Lecture 1: Definitions of quantum strategies

1 Notation, mathematical preliminaries

\( \mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z} \)
Calligraphic letters denote finite-dimensional complex Euclidean spaces of the form \( \mathbb{C}^n \).

\( \mathcal{X}_1 \ldots n \)
Shorthand notation for the tensor product \( \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n \).

\( \mathcal{L}(\mathcal{X}) \)
The (complex) space of all linear operators \( A : \mathcal{X} \to \mathcal{X} \), implicitly identified with \( \mathbb{C}^{n \times n} \).

\( \text{Her}(\mathcal{X}) \)
The (real) subspace of Hermitian operators within \( \mathcal{L}(\mathcal{X}) \).

\( \text{Pos}(\mathcal{X}) \)
The cone of positive semidefinite operators within \( \text{Her}(\mathcal{X}) \).

\( \text{Dens}(\mathcal{X}) \)
The compact convex set of density operators within \( \text{Pos}(\mathcal{X}) \). (An operator \( \rho \in \text{Pos}(\mathcal{X}) \) is a density operator or quantum state if \( \text{Tr}(\rho) = 1 \).)

\( A^* \)
The adjoint of an operator \( A : \mathcal{X} \to \mathcal{Y} \), which has the form \( A^* : \mathcal{Y} \to \mathcal{X} \).

\( \langle A, B \rangle \)
The standard inner product between two operators \( A, B : \mathcal{X} \to \mathcal{Y} \). Defined by \( \langle A, B \rangle \overset{\text{def}}{=} \text{Tr}(A^* B) \).

\( I_\mathcal{X} \)
The identity operator acting on \( \mathcal{X} \).

\( 1_\mathcal{X} \)
The identity super-operator acting on \( \mathcal{L}(\mathcal{X}) \).

\( E_{i,j} = |i\rangle\langle j| \)
The matrix whose \((i,j)\)th entry is 1 with all others 0. \( \{E_{i,j}\}_{i,j=1}^{\dim(\mathcal{X})} \) is an orthonormal basis for \( \mathcal{L}(\mathcal{X}) \).

States, measurements, channels

A state of a quantum system with associated space \( \mathcal{X} \) is an operator \( \rho \in \text{Pos}(\mathcal{X}) \) with \( \text{Tr}(\rho) = 1 \).

A measurement of a quantum system with associated space \( \mathcal{X} \) is a finite set \( \{P_a\} \subset \text{Pos}(\mathcal{X}) \) of operators indexed by outcomes \( a \) with \( \sum_a P_a = I_\mathcal{X} \).

Given a quantum system with associated space \( \mathcal{X} \) in state \( \rho \) and a measurement \( \{P_a\} \) the probability with which outcome \( a \) is observed is \( \langle \rho, P_a \rangle = \text{Tr}(\rho P_a) \).

Once it has been measured, a quantum system is destroyed.

An operator \( A : \mathcal{X} \to \mathcal{Y} \) is an isometry if \( A^* A = I_\mathcal{X} \).

Clearly, \( A \) can be an isometry iff \( \dim(\mathcal{Y}) \geq \dim(\mathcal{X}) \).

If \( \dim(\mathcal{Y}) = \dim(\mathcal{X}) \) then \( A \) is called unitary.

A super-operator is a linear mapping of the form \( \Phi : \mathcal{L}(\mathcal{X}) \to \mathcal{L}(\mathcal{Y}) \).

A super-operator \( \Phi \) is positive if \( \Phi(X) \succeq 0 \) whenever \( X \succeq 0 \).

\( \Phi \) is completely positive if \( \Phi \otimes 1_\mathcal{Z} \) is positive for every choice of space \( \mathcal{Z} \).
Any completely positive super-operator $\Phi$ can be written in *Kraus form*

\[ \Phi : X \mapsto \sum_{i=1}^{n} A_i X A_i^* \]

for some $n \leq \dim(X \otimes Y)$ and some choice of $A_1, \ldots, A_n : \mathcal{X} \to \mathcal{Y}$.

$\Phi$ is *trace-preserving* if $\text{Tr}(\Phi(X)) = \text{Tr}(X)$ for all $X$.

A *channel* is a completely positive and trace-preserving super-operator.

Each channel can be written in *Stinespring form*, meaning that there exists a space $\mathcal{Z}$ of dimension no larger than $\dim(X \otimes Y)$ and an isometry $A : \mathcal{X} \to \mathcal{Y} \otimes \mathcal{Z}$ with $\Phi : X \mapsto \text{Tr}_\mathcal{Z}(AXA^*)$.

