Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 61-66
https://idjams.com/index.php/jms/index

Minimum Distance Computation Efficiency in Module Codes over Finite Chain Rings

Ishlahrahmi Meishrin[1], Sisilia Sylviani[2,*], Amma Achiaa[3]

[1, 2] *Universitas Padjadjaran, Jl. Soekarno Km 21 Jatinangor, Kab. Sumedang, West Java 45363, Indonesia*

[3] *St. Monica's College of Education, Asante Mampong, Ghana*

[*] *Corresponding author: sisilia.sylviani@unpad.ac.id*

Copyright: ©2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License-(CC-BY-SA) (https://creativecommons.org/licenses/by-sa/4.0/)

Article Info

Article history:
Received: July 9, 2025
Revised: September 8, 2025
Accepted: September 9, 2025
Available online: October 22, 2025

DOI:
https://doi.org/10.71385/idjams.v2i2.26

Abstract

In coding theory, the module structure can be used in the construction and analysis of codes for reliable data transmission. A code that is effective in detecting and correcting errors that occur during data transmission is a good code. The parameter to determine the reliability of the code in error detection and correction is by calculating its minimum distance. However, to calculate the minimum distance, it is necessary to evaluate all the Hamming weights of all non-zero code words, if the size of the code are very long, the calculation of the minimum distance will take a long time so it is not very efficient if we use this method. Therefore, the module structure of the ring, especially over the finite chain ring, can be used to simplify the calculation process of the minimum distance. The complexity of calculating the minimum distance can be reduced by viewing the code as a module and utilizing its modular structure. Previous research has shown that certain structural characteristics of module codes can significantly simplify this computation. In this article, we present an efficient method for determining the minimum distance of a module code defined over a finite chain ring. We show that it only required the hamming weight of the code generator to find the code's minimum distance. This approach provide an efficient way to analyze the code's reability and give algebraic insight about the code's behaviour. Our article highlight the practical advantages of applying a module theory perspective to coding theory, which offers an efficient and theoretically grounded framework for evaluating and constructing error-correcting codes with strong performance guarantees.

Keywords: Error-correcting Codes; Finite Chain Ring; Hamming Weight; Minimum Distance; Module Codes

I. Introduction

Abstract algebra seems to be very theoretical but in reality, it is very useful especially in coding theory. One of the main uses of algebraic structures in this field is to develop an efficient and reliable communication systems [1]. The transmission of message across networks is often sensitive to noise, interference, or other forms of distortion [2]. The concept of modules over rings helps the construction of error-correcting with specific algebraic structure. These code makes the system not only can detect errors but also correct errors in the transmitted message. This theoretical concept is not limited to coding theory alone but also extends to other practical domains. For example, algebraic approaches have been applied in population dynamics through matrix-based models, as discussed in *An Algebraic Study of the Matrix Meta-Population Model* [3]. Moreover, the behavior of discrete linear systems can be analyzed using modules over rings, which is explored in *Behavior for Time Invariant Finite Dimensional Discrete*

Linear Systems [4]. These studies demonstrate that abstract algebra can effectively address real-world problems in modeling, system behavior analysis, and error correction.

Encoding and decoding messages is the main process in coding theory [5]. A message is first transformed into a codeword using a certain mathematical rule, which is then sent to a receiver [6]. Upon arrival, the receiver applies the inverse of the original rule to decode the message and retrieve the original information. However, due to transmission errors, such as caused by physical noise, signal fading, or data loss, errors may occur, altering some of the code symbols. Fortunately, coding theory provides the tools to solve this problem. The ability to detect and correct such errors is one of the most valuable contributions of algebraic coding.

A key parameter in assessing the reliability of a code is its minimum distance [7]. The higher the minimum distance, the more reliable a code's performance in errors detecting and correcting so the message can be less distorted. To obtain the minimum distance, we have to compute all of the distance of a code and compare all of them. In many problems, it is crucial to improve the efficiency of computing the minimum distance when developing codes for real-world applications, such as satellite communication, digital television, or internet data transmission [8].

Some module structure could help us to optimize the computation of minimum distance. In Sinha [1], they showed that to determine the distance of a module code, we only need to compute the weight of 127 non-zero elements of the code. In Gao et al. [9], using the structural properties of 1-generator QC codes, they obtain the lower bound of the minimum distance based on the generator polynomial. In this article, we will show how module structure over a finite chain ring can simplify our computation for the minimum distance of a code.

One promising approach to simplify this process involves the use of module structures. Codes can be seen as modules over certain rings, and this structural perspective allows more efficient manipulation and analysis. For instance, Sinha [1] demonstrated that in a particular class of linear codes, which are module codes, it is sufficient to compute the hamming weights of only 127 representative elements instead of all possible codewords. This reduction in computational cost is possible because of the symmetrical and algebraic properties embedded in the module structure. Similar insights are drawn in other works where module theory provides new frameworks for bounding or calculating minimum distance values.

