Palestine Journal of Mathematics

Vol 15(1)(2026) , 474–479

LINEAR CODES OVER RINGS: A STUDY OF UNIMODULARITY AND PURE PROJECTIVE STRUCTURE

P. Gupta, R. K. Mishra and H. Chakraborty

Communicated by: Manoj Patel

MSC 2020 Classifications: Primary 94B05, 13C10; Secondary 13C99.

Keywords and phrases: Pure projective module, Unimodular row, Linear code, Hamming distance, Torsion-free module.

Abstract This paper investigates the role of pure projective modules and unimodular rows in determining the structural properties of linear codes over rings. Focusing on the complex interactions between module theory and coding theory, we establish connections among unimodularity, torsion-free characteristics, minimum Hamming distance and pure projectivity in linear codes.

1 Introduction

Pure projective modules, characterised as direct summands of direct sums of finitely presented modules, extend the classical concept of projective modules and play a pivotal role in identifying when a linear code exhibits torsion-free behaviour. These modules allow for a structured approach to analysing linear codes over rings, a property that becomes crucial when assessing minimum distance, a key parameter in error correction. Linear codes, essential in error detection and correction, have traditionally been developed over fields. However, recent research has shifted towards codes defined over rings, exhibiting complex and intriguing behaviours that enrich module theory and algebraic coding theory. This extension invites a detailed examination of the interplay between a code's algebraic structure and the underlying ring. Notably, codes over rings, unlike their field-based counterparts, can exhibit torsion elements, impacting their distance properties and error-handling capacity. The study [9] investigates secondary representations and indecomposability of projective modules over graded Noetherian rings. Their approach reinforces the broader structural understanding of projective modules in graded settings, complementing the present work's focus on pure projective modules and unimodular completability. The study of codes that are torsion-free and pure projective often resembles classical codes over fields, particularly when the generator matrix contains unimodular rows that ensure a minimum distance of at least two, barring trivial cases. In [14], authors addressed the conditions for equivalence of linear codes, proving MacWilliams' theorem using the linear independence of group characters and exploring transformations that preserve weight. The other paper [15] by J. A. Wood extended these ideas for codes over finite Frobenius rings, focusing on extending weight-preserving homomorphisms to automorphisms. Another work [2] establishes a duality theory for modules over finite Frobenius rings, generalising MacWilliams' theorem through character theory to expand the applicability of coding theory over rings. In [13], Siap generalised MacWilliams' theorem to linear codes under the RT-metric by introducing a ρ-complete weight enumerator. The theory of linear codes over finite fields has been expanded by A. Nechaev to codes over quasi-Frobenius modules defined over commutative rings, and J. Wood extended these to codes over finite Frobenius rings that are not necessarily commutative. Studies (see [5, 12]) on weight functions for finite modules have further extended the Hamming weight concept, enriching the analysis of code properties over rings, while the construction of binary and ternary LCD codes from projective spaces demonstrates the practical applications of pure projective modules. Historically, coding theory over fields, as illustrated by the development of Hamming and Reed-Solomon codes [1], relied on vector spaces over finite fields. However, pioneer research by Greferath, Nechaev, and others (see [2, 5, 10, 16]) extended this framework to finite commutative rings, particularly Galois rings. They revealed that codes over rings dif-

fer fundamentally from those over fields by forming modules rather than vector spaces. This shift introduced module-theoretic techniques to the study of codes. Codes over rings often exhibit torsion, affecting decoding and error-correction properties, which adds complexity to their study and requires new theoretical approaches. Consequently, a crucial research question thus emerged: when can a code over a ring behave like a free, torsion-free module? The construction of skew cyclic codes as explored in [11] highlights the diversity of algebraic approaches to ring-based coding theory. In a complementary direction, the present study focuses on the use of unimodular rows and pure projective modules to generate torsion-free linear codes over commutative rings, linking module-theoretic properties with distance and structure. Pure projective modules offer insight into this question, as their properties provide a structured way to analyse code behaviour over rings. Furthermore, unimodular rows in a generator matrix guarantee that the rows can generate the entire free module over a commutative ring, imparting desirable structural properties to the linear code. This study establishes a series of new theorems linking linear codes, unimodular rows, and pure projective modules, and demonstrates how unimodular rows in a generator matrix influence a code's minimum distance and torsion-free characteristics.

