**Prosiding Seminar Nasional Matematika dan Pendidikan Matematika (SESIOMADIKA) 2025**
Tema: Mendidik dengan matematika, membentuk dunia dengan data: Peran pendidikan matematika, pemodelan dan machine learning dalam era peradaban cerdas

# Weight Distribution dari Kode atas *Galois Ring* $GR(2^3)$ Menggunakan *Lee Distance*

**Luthfi Mahendra Widiarto***
Universitas Sebelas Maret, *Penulis Korespondensi: luthfimw@student.uns.ac.id

**Santoso Budi Wiyono**
Universitas Sebelas Maret

**Putranto Hadi Utomo**
Universitas Sebelas Maret

**ABSTRAK**

Penelitian ini bertujuan untuk menganalisis konstruksi dan performa kode linear yang dibangun pada *Galois ring* $GR(2^3)$ menggunakan metrik *Lee distance* dalam menentukan kemampuan deteksi dan koreksi eror. Metode penelitian yang digunakan adalah kajian pustaka melalui studi literatur terhadap berbagai referensi relevan mengenai teori kode linear, *Galois ring,* dan penerapan *Lee distance*. Kode linear dibentuk sebagai submodul berdimensi dua dengan panjang kode $n = 3$, menggunakan dua pasangan vektor generator bebas linear yang berbeda, yaitu $g_1 = (7,7,7)$, $g_2 = (1,0,5)$ untuk matriks generator $G_1$, dan $g_1' = (7,6,7)$, $g_2' = (7,7,5)$ untuk matriks generator $G_2$. Setiap kombinasi linear dari kedua generator menghasilkan 64 *codeword*, yang kemudian dihitung bobot Lee-nya untuk menentukan distribusi bobot dan jarak minimum kode. Hasil penelitian menunjukkan bahwa submodul pertama memiliki bobot minimum $w_L = 2$ dengan jarak minimum $d_L = 2$, sehingga mampu mendeteksi satu eror namun belum dapat mengoreksi eror. Sementara itu, submodul kedua memiliki bobot minimum $w_L = 3$ dengan jarak minimum $d_L = 3$, sehingga mampu mendeteksi dua eror dan mengoreksi satu eror. Hasil ini menunjukkan bahwa pemilihan vektor generator berpengaruh terhadap peningkatan kemampuan deteksi dan koreksi eror pada kode linear yang dikonstruksi atas $GR(2^3)$.

**Kata kunci:** *Galois ring,* kode linear, *lee distance,* deteksi eror, koreksi eror

## PENDAHULUAN

Pada sistem komunikasi digital, keandalan dan keamanan transmisi data merupakan aspek yang sangat penting. Pesan yang dikirim melalui kanal komunikasi sering kali mengalami eror atau *noise*, sehingga diperlukan mekanisme yang mampu mendeteksi dan mengoreksi eror tersebut. Salah satu metode yang banyak digunakan adalah kode linear, yaitu himpunan *codeword* yang membentuk subruang vektor atau submodul dari suatu struktur aljabar tertentu. Menurut Gassner *et al.* (2022) dalam teori kode tradisional, kode linear didefinisikan sebagai subruang vektor berdimensi $k$ dari $\mathbb{F}_q^n$ dengan $\mathbb{F}_q$ adalah *finite field* berisi $q$ elemen. Du (2023) menyatakan bahwa penerapan kode linear mempu berperan sebagai mekanisme deteksi dan koreksi eror untuk menjaga keandalan serta keamanan sistem komunikasi dan penyimpanan data. Hal ini juga ditegaskan oleh Tao (2023) menyatakan bahwa pengembangan *error correction codes* berakar dari teori Shannon tentang pentingnya efektivitas dan keandalan transmisi informasi, serta menjadi dasar bagi kemajuan berbagai sistem komunikasi digital modern.

