Vol.4 (Iss.2),pp.49-60, 2024, ISSN:2788-5844 http://sciencemundi.net

On Some Aspects Of Degenerated Cyclic Codes

Boaz Simatwo Kimtai[1]
Lao Hussein Mude[2]
Patrick Wanjala Makila[3]

[1] *kimtaiboaz96@gmail.com*
[2] *hlao@kyu.ac.ke*
[3] *makilapatrick@yahoo.com*

[1] *Department of Mathematics and Actuarial Sciences, Kisii University, P.O.Box 408-40200, Kisii, Kenya.*
[2] *Department of Pure and Applied Sciences, Kirinyaga University, P. O. Box 143-10300, Kerugoya, Kenya.*
[3] *Department of Mathematics and Computer Science , University of Eldoret, P.O. Box 1125-30100, Eldoret, Kenya.*

Original Research Article

Received: 13 May 2024
Accepted: 26 July 2024
Published: 06 August 2024

ABSTRACT

Degenerated cyclic codes constitute a fascinating area of study within Coding Theory, offering profound insights into the realm of algebraic structures and their applications in error detection and correction. In this work, we delve into various aspects of degenerated cyclic codes, aiming to provide a comprehensive understanding of their properties and significance. We begin by elucidating the fundamental concepts underlying cyclic codes and their degeneration, establishing mathematical framework for analysis. Subsequently, we explore the algebraic structure of degener-ated cyclic codes, investigating their generator and parity-check matrices, as well as their relation-ships with conventional cyclic codes. Moreover, we investigate the decoding algorithms tailored for degenerated cyclic codes, evaluating their efficiency and performance under different error conditions. Furthermore, we examine the applications of degenerated cyclic codes in practical scenarios, highlighting their utility in diverse domains such as telecommunications, storage systems, and cryptography. Through theoretical analysis and numerical simulations, we demonstrate the efficacy and versatility of degenerated cyclic codes, thereby emphasizing their significance in modern information theory. Overall, this study contributes to the advancement of coding theory by shedding light on the intricacies of degenerated cyclic codes and paving the way for future research endeavors in this burgeoning field.

Keywords: Cyclic codes, linear block codes, algebraic coding, generator polynomials.

Mathematics Subject Classification: Primary 11H71; Secondary 14G50.

1 Introduction

Degenerate cyclic codes are subset of cyclic codes,[1, 4, 8, 12, 13, 16, 18, 20, 22] which are linear block codes defined by shifts of their codeswwords. Mathematically, a cyclic code of length n is generated by a polynomial $g(y)$ of degree r, where r is the dimension of the code. The codewords are obtained by polynomial multiplication of the message polynomial by $g(y)$ modulo $< y^n - 1 >$.
In the case of degenerate cyclic codes[22] , we intentionally introduce irregularities into the code by modifying certain coefficients of the generator polynomial $g(y)$. This modification results in a generator polynomial that may not conform to the standard form of a cyclic code. One common way to achieve degeneracy is by setting specific co-efficients of $g(y)$ to zero or adjusting them from their typical values. Mathematically, let $g(y) = g_0 \oplus g_y \oplus ... \oplus g_r y^r$ be the generator polynomial as defined in [2] of the cyclic code where $g_0, g_1, ..., g_r$ are coefficients in some finite field. To introduce degeneracy, we may set certain coefficients to zero, such as g_0 or g_r or modify them from their usual values. For instance, we could intentionally make $g(y)$ not monic, that is, $(g_r \neq 1)$, which leads to departure from the standard cyclic code.
Despite those modifications, degenerate cyclic codes still retain some crucial properties. For example, they remain cyclic, meaning that cyclic shifts of code words are still code words. This property facilitates efficient encoding and decoding algorithms, levaraging the structure inherent in cyclic codes thus contributing to coding theory [2, 5, 6, 7, 14, 19, 23].
Understanding Mathematical intricacies of degenerate cyclic codes is crucial for analyzing their properties, designing specific applications including specific applications and unique characteristics. Researchers often explore various methods for constructing and analyzing degenerate cyclic codes to unlock their potential advantages in error control, cryptography and their areas of information theory.

