

Algebraic Coding Theory

Tovohery H. Randrianarisoa

email: tovo@aims.ac.za

profile: <https://sites.google.com/a/aims.ac.za/tovo/>

Overview

The fundamentals of coding theory is studied. We learn about various algebraic constructions of linear codes and their properties. Applications of error correcting codes are presented.

Prerequisite

The students are expected to know linear algebra.

Course contents

- Applications of error correcting codes to information transmission and storage.
- Basic theory of finite field.
- Linear codes (Hamming distance, parity and generator matrix).
- Bounds on linear codes (Singleton, Hamming, Gilbert-Varshamov...).
- Various constructions of linear codes (BCH codes, Reed-Solomon codes, quadratic residue codes, Reed-Muller codes...)
- Decoding methods: syndrome decoding, decoding of BCH/Reed-Solomon codes.
- Application to Post-Quantum cryptography (Code-based cryptography).
- Extra: Generalized weights and their application, geometric approach to linear codes.

References

- J.H. van Lint, “Introduction to Coding Theory”, Graduate Texts in Mathematics, No. 86, Springer, 1982.
- E.R. Berlekamp, “Algebraic Coding Theory”, World Scientific Publishing Co., 2015.