Shannon's Theory of Secrecy Systems

See:

C. E. Shannon,
Communication Theory of Secrecy Systems, Bell Systems Technical Journal,
Vol. 28, pp. 656–715, 1948.

Notation

Given a cryptosystem, denote

$\boldsymbol{M}$ a message (plaintext)

$\boldsymbol{C}$ a ciphertext

$\boldsymbol{K}$ a key

$\boldsymbol{E}$ be the encryption function $\boldsymbol{C = E_K(M)}$

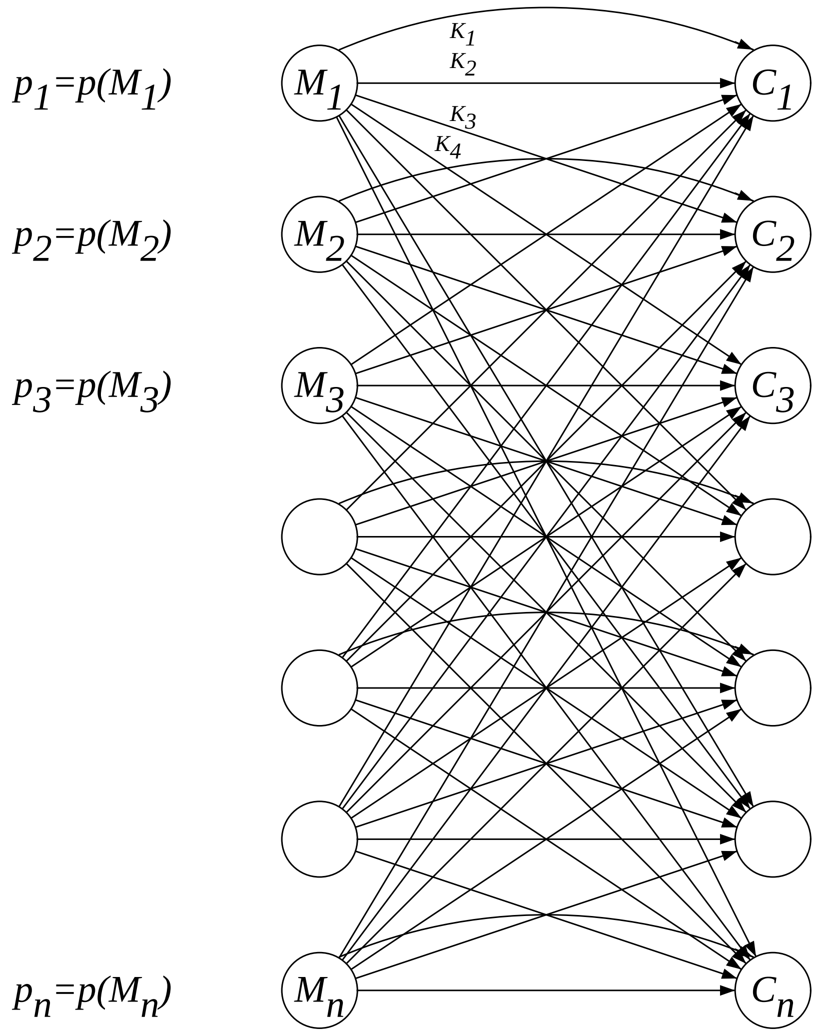
$\boldsymbol{D}$ be the decryption function $\boldsymbol{M = D_K(C)}$

For any key K, $E_K(\cdot)$ and $D_K(\cdot)$ are 1-1, and $D_K(E_K(\cdot))$ =Identity.

