International Journal of Interdisciplinary Research

International Journal of Interdisciplinary Research
ISSN(Online): 3090-2959
Vol 2 no 2 (2026): July 2026
https://journal.as-salafiyah.id/index.php/ijir/index
Email: ijireditor7@gmail.com

Construction Of Linear Codes Over The Galois Ring GR(2^3) With Hamming Distance

[1]**Arif Febrorianto Hidayat**, [2]**Santoso Budi Wiyono**, [3]**Putranto Hadi Utomo**
[1,2,3]*Universitas Sebelas Maret, Indonesia*
[1]*febroarif@gmail.com*, [2]*santosobudi@staff.uns.ac.id*, ,[3]*putranto@staff.uns.ac.id*

Correspodence Email: *putranto@staff.uns.ac.id*.

Abstract: *This study focuses on the construction and analysis of linear codes over a Galois ring with eight elements, motivated by the need to develop error correcting codes beyond finite fields. The objective is to examine how the selection of generator vectors influences the minimum Hamming distance and the resulting error detection and correction capabilities. The methodology involves constructing two linear codes of length four and dimension two using different generator matrices. Codewords are generated through linear combinations of generator vectors, and the minimum Hamming distance is determined by evaluating the weights of all nonzero codewords. The results show that the first generator matrix produces a minimum distance of three, allowing the detection of up to two errors and correction of one error, while the second produces a minimum distance of two, allowing only single-error detection. The findings indicate that code performance is primarily influenced by the linear relationships among generator vectors rather than solely by the presence of zero divisors. In conclusion, careful selection of generator vectors is essential for optimizing linear codes over Galois rings and improving their performance in digital communication systems.*

Keywords: *Galois Ring, Linear Codes, Hamming Distance, Generator Matrix, Error-Correcting Codes*

INTRODUCTION

Reliable data transmission is a fundamental requirement in modern digital communication systems. In practice, transmitted information is often affected by noise and interference, which may introduce errors during transmission. To maintain data integrity, efficient mechanisms for error detection and correction are essential (Hamming, 1950; Lin & Costello, 2004). One of the most widely used approaches to address this issue is linear coding theory. A linear code is defined as a set of codewords forming a vector space over a finite field or, more generally, a submodule over a finite ring (MacWilliams & Sloane, 1977; Pless, 1998). Classical coding theory has primarily focused on constructions over finite fields, leading to well known codes such as Hamming and Reed-Solomon codes, which have been extensively applied in communication and storage systems (Lint, 1999).

The development of error-correcting codes began with the pioneering work of Hamming, who introduced codes capable of detecting and correcting single-bit errors (Hamming, 1950). This work was later extended by MacWilliams and Sloane, who established a comprehensive algebraic framework for analyzing linear codes, including weight distribution and distance properties (MacWilliams & Sloane, 1977). These foundational results remain central to modern coding theory.

Despite their success, codes over finite fields have certain limitations in representing more general algebraic structures. In particular, they lack the flexibility needed to model systems involving non-field elements. To overcome this limitation, coding theory over finite rings has been developed as a natural generalization. Finite rings, especially finite chain rings and Galois rings, provide richer algebraic structures that allow more flexible and diverse code constructions (Greferath & Schmidt, 2000; Wan, 2003).

An important feature of ring based coding theory is the presence of zero divisors, which introduces structural properties that do not appear in field based codes. This has led to various significant developments. For instance, Dinh and López-Permouth studied cyclic and negacyclic codes over finite chain rings, revealing important structural characteristics (Dinh & López-Permouth, 2004). Similarly, Greferath and Schmidt established fundamental combinatorial results and equivalence theorems for codes over finite rings (Greferath & Schmidt, 2000). Moreover, Hammons et al. demonstrated that certain nonlinear binary codes can be interpreted as linear codes over $\mathbb{Z}_4$, highlighting the importance of ring structures in coding theory (Hammons et al., 1994).

Among finite rings, Galois rings play a central role because they generalize finite fields while preserving many of their algebraic properties. At the same time, they introduce additional features such as nilpotent elements and zero divisors, which enable more complex code structures(Holdman, 2016; Wan, 2003). These properties make Galois rings a promising framework for constructing and analyzing linear codes beyond the classical field based approach (Nechaev, 1991).

