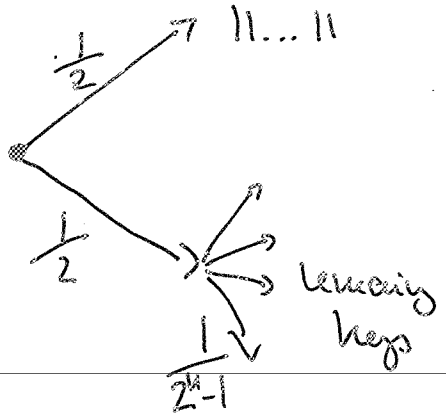
Tutorial exercises

① Differences in entropies

In this exercise, you will explore some fundamental differences of the Shannon/von Neumann entropies and the min-entropy that helps to illustrate why it is the min- and not the Shannon entropy that is used to quantify the security of a cryptographic key.

Imagine an n-bit key k chosen according to the following probability distribution:



$$P_{11\ldots11} = \frac{1}{2}$$

$$P_k = \frac{1}{2} \cdot \frac{1}{2^n - 1} \quad \forall\, k \neq 1\ldots1$$

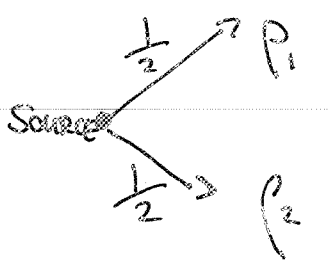
1.1] Do you think this is a secure key? Why/Why not?

1.2] Compute the Shannon entropy $H(k)$ of this key.

1.3] Compute the min-entropy $H_{min}(k)$ of this key. What do you conclude?

(2) Distinguishing quantum states

2.1] Imagine a source that outputs



ie it outputs ρ_1 with probability $\frac{1}{2}$ and ρ_2 with probability $\frac{1}{2}$.

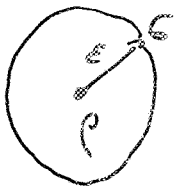
Recall we had claimed that the probability of distinguishing the two states obeys

$$P_{succ} = \frac{1}{2} + \frac{D(\rho_1, \rho_2)}{2}.$$

Prove this claim.

2.2. Imagine that we perform a measurement $\{M_x\}_x$ on a state ρ where outcome "x" occurs with probability $p_x = \mathrm{Tr}(M_x \rho)$

Suppose now that we replace ρ with a state σ in the ε-Ball of ρ, i.e., $D(\sigma, \rho) \leq \varepsilon$.



How much can the probabilities p_x change? I.e. bound $|\mathrm{Tr}(M_x \rho) - \mathrm{Tr}(M_x \sigma)| \leq ?$ for all x.

(3) Smoothing

Suppose a cq-state ρ_{KE} obeys $H_{\min}^{\varepsilon}(K|E)_\rho = \log d_K$ where d_K is the dimension of the register K.

What can you say about the distance $D(\rho_{KE}, \frac{\mathbb{I}_K}{d_K} \otimes \sigma_E)$ for some choice of σ_E?

(3.5) Min-entropy examples.

Compute the min-entropy $H_{min}(A|R)_\rho$ following 3 examples

① $\rho_{AR} = \frac{\mathbb{1}_A}{d_A} \otimes |a\rangle\langle a|_R$ uncorrelated

② $\rho_{AR} = \sum_a p_a \underbrace{|a\rangle\langle a|}_{A} \otimes \underbrace{|a\rangle\langle a|}_{R}$ classically perfectly correlated

③ $\rho_{AR} = |\phi_{AR}\rangle\langle\phi_{AR}|$

$$|\phi_{AR}\rangle = \frac{1}{\sqrt{d_A}} \sum_a |a\rangle|a\rangle$$

maximally entangled

(4) Properties of the min/max entropy

In this exercise, you will prove, and disprove, some basic properties of the min-entropy.

4.1. Show that for all states ρ_{AB}

$$H_{min}(AB) \geq H_{min}(A).$$

4.2. Show that for all states ρ_{ABC}

$$H_{min}(AB|C) \geq H_{min}(A|C).$$

Can you give an intuitive explanation why this should hold when A and B are classical?

4.3. Show that for all states ρ_{AB}

$$H_{min}(A|B) \geq H_{min}(A).$$

***4.4.** It may be tempting to conclude that for all ccq-states $\rho_{X_1X_2E}$ we have

$$H_{min}(X_1X_2|E) \leq H_{min}(X_1|E) + H_{min}(X_2|E)$$

like for the Shannon entropy.

