Today: boxworld; a general no-cloning theorem
Next: Quantum theory from simple postulates

July 23: Any interest in little barbecue @ Mechanrise after last lecture? Who still needs a new exercise?

7.6 Composite state spaces (continued)

Last time: 3 requirements on a meaningful composite AB of two state spaces A and B.
(Including local tomography)

\[ \Rightarrow \text{Vector spaces satisfy: } \mathbf{A} \mathbf{B} = \mathbf{A} \otimes \mathbf{B} \]
\[ \mathbf{U}_{\mathbf{A}\mathbf{B}} = \mathbf{U}_{\mathbf{A}} \otimes \mathbf{U}_{\mathbf{B}} \]
\[ \mathbf{W}_{\mathbf{A}} \in \mathbf{S}_{\mathbf{A}}, \mathbf{W}_{\mathbf{B}} \in \mathbf{S}_{\mathbf{B}} \Rightarrow \mathbf{W}_{\mathbf{A}} \otimes \mathbf{W}_{\mathbf{B}} \in \mathbf{S}_{\mathbf{A}\mathbf{B}} \]
(Independent preparation)
\[ \mathbf{e}_{\mathbf{A}} \in \mathbf{E}_{\mathbf{A}}, \mathbf{e}_{\mathbf{B}} \in \mathbf{E}_{\mathbf{B}} \Rightarrow \mathbf{e}_{\mathbf{A}} \otimes \mathbf{e}_{\mathbf{B}} \in \mathbf{E}_{\mathbf{A}\mathbf{B}} \]
(Local measurements)

If A and B are dynamical state spaces, we also demand that \( \mathbf{T}_{\mathbf{A}} \otimes \mathbf{T}_{\mathbf{B}} \in \mathbf{G}_{\mathbf{A}\mathbf{B}} \) for all reversible transformations \( \mathbf{T}_{\mathbf{A}} \in \mathbf{G}_{\mathbf{A}}, \mathbf{T}_{\mathbf{B}} \in \mathbf{G}_{\mathbf{B}} \).

Lemma: For any two state spaces \((\mathbf{A}, \mathbf{A'}, \mathbf{U}_{\mathbf{A}})\) and \((\mathbf{B}, \mathbf{B'}, \mathbf{U}_{\mathbf{B}})\), there is a smallest possible composite...
A \otimes_{\text{min}} B := (A \otimes B, R_{\text{max}} \cdot \Omega_{AB}^{\text{min}}, U_A \otimes U_B)

where \( \Omega_{AB}^{\text{min}} := \text{conv} \{ w_A \otimes w_B | w_A \in \Omega_A, w_B \in \Omega_B \} \),

and a largest possible composite

\[ A \otimes_{\text{max}} B := \{ w_{AB} \in A \otimes B | U_{AB}(w_{AB}) = 1 \text{ and } 0 \leq e_A \otimes e_B(w_{AB}) \leq 1 \text{ for all } e_A \in E_A, e_B \in E_B \} \]

Any choice of compact convex \( \Omega_{AB} \) with

\[ \Omega_{AB}^{\text{min}} \subseteq \Omega_{AB} \subseteq \Omega_{AB}^{\text{max}} \]

gives a possible composite state space \( AB \).

**Def.** A state \( w_{AB} \in \Omega_{AB} \) is entangled if it cannot be written as a convex combination of product states, i.e. as

\[ w_{AB} = \sum_{i=1}^{\infty} \alpha_i w_A^{(i)} \otimes w_B^{(i)} \quad \text{with} \quad \sum \alpha_i = 1, \alpha_i > 0. \]

\( A \otimes_{\text{min}} B \) does not contain any entangled states (similarly, \( A \otimes_{\text{max}} B \) does not contain entangled effects)

\[ \Rightarrow \text{ the standard quantum composite } AB \text{ of quantum state spaces } A \text{ and } B \text{ satisfies} \]

\[ \Omega_{AB}^{\text{min}} \subseteq \Omega_{AB} \subseteq \Omega_{AB}^{\text{max}}. \]

