FROM CLONING TO CHARACTERIZING SEPARABLE STATES

These notes contain the solutions of Exercise 4 on sheet 12 and an application of these ideas to the theory of quantum entanglement.

1. Cloning and the measure-prepare map

In the quantitative version of the no-cloning theorem we introduced the *optimal cloning map*, which we can restrict to the space $B(\mathcal{H}^{\vee n})$: Let $\text{clone}_{n\to m} : B\left(\mathcal{H}^{\vee n}\right) \to B\left(\mathcal{H}^{\vee m}\right)$ denote the map given by

$$\text{clone}_{n\to m}(X) = \frac{d[n]}{d[m]} P^m_{sym}\left(X \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right) P^m_{sym},$$

where we denote the dimension of the symmetric subspace $\mathcal{H}^{\vee k}$ by

$$d[k] := \binom{k+d-1}{k},$$

with $d = \dim(\mathcal{H})$. The map $\text{clone}_{n\to m}$ is the optimal cloning map from Theorem **??** restricted to the space $B(\mathcal{H}^{\vee n})$. It can also be checked that this map coincides (up to a normalization factor) with the adjoint $\text{Tr}^*_{m\to n}$ of the partial trace map $\text{Tr}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$. We will need another linear map on the symmetric operators: The *measure-prepare map* $\text{MP}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ is given by

$$\text{MP}_{m\to n}(X) = d[m] \int_{\mathcal{U}(\mathcal{H})} \langle \phi_U^{\otimes m} | X | \phi_U^{\otimes m}\rangle |\phi_U\rangle\langle\phi_U|^{\otimes n} d\eta(U),$$

where $|\phi_U\rangle = U|0\rangle$ for any $U \in \mathcal{U}(\mathcal{H})$. We will need the following lemma:

Lemma 1.1. *For any $m \geqslant n$ the maps $\text{MP}_{m\to n} : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ and $\text{clone}_{n\to m} : B(\mathcal{H}^{\vee n}) \to B(\mathcal{H}^{\vee m})$ are quantum channels.*

Proof. It is clear that these maps are completely positive. To see that they are trace-preserving we can compute

$$\text{Tr}\left[\text{MP}_{m\to n}(X)\right] = d[m] \int_{\mathcal{U}(\mathcal{H})} \langle \phi_U^{\otimes m} | X | \phi_U^{\otimes m}\rangle d\eta(U) = \text{Tr}\left[P^m_{sym} X\right] = \text{Tr}\left[X\right],$$

for every $X \in B(\mathcal{H}^{\vee m})$. Similarly, for every $Y \in B(\mathcal{H}^{\vee n})$ we have

$$\text{Tr}\left[\text{clone}_{n\to m}(Y)\right] = \frac{d[n]}{d[m]} \text{Tr}\left[P^m_{sym}\left(Y \otimes \mathbb{1}_{\mathcal{H}}^{\otimes(m-n)}\right)\right] = \text{Tr}\left[P^n_{sym} Y\right] = \text{Tr}\left[Y\right],$$

as in the proof of the quantitative no-cloning theorem. □

There is a remarkable identity connecting the optimal cloning maps to the measurement-prepare maps:

Theorem 1.2 (Chiribella identity)**.** *For any $m \geqslant n$ we have*

$$\text{MP}_{m\to n} = \frac{d[m]}{d[m+n]} \sum_{s=0}^{n} \frac{d[n]}{d[s]} \frac{\binom{m}{s}\binom{n}{s}}{\binom{m+n}{n}} \text{clone}_{s\to n} \circ \text{Tr}_{m\to s}\,.$$

Proof. From the exercises we know that

$$B\left(\mathcal{H}^{\vee k}\right) = \text{span}_{\mathbb{C}}\{|v\rangle\langle v|^{\otimes k} \;:\; |v\rangle \in \mathcal{H}\},$$

and to check equality of two linear maps $L_1, L_2 : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ it is therefore enough to check that

$$\langle |b\rangle\langle b|^{\otimes n}, L_1\left(|a\rangle\langle a|^{\otimes m}\right)\rangle_{HS} = \langle |b\rangle\langle b|^{\otimes n}, L_2\left(|a\rangle\langle a|^{\otimes m}\right)\rangle_{HS},$$

for all $|a\rangle, |b\rangle \in \mathcal{H}$ satisfying $\langle a|a\rangle = \langle b|b\rangle = 1$. In our case of interest, we find

