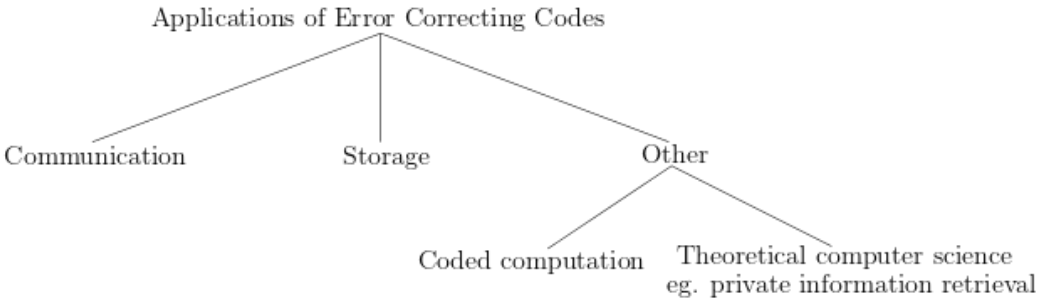
E2 205 Error-Control Coding
Lecture 1

Scribe - Shobhhit Bhatnagar

August 7, 2019

1 Applications/Scope of Error Correcting Codes

Error correcting codes find application in various areas.



1.1 Communication Applications

Every channel is associated to a channel capacity, which is the maximum amount of information that can be reliably communicated across the channel per channel use (Claude Shannon). In recent years, codes that achieve channel capacity have been discovered/constructed.

1.1.1 Timeline of Codes (Notes of Henry Pfister)

1948 - Shannon defines channel capacity and random codes
1950 - Hamming codes
1954 - Reed-Muller Codes
1955 - Elias (erasure channel), convolutional codes
1959 - Bose-Chaudhuri-Hocquenghem (BCH) codes
1960 - Low Density Parity Check (LDPC) codes
1960 - Reed-Solomon codes
1993 - Turbo codes (iterative decoding)
1995 - LDPC codes (rediscovered!)
2008 - Polar codes

1.1.2 Codes that Achieve Capacity

- Lattice based codes achieve capacity on the additive white gaussian noise channel (2004).
- Polar codes achieve capacity on binary input, output symmetric discrete memoryless channels (2009).
- Spatially coupled LDPC codes achieve capacity on binary inputy output symmetric, memoryless channels (2013).
- Reed-Muller codes achieve capacity on the binary erasure channel (2015).

1.2 Some Specific Applications

1.2.1 Deep Space Missions

1968 - Pioneer (convolutional codes + sequential decoding)
1969 - Mariner ([32,16,16] Reed-Muller code)
1977 - Voyager (concatenated code - Reed Solomon + Convolutional code, [255,223,33], incorporated as the deep space standard)

1.2.2 Storage

1980 - Compact Disks ([32,28,5],[28,24,5] Reed-Solomon codes)
Distributed storage - RAID, HDFS-RAID etc.

1.2.3 Communication

Turbo codes - Various wireless communication standards.
LDPC codes - Digital Video Broadcast IEEE 802.16 (WiMax); 5G data channel.
Polar codes - 5G control channel.

2 Basics of Block Codes

Consider the set $\mathbb{F}_2 = \{0, 1\}$ with two operators $+$ and $\cdot$ defined as

$+$	0	1
0	0	1
1	1	0

and

$\cdot$	0	1
0	0	0
1	0	1

Then, $\{\mathbb{F}_2, +, \cdot\}$ form a field.

Define $\mathbb{F}_2^n$ as

$$\mathbb{F}_2^n = \left\{ \underline{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} : x_i \in \mathbb{F} \right\}.$$

Elements of $\mathbb{F}_2^n$ are called vectors. As an example, for $n = 2$ we have

$$\mathbb{F}_2^2 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}.$$

Note that $|\mathbb{F}_2^n| = 2^n$.

2.1 Hamming Weight

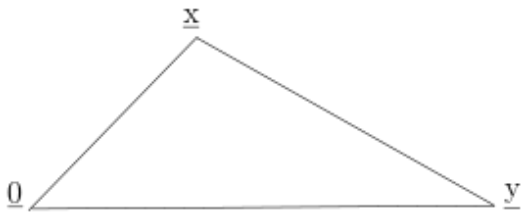
Definition 1 *The Hamming weight $w_H(\underline{x})$ of a vector $\underline{x} \in \mathbb{F}_2^n$ is the number of non-zero elements in $\underline{x}$.*

2.1.1 Properties of Hamming Weight

1. $w_H(\underline{x}) \geq 0$ with equality iff $\underline{x} = \underline{0}$.

2. $w_H(\underline{x}+\underline{y}) \leq w_H(\underline{x}) + w_H(\underline{y})$ (Triangle inequality).

- $w_H(\cdot)$ is a norm on $\mathbb{F}_2^n$.



The following is an example (and verification) of the triangle inequality in $\mathbb{F}_2^4$.

$$\underline{x} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}; \quad \underline{y} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}; \quad \underline{x}+\underline{y} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$w_H(\underline{x}) = 3, \quad w_H(\underline{y}) = 3, \quad w_H(\underline{x}+\underline{y}) = 2$
$w_H(\underline{x}) + w_H(\underline{y}) = 3+3 = 6 \geq 2 = w_H(\underline{x}+\underline{y})$.