Presentation Title: **Algebraic Coding Theory**

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Akash Talukder
IT-23610
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

Outline

- Error-Detecting and Correcting Codes
- Linear Codes
- Parity-Check and Generator Matrices
- Efficient Decoding
- Application
- Conclusion
- References

Objectives

- - Understand the fundamental principles of error detection and correction.
- - Explore the structure and significance of linear codes.
- - Learn about the roles of parity-check and generator matrices in coding theory.
- - Develop insights into efficient decoding strategies for codes.

Error-Detecting and Correcting Codes

Key Concepts:

- \- Error Detection: Techniques to identify errors in transmitted messages.
- \- Error Correction: Strategies to recover the original message.
- \- Importance: Reliable communication in digital systems (e.g., data storage, networking).

Key Terms:

- Hamming Distance: Measures the minimum difference between codewords.
- \- Error-Detecting Codes: Identify whether errors have occurred.
- \- Error-Correcting Codes: Recover data by fixing errors.

- \- Examples:
- 1. Parity Bits: Simple method for detecting single-bit errors.
- 2. Hamming Codes: Corrects single-bit errors and detects double-bit errors.

Linear Codes

Key Concepts:

- \- Linear Codes: A subspace of a vector space over a finite field.
- \- Advantages: Simplifies encoding and decoding processes.

Key Properties:

- \- Codeword Formation: A linear combination of basis vectors.
- \- Dimension (k): Represents the number of independent vectors (information bits).
- \- Length (n): Total number of bits in a codeword.
- \- Minimum Distance (d): Smallest Hamming distance between any two codewords.

Applications:

- \- Data transmission (e.g., satellite communication).
- \- Data storage (e.g., RAID systems).

Parity-Check and Generator Matrices

Key Concepts:

- - Generator Matrix (G): Converts a message vector into a codeword.
- - Dimensions: $k \times n$.
- - Ensures linearity of the code.
- - Parity-Check Matrix (H): Verifies the validity of codewords.
- - Relation: $H \cdot C^T = 0$, where C is a codeword.

Illustration:

- 1. Encoding with G: $C = m \cdot G$, where m is the message vector.
- 2. Error Detection with H: Compute $H \cdot r^T$, where r is the received vector.

Examples:

- - Hamming Codes: Use parity-check matrices for error detection and correction.

Efficient Decoding

Key Concepts:

- \- Objective: Decode received vectors efficiently, correcting errors where possible.

Techniques:

- \- Syndrome Decoding:
- \- Computes $S = H \cdot r^T$, where r is the received vector.
- \- Identifies the error pattern using the syndrome vector S.

Iterative Decoding:

- \- Used for advanced codes like LDPC and Turbo codes.

Applications:

- \- Wireless communication.
- \- Error-prone environments (e.g., deep-space communication).

Applications

- - Reliable data transmission in:
- 1. Wireless communication.
- 2. Satellite and deep-space communication.
- 3. Data storage systems.

Conclusion

- - Coding theory ensures reliability in data communication.
- - Applications span critical areas of technology and science.

References

- - Thomas W. Judson, *Abstract Algebra: Theory and Application.*
- - Additional research articles on coding theory.

Thank You