \mathbb{C}^{k_1} \to \mathbb{C}^{n_2}, \\ T_{2,1} &: \mathbb{C}^{n_1} \to \mathbb{C}^{k_2}, \\ T_{2,2} &: \mathbb{C}^{k_1} \to \mathbb{C}^{k_2}. \end{aligned}$$

So,

$$\begin{aligned} T \begin{pmatrix} a_1 \\ \vdots \\ a_{n_1} \\ a_{n_1+1} \\ \vdots a_{n_1+k_1} \end{pmatrix} &= T \begin{pmatrix} v \\ w \end{pmatrix}, \text{ where } v \in \mathbb{C}^{n_1}, w \in \mathbb{C}^{k_1}, \\ &= \begin{pmatrix} T_{1,1} & \vdots & T_{1,2} \\ T_{2,1} & \vdots & T_{2,2} \end{pmatrix} \begin{pmatrix} v \\ w \end{pmatrix} \\ &= \begin{pmatrix} T_{1,1}v + T_{1,2}w \\ T_{2,1}v + T_{2,2}w \end{pmatrix}, \end{aligned}$$

where, $T_{1,1}v + T_{1,2}w \in \mathbb{C}^{n_2}$, $T_{2,1}v + T_{2,2}w \in \mathbb{C}^{k_2}$.

7 Day - 9/Sep/11

7.1 Tensor Products

Definition. Given vector spaces X, Y, Z, a map $B : X \times Y \to Z$, $B(x, y) \in Z$, is called *bilinear* provided:

(1) $B(x_1 + x_2, y) = B(x_1, y) + B(x_2, y)$,

(2) $B(x, y_1 + y_2) = B(x, y_1) + B(x, y_2)$, and,

(3) for all $\lambda \in \mathbb{C}$, $B(\lambda x, y) = B(x, \lambda y) = \lambda B(x, y)$.

Notes. (1) $\lambda B(x,0) = B(x,\lambda\cdot 0) = B(x,0)$, for all $\lambda\in\mathbb{C}$. Hence, $B(x,0)=0$. Similarly, $B(0,y)=0$.

(2) $B(x_1+x_2,y_1+y_2) = B(x_1+x_2,y_1)+B(x_1+x_2,y_2) = B(x_1,y_1)+B(x_1,y_2)+B(x_2,y_1)+B(x_2,y_2)$. Hence, these are like products.

Motivation of Tensor Products: In the new space, bilinear becomes linear.

Axiom. We form the vector space $X\otimes Y$, which is the span of "elementary tensors" $x\otimes y$, for all $x\in X, y\in Y$, satisfying the universal property: Whenever $B: X\times Y\to Z$ is bilinear, there exists a corresponding linear map $L_B: X\otimes Y\to Z$ with $B(x,y)=L_B(x\otimes y)$.

Key: $X\otimes Y = span\{x\otimes y : x\in X, y\in Y\}$ and has the following relations:

- $(x_1+x_2)\otimes y = x_1\otimes y + x_2\otimes y$,
- $x\otimes(y_1+y_2) = x\otimes y_1 + x\otimes y_2$,
- $\lambda(x\otimes y) = (\lambda x)\otimes y = x\otimes(\lambda y)$.

Theorem. If $\{e_1,\ldots,e_k\},\{f_1,\ldots,f_m\}$ are bases for X,Y, respectively, then

$$\{e_i\otimes f_j : 1\le i\le k, 1\le j\le m\}$$

is a basis for $X\otimes Y$. Hence, $dim(X\otimes Y) = dim(X)\cdot dim(Y)$.

Proof. We first show that $\{e_i\otimes f_j\}$ is spanning. Given $x\in X$, $y\in Y$, write

$$x = \alpha_1 e_1 + \ldots + \alpha_k e_k,$$

$$y = \beta_1 f_1 + \ldots + \beta_m f_m.$$

Then,

$$\begin{aligned} x\otimes y &= (\alpha_1 e_1+\ldots+\alpha_k e_k)\otimes(\beta_1 f_1+\ldots+\beta_m f_m) \\ &= \sum_{i=1}^{k}\sum_{j=1}^{m}(\alpha_i e_i)\otimes(\beta_j f_j) \\ &= \sum_{i=1}^{k}\sum_{j=1}^{m}(\alpha_i\beta_j)(e_i\otimes f_j). \end{aligned}$$

Hence, they span the set.

To show linear independence, define $B: X\times Y\to M_{k,m}$ by

$$B(\alpha_1 e_1+\ldots+\alpha_k e_k, \beta_1 f_1+\ldots+\beta_m f_m) = (\alpha_i\beta_j)\in M_{k,m}.$$

Then, B is bilinear, and by the universal property, there exists $L_B: X\otimes Y\to M_{k,m}$, $L_B(x\otimes y)=B(x,y)$. However, $L_B(e_i\otimes f_j)=E_{i,j}$. So, if $\sum\alpha_{ij}(e_i\otimes f_j)=0$, then

$$0 = L_B\left(\sum\alpha_{ij}(e_i\otimes f_j)\right) = \sum\alpha_{ij}E_{i,j}.$$

Hence, $\alpha_{ij} = 0$ for all i, j.

$\boxtimes$

Proposition. Let $\{e_1, \ldots, e_k\}, \{f_1, \ldots, f_m\}$ be bases for X, Y, respectively, and $u \in X \otimes Y$. Then:

(1) there exists unique $x_1, \ldots, x_m \in X$ such that $u = x_1 \otimes f_1 + \ldots + x_m \otimes f_m$;

(2) there exists unique $y_1, \ldots, y_k \in Y$ such that $u = e_1 \otimes y_1 + \ldots + e_k \otimes y_k$.

Proof. Since $\{e_i \otimes f_j\}$ is a basis for $X \otimes Y$, there exists unique $\alpha_{ij} \in \mathbb{C}$ such that $u = \sum_{i=1}^{k} \sum_{j=1}^{m} \alpha_{ij}(e_i \otimes f_j)$. Let $x_j = \sum_{i=1}^{k} \alpha_{ij} e_i$. Then,

$$u = \sum_{j=1}^{m} x_j \otimes f_j.$$

Similarly, let $y_i = \sum_{j=1}^{m} \alpha_{ij} f_j$. Then,

$$u = \sum_{i=1}^{k} e_i \otimes y_i.$$

Uniqueness follows from the fact that $\{e_i \otimes f_j\}$ is a basis.

$\boxtimes$

Corollary. If $dim(X) = k$ and $dim(Y) = m$, then

$$\begin{array}{rcll} X \otimes Y & \cong & X \oplus \ldots \oplus X & (m \ times) \\ & \cong & Y \oplus \ldots \oplus Y & (k \ times). \end{array}$$

Key. In these last identifications, we needed to choose a basis!

Remark. Let $u \in X \otimes Y$. There exists many ways to write u as a sum of elementary tensors. For example,

$$\begin{array}{rcl} u & = & (2e_1 + 3e_2) \otimes (f_1 + f_2) + e_2 \otimes (3f_1 + 4f_2) \\ & = & 2e_1 \otimes f_1 + 2e_1 \otimes f_2 + 3e_2 \otimes f_1 + 3e_2 \otimes f_2 + 3e_2 \otimes f_1 + 4e_2 \otimes f_2 \\ & = & 2e_1 \otimes f_1 + 2e_1 \otimes f_2 + 6e_2 \otimes f_1 + 7e_2 \otimes f_2. \end{array}$$

Definition. Given $u \in X \otimes Y$, the *Schmidt rank* of u, denoted $rank_S(u)$ is the least number of elementary tensors in an expression for u.

8 Day - 12/Sep/11

8.1 Tensor Produts of Hilbert Spaces

Remark. Let H, K be Hilbert spaces. Then we set

$$\langle h_1 \otimes k_1 | h_2 \otimes k_2 \rangle = \langle h_1 | h_2 \rangle_H \cdot \langle k_1 | k_2 \rangle_K. \quad (*)$$

Theorem. $(*)$ extends to define a sesquilinear form on $H \otimes K$ satisfying $\langle u|u\rangle = 0$ if and only if $u = 0$. Therefore, this defines an inner product on $H \otimes K$. In finite dimensions, we call $H \otimes K$ with this inner product the *Hilbert space tensor product*.

When H, K are infinite dimensional, the vector space $H \otimes K$ will not be complete in the norm coming from this inner product. In this case, the Hilbert space tensor product means the completion.

Proposition. If $\{h_i\}_{i\in I}$ is an orthonormal basis for H and $\{k_j\}_{j\in J}$ is an orthonormal basis for K, then

$$\{h_i \otimes k_j \,:\, i \in I, j \in J\}$$

is an orthonormal basis for $H \otimes K$.

Proof. (Finite Dimensional Case) We see that

$$\begin{aligned}\langle h_{i_1} \otimes k_{j_1} | h_{i_2} \otimes k_{j_2}\rangle &= \langle h_{i_1}|h_{i_2}\rangle\langle k_{j_1}|k_{j_2}\rangle \\ &= \begin{cases} 1, & i_1 = i_2 \text{ and } j_1 = j_2 \\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

Therefore, they are orthonormal. Since this set has $|I| \cdot |J| = dim(H)dim(K) = dim(H \otimes K)$ elements, it is a basis.

(Sketch of Infinite Dimensional Case) We still have that

$$\{h_i \otimes k_j \,:\, i \in I, j \in J\}$$

is an orthonormal set. Then show that the linear span is dense.

$\boxtimes$

Summary. Given the Hilbert spaces $\mathbb{C}^n, \mathbb{C}^k$ and canonical orthonormal bases

$$\{e_i \,:\, 1 \le i \le n\}, \{e_j \,:\, 1 \le j \le k\},$$

$\mathbb{C}^n \otimes \mathbb{C}^k$ has an orthonormal basis $\{e_i \otimes e_j\}$. In physics notation, we write $e_i = |i\rangle$ and $e_i \otimes e_j = |ij\rangle$.

If we have $\mathbb{C}^n, \mathbb{C}^k, \mathbb{C}^p$ with canonical orthonormal bases $\{e_i\}, \{e_j\}, \{e_l\}$, then

$$\{e_i \otimes e_j \otimes e_l\}$$

is an orthonormal basis for $\mathbb{C}^n \otimes \mathbb{C}^k \otimes \mathbb{C}^p$ and $dim(\mathbb{C}^n \otimes \mathbb{C}^k \otimes \mathbb{C}^p) = nkp$. In physics notation, $e_i \otimes e_j \otimes e_l = |ijl\rangle$.

Example. For $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ (N copies), we have the orthonormal basis $\{e_{i_1} \otimes \ldots \otimes e_{i_N} = |i_1 \ldots i_N\rangle\}$. In mathematical notation, $I = (i_1, \ldots, i_N)$ is called a multi-index and we write $e_I = e_{i_1} \otimes \ldots \otimes e_{i_N}$.

A basis for $\mathbb{C}^2$ is $\{e_0, e_1\}$. Then, the multi-index $I = (i_1, \ldots, i_N) \in (\mathbb{Z}_2)^N$ for $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ (N copies).

8.2 Postulates of Quantum Mechanics

Postulate 1. To each isolated physical system, there corresponds a Hilbert space, called the *state space*, and the state of the system is completely described by a unit vector in H called the *state vector*.

Example. The system of a single photon with the state equal to the polarization described by a unit vector in $\mathbb{C}^2$.

Postulate 2. The time evolution from time t_1 to t_2, $t_1 < t_2$, of a closed quantum system is described by a unitary $U : H \to H$ so that if the system is in state ψ at time t_1, then it is in state $U\psi$ at time t_2. (Often, we have a *continuous time* and then we have $U(t)$ and $U(s+t) = U(s)U(t)$).

By *closed*, we mean "not interacting with anything outside the system." By *open*, we mean it is a piece of a larger system.

Quantum Measurements. When we want to observe a system, i.e., connect to the "outside world," the system is no longer closed because we interact with it. This leads to nonunitary changes.

Postulate 3. Quantum measurements are described by a collection of operators $\{M_m\}_{m=measurements}$ on H, called *measurement operators*. If the system is in state ψ before we measure, then the probability that we observe m is

$$\begin{aligned} p_m(\psi) = \langle\psi|M_m^* M_m|\psi\rangle & \\ &= \langle\psi|M_m^* M_m\psi\rangle \\ &= ||M_m\psi||^2. \end{aligned}$$

(Since $1 = \sum_m p_m(\psi) = \sum\langle\psi|M_m^* M_m\psi\rangle = \langle\psi|\sum_m M_m^* M_m|\psi\rangle = \langle\psi|I\psi\rangle$, we have that $\langle\psi|(I - \sum_m M_m^* M_m)\psi\rangle = 0$ for all ψ. Therefore, $I = \sum_m M_m^* M_m$.)

Also, after we observe m, then the system changes to the state $\frac{M_m\psi}{(p_m(\psi))^{1/2}}$.

9 Day - 14/Sep/11

9.1 Quantum Game

Alice has two states $\{\psi_1, \psi_2\}$. Bob knows that they are $\{\psi_1, \psi_2\}$. Alice picks one and sends to Bob. Can Bob create a measurement system $\{M_m\}$ that, with certainty, decides which one he is given?

Formally, we want M_1, M_2 such that $||M_1\psi_2|| = 0$, $||M_1\psi_1||^2 = p_1(\psi_1) = 1$, $||M_2\psi_1|| = 0$, and $||M_2\psi_2||^2 = 1$.

Case I ($\psi_1 \perp \psi_2$): Let

$$M_1 = |\psi_1\rangle\langle\psi_1|,$$

the projection onto the span of ψ_1, and let

$$M_2 = |\psi_2\rangle\langle\psi_2|.$$

Note that $M_1^2 = M_1^* M_1 = M_1$, $M_2^2 = M_2^* M_2 = M_2$. Let

$$M_3 = I - M_1 - M_2,$$

which is the projection onto the span of $\{\psi_1, \psi_2\}^\perp$. Note that $M_3^* M_3 = M_3^2 = M_3$. Then,

$$\begin{aligned} ||M_1\psi_1||^2 &= \langle M_1\psi_1 | M_1\psi_1\rangle \\ &= \langle \psi_1 | \psi_1\rangle \\ &= 1, \end{aligned}$$

and

$$\begin{aligned} ||M_1\psi_2|| &= \langle M_1\psi_2 | M_1\psi_2\rangle = 0, \\ ||M_2\psi_1|| &= 0, \\ ||M_2\psi_2|| &= 1. \end{aligned}$$

Therefore, we can distinguish with certainty.

Case II ($\psi_1 \not\perp \psi_2$): Suppose we had any measurement system $\{M_m\}$ such that $||M_1\psi_1|| = 1$. This implies $||M_l\psi_1|| = 1$ for all $l \neq 1$. Now, $\psi_2 = \alpha\psi_1 + \beta\gamma$, where $\psi_1 \perp \gamma$ and $||\gamma|| = 1$. So, $||\psi_2||^2 = 1$ implies $|\alpha|^2 + |\beta|^2 = 1$. Hence, $\alpha \neq 0$.

Now,

$$\begin{array}{ccccc} 1 & = & \sum_m p_m(\psi_2) & = & \sum_m \langle M_m\psi_2 | M_m\psi_2\rangle \\ & = & \sum_m ||M_m(\alpha\psi_1 + \beta\gamma)||^2 & = & ||M_1(\alpha\psi_1 + \beta\gamma)||^2 + \sum_{l\neq 1} ||M_l(\alpha\psi_1 + \beta\gamma)||^2 \\ & = & ||M_1(\alpha\psi + \beta\gamma)||^2 + \sum_{l\neq 1} ||M_l(\beta\gamma)||^2 & \leq & ||M_1(\psi_2)||^2 + \sum_l ||\beta M_l(\gamma)||^2 \\ & = & ||M_1(\psi_2)||^2 + |\beta|^2. & & \end{array}$$

This implies $1 - |\beta|^2 = |\alpha|^2 \leq ||M_1(\psi_2)||^2$. So, with probability $|\alpha|^2$, Measurement 1 will "light up" when ψ_2 is sent.

In spite of this problem we do have:

Theorem. Given states $\{\psi_1, \ldots, \psi_n\}$ which are linearly independent, there exists a measurement system $M_0, \ldots, M_n$ such that if the i^{th} occurs, then ψ_i is received.

Remark. Given $P \geq 0$,

$$U^* P U = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

where $\lambda_i \geq 0$, denote

$$P^{1/2} = U \begin{pmatrix} \lambda_1^{1/2} & & 0 \\ & \ddots & \\ 0 & & \lambda_n^{1/2} \end{pmatrix} U^*.$$

So, $P^{1/2} \geq 0$ and $(P^{1/2})^2 = P$.

Proof. Let $V_i = span\{\psi_j : j \neq i\}$. Let E_i be the projection onto $V_i^{\perp}$. Since $\psi_j \in V_i$ for $j \neq i$, we have that $E_i(\psi_j) = 0$ for all $i \neq j$. However, $\psi_i \in V_i$ implies $E_i(\psi_i) \neq 0$. For each i, $0 \leq E_i \leq I$ implies

$$0 \leq E_1 + \ldots + E_n \leq nI.$$

So,

$$0 \leq \frac{1}{n}E_1 + \ldots + \frac{1}{n}E_n \leq nI.$$

Let $M_i = \frac{1}{\sqrt{n}}E_i$. Then, $M_i = M_i^*$, $M_i^* M_i = \frac{1}{n}E_i$, and $\sum_{i=1}^n M_i^* M_i \leq I$. Hence,

$$P = I - \sum_{i=1}^{n} M_i^* M_i \geq 0.$$

Let $M_0 = P^{1/2}$. Then, $M_0^* M_0 = P$, and therefore,

$$\sum_{i=0}^{n} M_i^* M_i = I.$$

Thus, $\{M_0, \ldots, M_n\}$ is a measurement system.

If for $i = 1, \ldots, n$, M_i occurs, then

$$||M_i(\psi_j)|| = ||frac1\sqrt{n}E_i(\psi_j)|| = 0,$$

for $j \neq i$. So, if the i^{th} occurs, then ψ_i is received.

$\boxtimes$

Remark. Suppose we send ψ_1. Then, $M_i(\psi_1) = 0$ for $i = 2, \ldots, n$. However,

$$||M_1(\psi_1)||^2 = \frac{1}{n}||E_1(\psi_1)||^2 \leq \frac{1}{n}.$$

With probablity

$$1 - ||M_1(\psi_1)^2 \geq 1 - \frac{1}{n} = \frac{n-1}{n},$$

we get 0 for a measurement.

9.2 Projective Measurements, Expected Values, and Self-Adjoints

Recall the example from probablity: Roll a die, which has six outcomes, $\{1, \ldots, 6\}$, each with probablity $\frac{1}{6}$. Now roll the die a large number of times, say n times. Add up the numbers obtained and divide by n:

$$\begin{aligned} \frac{o_1 + \ldots + o_n}{n} &\cong \frac{\frac{n}{6} \cdot 1 + \ldots + \frac{n}{6} \cdot 6}{n} \\ &= \frac{1}{6} \cdot 1 + \ldots + \frac{1}{6} \cdot 6 \\ &= prob(1) \cdot 1 + \ldots + prob(6) \cdot 6. \end{aligned}$$

Let

$$E(X) = \sum_i prob(X = a_i) \cdot a_i,$$

which we call the *expected value of* X.

If we have measurements $\{M_m\}$, measurement outcomes are real numbers $\{\lambda_m\}$. If ψ is the state, the probability that the outcome occurs is $p_m(\psi) = ||M_m\psi||^2$. Hence, the expected value is

$$\begin{aligned} E &= \sum_m p_m(\psi) \cdot \lambda_m \\ &= \sum_m \lambda_m \langle M_m\psi | M_m\psi \rangle \\ &= \sum_m \lambda_m \langle \psi | M_m^* M_m \psi \rangle \\ &= \langle \psi | (\sum \lambda_m M_m^* M_m)\psi \rangle \\ &= \langle \psi | H\psi \rangle, \end{aligned}$$

where $H = \sum_m \lambda_m M_m^* M_m$ and $H^* = H$. Therefore, $\langle \psi | H\psi \rangle$ is equal to the expected value of the outcome when ψ passes through the system.

10 Day - 16/Sep/11

10.1 Positive Operator-Valued Measures

Let $\{M_m\}, \{\tilde{M}_m\}$ be measurement operators. If

$$M_m^* M_m = \tilde{M}_m^* \tilde{M}_m$$

for all m, then

$$\begin{aligned} p_m(\psi) &= ||M_m\psi||^2 \\ &= \langle M_m\psi | M_m\psi \rangle \\ &= \langle \psi | M_m^* M_m \psi \rangle \\ &= \langle \psi | \tilde{M}_m^* \tilde{M}_m \psi \rangle \\ &= \tilde{p}_m(\psi). \end{aligned}$$

Hence, we cannot distinguish these systems. Thus, only $M_m^* M_m$ matters and $\sum_m M_m^* M_m = I$.

Now suppose that we have $P_m \geq 0$ and $\sum_m P_m = I$. If we set $M_m = P_M^{1/2}$, then $\{M_m\}$ is a measurement system.

Definition. A *positive operator-valued measure* is a set $\{P_m\}$ of positive operators such that $\sum_m P_m = I$.

Note that some books and researchers focus on these as "measurements."

10.2 Composite System

Suppose we have two or more distinct physical systems. How do we describe it?

Postulate 4: The state space of a composite system is the tensor product of the state spaces of each component; that is, if these spaces are $H_1, \ldots, H_n$ and te i^{th} component is in state ψ_i, thent he system is in state $\psi_1 \otimes \ldots \otimes \psi_n$.

Example. Suppose we have two photons in a lab, the first given by $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and the second given by $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$. The pair is then described by a vector in $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ given by

$$\begin{aligned}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{|0\rangle + i|1\rangle}{\sqrt{2}}\right) &= \frac{|0\rangle \otimes |0\rangle + i|0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle + i|1\rangle \otimes |1\rangle}{2} \\ &= \frac{|00\rangle + i|01\rangle + |10\rangle + i|11\rangle}{2}.\end{aligned}$$

Note that this is a vector of Schmidt rank 1.

Remark. Suppose one just has two photons. They will be represented by a unit vector ψ in $\mathbb{C}^2 \otimes \mathbb{C}^2$. Are there two subsystems so that these can be thought of as two separate photons, one in each subsystem?

The answer is yes if and only if $\psi = \psi_1 \otimes \psi_2$ if and only if $rank_S(\psi) = 1$. When $rank_S(\psi) > 1$, this is a phenomenon known as *entanglement*.

Note that entanglement does happen in nature!

10.3 Measurements in Composite Systems

Tensor Products of Operators: Given $R : H \to H$, $T : K \to K$, there exists a unique operator

$$R \otimes T : H \otimes K \to H \otimes K$$

given by

$$(R \otimes T)\left(\sum_{l=1}^{n} h_l \otimes k_l\right) = \sum_l (Rh_l) \otimes (Tk_l).$$

Proof. Define $B : H \times K \to H \otimes K$ by $B(h,k) = (Rh) \otimes (Tk)$. This is obviously bilinear. So, there exists a unique linear map $L_B : H \otimes K \to H \otimes K$. Now set $R \otimes T = L_B$.

⊠

Properties: (1) If $R_i : H \to H$, $T_i : K \to K$, for $i = 1, 2$, then

$$(R_1 \otimes T_1)(R_2 \otimes T_2) = (R_1R_2) \otimes (T_1T_2).$$

(2) $(R \otimes T)^* = R^* \otimes T^*$.

Proof of (2). We have that

$$\begin{aligned}
\langle h_1 \otimes k_1 | (R \otimes T)^*(h_2 \otimes k_2)\rangle &= \langle (R \otimes T)(h_1 \otimes k_1) | h_2 \otimes k_2\rangle \\
&= \langle Rh_1 \otimes Tk_1 | h_2 \otimes k_2\rangle \\
&= \langle Rh_1 | h_2\rangle_H \cdot \langle Tk_1 | k_2\rangle_K \\
&= \langle h_1 | R^* h_2\rangle_H \cdot \langle k_1 | T^* k_2\rangle_K \\
&= \langle h_1 \otimes k_1 | (R^* \otimes T^*)(h_2 \otimes k_2)\rangle.
\end{aligned}$$

⊠

Remark. If lab A has measurement system $\{M_m\}$ and state space H, and if lab B has state space K, let $H \otimes K$ be the state space of the composite system. Then the measurement system for A is $\{M_m \otimes I_k\}$. So, if we had states ψ in A and ϕ in B, then

$$\begin{aligned}
p_m^{AB}(\psi \otimes \phi) &= ||(M_m \otimes I_k)(\psi \otimes \phi)||^2 \\
&= ||(M_m\psi) \otimes \phi||^2 \\
&= \langle (M_m\psi) \otimes \phi | (M_m\psi) \otimes \phi\rangle \\
&= \langle (M_m \otimes I)(\psi \otimes \phi) | (M_m \otimes I)(\psi \otimes \phi)\rangle \\
&= \langle \psi \otimes \phi | (M_m \otimes I)^*(M_m \otimes I)(\psi \otimes \phi)\rangle \\
&= \langle \psi \otimes \phi | (M_m^* M_m \otimes I)(\psi \otimes \phi)\rangle \\
&= \langle \psi | M_m^* M_m \psi\rangle_H \langle \phi | \phi\rangle_K \\
&= ||M_m\psi||^2 \\
&= p_m^A(\psi).
\end{aligned}$$

10.4 Two Applications of Entanglement

Example 1 - Simultaneous transfer of information; Eavesdropping: A and B share two entangled photons. Suppose the state is

$$\gamma = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

A prepares the experiment

$$M_0^* M_0 = |0\rangle\langle 0|, M_1^* M_1 = M_1 = |1\rangle\langle 1|.$$

Then,

$$\begin{aligned}
p_0(\gamma) &= \langle \gamma | (M_0 \otimes I)\gamma\rangle \\
&= \left\langle \frac{e_0 \otimes e_0 + e_1 \otimes e_1}{\sqrt{2}}, \frac{(M_0 e_0) \otimes e_0 + (M_0 e_1) \otimes e_1}{\sqrt{2}} \right\rangle \\
&= \left\langle \frac{e_0 \otimes e_0 + e_1 \otimes e_1}{\sqrt{2}}, \frac{e_0 \otimes e_0 + 0}{\sqrt{2}} \right\rangle \\
&= {}^1\!/_2 + 0 \\
&= {}^1\!/_2.
\end{aligned}$$

So, $p(\gamma) = {}^1/_2$.