In the analysis of linear codes, the minimum Hamming distance is a key parameter that determines the error detection and correction capability of a code. The Hamming distance measures the difference between codewords and provides a direct evaluation of code performance (Pless, 1998). In general, a code with minimum distance d can detect up to $d - 1$ errors and correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors (Hamming, 1950).

Based on these considerations, this study focuses on the construction of linear codes over the Galois ring $GR(2^3)$. The codes are constructed as submodules through the selection of generator matrices that satisfy linear independence and structural requirements (Wood, 1999). The resulting codewords are analyzed using Hamming weight and Hamming distance to determine the minimum distance and evaluate code performance.

The novelty of this research lies in examining how the selection of generator vectors influences the minimum distance of linear codes over $\mathrm{GR}(2^3)$, particularly in the presence of zero divisors. This study provides a clearer understanding of the relationship between algebraic structure and code performance, thereby contributing to the development of coding theory over finite rings and its applications in digital communication systems(Hammons et al., 1994).

METHOD

This study employs algebraic and computational approaches to construct and analyze linear codes over the Galois ring $\mathrm{GR}(2^3)$. The methods include ring construction, element classification, generator matrix determination, codeword generation, and minimum distance evaluation (Huffman & Pless, 2003).

The Galois ring $\mathrm{GR}(2^3)$ is a finite commutative ring isomorphic to $\mathbb{Z}_8$ with eight elements $\{0,1,2,3,4,5,6,7\}$(Hill, 1986). Elements in $\mathrm{GR}(2^3) \cong \mathbb{Z}_8$ can be classified based on their multiplicative properties into two categories, units and zero divisors(Blahut, 2003).

The set of units is $U = \{1,3,5,7\}$, consisting of elements with multiplicative inverses in $\mathbb{Z}_8$. The set of zero divisors is $Z = \{0,2,4,6\}$, where $2^3 \equiv 0 (\mathrm{mod}\ 8)$. The presence of zero divisors distinguishes codes over rings from codes over fields, as linear combinations involving zero divisors can produce codewords with lower weight (Peterson & Weldon, 1972).

Linear codes over rings form submodules rather than vector subspaces. Thus, the codes constructed in this study are submodules of $\left(\mathrm{GR}(2^3)\right)^n$ (Dougherty, 2017). The selection of the generator matrix must satisfy several criteria. The resulting code must form a submodule of R^n, defined as $C = \{uG \mid u \in R^k\}$. The rows of the generator matrix must be linearly independent to ensure the desired code dimension. The matrix must also be free of redundancy so that each row contributes independently. Furthermore, pivot elements must be units to ensure invertibility and algebraic stability (Norton & Sălăgean, 2000). Finally, the generator matrix must produce a non-trivial code with positive dimension and more than one codeword (Roman, 1992).

Based on these criteria, two generator matrices with different structures are used to analyze the effect of generator vector selection on the minimum distance:

$$G_1 = \begin{pmatrix} 1 & 0 & 3 & 5 \\ 0 & 1 & 6 & 7 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 1 & 0 & 3 & 5 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

For G_1, the generator vectors are $g_1 = (1,0,3,5)$ and $g_2 = (0,1,6,7)$, chosen such that the first row contains units 3 and 5 while the second row contains a zero divisor 6 and a unit 7. This combination aims to observe how the interaction between units and zero divisors affects the resulting codeword weights. For G_2, the generator vectors are $g_1 = (1,0,3,5)$ and $g_2 = (0,1,2,1)$, where the third component of the second row is changed from 6 to 2 . This change maintains the property that both 6 and 2 are zero divisors, so any difference in code performance arises solely from the linear structure of the generator vectors rather than from changes in the algebraic properties of the elements. This allows a focused analysis on the impact of generator vector selection on code performance.

