OTP is perfect

In order to prove that OTP has perfect secrecy we start from Shannon's definition and prove that

$$Pr\{M = m|C = c\} = Pr\{M = m\} \tag{1}$$

for any pair of plaintext m and ciphertext c.

Applying the Bayes Law to the left hand-side of Equation 1 we obtain:

$$Pr\{M = m|C = c\} = \frac{Pr\{M = m, C = c\}}{Pr\{C = c\}}. \tag{2}$$

It follows that

$$Pr\{M = m|C = c\} = Pr\{C = c|M = m\} \times \frac{Pr\{M = m\}}{Pr\{C = c\}}. \tag{3}$$

With reference to Equation 3, we now calculate $Pr\{C = c\}$. We initially consider the following lemma.

Lemma 1. *Given $m \in \mathcal{P}$ and $c \in \mathcal{C}$, there exists just one $k \in \mathcal{K}$, s.t., $c = m \oplus k$. Furthermore, $k = m \oplus c$.*

From the Law of Total Probability

$$Pr\{C = c\} = \sum_{m'} Pr\{C = c|M = m'\} \times Pr\{M = m'\} \tag{4}$$

Consider $Pr\{C = c|M = m'\}$. It is equivalent to the probability of generating a key such that m' encrypts to c, i.e., $Pr\{K = m' \oplus c\}$. As keys are generated in a perfectly random way, $Pr\{K = m' \oplus c\} = \frac{1}{2^n}$. It follows that Equation 4 becomes:

$$Pr\{C = c\} = \sum_{m'} 2^{-n} \times Pr\{M = m'\} = 2^{-n}. \tag{5}$$

With reference to Equation 3, we now calculate $Pr\{C = c|M = m\}$. We can repeat the reason above and, exploiting again the Lemma 1, we obtain

$$Pr\{C = c|M = m\} = \frac{1}{2^n}. \tag{6}$$

By substituting Equation 5 and Equation 6 into Equation 3, we obtain

$$Pr\{M = m|C = c\} = Pr\{M = m\} \tag{7}$$

which concludes the proof.