If we get outcome 0, γ changes to

$$\frac{(M_0 \otimes I)\gamma}{\sqrt{p_0(\gamma)}} = \frac{\frac{e_0 \otimes e_0}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} = e_0 \otimes e_0.$$

If we get outcome 1, γ changes to $e_1 \otimes e_1$.

Suppose lab B does measurements $I \otimes M_0, I \otimes M_1$. If A obtained outcome 0, then in Lab B, we get outcome 0 with probability 1. If A obtained outcome 1, then in lab B, we get outcome 1 with probability 1.

11 Day - 19/Sep/11

11.1 Example from Last Session

Example: "Super Dense Coding." Given two entangled qubits and state

$$\gamma = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

suppose that the first qubit is in Lab A and the second in Lab B.

Lab A		Send to Lab B
Does Nothing	$\longrightarrow$	$\gamma = \frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
Multiply by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$	$\longrightarrow$	$\gamma = \frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
Multiply by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\longrightarrow$	$\gamma = \frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
Multiply by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$	$\longrightarrow$	$\gamma = \frac{-\|10\rangle+\|01\rangle}{\sqrt{2}}$

Hence, the surprise is that Lab A can send one qubit but can communicate four possible pieces of information.

Similarly, if they share $2m$ entangled qubits, Lab A keeping m and Lab B keeping the other m, if Lab A does something to its m and then sends to Lab B, it can communicate 4^m possible pieces of information.

11.2 Some Binary and Quantum Gates

G. Boole (1854): Set $0 = F =$ "not in set" and $1 = T =$ "in set."

1 Bit Gates

NOT : $0 \to 1$, $1 \to 0$

1 Qubit Gates

NOT : $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which is unitary.

Others :

$$\begin{array}{rcccl} Z & = & \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) & := & e_0 \to e_0, e_1 \to -e_1 \\ Y & = & \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) & := & e_0 \to ie_1, e_1 \to -ie_0 \\ H & = & \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) & & \\ S & = & \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{smallmatrix}\right) & & \end{array}$$

H is called the *Hadamard gate* and has the property $H^2 = X$. S has the property that the two matrices generate all 2×2 unitaries.

2 Bit Gates

AND or $\cap$:

Input		*Output*
$0,0$	$\to$	0
$0,1$	$\to$	0
$1,0$	$\to$	0
$1,1$	$\to$	1

OR or $\cup$:

Input		*Output*
$0,0$	$\to$	0
$0,1$	$\to$	1
$1,0$	$\to$	1
$1,1$	$\to$	1

XOR or $A\delta B$:

Input		*Output*
$0,0$	$\to$	0
$0,1$	$\to$	1
$1,0$	$\to$	1
$1,1$	$\to$	0

NAND or $A^c \cup B^c$:

Input		*Output*
$0,0$	$\to$	1
$0,1$	$\to$	1
$1,0$	$\to$	1
$1,1$	$\to$	0

NOR or $A^c \cap B^c$:

Input		*Output*
$0,0$	$\to$	1
$0,1$	$\to$	0
$1,0$	$\to$	0
$1,1$	$\to$	0

Notes (1) C.S. Pierce (1880): Proved that NAND alone generates all other Boolean operations. In 1886, he wrote to N. Tesla and explained how Boolean operations could be done via circuits. Tesla built and patented the idea.

(2) Sheffer (1913): Proved that NOR generates all other Boolean operations.

2 Qubit Gates

No 2 bit gate is an allowable quantum gate because they have the property $2dim \to 1dim$, which are not unitary. They are also known as *irreversible*.

CNOT :

Input		*Output*
$0,0$	$\to$	$0,0$
$0,1$	$\to$	$0,1$
$1,0$	$\to$	$1,1$
$1,1$	$\to$	$1,0$

As a matrix, we have that

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

which is unitary.

3 Bit Gates

Tommaso Toffoli (1980): Proved that there existed a reversible binary gate that generates all Boolean operations, called the *Toffoli gate* or CCNOT.

CCNOT :

Input		*Output*
$0,0,0$	$\to$	$0,0,0$
$0,0,1$	$\to$	$0,0,1$
$0,1,0$	$\to$	$0,1,0$
$0,1,1$	$\to$	$0,1,1$
$1,0,0$	$\to$	$1,0,0$
$1,0,1$	$\to$	$1,0,1$
$1,1,0$	$\to$	$1,1,1$
$1,1,1$	$\to$	$1,1,0$

As a matrix, we have that

$$CCNOT = \begin{pmatrix} I_6 & 0 \\ 0 & \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \end{pmatrix}$$

which is unitary.

12 Day - 21/Sep/11

12.1 Correction from Last Time

Define

$$\begin{aligned} \mathrm{NOT}X &:= \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \\ H &:= \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right). \end{aligned}$$

Then,

$$H^2 = \frac{1}{2}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right) = I,$$

$$He_0 = H\left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right) = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\ 1\end{smallmatrix}\right) = \frac{e_0 + e_1}{\sqrt{2}},$$

which is a 45 degree rotation,

$$Xe_0 = \left(\begin{smallmatrix}0\\ 1\end{smallmatrix}\right) = e_1,$$

which is a 90 degree rotation,

$$Xe_1 = \left(\begin{smallmatrix}1\\ 0\end{smallmatrix}\right),$$

which rotates 90 degrees, and,

$$He_1 = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1\\ -1\end{smallmatrix}\right).$$

Hence, X is a reflection about $45°$. Since $H^2 = I$, H is also a reflection about $\frac{45°}{2} = \frac{\pi}{8}$.

12.2 Correction from Last Time

CNOT is described as

Input	Output
00	00
01	01
10	11
11	10

Hence, when $a = 0$, do nothing and save a. When $a = 1$, do NOT on b and save a.

CCNOT is described as

Input	Output
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

Hence, when $a = 0$, do nothing to b, c and save a. When $a = 1$, do CNOT to b, c.

12.3 Circuit Diagrams, Modular Arithmetic

We identify $\mathbb{Z}_2 \cong \{0, 1\}$. Then,

$$\text{NOT} = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}.$$

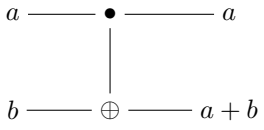
What we really mean is $a \mapsto a + 1$. With CNOT, we have

$$\text{CNOT: } |a, b\rangle = |a\rangle \otimes |b\rangle = e_a \otimes e_b,\ a, b \in \mathbb{Z}_2.$$

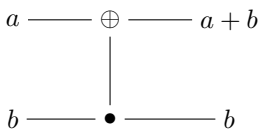
The operation is then $|a, b\rangle \mapsto |a, b + a\rangle$. This tells what the math does on the basis. Here, we used the notation

$$e_a \otimes e_b = |a, b\rangle.$$

Circuit Diagrams:



The diagram

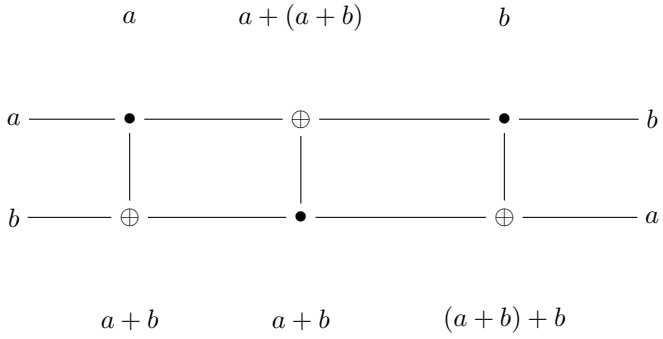


corresponds to the description and matrix:

Input	Output
00	00
01	11
10	10
11	01

; $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

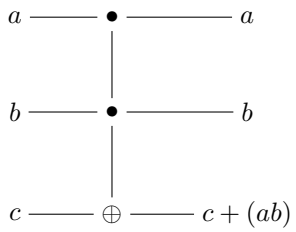
The diagram



corresponds to the permutation matrix

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

The Toffoli operation CCNOT is given by the diagram:



12.4 Cloning and No Cloning

For 1 bit, we have

$$\begin{aligned} 0 &\rightarrow 00 \\ 1 &\rightarrow 11 \end{aligned}$$

and

$$|a\rangle \rightarrow |aa\rangle.$$

In other words, if we take the unitary CNOT, call it U, then

$$U(e_a \otimes e_0) = e_a \otimes e_a.$$

On the computational basis, CNOT can "clone:"

$$|i_1, \ldots, i_n\rangle = e_{i_1} \otimes \ldots \otimes e_{i_n} \in \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2.$$

Then there exists a unitary U such that

$$U(|i_1, \ldots, i_n\rangle \otimes |0, \ldots, 0\rangle) = |i_1, \ldots, i_n\rangle \otimes |i_1, \ldots, i_n\rangle;$$

i.e., the computational basis can be cloned.

What does "no cloning" mean? Take

$$\psi = \alpha e_0 + \beta e_1 = \alpha|0\rangle + \beta|1\rangle.$$

Apply the CNOT unitary to $\psi \otimes e_0$:

$$\begin{aligned} U(\psi \otimes e_0) &= U((\alpha e_0 + \beta e_1) \otimes e_0) \\ &= U(\alpha e_0 \otimes e_0 + \beta e_1 \otimes e_0) \\ &\stackrel{?}{=} \psi \otimes \psi \\ &= \alpha^2 e_0 \otimes e_0 + \alpha\beta(e_0 \otimes e_1 + e_1 \otimes e_0) + \beta^2 e_1 \otimes e_1. \end{aligned}$$

When $\alpha\beta \neq 0$, then they are not equal. The only case for $U(\psi \otimes e_0) = \psi \otimes \psi)$ is $\psi = e_0$ or $\psi = e_1$.

No Cloning Theorem. To "clone," we want a state ψ and a unitary U on $H \otimes H$ such that

$$U(\psi \otimes \phi) = \psi \otimes \psi$$

for all $\psi \in H$. We show that this is impossible.

Proof. If $U(\psi \otimes \phi) = \psi \otimes \psi$ for all $\psi \in H$, then

$$U((-\psi) \otimes \phi) = (-\psi) \otimes (-\psi) = \psi \otimes \psi$$

for all $\psi \in H$. On the other hand,

$$U((-\psi) \otimes \phi) = U(-(\psi \otimes \phi)) = -U(\psi \otimes \phi) = -(\psi \otimes \psi)$$

for all $\psi \in H$, which is a contradiction.

$\boxtimes$

Remark. This proves that you cannot "clone" everything, but can "clone" the computational basis.

13 Day - 23/Sep/11

13.1 Quantum Parallelism

Recall that

$$H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$$

and

$$He_0 = \frac{e_0 + e_1}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Also,

$$\begin{aligned} H^{\otimes N}(e_0 \otimes \ldots \otimes e_0) &= (He_0) \otimes \ldots \otimes (He_0) \\ &= \frac{e_0 + e_1}{\sqrt{2}} \otimes \ldots \otimes \frac{e_0 + e_1}{\sqrt{2}}. \end{aligned}$$

When $N = 2$,

$$\begin{aligned} \frac{e_0 + e_1}{\sqrt{2}} \otimes \frac{e_0 + e_1}{\sqrt{2}} &= \frac{e_0 \otimes e_0 + e_0 \otimes e_1 + e_1 \otimes e_0 + e_1 \otimes e_1}{(\sqrt{2})^2} \\ &= \left(\frac{1}{\sqrt{2}}\right)^2 \sum_{J \in \mathbb{Z}_2^2} e_J. \end{aligned}$$

In general,

$$H^{\otimes N}(e_0 \otimes \ldots \otimes e_0) = \left(\frac{1}{\sqrt{2}}\right)^N \sum_{J \in \mathbb{Z}_2^N} e_J = \left(\frac{1}{\sqrt{2}}\right)^2 \sum_J |J\rangle.$$

Application. Suppose we have a function with two outcomes, say $f : \mathbb{Z}_2^N \to \mathbb{Z}_2$. We want to count how many of each outcome; i.e., we want

$$M = \#\{J \in \mathbb{Z}_2^N \ : \ f(J) = 0\}.$$

Now suppose we have $e_J \otimes e_i \to e_J \otimes e_{i+f(J)}$. Then,

$$\begin{aligned} \langle e_{J_1} \otimes e_{i_1+f(J_1)} | e_{J_2} \otimes e_{i_2+f(J_2)} \rangle &= \langle e_{J_1} | e_{J_2} \rangle \langle e_{i_1+f(J_1)} | e_{i_2+f(J_2)} \rangle \\ &= \begin{cases} 1, & J_1 = J_2, i_1 = i_2, \\ 0, & otherwise. \end{cases} \end{aligned}$$

We conclude that

$$\{e_J \otimes e_{i+f(J)} \ : \ J \in \mathbb{Z}_2^N\}$$

is an orthonormal basis for $(\mathbb{C}^2)^{\otimes N} \otimes \mathbb{C}^2$. So, there exists a unitary

$$U_f : (\mathbb{C}^2)^{\otimes (N+1)} \to (\mathbb{C}^2)^{\otimes (N+1)}$$

such that

$$U_f(e_J \otimes e_i) = e_J \times e_{i+f(J)}.$$

This unitary U_f is called an *oracle* for f.

Proposition. Given $\gamma \in H$ with $||\gamma|| = 1$, measurements $P_0 = M_0^* M_0 = |\gamma\rangle\langle\gamma|$, $P_1 = M_1^* M_1 = I - P_0$, and $\psi \in H$, then

$$p_0(\psi) = |\langle\gamma|\psi\rangle|^2, p_1(\psi) = 1 - |\langle\gamma|\psi\rangle|^2.$$

Proof. We have

$$p_0(\psi) = \langle\psi|M_0^* M_0 \psi\rangle = ||M_0\psi||^2,$$

$$\begin{aligned} M_0|\psi\rangle &= |\gamma\rangle\langle\gamma|\psi\rangle \cdot ||M_0\psi||^2 \\ &= ||\gamma||^2 |\langle\gamma|\psi\rangle|^2 \\ &= |\langle\gamma|\psi\rangle|^2. \end{aligned}$$

Take

$$X = (He_0) \otimes \ldots \otimes (He_0) = \left(\frac{1}{\sqrt{2}}\right)^N \sum_J e_J.$$

Input $x \otimes e_0$ into U_f to get the output

$$U_f(x \otimes e_0) = \left(\frac{1}{\sqrt{2}}\right)^N \sum_J U_f(e_J \otimes e_0) = \left(\frac{1}{\sqrt{2}}\right)^N \sum_J e_J \otimes e_{f(J)}.$$

Now, prepare measurements with $\gamma = x \otimes e_0$. For input $x \otimes e_0$,

$$\begin{aligned} p_0(U_f(x \otimes e_0)) &= \langle x \otimes e_0 | \left(\frac{1}{\sqrt{2}}\right)^N \sum_J e_J \otimes e_{f(J)} \rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)^N \sum_J \langle x|e_J\rangle\langle e_0|e_{f(J)}\rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)^N \sum_J \left(\frac{1}{\sqrt{2}}\right)^N \langle e_0|e_{f(J)}\rangle \\ &= \frac{1}{2^N} \cdot \#\{J|f(J)=0\} \\ &= \frac{M}{2^N}. \end{aligned}$$

This implies that $p_1(U_f(x \otimes e_0)) = 1 - \frac{M^2}{4^N}$, $p_0(U_f(x \otimes e_0)) = \frac{M_2}{4^N}$.

⊠

Remark. Note that this is a Bernoulli trial. Outcome 0 has probablity $p = \frac{M^2}{4^N}$ and outcome 1 has probablity $q = 1 - p$. Repeat K times, and we get outcome 0 L of those times. Then, $\frac{L}{K}$ is an estimator for p.

The cost is that we used $K(N+1)$ qubits. Take $K << \frac{2^N}{N+1}$ and we can get an estimate for M. We only want

$$\left|\frac{M^2}{4^N} - \frac{L}{K}\right|$$

in some confidence interval. Hence, we can take K to be quite small when compared to $\frac{2^N}{N+1}$.

14 Day - 26/Sep/11

14.1 Ensembles or Mixed States

Motivation: (1) Start with a state $\psi = a|0\rangle + b|1\rangle$ such that $|a|^1 + |b|^2 = 1$ and measurements $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Recall, after measurement, $p_0(\psi) = |a|^2$ and after state becomes

$$\frac{M_0\psi}{||M_0\psi||} = \frac{a}{|a|}|0\rangle;$$

similarly, $p_1(\psi) = |b|^2$ and after state becomes

$$\frac{M_1\psi}{||M_1\psi||} = \frac{b}{|b|}|1\rangle.$$

Later, we want to do measurements $\{\tilde{M}_\alpha\}$. What will be the expected outcomes?

Outcome α: $p_\alpha = |a|^2||\tilde{M}_\alpha(\frac{a}{|a|}|0\rangle)||^2 + |b|^2||\tilde{M}_\alpha(\frac{b}{|b|}|1\rangle)||^2$.

Definition. An *ensemble* $\{p_i, \psi_i\}_{i=1}^L$ is a set of states $\{\psi_i\}$ together with probabilities $p_i \geq 0$, $\sum_{i=1}^L p_i = 1$.

Given a measurement system $\{M_\alpha\}$, the probability of outcome α given this ensemble is

$$p_\alpha(\{p_i, \psi_i\}) = \sum_{i=1}^{L} p_i ||M_\alpha(\psi_i)||^2.$$

(2) Suppose Lab A has state space H_A. In reality, A is seldom truly isolated from the outside world. Imagine the environment described by a state space H_E. Our state really lives in $H_A \otimes H_E$. When we form measurements in Lab A, $\{M_\alpha : H_A \to H_A\}$, they really act as $M_\alpha \otimes I_{H_E}$.

Let $\psi \in H_A \otimes H_E$ such that $||\psi|| = 1$. Pick an orthonormal basis $\{f_l\}$ for H_E. Write

$$\psi = \sum_l \phi_l \otimes f_l,$$

$$\begin{aligned} ||\psi||^2 &= \langle \sum_l \phi_l \otimes f_l | \sum_k \phi_k \otimes f_k \rangle \\ &= \sum_{l,k} \langle \phi_l \otimes f_l : \phi_k \otimes f_k \rangle \\ &= \sum_{l,k} \langle \phi_l | \phi_k \rangle \langle f_l | f_k \rangle \\ &= \sum_l ||\phi_l||^2. \end{aligned}$$

Therefore, $\sum_l ||\phi_l||^2 = 1$. Also,

$$\begin{aligned} p_\alpha(\psi) &= ||(M_\alpha \otimes I)(\psi)||^2 \\ &= ||\sum_l (M_\alpha \phi_l) \otimes (I f_l)||^2 \\ &= ||\sum_l M_\alpha(\phi_l) \otimes f_l||^2 \\ &= \sum_l ||M_\alpha(\phi_l)||^2. \end{aligned}$$

Form an ensemble $\{p_l, \frac{\phi_l}{||\phi_l||}\}$, $p_l = ||\phi_i||^2 \geq 0$, and $\sum p_1 = \sum ||\phi_l||^2 = 1$. Then,

$$\begin{aligned} p_\alpha(\{p_l, \frac{\phi_l}{||\phi_l||}\}) &= \sum_l p_l ||M_\alpha(\frac{\phi_l}{||\phi_l||})||^2 \\ &= \sum_l p_l \cdot \frac{1}{||\phi_l||^2} ||M_\alpha(\phi_l)||^2 \\ &= \sum_l ||M_\alpha(\phi_l)||^2 \\ &= p_\alpha(\psi). \end{aligned}$$

So, $\psi \in H_A \otimes H_E$ behaves like the ensemble $\{p_l, \frac{\phi_l}{||\phi_l||}\}$.

14.2 Von Neumann's Density Matrix Approach

Von Neumann noticed (1) dealing with ensembles is messy from this viewpoint, and (2) state are not really vectors but functionals.

Given a state $\psi \in H_A$, then $e^{i\theta}\psi$ is also a state. For any measurement M_α,

$$p_\alpha(\psi) = ||M_\alpha \psi||^2 = ||M_\alpha(e^{i\theta}\psi)||^2 = p_\alpha(e^{i\theta}\psi).$$

Hence, measurements really identify $\psi \sim e^{i\theta}\psi$.

Note that

$$|\psi\rangle\langle\psi| = |e^{i\theta}\psi\rangle\langle e^{i\theta}\psi|.$$

In coordinates, if $\psi = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, then

$$|\psi\rangle\langle\psi| = (\alpha_i \overline{\alpha}_j),$$

$$|e^{i\theta}\psi\rangle\langle e^{i\theta}\psi| = ((e^{i\theta}\alpha_i)\overline{(e^{i\theta}\alpha_j)}) = (\alpha_i \overline{\alpha}_j).$$

Hence, we really think of the projection determined by ψ and not the vector.

Given <u>any</u> vector $\gamma = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$,

$$|\gamma\rangle\langle\gamma| = (\beta_i \overline{\beta}_j) = \gamma\gamma^*,$$

and

$$||\gamma|^2 = \sum_{i=1}^{n} |\beta_i|^2 = Tr(|\gamma\rangle\langle\gamma|).$$

Therefore, if we start with a state γ, and M_α is some measurement,

$$\begin{aligned} p_\alpha(\psi) &= ||M_\alpha\psi||^2 \\ &= Tr(|M_\alpha\psi\rangle\langle M_\alpha\psi|) \\ &= Tr((M_\alpha\psi)(M_\alpha\psi)^*) \\ &= Tr(M_\alpha\psi\psi^* M_\alpha^*) \\ &= Tr((M_\alpha^* M_\alpha)(\psi\psi^*)). \end{aligned}$$

This implies

$$p_\alpha(\psi) = ||M_\alpha \psi||^2 = Tr((M_\alpha^* M_\alpha)(\psi\psi^*)).$$

For an ensemble $\{p_l, \psi_l\}$,

$$\begin{aligned} p_\alpha(\{p_l, \psi_l\}) &= \sum_l p_l ||M_\alpha \psi_l||^2 \\ &= \sum_l p_l Tr((M_\alpha^* M_\alpha)(\psi_l \psi_l^*)) \\ &= Tr((M_\alpha^* M_\alpha)(\sum_l p_l \psi_l \psi_l^*)). \end{aligned}$$

So, for any measurement $\{M_\alpha\}$,

$$p_\alpha(\{p_l, \psi_l\}) = Tr(M_\alpha^* M_\alpha(P)),$$

where $P = \sum_l p_l |\psi_l\rangle\langle\psi_l|$.

Definition. $P = \sum_l p_l |\psi_l\rangle\langle\psi_l|$ is called the *density matrix* of the ensemble.

15 Day - 28/Sep/11

15.1 Continuation

Recall: For an ensemble $\{p_i, \psi_i\}$, we associate the density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. For measurements $\{M_\alpha\}$,

$$\begin{aligned} p_\alpha(\{p_i, \psi_i\}) &= \sum p_i ||M_\alpha \psi_i||^2 \\ &= Tr((M_\alpha^* M_\alpha)\rho) \\ &= \langle M_\alpha^* M_\alpha | \rho \rangle_{\mathcal{L}(H_A)}. \end{aligned}$$

Question: Which matrices are density matrices of an ensemble?

Proposition. For $\rho \in \mathcal{L}(H_A)$, then there exists an ensemble $\{p_i, \psi_i\}$ such that ρ is the density matrix of the ensemble if and only if $\rho \geq 0$ and $Tr(\rho) = 1$.

Proof. ($\Rightarrow$) Write $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$. This implies $\rho \geq 0$. Also,

$$Tr(\rho) = \sum p_i Tr(|\psi_i\rangle\langle\psi_i|) = \sum p_i = 1.$$

($\Leftarrow$) Since $\rho = \rho^*$, ρ has an orthonormal basis of eigenvectors. Let ψ, $i = 1, \ldots, n$, be an orthonormal basis such that $\rho\psi_i = \lambda_i \psi_i$. $\rho \geq 0$ implies $\lambda_i \geq 0$. Recall that $Tr(\rho) = \sum \lambda_i = 1$. Finally, we know $\rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$. Therefore, ρ is the density matrix of the ensemble $\{\lambda_i, \psi_i\}$.

Definition. $\rho \in \mathcal{L}(H_A)$ is called a *density matrix* when $\rho \geq 0$ and $Tr(\rho) = 1$. We call the ensemble $\{\lambda_i, \psi_i\}$, consisting of eigenvalues and an orthonormal basis of eigenvectors, the *spectral ensemble*.

Remark. Given ρ such that $\rho \geq 0$, $Tr(\rho) = 1$, in general, there are many ensembles that it is the density matrix of. Write

$$\rho = XX^* = [c_1 \vdots \ldots \vdots c_n] \begin{bmatrix} c_1^* \\ \ldots \\ \vdots \\ \ldots \\ c_n^* \end{bmatrix} = c_1 c_1^* + \ldots + c_n c_n^*.$$

Let $\psi_i = \frac{c_i}{||c_i||}$, which is a unit vector, and $p_i = ||c_i||^2$. This implies

$$\rho = \sum p_i \psi_i \psi_i^* = \sum p_i |\psi_i\rangle\langle\psi_i|.$$

Then,

$$1 = Tr(\rho) = \sum p_i Tr(|\psi_i\rangle\langle\psi_i|) = \sum p_i.$$

Therefore, $\{p_i, \psi_i\}$ is an ensemble and ρ is the density matrix of this ensemble.

Hence, the map $\{ensemble\} \mapsto \{density\ matrix\}$ is a many-to-one mapping. No uniqueness in general.

Question. Suppose we start with a standard state ψ. We get the density matrix

$$\rho = |\psi\rangle\langle\psi|.$$

What ensemble represents it?