Departure of degenerated cyclic codes:
Degenerate cyclic codes, a subset of cyclic codes, have been studied for their structural properties and practical applications in error correction. Here are some works that delve into these codes and highlight the point of departure from degenerate cyclic codes to more general or different types of codes.

Firstly, the research in [9] provides a comprehensive overview of various error-correcting codes, including cyclic codes and discusses the properties of degenerate cyclic codes and transitions into the study of more general cyclic codes, BCH codes, and Reed-Solomon codes. Secondly, San and Chaoping [11] discuss cyclic codes and then explores the limitations of degenerate cyclic codes, moving on to more robust coding schemes such as BCH codes and Goppa codes. In [15], Mattson provides a detailed examination of error control coding techniques including cyclic codes. The research highlights the characteristics of degenerate cyclic codes, and then transitions to more powerful error-correcting codes like LDPC codes and turbo codes. Also, Ron [17], explains the concept of degenerate cyclic codes and their limitations, before introducing more advanced topics such as algebraic geometry codes and convolutional codes. In [3], Blahut provides a thorough understanding of algebraic codes, including cyclic codes. The research discusses the departure from degenerate cyclic codes to more efficient

codes like Reed-Solomon codes, focusing on their application in data transmission.

These works collectively illustrate the evolution of coding theory from the study of degenerate cyclic codes to the development and application of more advanced and efficient error-correcting codes. They highlight the limitations of degenerate cyclic codes and the need for more powerful coding schemes in practical applications.

2 Preliminaries

Degenerate cyclic codes are a subset of cyclic codes characterized by repeated or linearly dependent code words due to the generator polynomial having repeated roots, resulting in reduced error-correcting capabilities and lower minimum distances. They illustrate the importance of polynomial selection in the design of cyclic codes. By studying these degenerate cases, we gain insights into the properties that make certain cyclic codes more effective for error correction, guiding the development of more powerful and reliable coding schemes.

Cyclic codes A *cyclic code* of length [1, 4, 8, 12, 18, 20, 22] n over a finite field F_q is a linear code such that if $c = (c_0, c_1, \ldots, c_{n-1})$ is a code word, then the cyclic shift $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also a code word. Mathematically, this can be expressed as follows:

Theorem 2.1. *Let C be a linear code of length n over F_q. Then C is a cyclic code if and only if for every code word $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the code word $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ also belongs to C.*

Generator polynomial: Given a cyclic code of length n over a finite field F_q, the generator polynomial $g(x)$ is a polynomial of degree k that divides $x^n - 1$ in $F_q[x]$. The code consists of all multiples of $g(x)$ modulo $x^n - 1$, and can be expressed as:

$$\mathcal{C} = \{c(x) = g(x)q(x)(x^n - 1) \mid q(x) \in F_q[x], \deg(q(x)) < n - k\}$$

Parity Check Matrix: The parity check matrix H of a cyclic code can be constructed using the generator polynomial g(y). It has dimensions $(n - r) \times n$ and it is derived from coefficients of $g(y)$ using certain algebraic structure.

Degenerated Cyclic Codes: A degenerate cyclic code of length n over a finite field F_q is a linear code characterized by the following properties:

i. It is a subset of the cyclic code, where the code words exhibit redundancy or linear dependence.

ii. The generator polynomial $g(x)$ of the code has at least one repeated root over F_q, causing the code to contain repeated or linearly dependent code words.

iii. Formally, if $g(x)$ is the generator polynomial of degree k, then the code can be described as:

$$\mathcal{C} = \{c(x) = g(x)q(x)(x^n - 1) \mid q(x) \in F_q[x], \deg(q(x)) < n - k\}$$

where $\mathcal{C}$ denotes the set of all code words of the degenerate cyclic code.

Relaxed ConStraints: Degenerated cyclic codes involve relaxing some of the constraints imposed on standard cyclic codes, such as the requirement for the generator polynomial to divide $< y^n - 1 >$ exactly. This relaxation allows for a border range of polynomial structures, potentially leading to improves code properties or easier encoding-decoding procedures.

