37. On the investigation of structure and properties cyclic codes over gf(2) and application of these codes to encryption and decryption of data.

Beatrice Munjuri Gacheri[1,*], Loyford Njagi[1] and Josephine Mutembei[1]

[1]Department of Mathematics. Meru University of Science and Technology.

*Corresponding author email: munjurib@gmail.com

Subtheme: Computing and Informatics - Leveraging Computing and informatics Technologies for Climate adaptation and resilience

Abstract

Cyclic codes are a crucial subset of linear error-correcting codes with distinct algebraic properties that facilitate efficient encoding and decoding. These properties make them highly suitable for various cryptographic applications, including encryption, decryption, error detection, and error correction. The research delves into the theoretical foundations of cyclic codes, focusing on their algebraic structures, including generator polynomials, invariance under cyclic shifts, and closure properties. The study also investigates encoding and decoding techniques, as well as error correction capabilities, using both analytical and practical approaches. Cyclic codes are implemented in various real-world cryptographic systems for tasks such as Redundancy Check, error-checking, and error correction. Their structure allows for efficient hardware and software implementations using shift registers. The research highlights the practicality and efficiency of using cyclic codes in secure communication protocols, enhancing the reliability and security of data transmission. The findings reveal that cyclic codes, defined by their generator polynomial, exhibit invariance under cyclic shifts and closure under addition and multiplication. The length of a cyclic code is determined by the degree of the generator polynomial plus one. The study shows that these codes can be systematically organized, simplifying the decoding process. Practical applications demonstrate that cyclic codes are effective in encrypting and decrypting data, providing robust security measures for cryptographic systems.

Key Words: *Cyclic codes, Encryption, Decryption*