Introduction to Module 04

This module consists of two separate topics.

The first topic builds on the previous module, where we looked at coding a source into short codewords. Instead of encoding each symbol that comes from the source separately, we will now code entire blocks at the same time: we wait until the source has emitted, say, n symbols, and then assign that block of n symbols a single codeword. Can we make shorter codes in this way?

It turns out the answer is yes: in some cases, the expected codeword length can shrink slightly. A code that achieves this will work as follows. Divide all possible source strings of length n into two groups: "typical" and "atypical". A typical source string will be assigned a short codeword, whereas an atypical source string will be assigned a longer codeword. Ideally, the source will almost always emit typical strings, but the set of typical strings (the "typical set") will be very small, so that you can assign very short codewords to its elements. This balance will be formalized in this module when we define typical sets. The concept of typicality will play an important role again in the final module of this course, when we prove Shannon's noisy-channel coding theorem.

The second topic is about *hiding* information: we will see some simple examples of encryption schemes, one of which is perfectly secure (we will define what that means later). We will consider the following question: how many bits of key are required to perfectly hide all the information in a message? Perhaps unsurprisingly, the answer will be related to the entropy of the message.

To understand perfectly secure encryption, we will complete our picture of entropy-related quantities by introducing conditional mutual information.

created: 2019-10-21