T-79.5501 Cryptology

Lecture 2
January 29, 2008

Kaisa Nyberg

Entropy

- **Definition 2.4** Suppose $\mathbf{X}$ is a discrete random variable which takes on values from a finite set $X = \{x_1, x_2, \ldots, x_n\}$ with probability distribution $p_i = \mathbf{Pr}[\mathbf{X} = x_i]$, $i = 1, 2, \ldots, n$. Then, the entropy of $\mathbf{X}$ is defined to be the quantity

$$H(\mathbf{X}) = -\sum_{i=1}^{n} p_i \log_2 p_i.$$

- If $p_i = 0$, then we take $p_i \log_2 p_i = 0$.
- Let $\mathbf{X}$ be a *binary* random variable that takes on only two values 0 or 1, that is, $X = \{0, 1\}$, and denote $p = \mathbf{Pr}[0]$. Then

$$H(\mathbf{X}) = -p \log_2 p - (1-p) \log_2 (1-p).$$

Properties of Entropy

- The following theorem states that the maximum entropy is achieved if the probability distribution is uniform.
- **Theorem 2.6** Let $\mathbf{X}$ be as in the definition above. Then $H(\mathbf{X}) \leq \log_2 n$, with equality if and only if $p_i = 1/n$, for all $i = 1, 2, \ldots, n$.
- For the proof see textbook.
- **Theorem 2.7** Let $\mathbf{X}$ and $\mathbf{Y}$ be discrete random variables. Then

$$H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y}),$$

  with equality if and only if $\mathbf{X}$ and $\mathbf{Y}$ are independent.
- For the proof see textbook.

Conditional Entropy

- **Definition 2.6** Suppose $\mathbf{X}$ and $\mathbf{Y}$ are two discrete random variables which takes on values from a finite set X and Y, respectively. Then for any fixed $y \in Y$, we get a *conditional* probability distribution on X and we denote the associated random variable by $\mathbf{X}|y$. Then

$$H(\mathbf{X}|y) = -\sum_{x \in X} \mathbf{Pr}[x|y] \log_2 \mathbf{Pr}[x|y].$$

- We define the *conditional entropy*, denoted by H($\mathbf{X|Y}$) to be the weighted average of $H(\mathbf{X}|y)$ over the values y of $\mathbf{Y}$, computed as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} \mathbf{Pr}[y] \mathbf{Pr}[x|y] \log_2 \mathbf{Pr}[x|y].$$

Properties of Conditional Entropy

- Suppose $\mathbf{X}$ and $\mathbf{Y}$ are two discrete random variables which take on values from a finite set X and Y, respectively. Then
- $H(\mathbf{X},\mathbf{Y}) = H(\mathbf{X}) + H(\mathbf{Y}|\mathbf{X})$ and $H(\mathbf{X},\mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$
- $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$

Cryptosystem

- **Definition 1.1** A *cryptosystem* is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

  1. $\mathcal{P}$ is a finite set of possible *plaintexts*;
  2. $\mathcal{C}$ is a finite set of possible *ciphertexts*;
  3. $\mathcal{K}$, the *keyspace*, is a finite set of possible *keys*;
  4. For each $K \in \mathcal{K}$, there is an *encryption rule* $e_k \in \mathcal{E}$ and a corresponding *decryption rule* $d_k \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every plaintext $x \in \mathcal{P}$.

Stochastic Model of Cryptosystem

- $\mathbf{P}$ is a random variable that takes on values in $\mathcal{P}$;
- $\mathbf{C}$ is a random variable that takes on values in $\mathcal{C}$; and
- $\mathbf{K}$ is a random variable that takes on values in $\mathcal{K}$.
- **Assumption:** $\mathbf{P}$ and $\mathbf{K}$ are independent random variables.
- As $e_K(x) = y$ for $x \in \mathcal{P}$ and $K \in \mathcal{K}$, the probability distributions of $\mathbf{P}$ and $\mathbf{K}$ induce the probability distribution of $\mathbf{C}$.
- In a cryptosystem the random variable $\mathbf{C}$ is not independent of $\mathbf{P}$ and $\mathbf{K}$.

Entropies Related to a Cryptosystem

- Total entropy:

$$H(\mathbf{P},\mathbf{C},\mathbf{K}) = H(\mathbf{C},\mathbf{K}) = H(\mathbf{P},\mathbf{K}) = H(\mathbf{P}) + H(\mathbf{K})$$

- Entropy of $\mathbf{K}$ and $\mathbf{C}$:

$$H(\mathbf{K},\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{C}|\mathbf{K}) \leq H(\mathbf{K}) + H(\mathbf{C})$$

- It follows that $H(\mathbf{P}) \leq H(\mathbf{C})$. In a good cryptosystem, $H(\mathbf{P}) \ll H(\mathbf{C})$.

- Theorem 2.10 states that

$$H(\mathbf{C}) - H(\mathbf{P}) = H(\mathbf{K}) - H(\mathbf{K}|\mathbf{C})$$

.

