1. Quantum states

1. Let $M_{m,n}$ be the set of $m \times n$ complex matrices, and let $M_n = M_{n,n}$.
2. Quantum states are density matrices, i.e., positive semidefinite matrices with trace 1.
3. Let D_n be the set of density matrices in M_n.
4. Pure states are rank one quantum states, i.e., rank one orthogonal projections.
5. For quantum states A and B in M_n and M_m their tensor state is
$$A \otimes B = (a_{ij}B) \in M_n \otimes M_m \equiv M_n(M_m) \equiv M_{mn}$$
in the bipartite system.
6. General quantum states in $M_n \otimes M_m$ are density matrices in M_{mn}.
7. Every $C \in M_n \otimes M_m$ is a linear combination of tensor states, i.e., $C = \sum_{j=1}^{N} \mu_j A_j \otimes B_j$.
8. A state $C \in D_{mn}$ is separable if it is a convex combination of tensor states, i.e., there are $p_1, \dots, p_r > 0$ with $\sum_{j=1}^{r} p_j = 1$ such that $C = \sum_{j=1}^{r} p_r A_r \otimes B_r$ with $A_r \in D_n, B_r \in D_m$. Otherwise, it is entangled.
9. It is easy to check whether $C = (C_{ij}) \in M_n(M_m)$ is a tensor state, namely, just check whether all the blocks C_{ij} are multiple of a density matrix B. If yes, write $C = A \otimes B$ and check whether A is a density matrix.
10. Important/difficult question. How to determine a state $C \in M_n \otimes M_m$ is separable/entangled.
11. Linear programming, positive semi-definite programming, etc. It is an NP-hard problem.
12. How about states with special structure?

2. Quantum operations

1. Mathematically, a quantum channel or a quantum operation is a trace preserving completely positive linear map $\Phi : M_n \to M_k$ admitting the following representation

$$\Phi(X) = \sum_{j=1}^{r} F_r X F_r^*$$

for some $F_1, \ldots, F_r \in M_{k,n}$ satisfying $\sum_{j=1}^r F_j^* F_j = I_n$.

2. A linear map Φ is a quantum channel if and only if

$$(P_{ij}) = (\Phi(E_{ij})) \in M_n(M_k)$$

is positive semidefinite with $\mathrm{tr}\,(P_{jj}) = 1$ for all j and $\mathrm{tr}\,(P_{ij}) = 0$ for all $i \neq j$, where $\{E_{11}, E_{12}, \ldots, E_{nn}\}$ is the standard basis for M_n.

3. The operator system corresponds to Φ is the linear span of

$$\{F_i^* F_j : 1 \leq i, j \leq r\} \subset M_n.$$

4. In general, an operator system $\mathcal{S}$ in M_n is a subspace containing I and self-adjoint, i.e., satisfies $A \in \mathcal{S}$ if and only if $\mathcal{S}$.

Proposition Every operator system in $\mathcal{S}$ is M_n can be viewed as the operator system of a quantum operation.

Proof. Let $\mathcal{S} \in M_n$ have a basis $\{I, A_1, \ldots, A_m\}$ with $A_j = A_j^*$ for $j = 1, \ldots, m$. Construct $Q = (Q_{ij}) \in M_{m+1}(M_n)$ such that $Q_{r,s} = A_j$ whenever $|r - s| = 1$, and all other blocks equal to zero. Then there is $r > 0$ such that $\tilde{Q} = \frac{1}{r(m+1)}(rI + Q)$ is positive semidefinite. So, $\tilde{Q} = F^*F = [F_1|\cdots|F_{m+1}]^*[F_1|\cdots|F_{m+1}]$, where $F_j \in M_{n,k}$, where n is the rank of $\tilde{Q}$. It follows that $\mathcal{S}$ is the operator system corresponding to $\Phi : M_n \to M_k$ defined by $\Phi(X) = \sum_{j=1}^{m+1} F_j X F_j^*$. $\square$

Remark Professor Y.T. Poon (Iowa State University) pointed out that one may set $k = [m/2]$ and $Q = (Q_{ij}) \in M_\ell(M_n)$ with $Q_{r,r+1} = A_{2r-1} + iA_{2r}$ for $r = 1, \ldots, [m/2]$, and for sufficiently large r (1) $Q_{rr} = rI$ if $m = 2\ell$, (2) $Q_{11} = rI + A_{m,m}, Q_\ell = rI - A_{m,m}$, and $Q_{rr} = rI$ for other r. Then we can do the factorization of $\tilde{Q}$ to get the desired result.