Can you find a counterexample to this claim?
(Hint: Consider X_1 and X_2 to be single bits and E one qubit)

I.e. find a ccq-state such that ⊛ is violated.

4.5. The Shannon entropy is concave. This is often given an intuitive interpretation by stating that "mixing increases entropy".

- Can you imagine why or why not "mixing increases entropy" could be desirable?

- Recall the definition of $H_{max}^{\varepsilon}(A)_\rho = \min_{\sigma \in B^\varepsilon(\rho)} H_{max}(A)_\sigma$

  Find a counterexample showing that H_{max}^{ε} is <u>not</u> concave.

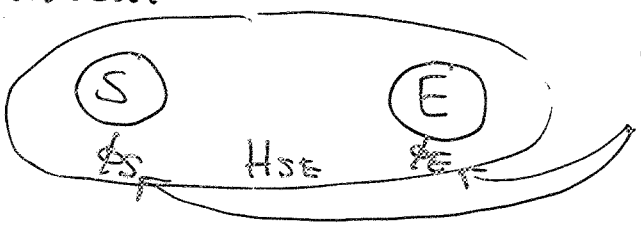
  (Hint: Consider a mixture of the form $\rho = \varepsilon \rho_1 + (1-\varepsilon)\rho_2$)

(5) In recent work (① del Rio, Hutter, Renner, W. and ② Hutter, W.) we have used the decoupling theorem to obtain interesting new results on the foundations of statistical mechanics. In this exercise, you will reproduce some of these!

5.1.) It is well known (Popescu, Linden, Short, Winter '07) that most pure states of the joint Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_E$ of the system S and its environment E are highly entangled, as long as the environment is large enough.

- Write down the decoupling theorem when the reference R is trivial. (ie not there)
- Can you think how we could use the decoupling theorem to prove the result above?

5.2. Imagine again a system and its environment



and an interaction given by the Hamiltonian H_{SE}. One aspect of understanding thermalization is the simple question: Does the state of the system after enough time ever depend on the initial state of the environment? Or does the system retain memory of the initial conditions of E? In the past, people have studied whether the time-averaged state of the system depends on the initial state of E. Armed with the decoupling theorem, we can make statements about the actual state at time t. Recently, we've shown that if the environment is only big enough, then for almost all states of the environment, the system will never depend on it. (Hutter, W.) In this exercise, you will reproduce this result!

- Consider the map

$$\tau_{E\to S}(\rho_E) := \mathrm{Tr}_E\left[U_{SE}(\phi_S \otimes \rho_E)U_{SE}^\dagger\right]$$

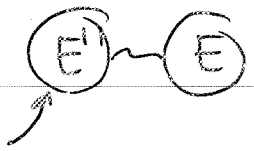
(E: environment, S: system) with $U_{SE} = e^{-iH_{SE}t}$ and ϕ_S pure.

Explain the input and output of this map.

- Let $\tau_{E'S} := (\mathbb{I}_{E'} \otimes \tau_{E\to S})(|\phi_{E'E}\rangle\langle\phi_{E'E}|)$

where $|\phi_{E'E}\rangle = \frac{1}{\sqrt{d_E}}\sum_j |j\rangle_{E'}|j\rangle_E$ is maximally entangled

"copy of E"



Show that

$$\tau_{E'ES} = (\mathbb{I}_{E'} \otimes U_{ES})(|\phi_{E'E}\rangle\langle\phi_{E'E}| \otimes \phi_S)(\mathbb{I}_{E'} \otimes U_{ES}^\dagger)$$

with ϕ_S pure is a purification of $\tau_{E'S}$.

- show that $H_{min}^{\varepsilon}(SE) \geq \log d_E$ for τ_{SE}! ↑ $\tilde{\tau}$

- show that for a trivial reference R and SE initially in the pure state $\phi_S \otimes |0\rangle\langle 0|_E$ the decoupling theorem using the map $\tilde{\tau}_{E\to S}$ and unitaries applied to E predicts

$$\int_{\mathcal{U}(E)} \| \tilde{\tau}_{E\to S}(\mathcal{U}|0\rangle\langle 0|_E \mathcal{U}^\dagger) - \tau_S \|_1 \leq \hat{\varepsilon}$$

where $\hat{\varepsilon} = 2^{-\frac{1}{2}H_{min}^{\varepsilon}(E'|S)_\tau} + R\varepsilon$

(Hint: remember we start in $\phi_S \otimes |0\rangle\langle 0|_E$)

- show that

$$H_{min}^{\varepsilon}(E'|S) \geq \log d_E - \log d_S$$

- prove that if E is large enough, then (on average) most initial states of E will be such that the system never depends on it.

- now instead of averaging, make a probabilistic statement