CPSC 418/MATH 318 Practice Problems

Probability, Entropy and Perfect Secrecy

Recall that a *random variable* X consists of a finite collection of *outcomes* $X_1, X_2, \ldots, X_n$and a *probability distribution* $p(X_1), p(X_2), \ldots, p(X_n)$ such that $0 \leq p(X_i) \leq 1$ for $1 \leq i \leq n$ and $\sum_{i=1}^{n} p(X_i) = 1$. The *entropy* of X is $H(X) = \sum_{\substack{i=1 \\ p(X_i)>0}}^{n} p(X_i) \log_2 \left(\frac{1}{p(X_i)} \right)$.

Recall also that a crytosystem provides *perfect secrecy* if $p(M|C) = p(M)$ for all plaintexts M and ciphertexts C with $p(C) > 0$. By Bayes' Theorem, this is equivalent to $p(C|M) = p(C)$ for all plaintexts M and ciphertexts C with $p(M) > 0$ and $p(C) > 0$.

1. Consider a six-faced die whose faces have respective colours red, red, red, blue, blue, green.
   (a) Describe the random variable (i.e. possible outcomes and probability distribution) of a fair die throw (i.e. one where each face ends up on top with equal likelihood).
   (b) What is the entropy of the random variable of part (a)?
   (c) Suppose two identical such dice are thrown simultaneously. What is the probability that
      i. both dice come up red?
      ii. the dice come up red and blue?
      iii. the dice come up red and some colour other than red?

2. Consider a cryptosystem with plaintext space $\mathcal{M} = \{X, YZ\}$, ciphertext space $\mathcal{C} = \{a, b, c, d\}$ and key space $\mathcal{K} = \{k_1, k_2, k_3\}$ that is given by the following encryption table:

Key	X	Y	Z
k_1	a	b	c
k_2	a	c	d
k_3	b	d	a

   Suppose each key is chosen with equal likelihood. Suppose also that message Y occurs half the time and messages X and Z each occur 25% of the time.

   (a) For all $C \in \mathcal{C}$ and all $M \in \mathcal{M}$, compute $p(C|M)$.
   (b) For all $C \in \mathcal{C}$, compute $p(C)$.
   (c) Does this system provide perfect secrecy?
   (d) Compute the entropy $H(\mathcal{K})$ of the key space.
   (e) Compute the entropy $H(\mathcal{C})$ of the ciphertext space.

3. Consider a cryptosystem with plaintext space $\mathcal{M} = \{X, Y\}$, ciphertext space $\mathcal{C} = \{a, b, c, d\}$ and key space $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$ that is given by the following encryption table:

Key	X	Y
k_1	a	b
k_2	c	d
k_3	b	a
k_4	d	c

   Suppose messages and keys are equidistributed, i.e. each message occurs with probability 1/2 and each key with probability 1/4.

   (a) Prove that ciphertexts are equidistributed.
   (b) Prove that this system provides perfect secrecy.