The resulting linear code is defined as $C = \{(a,b)G \mid a,b \in GR(2^3)\}$. Each codeword has the form $c = (a \cdot g_1 + b \cdot g_2) \bmod 8$. The code length is set to $n = 4$ and dimension $k = 2$, yielding a total of $8^2 = 64$ codewords for each generator matrix (Jitman & Ling, 2019). This parameter selection is based on the consideration that $n = 4$ provides sufficient space to observe variations in Hamming distance, while the total of 64 codewords remains computationally manageable without loss of generality.

Let C_1 and C_2 be the linear codes generated by G_1 and G_2. Each codeword is obtained from linear combinations of the generator rows over $\mathrm{GR}(2^3)$ (Esmaeili, 2009). The Hamming weight of a codeword $c = (c_1, c_2, \ldots, c_n)$ is defined as the number of nonzero components, $w_H(c) = |\{i \mid c_i \neq 0\}|$ (Pless, 1998). The Hamming distance between two codewords is defined as $d_H(c_x, c_y) = w_H(c_x - c_y)$ (Hamming, 1950). Thus, the minimum Hamming distance is $d_{\min} = \min_{c_x \neq c_y} d_H(c_x, c_y)$, which can be determined by analyzing nonzero codewords. Since the code is linear, the minimum distance equals the minimum weight among all nonzero codewords(Pless, 1998). Based on $d_{\min}$, the error detection capability is $d_{\min} - 1$ and the error correction capability is $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ (Hamming, 1950).

RESULT AND DISCUSSION

In this section, the results of the study are presented along with a comprehensive discussion. The results are organized to facilitate clear interpretation of the constructed codes and their properties. This study investigates the construction of linear codes over the Galois ring $\mathrm{GR}(2^3)$, which is isomorphic to $\mathbb{Z}_8(Holdman, 2016)$. The ring $GR(2^3) \cong \mathbb{Z}_8$ consists of eight elements, namely $\{0,1,2,3,4,5,6,7\}$. which serve as the base set for forming the module space and submodule that defines the linear code.

The code length is chosen as $n = 4$. The selection of this code length is based on the consideration that for $n < 4$, the code becomes too short to detect errors effectively, while for $n > 4$, the number of code elements increases exponentially, making the computation too complex. Therefore, the resulting module space is $\left(GR(2^3)\right)^4 = \mathbb{Z}_8^4$ which has $8^4 = 4096$ elements.

The linear code C is defined as a submodule of $\mathbb{Z}_8^4$ of dimension $k = 2$, meaning that the submodule is generated by two linearly independent vectors in $\mathbb{Z}_8^4$. In this study, the two generator matrices used are.

$$G_1 = \begin{pmatrix} 1 & 0 & 3 & 5 \\ 0 & 1 & 6 & 7 \end{pmatrix}, \qquad G_2 = \begin{pmatrix} 1 & 0 & 3 & 5 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

The resulting linear code is defined as.

$$C = \{(a \cdot g_1 + b \cdot g_2) \bmod 8 \mid a, b \in GR(2^3)\}$$

where g_1 and g_2 are the first and second rows of the generator matrix, respectively.

All codewords are generated by taking linear combinations of all possible pairs (a, b) with $a, b \in GR(2^3)$. Since $GR(2^3)$ has 8 elements, there are $8^2 = 64$ pairs (a, b) that produce 64 codewords. Table 2 and Table 3 present codewords generated by G_1 and G_2.

Table 1. *Codeword Generation Results Using* G_1

Message	Codeword	Message	Codeword	Message	Codeword
(0,0)	(0,0,0,0)	(2,6)	(2,6,2,4)	(5,4)	(5,4,7,5)
(0,1)	(0,1,6,7)	(2,7)	(2,7,0,3)	(5,5)	(5,5,5,4)
(0,2)	(0,2,4,6)	(3,0)	(3,0,1,7)	(5,6)	(5,6,3,3)
(0,3)	(0,3,2,5)	(3,1)	(3,1,7,6)	(5,7)	(5,7,1,2)
(0,4)	(0,4,0,4)	(3,2)	(3,2,5,5)	(6,0)	(6,0,2,6)
(0,5)	(0,5,6,3)	(3,3)	(3,3,3,4)	(6,1)	(6,1,0,5)
(0,6)	(0,6,4,2)	(3,4)	(3,4,1,3)	(6,2)	(6,2,6,4)
(0,7)	(0,7,2,1)	(3,5)	(3,5,7,2)	(6,3)	(6,3,4,3)
(1,0)	(1,0,3,5)	(3,6)	(3,6,5,1)	(6,4)	(6,4,2,2)
(1,1)	(1,1,1,4)	(3,7)	(3,7,3,0)	(6,5)	(6,5,0,1)
(1,2)	(1,2,7,3)	(4,0)	(4,0,4,4)	(6,6)	(6,6,6,0)
(1,3)	(1,3,5,2)	(4,1)	(4,1,2,3)	(6,7)	(6,7,4,7)

