CO 781 Assignment 1, Spring 2010, due May 24th in class.

Question 1. On data compression [20 marks]

We use the notation defined for the asymptotic equipartition theorem in p9-10 in the notes for lecture 1. Let X be the biased coin toss with $p(0) = 1/9$ and $p(1) = 8/9$.

(a) Using Chebyshev's inequality in the analysis, (i) if we're to compress n iid draws to about $0.75n$ bits and err with probability less than 1%, state a block length n_0 above which data compression works? (ii) If instead there are 500 bits available, and we want to keep the 1% error probability, how many draws can be stored?

(b) In this example, Hoeffding's inequality can be used instead of Chebyshev's inequality. It says that $\Pr\left(\left|\frac{1}{n}\sum_i Y_i - \mathbb{E}Y\right| \geq \epsilon\right) \leq 2\exp(-\frac{2n\epsilon^2}{(b-a)^2})$ where a, b are lower and upper bounds to the random variable Y. Exp is exponentiation to power 2. Redo both parts in (a).

Question 2. On CNOT and SWAP [20 marks]

In the computation basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, the CNOT and SWAP gates are defined respectively by:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1}$$

We view them as communication resources between Alice and Bob who can each choose an input qubit (can be part of an entangled state) and receive the qubit output. For example, If Alice inputs $|a\rangle$ for $a = 0, 1$ and Bob inputs $|0\rangle$ in CNOT, the outputs are $|a\rangle|a\rangle$ and a classical bit is transmitted from Alice to Bob. We will find out how much resources they can generate, and what are the costs of simulating them. We denote the ability to transmit one classical bit from Alice to Bob by $\text{cbit}_\rightarrow$, and that from Bob to Alice by $\text{cbit}_\leftarrow$, and similarly for coherent classical bit and qubit transmission.

(a) Show that $\text{qbit}_\rightarrow + \text{qbit}_\leftarrow \geq$ SWAP (i.e., show that there is a protocol consuming the LHS to produce the resources on the RHS.) Note that this protocol is 1-shot.

(b) Show that $n\ \text{qbit}_\rightarrow + n\ \text{qbit}_\leftarrow \leq (n+1)$ SWAP, where on the LHS, we assume that Alice and Bob take turns to send one qubit, and repeat n times. Thus asymptotically, as $n \rightarrow \infty$, we obtain, on average, $\text{qbit}_\rightarrow + \text{qbit}_\leftarrow \leq$ SWAP.

So asymptotically, $\text{qbit}_\rightarrow + \text{qbit}_\leftarrow =$ SWAP, or $2\ \text{cobit}_\rightarrow + 2\ \text{cobit}_\leftarrow =$ SWAP + 2 ebit

(c) Show that $\text{cobit}_\rightarrow + \text{cobit}_\leftarrow \geq$ CNOT + 1 ebit

Hint: there is a method to perform a remote CNOT between 2 parties due to Gottesman (see quant-ph/9807006 p18 or 0002039 p16 (C2)) using one ebit, 1 cbit→, and 1 cbit← in 1-shot (if you don't want to invent it from scratch). (quant-ph/XXYYZZZ can be accessed at http://arxiv.org/abs/quant-ph/XXYYZZZ.) Check that using cobits instead of cbits, you can regenerate 2 ebits in the end of the protocol. Using one of these newly generated ebits in the next remote CNOT etc, asymptotically, the above resource inequality holds on average.

(d) Show that $\text{cobit}_\rightarrow + \text{cobit}_\leftarrow \leq$ CNOT + 1 ebit (Hint: next page)

This shows $\text{cobit}_\rightarrow + \text{cobit}_\leftarrow =$ CNOT + 1 ebit

Therefore, 2 CNOT = SWAP asymptotically.

Note that in 1-shot, we can use 3 CNOTS to make up a SWAP (by running them in alternating directions) but it is also possible to prove that 2 CNOTS and local operations cannot simulate a SWAP). We found in quant-ph/0205057 by elementary methods that the SWAP has every capacity of interest twice that of the CNOT, and eventually the concept of cobits and the above analysis explained that.

Hint: what is $(H \otimes I)$ CNOT $(\sigma_x^a \otimes \sigma_z^b)$ $(|00\rangle + |11\rangle)$ where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard gate?