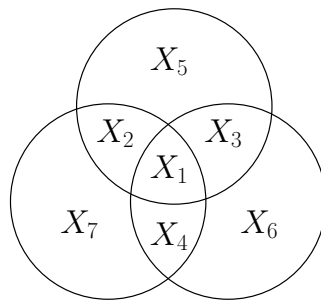


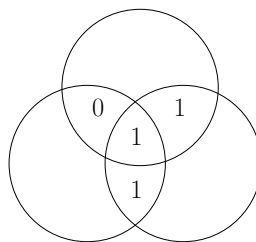
Homework Set #1

1. Entropy of Hamming Code.

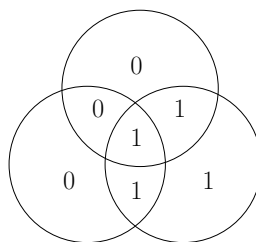
Consider information bits $X_1, X_2, X_3, X_4 \in \{0, 1\}$ chosen at random, and check bits X_5, X_6, X_7 chosen to make the parity of the circles even.



Thus, for example,



becomes



That is, 1011 becomes 1011010.

(a) What is the entropy of $H(X_1, X_2, \dots, X_7)$?

Now we make an error (or not) in one of the bits (or none). Let $\mathbf{Y} = \mathbf{X} \oplus \mathbf{e}$, where \mathbf{e} is equally likely to be $(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$, or $(0, 0, \dots, 0)$, and \mathbf{e} is independent of \mathbf{X} .

(b) What is the entropy of \mathbf{Y} ?

(c) Suppose $\mathbf{Y} = 0101110$. Given that 1 or fewer errors were made, what is (X_1, X_2, X_3, X_4) ?

(d) What is $H(\mathbf{X}|\mathbf{Y})$?

(e) What is $I(\mathbf{X}; \mathbf{Y})$?

2. Entropy of functions of a random variable.

Let X be a discrete random variable. Show that the entropy of a function of X is less than or equal to the entropy of X by justifying the following steps:

$$\begin{aligned} H(X, g(X)) &\stackrel{(a)}{=} H(X) + H(g(X)|X) \\ &\stackrel{(b)}{=} H(X). \\ H(X, g(X)) &\stackrel{(c)}{=} H(g(X)) + H(X|g(X)) \\ &\stackrel{(d)}{\geq} H(g(X)). \end{aligned}$$

Thus $H(g(X)) \leq H(X)$.

3. Functions.

(a) Let $Y = X^5$, where X is a random variable taking on positive and negative integer values. What is the relationship of $H(X)$ and $H(Y)$?

(b) What if $Y = X^2$?

(c) What if $Y = \tan X$?

4. Mutual information of heads and tails.

(a) Consider a fair coin flip. What is the mutual information between the top side and the bottom side of the coin?

(b) A 6-sided fair die is rolled. What is the mutual information between the top side and the bottom side?

(c) What is the mutual information between the top side and the front face (the side most facing you)?

5. **Bytes.**

The entropy, $H_a(X) = -\sum p(x) \log_a p(x)$ is expressed in bits if the logarithm is to the base 2 and in bytes if the logarithm is to the base 256. What is the relationship of $H_2(X)$ to $H_{256}(X)$?

6. **Coin weighing.**

Suppose one has n coins, among which there may or may not be one counterfeit coin. If there is a counterfeit coin, it may be either heavier or lighter than the other coins. The coins are to be weighed by a balance.

- (a) Count the number of states the n coins can be in, and count the number of outcomes of k weighings. By comparing them, find an upper bound on the number of coins n so that k weighings will find the counterfeit coin (if any) and correctly declare it to be heavier or lighter.
- (b) (*Difficult and optional.*) What is the coin weighing strategy for $k = 3$ weighings and 12 coins?

7. **Entropy of time to first success.**

A fair coin is flipped until the first head occurs. Let X denote the number of flips required.

- (a) Find the entropy $H(X)$ in bits. The following expressions may be useful:

$$\sum_{n=1}^{\infty} r^n = r/(1-r), \quad \sum_{n=1}^{\infty} nr^n = r/(1-r)^2.$$

- (b) Find an “efficient” sequence of yes-no questions of the form, “Is X contained in the set S ?” Compare $H(X)$ to the expected number of questions required to determine X .
- (c) Let Y denote the number of flips until the second head appears. Thus, for example, $Y = 5$ if the second head appears on the 5th flip. Argue that $H(Y) = H(X_1 + X_2) < H(X_1, X_2) = 2H(X)$, and interpret in words.

8. **Example of joint entropy.**

Let $p(x, y)$ be given by

	Y	
X	0	1
0	$\frac{1}{3}$	$\frac{1}{3}$
1	0	$\frac{1}{3}$

Find

- (a) $H(X), H(Y)$.
- (b) $H(X|Y), H(Y|X)$.
- (c) $H(X, Y)$.
- (d) $H(Y) - H(Y|X)$.
- (e) $I(X; Y)$.
- (f) Draw a Venn diagram for the quantities in (a) through (e).

9. Two looks.

Here is a statement about pairwise independence and joint independence. Let X, Y_1 , and Y_2 be binary random variables. If $I(X; Y_1) = 0$ and $I(X; Y_2) = 0$, does it follow that $I(X; Y_1, Y_2) = 0$?

- (a) Yes or no?
- (b) Prove or provide a counterexample.
- (c) If $I(X; Y_1) = 0$ and $I(X; Y_2) = 0$ in the above problem, does it follow that $I(Y_1; Y_2) = 0$? In other words, if Y_1 is independent of X , and if Y_2 is independent of X , is it true that Y_1 and Y_2 are independent?

10. A measure of correlation.

Let X_1 and X_2 be *identically distributed*, but not necessarily independent. Let

$$\rho = 1 - \frac{H(X_2|X_1)}{H(X_1)}.$$

- (a) Show $\rho = \frac{I(X_1; X_2)}{H(X_1)}$.
- (b) Show $0 \leq \rho \leq 1$.
- (c) When is $\rho = 0$?
- (d) When is $\rho = 1$?