

Prof. Anuradha Sharma

1. Introduction to Coding theory.
2. Coding differs from cryptography, the latter meaning sending secured messages.
3. In Coding, the primary objective is to transmit messages across noisy communication channels or to retrieve data stored in a storage medium as quickly and as reliably as possible.
4. Source encoding, Source decoding.
5. ASCII code converts each character to a byte of 8 bits.
6. Channel encoding (also called Algebraic coding) - involves encoding the source encoded message again by adding some form of redundancy so that errors can be detected or even corrected by channel decoder.
7. Definitions of a Code alphabet, Word, Code word, Block code, Size of a code, Communication channel.
8. A code C over a set A (of order q) is defined as a finite (nonempty) set consisting of q -ary words over A .
9. Hamming distance between code words is a metric space.
10. Nearest neighbor decoding or Minimum distance decoding.
11. A code C over A is u - error detecting if and only if $d(C) \geq u + 1$.
12. A code C over A is v - error correcting if and only if $d(C) \geq 2v + 1$.
13. Optimal code.
14. Sphere Packing Bound (Hamming Bound) and related results.
15. Perfect codes, Singleton bound.
16. Linear codes: Let $A = F_q$ be a Galois field of order q and n a positive integer. Then F_q^n is an n -dimensional vector space over F_q . A Linear code C of length n over F_q is a subspace of F_q^n .
17. Inner product on F_q^n , Dual code C^\perp of C , Dimension of a linear code C , Hamming Weight, Generator matrix, Parity check matrix.
18. Encoding and decoding a linear code.
19. Standard (Slepian) Array.
20. Syndrome decoding and complete decoding.
21. Hamming weight enumerator and Mac-William's identity.
22. Cyclic code (special linear code) (Pranje, 1957) : A linear code C of length n over F_q is called a cyclic code if $\sigma(c) \in C \ \forall c \in C$, where σ is cyclic shift operator over F_q^n .
23. Generator polynomials, Idempotent generators.
24. Encoding of cyclic codes, Meggitt decoding of cyclic codes.
25. Plotkin construction.
26. First order Reed - Muller codes.