University of California at San Diego – Department of Physics – Prof. John McGreevy

Physics 213 Winter 2023
Assignment 5 – Solutions

Due 11:00am Monday, February 14, 2023

1. **Error rate per bit.** Estimate the probability of failing to decode a message sent through a binary symmetric channel with error rate q per bit, using the Hamming [7,4] code. Note that there is a distinction between the probability of having an error in the decoded string, and an error in a given bit of the message (it doesn't matter if some of the check bits are misconstrued).

   We make an error somewhere in the code block if two or more bits of seven are wrong. There are
   $$\sum_{r=2}^{7} \binom{7}{r} q^r (1-q)^{7-r}$$
   ways for this to happen. This is approximately $21q^2$ when the error rate is small.

   But we actually only care if we get the message bits wrong, so the error rate per bit is somewhat smaller than this. Since the answer is dominated by the two-error case, let's focus on that. If there are two errors, the attempt to decode will result in a third bit being flipped, so there will actually be three wrong bits out of the seven transmitted bits. What's the probability that a given message bit is wrong?

   As we saw in lecture, the [7,4] Hamming code is actually symmetric among its seven outputs. So each bit has probability 3/7 of being one of the three out of seven that is wrong. So the full error rate per bit, for small q, is $\approx 21q^2 3/7 = 9q^2$.

2. **Control-X brainwarmer.**

   Show that the operator control-X can be written variously as
   $$\mathsf{CX}_{BA} = |0\rangle\langle 0|_B \otimes \mathbb{1}_A + |1\rangle\langle 1|_B \otimes \mathbf{X}_A = \mathbf{X}_A^{\frac{1}{2}(1-\mathbf{Z}_B)} = e^{\frac{\mathbf{i}\pi}{4}(1-\mathbf{Z}_B)(1-\mathbf{X}_A)}.$$

   $\frac{1}{2}(1-\mathbf{Z}) = |1\rangle\langle 1|$ is the projector onto $\mathbf{Z} = -1$. Therefore $\mathbf{Z}_B = e^{\mathbf{i}\pi\frac{1}{2}(1-\mathbf{Z}_B)}$ and similarly $\mathbf{X}_A = e^{\mathbf{i}\pi\left(\frac{1-\mathbf{X}_A}{2}\right)}$. $\mathbf{X}_A$ and $\mathbf{Z}_B$ commute, so we can move them around each other however we want.

3. **Density matrix exercises.**

(a) Show that the most general density matrix for a single qbit lies in the Bloch ball, *i.e.* is of the form

$$\boldsymbol{\rho}_v = \frac{1}{2}\left(\mathbb{1} + \vec{v}\cdot\vec{\boldsymbol{\sigma}}\right), \quad \sum_i v_i^2 \leq 1.$$

Find the determinant, trace, and von Neumann entropy of $\boldsymbol{\rho}_v$.

The general hermitian 2x2 matrix is $a_0\mathbb{1} + \vec{a}\cdot\vec{\sigma}$. Unit trace says $a_0 = \frac{1}{2}$. Positivity will impose a condition on the $\vec{a}$.

All these questions are basis independent, so if we wish we can rotate the basis to set $\vec{v} = v_z\hat{z}$ without changing the answers. The det is

$$\det \boldsymbol{\rho}_v = \frac{1}{4}(1 - v^2)$$

with $v^2 \equiv \sum_i v_i^2$ and the eigenvalues are

$$\frac{1}{2}\left(1 \pm \sqrt{v^2}\right) \equiv \frac{1}{2}\left(1 \pm v\right).$$

so that one becomes negative when $v^2 \geq 1$; this is the origin of the constraint on the length of the polarization vector. Pure states have $v^2 = 1$ so that the eigenvalues are $(1,0)$. The vN entropy is just the binary entropy with $p = \frac{1}{2}(1+v)$:

$$S(\boldsymbol{\rho}_v) = -\mathrm{tr}\boldsymbol{\rho}_v \log \boldsymbol{\rho}_v = \frac{1}{2}(1+v)\log\frac{1}{2}(1+v) + \frac{1}{2}(1-v)\log\frac{1}{2}(1-v).$$

(b) A single qbit state has $\langle \mathbf{X} \rangle = s$. Find the most general forms for the corresponding density operator with the minimum and maximum von Neumann entropy. (Hint: the Bloch ball is your friend.)