**Lemma.** If \( w_A \) and \( w_B \) are pure, then so is \( w_A \otimes w_B \).

**Proof.** Exercise.
Example of non-quantum composite: boxworld
(special case: two parties, local qubits)

A and B are qbits: $(A, A_t, u_A) = (B, B_t, u_B)$, $A \otimes B = \mathbb{R}^3$

\[ \Omega_A = \{ (\frac{1}{2}) \mid -1 \leq y \leq 1, -1 \leq z \leq 1 \}, \]
\[ u_A\left(\frac{1}{y}\right) = x. \]

$AB = A \otimes B \cong \mathbb{R}^9$ \(\Rightarrow\) $\Omega_{AB}$ is an 8-dim. compact convex set.

Choose $A \otimes \text{max} B$ as the composite.

Shown last time: for a single qbit, there are 2 pure 2-outcome measurements

\[ \begin{array}{c}
(\zeta_y, \overline{\zeta_y}) \\
\text{"measurement 0"}
\end{array} \quad \begin{array}{c}
(\zeta_z, \overline{\zeta_z}) \\
\text{"measurement 1"}
\end{array} \]

Every state $\eta_{AB} \in \Omega_{\text{max} AB}$ defines a behavior:

\[ P(u,v\mid a=0, b=1) \]

$\alpha, \beta \in \{0,1\}$ choices of measurement

$u,v \in \{-1,1\}$ outcomes

E.g., the four values of $P(u,v\mid a=0, b=1)$ are

\[ (u,v) = (-1,-1) : e_y \otimes e_z (\eta_{AB}) \]
\[ (-1,1) : e_y \otimes \overline{e_z} (\eta_{AB}) \]
\[ (+1,-1) : \overline{e_y} \otimes e_z (\eta_{AB}) \]
\[ (+1,1) : \overline{e_y} \otimes \overline{e_z} (\eta_{AB}) \]
Normalization: \( \sum_{u,v} P(u,v | a=0, b=1) \)

\( = (e_y + e_y) \otimes (e_z + e_z) (\nu_{AB}) = u_A \otimes u_B (w_{AB}) = u_{AB} (w_{AB}) = 1. \)

It turns out that

\( \mathcal{S}_{\text{max}}^{\text{AB}} \xrightarrow{1:1} (2,2,2) - \text{non-signalling} \)

(behaviors)

\( \mathcal{S}_{\text{max}}^{\text{AB}} \) is the \((2,2,2) - \text{no-signalling} \) polytope!

It is 8-dim. and has 24 pure states:

- 16 product states \( u_A^{(i)} \otimes u_B^{(j)}, \quad i,j = 1,2,3,4 \)
- 8 further pure states - the \( \text{PR-box states} \).

These are entangled states!

\[ \Sigma_A \otimes_{\text{max}} \Sigma_B = \mathcal{S}_{\text{max}}^{\text{AB}} \]

\( \mathcal{S}_{\text{max}}^{\text{AB}} \)

**Theorem**: (D. Gross, M.M., R. Colbeck, O. Dahlsten, PRL 104/080402 (2010))

The reversible transformations \( \mathcal{G}_{1...n} \) of \( n \) qubits are only the local transformations, and SICPs of the parties. (No reversible interactions?)

In particular, no rev. transf. can map any pure product state \( u_A^{(4)} \otimes u_B^{(1)} \) to a PR-box state.

This is different from QT, where there are unitaries with

\( U(10^A \otimes 10^B) = \frac{1}{\sqrt{2}} (10^A \overrightarrow{10^B} + 11^A \overrightarrow{11^B}) \)
However, composites of GPTs are very similar to quantum theory in many other respects:

8. A general no-cloning theorem

"A single quantum cannot be cloned"


Classical information can be copied, but not quantum information; for example, there is no quantum operation that maps $|4\rangle \otimes |0\rangle \rightarrow |4\rangle \otimes |4\rangle$

for all $|4\rangle$ (i.e., copying of an unknown quantum state).

