Data-Processing Inequality

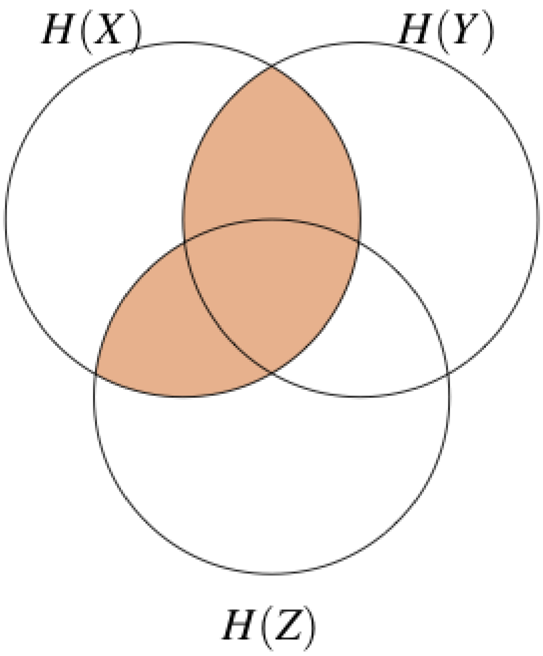
The whispering game in the example on the previous page exhibits an important property of Markov chains: you can only lose information down the line. Charlie's final message C does not contain any more information about Alice's original message A than what was already contained in Bob's message B. This observation is formalized in the following theorem:

Theorem: Data-processing inequality

If $X \to Y \to Z$, then $I(X;Y) \geq I(X;Z)$. Equality holds if and only if $I(X;Y|Z) = 0$.

Proof

The following entropy diagram depicts the area $I(X;YZ)$:



From the diagram, we can see that

$$I(X;Z) + I(X;Y|Z) = I(X;YZ) = I(X;Y) + I(X;Z|Y).$$

Combining this with part (c) of the proposition on the last page, it follows that

$$I(X;Z) + I(X;Y|Z) = I(X;Y).$$

Since $I(X;Y|Z) \geq 0$, the result follows: $I(X;Z) \leq I(X;Y)$, with equality iff $I(X;Y|Z) = 0$.

The following corollary formalizes the intuition that the mutual information between two random variables can only decrease by post-processing any of the two.

Corollary

$I(X;Y) \geq I(X;g(Y))$ for any two random variables X and Y, and any function g on the range of Y.

Paste proof here