Secara umum, implementasi kode linear selama ini berbasis pada *finite field* biner $GF(2)$, yang telah memunculkan berbagai jenis kode linear seperti Hamming, BCH, dan Reed–Solomon. Meskipun efektif, kode linear berbasis $GF(2)$ memiliki keterbatasan dalam menangani tipe eror tertentu dan kurang fleksibel untuk memenuhi kebutuhan sistem komunikasi modern. Di sisi lain, perkembangan teknologi seperti jaringan 5G, *Wi-Fi* berbasis *Orthogonal Frequency Division Multiplexing (OFDM)*, serta *DNA storage*

membutuhkan sistem pengkodean yang lebih adaptif terhadap kompleksitas sinyal dan struktur data non-biner.

Keterbatasan tersebut mendorong eksplorasi struktur aljabar yang lebih umum, salah satunya adalah *Galois ring* dengan karakteristik $2^a$, misalnya $GR(2^a)$ (Dinh *et al.* (2022). Menurut Holdman dan Keef (2016), *Galois ring* merupakan generalisasi dari *Galois field* yang memiliki fleksibilitas lebih tinggi dalam konstruksi kode linear. Struktur *Galois ring* menyediakan operasi penjumlahan dan perkalian yang memungkinkan pembentukan kode linear dengan sifat-sifat yang tidak dapat dicapai melalui *Galois field.* Dalam konteks analisis jarak kode pada *Galois Ring,* Mohan *et al.* (2020) menunjukkan metrik *Lee distance* efektif digunakan untuk mengevaluasi jarak antar *codeword*, karena mengukur jarak antar *codeword* berdasarkan selisih nilai tiap simbol, bukan sekadar jumlah posisi yang berbeda seperti pada *Hamming distance*.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada konstruksi dan analisis kode linear pada *Galois ring* $GR(2^3)$ menggunakan metrik *Lee distance*. Penelitian ini juga berupaya menjawab bagaimana metrik tersebut dapat digunakan untuk menentukan jarak minimum antar *codeword*, serta meninjau kemampuan deteksi dan koreksi eror yang dihasilkan dari konstruksi kode tersebut. Dengan demikian, tujuan penelitian ini adalah untuk mengkonstruksi kode linear pada *Galois ring* $GR(2^3)$, menerapkan metrik *Lee distance* dalam analisis jarak minimum, serta menilai kemampuan deteksi dan koreksi eror yang dihasilkan.

Diharapkan penelitian ini dapat memberikan alternatif rancangan kode yang lebih efisien dalam mendeteksi dan mengoreksi eror pada sistem komunikasi digital non-biner, serta menjadi referensi akademik bagi studi lanjutan dalam bidang teori kode, komunikasi modern, maupun kriptografi.

## METODE

Penelitian ini menggunakan dua pendekatan utama, yaitu studi literatur untuk kajian teoritis dan analisis komputasional untuk implementasi dan evaluasi kode linear. Studi literatur dilakukan dengan menelaah berbagai referensi berupa buku teks dan artikel ilmiah yang membahas teori kode linear, struktur *Galois ring,* serta penggunaan metrik *Lee distance* dalam analisis jarak kode. Kajian ini digunakan sebagai dasar konsptual dalam menentukan definisi, sifat, dan parameter kode linear yang dikonstruksi.

Berdasarkan kajian teoritis tersebut, dilakukan konstruksi kode linear pada *Galois ring* $GR(2^3)$. Panjang kode dipilih sebesar $n = 3$, dengan pertimbangan bahwa nilai tersebut cukup untuk menghasilkan struktur kode yang tidak trivial namun masih menungkinkan dilakukan analisis secara sistematis dan komputasional. Kode linear dibentuk sebagai submodul berdimensi dua dari $GR(2^3)^3$, dengan menggunakan dua himpunan vektor generator yang saling bebas linear. Setiap himpunan generator digunakan untuk membangun satu metrics generator, sehingga diperoleh dua konstruksi kode linear yang berbeda untuk keperluan perbandingan.