Algebraic Operations: Analysis of cyclic and degenerated cyclic codes involves algebraic operations in polynomial rings and quotient rings. Addition and scalar multiplication of polynomials modulo $< y^n - 1 >$ are fundamental operations used in code construction and manipulation.

Ring Theory: The study of quotient rings and ideals provide rigorous mathematical foundation for understanding the structure and properties of cyclic and degenerated cyclic codes. Concepts from Ring Theory, such as factorization and prime ideals, play a crucial role in code analysis.

Code distance and error correction: Analysing the distance properties both standard and degenerated cyclic codes involving examining the algebraic relationships between code elements and their implications for error detection and correction algorithms [10, 21].

Magma Algorithms for constructing the degenerated cyclic codes:

Example in Magma

```
n := 7;
F := GF(2);
R<x> := PolynomialRing(F);
g := (x - 1)^2 * (x^3 + x + 1);

C := CyclicCode(n, g);
Codewords := { c : c in C };
"Minimum Distance:", MinimumDistance(C);
"Weight Distribution:", WeightDistribution(C);

Cyclic Code: [7, 4, 3] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 1 1 0]
[0 1 0 0 0 1 1]
[0 0 1 0 1 1 1]
[0 0 0 1 1 0 1]
Minimum Distance: 3
Weight Distribution: [ <0, 1>, <3, 7>, <4, 7>, <7, 1> ]
```

3 Main Results

In the research work of the paper we assume $HCF(n, q) = 1$, hence give some aspects of degenerated cyclic codes of length n over F_q.

Theorem 3.1. *Let $HCF(n,q)=1$. These statements are equivalent. [20, 22]*

i. **The generator polynomial $g(y)$ has no repeated roots modulo y^n-1:** This asserts that the generator polynomial of the cyclic code, $g(y)$, does not have any repeated roots when considered modulo y^n-1, meaning that every root has multiplicity 1.

ii. **The code has no repeated code words:** This implies that the cyclic code does not contain any repeated code words. Each distinct message corresponds to unique code word in the code word. Now, lets establish the equivalence between these statements in the context where $gcd(n,q)=1$. Firstly, for cyclic codes [1, 4, 8, 12, 13, 16, 18, 20, 22] over $GF(q)$, where q is the size of the finite field. If the $gcd(n,q)=1$, then the order of any non-zero element in $GF(q)$ is co-prime to n. This implies that the polynomial y^n-1 has distinct roots in the field $GF(q)$, as every non-zero element generates a distinct root. Consequently, any polynomial $g(y)$ with distinct roots will also have distinct roots modulo y^n-1. Since the roots of $g(x)$ are distinct modulo y^n-1, it follows that the corresponding code words will also be distinct, ensuring that $gcd(n,q)=1$.
Thus, under the condition $gcd(n,q)=1$, the statements, "the generator polynomial $g(y)$ has no repeated roots modulo $<y^n-1>$," and, "the code has no repeated code words," are equivalent in the context of degenerated cyclic codes.

Proof. A cyclic code C of length n over F_q is degenerate:

i **Degeneracy of cyclic code:** Degeneracy of cyclic codes arises when certain coefficients of its generator polynomial manipulated to deviate from the typical form. This manipulation introduces irregulatories into the into the code's structure, leading to the departure from the standard cyclic geometry.

ii **Mathematical elaboration:** Let $g(y)$ be the generator polynomial of the cyclic code C. It is typically of the form $g(y)=g_0+g_1y+...+g_ry^r$ where $g_0,g_1,...,g_r$ are coefficients in F_q.
In the case of a degenerate cyclic code, certain coefficients of $g(y)$ are modified from their standard values. This modification could involve setting specific coefficients to zero, adjusting them arbitrarily, or making the polynomial non-monic, that is, leading coefficients g_r is not necessarily 1.

