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 $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n$.
$\mathrm{L}(\mathcal{X})$	The (complex) space of all linear operators $A : \mathcal{X} \to \mathcal{X}$, implicitly identified with $\mathbb{C}^{n\times n}$.
$\mathrm{Her}(\mathcal{X})$	The (real) subspace of Hermitian operators within $\mathrm{L}(\mathcal{X})$.
$\mathrm{Pos}(\mathcal{X})$	The cone of positive semidefinite operators within $\mathrm{Her}(\mathcal{X})$.
$\mathrm{Dens}(\mathcal{X})$	The compact convex set of density operators within $\mathrm{Pos}(\mathcal{X})$. (An operator $\rho \in \mathrm{Pos}(\mathcal{X})$ is a *density operator* or *quantum state* if $\mathrm{Tr}(\rho) = 1$.)
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 $\langle A, B\rangle \stackrel{\text{def}}{=} \mathrm{Tr}(A^*B)$.
$I_{\mathcal{X}}$	The identity operator acting on $\mathcal{X}$.
$\mathbb{1}_{\mathcal{X}}$	The identity super-operator acting on $\mathrm{L}(\mathcal{X})$.
$E_{i,j} = \lvert i\rangle\langle j\rvert$	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 $\mathrm{L}(\mathcal{X})$.

States, measurements, channels

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

A *measurement* of a quantum system with associated space $\mathcal{X}$ is a finite set $\{P_a\} \subset \mathrm{Pos}(\mathcal{X})$ 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 ρ and a measurement $\{P_a\}$ the probability with which outcome a is observed is $\langle \rho, P_a\rangle = \mathrm{Tr}(\rho P_a)$.

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 $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$.

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

Φ is *completely positive* if $\Phi \otimes \mathbb{1}_{\mathcal{Z}}$ is positive for every choice of space $\mathcal{Z}$.

Any completely positive super-operator Φ can be written in *Kraus form*

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

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

Φ is *trace-preserving* if $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ 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 $\dim(\mathcal{X} \otimes \mathcal{Y})$ and an isometry $A : \mathcal{X} \to \mathcal{Y} \otimes \mathcal{Z}$ with $\Phi : X \mapsto \mathrm{Tr}_{\mathcal{Z}}(AXA^*)$.

The operator-vector correspondence

Let vec be the unique linear mapping from matrices to vectors given by the following action on standard basis states

$$\mathrm{vec}(E_{i,j}) = \mathrm{vec}(|i\rangle\langle j|) \stackrel{\text{def}}{=} |i\rangle \otimes |j\rangle.$$

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:

$$\mathrm{vec}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

Properties:

1. $\mathrm{vec}(|\phi\rangle\langle\psi|) = |\phi\rangle \otimes |\overline{\psi}\rangle$.
2. $(A \otimes B)\,\mathrm{vec}(X) = \mathrm{vec}(AXB^{\mathsf{T}})$ for any A, X, B for which the product AXB^{T} makes sense.
3. $(\mathrm{vec}(I_{\mathcal{X}})^* \otimes I_{\mathcal{W}\otimes\mathcal{Y}})\,\mathrm{vec}(A \otimes B) = \mathrm{vec}(BA)$ for all $A : \mathcal{W} \to \mathcal{X}, B : \mathcal{X} \to \mathcal{Y}$.

   For clarity, note that $\mathrm{vec}(I_{\mathcal{X}}) \in \mathcal{X} \otimes \mathcal{X}$ and $\mathrm{vec}(A \otimes B) \in \mathcal{X} \otimes \mathcal{W} \otimes \mathcal{Y} \otimes \mathcal{X}$. The adjoint $\mathrm{vec}(I_{\mathcal{X}})^*$ is a row vector.
4. Interesting fact: $\mathrm{vec}(I) = \sum_i |i\rangle|i\rangle$ is an unnormalized maximally entangled state.

Choi-Jamiołkowski isomorphism

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

$$J(\Phi) \stackrel{\text{def}}{=} \sum_{i,j=1}^{\dim(\mathcal{X})} \Phi(E_{i,j}) \otimes E_{i,j}$$

Properties:

1. Φ is completely positive $\iff J(\Phi) \succeq 0$.
2. $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is trace-preserving $\iff \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = I_{\mathcal{X}}$.
3. Kraus form: if $\Phi : X \mapsto \sum_i A_i X A_i^*$ then $J(\Phi) = \sum_i \mathrm{vec}(A_i)\,\mathrm{vec}(A_i)^*$.
4. Stinespring form: if $\Phi : X \mapsto \mathrm{Tr}_{\mathcal{Z}}(AXA^*)$ then $J(\Phi) = \mathrm{Tr}_{\mathcal{Z}}(\mathrm{vec}(A)\,\mathrm{vec}(A)^*)$.
5. The action of $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ can be recovered from $J(\Phi)$ via the formula

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

Here $\mathsf{T}_{\mathcal{X}}$ denotes the partial transpose on $\mathcal{X}$.