Section 2 provides the foundational preliminaries, including essential definitions and key remarks utilized throughout this work. Section 3 is dedicated to establishing and proving the main results of our study included with some examples that illustrate how the unimodularity of rows in a generator matrix affects the properties of linear codes over rings. Examples include non-free modules, unimodularity's effect on minimum Hamming distance, and the relationship between minimum distance and torsion elements.

2 Preliminaries

Definition 2.1. [6] Let v_1 and v_2 be two codewords in a code C. Then the **Hamming distance** between v_1 and v_2, denoted by (v_1, v_2), is defined as the number of places at which v_1 and v_2 are not the same.

Definition 2.2. [6] Let v_1 be a codeword in F_q^n. The **Hamming weight** of v_1, denoted by $wt(v_1)$, is defined as α, where α is the number of nonzero coordinates in v_1. In other words, Hamming weight is also defined as the distance of v_1 from the zero codeword, i.e.

$$wt(v_1) = d(v_1, 0),$$

where 0 is the zero codeword.

Definition 2.3. [6] A **linear code** C of length n over F_q is defined as a subspace of F_q^n.

Definition 2.4. [6] Let C be a code containing at least two codewords. The minimum **distance of** C, denoted by $d(C)$, is defined as the least Hamming distance between two codewords in C. That is,

$$d(C) = min\{d(v_1, v_2) : v_1, v_2 \in C, v_1 \neq v_2\}.$$

Definition 2.5. [3] If a module is projective with regard to a pure short exact sequence, it is considered a **pure projective module**.

Definition 2.6. [7] Let R be a commutative ring and let N be an R-module. N is called **torsion-free** if $rn \neq 0$ for all nonzero divisors r in R and $n \neq 0$ in N.

Definition 2.7. [8] Let R be a ring. A **row** $(a_1, a_2, ..., a_n) \in M^n$ is called **unimodular** (of length n) in a pure projective module if the ideal

$$< a_1, a_2, ..., a_n >= M.$$

Or there exists $r_1, r_2, ...r_n \in R$, such that

$$a_1r_1 + a_2r_2 + ... + a_nr_n = 1.$$

Remark 2.8. [6] The distance of a linear code $d(C)$, is same as the least Hamming weight of $v_i, v_j \in C$; where $0 \neq v_i, 0 \neq v_j$.

3 Linear codes with unimodular rows in pure projective modules

Theorem 3.1. *A linear code C over a ring R is a free module if and only if its generator matrix G has unimodular rows.*

Proof. Let C be a free R-module. A basis (β) exists for C such that every element of C can be uniquely expressed as a linear combination of the elements of β with coefficients in R. Let rows $a_1, a_2, ..., a_k$ of G form β for C. Since C is free, rows must be linearly independent and spanning R^n. For any row a_i, there exists $r_1, r_2, ..., r_k \in R$ such that $a_{i1}r_1 + a_{i2}r_2 + ... + a_{ik}r_k = 1$. Hence, a_i is unimodular.

Conversely, let G has unimodular rows. Then for each row a_i, there exists $r_1, r_2, ..., r_n \in R$ such that $a_{i1}r_1 + a_{i2}r_2 + ... + a_{in}r_n = 1$. This implies each row generates the whole ring R and is linearly independent. Since the rows are linearly independent and span R^n, they form a basis for a free module R. Therefore, the linear code C generated by G is a free R-module. □

In Example 3.2, we demonstrate that a linear code defined over a ring R does not necessarily form a free R-module. However, when the rows of G are unimodular, the code exhibits assertive structural properties, as established in Theorem 3.1.

