Exercise sheet 2: Information-theoretic Secure Stegosystems

I Uniform covertext distributions

In the prisoner’s scenario, suppose Alice and Bob both have a copy of the Bible in their cells. The adversary allows them to make a reference to any verse of the Bible in their cells. The adversary allows them to make a reference to any verse of the Bible in a message. All verses are considered to occur equally likely in a conversation among prisoners and there is a publicly known way to associate codewords with Bible verses: let the set of verses be \( \{v_0, \ldots, v_{m-1}\} \).

Describe a way to exchange messages in \( \mathbb{Z}_m \) secretly between Alice and Bob and analyze the security of your solution.

II General distributions

Given a covertext \( C \), Alice constructs the embedding one-bit function from a binary partition of the covertext space \( \mathcal{C} \) such that both parts are assigned approximately the same probability under \( P_C \). In other words, let:

\[
\mathcal{C}_0 = \arg \min_{\mathcal{C}' \subseteq \mathcal{C}} | \sum_{c \in \mathcal{C}'} P_C(c) - \sum_{c \notin \mathcal{C}'} P_C(c) |
\]

and

\[
\mathcal{C}_1 = \mathcal{C} \setminus \mathcal{C}_0
\]

Alice and Bob share a uniformly distributed one-bit secret key \( K \). Define \( \mathcal{C}_0 \) to be the random variable with alphabet \( \mathcal{C}_0 \) and distribution \( P_{\mathcal{C}_0} \) equal to the conditional distribution \( P_{\mathcal{C} \mid C \in \mathcal{C}_0} \) and define \( \mathcal{C}_1 \) similarly on \( \mathcal{C}_1 \). Then Alice computes the stegotext to embed a message \( E \in \{0,1\} \) as

\[
S = C_E \oplus K
\]

Bob can decode the message because he knows that \( E = 0 \) if and only if \( S \in \mathcal{C}_K \). Note that the embedding provides perfect secrecy for \( E \).

Let \( \delta = \Pr[C \in \mathcal{C}_0] - \Pr[C \in \mathcal{C}_1] > 0 \)
1. Check that $P_S(c) = P_C(c)/1 + \delta$ if $c \in C_0$ and $P_S(c) = P_C(c)/1 - \delta$ otherwise.

2. Show that this one-bit stegosystem has security $\delta^2/\ln 2$ against passive adversaries.