Suppose $\{p_i, \psi_i\}_{i=1}^m$ so that $\rho = \sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i|$. Then,

$$1 = rank(\rho) = rank(\sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i|).$$

If we take a vector $\gamma \perp \psi$, then

$$\begin{aligned} \langle\gamma|\rho\gamma\rangle &= \langle\gamma|\psi\rangle\langle\psi|\gamma\rangle \\ &= \langle\psi|\gamma\rangle\langle\gamma|\psi\rangle \\ &= |\langle\psi|\gamma\rangle|^2 \\ &= 0. \end{aligned}$$

Therefore,

$$\begin{aligned} 0 &= \langle\gamma| \sum p_i |\psi_i\rangle\langle\psi_i|\gamma\rangle \\ &= \sum p_i \langle\gamma|\psi_i\rangle\langle\psi_i|\gamma\rangle \\ &= \sum p_i |\langle\psi_i|\gamma\rangle|^2. \end{aligned}$$

This implies $\gamma \perp \psi_i$, and so, ψ_i is parallel to ψ. Therefore, $\psi_i = \beta_i \psi$, with $|beta_i| = 1$. Hence,

$$|\psi_i\rangle\langle\psi_i| = |\psi\rangle\langle\psi|.$$

The density matrices (or states ψ) are called the *pure states*.

15.2 Composite Ensembles

Suppose we have for Lab A and Lab B the state spaces H_A, H_B. Let $\{p_i, \psi_i\}$ be an ensemble in A and $\{q_l, \phi_i\}$ an ensemble in B. The composite should be represented by a density matrix on $H_A \otimes H_B$.

Recall that if we just have ψ in A and ϕ in B, then it is in state $\psi \otimes \phi$. If we had a measurement system $\{M_\alpha\}$ on $H_A \otimes H_B$, then

$$p_\alpha(\psi_i \otimes \phi_l) = \langle \psi_i \otimes \phi_l | M_\alpha^* M_\alpha (\psi_i \otimes \phi_l) \rangle.$$

But, $\psi_i \otimes \phi_l$ will appear with probablity $p_i q_l$. Hence,

$$\begin{aligned} p_\alpha(composite) &= \sum_{i,l} p_i q_l \langle \psi_i \otimes \phi_l | M_\alpha^* M_\alpha | \psi_i \otimes \phi_l \rangle \\ &= p_\alpha(\{p_i q_l, \psi_i \otimes \phi_l\}). \end{aligned}$$

the density matrix is

$$\rho = \sum_{i,l} p_i q_l |\psi_i \otimes \phi_l\rangle\langle \psi_i \otimes \phi_l| = \sum p_i q_l (|\psi_i\rangle\langle\psi_i|) \otimes (|\phi_l\rangle\langle\phi_l|).$$

To see this, we only need to verify that if $\psi \in H_A, \phi \in H_B$, then

$$|\psi \otimes \phi\rangle\langle \psi \otimes \phi| \stackrel{?}{=} (|\psi\rangle\langle\psi|) \otimes (|\phi\rangle\langle\phi|).$$

Note that any vector in $H_A \otimes H_B$ is a sum of vectors of the form $h \otimes k$. To see if two linear maps on $H_A \otimes H_B$ are the same, it is enough to check on $h \otimes k$:

$$|\psi \otimes \phi\rangle\langle \psi \otimes \phi|(h \otimes k) = |\psi \otimes \phi\rangle\langle\psi|h\rangle_{H_A}\langle\phi|k\rangle_{H_B},$$

$$\begin{aligned} (|\psi\rangle\langle\psi|) \otimes (|\phi\rangle\langle\phi|)(h \otimes k) &= (|\psi\rangle\langle\psi|h\rangle_{H_A}) \otimes (|\phi\rangle\langle\phi|k\rangle_{H_B}) \\ &= \langle\psi|h\rangle_{H_A}\langle\phi|k\rangle_{H_B}|\psi \otimes \phi\rangle. \end{aligned}$$

Hence, they are the same.

15.3 Partial Traces

Motivation: Suppose we have Lab A, Lab B. So a general mixed state is given by a density matrix $\rho \in \mathcal{L}(H_A \otimes H_B)$ such that $\rho \geq 0$ and $Tr(\rho) = 1$. Measurements $\{M_\alpha\}$ in Lab A in the composite act as the operators $\{M_\alpha \otimes I_{H_B}\}$. So,

$$p_\alpha(\rho) = Tr((M_\alpha \otimes I)^*(M_\alpha \otimes I)\rho) = Tr((M_\alpha^* M_\alpha \otimes I)\rho).$$

The question is how do we compute? We will show that there exists a density matrix $\rho^A \in \mathcal{L}(H_A)$ such that for any $\{M_\alpha\}$,

$$Tr_{H_A \otimes H_B}((M_\alpha^* M_\alpha \otimes I)\rho) = Tr_{H_A}((M_\alpha^* M_\alpha)\rho^A).$$

16 Day - 30/Sep/11

16.1 More on Traces

Identify $\mathcal{L}(\mathbb{C}^n) \cong M_n$ and let $A = (a_{ij})$. Then

$$tr(A) = \sum_{i=1}^{n} a_{ii} = \sum_{i=1}^{n} \langle e_i | Ae_i \rangle.$$

Proposition. Let $\{u_1, \ldots, u_n\}$ be any orthonormal basis for $\mathbb{C}^n$. Then,

$$tr(A) = \sum_{i=1}^{n} \langle u_i | Au_i \rangle.$$

Proof. Let

$$U = [u_1 \vdots \ldots \vdots u_n].$$

Then U is unitary and $Ue_i = u_i$ for all i. So,

$$\begin{aligned} \sum_{i=1}^{n} \langle u_i | Au_i \rangle &= \sum_{i=1}^{n} \langle Ue_i | AUe_i \rangle \\ &= \sum_{i=1}^{n} \langle e_i | U^*AUe_i \rangle \\ &= tr(U^*AU) \\ &= tr(AUU^*) \\ &= tr(A). \end{aligned}$$

⊠

Recall. For $R \in \mathcal{L}(H_A)$, $T \in \mathcal{L}(H_B)$, there exists $R \otimes T \in \mathcal{L}(H_A \otimes H_B)$ such that

$$(R \otimes T)(h \otimes k) = (Rh) \otimes (Tk).$$

Proposition. $tr(R \otimes T) = tr(R)tr(T)$.

Proof. Pick orthonormal bases $\{e_1, \ldots, e_m\}$ for H_A and $\{f_1, \ldots, f_p\}$ for H_B. Then,

$$\{e_i \otimes f_j \, : \, 1 \leq i \leq m, 1 \leq j \leq p\}$$

is an orthonormal basis for $H_A \otimes H_B$. Therefore,

$$\begin{aligned} tr(R \otimes T) &= \sum_{i=1}^{m}\sum_{j=1}^{p}\langle e_i \otimes f_j | (R \otimes T)(e_i \otimes f_j)\rangle \\ &= \sum_{i}\sum_{j}\langle e_i \otimes f_j | (Re_i) \otimes (Tf_j)\rangle \\ &= \sum_{i}\sum_{j}\langle e_i | Re_i\rangle\langle f_j | Tf_j\rangle \\ &= (\sum_{i}\langle e_i | Re_i\rangle)(\sum_{j}\langle f_j | Tf_j\rangle) \\ &= tr(R)tr(T). \end{aligned}$$

$\boxtimes$

What we really have is a mapping $\Gamma : \mathcal{L}(H_A) \otimes \mathcal{L}(H_B) \to \mathcal{L}(H_A \otimes H_B)$, $R \otimes T \mapsto R \otimes T$.

Proposition. If $dim(H_A), dim(H_B) < +\infty$, then Γ is a vector space isomorphism.

Proof. Let $dim(H_A) = m$, $dim(H_B) = p$. Then, $dim(\mathcal{L}(H_A)) = m^2$, $dim(\mathcal{L}(H_B)) = p^2$. Hence,

$$dim((\mathcal{L}(H_A)) \otimes (\mathcal{L}(H_B))) = m^2p^2.$$

Also, $dim(H_A \otimes H_B) = mp$. Hence,

$$dim(\mathcal{L}(H_A \otimes H_B)) = (mp)(mp) = m^2p^2.$$

So, the dimensions are the same.

To show that Γ is an isomorphism, it is enough to show that it is one-to-one; i.e., show $ker(\Gamma) = \{0\}$. Identify $\mathcal{L}(H_B) \cong M_p$, which has a basis $\{E_{ij} : 1 \leq i, j \leq p\}$. Pick an orthonormal basis $\{f_1, \ldots, f_p\}$ for H_B such that

$$E_{ij}f_k = \begin{cases} f_i, & j = k, \\ 0, & j \neq k. \end{cases} .$$

Given $X \in \mathcal{L}(H_A) \otimes \mathcal{L}(H_B)$, there exists a unique $X_{ij} \in \mathcal{L}(H_A)$ such that

$$X = \sum_{i,j=1}^{p} X_{ij} \otimes E_{ij}.$$

Then, $X = 0$ if and only if $X_{ij} = 0$ for all i, j. So, we want to show that $\Gamma(X) = 0$ implies $X_{ij} = 0$ for all i, j. Now,

$$\begin{aligned} \Gamma(X) : H_A \otimes H_B \to H_A \otimes H_B, \Gamma(X)(h \otimes k) &= \sum_{i,j=1}^{p}(X_{ij} \otimes E_{ij})(h \otimes k) \\ &= \sum_{i,j=1}^{p}(X_{ij}h) \otimes (E_{ij}k) \\ &= (*). \end{aligned}$$

So, $\Gamma(X) = 0$ implies $(*) = 0$ for all h, k. Pick $k = f_l$. Then,

$$\begin{aligned} 0 &= \Gamma(X)(h \otimes f_l) \\ &= \sum_{i,j=1}^{p} (X_{ij}h) \otimes (E_{ij}f_l) \\ &= \sum_{i=1}^{p} (X_{il}h) \otimes (f_i); \end{aligned}$$

i.e., $X_{il}h = 0$ for all i, h. This implies $X_{il} = 0$ for all i. Now repeat for all l and we obtain $X_{il} = 0$ for all i, l. Therefore, $X = 0$.

$\boxtimes$

16.2 Partial Trace

Define the mapping $tr_B : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_A)$ as follows: identify $\mathcal{L}(H_A \otimes H_B) = \mathcal{L}(H_A) \otimes \mathcal{L}(H_B)$. Given $X = \sum_l R_l \otimes T_l$, then

$$tr_B(X) = \sum_l tr(T_l)R_l.$$

This map is well-defined since, $\mathcal{L}(H_A) \times \mathcal{L}(H_B) \to \mathcal{L}(H_A), (R, T) \mapsto tr(T)R$, is bilinear and by the universal property of tensor products. We also denote this by

$$X^A = tr_B(X) \in \mathcal{L}(H_A).$$

Similarly, we have $tr_A : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_B)$,

$$tr_A(X) = \sum_l tr(R_l)T_l,$$

and we write $X^B = tr_A(X) \in \mathcal{L}(H_B)$.

16.3 Partial Traces and Measurements

Suppose we have Lab A, B with respective spaces H_A, H_B. Then the composite space is $H_A \otimes H_B$. Then the density matrix is given by $p \in \mathcal{L}(H_A \otimes H_B)$ such that $p \geq 0$, $tr(p) = 1$.

Suppose that we can only do measurements in Lab A: $\{M_\alpha, \sum M_\alpha^* M_\alpha = I$. Then the measurements really look like $M_\alpha \otimes I_{H_B}$.

Write $p = \sum_l R_l \otimes T_l$. Then,

$$\begin{aligned} p_\alpha(p) &= tr((M_\alpha \otimes I)^*(M_\alpha \otimes I)p) \\ &= tr((M_\alpha^* M_\alpha \otimes I)p) \\ &= tr((M_\alpha^* M_\alpha \otimes I)(\sum_l R_l \otimes T_l)) \\ &= \sum_l tr((M_\alpha^* M_\alpha \otimes I)(R_l \otimes T_l)) \\ &= \sum_l tr((M_\alpha^* M_\alpha R_l) \otimes T_l) \\ &= \sum_l tr(M_\alpha^* M_\alpha R_l) tr(T_l) \\ &= \sum_l tr(M_\alpha^* M_\alpha (tr(T_l) R_l)) \\ &= tr(M_\alpha^* M_\alpha (t_B(p))) \\ &= tr(M_\alpha^* M_\alpha p^A). \end{aligned}$$

Therefore,

$$p_\alpha(p) = p_\alpha(p^A).$$

Similarly, when Lab B does measurements, we only see p^B; i.e., all measurements of p are the same as of p^B.

Check. For $p \geq 0, tr(p) = 1$, write $p = \sum R_l \otimes T_l$. Then

$$p^A = \sum tr(T_l) R_l$$

and

$$\begin{aligned} tr(p^A) &= \sum_l tr(tr(T_l) R_l) \\ &= \sum_l tr(T_l) tr(R_l) \\ &= \sum_l tr(R_l \otimes T_l) \\ &= tr(p) \\ &= 1. \end{aligned}$$

Also, we need $p \geq 0$ implies $p^A \geq 0$ (which happens to be true; i.e., see below).

17 Day - 3/Oct/11

17.1 More on Partial Traces

Last time, we saw that $\mathcal{L}(H_A) \otimes \mathcal{L}(H_B) \cong \mathcal{L}(H_A \otimes H_B)$ by the mapping

$$R \otimes T \leftrightarrow R \otimes T(h \otimes k) = (Rh) \otimes (Tk).$$

We also defined the partial traces:

$$tr_B : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_A), tr_B(R \otimes T) = tr(T)R \in \mathcal{L}(H_A),$$

$$tr_A : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_B), tr_B(R \otimes T) = tr(R)T \in \mathcal{L}(H_B).$$

17.2 Another View

Let $dim(H_A) = n$ with basis $\{e_1, \ldots, e_n\}$ and $dim(H_B) = p$ with basis $\{f_1, \ldots, f_p\}$. Then on H_B, we have the operator

$$E_{ij} f_l = \begin{cases} f_i, & l = j, \\ 0, & l \neq j, \end{cases}$$

where we call the E_{ij} the matrix units. We know that

$$\{E_{ij} : 1 \leq i, j \leq p\}$$

is a basis for $\mathcal{L}(H_B)$. Hence, every $X \in \mathcal{L}(H_A) \otimes \mathcal{L}(H_B)$ has a unique representation

$$X = \sum_{i,j=1}^{p} X_{ij} \otimes E_{ij},$$

where $X_{ij} \in \mathcal{L}(H_A)$. Then, we can write the partial traces as

$$tr_B(X) = \sum_{i,j=1}^{p} X_{ij} tr(E_{ij}) = \sum_{i=1}^{p} X_{ii} \in \mathcal{L}(H_A),$$

$$tr_A(X) = tr_A(\sum_{i,j=1}^{p} X_{ij} \otimes E_{ij}) = \sum_{i,j=1}^{p} tr(X_{ij}) E_{ij} \in \mathcal{L}(H_B).$$

If we identify $\mathcal{L}(H_B) \cong M_p$, then

$$tr_A(X) = (tr(X_{ij})).$$

Similarly, if we write $X = \sum E_{kl} \otimes Y_{kl}$, with the $Y_{kl} \in \mathcal{L}(H_B)$, then

$$tr_A(X) = \sum_{k,l} tr(E_{kl}) Y_{kl} = \sum_{k} Y_{kk} \in \mathcal{L}(H_B),$$

$$tr_B(X) = \sum_{k,l} E_{kl} tr(Y_{kl}) \cong (tr(Y_{kl})) \in M_n \cong \mathcal{L}(H_A).$$

Finally, what happens to $R \otimes T$ when we choose bases? Pick a basis for H_B and write in matrix units $T = \sum_{i,j=1}^{p} t_{ij} E_{ij}$. Then,

$$R \otimes T = \sum_{i,j=1}^{p} R \otimes (t_{ij} E_{ij}) = \sum_{i,j=1}^{p} (t_{ij} R) \otimes E_{ij}.$$

So far, we have seen the case of $\mathcal{L}(H_A) \otimes \mathcal{L}(H_B) \cong \mathcal{L}(H_A \otimes H_B)$. When we pick a basis $\{f_1, \ldots, f_p\}$ for H_B, then every vector $v \in H_A \otimes H_B$ has a unique representation

$$v = h_1 \otimes f_1 + \ldots + h_p \otimes f_p,$$

where $h_1, \ldots, f_p \in H_A$ and $||v||^2 = ||h_1||^2 + \ldots + ||h_p||^2$. This creates an isomorphism

$$H_A \otimes H_B \cong H_A \oplus \ldots \oplus H_A \ (p \ copies)$$

by the mappings

$$v = \sum_{i=1}^{p} h_i \otimes f_i \leftrightarrow (h_1, \ldots, h_p) \leftrightarrow \begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix}.$$

Then, $\mathcal{L}(H_A \otimes H_B) \cong \mathcal{L}(H_A^{(p)})$, where we denoted

$$H_A \oplus \ldots \oplus H_A \equiv H_A^{(p)}.$$

Here, it is natural to think of $X \in \mathcal{L}(H_A^{(p)})$ as $X = (X_{ij})_{i,j=1}^{p}$, where the $X_{ij} \in \mathcal{L}(H_A)$ and

$$X \begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix} = (X_{ij}) \begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{p} X_{1j} h_j \\ \vdots \\ \sum_{j=1}^{p} X_{pj} h_j \end{pmatrix}.$$

So, $X \cong (X_{ij}) \in \mathcal{L}(H_A \otimes H_B) \cong \mathcal{L}(H_A^{(p)})$.

On the other hand,

$$\mathcal{L}(H_A \otimes H_B) \cong \mathcal{L}(H_A) \otimes \mathcal{L}(H_B).$$

So, if $X = (X_{ij})$ is written in block matrix notation, we also have X as a sum of elementary tensors, $X = \sum_{i,j=1}^{p} X_{ij} \otimes E_{ij}$. Hence, we can write the partial traces in block notation:

$$tr_B((X_{ij})) = X_{11} + \ldots + X_{pp} \in \mathcal{L}(H_A),$$

$$tr_A((X_{ij})) = (tr(X_{ij}))_{p \times p}.$$

17.3 Reformulate Postulates

Postulate 1': Given a quantum system, there exists a Hilbert space H_A such that the state of the system is completely described by a density matrix $p \in \mathcal{L}(H_A)$; i.e., $p \geq 0$ and $tr(p) = 1$.

Postulate 2': Evolution of a closed system from t_1 to t_2 is described by a unitary $U \in \mathcal{L}(H_A)$ so that if at time t_1 we have the state given by p, then at t_2, the state is given by UpU^*.

Postulate 3': Measurement systems are given by $\{M_\alpha\}$ on H_A satisfying $\sum M_\alpha^* M_\alpha = I$ and the probability of outcome α given by density p is $p_\alpha(p) = tr(M_\alpha^* M_\alpha p)$.

Postulate 4': Given systems H_A, H_B with densities p_1, p_2, then the composite system is given by $H_A \otimes H_B$ and density $p_1 \otimes p_2$.

18 Day - 5/Oct/11

18.1 Measurement Maps

Suppose we have a measurement $\{M_\alpha\}$, $\sum M_\alpha^* M_\alpha = I$, on H_A. Given a state ψ, the probability $p_\alpha(\psi) = ||M_\alpha \psi||^2$ and the after state is $\frac{M_\alpha \psi}{||M_\alpha \psi}$. We can then build an ensemble with density matrix

$$\begin{aligned} p &= \sum_\alpha p_\alpha(\psi) \left| \frac{M_\alpha \psi}{||M_\alpha \psi} \right\rangle \left\langle \frac{M_\alpha \psi}{||M_\alpha \psi} \right| \\ &= \sum_\alpha \frac{p_\alpha(\psi)}{||M_\alpha \psi||^2} (M_\alpha \psi)(M_\alpha \psi)^* \\ &= \sum M_\alpha (\psi \psi^*) M_\alpha^*. \end{aligned}$$

If we had an ensemble $\{p_i, \psi_i\}$ and density matrix $p_1 = \sum p_i |\psi_i\rangle\langle\psi_i|$, after measurement, we would have a new density matrix

$$\begin{aligned} \sum_i p_i \mathcal{M}(|\psi_i\rangle\langle\psi_i|) &= \sum_\alpha M_\alpha (\sum_i p_i |\psi_i\rangle\langle\psi_i|) M_\alpha^* \\ &= \sum_\alpha M_\alpha p_1 M_\alpha^*. \end{aligned}$$

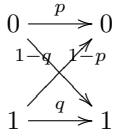
Hence, if we start with an ensemble with density matrix p_1, then after measurement, it behaves like the density matrix

$$\mathcal{M}(p_1) = \sum_\alpha M_\alpha p_1 M_\alpha^*;$$

i.e., we have a linear map $\mathcal{M} : \mathcal{L}(H_A) \to \mathcal{L}(H_A)$, $\mathcal{M}(X) = \sum_\alpha M_\alpha X M_\alpha^*$, recalling that $\sum_\alpha M_\alpha^* M_\alpha = I$.

18.2 Noise and Quantum Noise

For the classical bit $\{0, 1\}$, because of the environment (i.e., static, background magnetic field, etc.), after a period of time, 0 could flip to 1, and 1 could flip to 0:



If we start with p_0 being the probablity we are in state 0 and $p_1 = 1 - p_0$ being the probability of being in state 1, then after this time elapses, the probability we are in state 0 is $q_0 = pp_0 + (1-q)p_1$ and the probability we are in state 1 is $q_1 = (1-p)p_0 + qp_1$; i.e., we have

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} p & 1-q \\ 1-p & q \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}.$$

Definition. A matrix such that all entries are non-negative and each column sums to 1 is called a *stochastic matrix* (in the above, set $p = q$). If, in addition, each row sums to 1, then the matrix is called a *doubly stochastic matrix*.

Long Time Behavior: Markov chains.

18.3 Model for Quantum Noise

Suppose you have a state space H_A with density matrix $p \in \mathcal{L}(H_A)$. Also, we have an outside environment H_E in some state $|\phi\rangle$. Then, we are really in the state $p \otimes (|\phi\rangle\langle\phi|)$.

After some time goes by, there exists a unitary U on $H_A \otimes H_E$ such that $p \otimes (|\phi\rangle\langle\phi|)$ evolves to

$$U(p \otimes (|\phi\rangle\langle\phi|))U^*.$$

But, in Lab A, we only see the partial trace

$$tr_E(U(p \otimes (|\phi\rangle\langle\phi|))U^*).$$

Now, assume that $dim(H_E) = p < +\infty$, $\phi = (\alpha_1, \ldots, \alpha_p)^T$, and $|\phi\rangle\langle\phi| = (\alpha_i\overline{\alpha}_j)_{p\times p}$. Then,

$$p \otimes (\alpha_i\overline{\alpha}_j) \in \mathcal{L}(H_A \otimes H_E) = \mathcal{L}(H_A \oplus \ldots \oplus H_A),$$

and the tensor is written in block matrix form:

$$p \otimes (\alpha_i\overline{\alpha}_j) = (p(\alpha_i\overline{\alpha}_j))_{p\times p}.$$

For the unitary $U \in \mathcal{L}(H_A \otimes H_E)$, then $U = [U_{ij}]$ with each $U_{ij} \in \mathcal{L}(H_A)$ and

$$U^* = \begin{pmatrix} U_{11}^* & \ldots & U_{p1}^* \\ \vdots & \ddots & \vdots \\ U_{1p}^* & \ldots & U_{pp}^* \end{pmatrix} = (U_{ji}^*).$$

This implies

$$U(p\alpha_i\overline{\alpha}_j)U^* = (\sum_{k,l} U_{ik}(p\alpha_k\overline{\alpha}_l)U_{jl}^*)_{i,j}$$

and

$$tr_E(U(p\alpha_i\overline{\alpha}_j)U^*) = \sum_{i,k,l} U_{ik}(p\alpha_k\overline{\alpha}_l)U_{il}^*.$$

Let $W_i = \sum_k U_{ik}\alpha_k$. Then,

$$W_i^* = \sum_k U_{ik}^* \overline{\alpha}_k = \sum_l U_{il}^* \overline{\alpha}_l = \sum_i W_i p W_i^*.$$

So, noise, or interaction with the environment, transforms p to

$$\mathcal{E}(p) = \sum_i W_i p W_i^*.$$

Observe the

$$\begin{aligned} \sum_i W_i^* W_i &= \sum_{i,k,l} U_{il}^* \overline{\alpha}_l U_{ik} \alpha_k \\ &= \sum_{k,l} \overline{\alpha}_l \alpha_k (\sum_i U_{il}^* U_{ik}) \\ &= \sum \overline{\alpha}_l \alpha_l I \\ &= I. \end{aligned}$$

Hence, if a hostile person sneaks into the lab and does a measurement, or an outside environment introduces noise, both alter p via maps of the same form; that is,

$$p \mapsto \sum X_\alpha p X_\alpha^*, \sum X_\alpha^* X_\alpha = I.$$

18.4 Third Way: Axiomatic

Given H_A and a density matrix p, after some "quantum event," p transforms to a new density $\Phi(p)$. Assume that $\Phi(p) : \mathcal{L}(H_A) \to \mathcal{L}(H_A)$ is linear.

Proposition. Let $\Phi(p) : \mathcal{L}(H_A) \to \mathcal{L}(H_A)$. Then $\Phi(p)$ is a density matrix for all density matrices p if and only if both

1. $p \geq 0$ implies $\Phi(p) \geq 0$; i.e., Φ is a positive linear map; and,
2. for all X, $tr(\Phi(X)) = tr(X)$; i.e., Φ is trace-preserving,

hold. In addition, given any H_B, then

$$\Phi \otimes I_{\mathcal{L}(H_B)} : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_A \otimes H_B)$$

send density matrices to density matrices.

Definition. A map $\Phi : \mathcal{L}(H_A) \to \mathcal{L}(H_A)$ satisfying the condition: for all H_B such that $dim(H_B) < +\infty$, $\Phi \otimes I_{\mathcal{L}(H_B)} : \mathcal{L}(H_A \otimes H_B) \to \mathcal{L}(H_A \otimes H_B)$ sends positives to positives, is called a *completely positive map*.

Theorem (Choi-Kraus). A map $\Phi : \mathcal{L}(H_A) \to \mathcal{L}(H_A)$ is completely positive and trace-preserving if and only if there exists matrices $\{E_i\}$ with $\sum E_i^* E_i = I$ such that $\Phi(X) = \sum E_i X E_i^*$.