Example 3.2. Let C be a linear code over ring $\mathcal{Z}/4\mathcal{Z}$ spanned by S.

$$S = \{(2,0),(0,2)\}.$$

The generator matrix of C is given by

$$G = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

For any $\alpha, \beta \in \mathcal{Z}/4\mathcal{Z}$; $\alpha.(2,0) + \beta.(0,2)$ will be in C.

$$C = \{(0,0),(2,0),(0,2),(2,2)\} \subset (\mathcal{Z}/4\mathcal{Z})^2.$$

Hence C is a linear code over $\mathcal{Z}/4\mathcal{Z}$. But C is not free as a $\mathcal{Z}/4\mathcal{Z}$-module.
Also, rows of G are linearly independent but not unimodular. For any $r_1, r_2 \in \mathcal{Z}/4\mathcal{Z}$; $2.r_1 + 0.r_2$ or $0.r_1 + 2.r_2$ is either 0 or 2 but never 1; implying non-unimodularity of $(2,0)$ and $(0,2)$.

Theorem 3.3. *Let C be a linear code over a commutative ring R with G as generator matrix. Then the following are equivalent:*
(i) C is a torsion-free pure projective module, if R is a PID.
(ii) Rows of G are unimodular.
(iii) C is free as an R-module.
(iv) $d(C) \geq 2$.

Proof. **i)** $\Rightarrow$ **ii)** : Let G be a generator matrix of C with rows $g_1, g_2, \cdots, g_n \in R^n$; where

$$g_i = (g_{i1}, g_{i2}, \cdots, g_{in}).$$

Suppose that one of the rows, g_i, is not unimodular. Then,

$$< g_{i1}, g_{i2}, \cdots, g_{in} > \subset R.$$

The ideal generated by non unimodular row g_i is a proper ideal of R and there does not exist any $r_1, r_2, \cdots, r_n \in R$ such that

$$r_1 g_{i1} + r_2 g_{i2} + \cdots + r_n g_{in} = 1.$$

Also, $1 \notin < g_i >$ and $< g_i >$ is a proper ideal; $< g_i >$ will be contained in a maximal ideal (say m) of R. For every $r \in m$, $r.g_i = 0$ in R. This is a contradiction of C being torsion-free. Hence,

our assumption of g_i being non-unimodular is wrong. Therefore, rows of G are unimodular.

ii) $\Rightarrow$ **iii**) : The proof is followed by theorem 3.1.

iii) $\Rightarrow$ **iv**) : Let C be a free R-module. Let $g_i = (g_{i1}, g_{i2}, \cdots, g_{in})$ be a row of generator matrix G. Generator matrix G is of the form:

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{bmatrix}$$

Each row g_i is a codeword in C and is non-zero. Every codeword $c \in C$ can be expressed as a unique linear combination of the rows of the generator matrix G. Therefore, a general codeword $c \in C$ is given by:

$$\lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_k g_k;$$

where $\lambda_1, \lambda_2, \cdots, \lambda_k \in R$. The Hamming weight of a codeword $c = (c_1, c_2, \cdots, c_n)$ is the number of non-zero positions in the codeword c. C being free as an R-module, rows of G are linearly independent over R.
Suppose there is a codeword $0 \neq c \in C$ with $wt(c) = 1$. Then c can be represented as $c = (0, 0, \cdots, 0, r_i, 0, \cdots, 0)$, $r_i \neq 0$ that is non-zero at exactly one position (say at i^{th}-position). c being a linear combination of the rows of G, i^{th}-entry of c can be expressed as linear combination of i^{th}-entries of the rows $g_1, g_2, \cdots, g_n$ of G. Then,

$$\lambda_1 g_{1,i} + \lambda_2 g_{2,i} + \cdots + \lambda_n g_{n,i} = r_i,$$

where $g_{n,i}$ denotes the i^{th}-entry of the row g_n for each n. For all other positions $j \neq i$,

$$\lambda_1 g_{1,j} + \lambda_2 g_{2,j} + \cdots + \lambda_n g_{n,j} = 0.$$

The linear independence of rows of G does not allow any non-trivial linear combination of g_i's that can result in a codeword with only one non-zero entry. The assumption of c with Hamming weight 1 requires a choice of $\lambda_1, \lambda_2, \cdots, \lambda_n$ such that they satisfy the system of equations:

$$\lambda_1 g_{1,j} + \lambda_2 g_{2,j} + \cdots + \lambda_n g_{n,j} = 0,$$

for all $j \neq i$. This contradicts the linear independence of g_i's. To satisfy the above system of equations, the only choice of λ_i's is zero. Therefore, no non-trivial codeword can have Hamming weight 1 and hence, from 2.8, the minimum Hamming distance of C is greater than 1.

