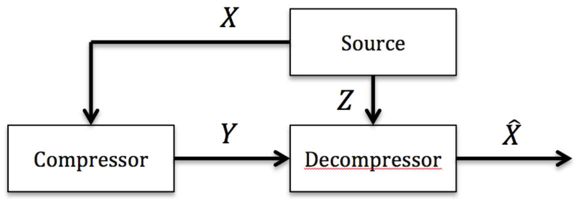
Quantum Information Theory
Series 4

HS 13
Dr. J.M. Renes

In this exercise sheet we will consider an extension of direct source coding that includes side information. Now, the source produces the random message X, as well as some side information Z, that may be correlated to X. If the side information is directly available during decompression, it can be used to increase the efficiency of decompression.



Exercise 4.1 Direct source coding theorem with side information

Prove that, given side information, the minimum length of the encoded message l^ϵ can be bounded by

$$l^\epsilon(X) \leq H_{\max}(X|Z) + \log\frac{1}{\epsilon} + 1$$

Use the proof for the standard source coding theorem from the lecture as reference.

The error is upper-bounded by the probability that a randomly chosen compressor maps a two letters of the input alphabet to the same letter. We only need to consider the inputs with non-zero probability, so there is an extra condition which introduces the dependence of the error on Z:

$$\begin{aligned} P_{err} &\leq \sum_{x\in\mathcal{X}} P_{X,Z}[x,z] P[\exists x' \neq x : \mathrm{comp}(x') = \mathrm{comp}(x), x' \in \mathrm{supp}\, P_{X|Z=z}] \\ &\leq \sum_{x,z} P_{X,Z}[x,z] \sum_{x'\neq x : x' \in \mathrm{supp}\, P_{X|Z}} P[\mathrm{comp}(x') = \mathrm{comp}(x)]. \end{aligned}$$

Take the expected value over all possible compressors. Given a uniform distribution of compressors, any letter x' will be mapped all letters of the output alphabet with equal probability. The probability that x' will be compressed to a fixed letter of the alphabet $comp(x)$ is exactly $\frac{1}{2^l}$, where $|\mathcal{Y}| = 2^l$ is the length of the output alphabet.

$$\begin{aligned} \langle P_{err} \rangle_{\mathrm{comp}} &\leq \sum_{x,z} P_{X,Z}[x,z] \sum_{x'\neq x : x' \in \mathrm{supp} P_{X|Z}} \frac{1}{2^l} \\ &\leq \sum_{x,z} P_{X,Z}[x,z] \frac{|\mathrm{supp} P_{X|Z=z}|}{2^l} \\ &\leq 2^{H_{\max}(X|Z)_P - l}. \end{aligned}$$

The last inequality comes from the definition of $H_{\max}$. Notice that all the different supports are weighted by different probabilities, but $H_{\max}(X|Z) = -\max_z |\mathrm{supp} P_{X|Z=z}|$.

Choosing the above l ensures ϵ error, and corrects for l being a discrete variable.

Exercise 4.2 Converse for i.i.d sources with side information

Given an i.i.d source with side information Z, it may be possible to compress the message better than without Z. Therefore, it is not possible to lower-bound the compressibility by $H(X)$ any more. Modify the proof given in the lecture to show that the compressibility with side information can be lower-bounded by $C(X|Z) \geq H(X|Z)$

In the Fano inequality the entropy is conditioned on all information known at the decoding stage. Originally it is just the encoded message Y, but now it is also the side information. Also, now we consider words of length n, so the size of the alphabet is $|\mathcal{X}|^N$, and the Fano inequality becomes $\epsilon_n \geq \frac{H(X^{\times n}|YZ^{\times n})-1}{n\log|\mathcal{X}|}$, where $\epsilon_n = P[\hat{X}^{\times n} \neq X^{\times n}]$. Rearranging that, we obtain

$$\begin{aligned}
\epsilon_n n\log|\mathcal{X}| + 1 &\geq H(X^{\times n}|YZ^{\times n}) \\
&= H(X^{\times n}Y|Z^{\times n}) - H(Y|Z^{\times n}) \\
&= H(Y|X^{\times n}Z^{\times n}) + H(X^{\times n}|Z^{\times n}) - H(Y|Z^{\times n}) \\
&= H(X^{\times n}|Z^{\times n}) - H(Y|Z^{\times n}) \\
&\geq H(X^{\times n}|Z^{\times n}) - \log|\mathcal{Y}| \\
&= nH(X|Z) - \log|\mathcal{Y}|.
\end{aligned}$$

Assuming that there exists a protocol with $\lim_{n\to\infty}\epsilon_n = 0$, the capacity becomes

$$\begin{aligned}
C(X|Z) &= \lim_{n\to\infty}\frac{1}{n}\log|\mathcal{Y}| \\
&\geq \lim_{n\to\infty} H(X|Z) - \epsilon_n\log|\mathcal{X}| - \frac{1}{n} \\
&= H(X|Z).
\end{aligned}$$