Quantum Cyber Security
Lecture 7: Intro to Quantum Information V: Entropies and Distances

Petros Wallden

University of Edinburgh

3rd February 2026

This Lecture

- How close are two quantum states: Fidelity and Trace-Distance
- Elements of classical information theory: Shannon Entropy
- Elements of quantum information theory: Von Neumann Entropy

How Close are Two Quantum States?

- Quantify how close the output of a protocol is to ideal
- The ideal protocol has some security property
- Can use this in security proofs:

  If the output state is close enough to the ideal, it is impossible for an adversary to extract more information from the real execution than the distance of the ideal/real states.

1. Fidelity: Measures closeness of two states (unit means states are the same, zero means they are orthogonal)
2. Trace-distance: Measures how distinct two states are (unit means that they are orthogonal, zero means they are the same)

Fidelity

Fidelity (intuitively): Given two quantum states ρ_1, ρ_2, what is the probability that given the one we "confuse" it for the other.

- Pure States: It should depends on the angle between the two vectors: $F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|) = |\langle\psi_1|\psi_2\rangle|^2$
- One Pure State: $F(|\psi_1\rangle\langle\psi_1|, \rho_2) = \langle\psi_1|\rho_2|\psi_1\rangle$
  We will use these expressions in general

Fidelity

Fidelity (intuitively): Given two quantum states ρ_1, ρ_2, what is the probability that given the one we "confuse" it for the other.

- Pure States: It should depends on the angle between the two vectors: $F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|) = |\langle\psi_1|\psi_2\rangle|^2$
- One Pure State: $F(|\psi_1\rangle\langle\psi_1|, \rho_2) = \langle\psi_1|\rho_2|\psi_1\rangle$
  We will use these expressions in general
- General Expression: $F(\rho_1, \rho_2) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right)^2$
  It is also the maximum overlap between purifications

Fidelity

Fidelity (intuitively): Given two quantum states ρ_1, ρ_2, what is the probability that given the one we "confuse" it for the other.

- Pure States: It should depends on the angle between the two vectors: $F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|) = |\langle\psi_1|\psi_2\rangle|^2$
- One Pure State: $F(|\psi_1\rangle\langle\psi_1|, \rho_2) = \langle\psi_1|\rho_2|\psi_1\rangle$
  We will use these expressions in general
- General Expression: $F(\rho_1, \rho_2) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right)^2$
  It is also the maximum overlap between purifications
- Crucially, Fidelity increases by applying a quantum channel (actions cannot increase the distinguishability of two states)

  Caution: Some people (incl N&C book) use different definition (square root fidelity) $F' = \sqrt{F}$

Trace Distance

Trace-Distance (intuitively): Given two states ρ_1, ρ_2, what is the **maximum probability to distinguish** them.

- $T(\rho_1, \rho_2) = \frac{1}{2}\mathrm{Tr}\sqrt{(\rho_1 - \rho_2)^2} = \frac{1}{2}\sum_i |\lambda_i|$ where λ_i are the eigenvalues of the Hermitian (but not positive) matrix $(\rho_1 - \rho_2)$

Trace Distance

Trace-Distance (intuitively): Given two states ρ_1, ρ_2, what is the **maximum probability to distinguish** them.

- $T(\rho_1, \rho_2) = \frac{1}{2}\mathrm{Tr}\sqrt{(\rho_1 - \rho_2)^2} = \frac{1}{2}\sum_i |\lambda_i|$ where λ_i are the eigenvalues of the Hermitian (but not positive) matrix $(\rho_1 - \rho_2)$
- Trace-Distance decreases by applying a quantum channel (actions make states less distinguishabile)
- More useful quantity than Fidelity (e.g. crypto), but harder to compute
- Commonly bounded using known relations with Fidelity

Relations and an example

- **Operational meaning of Trace-Distance**: Is related with the best guessing probability by: $p_{\text{guess}} = \frac{1}{2}(1 + T(\rho_1, \rho_2))$
- **Relation between Fidelity and Trace Distance**

$$1 - \sqrt{F(\rho_1, \rho_2)} \leq T(\rho_1, \rho_2) \leq \sqrt{1 - F(\rho_1, \rho_2)}$$

- **Example**: Bound Trace Distance between $|\psi_1\rangle = |0\rangle$ and $\rho_2 = 1/3\,|0\rangle\langle 0| + 2/3\,|+\rangle\langle +|$

$$F(|\psi_1\rangle, \rho_2) = \langle 0|\,\rho_2\,|0\rangle = 1/3 + 2/3|\langle 0|+\rangle|^2 = 1/3 + 1/3 = 2/3$$

$$0.18 \approx 1 - \sqrt{2/3} \leq T(\psi_1, \rho_2) \leq \sqrt{1/3} \approx 0.58$$

Distance of quantum channels

Diamond Norm: Given two channels $\mathcal{E}, \mathcal{F}$, what is the max probability to distinguish them.