Mathematically, the manipulation of coefficients might be represented as $g(x)=g_0'+g_1'y+...+g_r'y^r$ where $g(x)=g_0'+g_1'+...+g_r'$ are the altered coefficients. □

Implication of degeneracy: The introduction of irregularities into the generator polynomial alters the algebraic structure of the code. This deviation from the standard cyclic symmetry can affect the properties such as minimum distance, error-correction, and decoding complexity.
Degenerate cyclic codes may exhibit unique characteristics that make them suitable for specific applications, for example, intentional degeneracy might enhance the code's ability to correct certain types of errors to improve performance under particular channel conditions.

In summary, the degeneracy of cyclic codes over F_q is manifested through intentional modifications to its generator polynomial, leading to deviations from the standard cyclic structures. Understanding the mathematical implications of degeneracy is essential for analyzing the properties and applications of such codes in various communication and storage systems.

Theorem 3.2. *There exist integers* $r, 1 < r < n$, *and* $s, 1 < s < n$, *such that* $n = rs$ *and* $1 + y^s + ... + y^{(r-2)s} + y^{(r-1)s}$ *divides* $g_c(y)$.

Proof. Given $n = rs$, where $1 < r < n$ and $1 < s < n$, we can express $gC(y)$ as $gC(y) = (1 + y^s + ... + y^{(r-2)s} + y^{(r-1)s})Q(y)$ mod rs since $n = rs$, we can rewrite the expression as: $gC(y)$ mod n $= (1 + y^s + ... + y^{(r-2)s} + y^{(r-1)s})Q(y)$ mod n.

Now, we can see that each term of the $(1+y^s+...+y^{(r-2)s}+y^{(r-1)s})$polynomial will be congruent to zero modulo n because each term is divisible by s, (which divides n), modulo n, implying that n divides $g(y)$. So, $n = rs$ divides $gC(y)$, content... □

Theorem 3.3. *There exists integer* $r, 1 < r < n$, *and* $s, 1 < s < n$, *such that* $n = rs$ *and* $g_C^{\perp}(y)$ *divides* $y^s - 1$.

Proof. Given $n = rs$, where $1 < r < n$ and $1 < s < n$, we show that $g_C^{\perp}(y)$ divides $y^s - 1$. First, lets express $y^s - 1$ in terms of its factors.
By using the difference of squares formula, we have $y^s - 1 = (y^{\frac{s}{2}} - 1)(y^{\frac{s}{2}} + 1)$.
Now, we want to show that $g_C^{\perp}$ divides $y^s - 1$, or equivalently, that, $y^s - 1$ is congruent to zero modulo $g_C^{\perp}(y)$.

Lets express this mathemayically:
$y^s - 1 \equiv 0 \text{mod} g_C^{\perp}(y)$
This means that there exists some $P(y)$ such that $y^s - 1 = p(y).g_C^{\perp}(y)$
Now we need to show that such a polynomial $P(y)$ exists:
Given that $n = rs$ divides $gC(y)$ according to the definition of $gC(y)$ it follows that $g_C^{\perp}(y)$ must divide $y^s - 1$ because $y^s - 1$ is a factor of $y^r - 1$ (by setting $r = \frac{s}{2}$).
Therefore, we have shown that there exist integer r and s, such that $n = rs$ and $g_C^{\perp}(y)$ divides $y^r - 1$. □

Theorem 3.4. *Let* $m > 1$. *Let* C' *be a cyclic code of length* n'. *Let* $C = R_m(C')$ *be a degenerate cyclic code. Then given:*

i) $m > 1$

ii) C_1 *is a cyclic code of length* n_1

iii) $C = R_m(C_1)$ *is a degenerate cyclic code, where* R_m *denotes the* m^{th} *repeated concatenation operation.*

Proof. The repeated concatenation operation R_m takes cyclic code C_1 and replicates m times.
Now, we want to understand the properties of the degenerate cyclic code C obtained by $m-$fold repetition of C_1
Lets denote the generator polynomial of C_1 as $g_1(y)$. Since C_1 is cyclic, $g_1(y)$ generates C_1 and divide $(y^{n_1} - 1)$.