$$\begin{aligned}\langle |b\rangle\langle b|^{\otimes n}, \mathrm{MP}_{m\to n}\left(|a\rangle\langle a|^{\otimes m}\right)\rangle_{HS} &= d[m]\langle b^{\otimes n}\otimes a^{\otimes m}|\int_{\mathcal{U}(\mathcal{H})}|\phi_U\rangle\langle\phi_U|^{\otimes(m+n)}d\eta(U)|b^{\otimes n}\otimes a^{\otimes m}\rangle \\ &= \frac{d[m]}{d[m+n]}\langle b^{\otimes n}\otimes a^{\otimes m}|P^{n+m}_{sym}|b^{\otimes n}\otimes a^{\otimes m}\rangle \\ &= \frac{d[m]}{d[m+n]}\frac{1}{(m+n)!}\sum_{\sigma\in S_{m+n}}\langle b^{\otimes n}\otimes a^{\otimes m}|U_\sigma|b^{\otimes n}\otimes a^{\otimes m}\rangle \\ &= \frac{d[m]}{d[m+n]}\sum_{s=0}^{n}\frac{\binom{m}{s}\binom{n}{s}}{\binom{n+m}{n}}|\langle a|b\rangle|^{2s},\end{aligned}$$

where we used that there are

$$\binom{m}{s}\binom{n}{s}n!m!$$

possibilities to select s elements from $\{1,\dots,m\}$ and s elements from $\{1,\dots,n\}$ and match them with s elements out out $\{1,\dots,n\}$ and $\{1,\dots,m\}$, respectively. On the other hand, we have

$$\langle b^{\otimes n}|\,\mathrm{clone}_{s\to n}\circ\mathrm{Tr}_{m\to s}\left(|a\rangle\langle a|^{\otimes m}\right)|b^{\otimes n}\rangle = \frac{d[s]}{d[n]}|\langle a|b\rangle|^{2s},$$

and by comparing the two sides of the Chiribella identity the proof of the theorem follows.

□

2. The quantum de-Finetti theorem

Why is the Chiribella identity useful? Let us consider the coefficient of the last term on the right-hand side (i.e., the term for $s = n$):

$$\frac{d[m]}{d[m+n]}\frac{\binom{m}{n}}{\binom{m+n}{n}} = \frac{m!(m+d-1)!}{(m-n)!(m+n+d-1)!} \geqslant \left(1-\frac{d+n}{d+m}\right)^n \geqslant 1-\frac{n(d+n)}{m+d}.$$

Since $\mathrm{clone}_{n\to n} = \mathrm{id}_{B(\mathcal{H}^{\vee n})}$, we conclude that

$$\mathrm{MP}_{m\to n} = (1-\epsilon_{m,n,d})\,\mathrm{Tr}_{m\to n} + \epsilon_{m,n,d}R,$$

for some quantum channel $R : B(\mathcal{H}^{\vee m}) \to B(\mathcal{H}^{\vee n})$ and some

$$\epsilon_{m,n,d} \leqslant \frac{n(d+n)}{m+d}.$$

As a consequence we obtain the following theorem:

Theorem 2.1 (Quantum de-Finetti theorem)**.** *For any $m \geqslant n$ and any pure quantum state $|\psi\rangle \in \mathcal{H}^{\vee m}$ there exists a quantum state*

$$\sigma \in conv\{|v\rangle\langle v|^{\otimes n} \;:\; |v\rangle \in \mathcal{H}, \langle v|v\rangle = 1\},$$

such that

$$\|\,\mathrm{Tr}_{m\to n}[|\psi\rangle\langle\psi|] - \sigma\|_1 \leqslant \frac{2n(d+n)}{m+d}.$$

Proof. By the previous discussion, we have

$$\mathrm{MP}_{m\to n} = (1-\epsilon_{m,n,d})\,\mathrm{Tr}_{m\to n} + \epsilon_{m,n,d} R$$

for some quantum channel R. From this we conclude that

$$\|\,\mathrm{Tr}_{m\to n}\left[|\psi\rangle\langle\psi|\right] - \mathrm{MP}_{m\to n}\left(|\psi\rangle\langle\psi|\right)\|_1 \leqslant 2\epsilon_{m,n,d} = \frac{2n(d+n)}{m+d}.$$

Setting $\sigma = \mathrm{MP}_{m\to n}\left(|\psi\rangle\langle\psi|\right)$ this is the statement of the theorem. □

3. Extendibility

We will finish this lecture with an application of these ideas to the computational task of testing entanglement. The following theorem shows that only separable states admit arbitrary many (symmetric) extensions:

Theorem 3.1. *For complex Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ denote a quantum state such that for every $N \in \mathbb{N}$ there exists a quantum state $\sigma_{AB_1\cdots B_N} \in D(\mathcal{H}_A \otimes \mathcal{H}_B^{\otimes N})$ satisfying*

$$\sigma_{AB_i} = \rho_{AB},$$

for every $i \in \{1,\ldots,N\}$. Then, we have $\rho_{AB} \in Sep(\mathcal{H}_A,\mathcal{H}_B)$.

