CHAPTER 8: APPROXIMATE CLONING

§ 8.1 The no-cloning theorem

Classical and quantum information are fundamentally different!

Classical information can be cloned and thus replicated arbitrarily.

This is impossible for quantum information:

$\boxed{\text{Prop}}$ (No-cloning theorem)

Let A, B be d-dim. quantum systems. There is no unitary $U \in \mathcal{U}_{d^2}$ that achieves the transformation

$$U: |\psi\rangle_A \otimes |0\rangle_B \longmapsto |\psi\rangle_A \otimes |\psi\rangle_B$$

for arbitrary $|\psi\rangle \in \mathcal{X}_A$. Here, $|0\rangle_B$ is some reference state.

Proof: Let $|\psi\rangle, |\varphi\rangle \in \mathcal{X}_A$ be such that

$$U\left(|\psi\rangle_A \otimes |0\rangle_B\right) = |\psi\rangle_A \otimes |\psi\rangle_B,$$

$$U\left(|\varphi\rangle_A \otimes |0\rangle_B\right) = |\varphi\rangle_A \otimes |\varphi\rangle_B.$$

Then: $\langle\psi|\varphi\rangle^2 = (\langle\psi| \otimes \langle\psi|)(|\varphi\rangle \otimes |\varphi\rangle)$ $\qquad U^\dagger U = \mathbb{1}$

$$= \left(\langle\psi| \otimes \langle 0|\right) U^\dagger U \left(|\varphi\rangle \otimes |0\rangle\right) = \langle\psi|\varphi\rangle$$

$\Rightarrow \langle\psi|\varphi\rangle = 0$ or 1

$\Rightarrow$ no U can achieve $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle^{\otimes 2}$ for all $|\psi\rangle$ $\quad\square$

§ 8.2 Approximate cloning machines

Exact cloning is forbidden by no-cloning theorem.

What about approximate cloning?

We consider the following scenario:

- **Given:** Hilbert space $\mathcal{H}$ of dimension d and N copies of a pure state $|\psi\rangle \in \mathcal{H}$.
- **Goal:** Produce an approximation of M copies of $|\psi\rangle\langle\psi|$ for some $M > N$.
- **Figure of merit:** Let T be the approximate cloning map, $T: \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$

  (a linear map that is completely positive and trace-preserving)

  We define the "worst-case fidelity"

$$F(T) = \inf_{|\psi\rangle} F\left(\psi^{\otimes M}, T(\psi^{\otimes N})\right)^2$$

$$= \inf_{|\psi\rangle} \operatorname{tr}\left(\psi^{\otimes M}\, T(\psi^{\otimes N})\right).$$

Setting $d_N := \dim \mathrm{Sym}^N(\mathcal{H}) = \binom{d+N-1}{N}$, we first derive a general upper bound on $F(T)$:

$\boxed{\text{Lem}}$ For any approximate cloning map $T : \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$,

$$F(T) \leq \frac{d_N}{d_M} = \binom{d+N-1}{N} \binom{d+M-1}{M}^{-1}.$$

<u>Proof:</u> For given $T : \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$, define a twirled version

$$\overline{T}(X) := \int_{\mathcal{U}_d} (U^\dagger)^{\otimes M} \, T\left(U^{\otimes N} X (U^\dagger)^{\otimes N}\right) U^{\otimes M} \, dU.$$

which satisfies $\overline{T}\left(U^{\otimes N} X (U^\dagger)^{\otimes N}\right) = U^{\otimes M} \overline{T}(X) (U^\dagger)^{\otimes M} \quad \forall U.$

Let $|\varphi\rangle \in \mathcal{H}$ be arbitrary, then:

$$\mathrm{tr}\left(\varphi^{\otimes M} \overline{T}(\varphi^{\otimes N})\right) = \int dU \, \mathrm{tr}\left[\varphi^{\otimes M} (U^\dagger)^{\otimes M} T\left(U^{\otimes N} \varphi^{\otimes N} (U^\dagger)^{\otimes N}\right) U^{\otimes M}\right]$$

$$= \int dU \, \underbrace{\mathrm{tr}\left[(U\varphi U^\dagger)^{\otimes M} \, T\left((U\varphi U^\dagger)^{\otimes N}\right)\right]}_{\geq \inf_{|\psi\rangle} \mathrm{tr}\left(\psi^{\otimes M} T(\psi^{\otimes N})\right) = F(T)}$$

$$\geq \int dU \, F(T) = F(T)$$

$\Rightarrow \quad F(\overline{T}) \geq F(T)$ by taking infimum over $|\varphi\rangle \in \mathcal{H}$.

Now let $\tau_N := \frac{1}{d_N} \Pi_N$ where Π_N is the projector onto $\mathrm{Sym}^N(\mathcal{H})$.