□

Now, to understand C mathematically, we need to analyze its properties:

i) **Linearity:** C is still a linear code because repetition does not affect linearity of the code, [19].

ii) **Cyclic property:** C inherits the property from C_1 because the cyclic shifts of codewords in C_1 will result in cyclic shifts of codewords in C, [1, 4, 8, 12, 18, 20] .

iii) **Generator polynomial:** The generator polynomial of C is $g(y) = [g_1(y)]^m$,[2].

iv) **Minimum distance:** The minimum distance of C may change depending on the property of C_1 and m. If C_1 has a minimum distance d_1, then C will have a minimum distance atleast d_1 (but it could be higher depending on specific codewords resulting from the repetition), [20].

v) **Encoding and decoding:**Encoding and decoding for C can be derived from these of C_1, possibly with some modifications due to repetition, [6, 10, 21] .
In summary, a degenerate cyclic code obtained by repeating a cyclic code with modified parameters, while retaining many of the properties of the original code

From $g_C(y) = g_{C'}(y)(1 + y^{n'} + y^{2n'} + ... + y^{n-n'})$, then:

i) $gC(y)$ is the generator polynomial of a cyclic code C of length n.

ii) $gC_1(y)$ is the generator polynomial of a cyclic code C_1 of length n_1.

iii) The expression $(1 + y^{n'} + y^{2n'} + ... + y^{n-n'})$ represents the polynomial factor.

Thus the equation $g_C(y) = g_{C'}(y)(1 + y^{n'} + y^{2n'} + ... + y^{n-n'})$ states that the generator polynomial of C can be obtained by multiplying the generator polynomial of C_1 with a polynomial factor that accounts for certain cyclic shifts.

Hence elaborating Mathematically:

i. **Generator polynomial of C:** The generator polynomial $gC(y)$ of code C represent all the code words of C which generates the cyclic code C that has a length of n.

ii. **Generator polynomial of C_1:** The generator polynomial $gC_1(y)$ of code C_1 represent all the code words of C_1 which generates the cyclic code C_1 that has a length of n_1.

iii. **Polynomial factor:** The polynomial factor $(1 + y^{n'} + y^{2n'} + ... + y^{n-n'})$ represents a polynomial that includes terms corresponding to the cyclic shifts of the code words of C_1 to form code words of C. The terms account for the cyclic nature of the code.

iv. **Multiplication:** Multiplying $gC_1(y)$ by the polynomial factor results to a new polynomial, $gC(y)$, which includes all the terms needed to generate the codewords of C based on the codewords of C_1, and their cyclic shifts.

In summary, the equation $g_C(y) = g_{C'}(y)(1 + y^{n'} + y^{2n'} + ... + y^{n-n'})$ mathematically expresses how the generator polynomial of a cyclic code C can be constructed from the generator polynomial of a cyclic code C_1 by inco-orperating a polynomial factor that accounts for the cyclic shifts. Generally, see [2]. Given $g_C{}^{\perp}(y) = g_C{}^{\perp}(y)$ suggests that the dual generator polynomial of a cyclic code C is equal to the dual generator polynomial of another cyclic code C_1, that is:

i. $gC^{\perp}(y)$ is the dual generator polynomial of a cyclic code C.

ii. $gC_1{}^{\perp}(y)$ is the dual generator polynomial of another cyclic code C_1.

The dual generator polynomial represents the polynomial whose roots correspond to the non-zero elements of the dual code. The dual code of a cyclic code is also cyclic on $gC^{\perp}(y) = gC_1{}^{\perp}(y)$ mathematically, thus we can consider the properties of the dual codes:

i. **Generator polynomial of the dual code:** The dual generator polynomial $gC^{\perp}(y)$ of a code C generates a dual code, whose codewords are orthogonal to the codewords of C.

ii. **Generator polynomial of the dual code C_1:**
Similarly, $gC_1{}^{\perp}(y)$ generates the dual cyclic code $gC_1{}^{\perp}$ which is orthogonal to the codewords of C_1.

iii. **Equivalence of the dual codes:** The equation $gC^{\perp}(y) = gC_1{}^{\perp}(y)$ implies the dual cyclic code $C^{\perp}$ and $C_1{}^{\perp}$ polynomial. This means that the structure of the orthogonal codewords of C and C_1 is the same.

iv. **Orthogonal preservation:** Since the dual generator polynomial determines the structure of the orthogonal codewords, the equation suggests that orthogonality properties are preserved between $C^{\perp}$ and $C_1{}^{\perp}$.