Perfect Secrecy

- A cryptosystem achieves perfect secrecy if $\mathbf{Pr}(x|y) = \mathbf{Pr}(x)$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$. It means that a cryptosystem achieves perfect secrecy if and only if $\mathbf{P}$ and $\mathbf{C}$ are independent random variables.
- **Shannon's Pessimistic Inequality** If a cryptosystem achieves perfect secrecy, then $H(\mathbf{P}) \leq H(\mathbf{K})$.
- *Proof.* In a cryptosystem, we have

$$H(\mathbf{C})+H(\mathbf{P}|\mathbf{C}) = H(\mathbf{P},\mathbf{C}) \leq H(\mathbf{P},\mathbf{C},\mathbf{K}) = H(\mathbf{C},\mathbf{K}) \leq H(\mathbf{C})+H(\mathbf{K}).$$

- It follows that $H(\mathbf{P}|\mathbf{C}) \leq H(\mathbf{K})$. The claim follows from this when we observe that if the cyptosystem achieves perfect secrecy, then $H(\mathbf{P}|\mathbf{C}) = H(\mathbf{P})$ as $\mathbf{P}$ and $\mathbf{C}$ are independent.

Perfect Secrecy - Theorem 2.4

- **Theorem 2.4** Assume that $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. Then a cryptosystem achieves perfect secrecy if and only if the following conditions are satisfied:
  1. Keys are chosen equiprobably, i.e., from uniform distribution; and
  2. for each pair (x, y), $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key $K \in \mathcal{K}$ such that $e_K(x) = y$.
- For the proof that (1) and (2) are necessary, see the textbook. Here we give an alternative proof of sufficiency.
- **Corollary** One-time pad cryptosystem achieves perfect secrecy.

Conditions 1 and 2 imply perfect secrecy

- Assume that (1) and (2) hold. We express the properties in terms of entropy:
- (1) means that $H(\mathbf{K}) = \log_2 n$, where $n = |\mathcal{K}|$.
- (2) means that $H(\mathbf{K}|\mathbf{P},\mathbf{C}) = 0$. Then $H(\mathbf{P},\mathbf{C},\mathbf{K}) = H(\mathbf{P},\mathbf{C})$. On the other hand, $H(\mathbf{P},\mathbf{C},\mathbf{K}) = H(\mathbf{P},\mathbf{K})$ always. Hence

$$\begin{aligned} H(\mathbf{P},\mathbf{C}) &= H(\mathbf{P},\mathbf{K}) \\ H(\mathbf{C}) + H(\mathbf{P}|\mathbf{C}) &= H(\mathbf{P}) + H(\mathbf{K}).\ (*) \end{aligned}$$

- By (1) and $|\mathcal{C}| = n$, we get $H(\mathbf{K}) = \log_2 n \geq H(\mathbf{C})$.
- Then by $(*)$, $H(\mathbf{P}|\mathbf{C}) \geq H(\mathbf{P})$, and therefore H($\mathbf{P}|\mathbf{C}$) = H($\mathbf{P}$), which holds if and only if $\mathbf{P}$ and $\mathbf{C}$ are independent random variables.

Redundancy of a Natural Language

- A language consists of finite strings of characters drawn (not necessarily independently from each other) from an alphabet. Suppose L is a (natural) language with alphabet $\mathcal{P}$. Let $\mathbf{P}^n$ denote the random variable which takes on values on strings of length n, for $n = 1, 2, \ldots$.

- **Definition 2.7** The *entropy* of L is defined to be the quantity

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

The *redundancy* of L is defined to be

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

Redundancy of a Natural Language, cont'd

- The quantity $H(\mathbf{P}^n)$ is the entropy of n-letter strings of L. Divided by n we get the average entropy per letter in an n-letter string. Hence H_L is the average entropy per letter in L.
- $\log_2 |\mathcal{P}|$ is the maximum entropy in one letter of the language. The quantity $H_L/\log_2 |\mathcal{P}|$ measures the relative entropy in one letter. It takes on values between 0 and 1. Hence redundancy R_L measures how big proportion of the language is redundant.
- Let L be the English language. Then $H_L \approx 1.4$. The maximum entropy of 26 letter alphabet is $\log_2 26 \approx 4.7$. Then $R_L = 1 - 1.4/4.7 \approx 0.7$, that is, the English language is about 70% redundant.

Unicity distance

- Assume a string of n letters of a language L with alphabet $\mathcal{P}$ and redundancy R_L have been encrypted using the same key K in a cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$. Assume that $|\mathcal{P}| = |\mathcal{C}|$. By Thm 2.10 we have

$$H(\mathbf{K}) - H(\mathbf{K}|\mathbf{C}^n) = H(\mathbf{C}^n) - H(\mathbf{P}^n). \ (*)$$

- We estimate the righthand side by

$$n\log_2|\mathcal{C}| - nH_L = n\log_2|\mathcal{P}| - n(1-R_L)\log_2|\mathcal{P}| = nR_L\log_2|\mathcal{P}|$$

assuming that the ciphertext is uniformly distributed (as it should be for a good cipher).

Unicity distance, cont'd

- When n is large enough such that the right hand side of (*) is equal to $H(\mathbf{K})$, then $H(\mathbf{K}|\mathbf{C}^n) = 0$, that is, there is no uncertainty about the key any more. If the keys are chosen equiprobably this happens when

$$\log_2 |\mathcal{K}| = nR_L \log_2 |\mathcal{P}|,$$

that is, when

$$n \geq \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}.$$

- This bound is called the *unity distance* of the cryptosystem for language L.