**CS181A Notes #1**

**Entropy** Let $\Sigma$ be a finite set (alphabet) of size $n$. Consider a probability distribution $P$ defined over $\Sigma$. When the context is clear, we identify $\Sigma$ with $[n] = \{1, 2, \ldots, n\}$. A coding scheme $C$ is an assignment of binary sequences to each symbol in $\Sigma$. Thus, $C$ is a mapping from $\Sigma$ to $\{0, 1\}^\star$. Given a symbol $\sigma \in \Sigma$, the code length of $C(\sigma)$ is the length of that binary sequence, denoted by $|C(\sigma)|$. A source $X$ is a random variable whose value is in $\Sigma$. The *average code length* of coding scheme $C$ for $X$ is given by

$$L_X(C) = \mathbb{E}|C(X)| = \sum_{i=1}^{n} P(X = i)\ |C(i)|.$$

Let the entropy function $\mathbb{H}(P)$ of a probability distribution $P$ be defined as

$$\mathbb{H}(P) = -\sum_{i=1}^{n} P(i) \log_2 P(i).$$

The entropy of a random variable is equivalent to the entropy of its underlying distribution. Some basic facts about entropy is given below:

1. If $|\mathcal{X}| = n$ then $\mathbb{H}(X) \leq \log_2 n$.
2. (Additive law) $\mathbb{H}(X, Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$ (equality iff $X$ and $Y$ are independent).
3. (Conditional law) $\mathbb{H}(X, Y) = \mathbb{H}(X) + \mathbb{H}(Y|X)$.
4. (Conditioning reduces entropy) $\mathbb{H}(X|Y) \leq \mathbb{H}(X)$ (equality iff $X$ and $Y$ are independent).

Note that the conditional entropy $\mathbb{H}(X|Y = y)$ is defined as the entropy of $X$ over the conditional distribution $\mathbb{P}[X|Y = y]$. The conditional entropy $\mathbb{H}(X|Y)$ is then defined as the average over $y$ of $\mathbb{H}(X|Y = y)$.

Shannon proved the following beautiful lower bound for any coding scheme (no matter how clever).

**Theorem 1.** *(Shannon) Given any coding scheme $C$ for a source $X$, its average code length cannot be strictly smaller than the entropy of the source. Namely,*

$$\min_C L_X(C) \geq \mathbb{H}(X).$$

**Remark 1.** *The four entropic laws above follows from* Jensen's Inequality*: For any concave function $f$, we have*

$$\mathbb{E}[f(X)] \leq f(\mathbb{E}[X]). \tag{1}$$

**Remark 2.** *The Huffman coding scheme satisfies $L_X(\text{HUFFMAN}) \leq \mathbb{H}(X) + 1$.*

**Exercise 1.** *Determine the entropy of English. Find a natural language with the highest entropy. What about the highest redundancy?*

**Cryptosystem** A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$, where $\mathcal{P}$ is the plaintext space, $\mathcal{K}$ is the key space, $\mathcal{C}$ is the ciphertext space, $\mathcal{E}$ is the space of all encryption algorithms and $\mathcal{D}$ is the space of all decryption algorithms. Let $P$ be a prior distribution over $\mathcal{P}$ (prior knowledge of attacker) and let $K$ be distribution over the key space (corresponds to the random choice of secret keys). We assume also a choice of encryption and decryption algorithms over a collection of possible alternatives. This induces a distribution $C$ over the ciphertext space. In what follows, let $X$, $K$ (abuse of notation), $Y$ be random variables denoting the plaintext, key and ciphertext, respectively. Also, let $e$ and $d$ be the particular choice of algorithms used for encryption and decryption.

**Definition 1.** *A cryptosystem achieves* perfect secrecy *if*

$$\mathbb{P}[X = x | Y = y] = \mathbb{P}[X = x]. \tag{2}$$

By Bayes's law, perfect secrecy is equivalent to

$$\mathbb{P}[X = x | Y = y] = \frac{\mathbb{P}[Y = y | X = x]\mathbb{P}[X = x]}{\mathbb{P}[Y = y]}. \tag{3}$$

So, we achieve perfect secrecy if

$$\mathbb{P}[Y = y | X = x] = \mathbb{P}[Y = y]. \tag{4}$$

**Exercise 2.** *Confirm that the One-Time Pad protocol has perfect secrecy.*

Let $L$ be a language over $\mathcal{P}^\star$. So, $L$ is the set of all finite strings over the alphabet $\mathcal{P}$. Let $P^n$ denote the distribution induced by $P$ on $\mathcal{P}^n$. The *entropy* of $L$ is defined as

$$H_L = \lim_{n \to \infty} \frac{\mathbb{H}(P^n)}{n}. \tag{5}$$

The *redundancy* of $L$ is defined as

$$R_L = 1 - \frac{H_L}{\log_2 |\mathcal{P}|}. \tag{6}$$

Note that a random language has zero redundancy.