Table 1. Continued

Message	Codeword	Message	Codeword	Message	Codeword
(1,4)	(1,4,3,1)	(4,2)	(4,2,0,2)	(7,0)	(7,0,5,3)
(1,5)	(1,5,1,0)	(4,3)	(4,3,6,1)	(7,1)	(7,1,3,2)
(1,6)	(1,6,7,7)	(4,4)	(4,4,4,0)	(7,2)	(7,2,1,1)
(1,7)	(1,7,5,6)	(4,5)	(4,5,2,7)	(7,3)	(7,3,7,0)
(2,0)	(2,0,6,2)	(4,6)	(4,6,0,6)	(7,4)	(7,4,5,7)
(2,1)	(2,1,4,1)	(4,7)	(4,7,6,5)	(7,5)	(7,5,3,6)
(2,2)	(2,2,2,0)	(5,0)	(5,0,7,1)	(7,6)	(7,6,1,5)
(2,3)	(2,3,0,7)	(5,1)	(5,1,5,0)	(7,7)	(7,7,7,4)
(2,4)	(2,4,6,6)	(5,2)	(5,2,3,7)		
(2,5)	(2,5,4,5)	(5,3)	(5,3,1,6)		

Table 2. *Codeword generation results using* G_2

Message	Codeword	Message	Codeword	Message	Codeword
(0,0)	(0,0,0,0)	(2,6)	(2,6,2,0)	(5,4)	(5,4,7,5)
(0,1)	(0,1,2,1)	(2,7)	(2,7,4,1)	(5,5)	(5,5,1,6)
(0,2)	(0,2,4,2)	(3,0)	(3,0,1,7)	(5,6)	(5,6,3,7)
(0,3)	(0,3,6,3)	(3,1)	(3,1,3,0)	(5,7)	(5,7,5,0)
(0,4)	(0,4,0,4)	(3,2)	(3,2,5,1)	(6,0)	(6,0,2,6)
(0,5)	(0,5,2,5)	(3,3)	(3,3,7,2)	(6,1)	(6,1,4,7)
(0,6)	(0,6,4,6)	(3,4)	(3,4,1,3)	(6,2)	(6,2,6,0)
(0,7)	(0,7,6,7)	(3,5)	(3,5,3,4)	(6,3)	(6,3,0,1)
(1,0)	(1,0,3,5)	(3,6)	(3,6,5,5)	(6,4)	(6,4,2,2)
(1,1)	(1,1,5,6)	(3,7)	(3,7,7,6)	(6,5)	(6,5,4,3)

Table 2. Continued

Message	Codeword	Message	Codeword	Message	Codeword
(1,2)	(1,2,7,7)	(4,0)	(4,0,4,4)	(6,6)	(6,6,6,4)
(1,3)	(1,3,1,0)	(4,1)	(4,1,6,5)	(6,7)	(6,7,0,5)
(1,4)	(1,4,3,1)	(4,2)	(4,2,0,6)	(7,0)	(7,0,5,3)
(1,5)	(1,5,5,2)	(4,3)	(4,3,2,7)	(7,1)	(7,1,7,4)
(1,6)	(1,6,7,3)	(4,4)	(4,4,4,0)	(7,2)	(7,2,1,5)
(1,7)	(1,7,1,4)	(4,5)	(4,5,6,1)	(7,3)	(7,3,3,6)
(2,0)	(2,0,6,2)	(4,6)	(4,6,0,2)	(7,4)	(7,4,5,7)
(2,1)	(2,1,0,3)	(4,7)	(4,7,2,3)	(7,5)	(7,5,7,0)
(2,2)	(2,2,2,4)	(5,0)	(5,0,7,1)	(7,6)	(7,6,1,1)
(2,3)	(2,3,4,5)	(5,1)	(5,1,1,2)	(7,7)	(7,7,3,2)
(2,4)	(2,4,6,6)	(5,2)	(5,2,3,3)		
(2,5)	(2,5,0,7)	(5,3)	(5,3,5,4)		

