Fall 2023 QIC 820 / CO 781/486 / CS 867 Assignment 4

Due 5pm Friday Nov 24, 2023, on Crowdmark.

Question 1. AEP and source coding (classical) (5/18 marks)

Let X be a binary random variable with sample space $\Omega = \{0, 1\}$, with $p(0) = 0.995$, $p(1) = 0.005$.

(a) (1 mark) Consider a block of 100 iid samples of this rv, $X_1, X_2, \cdots, X_{100}$. How many outcomes have (i) zero 1's? (ii) one 1, (iii) two 1's, and (iv) three 1's?

(b) (1 mark) Consier a coding scheme $\mathcal{E}$ which acts on 100 iid samples of the rv X at a time, outputing an error symbol e if there are more than 3 1's, and assigning a unique binary string to other 100-bit strings. How many bits are required to represent the outcome of $\mathcal{E}$?

(c) (3 marks) If we now treat each outcome of $\mathcal{E}$ as a new random variable, and perform data compression by transmitting only typical sequences, how many bits per outcome of $\mathcal{E}$ are needed? (Note the symbol E also has to be transmitted.)

Question 2. Entanglement concentration (7/18 marks)

Suppose Alice and Bob share $|\psi\rangle^{\otimes n}$, that is, n copies of the state

$$|\psi\rangle = \sqrt{a}\,|00\rangle + \sqrt{1-a}\,|11\rangle$$

where $a \in [0, 1]$, and the first qubit belongs to Alice, and the second to Bob. Denote Alice's n-qubit system by $A = A_1 \otimes A_2 \otimes \cdots \otimes A_n$, Bob's n-qubit system $B = B_1 \otimes \cdots \otimes B_n$.

Both Alice and Bob have the same reduced state $\rho^{\otimes n}$ where $\rho = a|0\rangle\langle 0| + (1-a)|1\rangle\langle 1|$.

Let $H(a) = -a \log a - (1-a)\log(1-a)$ (the binary entropy function) which is also $S(\rho)$ here. (We use capitalized H here because lower case h labels the Hamming weight later.)

The goal is to show that for large n, *approximately* $nH(a)$ ebits can be obtained with local operations and no communication.

For an n-bit string x^n, denote the hamming weight by $h(x^n)$, which is the number of 1's in x^n.

For $k \in \{1, \cdots, n\}$, let $S_k = \text{span}\{|x^n\rangle : h(x^n) = k\}$, and Π_k be the projector onto S_k.

Define a measurement with POVM $\{\Pi_0, \Pi_1, \cdots, \Pi_n\}$ (and denote the corresponding outcome by the subscript).

(a) (2 marks) Show that Alice and Bob always get the same outcome. What is the probability they both get k?

(b) (1 mark) Write down the *normalized* state $|\Phi_k\rangle$ conditioned on both Alice and Bob obtaining outcome k. Note that it is maximally entangled.

(c) (2 marks) Show that the *expected* entropy of entanglement in the post-measurement state is $H(X^n|K)$ where K is the random variable associated with Alice's measurement outcome.

(iv) (1 mark) Show that $H(X^n|K) \geq nH(a) - \log(n+1)$.

(v) (1 mark) Why is communication not needed?

NB. The expression for the *expected* number of ebits is $\sum_{k=0}^{n} \binom{n}{k} a^{n-k}(1-a)^k \log \binom{n}{k}$. It is not so easy to lower bound directly.

NB To simplify the question, we ignore the possibility that the postmeasurement maximally entangled states need not have dimension which is a power of 2. This costs only a slight reduction in the yield.

NB The binary X can be generalized, and the final answer has $H(X)$ in place of $H(a)$, log(number of type classes) instead of $\log(n+1)$. See QIC 890 / CO781 / CS 867 F2020 A2 for details.

Question 3. Necessary condition for separability (6/18 marks)

(a) (3 marks) Let $\rho = \sum_{a \in \Gamma} p(a)\, \sigma_a \otimes \xi_a \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$, where $\forall a \in \Gamma, \sigma_a \in \mathrm{D}(\mathcal{X})$ and $\xi_a \in \mathrm{D}(\mathcal{Y})$.

Show that $S(\mathrm{XY}) \geq S(\mathrm{X}) + \sum_{a \in \Gamma} p(a)\, S(\xi_a)$.

(Note in particular, $S(\mathrm{XY}) \geq S(\mathrm{X})$, which does not hold for a general entangled state.)

(b) (2 marks) In general, does $S(\mathrm{XY}) \geq S(\mathrm{X})$ imply that XY is in a separable state? Justify your answer.

(c) (1 mark) Show that for 3 systems in an arbitrary state, $S(XY{:}Z) \leq S(X{:}YZ) + S(Y{:}Z)$.

(Note that the above expresses how much the quantum mutual information across a bipartition can be increased when a system is moved from one side to the other; in particular, $S(XY{:}Z) \leq S(X{:}YZ) + 2S(Y)$.)