We will see that

- classical prob. dist. also cannot be cloned,
- all pure states in a GPT can be cloned if and only if the theory is classical.

**Definition:** Let $(A, A_t, U_t)$ be any state space.

$(B, B_t, U_B) = (A, A_t, U_t)$ a copy of it, and $AB$ any (locally tomographic) composite.

A finite collection of states $W_1, \ldots, W_n \in \mathcal{H}_A$ is called cloneable if there exists a transformation $T: A \rightarrow AB$ such that $T(W_i) = W_i \otimes W_i$ for all $i = 1, \ldots, n$.

**Main Theorem:** $W_1, \ldots, W_n$ are cloneable if and only if they are perfectly distinguishable.
No matter what composite we choose (\(\otimes_{\min}\) or \(\otimes_{\max}\) or anything in between...)

In QT, states \(s_1, \ldots, s_n\) (density matrices) are perfectly distinguishable iff \(s_i \cdot s_j = 0\) for all \(i \neq j\) (proof: exercise).

In particular, if the states are pure, \(s_i = |4_i\rangle\langle 4_i|\) the condition is \(\langle 4_i | 4_j \rangle = 0_{ij}\).

\[\Rightarrow\] if \(|4\rangle \perp \perp |4\rangle\) there is no machine with

\[
\text{input:} \quad \begin{array}{c}
|4\rangle \text{ or } |4\rangle \\
\text{(dependant on input)}
\end{array}
\text{output:} \quad \begin{array}{c}
|4\rangle \quad \text{or} \\
|4\rangle \quad \text{or} \\
\end{array}
\]

Proof idea: We could iterate this machine, produce either \(|4\rangle \otimes N\) or \(|4\rangle \otimes N\) for \(N\) large, and determine reliably if we have \(|4\rangle\) or \(|4\rangle\) by tomography.

\(\Rightarrow\) \(|4\rangle, |4\rangle\) perf. dist.

In CPT, states \(p_1, \ldots, p_n\) (prob. distributions) are perfectly distinguishable iff \(p_i \cdot p_j = 0\) for all \(i \neq j\).

eg. \((1/2)\) and \((3/4)\) or not, but \((2/3)\) and \((0/1)\) are.

\(\Rightarrow\) if \(P \circ Q \neq 0\), there is no machine with

\[
\text{input:} \quad \begin{array}{c}
P \circ Q
\end{array}
\text{output:} \quad \begin{array}{c}
P \quad \text{or} \\
\text{or} \\
Q
\end{array}
\]

class. probability distributions also cannot be cloned.

Simple "copy" operations will produce correlated states instead of independent copies \(P \otimes P/Q \otimes Q\) (discuss...!)
Proof: If \( \omega_1, \ldots, \omega_n \) are proj. dist. by effects \( e_1, \ldots, e_n \), define

\[
T(\omega) = \sum_{i=1}^{n} e_i(\omega) \cdot \omega_i \otimes \omega_i
\]

\( \Rightarrow \) \( T \) linear, \( T(\omega_j) = \omega_j \otimes \omega_j \)

\[
U_{AB}(T(\omega)) = \sum_{i=1}^{n} e_i(\omega) U_{AB}(\omega_i \otimes \omega_i) = \mathbf{0} \cdot u(u)
\]

Normalization-preserving.

Clearly \( T(\omega) \in \mathcal{P}_{AB} \) if \( \omega \in \mathcal{P}_A \) \( \Rightarrow \) \( T \) is positive.

Suppose \( \omega_1, \ldots, \omega_n \) are clozable. Let \( T_N : A \to A^N \) be the \( N \)-fold iterate operation:

\[
T_N(\omega_j) = \underbrace{\omega_j \otimes \cdots \otimes \omega_j}_{N}
\]

\( T_1 = I, T_2 = T \)

To simplify proof, we assume that \( T \) is normalization-preserving (some arguments hold, with little complications, if \( T \) is normalization-decreasing).

