# Coding and Cryptography

January 19, 2018

# Contents

# 0 Miscellaneous

132

# 1 Introduction to communication channels and coding

For example, given a message $M$ = "*Callme*!" which we wish to send by email. We first encode t as binary strings using ASCII. So $f(C) = 1000011$, $f(a) = 1100001$, $f^*(M) = 10000111100001...0100001$.

The message goes from the source to the receiver after encoded by the source and decoded by the receiver via a channel, where errors could occur. The basic problem is, given a source and a channel (described probabilistically, we aim to design an encoder and a decoder in order to transmit information economically, reliably, and preserving privacy (secretly).

Some examples of each aspect:
*economcically*: Morse code, where common letters have shorter codewords;
*reliability*: every book has an ISBN of form $a_1...a_{10}$ where $a_i \in \{0, 1, ..., 9\}$ for $1 \leq i \leq 9$ and $a_{10} \in \{0, 1, ..., 9, X\}$, s.t. $10a_1 + 9a_2 + ... + a_{10} \equiv 0 \pmod{1}1$, where we treat $X$ as 10. In this way errors can be detected, although not corrected. There is another version of ISBN which is 13 digit;
*preserve privacy* RSA.

A communication channel takes letters from an input alphabet $\Sigma_1 = \{a_1, ..., a_r\}$ and emits letters from an output alphabet $\Sigma_2 = \{b_1, ..., b_s\}$.

A channel is determined by the probabilities $P(y_1, ..., y_k \text{ received}|x_1, ..., x_k \text{ sent})$.

**Definition.** A *discrete memoryless channel*(DMC) s a channel for which $P_{ij} = P(b_j \text{ received}|a_i \text{ sent})$ is the same each time the channel is used, and is independent of all past and future. The channel matrix is the $r \times s$ matrix with entrices $p_{ij}$. Note the rows sum to 1.

**Example.** (Binary Symmetric Channel, BSC)
BSC has $\Sigma_1 = \Sigma_2 = \{0, 1\}$, $0 \leq p \leq 1$. It has channel matrix $\binom{1-p\ \ p}{p\ \ 1-p}$, i.e. $p$ is the probability symbol is mistransmitted.

**Example.** (Binary Erasure Channel)
$\Sigma_1 = \{0, 1\}$, $\Sigma_2 = \{0, 1, *\}$, $0 \leq p \leq 1$. Then the channel matrix is $\binom{1-p\ \ p\ \ 0}{0\ \ p\ \ 1-p}$, i.e. $p$ is the probability that a synbol can't be read.

Informal definition: A channel's capacity is the highest rate at which information can be reliably transimitted over the channel. Here rate means the units of information per unit tme (we want that high), and reliably means arbitrarily small error probability.

There are 3 sections:
1) Noiseless coding (data compression);
2) Error control codes;
3) Cryptography.

## 1.1 Noiseless coding

**Notation.** For $\Sigma$ an alphabet that $\Sigma^* = \bigcup_{n\geq 0} \Sigma^n$ be th set of all finite strings of elements of $\Sigma$.

If $x = x_1...x_r$, $y = y_1...y_s$ are strings from $\Sigma$, write $xy$ for the concatenation $x_1...x_r y_1...y_s$. Further, $|x_1...x_r y_1...y_s| = r + s$ the length of string.

**Definition.** Let $\Sigma_1, \Sigma_2$ be two alphabets. A *code* is a function $f : \Sigma_1 \to \Sigma_2^*$. The strings $f(x)$ for $x \in E$ are called *codeworks*

**Example.** (Greek five code)
$\Sigma_1 = \{\alpha, \beta, ..., \omega\}$ (24 letters); $\Sigma_2 = \{1, 2, 3, 4, 5\}$ (more used). Now let $\alpha \to 11, \beta \to 12, \omega \to 54$.

**Example.** $\Sigma_1 = \{$all words in the dictionary$\}$. =,$\Sigma_2 = \{A, B, ..., space\}$. Tgeb $f =$'spell the word and a space.'

We sent a message $x_1, ..., x_n \in \Sigma^* 1$ as $f(x_1)f(x_2)...f(x_n) \in \Sigma_2^*$, i.e. extend $f$ to $f^* : \Sigma_1^* \to \Sigma_2^*$.

**Definition.** A code $f$ is *decipherable* if $f^*$ is injective, i.e. every string from $\Sigma_2$ arises from at most one message.