iv) $\Rightarrow$ **i**) : The minimum distance of C is 2, and a non-zero codeword in C with Hamming weight 1 does not exist. If $\exists 0 \neq r_i \in R$ such that $r.c = 0$, implying C has a torsion element. But the minimum distance of C being 2 implies that any non-trivial combination of $g_i's$ (rows of G) has more than one non-zero entry. Therefore, no such r exists; hence, no non-zero element (codeword) in C can be annihilated by a non-zero element in R. Hence, C is torsion-free. In particular, if C is a projective R-module, C can be embedded as a direct summand of free modules and the proof is done. But in general, this is not the case. Also, every linear code is finitely generated and therefore from (Theorem 2.4.1, [7]), C is free as an R-module. C is submodule of R^n (by definition). Being submodule of free module over PID, C is free and hence pure projective from section 3.5, [4]. Thus, C is a torsion-free pure projective module. □

Example 3.4 presents a linear code with non-unimodular rows in G, resulting in a minimum Hamming distance of 1. Through Examples 3.4 and 3.5, we explore how the unimodularity of G's rows directly influences the minimum Hamming distance of the code C. And, Example 3.6 illustrates that when the minimum distance of C is reduced to 1, the code necessarily includes torsion elements, underscoring the connection between minimum distance and torsion in module-based codes.

Example 3.4. Let C be a linear code over $\mathcal{Z}/6\mathcal{Z}$ with generator matrix G,

$$G = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

So codewords in C will be of the form,

$$a_1(2,0,0) + a_2(0,3,0); \quad a_1, a_2 \in \mathcal{Z}/6\mathcal{Z}.$$

$C = \{(0,0,0),(0,3,0),(2,0,0),(4,3,0),(4,0,0),(2,3,0)\} \subseteq (\mathcal{Z}/6\mathcal{Z})^3$.
The distance between two codewords in C are,

$$d(v_i, v_j) = \{1,2\}; \quad \forall v_i, v_j \in C.$$

Hence, $d(C) = 1$.
Also, in this example, rows of G are not unimodular. There does not exist any $r_1, r_2, r_3 \in \mathcal{Z}/6\mathcal{Z}$ such that

$$2.r_1 + 0.r_2 + 0.r_3 = 1$$

or

$$0.r_1 + 3.r_2 + 0.r_3 = 1$$

and the ideals generated by these rows are

$$< 2,0,0 >= \{\bar{0}, \bar{2}, \bar{4}\} \subset \mathcal{Z}/6\mathcal{Z}$$

and

$$< 0,3,0 >= \{\bar{0}, \bar{3}\} \subset \mathcal{Z}/6\mathcal{Z}.$$

The above ideals are not unit ideals ($\mathcal{Z}/6\mathcal{Z}$). Therefore, the rows $(2,0,0)$ and $(0,3,0)$ are not unimodular.

Example 3.5. Let C be linear code over $\mathcal{Z}/4\mathcal{Z}$ with generator matrix G,

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Rows of G are unimodular and
$C = \{(0,0,0),(1,1,0),(2,2,0),(0,1,1),(3,3,0),(1,2,1),(2,3,1),(3,0,1),(0,2,2),$
$(1,3,2),(2,0,2),(3,1,2),(1,0,3),(0,3,3),(2,1,3),(3,2,3)\}$
Here, the distance of two codewords in C are,

$$d(v_i, v_j) = \{2,3\}; \quad \forall v_i, v_j \in C.$$

Hence, $d(C) = 2$.

Example 3.6. Let C be a linear code over ring $\mathcal{Z}/4\mathcal{Z}$ spanned by S.

$$S = \{(1,0),(0,0)\}.$$

The generator matrix of C is given by

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

For any $\alpha, \beta \in \mathcal{Z}/4\mathcal{Z}$; $\alpha.(1,0) + \beta.(0,0)$ will be in C.

$$C = \{(0,0),(1,0),(2,0),(3,0)\} \subset (\mathcal{Z}/4\mathcal{Z})^2.$$

$d(C) = 1$ and C has a torsion element as, $2.(2,0) = (0,0)$. Hence, C is not a torsion-free module.