- $$d_\diamond(\mathcal{E},\mathcal{F}) := \|\mathcal{E}-\mathcal{F}\|_\diamond = \max_\rho T(\mathcal{E}\otimes I(\rho), \mathcal{F}\otimes I(\rho))$$
- Find the state ρ that maximises the distance between the output state of the two channels.

Shannon Entropy

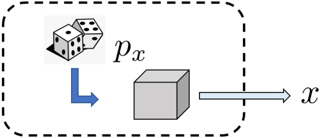
Given a random variable X with outcomes $\{1, 2, ..., N\}$

$$\boxed{H(X) = -\sum_{i=1}^{N} p_i \log p_i; \quad 0 \leq H(X) \leq \log N}$$

- $H(X) = 0$ iff deterministic variable X

  $\exists j$ s.t. $p_j = 1$ and $\forall i \neq j, \; p_i = 0$

- $H(X) = \log N$ for uniform distribution: $\forall i, \; p_i = 1/N$



$H(X)$ quantifies:

- randomness
- uncertainty

Shannon Conditional Entropy

Given two random variables X and Y :

$$H(Y|X) = -\sum_{x,y} p(x,y) \log p(y|x);\ \text{where } p(y|x) = p(x,y)/p(x)$$

- $H(Y|X) = 0$ iff $y = f(x)$
- $0 \leq H(Y|X) \leq H(Y) \leq \log N$

$$\begin{aligned} H(Y|X) &= -\sum_{x,y} p(x,y)(\log p(x,y) - \log p(x)) \\ &= -\sum_{x,y} p(x,y)(\log p(x,y) - \sum_{x} p(x) \log p(x) \\ &= H(X,Y) - H(X) \end{aligned}$$

$H(Y|X)$ quantifies:

Uncertainty of X on Y

- Info X needs to $X \to Y$
- Info Y can keep secret from X

Shannon Mutual Information

Given two random variables X, Y, we define the mutual information :

$$H(X:Y) = -\sum_{x,y} p(x,y) \log \frac{p(x)p(y)}{p(x,y)}$$

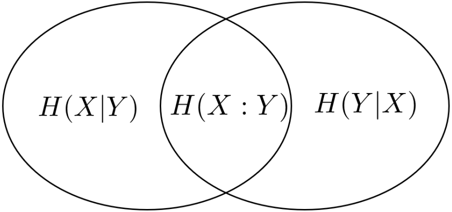
- $0 \leq H(X:Y) \leq \{H(Y), H(X)\} \leq \log N$
- $H(X:Y) = 0$ iff X and Y are independent.

$$\begin{aligned} H(X:Y) &= H(X) + H(Y) - H(X,Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \end{aligned}$$

$H(X:Y)$ quantifies:

- Correlations
- Randomness needed to decorrelate X and Y

Entropic Relations: Venn Diagram



$$H(X,Y) = H(X) + H(Y|X) \qquad H(X) = H(X|Y) + H(X:Y)$$

$$H(X,Y) = H(Y) + H(X|Y) \qquad H(Y) = H(Y|X) + H(X:Y)$$

Classical Information Theory: Summary and Extras

- Shannon Entropy: Average information produced by a random variable: $H(X) = -\sum_i p_i \log p_i$
- Conditional Entropy: The amount of randomness of variable Y given the variable X: $H(Y|X) = H(X,Y) - H(X)$
- Mutual Information: The amount of information obtain from one variable X by observing another one Y: $H(X:Y) = H(X) + H(Y) - H(X,Y) = D_{KL}(P_{(X,Y)} \| P_X \otimes P_Y)$

Classical Information Theory: Summary and Extras

- Shannon Entropy: Average information produced by a random variable: $H(X) = -\sum_i p_i \log p_i$
- Conditional Entropy: The amount of randomness of variable Y given the variable X: $H(Y|X) = H(X,Y) - H(X)$
- Mutual Information: The amount of information obtain from one variable X by observing another one Y: $H(X:Y) = H(X) + H(Y) - H(X,Y) = D_{KL}(P_{(X,Y)} \| P_X \otimes P_Y)$
- Relative Entropy: Measure of how one prob distribution $P(x_i)$ differs from another $Q(x_i)$: $H(P\|Q) = D_{KL}(P\|Q) = \sum_{x_i} P(x_i) \log\left(\frac{P(x_i)}{Q(x_i)}\right)$
- **Notation**: Given a binary variable X: Binary entropy $H(X) := h(p) = -p \log p - (1-p)\log(1-p)$