In summary, the equation $gC^{\perp}(y) = gC_1{}^{\perp}(y)$ mathematically expresses that the dual generator polynomial of a cyclic code is equal to the dual generator polynomial of another cyclic code C_1, indicating that their dual codes have same structure and orthogonal properties.

Theorem 3.5. *Let $gcd(n, g) = 1$. Let $n = p_1^{e_1}, ..., p_t^{e_t}$ be the prime decomposition of n, let $N(d)$ be the number of the divisors of $X^d - 1$ over F_q. Then the number of the degenerate cyclic codes of length n over F_q is $\sum_{l=1}^{t}(-1)^{l+1} \sum_{\{i_1,...,i_l\}\in\{1,...,t\}} N(\frac{n}{p_{i_1},...,p_{i_l}})$*

Proof. The proof can be found in [20] □

This theorem addresses the enumeration of degenerate cyclic codes over a finite field F_q of the length n, under the condition that the gcd of n and q is 1. Lets break down the theorem and its mathematical implications:

3.0.1 Degenerate cyclic codes

Cyclic codes are subclass with additional properties.

Definition 3.1. *N(d)is the number of divisors of $y^d - 1$ over F_q, In other words, it presents the number of elements in F_q that are roots of the polynomial $y^d - 1$.*

Cyclic codes are subclass with additional properties
Implications:
The theorem suggests a connection between the structure of cyclic codes and the roots of certain polynomials over the finite field F_q.
The prime factorization of n plays a crucial role in determining the number of degenerate cyclic codes of length n over F_q.
It involves the summation over subsets $\{i_1, ..., i_l\}$ of the subset $\{1, ..., t\}$, where t is the number of the distinct primr factors in the prime factorization of n.
For each subset, the product $n = p_1^{e_1}, ..., p_t^{e_t}$ is calculated, representing a divisor of n obtained by

selecting certain prime factors and their correspondiiing exponents.
The function N comes into play to count the number of roots of $y^d - 1$ over F_q where d is the divisor obtained from the current subset **Mathematical Elaboration:**
The theorem involves iterating over all possibilities subsets of prime factors of n, each time calculating a divisor d of n and finding the number of roots of $y^d - 1$ over F_q
These counts are then combined using a summation formula with alternating signs $(-1)^{l+1}$ where l is the size of the current subset being considered.
The result of this computation gives the number of degenerate cyclic codes lengthn n over F_q. In summary, the above Theorem provides a Mathematical relationship between the structure of cyclic codes and properties of certain polynomials over finite finite fields, specifically in terms of their roots and the prime factorization of the code length.

Theorem 3.6. *Let $m > 1$, let $C = R_m(C')$ degenerate cyclic code. Then $\mathcal{H}(C) = \mathcal{R}_m(\mathcal{H}(C'))$.*

Proof. The proof can be found in [20]. □

Definition 3.2. *Let C be a degenerate cyclic code over F_q, where $C = \mathcal{R}_m(C)$. Here, $\mathcal{R}_m$ denotes the ring formed by polynomials of degree less than m over F_q.*
Let $\mathcal{H}(C)$ be the parity-check matrix.
Let $C^\perp$ denote the dual code of C.

Theorem 3.7. $\mathcal{H}(C) = \mathcal{R}_m(\mathcal{H}^\perp_{C^\perp})$.

Proof. Let $\{g_1, g_2, ..., g_k\}$ be the basis for C, then, $\mathcal{H}(C)$ is formed by taking two row vectors corresponding to the orthogonal complements of $g_1, g_2, ..., g_k$.