After all codewords are obtained, Hamming distance calculations are performed to determine the minimum distance(Zhang et al., 2016). For example, generator matrix G_1, take two codewords $c_{(0,1)}$ and $c_{(6,7)}$. Their difference is:

$$c_{(0,1)} - c_{(6,7)} = (0-6, 1-7, 6-4, 7-7) \pmod{8} = (2,2,2,0)$$

The Hamming weight of the difference vector is $w_H = 3$, so the distance between the two codewords is 3 . Based on a complete evaluation of all codewords generated by G_1, the minimum distance obtained is $d_{\min} = 3$.

For generator matrix G_2, take two codewords $c_{(0,1)}$ and $c_{(6,7)}$. Their difference is:

$$c_{(0,1)} - c_{(6,7)} = (0-6, 1-7, 2-0, 1-5) \pmod{8} = (2,2,2,4)$$

The Hamming weight of the difference vector is $w_H = 4$. However, based on a complete evaluation of all codewords generated by G_2, a pair with smaller distance is found. For instance, take codewords $c_{(0,2)}$ and $c_{(6,0)}$:

$$c_{(0,2)} - c_{(6,0)} = (0-6,2-0,4-2,2-6) \pmod 8 = (2,2,2,4)$$

Further evaluation reveals the existence of codewords with Hamming weight 2, so the minimum distance obtained is $d_{\min} = 2$.

Based on the Hamming distance analysis from Table 1 and Table 2, the code generated by G_1 has $d_{\min} = 3$, while the code generated by G_2 has $d_{\min} = 2$. Therefore, the error detection capability for G_1 is $d_{\min} - 1 = 2$ with error correction capability $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$, while G_2 can only detect one error and has no error correction capability.

The difference in minimum distance between G_1 and G_2 is not solely due to the presence of zero divisors in the ring Z_8, but is more significantly influenced by the linear relationships among the generator vectors (Gassner et al., 2022). For generator G_2, certain linear combinations of the generator vectors produce codewords with lower Hamming weight. This is indicated by the existence of nontrivial solutions that cause multiple components to become zero simultaneously. This condition results in codewords with lower Hamming weight, thereby reducing the value of $\boldsymbol{d}_{\text{min.}}$. This reduction directly impacts the code's ability to detect and correct errors. Thus, although the ring structure contains zero divisors, the doominant factor affecting code performance in this case is the structure of the generator vectors that induces linear dependencies among components. Therefore, the selection of generator vectors is a critical aspect in determining the quality of linear codes constructed over $GR(2^3)$. (Greferath & Schmidt, 1999; Ling & Solé, 2001).

CONCLUSION

Based on the results of this study, the construction of linear codes over the Galois ring with eight elements produces codes of length four and dimension two with a total of 64 codewords. The findings show that different choices of generator matrices significantly influence the minimum Hamming distance and, consequently, the error detection and correction capabilities. The first generator matrix yields a minimum distance of three, enabling both error detection and correction, whereas the second produces a minimum distance of two, allowing only limited error detection.

The difference in performance is primarily caused by linear dependencies among the generator vectors, which can produce codewords with lower Hamming weight. This demonstrates that the effectiveness of linear codes over Galois rings is more strongly determined by the structure of the generator matrix than by the presence of zero divisors.

Hence, carefully selection of generator matrices is essential for constructing efficient linear codes over Galois rings. Future work may investigate systematic construction methods and alternative generator structures to obtain codes with improved minimum distance and enhanced performance in digital communication systems.

