MTS 513	Algebraic Coding Theory	4 Credits (48 hours)

Course Outcome: This course is intended to impart knowledge in concepts and tools of Applied Algebraic Coding Theory. Students will understand the concepts of Applied Algebraic Coding Theory and apply them in data compression, error correction, cryptography and network coding.

Course Specific Outcome At the end of the course Students will have the knowledge and skills to understand, explain in depth and apply in various situations the concepts –

- Binary codes
- Arithmetic operations modulo an irreducible binary polynomial
- Irreducible q-array polynomials
- Finite fields and the factorization of polynomials over finite fields
- Cyclic binary codes

Unit I - Basic Binary Codes :
Repetition Codes and Single-Parity-Check Codes, Linear Codes, Hamming Codes, Manipulative Introduction to Double-Error-Correcting BCH Codes, Problems.

(4Hours)

Unit II - Arithmetic Operations Modulo an Irreducible Binary Polynomial:
A Closer Look at Euclid's Algorithm, Logical Circuitry, Multiplicative Inversion, Multiplication, The Solution of Simultaneous Linear Equations, Special Methods for Solving Simultaneous Linear Equations When the Coefficient Matrix is Mostly Zeros.

(6 Hours)

Unit III - The Number of Irreducible q-array Polynomials of Given Degree:
A Brute-Force Attack, Generating Functions, The Number of Irreducible Monic q-ary, Polynomials of Given Degree—A Refined Approach, The Moebius Inversion Formulas.

(8 Hours)

Unit IV - The Structure of Finite Fields:
Definitions, Multiplicative Structure of Finite Fields, Cyclotomic Polynomials, Algebraic Structure of Finite Fields, Examples, Algebraic Closure, Determining Minimal Polynomials, Problems

(10 Hours)

Unit V - Cyclic Binary Codes:
Reordering the Columns of the Parity-Check Matrix of Hamming Codes, Reordering the Columns of the Parity-Check Matrix of Double-Error-Correcting Binary BCH Codes, General Properties of Cyclic Codes, The Chien Search, Outline of General Decoder for any Cyclic Binary Code, Example, Equivalence of Cyclic Codes Defined in Terms of Different Primitive nth Roots of Unity.

(10 Hours)

Unit VI - The Factorization of Polynomials Over Finite Fields:
A General Algorithm, Determining the Period of a Polynomial, Trinomials Over GF(2), Factoring $x^n - 1$ Explicitly, Determining the Degrees of the Irreducible, Factors of the Cyclotomic Polynomials, to check whether Number of Irreducible Factors of *f(x)* Over *GF(q)* is Odd or Even, Quadratic Reciprocity.

(10 Hours)

References

[1] Elwyn Berlekamp, *Algebraic Coding Theory*, Revised Ed., World Scientific Publishing Pvt. Ltd, 2015.

[2] L. R. Vermani, *Elements of Algebraic coding theory*, Chapman and Hall, First edition 1996.

[3] Raymond Hill, *A first course in coding theory*, Claronden Press Oxford, 1986.

[4] N Abrahamson, *Information theory and coding*, Mc Graw Hill, 1963.

[5] Sriraman Sridharan and R. Balakrishnan, *Discrete Mathematics, Graph algorithms Algebraic structures, Coding theory and Cryptography*, Chapman and Hall, CRC Press. 2019.