[This problem is from Barnett] Use the parametrization from the previous part. Then the constraint is $s = \langle \mathbf{X} \rangle_\rho = \mathrm{tr}\boldsymbol{\rho}\mathbf{X} = v_x$. The vN entropy of $\boldsymbol{\rho}_v$ is then

$$S(\boldsymbol{\rho}_v) = H_2\left(\frac{1+\sqrt{v^2}}{2}\right) = H_2\left(\frac{1+\sqrt{s^2+v_{yz}^2}}{2}\right) = f(v_{yz}^2 \equiv v_y^2 + v_z^2).$$

We wish to extremize this over the allowed set of v_y, v_z, which is $0 \leq v_y^2+v_z^2 \leq 1-s^2$. In this range (for $s^2 \in [0,1]$), the function is monotonically decreasing so the max is when $0 = v_y^2+v_z^2$ and the min is when $v_y^2+v_z^2 = 1$ (pure state).

(c) Show that the *purity* of a density matrix $\pi[\boldsymbol{\rho}] \equiv \mathrm{tr}\boldsymbol{\rho}^2$ satisfies $\pi[\boldsymbol{\rho}] \leq 1$ with saturation only if $\boldsymbol{\rho}$ is pure.

Use the spectral decomposition.

(d) Show from the definition that the quantum relative entropy satisfies the following

$$D(\boldsymbol{\rho}_A \otimes \boldsymbol{\rho}_B || \boldsymbol{\sigma}_A \otimes \boldsymbol{\sigma}_B) = D(\boldsymbol{\rho}_A || \boldsymbol{\sigma}_A) + D(\boldsymbol{\rho}_B || \boldsymbol{\sigma}_B). \tag{1}$$

$$\sum_i p_i D(\boldsymbol{\sigma}_i || \boldsymbol{\rho}) = \sum_i p_i D(\boldsymbol{\sigma}_i || \boldsymbol{\sigma}_{\mathrm{av}}) + D(\boldsymbol{\sigma}_{\mathrm{av}} || \boldsymbol{\rho}) \tag{2}$$

$$D(\boldsymbol{\sigma}_{\mathrm{av}} || \boldsymbol{\rho}) \leq \sum_i p_i D(\boldsymbol{\sigma}_i || \boldsymbol{\rho}) \tag{3}$$

for any probability distribution $\{p_i\}$ and density matrices $\boldsymbol{\rho}, \boldsymbol{\sigma}_i$, and where $\boldsymbol{\sigma}_{\mathrm{av}} \equiv \sum_i p_i \boldsymbol{\sigma}_i$.

4. **Thermal density matrix.** Suppose given a Hamiltonian H. In lecture we showed that the thermal density matrix $\boldsymbol{\rho}_T \equiv \frac{e^{-\frac{H}{k_B T}}}{Z}$ has the maximum von Neumann entropy S_{vN} of any state with the same expected energy. Show that if instead we are given a fixed temperature T, the thermal density matrix minimizes the free energy functional

$$F_T[\boldsymbol{\rho}] \equiv \mathrm{tr}\boldsymbol{\rho} H - T S_{vN}[\boldsymbol{\rho}].$$

The relative entropy between $\boldsymbol{\rho}$ and $\boldsymbol{\rho}_T$ is

$$0 \leq D(\boldsymbol{\rho}||\boldsymbol{\rho}_T) = \mathrm{tr}\boldsymbol{\rho}\log\boldsymbol{\rho} - \mathrm{tr}\boldsymbol{\rho}\log\frac{e^{-\frac{H}{k_B T}}}{Z} = \mathrm{tr}\boldsymbol{\rho}\log\boldsymbol{\rho} + \frac{\log e}{k_B T}\mathrm{tr}\boldsymbol{\rho}H + \log Z = \frac{\log e}{k_B T}\left(F_T[\boldsymbol{\rho}] - F_T[\boldsymbol{\rho}_T]\right)$$

which says

$$F_T[\boldsymbol{\rho}_T] \leq F_T[\boldsymbol{\rho}].$$

5. **Distinguishability of distributions.** Suppose we sample N times a distribution P on a binary variable with $(p_0, p_1) = (p, 1-p)$. What is the probability that we mistake the distribution for Q with probabilities $(q, 1-q)$?

Hint: the expected number of zeros $\langle n_0 \rangle_P$ is Np. The probability that we get it wrong is the probability that we get Nq zeros instead. Show that

$$\mathrm{Prob}(n_0 = Nq|P) \simeq 2^{-ND(Q||P)}$$

where $D(Q||P)$ is the relative entropy, and the approximation is Stirling's.

$$P(\text{number of zeros} = Nq|P) = \binom{N}{Nq} p^{Nq}(1-p)^{N-Nq} \tag{4}$$

$$\overset{\text{Stirling}}{\simeq} 2^{-N(q\log q-(1-q)\log(1-q)+q\log p+(1-q)\log(1-p))} = 2^{-ND(q||p)}. \tag{5}$$