Tahap analisis komputasional dilakukan untuk menghasilkan seluruh *codeword* dari masing-masing matriks generator serta menghitung bobot Lee dan jarak Lee antar *codeword.* Dari hasil perhitungan tersebut, ditentukan jarak minimum kode dan dianalisis kemampuan deteksi serta koreksi eror yang dimiliki oleh masing-masing konstruksi kode lienar. Implementasi komputasional dilakukan menggunakan bahasa pemrograman Python, dengan memanfaatkan operasi aritmetika modular dan struktur data vektor untuk merepresentasikan elemen-elemen *Galois ring* $GR(2^3)$. Hasil analisis komputasional kemudian digunakan untuk mendukung pembahasan teoritis yang diperoleh dari kajian literatur.

## HASIL DAN PEMBAHASAN

Penelitian ini mengkaji pembentukan kode linear pada *Galois ring* $GR(2^3)$ yang isomorfik terhadap $\mathbb{Z}_8$. *Ring* $GR(2^3) \cong \mathbb{Z}_8$ memililki delapan elemen, yaitu $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Struktur ini digunakan sebagai himpuanan dasar dalam membentuk ruang modul dan submodul yang akan menjadi kode linear.

Langkah pertama adalah menentukan panjang kode $n$. Dalam penelitian ini, panjang kode dipilih sebesar $n = 3$. Pemilihan panjang kode tersebut didasarkan pada pertimbangan bahwa untuk $n < 3$, kode menjadi terlalu pendek sehingga tidak dapat mendeteksi eror dengan baik, sedangkan untuk $n > 3$, jumlah elemen kode menigkat secara eksponensial sehingga perhitungan menjadi telalu kompleks untuk dilakukan. Oleh karena itu, ruang modul yang terbentuk adalah $\left(GR(2^3)\right)^3 = (\mathbb{Z}_8)^3$ yang memiliki $8^3 = 512$ elemen.

Kode linear $C$ didefinisikan sebagai submodul dari $\left(GR(2^3)\right)^3$ dengan dimensi $k = 2$. Submodul tersebut dibangkitkan oleh dua vektor generator yang bebas linear di dalam $(\mathbb{Z}_8)^3$. Untuk meninjau pengaruh pemilihan generator terhadap karakteristik kode, dibentuk dua matriks generator yang berbeda. Matriks generator pertama menggunakan vektor

$$g_1 = (7, 7, 7) \text{ dan } g_2 = (1, 0, 5),$$

sedangkan matriks generator kedua menggunakan

$$g_1' = (7, 6, 7) \text{ dan } g_2' = (7, 7, 5).$$

Terbentuk dua matriks generator yang berbeda yaitu

$$G_1 = [g_1; g_2],\ G_2 = [g_1'; g'_2].$$

Kedua matriks generator tersebut kemudian digunakan untuk menghasilkan seluruh *codeword* yang dibentuk oleh kombinasi linear

$$C = \langle g_1, g_2 \rangle = \{(ag_1 + bg_2) \bmod 8 \mid a, b \in GR(2^3)\}$$

dan

$$C' = \langle g_1', g_2' \rangle = \{(ag_1' + bg_2') \bmod 8 \mid a, b \in GR(2^3)\}.$$

Sebagai contoh perhitungan pada matriks generator $G_1 = [g_1; g_2]$ dengan $g_1 = (7, 7, 7)$ dan $g_2 = (1, 0, 2)$, misalkan dipilih $a = 2$ dan $b = 3$. Maka diperoleh

$$c = (2(7, 7, 7) + 3(1, 0, 5))(\text{mod } 8)$$
$$c = (2 \times 7 + 3 \times 1, 2 \times 7 + 3 \times 0, 2 \times 7 + 3 \times 5)(\text{mod } 8)$$
$$c = (14 + 3, 14 + 0, 14 + 15)(\text{mod } 8) = (17, 14, 29)(\text{mod } 8)$$

Sehingga diperoleh salah satu *codeword* dari submodul $C$ adalah $c = (1, 6, 5)$.

