Coding Theory

CO 331

Alfred Menezes

LaTeXed by Sibelius Peng

Preface

Disclaimer Much of the information on this set of notes is transcribed directly/indirectly from the lectures of CO 331 during Winter 2021 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

For any questions, send me an email via https://notes.sibeliusp.com/contact/.

You can find my notes for other courses on https://notes.sibeliusp.com/.

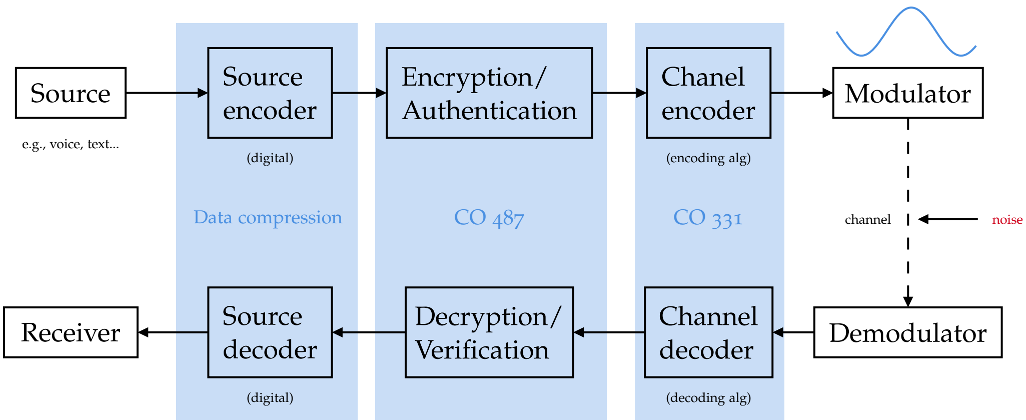
Sibelius Peng

Contents

Introduction

Coding theory is about clever ways of adding redundancy to messages to allow (efficient) error detection and error correction.

Here is our communication model:



Example: Parity Code

Encoding algorithm Add a 0 bit to the (binary) msg m if the number of 1's in m is even; else add a 1 bit.

Decoding algorithm If the number of 1's in a received msg r is even, then accept r; else declare that an error has occurred.

Example: Replication Code

Source msgs	Codeword	# err/codeword (always) detected	# err/codeword (always) corrected *	Information rate
0 1	0 1	0	0	1
0 1	00 11	1	0	$\frac{1}{2}$
0 1	000 111	2	1	$\frac{1}{3}$
0 1	0000 1111	3	1	$\frac{1}{4}$
0 1	00000 11111	4	2	$\frac{1}{5}$

$\xrightarrow{\text{encoding algorithm}}$

*: using "nearest neighbour decoding"

Goal of Coding Theory

Design codes so that:

1. High information rate
2. High error-correcting capability
3. Efficient encoding & decoding algorithms

Course Overview

This course deals with *algebraic methods* for designing good (block) codes. The focus is on error correction (not on error detection). These codes are used in wireless communications, space probes, CD/DVD players, storage, QR codes, etc.

Some modern stuff are not covered: Turbo codes, LDPC codes, Raptor codes, ... Their math theories are not so elegant as algebraic codes.

The big picture

Coding theory in its broadest sense deals with techniques for the *efficient*, *secure* and *reliable* transmission of data over communication channels that may be subject to *non-malicious errors* (noise) and *adversarial intrusion*. The latter includes passive intrusion (eavesdropping) and active intrusion (injection/deletion/modification).

1

Fundamentals

1.1 Basic Definitions and Concepts

alphabet

An **alphabet** A is a finite set of $q \geq 2$ symbols.

word

A **word** is a finite sequence of symbols from A (also: vector, tuple).

length

The **length** of a word is the number of symbols it has.

code

A **code** C over A is a set of words (of size ≥ 2).

codeword

A **codeword** is a word in the code C.

block code

A **block code** is a code in which all codewords have the same length.

A **block code of length** n **containing** M **codewords over** A is a subset $C \subseteq A^n$ with $|C| = M$. C is called an $[n, M]$-code over A.

Example:

$A = \{0,1\}$. $C = \{00000, 11100, 00111, 10101\}$ is a $[5,4]$-code over $\{0,1\}$.

Messages		Codewords
00	$\to$	00000
10	$\to$	11100
01	$\to$	00111
11	$\to$	10101

Encoding of messages (1-1 map)

Assumptions about the communications channel

(1) The channel only transmits symbols from A ("hard decision decoding").

(2) No symbols are deleted, added, interchanged or transposed during transmission.

(3) The channel is a q-symmetric channel:

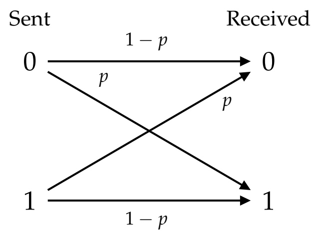
Let $A = \{a_1, \ldots, a_q\}$. Let X_i = the i^{th} symbol sent. Let Y_i = the i^{th} symbol received. Then for all $i \geq 1$, and all $i \leq j, k \leq q$,

$$\Pr(Y_i = a_j | X_i = a_k) = \begin{cases} 1-p, & \text{if } j = k \\ \frac{p}{q-1}, & \text{if } j \neq k. \end{cases}$$

p is called the **symbol error probability** of the channel ($0 \leq p \leq 1$).

Binary Symmetric Channel (BSC)

A 2-symmetric channel is called a binary symmetric channel.



For a BSC:

1. If $p = 0$, the channel is *perfect*.
2. If $p = 1/2$, the channel is *useless*.
3. If $1/2 < p \leq 1$, then flipping all received bits converts the channel to a BSC with $0 \leq p < 1/2$.
4. Henceforth, we will assume that $0 < p < 1/2$ for a BSC.

Exercise:

For a q-symmetric channel, show that one can take $0 < p < \frac{q-1}{q}$ WLOG.

One can first consider the case $q = 3$.

Hamming distance

The **Hamming distance** (or distance) between two n-tuples over A is the number of coordinate positions in which they differ.

The Hamming distance (or distance) of an $[n, M]$-code C is $d(C) = \min\{d(x,y) : x, y \in C, x \neq y\}$.

Example:
The distance of $C = \{00000, 11100, 00111, 10101\}$ is $d(C) = 2$.

Theorem 1.1: properties of Hamming distance

For all $x, y, z \in A^n$,

1. $d(x,y) \geq 0$, with $d(x,y) = 0$ iff $x = y$.
2. $d(x,y) = d(y,x)$.
3. $d(x,y) + d(y,z) \geq d(x,y)$ ($\triangle$ inequality).

1.2 Decoding Strategy

Index