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

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

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

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

(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

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

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.