19 Day - 7/Oct/11

19.1 Theory of CP Maps

Proposition. Let $X \in M_n = \mathcal{L}(\mathbb{C}^n)$. Then, $X = (P_1 - P_2) + i(P_3 - P_4)$, where each $P_i \geq 0$; i.e., $span(M_n^+) = M_n$.

Proof. $H = \frac{X+X^*}{2}$ and $K = \frac{X-X^*}{2i}$. Then, $H = H^*$,

$$K^* = \frac{X^* - X}{-2i} = K,$$

and $X = H + iK$. Then, the *spectral decomposition* of H is $H = \sum_{i=1}^n \lambda_i |\psi_i\rangle\langle\psi_i|$, where each $E_i = |\psi_i\rangle\langle\psi_i|$ is a rank one projection and each λ_i is an eigenvalue. Set

$$P_1 = \sum_{\lambda_i \geq 0} \lambda_i E_i, P_2 = -\sum_{\lambda_i < 0} \lambda_i E_i.$$

Then, $P_1, P_2 \geq 0$ and $H = P_1 - P_2$.

Similarly, we decompose $K = P_3 - P_4$.

$\boxtimes$

Definition. We call a linear map $\Phi : M_n \to M_d$ *positive* if $P \geq 0$, then $\Phi(P) \geq 0$.

Proposition. If $\Phi : M_n \to M_d$ is linear, then $\Phi(P)$ is a density matrix, for every density matrix P, if and only if Φ is positive and trace-preserving; i.e., $tr(\Phi(X)) = tr(X)$.

Proof. ($\Leftarrow$) Obvious.

($\Rightarrow$) Given a non-zero $P \geq 0$, $tr(P) \neq 0$. Therefore, $\rho = \frac{1}{tr(P)} P$ is a density matrix. Therefore,

$$\Phi\left(\frac{1}{tr(P)} P\right)$$

is positive semidefinite. This implies

$$\Phi(P) = tr(P)\Phi(\rho) \geq 0.$$

Therefore, Φ is positive. Also,

$$\begin{aligned} tr(\Phi(\rho)) &= tr(tr(P)\Phi(\rho)) \\ &= tr(P)tr(\Phi(\rho)) \\ &= tr(P). \end{aligned}$$

Now, given any $X = P_1 - P_2 + i(P_3 - P_4)$,

$$\begin{aligned} tr(\Phi(X)) &= tr(\Phi(P_1) - \Phi(P_2) + i(\Phi(P_3) - \Phi(P_4))) \\ &= tr(\Phi(P_1)) - tr(\Phi(P_2)) + i(tr(\Phi(P_3)) - tr(\Phi(P_4))) \\ &= tr(P_1) - tr(P_2) + i(tr(P_3) - tr(P_4)) \\ &= tr(X). \end{aligned}$$

⊠

Definition. A linear map $\Phi : M_n \to M_d$ is called *p-positive* if

$$\Phi \otimes id_{\mathcal{L}(\mathbb{C}^p)} : \mathcal{L}(\mathbb{C}^n \otimes \mathbb{C}^p) \to \mathcal{L}(\mathbb{C}^d \otimes \mathbb{C}^p)$$

is positive. Φ is *completely positive* if it is p-positive for all p.

Remark. In block matrix form,

$$\mathbb{C}^n \otimes \mathbb{C}^p \cong \mathbb{C}^n \oplus \ldots \oplus \mathbb{C}^n \ (p \ times)$$

and

$$\begin{aligned} M_n \otimes M_p &\cong \mathcal{L}(\mathbb{C}^n) \otimes \mathcal{L}(\mathbb{C}^p) \\ &\cong \mathcal{L}(\mathbb{C}^n \otimes \mathbb{C}^p) \\ &\cong \mathcal{L}(\mathbb{C}^n \oplus \ldots \oplus \mathbb{C}^n) \\ &\cong M_p(\mathcal{L}(\mathbb{C}^n)) \\ &\cong M_p(M_n). \end{aligned}$$

Hence, in block matrices,

$$\begin{array}{rcccc} \Phi \otimes id_{\mathcal{L}(\mathbb{C}^p)} & : & M_n \otimes M_p & \to & M_d \otimes M_p, \\ & & || & & || \\ & & M_p(M_n) & & M_p(M_d) \end{array}$$

$$(\Phi \otimes id)(X) = (\Phi \otimes id)((X_{ij})) = (\Phi(X_{ij})).$$

Definition. $\Phi : M_n \to M_d$ is p-positive if and only if for every $(X_{ij}) \in M_p(M_n)$ that is positive semidefinite, we have that $(\Phi(X_{ij})) \in M_p(M_d)$ is positive semidefinite. Φ is completely positive if and only if it is p-positive for every p.

Given $\Phi : M_n \to M_d$, we write $\Phi^{(p)} : M_p(M_n) \to M_p(M_d)$,

$$\Phi^{(p)}((X_{ij})) = (\Phi(X_{ij})).$$

Example. Let $\Phi : M_2 \to M_2$ be defined by $\Phi(A) = A^t$. Now, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \geq 0$ if and only if $c = \overline{b}$, $a, d \geq 0$. hence, it has two real eigenvalues λ_1, λ_2 such that $\lambda_1\lambda_2 = ad - |b|^2$. In addition, A and A^t have the same eigenvalues[1] Therefore, $A \geq 0$ if and only if $A^t \geq 0$. So, Φ is 1-positive.

[1]Let M_n^+ be the set of positive semidefinite matrices. We show that $P \in M_n^+$ implies $P^t \in M_n^+$. Write $P = (p_{ij})$ and $P^t = (p_{ji})$. Let $x, \overline{x} \in \mathbb{C}^n$, written as columns. Then,

$$\begin{aligned} \langle x|P^t x\rangle &= \sum_{i,j} \overline{x}_i P_{ji} x_j \\ &= \sum_{i,j} \overline{x}_j P_{ij} x_i \\ &= \sum_{i,j} x_i P_{ij} \overline{x}_j \\ &= \langle \overline{x}|P\overline{x}\rangle \\ &\geq 0. \end{aligned}$$

This implies $\Phi : M_n \to M_n$, $\Phi(X) = X^t$ is a positive map.

Let

$$X = \begin{pmatrix} E_{11} & E_{12} \\ E_{21} & E_{22} \end{pmatrix} = \begin{pmatrix} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \\ \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \end{pmatrix}.$$

Then, $X = X^*$ and $X^2 = 2X$. Therefore, $X^2 - 2X = 0$ implies $X(2 - X) = 0$ and $\lambda(\lambda - 2) = 0$. Thus, $spec(X) \subseteq \{0, 2\}$ and $X \geq 0$. However,

$$\Phi^{(2)}(X) = \begin{pmatrix} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \\ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) & \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \end{pmatrix}$$

and $det(\Phi^{(2)}(X)) = -1$. So, $\Phi^{(2)}(X)$ is not positive semidefinite, in general. Therefore, Φ is not 2-positive.

20 Day - 10/Oct/11

20.1 Continuation

Theorem (Choi, 1975). Let $\Phi : M_n \to M_d$ be linear. The following are equivalent:

(1) Φ is completely positive.

(2) Φ is n-positive.

(3) $P_\Phi = (\Phi(E_{ij})) \geq 0$ in $M_n(M_d)$.

(4) There exists $n \times d$ matrices B_i such that

$$\Phi(X) = \sum_{i=1}^{K} B_i X B_i^*.$$

Proof. (1) $\Rightarrow$ (2): Obvious.
(2) $\Rightarrow$ (3): Consider $P = (E_{ij}) \in M_n(M_n)$. Then, $P = P^*$ and

$$P^2 \quad = \quad \left(\sum_{k=1}^{n} E_{ik} E_{kj} \right) (nE_{ij}) = nP.$$

This implies $P^2 - nP = P(P - nI) = 0$. Hence, $\lambda(\lambda - n) = 0$ for all eigenvalues λ of P. So, the eigenvalues of P are $\{0, n\}$, and by definition, $P \geq 0$. So, $P \in M_n(M_n)^+$. Since Φ is n-positive, $\Phi^{(n)}(P) = (\Phi(E_{ij})) \geq 0$ in $M_n(M_d)$.
(3) $\Rightarrow$ (4): Since $P_\Phi \geq 0$ and of size $nd \times nd$, we have that

$$P_\Phi = \sum_{k=1}^{K} v_k v_k^*,$$

for $v_k \in \mathbb{C}^{nd}$. Write each

$$v_k = \begin{pmatrix} w_1^k \\ \cdots \\ \vdots \\ \cdots \\ w_n^k \end{pmatrix},$$

where $w_i^k \in \mathbb{C}^d$. Then,

$$v_k v_k^* = \begin{pmatrix} w_1^k \\ \cdots \\ \vdots \\ \cdots \\ w_n^k \end{pmatrix} ((w_1^k)^* \vdots \ldots \vdots (w_n^k)^*) = ((w_i^k)(w_i^k)^*) \in M_n(M_d).$$

This implies $\sum_{k=1}^K (w_i^k)(w_j^k)^* = \Phi(E_{ij})$.

Let $B_k = (w_1^k \vdots \ldots \vdots w_n^k)_{d \times n}$. Then,

$$B_k^* = \begin{pmatrix} (w_1^k)^* \\ \cdots \\ \vdots \\ \cdots \\ (w_n^k)^* \end{pmatrix}_{n \times d}.$$

Also,

$$B_k E_{ij} B_k^* = B_k \begin{pmatrix} 0 \\ \vdots \\ 0 \\ (w_j^k)^* \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (((w_i^k)(w_i^k)^*)_{d \times d}).$$

Therefore, $\sum_{k=1}^K B_k E_{ij} B_k^* = \left(\sum_{k=1}^K (w_i^k)(w_i^k)^* \right) = \Phi(E_{ij})$.

Take any $X \in M_n$ and write $X = \sum x_{ij} E_{ij}$. By linearity,

$$\begin{aligned} \Phi(X) &= \sum_{i,j=1}^n x_{ij} \Phi(E_{ij}) = \sum_{i,j} x_{ij} \sum_{k=1}^K B_k E_{ij} B_k^* \\ &= \sum_{k=1}^K B_k \left(\sum_{i,j} x_{ij} E_{ij} \right) B_k^* = \sum_k B_k X B_k^*. \end{aligned}$$

(4) $\Rightarrow$ (1): We have $\Phi(X) = \sum_{k=1}^{K} B_k X B_k^*$. We need to show that Φ is p-positive for all p. Recall that if $P \geq 0$ then $YPY^* \geq 0$ since

$$\langle h|YPY^*h\rangle = \langle (Y^*h)|P(Y^*h)\rangle \geq 0.$$

Therefore, if $P \geq 0$, $B_k P B_k^* \geq 0$, implying $\sum_{k=1}^{K} B_k P B_k^* \geq 0$. So, Φ is 1-positive.

To show that Φ is r-positive, let $P = (p_{ij})_{i,j=1}^{r} \in M_r(M_n)^+$ with each $p_{ij} \in M_n$. Then,

$$\begin{aligned} \Phi^{(r)}(P) &= (\Phi(p_{ij})) = \left(\sum_{k=1}^{K} B_k P_{ij} B_k^*\right) \\ &= \sum_{k=1}^{K} \begin{pmatrix} B_k & & 0 \\ & \ddots & \\ 0 & & B_k \end{pmatrix} (P_{ij}) \begin{pmatrix} B_k^* & & 0 \\ & \ddots & \\ 0 & & B_k^* \end{pmatrix} \geq 0. \end{aligned}$$

Therefore, Φ is r-positive for all r.

$\boxtimes$

Notes. (1) When Φ is completely positive, writing $\Phi(X) = \sum_{i=1}^{K} B_i X B_i^*$ is called a *Choi-Krauss representation* of Φ.

(2) The matrix $P_\Phi(\Phi(E_{ij}))$ is called the *Choi-Jamliokowska matrix*.

(3) Let $CP(M_n, M_d)$ be the set of completely positive maps from M_n to M_d. Then

$$\begin{array}{ccc} CP(M_n, M_d) & \overset{1-1}{\leftrightarrow} & M_n(M_d)^+ \\ \Phi & \leftrightarrow & P_\Phi \end{array}$$

(4) What about characterizing Φ such that Φ is trace-preserving or so that $\Phi(I_n) = I_d$? We need to check that $tr(\Phi(X)) = tr(X)$ for all X if and only if $tr(\Phi(E_{ij})) = tr(E_{ij})$. So, $P_\Phi = (R_{ij})$ is completely positive and trace-preserving if and only if $P_\Phi \geq 0$ and $tr(R_{ij}) = \delta_{ij}$.

(5) $P_\Phi = (R_{ij})$ is unital (i.e., unit preserving) and $CP(UCP)$ (i.e., unital completely positive) if and only if $\sum_{i=1}^{n} R_{ii} = I_d$ and $P_\Phi \geq 0$.

21 Day - 12/Oct/11

21.1 Continuation

Proposition. Let $\phi : M_n \to \mathbb{C}$ be linear. The following are equivalent:

(1) ϕ is positive.

(2) ϕ is completely positive.

(3) $P_\phi = (\phi(E_{ij})) \in M_n^+$.

Proof. (2) $\Leftrightarrow$ (3): By *Choi's theorem* with $d = 1$.
(2) $\Rightarrow$ (1): Obvious.
(1) $\Rightarrow$ (2): Take $P = (P_{ij}) \in M_r(M_n)$. Then,

$$\phi^{(r)} : M_r(M_n) \to M_r(\mathbb{C}) = M_r, \phi^{(r)}(P) = (\phi(P_{ij})).$$

We need to show that if $P \geq 0$, then $(\phi(P_{ij})) \in M_r^+$. Let $v = (\alpha_i) \in \mathbb{C}^r$. Then,

$$\langle v|(\phi(P_{ij}))v\rangle = \sum_{i,j=1}^{r} \overline{\alpha}_i \phi(P_{ij})\alpha_j = \phi(\sum_{i,j=1}^{r} \overline{\alpha}_i P_{ij}\alpha_j). \quad (*)$$

We claim that $\sum_{i,j=1}^{r} \overline{\alpha}_i\alpha_j P_{ij} \in M_n^+$. Let

$$Y = \begin{pmatrix} \alpha_1 I \\ \vdots \\ \alpha_r I \end{pmatrix}.$$

Then, $Y^*PY \geq 0$. However,

$$Y^*PY = (\overline{\alpha}_1 I, \ldots, \overline{\alpha}_r I)(P_{ij}) \begin{pmatrix} \alpha_1 I \\ \vdots \\ \alpha_r I \end{pmatrix} = \sum_{i,j=1}^{r} \overline{\alpha}_i\alpha_j P_{ij}.$$

By the claim, ϕ positive implies $(*) \geq 0$.

$\boxtimes$

Recall that if M_n, M_d are Hilbert spaces, then

$$\langle Y|X\rangle_{M_n} = tr(Y^*X).$$

Proposition. Let $\Phi : M_n \to M_d$ and $\Phi^* : M_d \to M_n$.
(1) If $\Phi(X) = \sum_{i=1}^{L} A_i X A_i^*$, where the A_i are $d \times n$ matrices, then $\Phi^*(Y) = \sum_{i=1}^{L} A_i^* Y A_i$.
(2) Φ is completely positive if and only if Φ^* is completely positive.
(3) Φ is completely positive and unital if and only if Φ^* is completely positive and trace-preserving.
Proof. (1) Let $X \in M_n$ and $Y \in M_d$. Then,

$$\begin{aligned}
\langle \Phi^*(Y)|X\rangle_{M_n} &= \langle Y|\Phi(X)\rangle_{M_d} = tr(Y^*\Phi(X)) \\
&= \sum_{i=1}^{L} tr(Y^* A_i X A_i^*) = \sum_{i=1}^{L} tr(A_i^* Y^* A_i X) \\
&= \sum_{i=1}^{L} tr((A_i^* Y A_i)^* X) = \sum_{i=1}^{L} L\langle A_i^* Y A_i|X\rangle \\
&= \langle \sum_{i=1}^{L} A_i^* Y A_i|X\rangle.
\end{aligned}$$

This implies $\Phi^*(Y) = \sum_{i=1}^L A_i^* Y A_i$.

(2)If Φ is completely positive, then $\Phi(X) = \sum A_i X A_i^*$. This implies $\Phi^*(Y) = \sum A_i^* Y A_i$, but we saw that all such maps are completely positive.

Conversely, if Φ^* is completely positive, then $(\Phi^*)^* = \Phi$ is completely positive by the above.

(3) Let $\Phi(X) = \sum_{i=1}^L A_i X A_i^*$. Then Φ is completely positive and unital if and only if $\Phi(I_n) = I_d$ if and only if $\sum_{i=1}^L A_i I A_i^* = I$ if and only if $\sum_{i=1}^L A_i A_i^* = I$. On the other hand, $\Phi^*(Y) = \sum_{i=1}^L A_i^* Y A_i$. So, Φ^* is completely positive and trace-preserving if and only if $tr(\Phi^*(Y)) = tr(Y)$ for all Y if and only if $tr(Y) = tr(\sum_{i=1}^L A_i^* Y A_i)$ if and only if $tr(Y) = tr((\sum_{i=1}^L A_i A_i^*)Y)$ for all Y.

We claim that if $B \in M_d$ and $tr(BY) = tr(Y)$ for all Y, then $B = I$. In fact,

$$b_{ii} = tr(BE_{ii}) = tr(E_{ii}) = 1$$

for all i, and

$$b_{ji} = tr(BE_{ij}) = tr(E_{ij}) = 0$$

for all $j \neq i$. Hence, $B = I$.

By the claim, Φ^* is completely positive and trace-preserving if and only if $\sum_{i=1}^L A_i A_i^* = I$ if and only if Φ is unital and completely positive.

$\boxtimes$

Definition. Let $\Phi : M_n \to M_d$ be completely positive. Then the *Choi rank* of Φ is defined to be

$$cr(\Phi) = min\{L : \Phi(X) = \sum_{l=1}^{L} B_l X B_l^*\}.$$

Theorem (Choi). $cr(\Phi) = rank(P_\Phi)$.

Proof. By the (3) $\Rightarrow$ (4) part of *Choi's main theorem*, we showed that when $P_\Phi = \sum_{l=1}^L v_l v_l^*$, then that gave rise to an expression for $\Phi(X) = \sum_{l=1}^L A_l X A_l^*$ (with the same L). When we use the *spectral decomposition* of P_Φ to write as a sum of "rank ones," this decomposition gives us $P_\Phi = \sum_{l=1}^r v_l v_l^*$., where r is the number of non-zero eigenvalues of P_Φ; i.e., $r = rank(P_\Phi)$. Therefore, $cr(\Phi) \leq rank(P_\Phi)$.

We now need a lemma:

Lemma. Let $P = (E_{ij}) \in M_n(M_n)^+$. Then $rank(P) = 1$.

Proof of Lemma. We have

$$P^2 = (\sum_{k=1}^{n} E_{ik} E_{kj}) = (nE_{ij}) = nP.$$

So, $\sigma(P) \subseteq \{0, n\}$. Thus, at least one eigenvalue of P is equal to n. Let $\lambda_1, \ldots, \lambda_{n^2}$ be the eigenvalues with $\lambda_1 = n$. Then,

$$\begin{aligned} \lambda_1 + \ldots + \lambda_{n^2} &= tr(E_{11}) + \ldots + tr(E_{nn}) \\ &= n. \end{aligned}$$

So, $\lambda_j = 0$ for all $j \neq 1$. Therefore, $rank(P) = 1$.

$\otimes$

Now, if $rank(B) = 1$, then $rank(ABC) \leq 1$ because

$$rank(ABC) = dim(range(ABC)) = dim(Arange(BC)) \leq dim(range(BC)).$$

However, $range(BC) \subseteq range(B)$. This implies

$$dim(range(BC)) \leq dim(range(B)) = rank(B) = 1.$$

Suppose $cr(\Phi) = L$ and write $\Phi(X) = \sum_{l=1}^{L} A_l X A_l^*$. Therefore,

$$P_\Phi = (\Phi(E_{ij})) = \sum_{l=1}^{L} \begin{pmatrix} A_l & & 0 \\ & \ddots & \\ 0 & & A_l \end{pmatrix} (E_{ij}) \begin{pmatrix} A_l^* & & 0 \\ & \ddots & \\ 0 & & A_l^* \end{pmatrix}.$$

Hence,

$$rank(P_\Phi) \leq \sum_{l=1}^{L} rank \left(\sum_{l=1}^{L} \begin{pmatrix} A_l & & 0 \\ & \ddots & \\ 0 & & A_l \end{pmatrix} (E_{ij}) \begin{pmatrix} A_l^* & & 0 \\ & \ddots & \\ 0 & & A_l^* \end{pmatrix} \right) \leq L = cr(\Phi).$$

$\boxtimes$

22 Day - 14/Oct/11

22.1 Continuation

Corollary. If $\Phi : M_n \to M_d$ is completely positive, then $\Phi(X) = \sum_{l=1}^{K} A_l X A_l^*$, where $K \leq nd$.

Proof. $cr(\Phi) = rank(P_\Phi)$ and $P_\Phi \in M_n(M_d) = M_{nd}$. Therefore, $rank(P_\Phi) \leq nd$.

$\boxtimes$

Conjecture. Suppose $\Phi : M_n \to M_d$ is completely positive. Does there exists unital completely positive $\{\Phi_1, \ldots, \Phi_n\}$ such that $cr(\Phi_l) \leq d$ and $\Phi = \frac{1}{n} \sum_{l=1}^{n} \Phi_l$?

This is equivalent to both of the following:

(i) Suppose $\psi : M_n \to M_d$ is completely positive and trace-preserving. Does there exists completely positive and trace-preserving $\{\psi_1, \ldots, \psi_n\}$ such that $cr(\psi_l) \leq d$ and $\psi = \frac{1}{n} \sum_{l=1}^{n} \psi_l$?

(ii) Suppose $P \in M_n(M_d)^+$ such that $tr_d(P) = I_d$. Does there exists positive $\{P_1, \ldots, P_n\}$ such that $rank(P_l) \leq d$, $tr_d(P_l) = I_d$, and $P = \frac{1}{n} \sum_{l=1}^{n} P_l$?

Lemma. Suppose $T : \mathbb{C}^r \to \mathbb{C}^m$ is one-to-one. Then $T^* : \mathbb{C}^m \to \mathbb{C}^r$ is onto.

Proof. The range of T^* is closed. So, it is enough to show that if $h \perp range(T^*)$, this implies $h = 0$. Suppose $\langle T^* k | h \rangle = 0$ for all k. This implies $\langle k | Th \rangle = 0$ for all k, which means $Th = 0$. Since T is one-to-one, $h = 0$.

$\boxtimes$

Proposition. If $\{v_1, \ldots, v_r\} \subseteq \mathbb{C}^k$ is linearly independent, then $\{v_i v_j^* : 1 \leq i, j \leq r\} \subseteq M_k$ is linearly independent.

Proof. Let $T : \mathbb{C}^r \to \mathbb{C}^k$. Write

$$T = [v_1 \vdots \ldots \vdots v_r].$$

So, T is one-to-one, and by the lemma,

$$T^* = \begin{bmatrix} v_1^* \\ \cdots \\ \vdots \\ \cdots \\ v_r^* \end{bmatrix}$$

is onto. For $h \in \mathbb{C}^k$,

$$T^* h = \begin{bmatrix} v_1^* h \\ \cdots \\ \vdots \\ \cdots \\ v_r^* h \end{bmatrix} = \begin{bmatrix} \langle v_1 | h \rangle \\ \cdots \\ \vdots \\ \cdots \\ \langle v_r | h \rangle \end{bmatrix}.$$

Suppose $\sum_{i,j=1}^r \alpha_{ij} v_i v_j^* = 0$. This implies, for all $h \in \mathbb{C}^k$,

$$\sum_{i,j=1}^r \alpha_{ij} v_i v_j^* h = \sum_{i=1}^r \left(\sum_{j=1}^r \alpha_{ij} \langle v_j | h \rangle \right) v_i = 0.$$

So, for all i, $\sum_{j=1}^r \alpha_{ij} \langle v_j | h \rangle = 0$. Hence

$$(\alpha_{ij})(T^* h) = 0.$$

So, if $T^* h$ is any vector, then $(\alpha_{ij}) = 0$; i.e., $\alpha_{ij} = 0$ for all i, j. Therefore, $\{v_i v_j^*\}$ is linearly independent.

$\boxtimes$

Lemma. If $0 \leq ww^* \leq P$, then $w \in range(P)$.

Proof. If

$$P = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix},$$

then,

$$ww^* = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}.$$

This implies $w = (w_1, \ldots, w_r, 0, \ldots, 0)^t$ and

$$w = P \begin{pmatrix} \lambda_1^{-1} w_1 \\ \vdots \\ \lambda_r^{-1} w_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Now use that P is unitary equivalent to such a matrix.

$\boxtimes$

Notation. We write $\mathcal{R}(P) = range(P)$.

Proposition. If $P \geq 0$ and $P = \sum_{l=1}^m w_l w_l^*$, then $\mathcal{R}(P) = span\{w_1, \ldots, w_m\}$.

Proof. $Ph = \sum_{l=1}^m w_l \langle w_l | h \rangle$. Therefore, $\mathcal{R}(P) \subseteq \{w_1, \ldots, w_m\}$. By the lemma above, $span\{w_1, \ldots, w_m\} \subseteq \mathcal{R}(P)$.

$\boxtimes$

Theorem. Suppose $P \geq 0$ and

$$P = \sum_{j=1}^r v_j v_j^* = \sum_{l=1}^m w_l w_l^*,$$

where $rank(P) = r$. Then, there exists $U = (\alpha_{ij})_{m \times r}$ such that $w_i = \sum_{j=1}^r \alpha_{ij} v_j$ and $U^* U = I_r$.

