Math 595 Representation-theoretic methods in QIT

Approximate cloning

Felix Leditzky

Fall term 2025

Last update: November 11, 2025

The no-cloning theorem

Cloning unknown quantum systems is impossible

No-cloning theorem

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

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

for arbitrary $|\psi\rangle \in \mathcal{H}_{\mathcal{A}}$. Here $|0\rangle_B$ is some reference state.

Proof.

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

$$U(|\psi\rangle_A \otimes |0\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B \qquad U(|\varphi\rangle_A \otimes |0\rangle_B) = |\varphi\rangle_A \otimes |\varphi\rangle_B.$$

Then,

$$\langle\psi|\varphi\rangle^2 = (\langle\psi| \otimes \langle\psi|)(|\varphi\rangle \otimes |\varphi\rangle) = (\langle\psi| \otimes \langle 0|)U^\dagger U(|\varphi\rangle \otimes |0\rangle) = \langle\psi|\varphi\rangle,$$

which shows that $\langle\psi|\varphi\rangle$ must be either 0 and 1. Hence, there is no unitary U that achieves $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle^{\otimes 2}$ for all $|\psi\rangle$. □

Cloning unknown quantum systems is impossible

The no-cloning theorem shows that classical and quantum information are **fundamentally different**.

Classical information can be cloned and thus replicated arbitrarily, while this is impossible for quantum information.

There is a generalization of the no-cloning theorem to mixed states and general quantum channels, commonly called the “no-broadcasting theorem” [Bar+96].

Approximate cloning machines

Approximate cloning

Setup

Given: d-dim. Hilbert space $\mathcal{H}$ and N copies of an unknown state $|\psi\rangle \in \mathcal{H}$.

Goal: Produce an approximation of M copies of ψ for some $M > N$.

Figure of merit: Let T be the approximate cloning map, $T : \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$.

We define the *worst case fidelity*

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

where we used the fact that $F(|\phi\rangle\langle\phi|, \rho)^2 = \langle\phi|\rho|\phi\rangle = \mathrm{tr}\,(|\phi\rangle\langle\phi|\rho)$.

Bound on worst-case fidelity [Wer98]

Define $d_N \coloneqq \dim \mathrm{Sym}^N(\mathcal{H}) = \binom{d+N-1}{N}$. For any cloning map $T : \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$,

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

Proof of worst-case fidelity bound

Proof in lecture notes and given in lecture.

Optimal approximate cloning map

The fidelity bound in the lemma is achieved by the following map:

$$T_{\text{opt}}(X) = \frac{d_N}{d_M} \Pi_M \left(X \otimes \mathbb{1}_d^{\otimes M-N}\right) \Pi_M.$$

The action of this map on $X \in \mathcal{L}(\mathcal{H}^{\otimes N})$ consists of the following three steps:

Step 1. Extend state trivially from $\mathcal{H}^{\otimes N}$ to $\mathcal{H}^{\otimes M}$.
Step 2. Project down to symmetric subspace $\text{Sym}^M(\mathcal{H})$.
Step 3. Normalize to get a quantum state.

T_{opt} achieves the fidelity bound [Wer98]

$$F(T_{\text{opt}}) = \binom{d+N-1}{N}\binom{d+M-1}{M}^{-1} \geq 1 - \frac{Kd}{N}$$

This bound shows that, for $N, M \to \infty$ with $K = M - N$ fixed, approximate cloning becomes possible with the worst-case fidelity $F(T)$ arbitrarily close to 1.

Optimal approximate cloning map

T_{opt} achieves the fidelity bound [Wer98]

$$F(T_{\mathrm{opt}}) = \binom{d+N-1}{N}\binom{d+M-1}{M}^{-1} \geq 1 - \frac{Kd}{N}$$

Proof.