Question Let $\mathcal{S} = \text{span}\{I, A_1, \dots, A_k\} \subseteq M_n$ be an operator system.

- Find the smallest k such that $\mathcal{S}$ is the operator system of a quantum channel $\Phi : M_n \to M_k$.
- Find the maximum number r for the existence of an $n \times r$ matrix X such that X^*AX is a diagonal matrix for all $A \in \{I, A_1, \dots, A_m\}$.

  The maximum value r is the capacity of the channel/operator system.
- Find the maximum number r for the existence of a $n \times r$ matrix X such that X^*AX is a scalar matrix for all $A \in \{I, A_1, \dots, A_m\}$.

  The maximum r is the maximum dimension of an error correction code of the channel.

Some Partial Results

Question Find the minimum k for the existence of a quantum operation $\Phi : M_n \to M_k$ defined by $\Phi(A) = \sum_{j=1}^r F_j A F_j^*$ with $\sum_{j=1}^r F_j^* F_j = I_n$ satisfying $\text{span}\{F_i^* F_j : 1 \le i, j \le r\} = \mathcal{S}$ for a given operator system $\mathcal{S}$ in M_n.

Here is a useful lemma.

Lemma Let $\mathcal{S}$ be an operator system be spanned by a basis $\{A_0, \dots, A_m\} \in M_n$. Then $F_1, \dots, F_r \in M_{k,n}$ satisfy $\sum_{j=1}^r F_j^* F_j$ and $\mathcal{S} = \text{span}\{F_i^* F_j : 1 \le i, j \le r\}$ if and only if for any unitary $U \in M_n, V \in M_k$ the matrices $\hat{F}_j = U F_j V$ for $j = 1, \dots, j$ satisfy $\sum_{j=1}^r \hat{F}_j^* \hat{F}_j$ and $\text{span}\{\hat{F}_i^* \hat{F}_j : 1 \le i, j \le r\} = V^* \mathcal{S} V = \text{span}\{V^* A_j V : 0 \le j \le m\}$.

Theorem Suppose $\mathcal{S}$ is commutative, i.e., $XY = YX$ for all $X, Y \in \mathcal{S}$. Then $k = n$.

Proof. Suppose $\mathcal{S} = \text{span}\{I_n, A_1, \dots, A_m\}$. We may assume that $A_1, \dots, A_m$ are diagonal matrices. Then for a sufficiently large $\mu > 0$ such that $\mu I \ge A_j$ for all $j = 1, \dots, m$. We may let $F_j = \sqrt{\mu I - A_j}$ for $j = 1, \dots, m$. Now, let $\nu > 0$ be (sufficiently large) such that $D_0 = \nu I - \sum_{j=1}^m F_j^2 \ge 0$. Then for $F_0 = \sqrt{D_0}$ one readily checks that the linear map $\Phi : M_n \to M_n$ defined by

$$\Phi(A) = \frac{1}{\nu} \sum_{j=0}^m F_j A F_j^*$$

satisfies $\mathcal{S}(\Phi) = \mathcal{S}$.

Now, suppose $k < n$, and $\Phi : M_n \to M_r$ defined by $\Phi(A) = \sum_{j=1}^r F_j A F_j^*$ satisfies $\mathcal{S}(\Phi) = \mathcal{S}$, and hence $F_i^* F_j$ are diagonal matrices. Then there is a unitary $U \in M_n$ such that such that $U_1 F_1 \in \text{span}\{E_{11}, \dots, E_{kk}\} \subseteq M_{n,k}$. We may replace F_j by $U_1 F_j$ for all $j = 1, \dots, r$. Now, $F_2^* F_1$ is a diagonal matrix, we can adjust U_1 to get a unitary U_2 such that $U_2 F_1, U_2 F_2 \in \text{span}\{E_{11}, \dots, E_{kk}\}$. Next, $F_3^* F_1, F_3^* F_2$ are diagonal matrices, we can further adjust U_2 to get a unitary U_3 such that $U_3 F_1, U_3 F_2, U_3 F_3 \in \text{span}\{E_{11}, \dots, E_{kk}\}$. Repeat this argument until we get a unitary $U_r \in M_n$ such that $\{U_r F_1, \dots, U_r F_r\} \subseteq \text{span}\{E_{11}, \dots, E_{kk}\}$. But then $I_n \notin \mathcal{S}$, which is a contradiction. $\square$

Note that if $\mathcal{S} = \{I\}$, then we can use the $\Phi(I) = I$. If $\mathcal{S} \in M_n$ is commutative with dimension n, then $\mathcal{S} = \operatorname{span}\{F_1, \ldots, F_n\} \subseteq M_n$ with $F_1 = u_1u_1^*, \ldots, F_n = u_nu_n^*$ for an orthonormal basis $\{u_1, \ldots, u_n\}$, and we can use $\Phi(A) = \sum_{j=1}^n F_jAF_j^*$.