Shannon's Theory of Secrecy Systems (1949)

Let $\{M_1, M_2, \ldots, M_n\}$ be the message space.
The messages $M_1, M_2, \ldots, M_n$ are distributed with known probabilities $p(M_1), p(M_2), \ldots, p(M_n)$ (not necessarily uniform).
Let $\{K_1, K_2, \ldots, K_l\}$ be the key space. The keys $K_1, K_2, \ldots, K_l$ are distributed with known probabilities $p(K_1), p(K_2), \ldots, p(K_l)$. Usually (but not necessarily) the keys are uniformly distributed: $p(K_i) = 1/l$.
Each key projects all the messages onto all the ciphertexts, giving a bipartite graph:

Shannon's Theory of Secrecy Systems (1949) (cont.)



Perfect Ciphers

Definition: A cipher is **perfect** if for any M, C

$$p(M|C) = p(M)$$

(i.e., the ciphertext does not reveal any information on the plaintext).
By this definition, a perfect cipher is immune against ciphertext only attacks, even if the attacker has infinite computational power (unconditional security in context of ciphertext only attacks).
Note that

$$p(M)p(C|M) = p(M, C) = p(C)p(M|C).$$

Perfect Ciphers (cont.)

and thus it follows that

Theorem: A cipher is perfect iff

$$\forall M, C \quad p(C) = p(C|M).$$

Note that

$$p(C|M) = \sum_{\substack{K \\ E_K(M)=C}} p(K).$$

Therefore, a cipher is perfect iff

$$\forall C \quad \left(\sum_{\substack{K \\ E_K(M)=C}} p(K) \text{ is independent of } M \right)$$

Perfect Ciphers (cont.)

Theorem: A perfect cipher satisfies $l \geq n$ (#keys $\geq$ #messages).
Proof: Assume the contrary: $l < n$. Let C_0 be such that $p(C_0) > 0$. There exist l_0 $(1 \leq l_0 \leq l)$ messages M such that $M = D_K(C_0)$ for some K. Let M_0 be a message not of the form $D_K(C_0)$ (there exist $n - l_0$ such messages). Thus,

$$p(C_0|M_0) = \sum_{\substack{K \\ E_K(M_0)=C_0}} p(K) = \sum_{K \in \emptyset} p(K) = 0$$

but in a perfect cipher

$$p(C_0|M_0) = p(C_0) > 0.$$

Contradiction. QED

Perfect Ciphers (cont.)

Example: Encrypting only one letter by Caesar cipher: $l = n = 26$, $p(C) = p(C|M) = 1/26$.
But:
When encrypting two letters: $l = 26$, $n = 26^2$, $p(C) = 1/26^2$.
Each M has only 26 possible values for C, and thus for those C's: $p(C|M) = 1/26$, while for the others C's $p(C|M) = 0$.
In particular, $p(C = XY|M = aa) = 0$ for any $X \neq Y$.

Vernam is a Perfect Cipher

Theorem: Vernam is a perfect cipher.
Vernam is a Vigenere with keys as long as the message. Clearly, if the keys are even slightly shorter, the cipher is not perfect.
Proof: Clearly, in Vernam $l = n$. Given that the keys are uniformly selected at random, $p(K) = 1/l = 1/n$.

$$p(C|M) = p(K = C - M) = \frac{1}{n} = \frac{1}{l}.$$

Since $p(C|M) = 1/l$ for any M and C, clearly also $p(C|M) = p(C)$. QED

Entropy

Let S be a source of n elements distributed with the probabilities $p_1, p_2, \ldots, p_n$.

Definition: The **entropy** $H(S)$ of S is

$$H(S) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \log p_i$$

(log is used in all the course in base 2).

The entropy is measured in units of **bits**. It measures the amount of **unknown information** in S.

Entropy (cont.)

Example: English text: We already mentioned that the frequency of the letters in English texts are

Letter	Frequency	Letter	Frequency	Letter	Frequency
e	12.31%	l	4.03%	b	1.62%
t	9.59%	d	3.65%	g	1.61%
a	8.05%	c	3.20%	v	0.93%
o	7.94%	u	3.10%	k	0.52%
n	7.19%	p	2.29%	q	0.20%
i	7.18%	f	2.28%	x	0.20%
s	6.59%	m	2.25%	j	0.10%
r	6.03%	w	2.03%	z	0.09%
h	5.14%	y	1.88%		

The entropy of such a source of letters is then

$$H(S) = -0.1231 \log 0.1231 - 0.0959 \log 0.0959 - \ldots - 0.0009 \log 0.0009 \approx 4$$

Entropy (cont.)