**The operator-vector correspondence**

Let $\text{vec}$ be the unique linear mapping from matrices to vectors given by the following action on standard basis states

\[ \text{vec}(E_{i,j}) = \text{vec}(|i\rangle\langle j|) \overset{\text{def}}{=} |i\rangle \otimes |j\rangle. \]

Intuitively, the vec mapping acting upon a matrix $A$ transposes each row $a$ of $A$ to form a column $a^T$ and then stacks all those columns to form a single, large column:

\[ \text{vec} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \]

**Properties:**

1. $\text{vec}(|\phi\rangle\langle \psi|) = |\phi\rangle \otimes |\psi\rangle$.

2. $(A \otimes B) \text{vec}(X) = \text{vec}(AXB^T)$ for any $A, X, B$ for which the product $AXB^T$ makes sense.

3. $(\text{vec}(I_{\mathcal{X}})^* \otimes I_{\mathcal{W}}) \text{vec}(A \otimes B) = \text{vec}(BA)$ for all $A : \mathcal{W} \to \mathcal{X}, B : \mathcal{X} \to \mathcal{Y}$.

   For clarity, note that $\text{vec}(I_{\mathcal{X}}) \in \mathcal{X} \otimes \mathcal{X}$ and $\text{vec}(A \otimes B) \in \mathcal{X} \otimes \mathcal{W} \otimes \mathcal{Y} \otimes \mathcal{X}$. The adjoint $\text{vec}(I_{\mathcal{X}})^*$ is a row vector.

4. Interesting fact: $\text{vec}(I) = \sum_i |i\rangle\langle i|)$ is an unnormalized maximally entangled state.

**Choi-Jamiolkowski isomorphism**

For each super-operator $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$ define $J(\Phi) \in L(\mathcal{Y} \otimes \mathcal{X})$ by

\[ J(\Phi) \overset{\text{def}}{=} \sum_{i,j=1}^{\dim(\mathcal{Y})} \Phi(E_{i,j}) \otimes E_{i,j} \]

**Properties:**
1. $\Phi$ is completely positive $\iff J(\Phi) \succeq 0$.

2. $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ is trace-preserving $\iff \text{Tr}_{\mathcal{Y}}(J(\Phi)) = I_{\mathcal{X}}$.

3. Kraus form: if $\Phi : X \mapsto \sum_i A_i X A_i^*$ then $J(\Phi) = \sum_i \text{vec}(A_i) \text{vec}(A_i)^*$.

4. Stinespring form: if $\Phi : X \mapsto \text{Tr}_{\mathcal{Z}}(A X A^*)$ then $J(\Phi) = \text{Tr}_{\mathcal{Z}}(\text{vec}(A) \text{vec}(A)^*)$.

5. The action of $\Phi : L(\mathcal{X}) \rightarrow L(\mathcal{Y})$ can be recovered from $J(\Phi)$ via the formula

$$\Phi(\rho) = \text{Tr}_{\mathcal{Y}} \left( (I_{\mathcal{X}} \otimes \rho^T) J(\Phi) \right) = \text{Tr}_{\mathcal{Y}} \left( (I_{\mathcal{X}} \otimes \rho) J(\Phi)^T \right)$$

Here $T_{\mathcal{X}}$ denotes the partial transpose on $\mathcal{X}$.

Example 1 (Choi matrix of states, measurements, trace). A state $\rho \in \text{Dens}(\mathcal{X})$ can be viewed as a channel $\rho : \mathbb{C} \rightarrow L(\mathcal{X}) : \alpha \mapsto \alpha \rho$. Clearly, $J(\rho) = \rho$.

For any measurement $\{P_a\} \subset \text{Pos}(\mathcal{X})$ each operator $P_a$ can be viewed as a channel $P_a : L(\mathcal{X}) \rightarrow \mathbb{C} : X \mapsto \langle X, P_a \rangle$. Given that, it is easy to compute

$$J(P_a) = \sum_{i,j=1}^{\dim(\mathcal{X})} \langle E_{i,j}, P_a \rangle E_{i,j} = P_a^T.$$

For the trace we have

$$J(\text{Tr}) = \sum_{i,j} \text{Tr}(E_{i,j}) \otimes E_{i,j} = \sum_i E_{i,i} = I$$

\[\square\]

## 2 Operational definition of a strategy

Intuition: a strategy is a complete description of one party’s actions in a multiple-round (finite) interaction involving the exchange of quantum information with one or more other parties.

Every interaction decomposes naturally into $r$ rounds: message comes in, the message is processed, reply is sent out.

Outgoing messages can depend upon messages exchanged in previous rounds $\implies$ memory.

Example: $r$-round two-party interaction:

The strategy for Alice in the above interaction:
To extract classical information from an interaction, a strategy might call for one or more measurements throughout the interaction.

Without loss of generality we may assume that all measurements are simulated by a single measurement on the last memory space.

