Exercise 1. *Thermalization through entanglement*

In the lecture we have seen a theorem stating the following:

Let $\mathcal{H}_S \otimes \mathcal{H}_E$ be a bipartite Hilbert space of dimension $d_S \cdot d_E$ and $\mathcal{H}_R \subset \mathcal{H}_S \otimes \mathcal{H}_E$ a subspace (reflecting some constraint on the possible states) of dimension d_R. Define $\mathcal{E}_R = \frac{\mathbb{1}_R}{d_R}$ to be the fully mixed state on the subspace $\mathcal{H}_R$ and the corresponding marginals $\Omega_S = \mathrm{tr}_E[\mathcal{E}_R]$ and $\Omega_E = \mathrm{tr}_S[\mathcal{E}_R]$. Then for a randomly chosen pure state on $\mathcal{H}_R$, $|\phi\rangle \in \mathcal{H}_R$, and arbitrary $\varepsilon > 0$, the distance between the actual reduced state on S, $\rho_S = \mathrm{tr}_E[|\phi\rangle\langle\phi|]$, and the canonical state Ω_S is given probabilistically by

$$P[\, \|\rho_S - \Omega_S\|_1 \geq \eta \,] \leq \eta' \,, \tag{1}$$

where

$$\eta = \varepsilon + \sqrt{\frac{d_S}{d_E^{\mathrm{eff}}}} \,, \quad \eta' = 2e^{-C d_R \varepsilon^2} \,, \quad d_E^{\mathrm{eff}} = \frac{1}{\mathrm{tr}[\Omega_E^2]} \geq \frac{d_R}{d_S} \,, \quad C = \frac{1}{18\pi^3} \,. \tag{2}$$

In applications the environment will be much larger than the system, $d_E \gg d_S$, and $d_R \gg 1$ s.t. both η and η' will be small. Thus the actual state ρ_S will be close to the so called canonical *state Ω_S with high probability.*

(a) *Find a lower bound on d_E^{eff} in terms of $H_{\min}(E)_{\Omega_E}$ and argue why we can set $d_S = 2^{H_{\max}(S)_{\Omega_S}}$. Bound η in terms of ε and the two entropies.*

In the remaining part of this exercise we will explore the above theorem by considering the example of an ensemble of n spin-$\frac{1}{2}$ systems in an external magnetic field B. The field points to the $+z$ direction and the first k spins form the system S while the remaining $n-k$ spins are the environment. The Hamiltonian is

$$H = -\sum_{i=1}^{n} \frac{B}{2} \sigma_z^{(i)} \,, \tag{3}$$

where $\sigma_z^{(i)} = \mathbb{1}_1 \otimes \cdots \otimes \mathbb{1}_{i-1} \otimes \sigma_z \otimes \mathbb{1}_{i+1} \otimes \cdots \otimes \mathbb{1}_n$. We now consider the restriction to the subspace $\mathcal{H}_R \subset \mathcal{H}_S \otimes \mathcal{H}_E$ in which np spins are in the excited state $|1\rangle$ (opposite to the field) and the remaining $n(1-p)$ spins are in the ground state $|0\rangle$. Our goal is to show that $\Omega_S \propto \exp\big(-\frac{H_S}{k_B T}\big)$, where H_S is the Hamiltonian (3) restricted to the first k spins and T is the temperature of the environment according to Boltzmann (see definition below).

(b) *Show that for $n \gg k^2$ the canonical state Ω_S is approximately given by*

$$\Omega_S \approx \big(p|1\rangle\langle 1| + (1-p)|0\rangle\langle 0|\big)^{\otimes k} \,. \tag{4}$$

(c) *Boltzmann's formula relates the entropy of the environment at energy E, $S_E(E)$, to the number of states available at this energy, $N_E(E)$, by $S_E(E) = k_B \ln N_E(E)$. Having an expression for $S_E(E)$ then allows us to find the thermodynamic temperature by means of $\frac{1}{T} = \frac{\mathrm{d}S_E(E)}{\mathrm{d}E}\big|_{E=\langle E\rangle}$. Using Stirling's approximation, find that*

$$\frac{1}{T} \approx \frac{k_B}{B} \ln\left(\frac{1-p}{p}\right) \,. \tag{5}$$

(d) *Use (b) and (c) to show that the canonical state on S approximately fulfils*

$$\Omega_S \propto \exp\left(-\frac{H_S}{k_B T}\right) \,. \tag{6}$$

Solution.