Example: Let S be uniformly distributed: $p_i = 1/n$. Then,

$$H(S) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = n \cdot \frac{1}{n} \cdot \log n = \log n.$$

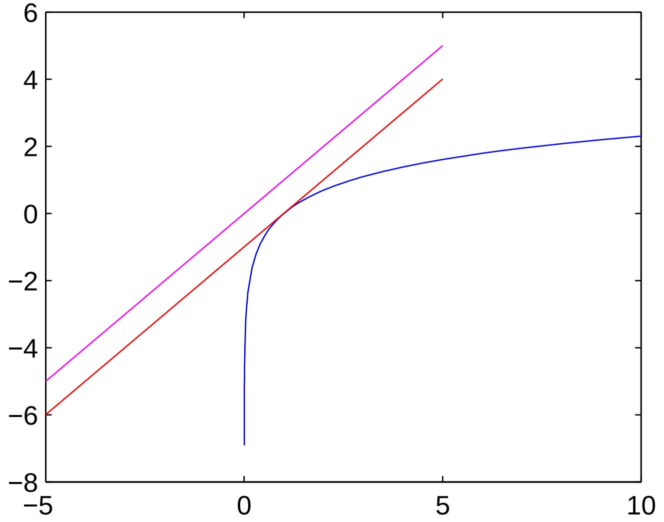
In particular, if $n = 2^k$ then $H(S) = \log n = k$.
If $n = 26$ then $H(S) = \log 26 = 4.7$. As we noticed, in English S is not uniformly distributed, and $H(S) = 4$.
Lemma: If the distribution is not uniform $H(S) < \log n$. (to be proven shortly).
In this case, a long string whose characters are distributed as in S can be compressed to $H(S)$ bits.

Entropy (cont.)

Claim: $\ln x \leq x - 1$.

Proof: Consider the function $\ln x - (x-1)$. Its derivative is $\frac{d(\ln x-(x-1))}{dx} = \frac{1}{x} - 1$, and thus the maximum is at $x = 1$ where $\ln x - (x-1) = 0$.

The figure shows the curves of x, of $x - 1$, and of $\ln x$:



QED

Entropy (cont.)

Lemma: $H(S) \le \log n$ (equality iff S is uniformly distributed).
Proof: Let p_i and q_i be two distributions, $\Sigma\, p_i = \Sigma\, q_i = 1$. Then

$$\begin{aligned}
&\Sigma\, p_i \log \frac{1}{p_i} - \Sigma\, p_i \log \frac{1}{q_i} = \Sigma\, p_i \log \frac{q_i}{p_i} = \\
&= \frac{1}{\ln 2} \Sigma\, p_i \ln \frac{q_i}{p_i} \le \frac{1}{\ln 2} \Sigma\, p_i \left(\frac{q_i}{p_i} - 1 \right) = \\
&= \frac{1}{\ln 2} (\Sigma\, q_i - \Sigma\, p_i) = \frac{1}{\ln 2} (1 - 1) = 0
\end{aligned}$$

and thus,

$$\Sigma\, p_i \log \frac{1}{p_i} \le \Sigma\, p_i \log \frac{1}{q_i} \qquad (*)$$

Entropy (cont.)

and in particular for $q_i \equiv 1/n$:

$$\begin{aligned} H(S) &= \sum p_i \log \frac{1}{p_i} \leq \sum p_i \log \frac{1}{q_i} = \\ &= \sum p_i \log \frac{1}{1/n} = \log n. \end{aligned}$$

QED

Properties of the Entropy

Let A and B be two independent sources with distributions p, q, respectively.

