Claude Shannon, American mathematician, electrical engineer, and cryptographer wrote a paper titled "A Mathematical Theory of Communication" in 1948. It is 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.

---

**History**


- 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.

---

**Definitions**

- Coding Theory is the study of methods for efficient and accurate transport of information from one place to another; finding noise side 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.

- Length is the number of digits in a codeword.

- A binary channel is symmetric if 0 and 1 are transmitted in equal accuracy.

- The transmission rate is a number designed to measure the proportion of each codeword that is carrying the message - 1/(log_2(C)) code of length n.

- The Hamming weight is the number of times the digit 1 occurs in a codeword v, denoted wt(v).

- The Hamming distance is the number of positions in which w and v disagree, denoted d(w,v).

- A 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 code C is a cyclic code where the circular shifts of each codeword gives another word that belongs to the code with the first symbol being $x^n$.

- 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 changing sign.

- 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.

- Constacyclic codes discovered.

---

**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 of the algebraic coding theory lies with linear codes, including cyclic and constacyclic codes as well. In this paper, 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.

---

**Compact Disc (CD)**

- Reed Solomon Codes with binary digits represented on the disc as pits and lands, first instituted in 1982.

- Code is so strong most playback error comes from tracking error causing the laser to jump tracks.

- Reed Solomon codes discovered in 1960 by Irving Reed and Gustave Solomon.

- Can detect and correct multiple errors, including burst errors.

- Can correct a burst error of up to 4000 bad bits, or a physical defect of 2.47 mm long through parity digits and interleaving.

- Interpolation can conceal errors up to 13,700 bits of 8.5 mm long.

- Two layers of Reed-Solomon code separated by a 28-way convolutional interleaver. Cross-interleaved Reed-Solomon Code (CIRC)

  - High random error correctability
  - Long burst error correctability
  - In case exceeded, interpolation provide concealment approximation
  - Very high efficiency
  - Simple decoder strategy with reasonable sized memory

- Codewords consist of all function tables of polynomials of degree less than k over the finite field with n elements. (n is prime)

- Interpolat k given symbols as the first segment of the function table. Remaining n-k symbols generated by evaluating polynomial at points.

- Since n transmitted symbols from an overdetermined system that specifies polynomial of degree less than k, interpolation can recover original message.

- Adds a parity digits to every three.

- 1st Circle: relatively weak Reed-Solomon (32,28) can correct up to 2 bit errors in 32 bit block and flags errors with more than 2 bit

- 2nd Circle: Reed-Solomon (28,24) can correct up to 4 erasures per block

- CIRC interleave audio frames through disc over several consecutive frames.

- A physical frame contains information from many audio frames. This adds 84 bit of error correction data to each frame.

- 8 bits of subcode added to each frame.

---

**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 orbit.

- Asymmetrical uplink and downlink capacities

- Limited mass, power source, and volume

- Internally of electromagnetic radiation decreases according to $1/r^2$ 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.

- $c(x) = a(x)c_1(x) + a(x)c_2(x) + ... + a(x)c_m(x)$

- By adding specific types of redundancy, can recover data perfectly with high probability, even under huge amount 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 is decreased, low rate LDPC more powerful.

- Turbo codes are constructed by applying or 2 more simple to decode encoding rules to different permutations of the same information sequence, achieve data rates more than Shannon limit (theoretical max).

- Turbo codes decoded on softie with one trellis per information bit corresponding to several code symbols in LDPC, more powerful, while Turbo codes are used for extremely long transmission (outer planets or other solar system)