**Definition 2** (strategy, operational definition (intuitive but useless)). An \( r \)-round non-measuring strategy for an interaction with input spaces \( X_1, \ldots, X_r \) and output spaces \( Y_1, \ldots, Y_r \) consists of:

1. memory spaces \( Z_1, \ldots, Z_r \), and
2. channels \( \Phi_1, \ldots, \Phi_r \) of the form
   \[
   \Phi_1 : L(X_1) \to L(Y_1 \otimes Z_1) \\
   \Phi_i : L(X_i \otimes Z_{i-1}) \to L(Y_i \otimes Z_i) \quad (2 \leq i \leq r).
   \]

An \( r \)-round measuring strategy with outcomes indexed by \( a \) consists of items 1 and 2 and:

3. a measurement \( \{P_a\} \) on the last memory space \( Z_r \).

Problems with the operational definition:

1. **No distributive property for probabilistic mixtures.** States and channels are distributive:
   - A system prepared in state \( \rho_i \) w/prob \( p_i \) has \( \rho = p_1 \rho_1 + p_2 \rho_2 \).
   - A channel that applies \( \Phi_i \) w/prob \( p_i \) has \( \Phi = p_1 \Phi_1 + p_2 \Phi_2 \).
   - What is the strategy that implements \( (\Phi_1, \ldots, \Phi_r) \) w/prob \( p_i \)?

2. **No uniqueness.** Two “different” strategies cannot be physically distinguished by any interacting party.

3. **Non-convex optimization over strategies.** State of final systems \( Z_r \otimes W_r \) depends non-linearly on \( \Phi_1, \ldots, \Phi_r \), etc.

**Definition 3** (Non-measuring strategy). Given: an operational non-measuring strategy \( \Phi_1, \ldots, \Phi_r \) for input spaces \( X_1, \ldots, X_r \) and output spaces \( Y_1, \ldots, Y_r \). Let

\[
\Xi : L(X_{1..r}) \to L(Y_{1..r})
\]

be the channel composed of \( \Phi_1, \ldots, \Phi_r \) as follows.
With some abuse of notation, this composition may be expressed succinctly as

\[ \Xi = \text{Tr}_{Z_r} \circ \Phi_r \circ \cdots \circ \Phi_1. \]

(Here a tensor product with the identity super-operator \( I \) on the appropriate spaces is implicitly inserted where necessary in order for this composition to make sense.)

An operator

\[ Q \in \text{Pos}(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}) \]

is an \( r \)-round non-measuring strategy if \( Q = J(\Xi) \).

**Definition 4** (Measuring strategy). Given an operational measuring strategy \( \Phi_1, \ldots, \Phi_r, \{P_a\} \). For each outcome \( a \) let

\[ \Xi_a : L(\mathcal{X}_{1\ldots r}) \to L(\mathcal{Y}_{1\ldots r}) \]

be the channel composed of \( \Phi_1, \ldots, \Phi_r, P_a \) as follows.

[*Same figure as above except \( P_a \) applied to the memory space before trace-out.*]

For each measurement outcome \( a \) let

\[ \Xi_a = \Gamma_a \circ \Phi_r \circ \cdots \circ \Phi_1 \]

where the super-operator \( \Gamma_a \) is given by

\[ \Gamma_a : X \mapsto \text{Tr}_{Z_i} \left( (P_a \otimes I_{Y_{1\ldots r}}) X \right). \]

(Compare: for non-measuring strategies we defined \( \Xi \) via the partial trace \( \text{Tr}_{Z_r} \). For measuring strategies we define \( \Xi_a \) via \( \Gamma_a \) instead of the partial trace.)

A set of operators

\[ \{Q_a\} \subset \text{Pos}(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}) \]

is an \( r \)-round measuring strategy if each \( Q_a = J(\Xi_a) \). 

Convention for \( r = 0 \): a zero-round non-measuring strategy \( Q \) is just the scalar \( 1 \). A zero-round measuring strategy is a set \( \{p_a\} \) of positive reals with \( \sum_a p_a = 1 \).

Given \( \Phi_1, \ldots, \Phi_r \) we can assume WOLOG that \( \Phi_i : X \mapsto A_i X A_i^* \) for some isometry \( A_i \). (Absorb extra garbage output into memory space \( Z_i \).

In this case, we sometimes write \( A = A_r \cdots A_1 \) for the composition of \( A_1, \ldots, A_r \), so that \( \Xi : X \mapsto \text{Tr}_{Z_r} (AXA^*) \) and hence \( Q = J(\Xi) = \text{Tr}_{Z_i} (\text{vec}(A) \text{vec}(A)^*) \).

For measuring strategies, we have

\[ \Xi_a : X \mapsto \text{Tr}_{Z_i} \left( (P_a \otimes I_{Y_{1\ldots r}}) AXA^* \right) \]

and hence

\[ Q_a = J(\Xi_a) = \text{Tr}_{Z_r} \left( (P_a \otimes I_{Y_{1\ldots r}} \otimes \mathcal{X}_{1\ldots r}) \text{vec}(A) \text{vec}(A)^* \right) \]

(1)