4 Conclusion

This study highlights the role of pure projective modules in the structural characterisation of linear codes over rings. Our findings bridge a gap in the literature, expanding traditional coding theory beyond fields to rings. We reveal a nuanced interplay between module-theoretic structures and minimum Hamming distance by linking unimodular rows in a code's generator matrix with desirable torsion-free properties. The results contribute to a deeper understanding of coding theory beyond fields, laying the groundwork for future explorations into coding over rings and extending the utility of pure projective modules. Further research could explore applications in decoding algorithms and practical code constructions, especially in modular and ring-theoretic settings.

References

[1] Couselo E, Gonzalez S, Markov VT, Martinez C, Nechaev AA. Ideal Representation of Reed-Solomon and Reed-Muller Codes, Algebra and Logic, 51 (3), 2012.

[2] Greferath M, Nechaev A, Wisbauer R. Finite Quasi-Frobenius Modules and Linear Codes, Journal of Algebra and Its Applications, 03(03), 2011.

[3] Gupta P, Mishra RK. Some Results On Pure Projective Modules, Palestine Journal of Mathematics, vol. 12, 92-96, 2023.

[4] Gupta P, Mishra RK. On the relation of pure projective modules with other modules, Springer Proceedings of the International Conference on Algebra and its Applications - 2023, 2024.

[5] Kurakin VL, Kuzmin AS, Markov VT, Mikhalev AV, Nechaev AA. Linear Codes and Polylinear Recurrences over Finite Rings and Modules (a Survey), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 13th International Symposium: Lecture Notes in Computer Science 1719, AAECC-13 Honolulu, Hawaii, USA, November 15-19, 1999 Proceedings, pp 365-391, 1999.

[6] Ling S, Xing C. Coding Theory: A First Course, Cambridge University Press 2004.

[7] Mandal S. Projective modules and complete intersections, volume 1672. Springer Science & Business Media, 1997.

[8] Mandlik N. Classical K-Theory: Completion of Unimodular Rows, PhD thesis, 2015.

[9] Mishra RK, Pratibha, Mohan R. Projective modules over commutative Noetherian graded rings, Palestine Journal of Mathematics, vol. 12, 19-23, 2023.

[10] Nechaev AA, Kuz'min AS, Markov VT. Linear codes over finite rings and modules, Fundamental and Applied Mathematics (Fundanientalnaya i prikladnaya matematika), Volume 3, Issue 1, 195-254, 1997(in Russian with an abstract in English).

[11] Rai P, Singh B, Gupta A. Skew cyclic codes over $F_q[u_1, u_2, ..., u_r]/ < u_i^3 - u_i, u_iu_j - u_ju_i >_{i,j=1}^{r}$, Palestine Journal of Mathematics, vol. 13, 216-229, 2024.

[12] Seneviratne P, Melcher L. Binary and ternary LCD codes from projective spaces, Discrete Mathematics, Algorithms and Applications: World Scientific, Volume 10(06), 1850079, 2018.

[13] Siap I. A MacWilliams Type Identity, Turkish Journal of Mathematics, 26, 465-473, 2002.

[14] Ward HN, Wood JA. Characters and the Equivalence of Codes, Journal of Combinatorial Theory, Series A 73, 348-352, 1996.

[15] Wood JA. Extension Theorems for Linear Codes over Finite Rings, International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes: Lecture Notes in Computer Science (LNCS, volume 1255), pp 329-340, 1997, 1st online 2005.

[16] Lu Y, Shi M, Greferath M, Sole P. Linear codes over finite rings are trace codes, Discrete Mathematics, 343, 111919, 2020.

Author information

P. Gupta, Department of Mathematics, National Institute of Technology Jamshedpur, India.
E-mail: poojagupta2327@gmail.com

R. K. Mishra, Department of Mathematics, National Institute of Technology Jamshedpur, India.
E-mail: ratnesh.math@nitjsr.ac.in

H. Chakraborty, Department of Mathematics, National Institute of Technology Nagaland, India.
E-mail: himanchakra@gmail.com

Received: 2025-04-02
Accepted: 2025-07-25