Proof. Note first that without loss of generality we may assume that

$$(\mathbb{1}_{\mathcal{H}_A} \otimes U_\sigma)\sigma_{AB_1\cdots B_N}(\mathbb{1}_{\mathcal{H}_A} \otimes U_\sigma^\dagger) = \sigma_{AB_1\cdots B_N},$$

for every $\sigma \in S_N$ and every $N \in \mathbb{N}$ since otherwise we can consider symmetrizations of $\sigma_{AB_1\cdots B_N}$ instead.

For every $N \in \mathbb{N}$, we can now find a purification

$$|\psi_{AA'B_1B_1'\cdots B_NB_N'}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_A \otimes (\mathcal{H}_B \otimes \mathcal{H}_B)^{\vee N}$$

of $\sigma_{AB_1\cdots B_N}$. Indeed, we first note that (by an argument from an exercise)

$$(\mathbb{1}_{\mathcal{H}_A} \otimes U_\sigma)\sqrt{\sigma_{AB_1\cdots B_N}}(\mathbb{1}_{\mathcal{H}_A} \otimes U_\sigma)^\dagger = \sqrt{\sigma_{AB_1\cdots B_N}},$$

for every $\sigma \in S_N$. Then, the pure state

$$|\psi_{AA'B_1B_1'\cdots B_NB_N'}\rangle = \mathrm{vec}\left(\sqrt{\sigma_{AB_1\cdots B_N}}\right),$$

has the desired properties. Next, we will apply the identity

$$\mathrm{MP}_{N\to 1} = (1-\epsilon_{N,1,d_B^2})\,\mathrm{Tr}_{N\to 1} + \epsilon_{N,1,d_B^2} R,$$

for the measure-prepare channel $\mathrm{MP}_{N\to 1} : B((\mathcal{H}_B^{\otimes 2})^{\vee N}) \to B(\mathcal{H}_B^{\otimes 2})$ the partial trace $\mathrm{Tr}_{N\to 1} : B((\mathcal{H}_B^{\otimes 2})^{\vee N}) \to B(\mathcal{H}_B^{\otimes 2})$ and some other quantum channel R. This identity implies that

$$\|\,\mathrm{Tr}_{N\to 1} - \mathrm{MP}_{N\to 1}\|_\diamond \leqslant 2\epsilon_{N,1,d_B^2}.$$

Therefore, we have that

$$\|(\mathrm{id}_{AA'}\otimes\mathrm{Tr}_{N\to 1})\left(\psi_{AA'B_1B_1'\cdots B_NB_N'}\right) - (\mathrm{id}_{AA'}\otimes\mathrm{MP}_{N\to 1})\left(\psi_{AA'B_1B_1'\cdots B_NB_N'}\right)\|_1 \leqslant \frac{2(d_B^2+1)}{N+d_B^2}.$$

Finally, we note that

$$\mathrm{Tr}_{A'B'}\left[(\mathrm{id}_{AA'}\otimes\mathrm{Tr}_{N\to 1})\left(\psi_{AA'B_1B_1'\cdots B_NB_N'}\right)\right] = \rho_{AB},$$

and

$$\begin{aligned}&\mathrm{Tr}_{A'B'}\left[(\mathrm{id}_{AA'}\otimes\mathrm{MP}_{N\to 1})\left(\psi_{AA'B_1B_1'\cdots B_NB_N'}\right)\right]\\ &\quad= d[m]\int_{\mathcal{U}(\mathcal{H})}\left(\mathbb{1}_A \otimes \langle\phi_U^{\otimes N}|\right)\psi_{AB_1B_1'\cdots B_NB_N'}\left(\mathbb{1}_A \otimes |\phi_U^{\otimes N}\rangle\right)\otimes|\phi_U\rangle\langle\phi_U|d\eta(U)\\ &\quad\in \mathrm{Sep}\left(\mathcal{H}_A,\mathcal{H}_B\right).\end{aligned}$$

Since the partial trace over the $A'B'$ systems is a quantum channel, we have

$$\|\rho_{AB} - \mathrm{Tr}_{A'B'}\left[(\mathrm{id}_{AA'} \otimes \mathrm{MP}_{N\to 1})\left(\psi_{AA'B_1B_1'\cdots B_NB_N'}\right)\right]\|_1 \leqslant \frac{2(d_B^2+1)}{N+d_B^2}.$$

Since this is true for all $N \in \mathbb{N}$ we conclude that there is a sequence of separable quantum states $(\sigma_{AB}^{sep,N})_{N\in\mathbb{N}} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)^{\mathbb{N}}$ such that

$$\|\rho_{AB} - \sigma_{AB}^{sep,N}\|_1 \leqslant \frac{2(d_B^2+1)}{N+d_B^2} \to 0,$$

as $N \to \infty$. By compactness of the intersection $D(\mathcal{H}_A \otimes \mathcal{H}_B) \cap \mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$, we conclude that $\rho_{AB} \in \mathrm{Sep}\,(\mathcal{H}_A, \mathcal{H}_B)$.

□