Untuk matriks generator kedua $G_2 = [g_1'; g_2']$ dengan $g_1' = (7, 6, 7)$ dan $g_2' = (7, 7, 5)$, misalkan juga dipilih $a = 2$ dab $b = 3$. Maka diperoleh

$$c' = (2(7, 6, 7) + 3(7, 7, 5))(\text{mod } 8)$$
$$c' = (2 \times 7 + 3 \times 7, 2 \times 6 + 3 \times 7, 2 \times 7 + 3 \times 5)(\text{mod } 8)$$
$$c' = (14 + 21, 12 + 21, 14 + 15)(\text{mod } 8) = (35, 33, 29)(\text{mod } 8)$$

Sehingga diperoleh salah satu *codeword* dari submodul $C'$ adalah $c' = (3, 1, 5)$.

Dengan cara serupa, seluruh kombinasi pasangan $(a, b)$ dengan $a, b \in GR(2^3)$ menghasilkan total $8^2 = 64$ *codeword* yang berbeda dari masing-masing matriks generator $G_1$ dan $G_2$.

Setelah semua *codeword* diperoleh dari masing-masing matriks generator, langkah berikutnya adalah menghitung bobot Lee dari setiap *codeword*. Bobot Lee dihitung berdasarkan jumlah jarak Lee dari setiap komponen dalam vektor terhadap komponen vektor nol. Untuk elemen $x \in \mathbb{Z}_8$, bobot Lee didefinisikan sebagai berikut,

$$w_L(x) = \min(x, 8 - x),$$

dan jarak Lee antara dua *codeword* $x = (x_1, x_2, \ldots, x_n)$ dan $y = (y_1, y_2, \ldots, y_n)$ didefinisikan sebagai,

$$d_L(x,y) = \sum_{i=1}^{n} w_L(x_i - y_i).$$

Sebagai contoh, dari hasil kombinasi pada matriks generator $G_1$ diperoleh salah satu *codeword* $c = (1,6,5)$. Untuk menentukan bobot Lee dari *codeword* ini, dilakukan perhitungan sebagai berikut,

$$w_L(1) = \min(1\ ,8-1) = 1,$$
$$w_L(6) = \min(6, 8-6) = 2,$$
$$w_L(5) = \min(5, 8-5) = 3.$$

Maka total bobot Lee dari *codeword* $c = (1,6,5)$ adalah,

$$w_L(c) = 1 + 2 + 3 = 6.$$

Kemudian bobot Lee dari *codeword* $c'$ pada matriks generator $G_2$ sebagai berikut,

$$w_L(3) = \min(3, 8-3) = 3$$
$$w_L(1) = \min(1, 8-1) = 1$$
$$w_L(5) = \min(5, 8-5) = 3$$

Maka total bobot Lee dari *codeword* $c' = (3,1,5)$ adalah,

$$w_L(c') = 3 + 1 + 3 = 7.$$

Dari dua contoh tersebut, dapat dilihat bahwa *codeword* $c$ dan $c'$ memiliki bobot Lee yang berbeda, yaitu 6 dan 7. Perbedaan bobot Lee ini menunjukkan bahwa struktur generator yang digunakan memengaruhi distribusi jarak minimum pada kode linear yang dibentuk. Nilai jarak minimum tersebut kemudian dibandingkan dengan nilai *codeword* lainnya untuk menganalilsis kemampuan kode dalam mendeteksi dan mengkoreksi eror pada sistem komunikasi digital.

Setelah dilakukan perhitungan terhadap contoh *codeword* dari masing-masing matriks generator $G_1$ dan $G_2$, langkah selanjutnya adalah menerapkan prosedur yang sama untuk seluruh kombinasi $a, b \in GR(2^3)$ pada masing-masing generator. Dengan demikian, seluruh *codeword* yang dihasilkan dari setiap pasangan vektor generator dihitung bobot Lee nya secara menyeluruh. Setiap *codewrod* pada $GR(2^3)^3$ dengan dimensi submodul $k = 2$ kemudian dikelompokkan berdasarkan nilai bobot totalnya.