Proof. We have that

$$span\{v_1, \ldots, v_r\} \mathcal{R}(P) = span\{w_1, \ldots, w_m\}.$$

Since $dim(\mathcal{R}(P)) = r$, it implies $v_1, \ldots, v_r$ is a basis, and in particular, linearly independent. Therefore, there exists unique α_{ij} such that $w_i = \sum_{j=1}^r \alpha_{ij} v_j$ and

$$\begin{aligned} \sum_{j=1}^r v_j v_j^* &= P \\ &= \sum_{k=1}^m w_k w_k^* \\ &= \sum_{k=1}^m (\sum_{j=1}^r \alpha_{kj} v_j)(\sum_{i=1}^r \alpha_{ki} v_i)^* \\ &= \sum_{k=1}^m m \sum_{j=1}^r \sum_{i=1}^r \alpha_{kj} \overline{\alpha}_{ki} v_j v_i^* \\ &= \sum_{j=1}^r \sum_{i=1}^r \delta_{ij} v_j v_i^*, \end{aligned}$$

where δ_{ij} is the (i,j)-entry of U^*U. Therefore,

$$\sum_{i,j=1}^{r} \delta_{ij} v_j v_i^* = \sum_{j=1}^{r} v_j v_j^*.$$

Since the $v_j v_i^*$ are linearly independent,

$$\delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j; \end{cases}$$

i.e., $U^*U = I_r$.

$\boxtimes$

Theorem 2 (Choi). If $\Phi : M_n \to M_d$ is completely positive, $cr(\Phi) = r$, and

$$\Phi(X) = \sum_{j=1}^{r} V_j X V_j^* = \sum_{l=1}^{m} W_l X W_l^*,$$

then there exist unique α_{ij} such that

$$W_i = \sum_{j=1}^{r} \alpha_{ij} V_j$$

and if $U = (\alpha_{ij})$, then $U^*U = I_r$.

Proof. Given $V = [h_1 \vdots \ldots \vdots h_n]_{d \times n}$, then write

$$v = \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}_{1 \times nd} \in \mathbb{C}^{nd}.$$

In the proof of *Choi's theorem 1*, we saw that Φ written as above form vectors $v_1, \ldots, v_r, w_1, \ldots, w_m \in \mathbb{C}^{nd}$, then

$$P_\Phi = \sum_{j=1}^{r} v_j v_j^* = \sum_{l=1}^{m} w_l w_l^*.$$

Therefore, there exists unique α_{ij} such that $w_i = \sum_{j=1}^{r} \alpha_{ij} v_j$ and $U = (\alpha_{ij})$ such that $U^*U = I_r$. This implies

$$W_i = \sum_{j=1}^{r} \alpha_{ij} V_j.$$

$\boxtimes$

23 Day - 17/Oct/11

23.1 Continuation

Proposition. Suppose that $\Phi : M_n \to M_d$ is completely positive, $cr(\Phi) = r$, and $\Phi(X) = \sum_{i=1}^{r} V_i^* X V_i$. Then, $\{V_1, \ldots, V_r\}$ are linearly independent.

Proof. Since $rank(P_\Phi) = r$, $\mathcal{R}(P_\Phi) = span\{v_1, \ldots, v_r\}$. Since $dim(\mathcal{R}(P_\Phi)) = r$, $v_1, \ldots, v_r$ are linearly independent. This implies $\{V_1, \ldots, V_r\}$ are linearly independent since, for example,

$$V_1 = [v_1^1 \vdots \ldots \vdots v_1^n]$$

and

$$v_1 = \begin{pmatrix} v_1^1 \\ \vdots \\ v_1^n \end{pmatrix}.$$

23.2 Convex Sets in Vector Spaces

Definition. Let V be a vector space. A set $C \subseteq V$ is *convex* provided whenever $v_1, v_2 \in C$ implies $tv_1 + (1-t)v_2 \in C$ for all $0 \leq t \leq 1$.

A point v in a convex set C is called *extreme* of $v_1, v_2 \in C$ and $v = \frac{1}{2}(v_1 + v_2)$ implies $v = v_1 = v_2$.

Examples. (1) If C is a closed squared area, then C is convex and the extreme points are the corners of the square.

(2) If C is a closed disc, then C is convex and the boundary points are extreme points.

Theorem (Krein-Milman). If V is a real vector space with $dim(V) < +\infty$, and $C \subseteq V$ is convex and compact, then C is the convex hull of its extreme points.

Definition. Given a set E, a *convex combination* of points in E is any point of the form $v = t_1 e_1 + \ldots + t_m e_m$, where $e_1, \ldots, e_m \in E$ and $t_i \geq 0$ such that $t_1 + \ldots + t_m = 1$. the set of all convex combinations of points in E is called the *convex hull*.

Definition. Let $C_1 \subseteq V_1$ and $C_2 \subseteq V_2$ both be convex. A map $T : C_1 \to C_2$ is called *affine* if $T(tv_1 + (1-t)v_2) = tT(v_1) + (1-t)T(v_2)$ for all $v_1, v_2 \in C_1$, for all $0 \leq t \leq 1$.

Two convex sets are called *affinely isomorphic* if there exists a bijective affine $T : C_1 \to C_2$ such that $T^{-1} : C_2 \to C_1$ is affine.

Examples. (1) Let

$$UCP(M_n, M_d) = \{\Phi : M_n \to M_d \,:\, \Phi \, unital, \, completely \, positive\} \subseteq \mathcal{L}(M_n, M_d).$$

This is a convex set. In fact, let $\Phi_1, \Phi_2 \in UCP(M_n, M_d)$, $0 \leq t \leq 1$, and define

$$\Phi(X) = t\Phi_1(X) + (1-t)\Phi_2(X).$$

Then,

$$\begin{aligned}\Phi(I) &= t\Phi_1(I) + (1-t)\Phi_2(I)\\ &= tI + (1-t)I\\ &= I.\end{aligned}$$

So, Φ is unital. Also,

$$\begin{aligned}P_\Phi &= (\Phi(E_{ij}))\\ &= (t\Phi_1(E_{ij}) + (1-t)\Phi_2(E_{ij}))\\ &= tP_{\Phi_1} + (1-t)P_{\Phi_2}\\ &\geq 0.\end{aligned}$$

Therefore, it is convex.

This set is also compact. It is easy to see that it is closed. To see bounded, observe that $\Phi(I) = I$ implies $\sum \Phi(E_{ii}) = I$ implies $0 \leq \Phi(E_{ii}) \leq I$. If $0 \leq (r_{ij}) \leq I$ implies

$$\begin{pmatrix} 1-r_{11} & -r_{12} & \dots & -r_{1n} \\ 0 & 1-r_{22} & & * \\ & & \ddots & \\ 0 & & & 1-r_{nn} \end{pmatrix} \geq 0.$$

Hence, $r_{ii} \leq 1$. Look at any 2×2 $\left(\begin{smallmatrix} r_{ii} & r_{ij} \\ r_{ji} & r_{jj} \end{smallmatrix}\right) \geq 0$. This implies $|r_{ij}|^2 \leq r_{ii}r_{jj} \leq 1$. Therefore, $|r_{ij}| \leq 1$.

(2) Let

$$CPTP(M_d, M_n) = \{\Phi : M_d \to M_n \,:\, \Phi \, completely\, positive,\, trace\, preserving\}.$$

This set is also compact and convex. In fact, recall that $\Phi : M_n \to M_d$ is unital and completely positive if and only if $\Phi^* : M_d \to M_n$ is completely positive and trace-preserving. The map $\Gamma : UCP(M_n, M_d) \to CPTP(M_d, M_n)$, given by $\Gamma(\Phi) = \Phi^*$, satisfies

$$\begin{aligned}\Gamma(t\Phi_1 + (1-t)\Phi_2) &= (t\Phi_1 + (1-t)\Phi_2)^*\\ &= t\Phi_1^* + (1-t)\Phi_2^*\\ &= t\Gamma(\Phi_1) + (1-t)\Gamma(\Phi_2).\end{aligned}$$

Theorem 3 (Choi). If $\Phi : M_n \to M_d$ is unital and completely positive, $\Phi(X) = \sum_{i=1}^r V_i^* X V_i$, and $r = cr(\Phi)$, then Φ is an extreme point of $UCP(M_n, M_d)$ if and only if

$$\{V_i^* V_j \,:\, 1 \leq i, j \leq r\} \subseteq M_d$$

are linearly independent.

Corollary. If Φ is extreme, then $cr(\Phi) \leq d$.

Proof. $\#\{V_i^* V_j \,:\, 1 \leq i, j \leq r\} = r^2 \leq dim(M_d) = d^2$. So, $r \leq d$.

$\boxtimes$

Corollary. If $\Phi : M_d \to M_n$ is completely positive and trace-preserving, $\Phi(X) = \sum_{i=1}^r V_i X V_i^*$, and $r = cr(\Phi)$, then Φ is extreme in $CPTP(M_d, M_n)$ if and only if

$$\{V_i^* V_j \ : \ 1 \leq i, j \leq r\} \subseteq M_d$$

is linearly independent.

Proof. If $\psi(X) = \sum V_i^* X V_i$, then $\psi^*(Y) = \sum V_i Y V_i^*$.

$\boxtimes$

Proof of Theorem 3 (Choi). ($\Rightarrow$) Suppose that $\sum_{i,j=1}^r \lambda_{ij} V_i^* V_j = 0$. This implies

$$\sum_{i,j=1}^r \overline{\lambda}_{ij} V_j^* V_i = 0.$$

This implies $\sum_{i,j=1}^r \overline{\lambda}_{ji} V_i^* V_j = 0$. So,

$$\sum_{i,j=1}^r (\lambda_{ij} + \overline{\lambda}_{ji}) V_i^* V_j = 0.$$

Note that $\mu = (\lambda_{ij} + \overline{\lambda}_{ji}) = \lambda + \lambda^*$. Hence, μ is self-adjoint. Suppose that we know that

$$\sum_{i,j=1}^r \mu_{ij} V_i^* V_j = 0$$

for all $\mu = \mu^*$ implies $\mu = 0$. Given $\sum \lambda_{ij} V_i^* V_j = 0$ and $\lambda = (\lambda_{ij})$, we would know that $\lambda + \lambda^* = 0$. Also,

$$\frac{\lambda - \lambda^*}{2i} = \frac{\lambda_{ij} - \overline{\lambda}_{ji}}{2i}$$

is also self-adjoint. Therefore,

$$\frac{\lambda - \lambda^*}{2i} = 0$$

implies $\lambda = 0$.

So, to show that $\{V_i^* V_j\}$ is linearly independent, it is enough to show that $\sum \mu_{ij} V_i^* V_j = 0$ for all $\mu = \mu^*$ implies $\mu = 0$.

Let $\sum_{i,j=1}^r \mu_{ij} V_i^* V_j = 0$, where $\mu = \mu^*$. It is enough to assume that $-I \leq \mu \leq I$. This implies $I + \mu \geq 0$ and $I - \mu \geq 0$.

Let $\psi_\pm(X) = \sum_{i=1}^r V_i^* X V_i \pm \sum_{i,j=1}^r \mu_{ij} V_i^* X V_j$. Then,

$$\frac{1}{2}(\psi_+ + \psi_-) = \Phi.$$

(finish next time ...)

24 Day - 19/Oct/11

24.1 Continuation

Theorem 3 (Choi). If $\Phi : M_n \to M_d$, $cr(\Phi) = r$, and $\Phi(X) = \sum_{i=1}^{r} V_i^* X V_i$, then Φ is extreme in $UCP(M_n, M_d)$ if and only if

$$\{V_i^* V_j \ : \ 1 \leq i, j \leq r\} \subseteq M_d$$

is linearly independent.

Proof. ($\Rightarrow$): Last time we had shown that it is enough to show that if $\sum_{i,j=1}^{r} \mu_{ij} V_i^* V_i = 0$ and $\mu = (\mu_{ij}) = \mu^*$, then $\mu = 0$. We scaled $-I \leq \mu \leq +I$ and let

$$\psi_{\pm}(X) = \sum_{i,j=1}^{r} V_i^* X V_i \pm \sum_{i,j=1}^{r} \mu_{ij} V_i^* X V_j.$$

Write $(I + \mu) = (\alpha_{ij})^*(\alpha_{ij})$. Let

$$W_i = \sum_{j=1}^{r} \alpha_{ij} V_j.$$

Then,

$$\begin{aligned}
\sum_{k=1}^{r} W_k^* X W_k &= \sum_{k=1}^{r} (\sum_{i=1}^{r} \overline{\alpha}_{ki} V_i^*) X (\sum_{j=1}^{r} \alpha_{kj} V_j) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{r} (\sum_{k=1}^{r} \overline{\alpha}_{ki} \alpha_{kj}) V_i^* X V_j \\
&= \sum_{i=1}^{r} (1 + \mu_{ii}) V_i^* X V_i + \sum_{i \neq j} \mu_{ij} V_i^* X V_j \\
&= \sum_{i=1}^{r} V_i^* X V_i + \sum_{i,j} \mu_{ij} V_i^* X V_j \\
&= \psi_+(X).
\end{aligned}$$

Therefore, ψ_+ is a completely positive map. Also,

$$\begin{aligned}
\psi_+(I_n) &= \sum_{i=1}^{r} V_i^* I_n V_i + \sum_{i,j=1}^{r} \mu_{ij} V_i^* V_j \\
&= \Phi(I_n) + 0 \\
&= I.
\end{aligned}$$

Similarly, $0 \leq I - \mu = (\beta_{ij})^*(\beta_{ij})$. Set $\tilde{W}_i = \sum \beta_{ij} V_j$, and we get

$$\sum_{k=1}^{r} \tilde{W}_i^* X \tilde{W}_i = \psi_-(X).$$

Therefore, ψ_- is completely positive and

$$\psi_-(I) = \Phi(I) + 0 = I.$$

Now,

$$\begin{aligned}\frac{1}{2}(\psi_+(X) + \psi_-(X)) &= \frac{1}{2}(\sum_{i=1} rV_i^*XV_i + \sum_{i,j=1}^{r} \mu_{ij}V_i^*XV_j + \sum_{i=1}^{r} V_i^*XV_i - \sum_{i,j=1}^{r} \mu_{ij}V_i^*XV_j) \\ &= \Phi(X).\end{aligned}$$

Since Φ is extreme, $\Phi = \psi_+ = \psi_-$. However,

$$\psi_+(X) = \sum_{k=1}^{r} W^*XW_k = \Phi(X).$$

By Choi's earlier theorem, there exists unique $U = (u_{ij})$ such that

$$W_i = \sum_{j=1}^{r} u_{ij}V_j$$

and $U^*U = I$. We also know that $\{V_1, \ldots, V_r\}$ are linearly independent.

Earlier, we had $W_i = \sum_{j=1}^{r} \alpha_{ij}V_j$. Therefore, $\alpha_{ij} = u_{ij}$ and

$$I = U^*U = (\alpha_{ij})^*(\alpha_{ij}) = I + \mu.$$

This implies $\mu = 0$ and $\mu_{ij} = 0$ for all i, j. Therefore, the $V_i^*V_j$ are linearly independent.

($\Leftarrow$): Note that if $\{V_i^*V_j\}$ are linearly independent, we claim that the $\{V_1, \ldots, V_r\}$ are linearly independent. In fact, suppose that

$$\beta_1V_1 + \ldots + \beta_rV_r = 0.$$

Then,

$$(\sum_{i=1}^{r} \beta_iV_i)^*(\sum_{j=1}^{r} \beta_jV_j) = 0.$$

This implies $\sum_{i,j=1}^{r} \overline{\beta}_i\beta_jV_i^*V_j = 0$. Hence, $\overline{\beta}_i\beta_j = 0$ for all i, j, which implies $\beta_i = 0$ for all i.

Now, suppose that $\Phi(X) = \frac{1}{2}(\psi_1(X) + \psi_2(X))$, where the ψ_j are unital and completely positive. Let

$$\psi_1(X) = \sum_{p=1}^{m_1} W_p^*XW_p, \psi_2(X) = \sum_{p=m_1+1}^{m_1+m_2} W_p^*XW_p.$$

Then,

$$\Phi(X) = \sum_{p=1}^{m_1+m_2} (\frac{1}{\sqrt{2}}W_p)^*X(\frac{1}{\sqrt{2}}W_p).$$

Therefore, there exists unique α_{pj} so that

$$\frac{1}{\sqrt{2}}W_p = \sum_{j=1}^{r} \alpha_{pj} V_j$$

and $U = (\alpha_{pj})_{(m_1+m_2)\times r}$ satisfies $U^*U = I_r$.

By the above,

$$\begin{aligned} I &= \sum_{i=1}^{r} V_i^* V_i = \psi_1(I) \\ &= \sum_{p=1}^{m_1} W_p^* W_p \\ &= 2\sum_{p=1}^{m_1} (\sum_{i=1}^{r} \overline{\alpha}_{pi} V_i^*)(\sum_{j=1}^{r} \alpha_{pj} V_j) \\ &= 2\sum_{i,j=1}^{r} (\sum_{p=1}^{m_1} \overline{\alpha}_{pi}\alpha_{pj}) V_i^* V_j. \end{aligned}$$

Therefore,

$$2\sum_{p=1}^{m_1} \overline{\alpha}_{pi}\alpha_{pj} = \delta_{ij}.$$

Therefore, if we set

$$U = \begin{pmatrix} (U_1)_{m_1} \\ \cdots \\ (U_2)_{m_2} \end{pmatrix},$$

we have

$$\begin{aligned} I &= U^*U \\ &= (U_1^* \vdots U_2) \begin{pmatrix} U_1 \\ \cdots \\ U_2 \end{pmatrix} \\ &= U_1^*U_1 + U_2^*U_2. \end{aligned}$$

The above sums are the entries of $U_1^*U_1$. This implies $2U_1^*U_1 = I_r$. So, $U_1^*U_1 =$

$\frac{1}{2}I_r$. Similarly, $U_2^*U_2 = \frac{1}{2}I_r$. Thus,

$$\begin{aligned}
\psi_1(X) &= \sum_{p=1}^{m_1} W_p^* X W_p \\
&= \sum_{p=1}^{m_1} (\sqrt{2}\sum_{i=1}^{r} \overline{\alpha}_{pi} V_i^*) X (\sqrt{2}\sum_{i=1}^{r} \alpha_{pi} V_i) \\
&= 2\sum_{i,j=1}^{r} (\sum_{p=1}^{m_1} \overline{\alpha}_{pi}\alpha_{pj}) V_i^* X V_j \\
&= \sum_{i=1}^{r} V_i^* X V_i \\
&= \Phi(X).
\end{aligned}$$

Similarly, $\psi_2(X) = \Phi(X)$. By definition, Φ is extreme.

$\boxtimes$

Examples. (1) Let U be an $n \times n$ unitary and $\Phi : M_n \to M_n \in UCP(M_n, M_n)$. Suppose $\Phi(X) = U^*XU$. Then $r = 1$ and $\{U^*U\}$ is linearly independent. So, Φ is extreme.

(2) Suppose that U_1, U_2 are unitaries. Then

$$\Phi : M_n \to M_n, \Phi(X) = \frac{1}{2}(U_1^*XU_1 + U_2^*XU_2),$$

is not extreme because if we let $V_1 = \frac{1}{\sqrt{2}}U_1$, $V_2 = \frac{1}{\sqrt{2}}U_2$, then,

$$\{V_i^*V_j \,:\, 1 \le i,j \le 2\} = \{\frac{1}{2}U_1^*U_1, \frac{1}{2}U_1^*U_2, \frac{1}{2}U_2^*U_1, \frac{1}{2}U_2^*U_2\}$$

is not linearly independent since $\frac{1}{2}U_1^*U_1 = \frac{1}{2}U_2^*U_2 = \frac{1}{2}I$.

(3) Let $\Phi : M_n \to M_d$ be given by $\Phi(X) = tr(X)I_d$. Then, $\Phi(E_{ij}) = tr(E_{ij})I_d = \delta_{ij}I_d$. So,

$$P_\Phi = (\Phi(E_{ij})) = (\delta_{ij}I_d) \in M_n(M_d).$$

So, $cr(\Phi) = nd > d$. This implies Φ is not extreme.

(4) Let $\Phi : M_n \to M_n$ be given by

$$\Phi(X) = diag(X) = \begin{pmatrix} x_{11} & & 0 \\ & \ddots & \\ 0 & & x_{nn} \end{pmatrix}.$$

Then $rank(P_\Phi) = rank \begin{pmatrix} E_{11} & & 0 \\ & \ddots & \\ 0 & & E_{nn} \end{pmatrix} = n$ and $n = d$. However,

$$\Phi(X) = \sum_{i=1}^{n} E_{ii}XE_{ii},$$

and if we set $V_i = E_{ii}$, $\{V_i^*V_j\}$ is not linearly independent.

25 Day - 24/Oct/11

25.1 Operator Systems, Arveson's Correspondence, Arveson's Extension Theorem

Overview. Recall that Choi showed that

$$\Phi : M_n \to M_d \leftrightarrow P_\Phi \in M_n(M_d)$$

and his work also showed

$$\Phi \text{ completely positive} \Leftrightarrow \Phi n\text{-positive.}$$

Arverson's correspondence will show that

$$\Phi : M_n \to M_d \leftrightarrow S_\Phi : M_d(M_n) \to \mathbb{C},$$
$$CP(M_n, M_d) \leftrightarrow \text{positive linear functionals,}$$
$$\text{and}$$
$$\Phi \text{ completely positive} \Leftrightarrow \Phi d\text{-positive.}$$

Definition. A subspace $S \subset B(H)$ of the bounded linear functionals on H is called an *operator system* provided $I \in S$ and $X \in S$ implies $X^* \in S$.

Given an operator system $S \subseteq B(H)$, we identify

$$M_p(S) \subset B(H \oplus \ldots \oplus H)$$

by letting $(X_{ij}) \in M_p(S)$ be identified with the operator

$$(X_{ij}) : H \oplus \ldots \oplus H \to H \oplus \ldots \oplus H,$$
$$(X_{ij}) \begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^p X_{1j} h_j \\ \vdots \\ \sum_{j=1}^p X_{pj} h_j \end{pmatrix}.$$

In particular, this allows us to define $M_p(S)^+$ as the elements that define positive operators.

Note. $M_p(S)$ is an operator system in $B(H \oplus \ldots \oplus H)$ because the identity is

$$\begin{pmatrix} I & & 0 \\ & \ddots & \\ 0 & & I \end{pmatrix}$$

and $X = (X_{ij}) \in M_p(S)$ implies $X^* = (X_{ji}^*) \in M_p(S)$.

Definition. If S is an operator system, then $\Phi : S \to M_d$ is *completely positive* provided $(X_{ij}) \in M_p(S)^+$ implies $(\Phi(X_{ij})) \in M_p(M_d)$ for all p. Similarly, we define *k-positive* when this is true for $p = k$.

Proposition. Let S be an operator system and $X \in S$. Then there exists $P_1, P_2, P_3, P_4 \in S^+$ such that $X = (P_1 - P_2) + i(P_3 - P_4)$.

Proof. Since $X \in S$, $X^* \in S$. This implies

$$X = H + iK,$$

where $H = \frac{X+X^*}{2}$ and $K = \frac{X-X^*}{2i}$. Since $H = H^*, K = K^*$, $H, K \in S$. Now, $H = H^* \in S \subseteq B(H)$ and we know that $||H||I - H \geq 0$ and $||H||I + H \geq 0$. Let

$$P_1 = \frac{||H||I + H}{2}, P_2 = \frac{||H||I - H}{2}.$$

Then, $P_1, P_2 \in S^+$ and $H = P_1 - P_2$. We similarly do this for K.

$\boxtimes$

25.2 Arveson's Extension Theorem

Theorem (Arveson's Extension, 1969). If $S \subseteq M_n$ is an operator system and $\Phi : S \to M_d$ is completely positive, then there exists $\psi : M_n \to M_d$ that is completely positive and $\psi(X) = \Phi(X)$ for all $X \in S$.

Corollary. If $\Phi : S \to M_d$ is completely positive, then there exists $n \times d$ $A_1, \ldots, A_r$ so that

$$\Phi(X) = \sum_{i=1}^{r} A_i^* X A_i.$$

Proof. Extend Φ to ψ and use the *Choi-Krauss representation* of ψ.

$\boxtimes$

25.3 Arveson's Correspondence

Definition. Given $\Phi : S \to M_d$ and an orthonormal basis $e_1, \ldots, e_d$ on $\mathbb{C}^d$, let

$$f_{ij} : S \to \mathbb{C}$$

be defined by

$$f_{ij}(X) = \langle e_i | \Phi(X) e_j \rangle.$$

Hence, $\Phi(X) = (f_{ij}(X))_{d \times d}$. Now define

$$S_\Phi : M_d(S) \to \mathbb{C}$$

by

$$S_\Phi((X_{ij})) = \frac{1}{d} \sum_{i,j=1}^{d} f_{ij}(X_{ij}).$$

Theorem (Arveson). If S is an operator system and $\Phi : S \to M_d$ is linear, then the following are equivalent:

(1) Φ is completely positive;

(2) Φ is d-positive;

(3) S_Φ is a positive linear functional.

Proof. (1) $\Rightarrow$ (2): Obvious.
(2) $\Rightarrow$ (3): Let $(X_{ij})_{i,j=1}^d \in M_d(S)^+$. Then, $(\Phi(X_{ij})) \in M_d(M_d)^+$. Consider

$$v = \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix} \in \mathbb{C}^d \oplus \ldots \oplus \mathbb{C}^d.$$

Hence,

$$(X_{ij}) \in M_d(S)^+$$

implies

$$\begin{aligned} 0 &\leq \langle v|(\Phi(X_{ij}))v\rangle \\ &= \left\langle \begin{pmatrix} e_1 \\ \vdots \\ e_d \end{pmatrix} | \begin{pmatrix} \sum_{j=1}^{\Phi}(X_{1j})e_j \\ \vdots \\ \sum_{j=1}^d \Phi(X_{dj})e_j \end{pmatrix} \right\rangle \\ &= \sum_{i,j=1}^d \langle e_i|\Phi(X_{ij})e_j\rangle \\ &= \sum_{i,j} = 1^d f_{ij}(X_{ij}) \\ &= dS_\Phi((X_{ij})). \end{aligned}$$

Therefore, S_Φ is a positive linear functional.