Proposition Suppose $\mathcal{S} = M_n$. Then we can let $k = 1$ and set $\Phi(A) = \sum_{j=1}^n e_j^tAe_j = \operatorname{tr} A$. Then $\operatorname{span}\{e_ie_j^t : 1 \leq i, j \leq n\} = M_n$.

The case when $n = 2$. The operator system $\mathcal{S} = \operatorname{span}\{I, A_1, \ldots, A_m\}$ may have dimension $d \in \{1, 2, 3, 4\}$. The previous propositions cover the cases for $d = 1, 2, 4$. For $d = 3$, it was shown by P.S. Pan, Y.T. Poon, and C.K. Li that $k = 2$ in this case.

Proof. If $\mathcal{S} = \operatorname{span}\{I_2, A_1, A_2\}$. we may apply a unitary similarity and change I_2, A_1 to E_{11}, E_{22}, then we may assume A_2 has diagonal entries. Then apply a diagonal unitary similarity, we may assume that $A_2 = E_{12} + E_{21}$. Thus, § is the set of symmetric matrices.

Let

$$F_1 = \frac{1}{\sqrt{24}}\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}, \quad F_2 = \frac{1}{\sqrt{24}}\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}, \quad F_3 = \frac{1}{\sqrt{24}}\begin{pmatrix} 0 & -1 \\ -2 & 3 \end{pmatrix}.$$

Then $F_1^*F_2 + F_2^*F_2 + F_3^*F_3 = I_2$ and

$$\operatorname{span}\{F_i^*F_j : 1 \leq i, j \leq 3\} = \mathcal{S} = \operatorname{span}\{E_{11}, E_{22}, E_{12} + E_{21}\}.$$

Alternatively, one may consider the rank 2 positive semidefinite matrix

$$Q = \frac{1}{4\sqrt{2}}\begin{pmatrix} \sqrt{2}I_2 & (1+i)(E_{12}+E_{21}) \\ (1-i)(E_{12}+E_{21}) & \sqrt{2}I_2 \end{pmatrix},$$

and find the factorization $[F_1\ F_2]^*[F_1\ F_2]$ with $F_1, F_2 \in M_2$ so that $\Phi : M_2 \to M_2$ defined by $\Phi(X) = F_1XF_1^* + F_2XF_2^*$ satisfies $\mathcal{S}(\Phi) = \mathcal{S}$. $\square$

Further work Study the problem for $n = 3$. The propositions cover the cases when $\mathcal{S}$ has dimension $d = 1, 2, 9$, and the commutative case when $d = 3$. So, it remain to consider the case when $d = 4, 5, 6, 7, 8$ and the non-commutative case when $n = 3$.

Construction of some special matrix sets

1. (Mutually unbiased bases - MUB) Construct unitary $U_1 = I_n, U_2, \ldots, U_k \in M_n$ such that every entries of $U_i^* U_j$ has modulus $1/\sqrt{n}$.

   One may take $U_2 = \frac{1}{\sqrt{n}}(w^{(r-1)(s-1)})$ with $w = e^{i2\pi/n}$.

   It is known that $k \le n+1$. If n is a prime power, i.e., $n = p^m$, then one can get $n+1$ such matrices.

   Big open question. When $n = 6$ can we construct 3,4,5,6, or 7?

2. (Werner-Holevo channel decomposition) Consider the channel $\Phi : M_n \to M_n$ defined by

$$\Phi(X) = \frac{1}{n+1}(X + (\operatorname{tr} X) I_n) = \frac{1}{N}\left\{\sum_{j=1}^{n}(\sqrt{2})E_{jj})X(\sqrt{2})E_{jj} + \sum_{i<j} E_{ij} X E_{ji}\right\},$$

   where $N = N(N+1)/2$. Find symmetric unitary matrices $U_1, \ldots, U_N$ such that $\operatorname{tr}(U_i^* U_j) = 0$ for all $i \neq j$ and

$$\Phi(X) = \frac{1}{N}\sum_{j=1}^{N} U_j X U_j^*.$$