Given a ciphertext $y \in \mathcal{C}^n$, the set of possible keys for $y$ is defined as

$$K(y) = \{k \in \mathcal{K} : \exists x \in \mathcal{P}^n \text{ with } \mathbb{P}[X = x] > 0 \text{ and } e_k(x) = y\}. \tag{7}$$

Given a ciphertext $y$, a key is called *spurious* if it is a possible but incorrect key. The number of spurious keys given the ciphertext $y$ is $|K(y)| - 1$. Let $s_n$ be the average of the number of spurious keys over different values of $y$. Thus,

$$s_n = \mathbb{E}[|K(Y)| - 1] = \mathbb{E}[|K(Y)|] - 1. \tag{8}$$

**Claim 1.**

$$\mathbb{H}(K|C^n) = \mathbb{H}(K) + \mathbb{H}(P^n) - \mathbb{H}(C^n). \tag{9}$$

Note that

$$\begin{aligned} \mathbb{H}(C^n) &\leq n \log_2 |\mathcal{C}| & (10) \\ \mathbb{H}(P^n) &\cong nH_L = n(1 - R_L) \log_2 |\mathcal{P}|. & (11) \end{aligned}$$

For simplicity, assume the plaintext and ciphertext spaces are of the same size, that is, $|\mathcal{P}| = |\mathcal{C}|$. Thus,

$$\mathbb{H}(K|C^n) \geq \mathbb{H}(K) - nR_L \log_2 |\mathcal{P}|. \tag{12}$$

Moreover,

$$\mathbb{H}(K|C^n) = \mathbb{E}[\mathbb{H}(K|Y)] \leq \mathbb{E}[\log_2 |K(Y)|] \leq \log_2 \mathbb{E}[|K(Y)|] = \log_2(s_n + 1). \tag{13}$$

Thus, assuming the uniform distribution on the keyspace, we get

$$nR_L \log_2 |\mathcal{P}| \geq \log_2 |\mathcal{K}| - \log_2(s_n + 1). \tag{14}$$

The *unicity distance* of a cryptosystem is a value $\hat{n}$ so that $s_{\hat{n}} = 0$. Using the previous inequality, we get

$$\hat{n} \cong \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}. \tag{15}$$

# A Entropy proofs

For brevity, we use the following shorthands:

$$\begin{aligned} p(a) &= \Pr[X = a] \\ p(b) &= \Pr[Y = b] \\ p(a,b) &= \Pr[X = a, Y = b] \\ p(a|b) &= \Pr[X = a | Y = b] \end{aligned}$$

**Theorem 2.** *$Ent(X) \leq \log_2 |A|$, where $X$ ranges over $A$.*

*Proof.* By the definition of $\mathbb{H}(X)$, we have

$$\mathbb{H}(X) = \sum_{a \in A} p(a) \log(1/p(a)) \leq \log \sum_{a} 1 = \log |A|,$$

where the inequality follows from Jensen's inequality. □

**Theorem 3.** $\mathbb{H}(X, Y) = \mathbb{H}(X|Y) + \mathbb{H}(Y)$.

*Proof.* By the definition of $\mathbb{H}(X, Y)$, we have

$$\begin{aligned} \mathbb{H}(X,Y) &= \sum_{a,b} p(a,b) \log \frac{1}{p(a,b)} \\ &= \sum_{a,b} p(a,b) \left[ \log \frac{1}{p(a|b)} + \log \frac{1}{p(b)} \right] \\ &= \sum_{a,b} p(a,b) \log \frac{1}{p(a|b)} + \sum_{a,b} p(a,b) \log \frac{1}{p(b)} \\ &= \sum_{b} p(b) \sum_{a} p(a|b) \log \frac{1}{p(a|b)} + \sum_{b} p(b) \log \frac{1}{p(b)} \sum_{a} p(a|b) \\ &= \sum_{b} p(b) \mathbb{H}(X|Y=b) + + \sum_{b} p(b) \log \frac{1}{p(b)} \\ &= \mathbb{H}(X|Y) + \mathbb{H}(Y). \end{aligned}$$

□

**Theorem 4.** $\mathbb{H}(X|Y) \leq \mathbb{H}(X)$.

*Proof.* We show that $\mathbb{H}(X|Y) - \mathbb{H}(X) \leq 0$.

$$\begin{aligned}
\mathbb{H}(X|Y) - \mathbb{H}(X) &= \sum_b p(b)\mathbb{H}(X|Y=b) - \sum_a p(a) \log \frac{1}{p(a)} \\
&= \sum_b p(b) \sum_a p(a|b) \log \frac{1}{p(a|b)} - \sum_a p(a) \log \frac{1}{p(a)} \\
&= \sum_{a,b} p(a,b) \log \frac{1}{p(a|b)} - \sum_a p(a) \log \frac{1}{p(a)} \sum_b p(b|a) \\
&= \sum_{a,b} p(a,b) \left[ \log \frac{1}{p(a|b)} - \log \frac{1}{p(a)} \right] \\
&= \sum_{a,b} p(a,b) \log \frac{p(a)}{p(a|b)} = \sum_{a,b} p(a,b) \log \frac{p(a)p(b)}{p(a,b)} \\
&\leq \log \sum_{a,b} p(a)p(b) = \log 1 = 0.
\end{aligned}$$

□

**Theorem 5.** $\mathbb{H}(X,Y) \leq \mathbb{H}(X) + \mathbb{H}(Y)$.

*Proof.* Since $\mathbb{H}(X,Y) = \mathbb{H}(X|Y) + \mathbb{H}(Y)$ and $\mathbb{H}(X|Y) \leq \mathbb{H}(X)$, the claim holds. □