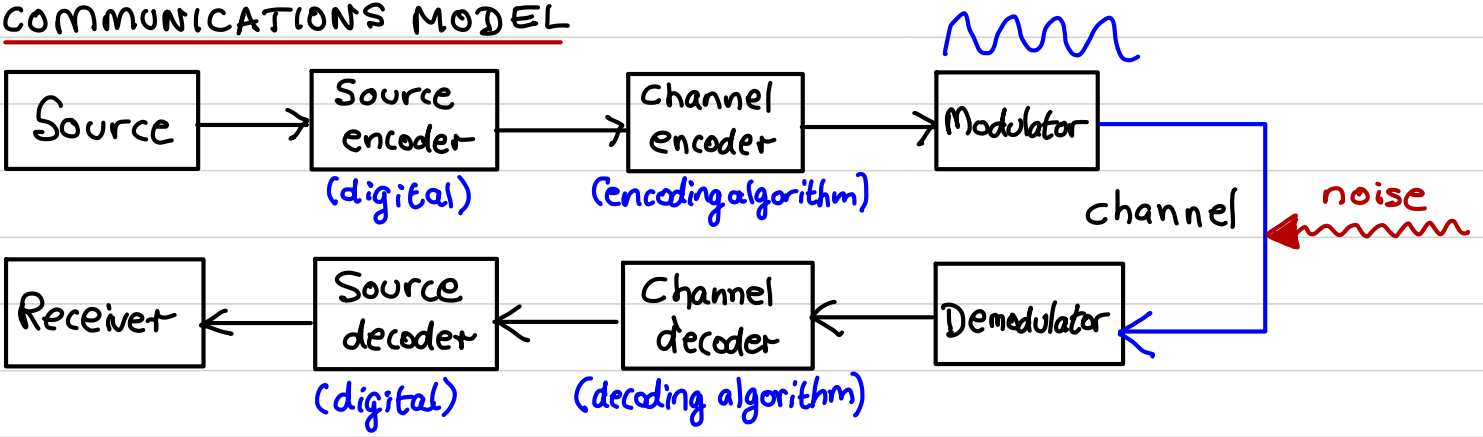
VO INTRODUCTION

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



- EXAMPLE (parity code)

  Encoding algorithm: Add a parity bit to the (binary) message.

  Decoding algorithm: If the number of 1's in the received message is even, then accept it; else reject it.

EXAMPLE (binary replication code)

Source messages	Codeword	# errors/codeword that can always be detected	# errors/codeword that can always be corrected *	Information rate
0	0	0	0	1
1	1			
0	00	1	0	1/2
1	11			
0	000	2	1	1/3
1	111			
0	0000	3	1	1/4
1	1111			
0	00000	4	2	1/5
1	11111			

encoding algorithm →

* using "nearest neighbour decoding"

GOALS OF CODING THEORY

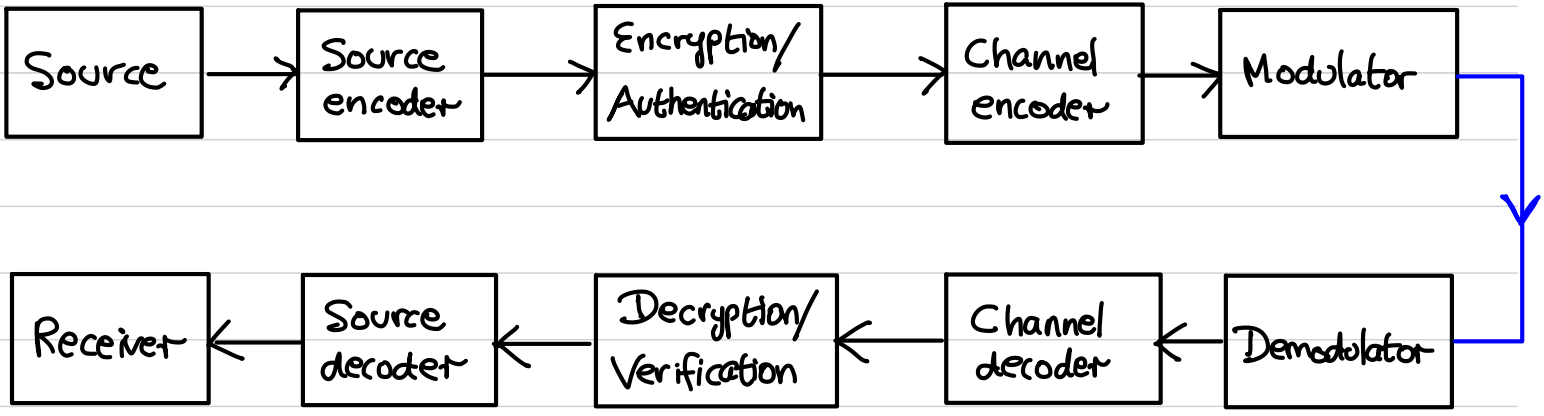
- Design codes with (i) High error-correcting capability.
  (ii) High information rate.
  (iii) Efficient encoding and decoding algorithms.
- "Efficient" = efficient in hardware and software.

- COURSE OVERVIEW This course deals with algebraic methods for designing good (block) codes. These codes are used for reliable communications and storage: space probes, CD/DVD/BlueRay, wireless, disk storage, QR codes, etc.

- NOT COVERED LDPC codes, Turbo codes, Raptor codes, Polar codes, ... And newer applications: Distributed storage, compressed sensing, group testing, learning theory, algorithm design, complexity theory, ...

THE BIG PICTURE

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



COURSE OUTLINE

LEARNING OUTCOMES

1) Demonstrate a fundamental understanding of the binary symmetric channel, decoding strategies, and the challenges in designing good codes.

2) Construct codes, and devise efficient encoding and decoding algorithms for them as a means of gaining exposure to the applications of linear algebra and abstract algebra.

3) Analyze the properties of major families of algebraic codes including linear codes, Hamming codes, Golay codes, cyclic codes, BCH codes, and Reed-Solomon codes.

COURSE PREREQUISITES

- Linear Algebra: vector spaces, linear independence, basis, Gaussian elimination, null space of a matrix, rank of a matrix.
- Elementary Number Theory: congruences, integers modulo n ($\mathbb{Z}_n$), primes, Fermat's Little Theorem.

COURSE INGREDIENTS

- Linear Algebra
- Abstract Algebra (groups, rings, fields)

EXERCISES

- Problem sets for each chapter (with solutions).

REFERENCES

- "An Introduction to Error Correcting Codes", Paul van Oorschot & Scott Vanstone (1989).

- "Modern Coding Theory", Tom Richardson & Rüdiger Urbanke (2008)

- "Essential Coding Theory", Venkatesan Guruswami, Atri Rudra & Madhu Sudan (2023)

- "Algebraic Coding Theory", Mary Wootters (2021)