Moreover, in the study of quasi-cyclic (qc) codes, researchers have used generator polynomials and module theory to establish lower bounds on the minimum distances [10]. For example, in Gao et al. [9], they leverage the algebraic properties of 1-generator qc codes over finite rings to derive such bounds analytically. These techniques not only enhance computational efficiency but also help in classifying and constructing new families of codes with guaranteed performance levels. The interaction between algebraic structures and coding parameters like distance continues to be a vibrant research area with both theoretical depth and practical relevance. In this article, we explore the application of module structures over finite chain rings to optimize minimum distance computations in linear codes. By reinterpreting the code as a module and utilizing the algebraic characteristics of the ring, we can obtain efficient strategies to evaluate the code's performance.

II. Materials and Method

It is important to define several fundamental concepts as the foundation for our analysis before doing the main discussion. Specifically, we need to understand the definition of a module, submodule, module code and the minimum distance. Here, we state all of these definitions. The concept of module provides the algebraic structure in which the codes are defined, while submodules are used to identify smaller code within a larger module. The concept of minimum distance is essential for measuring the code's capability in error detection and error correction. In the subsequent sections, we apply these definitions to construct the module code of interest and to evaluate its performance in minimum distance computation.

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 61-66
https://idjams.com/index.php/jms/index

Definition 1 (module) [3]**.** Let $(M,+)$ be an abelian group, R is a ring, and $(r,m) \mapsto rm$, a mapping of $R \times M$ into M, satisfying the following properties for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$,

i. $r(m_1 + m_2) = rm_1 + rm_2$,
ii. $(r_1 + r_2)m = r_1m + r_2m$,
iii. $(r_1r_2)m = r_1(r_2m)$,
iv. $1m = m, if\ 1 \in R$,

then, M is called a module over R or R-module.

Definition 2 (submodule) [3]**.** Let $N \neq \emptyset$ be a subset of an R-module M. N is a submodule of M if

i. $x - y \in N\ for\ all\ x, y \in N$,
ii. $rx \in N\ for\ all\ x \in N, r \in R$.

Definition 3 (module code) [1]**.** Let R be a ring and an encoding function $E: R^m \mapsto R^n$. If $C = E(R^m)$ satisfies closure under addition and scalar multiplication by any element of R, i.e., C is a submodule of R^n, then the code C is a module code.

Definition 4 (Hamming distance) [7]**.** Let $x, y \in \mathbb{F}_n^q$. The Hamming distance between x and y, denoted by $d(x,y)$, is defined as the total number of positions at which their corresponding elements of x and y are different. The weight of a codeword is the distance between the code and the zero codeword.

Definition 5 (minimum distance) [12]**.** If C is a code, then its minimum distance is the minimum weight among all its nonzero codeword, formally given by

$$d_{min}(C) = min\{wt(c(x)) \mid c(x) \in C, c(x) \neq 0\}$$

Where $wt(c(x))$ is the total number of nonzero entries in the codeword $c(x)$.

The minimum distance of a code is a parameter that determines the code's ability to detecting and correcting errors. Moreover, if a code has minimum distance d, then the code can detect up to $d-1$ errors and correct up to $\frac{d-1}{2}$ errors [12].

Definition 6 (finite chain ring) [13]**.** Let R be a finite chain ring and its unique maximal ideal M generated by γ, i.e., $M = \langle\gamma\rangle = R\gamma = \{a\gamma \mid \alpha \in R\}$. Then R admits a descending chain of ideals:

$$R = \langle\gamma^0\rangle \supseteq \langle\gamma^1\rangle \supseteq \langle\gamma^2\rangle \supseteq \cdots \supseteq \langle\gamma^i\rangle \supseteq \cdots$$

this chain terminates at $\{0\}$, the trivial ideal of R.

Proposition. Suppose R is a finite chain ring with $M = \langle\gamma\rangle$ as its unique maximal ideal, and $R_n = R[x] / \langle x^n - 1\rangle$ is an additive abelian group. Define the code

$$C = \langle g(x)\rangle = \{r(x) \cdot g(x) \mid r(x) \in R_n\} \subseteq R_n,\ g(x) \in M[x].$$

Then, the minimum distance of C satisfies:

$$d_{min}(C) = wt(g(x)). \quad (1)$$

Remark. Since the minimum distance can be determined by examining only the generator, this highlights the efficiency of using the module structure in the analysis of the code.