$$\begin{aligned}
\mathrm{tr}\left[\varphi^{\otimes M} T_{\mathrm{opt}}(\varphi^{\otimes N})\right] &= \frac{d_N}{d_M}\mathrm{tr}\left[\varphi^{\otimes M}\Pi_M(\varphi^{\otimes N}\otimes \mathbb{1})\Pi_M\right] \\
&= \frac{d_N}{d_M}\mathrm{tr}\left[\Pi_M\varphi^{\otimes M}\Pi_M(\varphi^{\otimes N}\otimes \mathbb{1})\right] \\
&= \frac{d_N}{d_M}\mathrm{tr}\left[\varphi^{\otimes M}(\varphi^{\otimes N}\otimes \mathbb{1})\right] \qquad \text{since } \varphi^{\otimes M} \text{ is fully supported on } \mathrm{Sym}^M \\
&= \frac{d_N}{d_M}.
\end{aligned}$$

Therefore, with $K = M - N$, we have $F(T) = \frac{d_N}{d_M} \geq 1 - \frac{Kd}{N}$. □

Average fidelity criterion

We chose the *worst-case fidelity*

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

for our analysis of approximate cloning in this section. An alternative criterion is the *average fidelity*

$$F_{\text{avg}}(T) = \int d\psi \, F(\psi^{\otimes n}, T(\psi^{\otimes N}))^2,$$

where $d\psi$ denotes the measure on pure states induced by the Haar measure on $\mathcal{U}_d$. Evidently, we have $F(T) \leq F_{\text{avg}}(T)$ for every map T, and hence the worst-case fidelity is a stronger approximation criterion than the average fidelity.

However, a similar proof as for the worst-case fidelity shows that we also have

$$F_{\text{avg}}(T) \leq d_N / d_M$$

for every map $T : \mathcal{L}(\mathcal{H}^{\otimes N}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$ (exercise), and hence the map $T_{\text{opt}}(X) = \frac{d_N}{d_M} \Pi_M \left(X \otimes \mathbb{1}_d^{\otimes M-N} \right) \Pi_M$ is also optimal for the weaker average fidelity criterion.

Further results on approximate cloning

1. The approximate cloning map T_{opt} is actually the *unique* cloning map achieving $F(T) = \frac{d_N}{d_M}$ [Wer98].
2. The worst-case fidelity $F(T) = \inf_{|\psi\rangle} F(\psi^{\otimes M}, T(\psi^{\otimes N}))^2$ measures the quality of the full output state, which includes correlations between different systems. However, in applications we might only be interested in comparing *single copies*; can we find a better map in this case? Interestingly, the answer is no. As proved in [KW99], the cloning map T_{opt} is also optimal for the *single-copy worst-case fidelity*

$$F_S(T) = \inf_{|\psi\rangle} F\left(\psi, \operatorname{tr}_{2\ldots M} T(\psi^{\otimes N})\right).$$

3. There are *asymmetric cloning* machines for which the single-copy fidelities on different sites are not necessarily equal. Because of the generality of this setting it is hard to obtain optimality results as in [Wer98; KW99].

Further results on approximate cloning

4. There are also *state-dependent approximate cloning* protocols that exploit some known structure in the state to be cloned; see for example [KC22].
5. 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 can be used to obtain security proofs for QKD. This connection between cryptography and approximate cloning is explained further in the comprehensive review article [Sca+05] on quantum cloning.

References

[Bar+96] Howard Barnum et al. **"Noncommuting Mixed States Cannot Be Broadcast".** *Physical Review Letters* 76 (15 Apr. 1996), pp. 2818–2821. arXiv: quant-ph/9511010.

[KC22] Chloe Kim and Eric Chitambar. **"Process-optimized phase-covariant quantum cloning".** *Physical Review A* 106 (2 Aug. 2022), p. 022405. arXiv: 2107.03042 [quant-ph].

[KW99] M. Keyl and R. F. Werner. **"Optimal cloning of pure states, testing single clones".** *Journal of Mathematical Physics* 40.7 (July 1999), pp. 3283–3299. arXiv: quant-ph/9807010.

[Sca+05] Valerio Scarani et al. **"Quantum cloning".** *Reviews of Modern Physics* 77 (4 Nov. 2005), pp. 1225–1256. arXiv: quant-ph/0511088.

[Wer98] R. F. Werner. **"Optimal cloning of pure states".** *Physical Review A* 58 (3 Sept. 1998), pp. 1827–1832. arXiv: quant-ph/9804001.