(3) $\Rightarrow$ (1): We must show that for any q, when $(X_{rs})_{r,s=1}^q \in M_q(S)^+$, then $(\Phi(X_{rs})) \in M_q(M_d)^+$. To do this, let $v_s \in \mathbb{C}^d$, for $1 \leq s \leq q$. Then,

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_q \end{pmatrix} \in \mathbb{C}^d \oplus \ldots \oplus \mathbb{C}^d.$$

Then,

$$\begin{aligned} 0 &\leq \langle v|(\Phi(X_{rs}))v\rangle \\ &= \sum_{r,s=1}^q \langle v_r|\Phi(X_{rs})v_s\rangle \\ &= (*) \end{aligned}$$

If we write $v_s = \sum_{j=1}^{d} v_{sj} e_j$, then

$$\begin{aligned}(*) &= \sum_{r,s=1}^{q} \sum_{i,j=1}^{d} \overline{v}_{ri} v_{sj} \langle e_i | \Phi(X_{rs}) e_j \rangle \\ &= \sum_{r,s=1}^{q} \sum_{i,j=1}^{d} \overline{v}_{ri} v_{sj} f_{ij}(X_{ij}) \\ &= \sum_{i,j=1}^{d} f_{ij}\Big(\sum_{r,s=1}^{q} \overline{v}_{ri} v_{sj} X_{rs}\Big).\end{aligned}$$

Let

$$Y_{ij} = \sum_{r,s=1}^{q} \overline{v}_{ri} v_{sj} X_{rs} \in S.$$

Then,

$$Y = (Y_{ij})_{i,j=1}^{d} \in M_d(S)$$

and

$$(*) = dS_{\Phi}(Y).$$

Hence, it is enough to show that $Y \in M_d(S)^+$. Let

$$A = \begin{pmatrix} v_1^t \\ \vdots \\ v_q^t \end{pmatrix}_{q \times d}.$$

Then a calculation shows that $Y = A^* X A$. Since $X \geq 0$, $Y \geq 0$.

$\boxtimes$

26 Day - 26/Oct/11

26.1 Arveson Correspondence

$$\begin{array}{ccc} \mathcal{L}(S, M_d) & & \mathcal{L}(M_d(S), \mathbb{C}) \\ \Phi(X) = (f_{ij}(X)) & \mapsto & S_{\Phi}((X_{ij})) = \frac{1}{d} \sum_{i,j=1}^{d} f_{ij}(X_{ij}) \end{array}$$

If we start with $f : M_d(S) \to \mathbb{C}$, define $f_{ij} : S \to \mathbb{C}$ by $f_{ij}(X) = f(E_{ij} \otimes X)$. Then we define $\Phi_f : S \to M_d$ by $\Phi_f(X) = d(f_{ij}(X))$.

$$\begin{array}{ccc} \mathcal{L}(M_d(S), \mathbb{C}) & & \mathcal{L}(S, M_d) \\ f & \mapsto & \Phi_f \end{array}$$

We want to check that these operations are mutual inverses.

If we begin with $f : M_d(S) \to \mathbb{C}$, we obtain $\Phi_f : S \to M_d$ and $S_{\Phi_f} : M_d(S) \to \mathbb{C}$. We need to show that $S_{\Phi_f} = f$. Given $(X_{ij}) \in M_d(S)$, then $(X_{ij}) = \sum_{i,j} E_{ij} \otimes X_{ij}$. Therefore,

$$f((X_{ij})) = \sum_{i,j} f(E_{ij} \otimes X_{ij}) = \sum_{i,j} f_{ij}(X_{ij}).$$

However,

$$S_{\Phi_f}(X_{ij})(X_{ij}) = \frac{1}{d} \sum_{i,j=1}^{d} df_{ij}(X_{ij}).$$

The other direction is an exercise.

Definition. Let $P(M_d(S), \mathbb{C})$ denote the set of positive linear functionals from $M_d(S)$ to $\mathbb{C}$ and $UP(M_d(S), \mathbb{C})$ the unital positive linear functionals, which are also called *states*.

Theorem (Arveson Correspondence). The map $\Phi \to S_\Phi$ defines an affine isomorphism from $CP(S, M_d)$ onto $P(M_d(S), \mathbb{C})$. If Φ is also unital, then $S_\Phi \in UP(M_d(S), \mathbb{C})$.

Proof. Last time we showed that $\Phi \in CP(S, M_d)$ if and only if $S_\Phi \in P(M_d(S), \mathbb{C})$. Given $f \in (M_d(S), \mathbb{C})$, form $\Phi_f : S \to M_d$ and $S_{\Phi_f} = f$ because of mutual inverses. Therefore, $S_{\Phi_f} \in P(M_d(S), \mathbb{C})$ implies $\Phi_f \in CP(S, M_d)$. Hence, $\Phi \to S_\Phi$ maps $CP(S, M_d)$ onto $P(M_d(S), \mathbb{C})$.

Let $\Phi = (f_{ij})$ and $\Psi = (g_{ij})$. Then

$$t\Phi + (1-t)\Psi = (tf_{ij} + (1-t)g_{ij}).$$

So,

$$\begin{aligned} S_{t\Phi+(1-t)\Psi}((X_{ij})) &= \frac{1}{d} \sum_{i,j} (tf_{ij} + (1-t)g_{ij})(X_{ij}) \\ &= tS_\Phi + (1-t)S_\Psi. \end{aligned}$$

Suppose $\Phi : S \to M_d$ is unital and $\Phi = (f_{ij})$. Then, $I = \Phi(I)$ implies

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{d \times d} = \begin{pmatrix} f_{11}(I) & \dots & f_{1d}(I) \\ & \ddots & \\ f_{d1}(I) & \dots & f_{dd}(I) \end{pmatrix}.$$

So, $f_{ij}(I) = \delta_{ij}$. Therefore, $S_\Phi : M_d \to \mathbb{C}$ satisfies

$$S_\Phi \left(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right) = \frac{1}{d} \sum_{i=1}^{d} f_{ii}(I) = 1.$$

$\boxtimes$

Note: If $f : M_d(S) \to \mathbb{C}$, then f unital does not imply $\Phi_f : S \to M_d$ unital. Observe that f unital implies

$$f\left(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\right) = 1.$$

Since $f_{ij}(X) = f(E_{ij} \otimes X)$,

$$\begin{aligned} f\left(\begin{pmatrix} I & & 0 \\ & \ddots & \\ 0 & & I \end{pmatrix}\right) &= f(\sum_{i=1}^{d} E_{ii} \otimes I) \\ &= \sum_{i=1}^{d} f_{ii}(I) \\ &= 1. \end{aligned}$$

However,

$$\Phi_f(I) = d(f_{ij}(I)) = d\begin{pmatrix} f_{11}(I) & \dots & f_{1d}(I) \\ & \ddots & \\ f_{d1}(I) & \dots & f_{dd}(I) \end{pmatrix}.$$

All we get is $tr(\Phi_f(I)) = 1$.

26.2 Hahn-Banach Theorem

Definition. Let W be a normed space. A linear functional $f : W \to \mathbb{C}$ is called *bounded* if there exists a constant C such that $|f(W)| \leq C||w||$. When f is bounded, the least such C is called the *norm of* f, denoted $||f||$, and is given by

$$||f|| = sup\{|f(w)| \, : \, ||w|| \leq 1\}.$$

Theorem (Hahn-Banach). Let W be a normed space and $V \subseteq W$ a subspace. Let $g : V \to \mathbb{C}$ be a bounded linear functional. Then there exists a bounded linear functional $f : W \to \mathbb{C}$ with $||f|| = ||g||$ and $f(v) = g(v)$ for all $v \in V$.

26.3 Arveson's Extension Theorem

Theorem (Arveson's Extension Theorem). Let $S \subseteq M_n$ be an operator system and $\Phi : S \to M_d$ a completely postive map. Then there exists $\Psi : M_n \to M_d$ that is completely positive and $\Psi(X) = \Phi(X)$ for all $X \in S$.

To prove this, we need lemmas:

Proposition. Let S be an operator system and $f : S \to \mathbb{C}$ be linear such that $f(I) = 1$. Then f is positive if and only if $||f|| = 1$.

Proof. ($\Leftarrow$): Let $P \in S^+$. Suppose $f(P) = \lambda$ is not positive. Recall that $\sigma(P) \subseteq [0, ||p||]$. Pick $a \in \mathbb{C}$ and $r > 0$ so that $|\lambda - a| > r$ but $0 \leq t \leq ||p||$ implies $|t - a| < r$. Look at $P - aI$, which is diagonalizable. Then,

$$\sigma(P - aI) \subseteq \{t - a \, : \, 0 \leq t \leq ||p||\}.$$

$$||P - aI|| = max\{|\lambda - a \, : \, \lambda \in \sigma(P - aI)\}$$

implies $||P - aI|| < r$. However,

$$f(P - aI) = f(P) - af(I) = \lambda - a$$

and

$$|f(P - aI)| = |\lambda - a| > r > ||P - aI||.$$

This contradicts $||f|| = 1$. Therefore, $f(P) \in [0, ||p||]$ and $f(P) \geq 0$.

($\Rightarrow$): Given $H = H^* \in S$, we proved that $H = P_1 - P_2$ such that $P_1, P_2 \in S^+$. This implies

$$f(H) = f(P_1) - f(P_2) \in \mathbb{R}.$$

Also,

$$-||H||I \leq H \leq +||H||I;$$

i.e.,

$$||H||I - H, H - ||H||I \in S^+.$$

This implies

$$||H|| - f(H) = f(||H||I - H) \geq 0.$$

So, $f(H) \leq ||H||$. Using the other inequality, we get

$$-||H|| \leq f(H).$$

So, $|f(H)| \leq ||H||$.

Now, let $X \in S$ such that $||X|| \leq 1$. We need to show that $|f(X)| \leq 1$. Let $f(X) = \lambda = e^{i\theta}r$, where $r = |\lambda|$. This implies

$$f(e^{-i\theta}X) = r \geq 0.$$

Write $e^{-i\theta}X = H + iK$. Then,

$$H = \frac{e^{-i\theta}X + (e^{-i\theta}X)^*}{2}$$

and $||H|| \leq 1$. So,

$$0 \leq r = f(H + iK) = f(H) + if(K).$$

This implies $r = f(H)$ and $|r| = |f(H)| \leq ||H|| \leq 1$. Therefore, $|f(X)| = r \leq 1$. $\boxtimes$

27 Day - 28/Oct/11

27.1 Continuation

Proposition. If $\Phi : S \to M_d$ is completely positive such that $\Phi(I) = P$, then there exists a unital completely positive map $\psi : S \to M_r$ and a $d \times r$ matrix V such that $\Phi(X) = V^* \psi(X) V$.

Proof. First suppose that P is invertible. Let

$$\psi(X) = P^{-1/2} \Phi(X) P^{-1/2}.$$

Then ψ is completely positive and

$$\psi(I) = P^{-1/2} \Phi(I) P^{-1/2} = I.$$

When P is not invertible, after a unitary conjugation, we can assume

$$P = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix}.$$

Take any $H = H^* \in S$. Then

$$-||H|| I \leq H \leq +||H|| I.$$

This implies

$$-||H|| \Phi(I) \leq \Phi(H) \leq +||H|| \Phi(I).$$

Hence,

$$-||H|| \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix} \leq \Phi(H) \leq +||H|| \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix},$$

which implies

$$||H|| \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & 0 \\ 0 & 0 \end{pmatrix} \pm \Phi(H) \geq 0.$$

Thus,

$$\Phi(H) = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}.$$

Since $X \in S$, we write $X = H + iK$. So,

$$\Phi(X) = \Phi(H) + i\Phi(K) = \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}.$$

So,

$$\Phi(X) = \begin{pmatrix} \tilde{\Phi}(X) & 0 \\ 0 & 0 \end{pmatrix},$$

where $\tilde{\Phi} : S \to M(r)$ is given by

$$\tilde{\Phi}(I) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix}.$$

Now let $\psi : S \to M_r$ be defined by

$$\psi(X) = \begin{pmatrix} \lambda_1^{-1/2} & & 0 \\ & \ddots & \\ 0 & & \lambda_r^{-1/2} \end{pmatrix} \tilde{\Phi}(X) \begin{pmatrix} \lambda_1^{-1/2} & & 0 \\ & \ddots & \\ 0 & & \lambda_r^{-1/2} \end{pmatrix}.$$

Then ψ is a unital completely positive map. Let

$$V = \begin{pmatrix} \begin{pmatrix} \lambda_1^{1/2} & & 0 \\ & \ddots & \\ 0 & & \lambda_r^{1/2} \end{pmatrix} \\ 0 \end{pmatrix}.$$

Then,

$$V^* \psi(X) V = \begin{pmatrix} \tilde{\Phi}(X) & 0 \\ 0 & 0 \end{pmatrix} = \Phi(X).$$

$\boxtimes$

Proposition. Let $\Phi : M_n \to M_d$ be a completely positive map. Then there exists $r > 0$, a $r \times n$ matrix V, and a completely positive and trace-preserving map $\psi : M_r \to M_d$ such that

$$\Phi(X) = \psi(VXV^*).$$

Proof. Consider a completely positive map $\Phi^* : M_d \to M_n$. Then there exists a unital completely positive map $\psi : M_d \to M_r$ and a $d \times r$ matrix V such that

$$\Phi^*(Y) = V^* \psi(Y) V.$$

Therefore, if $X \in M_n, Y \in M_d$,

$$\begin{aligned} tr(Y^* \Phi(X)) &= tr(\Phi^*(Y^*)X) \\ &= tr(V^* \psi(Y^*) VX) \\ &= tr(\psi(Y^*) VXV^*) \\ &= tr(Y^* \psi^*(VXV^*)). \end{aligned}$$

Therefore, $\Phi(X) = \psi^*(VXV^*)$. Since $\psi : M_d \to M_r$ is unital and completely positive, we have that $\psi^* : M_r \to M_d$ is completely positive and trace-preserving.

$\boxtimes$

Theorem (Arveson Extension). Let $S \subseteq M_n$ be an operator system and $\Phi : S \to M_d$ be a completely positive map. Then there exists a completely positive map $\psi : M_n \to M_d$ such that $\psi(X) = \Phi(X)$ for all $X \in S$.

Proof. We only do the case when $\Phi(I) = I$. Consider $S_\Phi : M_d(S) \to \mathbb{C}$, which is a unital positive linear functional. We write $\Phi(X) = (f_{ij}(X))$ and

$$S_\Phi((X_{ij})) = \frac{1}{d} \sum_{i,j=1}^{d} f_{ij}(X_{ij}).$$

Last time we saw that S_Φ unital and positive implies $||S_\Phi|| = 1$. Since $M_d(S) \subseteq M_d(M_n)$, we apply the *Hahn-Banach theorem* to obtain $f : M_d(M_n) \to \mathbb{C}$ such that $||f|| = 1$. Then,

$$S_\Phi\left(\begin{pmatrix} I & & 0 \\ & \ddots & \\ 0 & & I \end{pmatrix}\right) = 1$$

implies

$$f\left(\begin{pmatrix} I & & 0 \\ & \ddots & \\ 0 & & I \end{pmatrix}\right) = 1.$$

Therefore, f is unital and $||f|| = 1$. This implies f is positive.

Now consider $\Phi_f : M_n \to M_d$ which is unital and completely positive. By *Arveson's Correspondence*, Φ_f extends Φ because for any $X \in S$, $\Phi_f(X) = (\tilde{f}_{ij}(X))$ and $\tilde{f}_{ij} : M_n \to \mathbb{C}$ extends $f_{ij} : S \to \mathbb{C}$.

When Φ is not unital, write $\Phi(X) = V^* \psi(X) V$ with ψ unital and completely positive. The apply the above casse to ψ.

$\boxtimes$

Corollary. If $\Phi : S \to M_d$ is completely positive, then there exists $n \times d$ matrices A_i such that $\Phi(X) = \sum_{i=1}^{r} A_i^* X A_i$.

Proof. Extend Φ to $\psi : M_d \to M_d$, then ψ has this form by *Choi-Krauss*.

$\boxtimes$

27.2 Entanglement Revisited

Recall that given H_A, H_B in states ψ, ϕ, respectively, then $H_A \otimes H_B$ is in state $\psi \otimes \phi$. The matrix identification of states as rank one density matrices gives

$$|\psi \otimes \phi\rangle\langle\psi \otimes \phi| = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| \in \mathcal{L}(H_A) \otimes \mathcal{L}(H_B) = \mathcal{L}(H_A \otimes H_B).$$

If we have ensembles (or mixed states), $\{\psi_i, p_i\}$ on H_A and $\{\phi_j, q_j\}$ on H_B, with $p_i, q_j \geq 0$ such that $\sum p_i = 1 = \sum q_j$ and $||\psi_i|| = ||\phi_j|| = 1$, then this is represented by

$$\{\psi_i \otimes \phi_j, p_i q_j\} \leftrightarrow \sum p_i q_j |\psi_i\rangle\langle\psi_i| \otimes |\phi_j\rangle\langle\phi_j|,$$

which is a positive matrix of trace one; i.e., a density matrix.

Definition. A density matrix $P \in \mathcal{L}(H_A \otimes H_B)$ is called *separable* if it has the form

$$P = \sum p_l |\psi_l\rangle\langle p_l| \otimes |\phi_l\rangle\langle\phi_l|,$$

where $||\psi_l|| = ||\phi_l|| = 1$, $\psi_l \in H_A$, $\phi_l \in H_B$, $p_l \geq 0$, $\sum p_l = 1$.

A density matrix $P \in \mathcal{L}(H_A \otimes H_B)$ is *entangled* if it is not separable.

Issues. (1) Are there any entangled density matrices?

(2) How can we tell? (Detection/Witnesses)

28 Day - 31/Oct/11

28.1 Continuation

Last time we saw that, for ensembles $\{\psi_i, p_i\}$ on H_A and $\{\phi_j, q_j\}$ on H_B, we obtain

$$\sum p_i q_j |\psi_i\rangle\langle\psi_i| \otimes |\phi_j\rangle\langle\phi_j|.$$

In matrix form, we have

$$\sum_l P_l \otimes Q_l \in \mathcal{L}(H_A \otimes H_B)^+,$$

where $P \in \mathcal{L}(H_A)^+, Q \in \mathcal{L}(H_B)^+$. We defined such a matrix $\sum_l P_l \otimes Q_l$ to be separable. Also, $P \in \mathcal{L}(H_A \otimes H_B)^+$ is not separable if and only if P is entangled.

Proposition. If $\Phi : M_n \to M_d$ is positive and

$$R \in M_r(M_n)^+ = \mathcal{L}(\mathbb{C}^r \otimes \mathbb{C}^n)^+$$

is separable, then $\Phi^{(r)}(R) \in M_r(M_d)^+$.

Proof 1. First suppose that $R = P \otimes Q$, where $P \in M_r^+, Q \in M_n^+$. Recall that

$$\Phi^{(r)} = id_r \otimes \Phi : M_r \otimes M_n \to M_r \otimes M_d.$$

Therefore,

$$\Phi^{(r)}(R) = (id_r \otimes \Phi)(P \otimes Q) = P \otimes \Phi(Q) \in M_r \otimes M_d^+.$$

Proof 2. If $P = (p_{ij})_{r \times r}$, then

$$R = P \otimes Q = (p_{ij}Q) \in M_r(M_n).$$

So,

$$\Phi^{(r)}(p_{ij}Q) = (p_{ij}\Phi(Q)) \in M_r(M_d).$$

Hence, we want to show that this is positive.

First suppose that P is rank one; i.e., $P = (\alpha_i \overline{\alpha}_j)$. Therefore,

$$\Phi^{(r)}((\alpha_i \overline{\alpha}_j Q)) = (\alpha_i \overline{\alpha}_j \Phi(Q)) \in M_r(M_d) = \mathcal{L}(\mathbb{C}^d \oplus \ldots \oplus \mathbb{C}^d).$$

Take $h_1, \ldots, h_r \in \mathbb{C}^d$. Then,

$$\begin{aligned}\langle \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} | (\alpha_i \overline{\alpha}_j \Phi(Q)) \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} \rangle &= \sum_{i,j=1}^{r} \langle h_i | \alpha_i \overline{\alpha}_j \Phi(Q) h_j \rangle \\ &= \langle | \Phi(Q) h \rangle,\end{aligned}$$

where $h = \sum_{j=1}^{r} \overline{\alpha}_j h_j$.

Now, P, in general, is a sum of rank one positive matrices. Decomposing P as a sum of rank one matrices decomposes $(p_{ij}\Phi(Q))$ as a sum of positive matrices. This shows that if $R = P \otimes Q$, then $\Phi^{(r)}(R) \geq 0$.

For a general separable R, write $R = \sum_l P_l \otimes Q_l$. Then, $\Phi^{(r)}(R) = \sum_l \Phi(P_l \otimes Q_l)$, where each term is the sum is positive. So, $\Phi^{(r)}(R)$ is positive.

$\boxtimes$

Corollary. If $R \in M_r(M_n)^+$ and $\Phi : M_n \to M_d$ is positive, then $\Phi^{(r)}(R)$ not positive implies R entangled.

Examples. If $i \neq j$, then

$$\begin{pmatrix} E_{ii} & E_{ij} \\ E_{ji} & E_{jj} \end{pmatrix}$$

is a positive matrix. Also, $(E_{ij}) \in M_n(M_n)^+$. Both of these are entangled. For example, take $\Phi : M_n \to M_n$, $\Phi(X) = X^t$, which is positive. However,

$$\Phi^{(2)} \left(\begin{pmatrix} E_{ii} & E_{ij} \\ E_{ji} & E_{jj} \end{pmatrix} \right) = \begin{pmatrix} E_{ii} & E_{ji} \\ E_{ij} & E_{jj} \end{pmatrix}.$$

Take $h = \left(\begin{smallmatrix} e_j \\ -e_i \end{smallmatrix} \right)$. Then,

$$\begin{aligned}\langle \left(\begin{smallmatrix} e_j \\ -e_i \end{smallmatrix} \right) | \begin{pmatrix} E_{ii} & E_{ji} \\ E_{ij} & E_{jj} \end{pmatrix} \left(\begin{smallmatrix} e_j \\ -e_i \end{smallmatrix} \right) \rangle &= \langle \left(\begin{smallmatrix} e_j \\ -e_i \end{smallmatrix} \right) | \left(\begin{smallmatrix} -e_j \\ e_i \end{smallmatrix} \right) \rangle \\ &= -\langle e_j | e_j \rangle - \langle e_i | e_i \rangle \\ &= -2.\end{aligned}$$

Similarly, $\Phi^(n)((E_{ij})) = (E_{ji})$, which was previously shown to not be positive.

$\boxtimes$

Our goal is to prove the following two theorems:

Theorem. Let $R \in M_r(M_n)$. Then R is separable if and only if $\Phi^{(r)}(R) \geq 0$ for all positive maps $\Phi : M_n \to M_n$.

Corollary. If $R \in M_r(M_n)^+$ is entangled, then there exists a positive map $\Phi : M_n \to M_n$ such that $\Phi^{(r)}(R)$ is not positive.

Notation. Let $Sep \subseteq M_r(M_n)$ be the set of separable matrices: $Sep = \{\sum_l P_l \otimes Q_l\}$.

Proposition. Let $f : M_r(M_n) \to \mathbb{C}$ be a linear functional. Then $f(Sep) \geq 0$ if and only if $\Phi_f : M_n \to M_r$ is positive.

Proof. ($\Rightarrow$): Let $P \in M_n^+$ and $v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix} \in \mathbb{C}^r$. We must show that $\langle v|\Phi_f(P)v\rangle \geq 0$:

$$\begin{aligned} \langle v|\Phi_f(P)v\rangle &= \sum \overline{\alpha}_i\alpha_j\langle e_i|\Phi_f(P)e_j\rangle \\ &= \sum \overline{\alpha}_i\alpha_j f_{ij}(P) \\ &= \overline{\alpha}_i\alpha_j f(E_{ij}\otimes P) \\ &= f((\sum_{i,j} \overline{\alpha}_i\alpha_j E_{ij})\otimes P) \\ &\geq 0 \end{aligned}$$

since $(\sum_{i,j} \overline{\alpha}_i\alpha_j E_{ij}) \otimes P \in Sep$.

($\Leftarrow$): Let $P \in M_n^+$ and $Q = (q_{ij}) \in M_r^+$. We want to show $f(Q\otimes P) \geq 0$. It is enought to do the case when Q is a rank one positive matrix. In this case, write $Q = (\overline{\alpha}_i\alpha_j) = \sum \overline{\alpha}_i\alpha_j E_{ij}$. Therefore,

$$\begin{aligned} f(Q\otimes P) &= \sum_{i,j=1}^{r} \overline{\alpha}_j\alpha_j f(E_{ij}\otimes P) \\ &= 7\sum_{i,j=1}^{r} \overline{\alpha}_i\alpha_j\langle e_i|\Phi_f(P)e_j\rangle \\ &= \langle v|\Phi_f(P)v\rangle \\ &\geq 0. \end{aligned}$$

⊠

28.2 Theory of Convex Sets and Linear Functionals

Definition. Let V be a finite dimensional real vector space. A subset $C \subset V$ is a *cone* provided if $x, y \in C$ and $0 \leq t, s$, then $tx + sy \in C$.

Alternatively, C is a cone if C is convex and $x \in C$ implies $tx \in C$ for all $t \geq 0$.

Theorem. Let V be a real vector space, $K \subseteq V$ a closed convex subspace, and $y \notin K$. Then there exists a linear functional $f : V \to \mathbb{R}$ and $\alpha \in \mathbb{R}$ so that $f(y) < \alpha \leq f(K)$.

Corollary. Let V be a real vector space, $C \subseteq V$ a closed cone, and $y \notin C$. Then there exists a linear functional $f : V \to \mathbb{R}$ such that $f(y) < 0 \leq f(C)$.

Proof. Take the f given by the theorem. Then there exists α such that $f(y) < \alpha \leq f(C)$. Since $0 \in C$, $\alpha \geq 0$. Suppose there was $x \in C$ such that $f(x) < 0$. Then $tx \in C$ for all $t \geq 0$. This implies $\alpha < f(tx) = tf(x)$. By taking t large enough, we get $tf(x) < \alpha$, a contradiction. So, $0 \leq f(x)$ for all $x \in C$.