Let \( e_1, \ldots, e_k \in E_A \) be an unificationally complete measurement, i.e. \( \sum e_i = U_A \) and \( e_i(\omega) = e_i(\varphi) \forall i \Rightarrow \omega = \varphi \).

(Discuss why this exists.)

For \( \mathbf{x} = (x_1, \ldots, x_N) \in \{1, \ldots, K\}^N \) set \( P_j(\mathbf{x}) = e_{x_1} \otimes \cdots \otimes e_{x_N}(T_N(\omega_j)) \)

\[
= \prod_{i=1}^{N} e_{x_i}(\omega_j)
\]
\[\Rightarrow \sum_{x} \mathbb{P}_j(x) = \mathbb{U}(T_N(w_j)) = \mathbb{U}(w_j) = 1.\]

For \(k = 1, \ldots, K\) set
\[
Q_x(l) = \frac{\{x: i, l_i = l\}}{N}
\]
(relative number of times that outcome \(l\) occurred).

Set of outcome sequences where the observed frequency is approximately the (one-shot) probability of that outcome:

For \(\varepsilon > 0\), set
\[
A_{j,N,\varepsilon} := \{ x \mid \max \{ e_x(w_j) - Q_x(l) \} < \varepsilon \}
\]

Weak law of large numbers:

If \(N\) is large enough (say, \(N > N_0\)) then
\[
\mathbb{P}_j(A_{j,N,\varepsilon}) > 1 - \varepsilon.
\]

If \(\varepsilon\) is small enough then \(A_{j,N,\varepsilon} \cap A_{k,N,\varepsilon} = \emptyset\) for \(j \neq k\)

because \((e_1^{(w_j)})\) are different distributions for different \(j\).

For \(j = 1, \ldots, n\) set
\[
f_{j,N,\varepsilon}(w) := \sum_{x \in A_{j,N,\varepsilon}} e_x \otimes \cdots \otimes e_x(T_N(w))
\]

\(> 0\) if \(w \in \Omega_A\), and
\[
\sum_{j=1}^{n} f_{j,N,\varepsilon}(w) = \sum_{x \in \bigcup_j A_{j,N,\varepsilon}} e_x \otimes \cdots \otimes e_x(T_N(w)) \leq \sum_{x} e_x \otimes \cdots \otimes e_x(T_N(w))
\]
\[ = u(T_n(w)) = u(w) = 1 \]

\[ \Rightarrow \text{all } \tilde{f}_{i,n,e} \in E_A, \text{ and they define a (sub-)measurement.} \]

For \( \varepsilon = \frac{1}{m} \), \( m \in \mathbb{N} \), consider

\[ (f_1, \ldots, f_n, \varepsilon, \ldots) \in E_A \times E_A \]

Since \((E_A)^n\) is compact, there is a convergent subsequence. Call its limit \((f_1, \ldots, f_n)\).

If \( i \neq j \), then

\[ \left( \tilde{f}_{i,m,e}(w_i) \right) = \sum_{x \in A_{i,j,n,e}} e_x \otimes \ldots \otimes e_x^{(T_n(w_i))} \]

\[ = P_i(A_{i,j,n,e}) \leq 1 - P_i(A_{i,j,n,e}) \]

\[ \leq 1 - P_i(A_{i,n,e}) < \varepsilon \]

\[ \Rightarrow \tilde{f}_j(w_i) = 0 \]

Similarly, \( \tilde{f}_{j,m,e}(w_j) = P_j(A_{j,n,e}) > 1 - \varepsilon \)

\[ \Rightarrow \tilde{f}_j(w_j) = 1 \]

Set \( \tilde{f}_n = f_1, \ldots, \tilde{f}_{n-1} = f_{n-1}, \tilde{f}_n = f_n + (u_n - (f_{n-1} + f_{n-2})) \)

Then \( \tilde{f}_1, \ldots, \tilde{f}_n \) perfectly distinguishes \( u_1, \ldots, u_n \).