Shannon's theorem

Theorem 1. *In a perfect cipher* $|\mathcal{K}| \geq |\mathcal{P}|$*, i.e., the number of keys cannot be smaller than the number of messages.*

Proof. The proof is by contradiction.

First, let us assume that $|\mathcal{K}| < |\mathcal{P}|$. Then, let us observe that it had better be the case that $|\mathcal{C}| \geq |\mathcal{P}|$ or, otherwise, the cipher would not be an invertible (two plaintext messages would map into the same cipher-text message under the same key). It follows that

$$|\mathcal{C}| > |\mathcal{K}|. \tag{1}$$

Let us now look at the consequences of this inequality. Let us consider a p^* such that $Pr\{P = p^*\} \neq 0$. Let us encrypt p^* under every possible key. Since the number of keys is smaller than the number of ciphertexts because of inequality 1, then there must be a ciphertext, namely c^* that is not image of p^* under any key. If follows that $Pr\{P = p^* | C = c^*\} = 0$. It follows that there exists at least a pair (p^*, c^*), s.t. $Pr\{P = p^* | C = c^*\} \neq Pr\{P = p^*\}$.

□