⊠

29 Day - 2/Nov/11

29.1 Continuation

Theorem. Let V be a real finite dimensional vector space, $C \subseteq V$ a closed cone, and $w \notin C$. Then there exists a real linear functional $f : V \to \mathbb{R}$ such that $f(w) < 0 \leq f(C)$.

Note. Let $M_r(M_n)_h$ be the set of Hermitian (or self-adjoint) matrices, which is a real vector space. Let

$$C = \{\sum_l P_l \otimes Q_l \, : \, P_l \in M_r^+, Q_l \in M_n^+\}.$$

Then C is a closed cone.

$R \in M_r(M_n)^+$ entangled means that $R \notin C$. So, there exists a real linear functional $f : M_r(M_n) \to \mathbb{R}$ such that $f(R) < 0 \leq f(C)$.

Given $X \in M_r(M_n)$, write $X = H + iK$ with H, K self-adjoint. Define $\tilde{f} : M_r(M_n) \to \mathbb{C}$ by

$$\tilde{f}(H + iK) = f(H) + if(K).$$

We show that $\tilde{f}$ is complex linear:

$$\begin{aligned} \tilde{f}((a+ib)(H+iK)) &= \tilde{f}((aH - bK) + i(bH + aK)) \\ &= f(aH - bK) + if(bH + aK) \\ &= af(H) - bf(K) + ibf(H) + af(K) \\ &= (a+ib)(f(H) + if(K)) \\ &= (a+ib)\tilde{f}(H+iK). \end{aligned}$$

Note. We have that $\tilde{f}(R) = f(R)$ and $\tilde{f}(C) = f(C)$. So, $\tilde{f}(R) < 0 \leq \tilde{f}(C)$. By *Arveson correspondence*,

$$\tilde{f} \leftrightarrow \Phi_{\tilde{f}} : M_n \to M_r.$$

We also proved that $\tilde{f} \geq 0$ on separable matrices if and only if $\Phi_{\tilde{f}}$ is a positive map.

Theorem. Let $R \in M_r(M_n)^+$. Then R is separable if and only if $\Phi^{(r)}(R) \geq 0$ for all positive maps $\Phi : M_n \to M_r$.

Proof. ($\Rightarrow$): We have already shown that R separable implies $\Phi^{(r)}(R) \geq 0$.

($\Leftarrow$): We show the contrapositive; i.e., if R is entangled, then there exists a positive map $\Phi : M_n \to M_r$ such that $\Phi^{(r)}(R)$ is not positive.

We know that there exists a linear functional $f : M_r(M_n) \to \mathbb{C}$ such that $f(Sep) \geq 0$, $f(R) < 0$, and corresponds to a positive map

$$\Phi_f : M_n \to M_r.$$

We want to show that $\Phi_f^{(r)}(R)$ is not positive.

Recall that $\Phi_f(X) = d(f_{ij}(X))$, $1 \leq i,j \leq r$ and $f_{ij}(X) = f(E_{ij} \otimes X)$. Write

$$R = (R_{ij}) \in M_r(M_n),\ R_{ij} \in M_n$$

and

$$R = \sum_{i,j=1}^{r} E_{ij} \otimes R_{ij} \in M_r \otimes M_n.$$

Let

$$e = \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix},$$

where $e_1, \ldots, e_r$ is a basis for $\mathbb{C}^r$. We compute:

$$\begin{aligned} \langle e|\Phi^{(r)}(R)e\rangle &= \langle \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} |(\Phi_f(R_{ij})) \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} \rangle \\ &= \sum_{i,j=1}^{r} \langle e_i|\Phi_f(R_{ij})e_j\rangle \\ &= d \sum_{i,j=1}^{r} f_{ij}(R_{ij}) \\ &= \sum_{i,j=1}^{r} f(E_{ij} \otimes R_{ij}) \\ &= df(R) \\ &< 0. \end{aligned}$$

So, $\Phi_f^{(r)}(R)$ is not positive.

⊠

29.2 Universal Entanglement Witnesses

Question: Does there exists a positive map $\Phi : M_n \to M_r$ so that for any $R \in M_r(M_n)^+$, R is entangle if and only if $\Phi^{(r)}(R)$ is not positive?

Answer: Sadly, no for most n, r.

Theorem (Horodecki-Peres). Let $\Phi : M_2 \to M_2$ be defined by $\Phi(X) = X^t$. Let $v \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Then v is separable if and only if $\Phi^{(r)}(|v\rangle\langle v|) \geq 0$; i.e., if v is entangled, then $\Phi^{(2)}(|v\rangle\langle v|)$ is not positive.

Proof. Write $v = \alpha \otimes \beta$, where $\alpha = \left(\begin{smallmatrix} \alpha_1 \\ \alpha_2 \end{smallmatrix}\right)$, $\beta = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}$. In block form,

$$v = \begin{pmatrix} \alpha_1\beta \\ \alpha_2\beta \end{pmatrix} = \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right) \in \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^2 \oplus \mathbb{C}^2.$$

Now, v is separable if and only if v_1, v_2 are parallel. Hence, v is entangled if and only if v_1, v_2 are linearly independent.

Observe that

$$|v\rangle\langle v| = vv^* = \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right)(v_1^*, v_2^*) = \left(\begin{smallmatrix} v_1v_1^* & v_1v_2^* \\ v_2v_1^* & v_2v_2^* \end{smallmatrix}\right) \in M_2(M_2).$$

Therefore,

$$\Phi^{(2)}(|v\rangle\langle v|) = \left(\begin{smallmatrix} \Phi(v_1v_1^*) & \Phi(v_1v_2^*) \\ \Phi(v_2v_1^*) & \Phi(v_2v_2^*) \end{smallmatrix}\right) = \left(\begin{smallmatrix} (v_1v_1^*)^t & (v_1v_2^*)^t \\ (v_2v_1^*)^t & (v_2v_2^*)^t \end{smallmatrix}\right).$$

Write $v_j = (x_j, y_j)^t$, $j = 1, 2$. Then,

$$v_1v_1^* = \begin{pmatrix} x_1\overline{x}_1 & x_1\overline{y}_1 \\ y_1\overline{x}_1 & y_1\overline{y}_1 \end{pmatrix}$$

implies

$$(v_1v_1^*)^t = \begin{pmatrix} x_1\overline{x}_1 & y_1\overline{x}_1 \\ x_1\overline{y}_1 & y_1\overline{y}_1 \end{pmatrix} = \left(\begin{smallmatrix} \overline{x}_1 \\ \overline{y}_1 \end{smallmatrix}\right)(x_1, y_1) = \overline{v}_1\overline{v}_1^*.$$

Similarly,

$$\begin{aligned} (v_1v_2^*)^t &= \begin{pmatrix} x_1\overline{x}_2 & x_1\overline{y}_2 \\ y_1\overline{x}_2 & y_1\overline{y}_2 \end{pmatrix}^t \\ &= \begin{pmatrix} x_1\overline{x}_2 & y_1\overline{x}_2 \\ x_1\overline{y}_2 & y_1\overline{y}_2 \end{pmatrix} \\ &= \left(\begin{smallmatrix} \overline{x}_2 \\ \overline{y}_2 \end{smallmatrix}\right)(x_1, y_1) \\ &= \overline{v}_2\overline{v}_1^*. \end{aligned}$$

Therefore,

$$\Phi^{(2)}(|v\rangle\langle v|) = \begin{pmatrix} \overline{v}_1\overline{v}_1^* & \overline{v}_2\overline{v}_1^* \\ \overline{v}_1\overline{v}_2^* & \overline{v}_2\overline{v}_2^* \end{pmatrix}.$$

We apply this to the vector $w = \left(\begin{smallmatrix} -\overline{v}_2 \\ \overline{v}_1 \end{smallmatrix}\right)$:

$$\begin{aligned} \langle \left(\begin{smallmatrix} -\overline{v}_2 \\ \overline{v}_1 \end{smallmatrix}\right) | \begin{pmatrix} \overline{v}_1\overline{v}_1^* & \overline{v}_2\overline{v}_1^* \\ \overline{v}_1\overline{v}_2^* & \overline{v}_2\overline{v}_2^* \end{pmatrix} \left(\begin{smallmatrix} -\overline{v}_2 \\ \overline{v}_1 \end{smallmatrix}\right) \rangle &= \langle \left(\begin{smallmatrix} -\overline{v}_2 \\ \overline{v}_1 \end{smallmatrix}\right) | \left(\begin{smallmatrix} -\overline{v}_1\langle\overline{v}_1|\overline{v}_2\rangle + \overline{v}_2\langle\overline{v}_1|\overline{v}_1\rangle \\ -\overline{v}_1\langle\overline{v}_2|\overline{v}_2\rangle + \overline{v}_2\langle\overline{v}_2|\overline{v}_1\rangle \end{smallmatrix}\right) \rangle \\ &= \langle\overline{v}_2|\overline{v}_1\rangle\langle\overline{v}_1|\overline{v}_2\rangle - 2||\overline{v}_2||^2||\overline{v}_1||^2 \\ &\quad + \langle\overline{v}_1|\overline{v}_2\rangle\langle\overline{v}_2|\overline{v}_1\rangle \\ &= 2|\langle\overline{v}_2|\overline{v}_1\rangle|^2 - 2||\overline{v}_2||^2||\overline{v}_1||^2 \\ &< 0, \end{aligned}$$

unless $\overline{v}_1, \overline{v}_2$ are parallel and by *Cauchy-Schwarz theorem.*

⊠

30 Day - 7/Nov/11

30.1 Error Detection/Correction - Classic Binary

We start with a binary n-tuple; i.e., $v \in \mathbb{Z}_2^n$. We want to transmit v, but there is a possibility of 0 being switched to 1 or 1 to 0. Note that this corresponds

to adding +1. This could be caused by static, stray magnetism, or any other interaction with the environment. The question is how to fix it.

The idea is as follows:

$$\begin{aligned} v \in \mathbb{Z}_2^n &\xrightarrow[encoding]{\phi} \mathbb{Z}_2^{n+k} \\ &\xrightarrow{transmit} \phi(v) + error \\ &\xrightarrow{decode} v. \end{aligned}$$

Example ("Repetition"). Define $v \in \mathbb{Z}_2^n \mapsto (v, v) \in \mathbb{Z}_2^{2n}$. In the $n = 3$ case, we have

$$v = (a, b, c) \mapsto (a, b, c, a, b, c) \mapsto (a, b, c, a, b, c) + error.$$

This method and detect one error, but two errors may go undetected. Correction of errors is unknown and the cost rises from n to $2n$.

⊠

Example ("Parity Check"). Define

$$v = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n \mapsto (a_1, \ldots, a_n; a_1 + \ldots + a_n) \in \mathbb{Z}_2^{n+1}.$$

This map can detect one error but misses every pair of errors, and cannot correct even one error. However, the cost is much better than the *repetition method*.

⊠

Example (Hamming [7,1,3]). Define

$$(a_1, \ldots, a_7) \mapsto (a_1, \ldots a_7; a_1 + a_2 + a_3 + a_4; a_1 + a_2 + a_5 + a_6; a_1 + a_3 + a_5 + a_7).$$

This is equivalent to the matrix

$$\begin{pmatrix} I_7 \\ \begin{smallmatrix} 1&1&1&1&0&0&0 \\ 1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1 \end{smallmatrix} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_7 \end{pmatrix}.$$

This method can detect and correct one error.

⊠

Remark. What we seek are one-to-one maps $\mathbb{Z}_2^n \xrightarrow[encoding]{\phi} \mathbb{Z}_2^{n+k}$, where $range(\phi) = S \subseteq \mathbb{Z}_2^{n+k}$. Since $|\mathbb{Z}_2^n| = 2^n = |S|$, we want the points in S to be "far apart."

Definition. Given $w \in \mathbb{Z}_2^m$, its *Hamming weight* is defined as

$$||w|| = \#\text{ of non-zero entries of } w.$$

For $\phi(v_1)$ to be mistaken for $\phi(v_2)$, we would need a vector of errors e added to $\phi(v_1)$ so that

$$\phi(v_1) + e = \phi(v_2).$$

The number of errors that must occur is

$$||e|| = ||\phi(v_2) - \phi(v_1)||.$$

So, given $S \subseteq \mathbb{Z}_2^m$ with $|S| = 2^n$, the *Hamming weight* of S is defined as

$$min\{||v - w|| \, : \, v, w \in S, v \neq w\},$$

which is equivalent to the minimum number of errors to go from one point in S to another point in S.

Remark. For $S \subseteq \mathbb{Z}_2^m$, $|S| = 2^n$, the best Hamming weight we can hope for is when S is a subspace. In this case, for $v, w \in S$, $(v - w) \in S$. So the Hamming weight of S is equal to

$$min\{||v|| \, : \, v \in S, v \neq 0\}$$

and S a subspace implies $dim_{\mathbb{Z}_2}(S) = n$. Hence, there exists a linear map

$$\phi : \mathbb{Z}_2^n \to S \subseteq \mathbb{Z}_2^m$$

given by a matrix of ones and zeroes. Also, decoding amounts to choosing a left inverse for the matrix of ϕ.

Example. Suppose we have

$$(a, b, c) = (a, b, c; a + b + c).$$

This is equivalent to the mapping

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} : \mathbb{Z}_2^3 \to \mathbb{Z}_2^4.$$

One left inverse for ϕ is

$$\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \gamma \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Another left inverse is given as

$$\tilde{\gamma} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b + c + d \\ a + c + d \\ a + b + d \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Note that, start with $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, and observed the error

$$\phi \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

γ would produce the correction $\begin{pmatrix}0\\0\\0\end{pmatrix}$ and $\tilde{\gamma}$ would produce the correction $\begin{pmatrix}1\\1\\1\end{pmatrix}$.
$\boxtimes$

Remarks. Some of the best binary codes use Galois theory and Number theory, which are called "cyclic codes." The idea is to identity

$$\mathbb{Z}_2^m \cong P(x)/\langle x^m - 1\rangle.$$

Instead of vector subspaces, they look for ideals in $P(x)/\langle x^m - 1\rangle$. These are generated by a divisor g of $x^m - 1$.

Suppose $g(x)|(x^m-1)$ in $P(x)$ over $\mathbb{Z}_2$ and $deg(g) = m-n$. Given $p, q \in P(x)$ with $deg(p) \leq n-1$, $deg(q) \leq n-1$, we have

$$deg(gp), deg(gq) < m.$$

Therefore, if $p \neq q$, we have $gp \not\equiv gq$.

For encoding, we have

$$v = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_2^n \to p(x) = a_0 + \ldots + a_{n-1}x^{n-1} \xrightarrow{\phi} gp.$$

To decode, suppose we have

$$(b_0, \ldots, b_{m-1}) \leftrightarrow b(x) = b_0 + \ldots + b_{m-1}x^{m-1}.$$

We then do synthetic division by g, writing $b(x) = gp + r$. Here, no remainder is good, else, we keep p as the "decoded" part.

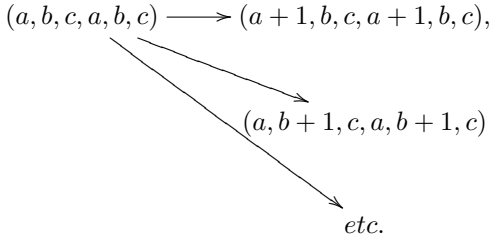
In addition, a great deal known is about detection and correction.

31 Day - 9/Nov/11

31.1 Binary: Errors and Probability

Assume that a bit changes $i \mapsto i+1$ with probability p. Then no change has probability $q = 1 - p$. Recall that, for independent events, we multipy the probabilities.

Example (Repetition on 3 Bits). Let $(a, b, c) \mapsto (a, b, c, a, b, c)$. Then, undetected errors may look like:



The probability for two undetected errors is $3p^2(1-p)^4$, for four undetected errors is $3p^4(1-p)^2$, and for six undetected errors is p^6. So, the probability of an undetected error is

$$3p^2(1-p)^4 + 3p^4(1-p)^2 + p^6.$$

Example (Parity on 3 Bits). Let $(a, b, c) \mapsto (a, b, c, a+b+c)$. Then, undetected errors happen when any two bits are switched. Hence, the probability of an undetected error is

$$\binom{4}{2} p^2(1-p)^2 + p^4.$$

When we compare with the previous example,

$$3p^2(1-p)^4 + 3p^4(1-p)^2 + p^6 < \binom{4}{2} p^2(1-p)^2 + p^4$$

whenever $p < \frac{1}{2}$.

31.2 Error Detecting/Correcting Code

Majority Rule Code. We encode as follows:

$$0 \mapsto 000, 1 \mapsto 111.$$

Suppose that there was one error; e.g.,

$$0 \mapsto 100, 010, or, 001.$$

Since the majority are still 0's, we decode as a 0.

Whenever two or three errors occur, the majority changes, and we have an "incorrectly corrected" vector. For example,

$$0 \mapsto 110, 101, 011$$

would decode as a 1.

The probability of uncorrected errors is $3p^2(1-p) + p^3$.

31.3 Quantum Error Detection/Correction

Note that we cannot clone, in general, but we can clone basis vectors. In addition, measurements destroy information and can also be used for decoding.

Examples (Analogue of Bit Switch, Majority Rule). Let

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

Recall that $Xe_0 = e_1, Xe_1 = e_0$. Observe the cases where

$$\psi_1 \otimes \ldots \otimes \psi_n, \psi_i \in \mathbb{C}^2.$$

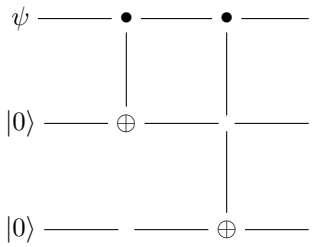
The only errors allowed are "qubit flips:" for one error, $X \otimes I \otimes \ldots \otimes I$, $I \otimes X \otimes I \otimes \ldots \otimes I$, ..., $I \otimes \ldots \otimes I \otimes X$; for two errors, we have two X's in the tensor product; for three errors, three X's in the tensor product; etc.

For a general qubit $\psi = a|0\rangle + b|1\rangle$, $X\psi = b|0\rangle + a|1\rangle$.

Three Qubit Bit Flip Code: We encode by

$$a|0\rangle + b|1\rangle \mapsto a|000\rangle + b|111\rangle,$$

which is an analogue of majority rule code. The diagram is as follows:



After we encode $a|0\rangle + b|1\rangle \to a|000\rangle + b|111\rangle$, possible errors are as follows:

$$\begin{array}{rc} & a|100\rangle + b|011\rangle \\ 1\,error: & a|010\rangle + b|101\rangle \\ & a|001\rangle + b|110\rangle \\ 2\,error: & etc. \\ 3\,error: & etc. \end{array}$$

Decoding is done in two steps:

1. **Error Detection/Syndrome Diagnosis** We create a measurement system:

$$\begin{array}{rcll} P_0 & = & |000\rangle\langle 000| + |111\rangle\langle 111| & No\,errors \\ P_1 & = & |100\rangle\langle 100| + |011\rangle\langle 011| & 1\,errors \\ P_2 & = & |010\rangle\langle 010| + |101\rangle\langle 101| & 2\,errors \\ P_3 & = & |001\rangle\langle 001| + |110\rangle\langle 110| & 3\,errors \end{array}$$

Note that

$$P_0^2 + P_1^2 + P_2^2 + P_3^2 + P_0 + P_1 + P_2 + P_3 = I_{\mathbb{C}^8}.$$

If $\psi = a|000\rangle + b|111\rangle$, then $\langle\psi|P_0\psi\rangle = 1$. After measurement, the new state becomes

$$\frac{P_0\psi}{||P_0\psi||} = \psi.$$

If $\psi_1 = a|100\rangle + b|011\rangle$, then $\langle\psi_1|P_0\psi_1\rangle = 0$ but $\langle\psi_1|P_1\psi_1\rangle = 1$. After measurement,

$$\frac{P_1\psi_1}{||P_1\psi_1||} = \psi_1.$$

Similarly, if the second or third error occurs, the vectors are left alone by P_2, P_3, respectively.

Now, what if two errors occurred, say $\psi \mapsto a|011\rangle + b|100\rangle = \gamma$? Then it will be detected by P_1, $P_1\gamma = \gamma$. So, when zero or one error occurs, the measurements show us where the error occurred.

2. Recovery Define $\mathcal{R} : M_2 \otimes M_2 \otimes M_2 \to M_2 \otimes M_2 \otimes M_2$ by

$$\begin{aligned}\mathcal{R}(Y) &= P_0YP_0 + (X \otimes 1 \otimes 1)P_1YP_1(X \otimes 1 \otimes 1) \\ &\quad +(1 \otimes X \otimes 1)P_2YP_2(1 \otimes X \otimes X) + (1 \otimes 1 \otimes X)P_3YP_3(1 \otimes 1 \otimes X).\end{aligned}$$

Note that

$$\mathcal{M}(Y) = P_0YP_0 + P_1YP_1 + P_2YP_2 + P_3YP_3$$

is a measurement map. Also, $\mathcal{R}$ is a completely positive map. Recall that $\Phi(Y) = \sum A_iYA_i^*$ is trace-preserving if and only if $\sum A_i^*A_i = I$. Since

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

and $X^2 = I$,

$$P_0P_0+P_1(X\otimes1\otimes1)(X\otimes1\otimes1)P_1+P_2(1\otimes X\otimes1)(1\otimes X\otimes1)P_2+P_3(1\otimes1\otimes X)(1\otimes1\otimes X)P_3$$

can be reduced to

$$P_0^2 + P_1^2 + P_2^2 + P_3^2 = I.$$

Therefore, $\mathcal{R}$ is completely positive and trace-preserving, and hence, is physically realizable.

Lastly, if Y is the outcome of $\psi = a|000\rangle + b|111\rangle$ after zero or one errors, then $R(Y) = |\psi\rangle\langle\psi|$. If ψ_i is the outcome witht he ith error, then

$$\mathcal{R}(|\psi_1\rangle\langle\psi_1|) = |\psi\rangle\langle\psi|,$$

for all $i = 1, 2, 3$. Therefore, $\mathcal{R}$ recovers ψ if no or one error occurred.

32 Day - 11/Nov/11

32.1 Three Qubit Bit Flip Code: Operator Viewpoint

Let $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ with probability p. If we do nothing to $\psi = a|0\rangle + b|1\rangle$, then

$$\begin{aligned}\psi &\xrightarrow[Ensemble]{Error} \{(1-p), \psi\}, \{pX\psi = a|0\rangle + a|1\rangle\} \\ &\xrightarrow[Matrix]{Density} (1-p)|\psi\rangle\langle\psi| + p|X\psi\rangle\langle X\psi|.\end{aligned}$$

The error map is

$$\mathcal{E}(|\psi\rangle\langle\psi|) = (1-p)|\psi\rangle\langle\psi| + p|X\psi\rangle\langle X\psi|,$$

and for a general Y, the error map is

$$\mathcal{E}(Y) = (1-p)Y + pXYX^*,$$

which is completely positive and trace-preserving.

If we do the three bit encoding,

$$a|0\rangle + b|1\rangle \rightarrow \psi \equiv a|000\rangle + b|111\rangle,$$

then,

$$\begin{aligned}\psi \quad \xrightarrow[Ensemble]{Errors} \quad & \{(1-p)^3, \psi\}, \{p(1-p)^2, (X\otimes I\otimes I)\psi\},\\ & \{p(1-p)^2, (I\otimes X\otimes I)\psi\}, \{p(1-p)^2, (I\otimes I\otimes X)\psi\},\\ & \{p^2(1-p), (I\otimes X\otimes X)\psi\}, \{p^2(1-p), (X\otimes I\otimes X)\psi\},\\ & \{p^2(1-p), (X\otimes X\otimes I)\psi\}, \{p^3, (X\otimes X\otimes X)\psi\}.\end{aligned}$$

The error map is

$$\begin{aligned}\mathcal{E}(Y) \quad = \quad & (1-p)^3 Y + p(1-p)^2 (X\otimes I\otimes I)Y(X\otimes I\otimes I)^*\\ & + p(1-p)^2 (I\otimes X\otimes I)Y(I\otimes X\otimes I)^* + \ldots\\ & + p^3 (X\otimes X\otimes X)Y(X\otimes X\otimes X)^*.\end{aligned}$$

We had the recovery/decoding mapping

$$\begin{aligned}\mathcal{R}(Y) \quad = \quad & P_0 Y P_0 + (X\otimes I\otimes I)P_1 Y P_1 (X\otimes I\otimes I)\\ & (I\otimes X\otimes I)P_2 Y P_2 (I\otimes X\otimes I) + (I\otimes I\otimes X)P_3 Y P_3 (I\otimes I\otimes X).\end{aligned}$$

So the errors followed by the recovery, for ψ, obey

$$\begin{aligned}\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|) \quad = \quad & ((1-p)^3 + 3p(1-p)^2)|\psi\rangle\langle\psi|\\ & + (3p^2(1-p) + p^3 + p^3)(X\otimes X\otimes X)(|\psi\rangle\langle\psi|)(X\otimes X\otimes X),\end{aligned}$$

and for a general Y,

$$\begin{aligned}\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|) \quad = \quad & ((1-p)^3 + 3p(1-p)^2)Y\\ & + (3p^2(1-p) + p^3 + p^3)(X\otimes X\otimes X)Y(X\otimes X\otimes X).\end{aligned}$$

In summary, if we do nothing,

$$|\psi\rangle\langle\psi| \rightarrow (1-p)|\psi\rangle\langle\psi| + p|X\psi\rangle\langle X\psi|,$$

and if we use code recovery,

$$|\tilde{\psi}\rangle\langle\tilde{\psi}| \rightarrow ((1-p)^3 + 3p(1-p)^2)|\tilde{\psi}\rangle\langle\tilde{\psi}| + (3p^2(1-p) + p^3)|(X\otimes X\otimes X)\tilde{\psi}\rangle\langle(X\otimes X\otimes X)\tilde{\psi}|,$$

where $\psi = a|0\rangle + b|1\rangle$ and $\tilde{\psi} = a|000\rangle + b|111\rangle$. The code recovery "looks better" because $(1-p)^3 + 3p(1-p)^2$ "looks bigger" than $(1-p)$. In addition, the code recovery is "better" when $(1-p)^3 + 3p(1-p)^2 \geq (1-p)$ if and only if $(1-p)^2 + 3p(1-p) \geq 1$ if and only if $p \leq 1/2$.