The dual code $C^\perp$ consist of all vectors v such that $< v, c >= 0$ for all $c \in C$, where $< ., . >$ denote the dot product.
Let $\{h_1, h_2, ..., h_k\}$ be a basis for $C^\perp$.
Then, $\mathcal{H}^\perp_{C^\perp}$ is formed by taking the row vectors corresponding to $\{h_1, h_2, ..., h_k\}$.
Since C is degenerate cyclic code, its generator polynomial can be represented as $g(y) = yhy$, where $h(x)$ is a polynomial degree $k - m$
$\mathcal{H}(C)$ be represented as $\mathcal{H}^\perp_{C^\perp}$ due to specific structure induced by degenerate by cyclic code of C.
Thus, theorem establishes a specific relationship between the parity-check matrix of a degenerate cyclic code and the parity-check matrix of its dual code. □

Corollary 1. *Let $m > 1$, let $C = R_m(C')$ degenerate cyclic code. Then $\mathcal{H}(C) = \mathcal{R}_m(\mathcal{H}(C'))$, See [20].*

In this corollary, C' represents the generator polynomial of the cyclic code C. The statement suggests the Hamming Weight of a code C is euivalent to the hamming weight of its generator polynomial C'.
Elaborating mathematically, we can explain it as follows:

a **Degenerate cyclic codes:** A cyclic code C is called degenerate if its generator polynomial has roots in common, $y^m - 1$ for $m > 1$.

Licensed Under Creative Commons Attribution (CC BY-NC)

b **Generator polynomial:** Let C' be the generator polynomial of C. Since C is a cyclic code, C' is a divisor of $y^m - 1$, that is, $y^m - 1 = g(y).C'(y)$ for a polynomial $g(y)$, [22].

c **Hamming Weight of C:** The Hamming Weight of code C is the minimum weight among all non-zero codewords in C denoted by $dim_H(C)$. This represents the number of non-zero elements in the smallest non-zero codeword.

d **Hamming Weight of C':** Similarly, the Hamming Weight of C', denoted by $dim_H(C')$, represents the number of non-zero co-efficients in C'.

Given the degeneracy property, the number of non-zero co-efficients in C' is the same as the minimum weight of C, which is the number of non-zero elements in the smallest non-zero codeword in C. Thus $dim_H(C) = dim_H(C')$.

Definition 3.3. *Degenerated cyclic codes, also known as degenerate cyclic codes, are a type of a linear code where some codewords are repeated or redundant, leading to reduced effective capability*

Here is a perfect example to illustrate this concept:
Consider a binary cyclic code with a generator polynomial $g(y)$. In degenerated cyclic codes, the generator polynomial $g(y)$ is such that the contains repeated codewords. This can occur when $g(y)$ is not irreducible or when the code length is not relatively to the field size.
Example of a degenerated cyclic code:

i **Field:** Lets work over the binary field $GF(2)$.

ii **Code length:** Consider a code of length 4.

iii **Generator polynomial:** Let $g(y) = y^2 + 1$

Step-by-step construction:

i **Generating the code:**
The generator polynomial $g(y) = y^2 + 1$ is used to generate codewords. The codewords are obtained by multiplying $g(y)$ by all polynomials of degree less than $n - k$, where n is the code length and k is the degree of the generator polynomial.

ii **Codewords:**
-Multiply $g(y)$ by 1: $g(y) \times 1 = y^2 + 1 \rightarrow 1100$
-Multiply $g(y)$ by y: $g(y) \times y = y^3 + y \rightarrow 0110$
-Multiply g(y) by y^2: $g(y) \times y^2 = y^4 + y^2 = y^4 + y^2 \equiv y^2$ (Since y^4 in a binary field of length 4 cycles back to $x^0 \rightarrow 0011$
-Multiplying $g(y)$ by $y^3 : g(y) \times y = y^5 + y^3 \Longrightarrow y^5 + y \equiv 0$ (Since y^5 in the binary field of length 4 cycles back to y^1 and adding y in binary results in o) $\rightarrow 0000$

Thus, here the codewords are:

- 1100
- 0110
- 0011
- 0000

Notice that 0000 is the repeated codeword that reduces the effective error-correcting capability of the code. This repetition makes the code degenerate or degenerated.

The above example shows a degenerated cyclic code where the presence of all-zero codeword 0000 (resulting from the polynomial multiplication) indicates redundancy and a reduction in the effective error-correcting power of the code. This is a typical characteristic of degenerated cyclic codes.