III. Result

Suppose R is a finite chain ring with $M = \langle\gamma\rangle$ as its unique maximal ideal, and $R_n = R[x] / \langle x^n - 1\rangle$ is an additive abelian group. Define the code $C = \langle g(x)\rangle = \{r(x) \cdot g(x) \mid r(x) \in R_n\} \subseteq R_n$, $g(x) \in M[x]$. Then,

$$d_{min}(C) = wt(g(x)). \quad (2)$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 61-66
https://idjams.com/index.php/jms/index

First, we can say that R_n is a R-module because it holds all of these properties,

i. $r(f(x)+h(x)) = rf(x)+rh(x)$,
ii. $(r_1+r_2)f(x) = r_1f(x)+r_2f(x)$,
iii. $(r_1r_2)f(x) = r_1(r_2f(x))$,
iv. $1f(x) = f(x), if\ 1 \in R$.

Since R_n is an R-module, then $0 \in R_n$.

Let $r(x) = 0 \in R_n$,

$r(x) \cdot g(x) = 0 \cdot g(x) = 0 \in C$

therefore, $C \neq \emptyset$.

Clearly it holds all of these properties,

i. $f(x) - g(x) \in C\ for\ all\ f(x), g(x) \in C$,
ii. $rf(x) \in C\ for\ all\ f(x) \in C, r \in R$.

Thus, C is a submodule of R_n, which means C is a module code over finite chain ring R.

Now, we will prove that the minimum distance of C is equals to the weight of its generator. By the definition of minimum distance, we know that

$$d_{min}(C) = \min\{wt(c(x)) \mid c(x) \in C, c(x) \neq 0\}$$
$$= \min\{wt(r(x) \cdot g(x) \mid r(x) \in R_n, r(x) \cdot g(x) \neq 0\}$$

By taking $r(x) = 1 \in R_n$,

$$r(x) \cdot g(x) = g(x)$$

Since $g(x) \in M[x] \subset R\backslash\{0\}$, then $g(x) \neq 0$.
Thus, $g(x) \in C\ \backslash\{0\}$. So, we can write

$$d_{min}(C) = \min\{wt(r(x)g(x) \mid r(x) \in R_n, r(x)g(x) \neq 0\} \leq wt(g(x)).$$

Therefore,

$$d_{min}(C) \leq wt(g(x)) \tag{3}$$

Now, let:

$$r(x) = \sum r_i x^i \in R_n$$
$$g(x) = \sum g_j x^j \in R_n$$

Recall that R is defined as a finite chain ring. Using the finite chain ring theorem, we conclude that $\forall r_i \in R, \exists k_i \ni r_i \in \langle \gamma^{k_i} \rangle$. Similiarly, $\forall g_j \in R, \exists l_j \ni g_j \in \langle \gamma^{l_j} \rangle$.
Therefore,

$$r_i \cdot g_j \in \langle \gamma^{k_i + l_j} \rangle$$

if $k_i + l_j < v$, then $r_i \cdot g_j \neq 0$.
This proves that the product of $(r(x) \cdot g(x)) \neq 0$, and the positions where g_j is nonzero will remain in $r(x) \cdot g(x)$.
Thus, $wt(g(x)) \leq wt(r(x).g(x)),\ \ \forall r(x) \neq 0$.
Therefore, can conclude that

$$wt(g(x)) \leq \min\{wt(r(x).g(x))\} = d_{\min}(C) \tag{4}$$

From (2) and (3), we obtain:

$$d_{min}(C) = wt(g(x)) \quad \blacksquare.$$

Indonesian Journal of Applied Mathematics and Statistics (IdJAMS)
ISSN 3064-4062
Volume 2 Issue 2, December 2025, pp. 61-66
https://idjams.com/index.php/jms/index

In general, $d_{min}(C) = wt(g(x))$ does not always hold. An additional condition is needed for this quality to be valid. The specific condition required here is $g(x) \in M[x]$, where M is the maximal ideal of R [16]. This condition is essential to guarantee that the Hamming weight of any nonzero codeword in C cannot be smaller than the generator weight.

Example

Let $R = \mathbb{Z}_4,\ R_n = \mathbb{Z}_4/(x^4 - 1)\,,\ g(x) = 2 + 2x.$

Construct a code $C = \langle g(x) \rangle$. We will show that the minimum weight of C is equals to the generator weight. The maximum ideal of $\mathbb{Z}_4$ is $\langle 2 \rangle$. Clearly, we can see that $g(x) \in \langle 2 \rangle [x]$, R_n is a module over R and $g(x)$ is a submodule over R_n. This satisfies all of the condition to use the Equation (1). Therefore,

$$d_{min}(C) = wt(g(x))$$
$$= 2.$$

To compare the result with the traditional computation, note that there are 63 nonzero codeword. However, some of them are equal, so only the unique nonzero codewords are shown here.

