CS3235 Tutorial for week 6 (Sept 17-Sept 21, 2007)

September 13, 2007

Present your answer (on paper) to the following tutorial question at the beginning of the tutorial session.

1 (To be handed in). In the discussion on entropy and transmission rate, the received data was corrupted 50% of the time, with each bit of input data being inspected and then either being changed (flipped), or not, with a probability of 0.5. Consider the case where the bit is forced to a 1, or not, with a probability of 0.5. Does this change the situation? Justify your intuition about this by re-working the entropy calculation for $r(X)$.

Please come to the tutorial ready to present your answers to these questions as well:

2 (Do not hand in). Let $X$ represent a 2-bit string that can have the values 00 (= 0), 01 (= 1), 10 (= 2) or 11 (= 3) with equal probability, and then assume that this string is corrupted by a signal, giving a result $Y$.

(a) if the corruption signal sets each bit to a 1 with probability 50%, calculate $p(X = 1 \mid Y \geq 1)$ (The probability that $X$ was 01 given that $Y$ is now greater than or equal to 01, i.e. it is 01 = 1, 10 = 2 or 11 = 3).

(b) if the corruption signal flips each bit with probability 50%, calculate $p(X = 1 \mid Y \geq 1)$ (The probability that $X$ was 01 given that $Y$ is now greater than or equal to 01, i.e. it is 01 = 1, 10 = 2 or 11 = 3).

3 (Do not hand in). What is the unicity distance of the one-time pad? Justify your reasoning using the unicity distance equation.

4 (Do not hand in). (Intuition/readings) Please read sections 1, 2 and 10 of Shannon’s paper at http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf Explain in your own words the import of the “necessary and sufficient condition for perfect secrecy” described in Section 10.