Theorem: $H(A,B) = H(A) + H(B)$.

Proof:

$$\begin{aligned}
-H(A,B) &= \sum_{i,j} p_i q_j \log(p_i q_j) \\
&= \sum_j q_j \sum_i p_i \log p_i + \sum_i p_i \sum_j q_j \log q_j \\
&= \sum_i p_i \log p_i + \sum_j q_j \log q_j \\
&= -(H(A) + H(B)).
\end{aligned}$$

QED

Conditional Entropy

Let $p_{i,j}$ be the distribution of $i \in A$, $j \in B$ ($\sum_{i,j} p_{i,j} = 1$).

Let

$$\begin{aligned} p_i &= \sum_j p_{i,j} \\ q_j &= \sum_i p_{i,j} \\ q(j|i) &= p_{i,j}/p_i \qquad \text{(Normalized in each row)} \end{aligned}$$

Conditional Entropy (cont.)

Example:

	B_1	B_2		B_j			Sum
A_1	$p_{1,1}$	$p_{1,2}$		$p_{1,j}$			p_1
A_2	$p_{2,1}$	$p_{2,2}$		$p_{2,j}$			p_2
A_i	$p_{i,1}$	$p_{i,2}$		$p_{i,j}$			p_i
Sum	q_1	q_2		q_j			1

A special example is pairs of consecutive letters in English. The entry (Q,U) has probability 0, while (T,H) has probability above average.

Conditional Entropy (cont.)

Definition:

$$H(B|A_i) = -\sum_j q(j|i) \log q(j|i)$$

(the entropy of B given the exact value of A_i).

The **Conditional Entropy** is defined to be

$$H(B|A) = \sum_i p_i H(B|A_i).$$

Conditional Entropy (cont.)

Theorem: $H(A,B) = H(A) + H(B|A)$.

Proof:

$$\begin{aligned}
-H(A,B) &= \sum_{i,j} p_i q(j|i) \log(p_i q(j|i)) \\
&= \sum_i p_i \log p_i \sum_j q(j|i) + \sum_i p_i [\sum_j q(j|i) \log q(j|i)] \\
&= \sum_i p_i \log p_i + \sum_i p_i [-H(B|A_i)] \\
&= -H(A) - H(B|A)
\end{aligned}$$

QED

Conclusion: $H(A,B) \geq H(A)$.

Conditional Entropy (cont.)

Theorem: $H(B|A) \leq H(B)$ (equality only if A and B are independent).
Proof:

$$H(B|A) = \sum_i p_i H(B|A_i) = \sum_i p_i \sum_j q(j|i) \log \frac{1}{q(j|i)}$$

By (*):

$$\begin{aligned} &\leq \sum_i p_i \sum_j q(j|i) \log \frac{1}{q_j} = \sum_j \left(\sum_i p_i q(j|i) \right) \log \frac{1}{q_j} \\ &= \sum_j q_j \log \frac{1}{q_j} = H(B) \end{aligned}$$

QED
Similarly, $H(C|B, A) \leq H(C|B)$.

Long Message Encryption

To encrypt a long message $M = M_1 M_2 \ldots M_N$ (M is the full message, the M_i's are the various letters) we encrypt each block M_i to $C_i = E_K(M_i)$ under the same key K, and concatenate the results $C = C_1 C_2 \ldots C_N$.

This cipher is not perfect since there is N such that #keys < #messages of length N (and since $p(XY|aa) = 0 \neq p(XY)$ when $X \neq Y$).

Thus, we can gain information on the key or the message given the ciphertext only (for a given C there are only #keys possible messages, rather than #messages).

Long Message Encryption (cont.)