Table 1. Minimum distance computation with traditional method

$r(x)$	$c(x)$	Hamming Weight
1	$2 + 2x$	2
3	$2 + 2x$	2
x	$2x + 2x^2$	2
$1 + x$	$2 + 2x^2$	2
$2 + x$	$2x + 2x^2$	2
$3 + x$	$2 + 2x^2$	2
$3x$	$2x + 2x^2$	2
x^2	$2x^2 + 2x^3$	2
$1 + x^2$	$2 + 2x + 2x^2 + 2x^3$	4
$2 + x^2$	$2x^2 + 2x^3$	2
$3 + x^2$	$2 + 2x + 2x^2 + 2x^3$	4
$x + x^2$	$2x + 2x^3$	2
$1 + x + x^2$	$2 + 2x^3$	2
$2 + x + x^2$	$2x + 2x^3$	2
$3 + x + x^2$	$2 + 2x^3$	2

The result from the traditional computation is $d_{min}(C) = \min\{2, 4\} = 2$.

IV. Conclusion

Certain module structures can provide a more efficient way to compute the code's minimum distance, one of which is a module code over a finite chain ring. In particular, we show that the minimum distance can be determined by only computing the generator weights. This significantly reduces the computational time and cost, which is very important in decoding processes where error detection and correction are required. Efficiency in terms of computation time and cost makes this method more valuable in real-time communication systems where decoding speed is critical. Therefore, the use of module code structure provides a more efficient approach to analysing how well the code performs in detecting and correcting errors. This approach could be extended to multi-generator codes and explored further in terms of formal computational complexity.

References

[1] A. K. Sinha, "Application of Module Structure of Algebra in Coding Theory in Different Branches of Engineering," *Int. J. Sci. Eng. Technol.*, vol. 2, no. 4, pp. 295–297, 2013.

[2] K. Schnoor, "Applications of Algebraic Coding Theory to Cryptography," M.S. thesis, University of Northern Colorado, Greeley, CO, USA, 2022. [Online]. Available: https://digscholarship.unco.edu/honors/1067.

[3] Sylviani, S., Carnia, E., & Supriatna, A. K., "An Algebraic Study of the Matrix Meta-Population Model," *J. Phys.: Conf. Ser.*, vol. 893, no. 1, p. 012009, 2017. DOI: 10.1088/1742-6596/893/1/012009

[4] Sylviani, S., Garminia, H., and Astuti, P. "Behavior for Time Invariant Finite Dimensional Discrete Linear Systems," *J. Math. Fund. Sci.*, vol. 45, no. 1, pp. 39-52, 2013, DOI: https://doi.org/10.5614/j.math.fund.sci.2013.45.1.4

[5] H. Bordbar, "A Note on the Support of a Hypermodule," *J. Algebr. Appl.*, vol. 19, no. 1, pp. 2050019, 2020, DOI: 10.1142/S021949882050019X

[6] O. Khadir, "A Simple Coding-decoding Algorithm for the Hamming Code," *arXiv*, preprint arXiv: 2201.02066 [cs.IT], Jan. 2022. [Online]. Available: https://arxiv.org/abs/2201.02066, DOI: 10.48550/arXiv.2201.02066

[7] M. Rowshan and J. Yuan, "On the Minimum Weight Codewords of Pac Codes: the Impact of Pre-transformation," *IEEE J. Sel. Areas Inf. Theory*, vol. 4, pp. 487-498, 2023, DOI: 10.1109/JSAIT.2023.3312678

[8] G. Quintana-Ortí, F. Hernando, and F. D. Igual, "Algorithm 1033: Parallel Implementations for Computing the Ninimum Distance of a Random Linear Code on Distributed-memory Architectures," *ACM Trans. Math. Software*, vol. 49, no. 1, Art. no. 8, pp. 1–24, 2023, DOI: 10.1145/3573383.

[9] J. Gao, L. Shen, and F.-W. Fu, "Quasi-cyclic Codes Over Finite Chain Rings," arXiv preprint arXiv:1309.1623 [cs.IT], Sep. 2013. [Online]. Available: https://arxiv.org/abs/1309.1623

[10] N. Aydin and T. Asamov, "Search for Good Linear Codes in the Class of Quasi-cyclic and Related Codes," *World Scientific Review*, vol. 22, no. 36, pp. 1-48, 2008. [Online]. Available: https://www.worldscientific.com

[11] P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul, "Modules and Vector Spaces," in *Basic Abstract Algebra*, 2nd ed. Cambridge University Press, 2012.

[12] C. Okeke, "A Comparative Study between Hamming Code and Reed-Solomon Code in Byte Error Detection and Correction," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 3, no. 12, pp. 34-39, 2015.

[13] Monika, S. Dutt, and R. Sehmi, "On Cyclic Codes Over Finite Chain Rings," *J. Phys.: Conf. Ser.*, vol. 1850, P. 012010, 2021, DOI: 10.1088/1742-6596/1850/1/012010