Unicity Distance: An Example

Consider the binary "one-time pad" cryptosystem with $n = 1$. We have $\mathcal{K} = \mathcal{P} = \mathcal{C} = \mathbb{Z}_2 = \{0, 1\}$. The keybit is chosen equiprobably from $\{0, 1\}$. If each key is used only once, that is, a fresh independent keybit is chosen for each plaintext bit, we know, that the cipher achieves perfect secrecy, independently of the plaintext statistics.

Let us now examine how the secrecy is weakened if we use key bits more than once. It is straightforward to find the key with known plaintext, so let us consider ciphertext-only attack, which is based on knowledge about plaintext statistics. In this example we are given the probability $p_{\mathcal{P}}(x = 0) = p$. We assume that $p \neq 0$ and $p \neq 1$, otherwise there is no uncertainty about the plaintext, and nothing to solve. It is also given that the plaintext bits are mutually independent. Consequently, the plaintext language L has entropy

$$H_L = \lim_{n\to\infty} \frac{H(\mathbf{P}^n)}{n} = h(p) = -p \log_2 p - (1-p)\log_2(1-p)$$

and redundancy

$$R_L = 1 - \frac{H_L}{\log_2 |\mathcal{P}|} = 1 - h(p)$$

Further, we determine the unicity distance

$$n_0 = \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|} = \frac{1}{1 - h(p)}$$

Clearly, the closer p is to $1/2$, the more ciphertext is needed to determine the key, and one never achieves 100% certainty about the key.

If $h(p) < 1$, that is, $p \neq 1/2$, then the plaintext language has redundancy which can be exploited to launch the following ciphertext only attack. Given a string $(y_1, y_2, \ldots, y_r)$ of ciphertext bits, encrypted using the same key bit K, let t be the number of 0 bits. Then we have the following three cases:

1. If $|t/r - p| < |t/r - (1-p)|$, then guess $K = 0$.
2. If $|t/r - p| > |t/r - (1-p)|$, then guess $K = 1$.
3. Else $t/r = 1/2$. In this case the result is ambiguous.

It is not difficult to derive a general formula for the probability a correct guess in terms of p and r.

As an example, let us consider $p_{\mathcal{P}}(x = 0) = p = 1/9$. Then $h(p) \approx .7$ and consequently, $n_0 \approx 3$. On the other hand, assume that three ciphertext bits are given, and we guess the keybit using the above described attack. If the three bits are 000, 001, 010, or 100, the guess is $K = 1$. Otherwise, the guess is $K = 0$. Then the probability that the guess is correct is

$$\begin{aligned}
&p_{\mathcal{K}}(K = 0)p(\text{correct guess}|\, K = 0) + p_{\mathcal{K}}(K = 1)p(\text{correct guess}|\, K = 1) = \\
&p_{\mathcal{K}}(K = 0)p_{\mathcal{P}^3}(011, 101, 110, 111) + p_{\mathcal{K}}(K = 1)p_{\mathcal{P}^3}(011, 101, 110, 111) = \\
&p_{\mathcal{P}^3}(011, 101, 110, 111) = 3(1/9)(8/9)^2 + (8/9)^3 \approx .966
\end{aligned}$$

Hence, the guess is correct if and only if the three plaintext bits were 011, 101, 110, or 111, which happens with probability .966. So we have seen that in this example the approximative unicity distance $n_0 = 3$ gives 96.6% confidence about the key.