Theorem: for any $S \geq N$, and for any A,

1. $H(K|C_1C_2\ldots C_S) \leq H(K|C_1C_2\ldots C_N)$
2. $H(M_1M_2\ldots M_A|C_1C_2\ldots C_S) \leq$
   $H(M_1M_2\ldots M_A|C_1C_2\ldots C_N)$
3. $H(M_1M_2\ldots M_N|C_1C_2\ldots C_N) \leq H(K|C_1C_2\ldots C_N)$

Thus, when the size of C grows, the entropies of the message and the key are reduced.

Proof: Exercise.

Unicity Distance

How long should M and C be so we can identify the message M uniquely given the ciphertext C?

We wish that $H(M|C) = H(M_1M_1\ldots M_N|C_1C_2\ldots C_N)$ be zero (or very small; we know that it reduces when N is increasing).

Observe that some keys may be equivalent, and thus $H(K)$ may be just an upper bound on the effective entropy of the key

$$H(C|M).$$

Unicity Distance (cont.)

Look at the equations:

$$H(C) + H(M|C) = H(M,C) = H(M) + H(C|M)$$

By moving terms we get:

$$H(C) - H(M) = H(C|M) - H(M|C)$$

Let $H(M') \triangleq H(M)/N$ and $H(C') \triangleq H(C)/N$, be the average additional entropy for each additional letter, where N is the message length, and assume that $H(M|C) = 0$ (as the message is unique given C).
Then,

$$N\left(H(C') - H(M')\right) = H(C|M)$$

Unicity Distance (cont.)

$H(K)$, $H(C')$, and $H(M')$ are fixed. Thus, in order to get a unique key we need

$$N \geq \frac{H(C|M)}{H(C') - H(M')}.$$

$H(K) \geq H(C|M)$ and thus it suffices to assume that we get a message of length

$$N \geq \frac{H(K)}{H(C') - H(M')}$$

(which is the unicity distance of identifying the key uniquely).

Unicity Distance (cont.)

Definition: **the unicity distance N** is

$$N = \frac{H(K)}{H(C') - H(M')}$$

If $H(C') = H(M')$, then $H(M|C) = H(C|M) > 0$, then the message is never unique. In this case we say that $\boldsymbol{N = \infty}$.
Moreover, if $H(K) \not< H(M)$ then $H(M|C) = H(K) \geq H(M)$ so the ciphertext does not disclose any information on the message M if the key has sufficient entropy.
Conclusion: Compression of a message before encrypting reduces $H(C') - H(M')$ and thus increases the unicity distance.

Random Ciphers

Assume that the message space and the ciphertext space are of size n (n different messages of size N).

The messages are **redundant**, i.e., not all the n messages are legal, or not all have the same probabilities.

Each key represents a random permutation of the letters, each with probability $1/n!$. Thus,

$$\begin{aligned} p(C_1) &= 1/n \\ H(C_1) &= \log n \end{aligned}$$

Random Ciphers (cont.)

Let $H(C')$ and $H(M')$ be $H(C') \triangleq H(C)/N$, and $H(M') \triangleq H(M)/N$.

Definition: $D \triangleq H(C') - H(M')$ is called the **source redundancy**.

Definition: The **unicity distance** is

$$N = \frac{H(K)}{H(C') - H(M')} = \frac{H(K)}{D}$$

Random Ciphers (cont.)

Example: In English $D = \log 26 - H(M')$. $\log 26 = 4.7$, $H(M') = 1.5$ (as letters are dependent in English). $D = \log 26 - H(M') = 4.7 - 1.5 = 3.2$.

In Caesar's cipher (26 possible shifts), the unicity distance is thus

$$N = \frac{H(K)}{3.2} = \frac{\log 26}{3.2} = 1.5$$

In a substitution cipher

$$N = \frac{H(K)}{3.2} = \frac{\log 26!}{3.2} = \frac{88.4}{3.2} = 27.6$$

In a uniformly random letter distribution, whose frequencies are as in English, $D = 4.7 - 4 = 0.7$ and the unicity distances would be 7 and 126, respectively.