REFERENCE

Blahut, R. E. (2003). *Algebraic Codes for Data Transmission*. Cambridge University Press. https://doi.org/10.1017/CBO9780511800467

Dinh, H. Q., & López-Permouth, S. R. (2004). Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, *50*(8), 1728–1744. https://doi.org/10.1109/TIT.2004.831789

Dougherty, S. T. (2017). Codes over finite rings. In *Handbook of Coding Theory*. Elsevier. https://doi.org/10.1016/B978-0-444-52927-7.00012-4

Esmaeili, R. S. and M. (2009). Cyclic and negacyclic codes over the Galois ring GR(p^2,m),". *Discrete Applied Mathematics*, *157*(13), 2892–2903. https://doi.org/10.1016/j.dam.2009.03.001

Gassner, N., Greferath, M., Rosenthal, J., & V. Weger. (2022). Bounds for coding theory over rings. *Entropy*, *24*(10). https://doi.org/10.3390/e24101473

Greferath, M., & Schmidt, S. E. (1999). Gray isometries for finite chain rings and nonlinear codes. *IEEE Transactions on Information Theory*, *45*(7), 2522–2524. https://doi.org/10.1109/18.796389

Greferath, M., & Schmidt, S. E. (2000). Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, *92*(1), 17–28. https://doi.org/10.1006/jcta. 1999.3033

Hamming, R. W. (1950). Error detecting and error correcting codes. *Bell System Technical Journal*, *29*(2), 147–160. https://doi.org/10.1002/j.1538-7305.1950.tb00463.x

Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., & Solé, P. (1994). The Z4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, *40*(2), 301–319. https://doi.org/10.1109/18.312154

Hill, R. (1986). *A First Course in Coding Theory*. Oxford University Press.

Holdman, G. R. (2016). *Error-Correcting Codes Over Galois Rings* [Undergraduate Honors Thesis]. Whitman College.

Huffman, W. C., & Pless, V. (2003). *Fundamentals of Error-Correcting Codes. Cambridge*. Cambridge University Press. https://doi.org/10.1017/CBO9780511807077

Jitman, S., & Ling, S. (2019). On codes over Galois rings and related structures. *Journal of Algebra and Its Applications*, *18*(4). https://doi.org/10.1142/S021949881950073X

Lin, S., & Costello, D. J. (2004). *Error Control Coding, 2nd ed*. Prentice Hall.

Ling, S., & Solé, P. (2001). On the algebraic structure of quasi-cyclic codes I: Finite fields. *IEEE Transactions on Information Theory*, *47*(7), 2751–2760. https://doi.org/10.1109/18.945292

Lint, J. H. van. (1999). *Introduction to Coding Theory, 3rd ed*. https://doi.org/10.1007/978-3-662-03933-5

MacWilliams, F. J., & Sloane, N. J. A. (1977). *The Theory of Error-Correcting Codes*. North-Holland.

Nechaev, A. A. (1991). Kerdock code in a cyclic form. *Discrete Mathematics and Applications*, *1*(4), 365–384.

Norton, G. H., & Sălăgean, A. (2000). On the structure of linear and cyclic codes over a finite chain ring. *Applicable Algebra in Engineering, Communication and Computing*, *10*, 489–506. https://doi.org/10.1007/s002000050137

Peterson, W. W., & Weldon, E. J. (1972). *Error-Correcting Codes, 2nd ed*. MIT Press.

Pless, V. (1998). *Introduction to the Theory of Error-Correcting Codes, 3rd ed*. Wiley.

Roman, S. (1992). *Coding and Information Theory*. Springer. https://doi.org/10.1007/978-1-4612-2824-1

Wan, Z.-X. (2003). *Lectures on Finite Fields and Galois Rings* (Vol. 8). World Scientific. https://doi.org/10.1142/5342

Wood, J. A. (1999). Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, *121*(3), 555–575.

Zhang, A., Li, J., & Feng, K. (2016). Linear codes over Galois rings related to Gauss sums. *IEEE Transactions on Information Theory*, *62*(11), 6150–6157. https://doi.org/10.1109/TIT.2016.2608890