(a) Let $\{\lambda_i\}_i$ be the eigenvalues of Ω_E. The term $\mathrm{tr}[\Omega_E^2] = \sum_i \lambda_i^2$ can be seen as the 'expected' eigenvalue of Ω_E, which is certainly upper bounded by the maximal eigenvalue, $\max_i \lambda_i$. Therefore we have

$$d_E^{\mathrm{eff}} = \mathrm{tr}[\Omega_E]^{-1} = 2^{-\log \sum_i \lambda_i^2} \geq 2^{-\log \max_i \lambda_i} = 2^{H_{\min}(E)}\,, \tag{S.1}$$

as $H_{\min}(E)_{\Omega_E} = -\log \max_i \lambda_i$.

On the other hand, we can always restrict S to be the subspace on which Ω_S has support because, according to the result (1), this is the space of interest (to very good approximation). Therefore, we can set $d_S = |\mathrm{supp}(\Omega_S)| = 2^{H_{\max}(S)}$ as $H_{\max}(S)_{\Omega_S} = \log |\mathrm{supp}(\Omega_S)|$.

In total we find

$$\eta = \varepsilon + \sqrt{\frac{d_S}{d_E^{\mathrm{eff}}}} \leq \varepsilon + 2^{\frac{1}{2}\left(H_{\max}(S) - H_{\min}(E)\right)}\,. \tag{S.2}$$

Importantly, this bound only depends on the canonical states, which arise as a consequence of the (physical) restriction defining $\mathcal{H}_R$.

(b) Before going into the calculation of Ω_S we first use Stirling's approximation, $\ln n! = n \ln n - n + O(\ln n)$, denoted by $^{(*)}$, to show that for large n and $k \ll n$: $(n-k)! \approx n!/n^k$. We have

$$\begin{aligned}\ln(n-k)! &\overset{(*)}{\approx} (n-k)\ln(n-k) - (n-k) = (n-k)\ln n + (n-k)\ln\left(1-\tfrac{k}{n}\right) - n + k \\ &\overset{(*)}{\approx} \ln n! - k\ln n + (n-k)\ln\left(1-\tfrac{k}{n}\right) + k \approx \ln n! - k\ln n + (n-k)\left(-\tfrac{k}{n}\right) + k \\ &= \ln n! - k\ln n + \tfrac{k^2}{n} \approx \ln n! - k \ln n\,,\end{aligned} \tag{S.3}$$

where we used $\frac{k^2}{n} \ll 1$ and $\ln(1-x) \approx x$ for small x together with $\frac{k}{n} \ll 1$. Exponentiating gives the desired approximation.

In the following we use the notation $|\vec{s}\rangle = |s_1\rangle|s_2\rangle\cdots|s_k\rangle$ for $\vec{s} \in \{0,1\}^k$ and define $|\vec{s}| := \sum_i s_i$. We can write the canonical state on S as

$$\Omega_S = \frac{1}{d_R}\sum_{\vec{s}} \binom{n-k}{np-|\vec{s}|} |\vec{s}\rangle\langle\vec{s}|\,, \tag{S.4}$$

where $d_R^{-1} = \binom{n}{np}^{-1}$ stands for normalization and the binomial coefficients arise due to the $n-k$ spins of the environment which can have $np - |\vec{s}|$ excitations if there are $|\vec{s}|$ excitations in S. For fixed p and sufficiently large n (we assume it to be sufficiently large) the approximation (S.3) also applies to

$$(np-|\vec{s}|)! \approx (np)!/(np)^{|\vec{s}|}\,, \quad \text{and} \quad (n(1-p)-(k-|\vec{s}|))! \approx (n(1-p))!/(n(1-p))^{k-|\vec{s}|} \tag{S.5}$$

due to $|\vec{s}|^2 \leq k^2 \ll n$. We therefore find

$$
\begin{aligned}
\Omega_S &\approx \binom{n}{np}^{-1} \sum_{\vec{s}} \frac{n!/n^k}{(np)!/(np)^{|\vec{s}|}\,(n(1-p))!/(n(1-p))^{k-|\vec{s}|}} |\vec{s}\rangle\langle\vec{s}| \\
&= \binom{n}{np}^{-1} \sum_{\vec{s}} \frac{n!}{(np)!(n-np)!} p^{|\vec{s}|}(1-p)^{k-|\vec{s}|}|\vec{s}\rangle\langle\vec{s}| \\
&= \sum_{\vec{s}} p^{|\vec{s}|}(1-p)^{k-|\vec{s}|}|\vec{s}\rangle\langle\vec{s}| \\
&= \big(p|1\rangle\langle 1| + (1-p)|0\rangle\langle 0|\big)^{\otimes k}.
\end{aligned} \tag{S.6}
$$