We have:

$\cdot)$ $U^{\otimes N} \Pi_N (U^\dagger)^{\otimes N} = \Pi_N$ for all $U \in \mathcal{U}_d$

$$\Rightarrow \quad U^{\otimes M} \overline{T}(\tau_N) (U^\dagger)^{\otimes M} = \overline{T}(U^{\otimes N} \tau_N (U^\dagger)^{\otimes N})$$

$$= \overline{T}(\tau_N) \quad \forall\, U \in \mathcal{U}_d$$

$$\overset{\text{SW-duality}}{\Rightarrow} \quad \overline{T}(\tau_N) = \lambda \tau_M + (1-\lambda)\sigma \quad \text{where } \sigma \perp \mathrm{Sym}^M(\mathcal{H}),\ \lambda \in [0,1].$$

$\cdot)$ For every $|\varphi\rangle \in \mathcal{H}$, $\quad \Pi_N - |\varphi\rangle\langle\varphi|^{\otimes N} \geq 0$

$$\Rightarrow \quad 0 \leq \overline{T}(\Pi_N - |\varphi\rangle\langle\varphi|^{\otimes N})$$

$$= \overline{T}(\Pi_N) - \overline{T}(\varphi^{\otimes N})$$

$$= d_N \lambda \tau_M + d_N (1-\lambda)\sigma - \overline{T}(\varphi^{\otimes N})$$

$$\Rightarrow \quad 0 \leq \mathrm{tr}\left[\varphi^{\otimes M}\, \overline{T}(\Pi_N - |\varphi\rangle\langle\varphi|^{\otimes N})\right]$$

$$= d_N \lambda \underbrace{\mathrm{tr}(\varphi^{\otimes M} \tau_M)}_{(*)} + d_N (1-\lambda) \overbrace{\mathrm{tr}(\varphi^{\otimes M} \sigma)}^{(**)}$$

$$- \mathrm{tr}\left[\varphi^{\otimes M}\, \overline{T}(\varphi^{\otimes N})\right]$$

$$(*) = \mathrm{tr}(\varphi^{\otimes M} \Pi_M d_M^{-1}) = \frac{1}{d_M} \mathrm{tr}(\varphi^{\otimes M}) = \frac{1}{d_M}$$

$$(**) = \mathrm{tr}(\Pi_M \varphi^{\otimes M} \Pi_M \sigma) = \mathrm{tr}(\varphi^{\otimes M} \underbrace{\Pi_M \sigma \Pi_M}_{=0}) = 0$$

$$\Rightarrow \quad F(T) \leq F(\overline{T}) \leq \mathrm{tr}\left[\varphi^{\otimes M}\, \overline{T}(\varphi^{\otimes N})\right] \leq \frac{d_N}{d_M} \lambda \leq \frac{d_N}{d_M}. \quad \square$$

Can we achieve this bound? Yes!

Set $T(X) = \frac{d_N}{d_M} \Pi_M \left(X \otimes \mathbb{1}_d^{\otimes M-N} \right) \Pi_M$

What does this map do?

Step 1: Extend state trivially from $\mathcal{H}^{\otimes N}$ to $\mathcal{H}^{\otimes M}$

Step 2: Project down to symmetric subspace $\mathrm{Sym}^M(\mathcal{H})$.

Step 3: Normalize to get a quantum state.

Fidelity $F(T)$: For arbitrary $|\varphi\rangle \in \mathcal{H}$,

$$\begin{aligned}
\mathrm{tr}\left[\varphi^{\otimes M} T(\varphi^{\otimes N})\right] &= \frac{d_N}{d_M} \mathrm{tr}\left[\varphi^{\otimes M} \Pi_M (\varphi^{\otimes N} \otimes \mathbb{1}) \Pi_M\right] \\
&= \frac{d_N}{d_M} \mathrm{tr}\left[\underbrace{\Pi_M \varphi^{\otimes M} \Pi_M}_{=\varphi^{\otimes M}} (\varphi^{\otimes N} \otimes \mathbb{1})\right] \\
&= \frac{d_N}{d_M} \mathrm{tr}\left[\underbrace{\varphi^{\otimes M} (\varphi^{\otimes N} \otimes \mathbb{1})}_{=\varphi^{\otimes M}}\right] \\
&= \frac{d_N}{d_M}
\end{aligned}$$

$\Rightarrow F(T) = \frac{d_N}{d_M} \geq 1 - \frac{Kd}{N}$ for $M = N + K$.

These results are due to Werner [PRA 58, 1827 (1998)]
arXiv: quant-ph/9804001

§ 8.3 Further results on approximate cloning

·) The approximate cloning map

$$T(\rho) = \frac{d_N}{d_M} \Pi_M \left(\rho \otimes \mathbb{1}^{\otimes M-N}\right) \Pi_M \qquad (*)$$

is the unique cloning map achieving $F(T) = \frac{d_N}{d_M}$.

·) The fidelity $F(T) = \inf_{|\psi\rangle} F\left(\psi^{\otimes M}, T(\psi^{\otimes N})\right)^2$ measures

the quality of the full output state, which includes

correlations between different systems.

We might only be interested in comparing single copies

→ can we find a better map in this case?

Interestingly, the answer is no:

The cloning map (*) is also optimal for the

single-copy worst-case fidelity

$$F_s(T) = \inf_{|\psi\rangle} F\left(\psi, \mathrm{tr}_{[M]\setminus\{1\}} T(\psi^{\otimes N})\right)$$

[Keyl, Werner, J. Math. Phys. 40 (1999)]
arXiv: quant-ph/9807010

- There are asymmetric cloning machines for which the single-copy fidelities on different sites are not necessarily equal. → hard to obtain optimality results in general.
- There are also state-dependent approximate cloning protocols that exploit some known structure in the state to be cloned.
- An important application of approximate cloning is in quantum cryptography, specifically quantum key distribution (QKD). Here, a set of eavesdropping attacks can be described and analyzed using the approximate cloning framework, which leads to security proofs for QKD.

More information on quantum cloning:

Scarani et al., Quantum cloning, arXiv: quant-ph/0511088