Von Neumann Entropy: Shannon entropy of eigenvalues

Given a quantum state ρ

$$\boxed{S(\rho) = -\sum_{i=1}^{N} \lambda_i \log \lambda_i = H(\bar{\lambda})}$$

- $S(\rho) = 0$ iff $\rho = |\psi\rangle\langle\psi|$ (pure state)
- $S(\rho) = \log N$ for maximally mixed states: $\rho = I/N$

$S(\rho)$ quantifies:

- purity/mixedness
- quantum information

Quantum Conditional Entropy

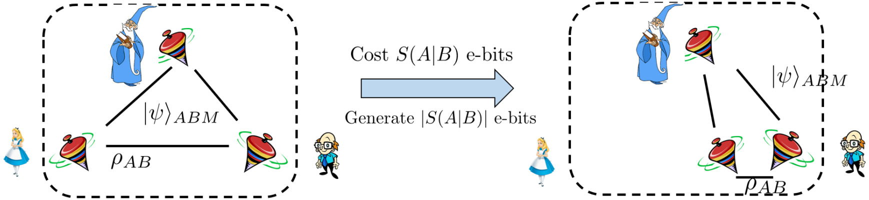
$$S(A|B) = S(A,B) - S(B) = S(\rho_{AB}) - S(\rho_A) = H(\lambda_{AB}) - H(\lambda_A)$$

- $-S(B) \leq S(A|B) \leq S(A)$

$|\psi\rangle_{AB}$ entangled

A and B independent

$S(A|B)$ quantifies: entanglement cost (or generation) of state merging.



Cost $S(A|B)$ e-bits

Generate $|S(A|B)|$ e-bits

Quantum Mutual Information

$$S(A:B) = S(A) + S(B) - S(A,B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

- $0 \leq S(A:B) \leq S(A) + S(B) \leq 2 \log N$

A and B independent

$|\psi\rangle_{AB}$ entangled

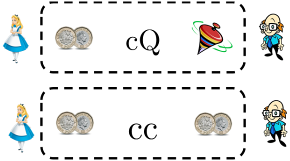
$S(A:B)$ quantifies: classical + quantum correlations

- entanglement assisted classical communication
- randomness needed to decorrelate the two parties

When one register is classical

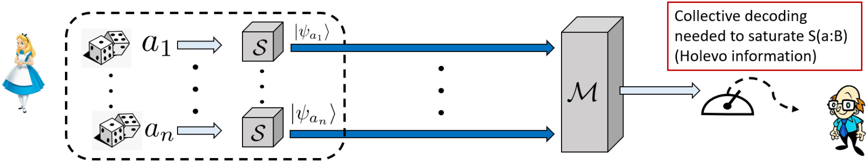
cc-state: $\rho_{ab} = \sum_{a,b} p(a,b)|a\rangle\langle a| \otimes |b\rangle\langle b|$

cQ-state: $\rho_{aB} = \sum_{a} p(a)|a\rangle\langle a| \otimes \rho_{B|a}$



cc-state: $S(a:b) = H(a:b)$

cQ-state: $S(a:B) = S(a) + S(B|a) = H(a) + \sum_{a} p(a)\rho_{B|a}$



Collective decoding needed to saturate S(a:B) (Holevo information)

Quantum Information Theory: Summary and Extras

- Von Neuman Entropy: Quantum version of Shannon Ent:
  $S(\rho) = -\mathrm{Tr}\,(\rho \log \rho)$ (0 for pure, max for totally mixed)
  $S(\rho) = -\sum_i (\lambda_i \log \lambda_i)$ where λ_i the eigenvalues of ρ
- Recall: reduced density matrix $\rho^A := \mathrm{Tr}_B(\rho^{AB})$
- Quantum Conditional Entropy:
  $S(A|B) = S(A, B) - S(B) = \mathrm{Tr}\rho_{AB} \log \rho_{AB} - \mathrm{Tr}\rho_B \log \rho_B$
  $= H(\lambda_{AB}) - H(\lambda_A)$
- Quantum Mutual Information: The relative entropy of a global state from the tensor product of the reduced density matrices:
  $S(A : B) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) = S(\rho^{AB} \| \rho^A \otimes \rho^B)$
  "extra info beyond the product of the reduced matrices"
- Quantum Relative Entropy: $S(\rho_1 \| \rho_2) = \mathrm{Tr}\rho_1(\log \rho_1 - \log \rho_2)$