A better measurement of how well a code behavior is *fidelity*.

32.2 Introduce and Motivate Fidelity

Recall that a state is equal to some unit vector.

Start with a state ψ, perturbed to $\psi' = a\psi + b\psi_\perp$. How close a is to 1 measures how "little" ψ' is perturbed. Since $e^{i\theta}\psi, \psi$ are the same state, so we only need $|a| = |\langle\psi'|\psi\rangle|$. So, *fidelity* for states is defined $F \equiv |\langle\psi'|\psi\rangle|$.

For density matrices $\psi \mapsto |\psi\rangle\langle\psi| = p$, $\psi' \mapsto |\psi'\rangle\langle\psi'| = p'$,

$$\begin{aligned}\langle p|p'\rangle &= Tr(pp') \\ &= Tr(|\psi\rangle\langle\psi||\psi'\rangle\langle\psi'|) \\ &= Tr(\langle\psi|\psi'\rangle\langle\psi'|\psi\rangle) \\ &= |\langle\psi'|\psi\rangle|^2.\end{aligned}$$

So, fidelity is defined $F \equiv \sqrt{Tr(pp')}$.

The measure used for comparing error correction is fidelity:

$$F = \sqrt{Tr(|\psi\rangle\langle\psi|\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|))} = \sqrt{\langle\psi|\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle|psi|)\psi\rangle}.$$

Then we are interested in either

$$min_\psi(\sqrt{\langle\psi|\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|)\psi\rangle})$$

or some type of average fidelity, say

$$\int_{sphere in \mathbb{C}^2} \langle\psi|(\mathcal{R}\circ\mathcal{E}(|\psi\rangle\langle\psi|))\psi\rangle ds(\psi).$$

Example. We compare the minimum fidelities for "do nothing" and "three-qubit error/recovery code." For the "do nothing"

$$|\psi\rangle\langle\psi| \to \mathcal{E}(|\psi\rangle\langle\psi|) = (1-p)|\psi\rangle\langle\psi| + p|X\psi\rangle\langle X\psi|,$$

the fidelity is

$$\begin{aligned}F &= \sqrt{\langle\psi|[(1-p)|\psi\rangle\langle+p|X\psi\rangle\langle X\psi|]\psi\rangle} \\ &= \sqrt{(1-p)\langle\psi|\psi\rangle + p\langle X\psi|\psi\rangle\langle\psi|X\psi\rangle} \\ &= \sqrt{(1-p) + p|\langle X\psi|\psi\rangle|^2}.\end{aligned}$$

Since $X|0\rangle\perp|0\rangle$, $minF = \sqrt{1-p}$.

For the "recovery"

$$\begin{aligned}|\tilde{\psi}\rangle\langle\tilde{\psi}| &\to \mathcal{R}\circ\mathcal{E}(|\tilde{\psi}\rangle\langle\tilde{\psi}|) \\ &= ((1-p)^3 + 3p(1-p)^2)|\tilde{\psi}\rangle\langle\tilde{\psi}| + (3p^2(1-p)+p^3)|(X\otimes X\otimes X)\tilde{\psi}\rangle\langle(X\otimes X\otimes X)\tilde{\psi}|,\end{aligned}$$

the fidelity is

$$\begin{aligned}F &= \sqrt{\langle\tilde{\psi}|\mathcal{R}\circ\mathcal{E}(|\tilde{\psi}\rangle\langle\tilde{\psi}|)\tilde{\psi}\rangle} \\ &= [((1-p)^3 + 3p(1-p)^2)\langle\tilde{\psi}|\tilde{\psi}\rangle^2 + (3p^2(1-p)+p^3)|\langle\tilde{\psi}|(X\otimes X\otimes X)\tilde{\psi}\rangle|^2]^{1/2}.\end{aligned}$$

Pick $\tilde{\psi} = |000\rangle$. Then $(X\otimes X\otimes X)\tilde{\psi} = |111\rangle\perp\tilde{\psi}$. So,

$$minF = \sqrt{(1-p)^3 + 3p(1-p)^2}.$$

33 Day - 14/Nov/11

33.1 Three Qubit Phase Flip Code

Let $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Then $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$. Set

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Note that

(1) $|+\rangle \perp |-\rangle$.

(2) $Z|+\rangle = |-\rangle$, $Z|-\rangle = |+\rangle$.

So, this is completely analogous to the bit flip $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

We encode by

$$|0\rangle \to |++\!+\rangle = |+\rangle \otimes |+\rangle \otimes |+\rangle,$$
$$|1\rangle \to |--\!-\rangle.$$

This behaves exactly like the bit flip code, only now for detecting/correcting phase flips.

We similarly define for $Y = \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right)$. Set $|+\rangle$ as above. Then

$$Y|+\rangle = \frac{i|0\rangle - i|1\rangle}{\sqrt{2}} = i\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \beta.$$

Observe that $|+\rangle \perp \beta$, $Y|+\rangle = \beta$, and $Y\beta = |+\rangle$. We encode as

$$|0\rangle \to |++\!+\rangle,$$
$$|1\rangle \to |\beta\beta\beta\rangle = \beta \otimes \beta \otimes \beta.$$

33.2 The Shor Code

The encoding is as follows:

$$|0\rangle \to |0_L\rangle = \frac{(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)}{2\sqrt{2}} \in \mathbb{C}^{2^9},$$
$$|0\rangle \to |1_L\rangle = \frac{(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)}{2\sqrt{2}} \in \mathbb{C}^{2^9}.$$

Theorem (Shor). There exists a completely positive and trace-preserving map $\mathcal{R} : M_{2^9} \to M_{2^9}$ such that, for all 2×2 unitaries U, for all i,

$$\tilde{U} = I \otimes \ldots \otimes I \otimes U \otimes I \otimes \ldots \otimes I,$$

and for all $\psi = a|0_l\rangle + b|1_L\rangle$, we have

$$\mathcal{R}(\tilde{U}|\psi\rangle\langle\psi|\tilde{U}^*) = |\psi\rangle\langle\psi|.$$

In other words, the recovery operation $\mathcal{R}$ corrects all single errors, but for arbitrary $U \in M_2$.

Proposition. Let $\mathcal{V} \subseteq \mathbb{C}^n$ be a subspace and let $\{U_1, \ldots, U_t\} \subseteq M_n$ be unitaries. If $U_i\mathcal{V} \perp U_j\mathcal{V}$ for all $i \neq j$, then there exists a completely positive and trace-preserving $\mathcal{R} : M_n \to M_n$ such that

$$\mathcal{R}(U_i|\psi\rangle\langle\psi|U_i^*) = |\psi\rangle\langle\psi|$$

for all $\psi \in \mathcal{V}$, for all i.

Proof. Let P_i be the orthogonal projection onto $U_i\mathcal{V}$. Let

$$P_0 = I - P_1 - \ldots - P_t.$$

These will be teh syndrome. Set $U_0 = I$. Define

$$\mathcal{R}(X) = \sum_{i=0}^{t} U_i^* P_i X P_i U_i.$$

We know that $\mathcal{R}$ is completely positive. Since

$$\sum_{i=0}^{t} (P_i U_i)(U_i^* P_i) = \sum_{i=0}^{t} P_i^2 = \sum_{i=0}^{t} P_i = I,$$

we have that $\mathcal{R}$ is trace-preserving.

For $\psi \in \mathcal{V}$,

$$P_i(|U_j\psi\rangle\langle U_j\psi|)P_i = \begin{cases} 0, & i \neq j, \\ |U_j\psi\rangle\langle U_j\psi|, & i = j. \end{cases}$$

Now,

$$|U_j\psi\rangle\langle U_j\psi| = U_j(|\psi\rangle\langle\psi|)U_j^*.$$

Therefore,

$$\begin{aligned} \mathcal{R}(|U_j\psi\rangle\langle U_j\psi|) &= U_j^* P_j(|U_j\psi\rangle\langle U_j\psi|)P_j U_j \\ &= |\psi\rangle\langle\psi|. \end{aligned}$$

$\boxtimes$

Recall the Pauli matrices I, X, Y, Z as above. A tensor of the form

$$I \otimes \ldots \otimes I \otimes U \otimes I \otimes \ldots \otimes I,$$

where U is a Pauli matrix, is called a *1-Pauli*. The set of all 1-Pauli in $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ (nine copies) is a finite set of unitaries. In fact, $3^9 + 1$.

Proposition. Let $\mathcal{V} = span\{|0_L\rangle, |1_L\rangle\} \subseteq \mathbb{C}^{2^9}$. Let U, V be 1-Pauli such that $U \neq V$. Then $U\mathcal{V} \perp V\mathcal{V}$.

Proof (Sketch). We check a few to convince us of the proof. First off, suppose U, V occur in the ith, jth tensor, $i \neq j$, involving one of X, Y, Z. For example,

$$U = X \otimes I \otimes \ldots \otimes I, V = I \otimes X \otimes I \otimes \ldots \otimes I.$$

Then,

$$\begin{aligned} U|0_L\rangle &= (|100\rangle + |011\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ U|1_L\rangle &= (|100\rangle - |011\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle), \\ V|0_L\rangle &= (|010\rangle + |101\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ V|1_L\rangle &= (|010\rangle - |101\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \end{aligned}$$

All of these are perpendicular. It is pretty easy to see that when U, V occur in the ith,jth tensor with $i \neq j$, then $U\mathcal{V} \perp V\mathcal{V}$. The harder case to see is why, say

$$U = (X \otimes I \otimes \ldots \otimes I)\mathcal{V} \perp V = (Z \otimes I \otimes \ldots \otimes I)\mathcal{V}.$$

We saw what $U|0_L\rangle, U|1_L\rangle$ are. Since,

$$\begin{aligned} V|0_L\rangle &= (|100\rangle - |011\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ V|1_L\rangle &= (|000\rangle + |111\rangle)(|100\rangle - |011\rangle)(|100\rangle - |011\rangle), \end{aligned}$$

they are perpendicular.

⊠

33.3 "Pauli Magic"

Proposition. I, X, Y, Z are orthogonal in M_2 and all have 2-norm $\sqrt{2}$.

Proof. We need to compute $\langle U, V\rangle = Tr(U^*V) = Tr(UV)$, for Pauli U, V. Obviously, $I \perp X$, $I \perp Y$. Since $\langle I, Z\rangle = 1^2 - 1^2 = 0$, $I \perp Z$. Again, we clearly see $X \perp Z$, $Y \perp Z$. Lastly, $\langle X, Y\rangle = i - i = 0$. Hence, $X \perp Y$.

They all have norm $\sqrt{2}$.

⊠

Proposition. If $U \in M_2$ unitary and $U = a_0 I + a_1 X + a_2 Y + a_3 Z$, then

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1.$$

34 Day - 16/Nov/11

34.1 Fixes from Last Time

Set $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right)$, and $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Now define

$$\begin{aligned} X_1 = X \otimes I \otimes \ldots \otimes I, \ldots, X_9 = I \otimes \ldots I \otimes X, \\ Y_1 = Y \otimes I \otimes \ldots \otimes I, \ldots, Y_9 = I \otimes \ldots I \otimes Y, \\ Z_1 = Z \otimes I \otimes \ldots \otimes I, \ldots, Z_9 = I \otimes \ldots I \otimes Z. \end{aligned}$$

So, there are $3 \cdot 9 + 1$ tensors.

Let $\mathcal{V} = span\{|0_L\rangle, |1_L\rangle\}$, where

$$|0_L\rangle = \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}},$$
$$|1_L\rangle = \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}.$$

Proposition. (1) $\mathcal{V}$, $X_1\mathcal{V}, \ldots, X_9\mathcal{V}$, $Y_1\mathcal{V}, \ldots, Y_9\mathcal{V}$, $Z_1\mathcal{V}$, $Z_4\mathcal{V}$, $Z_7\mathcal{V}$ are orthogonal subspaces.

(2) For $v \in \mathcal{V}$,

$$Z_1 v = Z_2 v = Z_3,$$
$$Z_4 v = Z_5 v = Z_6,$$
$$Z_7 v = Z_8 v = Z_9.$$

Proof (Sketch). (1) This involves a lot of checking and we did a few cases last time.

(2) This involves a lot of checking. For example,

$$\begin{aligned} Z_1|0_L\rangle &= (|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ &= |0_9\rangle + |0_6 1_3\rangle + |0_3 1_3 0_3\rangle + |0_3 1_6\rangle \\ &\quad -|1_3 0_6\rangle - |1_3 0_3 1_3\rangle - |1_6 0_3\rangle - |1_9\rangle \\ &= Z_2|0_L\rangle \\ &= Z_3|0_L\rangle \end{aligned}$$

and

$$\begin{aligned} Z_1|1_L\rangle &= (|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \\ &= Z_2|1_L\rangle \\ &= Z_3|1_L\rangle. \end{aligned}$$

Compare this to

$$\begin{aligned} Z_4|0_L\rangle &= (|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle) \\ &= |0_9\rangle + |0_6 1_3\rangle - |0_3 1_3 0_3\rangle - |0_3 1_6\rangle \\ &\quad +|1_3 0_6\rangle + |1_3 0_3 1_3\rangle - |1_6 0_3\rangle - |1_9\rangle. \end{aligned}$$

In addition, $\langle Z_1|0_L\rangle | Z_4|0_L\rangle\rangle = 0$.

$\boxtimes$

34.2 Continuation from Last Time

Let

$$P_0, P_1^X, \ldots, P_9^X, P_1^Y, \ldots, P_9^Y, P_1^Z, P_4^Z, P_7^X,$$

be the projection onto these subspaces of $\mathbb{C}^{2^9}$ and

$$Q = I - \text{ sum of the projections.}$$

Define

$$\begin{aligned}\mathcal{R}(W) &= P_0(W)P_0 + X_1^* P_1^X W P_1^X X_1 + \ldots + X_9^* P_9^X W P_9^X X_9 \\ &\quad + Y_1^* P_1^Y(W) P_1^Y Y_1 + \ldots + Y_9^* P_9^Y(W) P_9^Y Y_9 \\ &\quad + Z_1^* P_1^Z(W) P_1^Z Z_1 + Z_4^* P_4^Z(W) P_4^Z Z_4 + Z_7^* P_7^Z(W) P_7^Z Z_7 + QWQ.\end{aligned}$$

Then, $\mathcal{R}$ is completely positive and trace-preserving, and if $\psi \in \mathcal{V}$ and is changed by any 1-Pauli U to $U\psi$, then

$$\mathcal{R}(|U\psi\rangle\langle U\psi|) = \mathcal{R}(U(|\psi\rangle\langle\psi|)U^*) = |\psi\rangle\langle\psi|.$$

Recall the following propositions:

(i) **Proposition**. I, X, Y, Z are orthogonal in the Hilbert space M_2 and they all have 2-norm $\sqrt{2}$.

Proposition. If $U \in M_2$ is unitary and we write

$$U = a_0 I + a_1 X + a_2 Y + a_3 Z,$$

then

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1.$$

Proof. Observe that

$$U = (\sqrt{2}a_0)\frac{I}{\sqrt{2}} + (\sqrt{2}a_1)\frac{X}{\sqrt{2}} + (\sqrt{2}a_2)\frac{Y}{\sqrt{2}} + (\sqrt{2}a_3)\frac{Z}{\sqrt{2}}$$

is an expression of U with respect to an orthonormal basis. Therefore,

$$2 = ||U||_2^2 = 2|a_0|^2 + 2|a_1|^2 + 2|a_2|^2 + 2|a_3|^2.$$

$\boxtimes$

Theorem. Let $\psi \in \mathcal{V}$ and $U \in M_2$ be unitary. Let

$$U_j = I \otimes \ldots \otimes I \otimes U \otimes I \otimes \ldots \otimes I \in M_{2^9} \ (jth\, tensor).$$

Then,

$$\mathcal{R}(|U_j\psi\rangle\langle U_j\psi|) = |\psi\rangle\langle\psi|.$$

Proof. Write

$$U = a_0 I + a_1 X + a_2 Y + a_3 Z.$$

This implies

$$U_j = a_0 I + a_1 X_j + a_2 Y_j + a_3 Z_j.$$

Therefore,

$$\begin{aligned}|U_j\psi\rangle\langle U_j\psi| &= U_j(|\psi\rangle\langle\psi|)U_j^* \\ &= a_0\overline{a}_0|\psi\rangle\langle\psi| + a_0\overline{a}_1|\psi\rangle\langle\psi X_j \\ &\quad + \ldots + a_3\overline{a}_3 Z_j|\psi\rangle\langle\psi|Z_j.\end{aligned}$$

So

$$\mathcal{R}(U_j|\psi\rangle\langle\psi|U_j^*) = \text{sum of these 16 terms.}$$

However, for example, $|\psi\rangle\langle\psi|X_j = |\psi\rangle\langle X_j\psi|$. When we do a projection to this, they all annihilate it, even Q. The only terms not annihilated are the "diagonal terms:"

$$|a_0|^2|\psi\rangle\langle\psi|, |a_1|^2|X_j\psi\rangle\langle X_j\psi|, |a_2|^2|Y_j\psi\rangle\langle Y_j\psi|, |a_3|^2|Z_j\psi\rangle\langle Z_j\psi|.$$

Note that

$$\begin{gathered}\mathcal{R}(|a_0|^2|\psi\rangle\langle\psi|) = |a_0|^2|\psi\rangle\langle\psi|,\\ \mathcal{R}(|a_1|^2|X_j\psi\rangle\langle X_j\psi|) = |a_1|^2|\psi\rangle\langle\psi|,\\ \mathcal{R}(|a_2|^2|Y_j\psi\rangle\langle Y_j\psi|) = |a_2|^2|\psi\rangle\langle\psi|,\\ \mathcal{R}(|a_3|^2|Z_j\psi\rangle\langle Z_j\psi|) = |a_3|^2|\psi\rangle\langle\psi|.\end{gathered}$$

So,

$$\mathcal{R}(Sum) = (|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2)|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|.$$

⊠

35 Day - 18/Nov/11

35.1 Continuation

Proposition. For $\mathcal{V} \subseteq \mathbb{C}^n$, let $\mathcal{E} : M_n \to M_n$ be the error map and $\mathcal{R} : M_n \to M_n$ be the recovery map, which are completely positive, trace-preserving. Then,

$$\mathcal{R} \circ \mathbb{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$$

for all $\psi \in \mathcal{V}$ if and only if $\mathcal{R} \circ \mathcal{E}(PXP) = PXP$ for all $X \in M_n$, where $P : \mathbb{C}^n \to \mathcal{V}$.

Theorem 1. Let $\mathcal{V} \subseteq \mathbb{C}^n$ and $\mathcal{E} : M_n \to M_n$, $\mathcal{E}(X) = \sum_{i=1}^r E_i X E_i^*$, be a completely positive and trace-preserving map. Then there exists a completely positive and trace-preserving map $\mathcal{R} : M_n \to M_n$ such that $\mathcal{R}\mathcal{E}(PXP) = PXP$ for all $X \in M_n$ if and only if there exists $\alpha_{ij} \in \mathbb{C}$ such that $PE_i^* E_j P = \alpha_{ij} P$.

Theorem 2. Let $\mathcal{E}, \mathcal{R}$ be as in *Theorem 1.* Let $G_i \in span\{E_j\}_{j=1}^r$ such that $\sum_{i=1}^t G_i^* G_i = I$. Let $\mathcal{G}(X) = \sum_{i=1}^t G_i X G_i^*$. Then,

$$\mathcal{R} \circ \mathcal{G}(PXP) = PXP,$$

for all X.

Proof of Proposition. ($\Leftarrow$): Let $\psi \in \mathcal{V}$ with $P\psi = \psi$. Then $P(|\psi\rangle\langle\psi|)P = |\psi\rangle\langle\psi|$. Therefore,

$$\mathcal{R} \circ \mathcal{E}(|\psi\rangle\langle\psi|) = \mathcal{R} \circ \mathcal{E}(P|\psi\rangle\langle\psi|P) = P|\psi\rangle\langle\psi|P = |\psi\rangle\langle\psi|.$$

($\Rightarrow$): If $X \geq 0$, then $PXP \geq 0$, $(PXP)\mathcal{V} \subseteq \mathcal{V}$, and $(PXP)\mathcal{V}^{\perp} = 0$. So, non-zero eigenvectors of PXP are all in $\mathcal{V}$. This implies $PXP = \sum |\psi_l\rangle\langle\psi_l|$, for $\psi_l \in \mathcal{V}$. Therefore,

$$\begin{aligned} \mathcal{R} \circ \mathcal{E}(PXP) &= \mathcal{R} \circ \mathcal{E}(\sum |\psi_l\rangle\langle\psi_l|) \\ &= \sum |\psi_l\rangle\langle\psi_l| \\ &= PXP. \end{aligned}$$

Given any $X \in M_n$, write

$$X = (P_1 - P_2) + i(P_3 - P_4).$$

Then,

$$\begin{aligned} \mathcal{R} \circ \mathcal{E}(PXP) &= \mathcal{R} \circ \mathcal{E}(PP_1P - PP_2P + iPP_3P - iPP_4P) \\ &= PP_1P - PP_2P + iPP_3P - iPP_4P \\ &= PXP. \end{aligned}$$

$\boxtimes$

Proof of Theorem 1. ($\Rightarrow$): Let $\mathcal{R}(W) = \sum A_l W A_l^*$ and $\sum A_l^* A_l = I$. Then,

$$\begin{aligned} \mathcal{R} \circ \mathcal{E}(PXP) &= \sum_{l,i} A_l E_i PX(PE_i^* A_l^*) \\ &= \sum_{l,i} (A_l E_i P) X (A_l E_i P)^* \\ &= PXP. \end{aligned}$$

So, we have two ways to write the map $X \to PXP$. Note that the right-hand side is clearly minimal Choi rank.

By *Choi's theorem*, there exists $\beta_{il} \in \mathbb{C}$ so that $A_l E_i P = \beta_{il} P$, which we note is a row vector. This implies $\sum |\beta_{il}|^2 = 1$, meaning the same matrix was an "isometry." Hence,

$$(PE_i^* A_l^*)(A_l E_j P) = (\overline{\beta}_{il} P)(\beta_{jl} P) = \overline{\beta}_{il}\beta_{jl} P,$$

$$\sum_l PE_i^*(A_l^* A_l) E_j P = PE_i^* E_j P.$$

Therefore,

$$PE_i^* E_j P = (\sum_l \overline{\beta}_{il}\beta_{jl}) P = \alpha_{ij} P.$$

($\Leftarrow$): Note that

$$(\alpha_{ij} P) = (PE_i^* E_j P) = \begin{pmatrix} PE_1^* \\ \vdots \\ PE_r^* \end{pmatrix} (E_1 P, \ldots, E_r P) \geq 0.$$

This implies $(\alpha_{ij}) \geq 0$. Also,

$$\sum \alpha_{ii} P = \sum_i P E_i^* E_i P = P,$$

implying $\sum \alpha_{ii} = 1$. So, $Tr((\alpha_{ij})) = 1$; i.e., (α_{ij}) is a density matrix. We diagonalize by picking a unitary $U = (u_{ij})$ such that

$$U(\alpha_{ij})U^* = D = (d_{ij}),$$

where D is diagonal, $d_{ii} \geq 0$, and $\sum d_{ii} = 1$. Let

$$F_i = \sum_{k=1}^{r} \overline{u}_{ik} E_k, 1 \leq i \leq r.$$

By *Choi's theorem*, $\sum_{i=1}^{r} F_i X F_i^* = \mathcal{E}(X)$. Also,

$$\begin{aligned} PF_i^* F_j P &= P((\sum_k u_{ik} E_k)(\sum_l \overline{u}_{jl} E_l))P \\ &= \sum_{k,l} u_{ik} \overline{u}_{jl} P E_k^* E_l P \\ &= (\sum_{k,l} u_{ik} \alpha_{kl} \overline{u}_{jl}) P \\ &= d_{ij} P. \end{aligned}$$

Therefore,

$$PF_i^* F_j P = \begin{cases} 0, & i \neq j, \\ d_{ii} P, & i = j. \end{cases}$$

When $i \neq j$, and for $\psi_1, \psi_2 \in \mathcal{V}$, we have

$$\langle F_i P \psi_1 | F_j P \psi_2 \rangle = \langle \psi_1 | P F_i^* F_j P \psi_2 \rangle = 0,$$

which implies

$$\langle F_i \psi_1 | F_j \psi_2 \rangle = 0.$$

Therefore, $F_i \mathcal{V} \perp F_j \mathcal{V}$.

Now, when $d_{ii} = 0$, $PF_i^* F_i P = 0$, which implies $F_i \mathcal{V} = (0)$. When $d_{ii} \neq 0$,

$$\frac{1}{d_{ii}} P F_i^* F_i P = P,$$

and for $\psi_1, \psi_2 \in \mathcal{V}$, we have

$$\begin{aligned} \frac{1}{d_{ii}} \langle F_i P \psi_2 | F_i P \psi_1 \rangle &= \frac{1}{d_{ii}} \langle \psi_2 | P F_i^* F_i P \psi_1 \rangle \\ &= \langle \psi_2 | \psi_1 \rangle. \end{aligned}$$

Therefore,

$$\frac{1}{\sqrt{d_{ii}}} F_i P : \mathcal{V} \to \mathcal{V}_i$$

is an isometry.

Let $R_i = \frac{1}{\sqrt{d_{ii}}} P F_i^*$ when $d_{ii} \neq 0$, and $R_i = 0$ otherwise. Then

$$R = \sum R_i^* R_i = \sum \frac{1}{d_{ii}} F_i P F_i^*$$

and

$$\begin{aligned} R^2 &= \sum_{i,j} \frac{1}{d_{ii}} \frac{1}{d_{jj}} (F_i P F_i^*)(F_j P F_j^*) \\ &= \sum_i \frac{1}{d_{ii}^2} F_i (d_{ii} P) F_i^* \\ &= R. \end{aligned}$$

Hence, R is a projection. Let $Q = I - R$. Define

$$\mathcal{R}(X) = \sum_i R_i X R_i^* + QXQ.$$

This is completely positive and trace-preserving since

$$\sum R_i^* R_i + Q^* Q = R + Q = I.$$