4 Conclusion

Let C be a cyclic code over F_q of length n and dimension k. The cyclic code C is defined by a generator polynomial $g(y)$ and its elements are multiples of this polynomial in $F_q[y]/< y^n - 1 >$.
For $m > 1$, the code $R^m(C)$ is formed by taking all multiples of $g(y^m)$ in $\frac{F_q[y]}{y^n-1}$.
These multiples form a cyclic code. Thus, researchers can further explore on circulant bases for degenerated cyclic codes. The condition likely effects the properties and behaviour of cyclic codes, but its specific implications need to be explored further. It may influence the structure of the code, the existence of certain types of codewords, or other properties to their relevant study. To elaborate further mathematically, one could delve into specific algebraic structures and properties of cyclic codes. Additionally, exploring the impact of the condition $gcd \neq 1$ on algebraic properties of cyclic codes would be crucial for comprehensive understanding.

References

[1] Intan M. A., Djoko S., Aleams B., (2021). Cyclic codes from a sequence over finite fields. *European Journal of Pure and Applied Mathematics*, 14(3).

[2] Louis B (2014). On the generators of cyclic codes. International *Journal of Pure and Applied Mathematics*, 94(1):71–80.

[3] Richard E. B., (2003). Algebraic codes for data transmission. *Cambridge University Press*.

[4] Steven T. D., Suat K., and Bahattin Y.(2012). Cyclic codes over r k. Designs, Codes and Cryptography, 63:113–126.

[5] Thomas E. and Victor Z. (2001). Codes on Euclidean spheres. *Elsevier*.

[6] Olege F. (2019). On the generators of codes of ideals of the polynomial ring fn. *In International Mathematical Forum*, volume 14, 189–203.

[7] David F.(1965) Concatenated codes.

[8] Lao H., Benard K., Patrick K., and Geoffrey M. (2018). On the number of cyclotomic cosets and cyclic codes over.

[9] Florence J. M., and Neil J. A. (1977) The theory of error correcting codes," North-Holland mathematical library"." *North-Holland Pub. Co. New York*.

Licensed Under Creative Commons Attribution (CC BY-NC)

[10] Jeffrey L.(1982). Computing Automorphism groups of error-correcting codes. IEEE Transactions on Information Theory, 28(3):496–511.

[11] San L. and Chaoping X.(2004) Coding theory: a first course. Cambridge university press.

[12] Zhuojun L.(1998) A class of generalized cyclic codes. , 1038:223–229.

[13] Sergio R. L., Benigno R. P., and Steve S. (2009). Dual generalizations ´ of the concept of cyclicity of codes. *Adv. Math. Commun.*, 3(3), 227–234.

[14] Rolando G. M. and Felipe Z. (2014). On the category of group codes. arXiv preprint arXiv:1409.6382.

[15] Mattson J.(1985). Error control coding: Fundamentals and applications.

[16] Biljana R. (2019). Cyclic codes. *In Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research*, Singidunum University, 465–471.

[17] Roth, R. M. (2006). Introduction to coding theory. *IET Communications*, 47(18-19), 4.

[18] Simatwo, K. B., Mati, R. F., and Karieko, O. R. (2023). Enumeration of cyclic codes over GF (23). *Journal of Advances in Mathematics and Computer Science*, 38(9), 194-206.

[19] Nicolas S. (2000). Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Transactions on Information Theory*, 46(4):1193–1203.

[20] Kimtai B. S., Runji F. M., and Obogi R. K.(2023). Enumeration of cyclic codes over gf (23). *Journal of Advances in Mathematics and Computer Science*, 38(9),194–206.

[21] Gintaras S. (2000) Computing permutation groups of error-correcting codes. *Lietuvos matematikos rinkinys*, 40,320–328, 2000.

[22] Gintaras S.(2005) On degenerated cyclic codes. Lietuvos matematikos rinkinys, 45, 57–59.

[23] Qifu S.(2009). Network coding theory based on commutative algebra and matroids. *PhD thesis, Chinese University of Hong Kong.*