Algebraic Coding Theory and Applications

Jillian Galetto, Senior, Pure Mathematics, Kent State University
Advisor: Hai Q. Dinh, Ph.D., Professor of Mathematics, Kent State University

Abstract

When communicating across a channel, it is inevitable that such pathways of communication be "noisy", thus there is always some sort of interference across the channel. This results in messages not always being received as they were sent. In order to solve these problems, coding theory developed and is used both to detect and correct errors. It is used for data compression, error correction, cryptography, and network coding. In error correction, a concentration on an algebraic coding theory lies with linear codes, including cyclic and constacyclic codes. In this poster presentation, we will discuss the history of coding theory, going in depth with cyclic and constacyclic codes, as well as discussing applications and current problems being resolved using algebraic coding theory.

Definitions

- Coding Theory is the study of methods for efficient and accurate transfer of information from one place to another; finding noise correcting errors
- Code is a set of codewords. A block code is a set of codewords of the same length
- Codewords are the words belonging to a given code; made up of digits
- A channel is the physical medium through which the information is transmitted. A binary channel only sends digits of 0 or 1.
- Noise is the undesirable disturbances which may cause information received to differ from that which was sent
- Hamming weight is the number of times the digit 1 occurs in a codeword, denoted \(\omega\)
- Hamming distance is the number of positions in which \(w\) and \(v\) disagree, denoted \(d(w,v)\)
- Parity Digit is an added digit that follows a certain algorithm to reduce errors
- A code \(C\) of distance \(d\) is an error correcting code if it detects all error patterns of weight less than or equal to \((d-1)\) and there is at least one error pattern of weight \(d\) which \(C\) will not detect.
- A cyclic code is a block code where the circular shifts of each codeword gives another word that belongs to the code, error-correcting
- A constacyclic code is a cyclic code where the circular shifts of each codeword gives another word that belongs to the code with the first symbol being \(x\)-tuple
- A negacyclic code is a cyclic code where the circular shifts of each codeword gives another word that belongs to the code with the first symbol changing sign

History

- Claude Shannon, American mathematician, electrical engineer, and cryptographer wrote a paper titled “A Mathematical Theory of Communication” in 1948
- Not related to what you say but what you could say.
- Focused on the best way to encode information that a sender wants to transmit.
- Introduced the term “bits” to reference a binary digit.

Deep Space Communication

- Deep space communication is communication between earth stations and remote spacecraft, other planets, or space beyond Earth’s gravitational field
- Most missions never return to earth, failed reception and consequent retransmission not an option
- Communication sporadic and ultra long distances
- Long delay, weak received signal, and variable distances according with orbits
- Asymmetrical uplink and downlink capacities
- Limited mass, power source, and volume
- Intensity of electromagnetic radiation decreases according to \(\frac{\tau}{t}\) as you leave Earth

- Channel coding major solution to deep space issues
- Traditionally used concatenation of convolutional code and Reed-Solomon Code
- Convolutional code have greater simplicity of implementation over a block code of equal power
- Infinite but fundamentally don’t offer more protection against noise than the equivalent block code
- Encoder usually a simple circuit with memory and logic while decoder in software or firmware
- By adding specific types of redundancy, can recover data perfectly with high probability, even under huge amounts of noise
- Low-Density Parity-Check (LDPC) are on a matrix containing only a few ones in each row and column
- LDPC decoded on parity check matrix which grows larger as the code rate decreases, low rate LDPC more correctable
- Turbo codes are constructed by applying or more simple to decode encoding rules to different permutations of the same information sequence, achieve data rates more near Shannon limit (theoretical max)
- Turbo codes decoded on trellises with only four bit per information bit corresponding to several code symbols
- UPC now international standard while Turbo codes are used for extremely long transmissions(outside planets or outside solar system)

Resources:
- https://www.cs.cmu.edu/~guyb/realworld/reedsolomon
- http://www.cs.cmu.edu/~guyb/realworld/reedsolomon
- http://celebratemath.org/1910-2010/