(c) Let e be the number of excitations in the environment of $n-k$ spins. The average value for e obviously is $(n-k)p$. The logarithm of the number of states in the environment with e excitations reads

$$
\ln N_E(e) = \ln \binom{n-k}{e} \approx (n-k)\ln(n-k) - e\ln e - (n-k-e)\ln(n-k-e)\,, \tag{S.7}
$$

where we again used Stirling's approximation. We now use Boltzmann's formula for the entropy, $S_E(e) = k_B \ln N_E(e)$, to obtain the inverse temperature $\frac{1}{T} = \frac{\mathrm{d}S_E(E)}{\mathrm{d}E}\big|_{E=\langle E\rangle}$, where $E = eB - (n-k)B/2$:

$$
\begin{aligned}
\frac{1}{T} &= \frac{\mathrm{d}S_E(E)}{\mathrm{d}E}\bigg|_{E=\langle E\rangle} = \frac{1}{B}\frac{\mathrm{d}S_E(e)}{\mathrm{d}e}\bigg|_{e=\langle e\rangle} \approx \frac{k_B}{B}\ln\left(\frac{n-k-e}{e}\right)\bigg|_{e=(n-k)p} \\
&= \frac{k_B}{B}\ln\left(\frac{1-p}{p}\right).
\end{aligned} \tag{S.8}
$$

(d) From (b) and (c) we get

$$
\begin{aligned}
\Omega_S &\approx (1-p)^k \sum_{\vec{s}} \left(\frac{p}{1-p}\right)^{|\vec{s}|} |\vec{s}\rangle\langle\vec{s}| = (1-p)^k \sum_{\vec{s}} \exp\left(-|\vec{s}|\ln\left(\frac{1-p}{p}\right)\right)|\vec{s}\rangle\langle\vec{s}| \\
&= (1-p)^k \sum_{\vec{s}} \exp\left(-\frac{|\vec{s}|B}{k_B T}\right)|\vec{s}\rangle\langle\vec{s}| \propto \exp\left(-\frac{H_S}{k_B T}\right).
\end{aligned} \tag{S.9}
$$

Together with the above theorem we learn that in this example on n spins (n sufficiently large), the state of the first k spins is very close to thermal for a typical pure state on the total system with np excitations.

Exercise 2. *One-time Pad*

Consider three random variables: a message M, a secret key K and a ciphertext C. We want to encode M as a ciphertext C using K with perfect secrecy, so that no one can guess the message from the cipher: $I(C:M) = 0$.

After the transmission, we want to be able to decode the ciphertext: someone who knows the key and the cipher should be able to obtain the message perfectly, i.e. $H(M|CK) = 0$.

(a) *Show that this is only possible if the key contains at least as much randomness as the message, namely $H(K) \geq H(M)$.*

(b) *Give an optimal algorithm for encoding and decoding.*

Solution.

(a) First note that

$$\begin{aligned} I(C:M) - I(C:M|K) &= I(M:K) - I(M:K|C) \\ &= I(K:C) - I(K:C|M), \end{aligned} \tag{S.10}$$

and that mutual information is non-negative. We introduce $x = I(C:M|K)$, $y = I(M:K|C)$ and $z = I(K:C|M)$ and, using $I(C:M) = 0$, we get

$$x - I(C;M) = x = y - I(M:K) = z - I(K:C). \tag{S.11}$$

Using the two conditions, we write

$$\begin{aligned} H(M) &= H(M|CK) + I(C:M) + I(K:M|C) = y, \quad \text{and} \\ H(K) &= H(K|MC) + I(M:K) + I(M:C|K) \geq y - x + z. \end{aligned} \tag{S.12}$$

However, since $y \geq x$ and $z \geq x$ (from (S.11)), we get $H(K) \geq H(M)$.

(b) Given a message M of m bits, an optimal encoding algorithm could first compress the message to $H(M)$ bits and then use a secret and completely random binary key of length $H(M)$ to encode it. Given a message bit M_i and a secret code bit K_i, the ciphertext bit would be generated $C_i = M_i \oplus K_i$ using XOR. The decoding would recreate the message bit $M_i = C_i \oplus K_i$ and then decompress it.

This way of encoding is called one-time pad and by showing that $H(K) \geq H(M)$ is necessary we have in particular shown optimality of the one-time pad in terms of the number of used key bits.