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

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

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

For the trace we have

$$J(\mathrm{Tr}) = \sum_{i,j} \underbrace{\mathrm{Tr}(E_{i,j})}_{\delta_{i,j}} \otimes E_{i,j} = \sum_i E_{i,i} = I$$

□

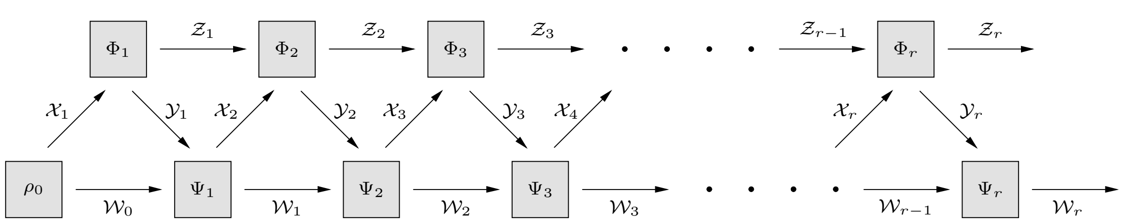
2 Operational definition of a strategy

Intuitition: 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.

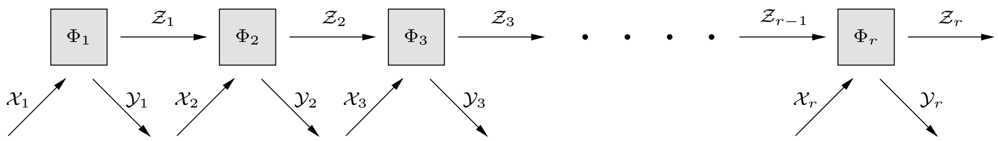
Every interaction decomposes naturally into r *rounds*: message comes in, the message is processed, reply is sent out.

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* $\mathcal{X}_1, \ldots, \mathcal{X}_r$ and *output spaces* $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$ consists of:

1. *memory spaces* $\mathcal{Z}_1, \ldots, \mathcal{Z}_r$, and
2. channels $\Phi_1, \ldots, \Phi_r$ of the form

$$\Phi_1 : \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Z}_1)$$
$$\Phi_i : \mathrm{L}(\mathcal{X}_i \otimes \mathcal{Z}_{i-1}) \to \mathrm{L}(\mathcal{Y}_i \otimes \mathcal{Z}_i) \quad (2 \leq i \leq r).$$

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 $\mathcal{Z}_r$.

□

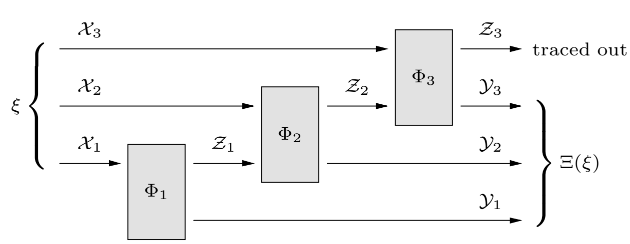
Problems with the operational definition:

1. *No distributive property for probabilistic mixtures.* States and channels are distributive:
   A system prepared in state ρ_i w/prob p_i has $\rho = p_1\rho_1 + p_2\rho_2$.
   A channel that applies Φ_i w/prob p_i has $\Phi = p_1\Phi_1 + p_2\Phi_2$.
   What is the strategy that implements $(\Phi_1, \ldots, \Phi_r)_i$ 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 $\mathcal{Z}_r \otimes \mathcal{W}_r$ 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 $\mathcal{X}_1, \ldots, \mathcal{X}_r$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$. Let

$$\Xi : \mathrm{L}(\mathcal{X}_{1\ldots r}) \to \mathrm{L}(\mathcal{Y}_{1\ldots r})$$

be the channel composed of $\Phi_1, \ldots, \Phi_r$ as follows.



With some abuse of notation, this composition may be expressed succinctly as

$$\Xi = \mathrm{Tr}_{\mathcal{Z}_r} \circ \Phi_r \circ \cdots \circ \Phi_1.$$

(Here a tensor product with the identity super-operator $\mathbb{1}$ on the appropriate spaces is implicitly inserted where necessary in order for this composition to make sense.)

An operator

$$Q \in \mathrm{Pos}(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r})$$

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

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

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 Γ_a is given by

$$\Gamma_a : X \mapsto \mathrm{Tr}_{\mathcal{Z}_r} \left((P_a \otimes I_{\mathcal{Y}_{1\ldots r}}) \, X \right).$$

(Compare: for non-measuring strategies we defined Ξ via the partial trace $\mathrm{Tr}_{\mathcal{Z}_r}$. For measuring strategies we define Ξ_a via Γ_a instead of the partial trace.)

A set of operators

$$\{Q_a\} \subset \mathrm{Pos}(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r})$$

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 $\mathcal{Z}_i$.

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

For measuring strategies, we have

$$\Xi_a : X \mapsto \mathrm{Tr}_{\mathcal{Z}_r}((P_a \otimes I_{\mathcal{Y}_{1\ldots r}}) \, AXA^*)$$

and hence

$$Q_a = J(\Xi_a) = \mathrm{Tr}_{\mathcal{Z}_r} \left((P_a \otimes I_{\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}}) \, \mathrm{vec}(A) \, \mathrm{vec}(A)^* \right) \tag{1}$$