Hasil perhitungan ini memberikan gambaran mengenai distribusi bobot Lee pada masing-masing submodul, yang menggambarkan perbedaan karakteristik jarak minimum serta kemampuan deteksi dan koreksi eror dari setiap kode linear yang dibentuk. Hasil perhitungan ditampilkan pada Tabel 1, yang memuat jumlah *codeword* untuk setiap nilai bobot Lee pada masing-masing matriks generator.

Distribusi bobot Lee pada Tabel 1 menunjukkan bahwa distribusi bobot Lee berbeda untuk masing-masing pilihan matriks generator. Berdasarkan teori pengkodean, sebuah kode dengan jarak minimum $d$ dapat mendeteksi hingga $d-1$ eror dan mampu mengoreksi hingga $\lfloor \frac{d-1}{2} \rfloor$ eror. Nilai bobot minimum yang diperoleh dari masing-masing submodul kemudian digunakan untuk menilai kemampuan deteksi dan koreksi erornya.

Untuk submodul pertama dengan generator $g_1 = (7,7,7)$ dan $g_2 = (1,0,5)$, diperoleh bobot minimum vektor *non-zero* sebesar $w_L = 2$, sehingga jarak minimum Lee nya adalah $d_L = 2$. Berdasarkan rumus tersebut, kode ini mampu mendeteksi hingga $d_L - 1 = 1$ eror, namun belum dapat melakukan koreksi karena $\lfloor \frac{d_L-1}{2} \rfloor = 0$.

Sementara itu, untuk submodul kedua dengan generator $g_1' = (7,6,7)$dan $g_2' = (7,7,5)$, diperoleh bobot minimum vektor *non-zero* sebesar $w_L = 3$, yang berarti jarak minimum Lee-nya adalah $d_L = 3$. Dengan demikian, kode pada submodul kedua dapat mendeteksi hingga $d_L - 1 = 2$ eror dan mengoreksi hingga $\lfloor \frac{d_L-1}{2} \rfloor = 1$ eror.

Tabel 1. Tabel Distribusi Bobot Lee pada Submodul Berdimensi Dua

| $g_1 = (7,7,7)$ dan $g_2 = (1,0,5)$ | | $g_1' = (7,6,7)$ dan $g_2' = (7,7,5)$ | |
|---|---|---|---|
| Bobot $w_L(c)$ | Jumlah *Codeword* | Bobot $w_L(c)$ | Jumlah *Codeword* |
| 0 | - | 0 | - |
| 1 | 0 | 1 | 0 |
| 2 | 2 | 2 | 0 |
| 3 | 4 | 3 | 6 |
| 4 | 7 | 4 | 11 |
| 5 | 12 | 5 | 10 |
| 6 | 12 | 6 | 8 |
| 7 | 12 | 7 | 10 |
| 8 | 7 | 8 | 11 |
| 9 | 4 | 9 | 6 |
| 10 | 2 | 10 | 0 |
| 11 | 0 | 11 | 0 |
| 12 | 1 | 12 | 1 |

Hasil ini menunjukkan bahwa variasi pemilihan vektor generator memberikan pengaruh langsung terhadap peningkatan kemampuan deteksi dan koreksi eror dari kode linear yang dibangun di atas $GR(2^3)$. Temuan ini sejalan dengan hasil penelitian Mohan *et al.* (2020) yang menyatakan bahwa struktur kode linear pada *Galois ring* sangat dipengaruhi oleh pemilihan matriks generator. Penelitian ini juga mendukung pandangan Holdman dan Keef (2016) bahwa *Galois ring* menyediakan fleksibilitas structural yang lebih besar dibandingkan *Galois field* dalam konstruksi kode linear non-biner.

## SIMPULAN

Penelitian ini menunjukkan bahwa konstruksi kode linear pada *Galois ring* $GR(2^3)$ dengan panjang kode $n = 3$ dan dimensi submodul $k = 2$ menghasilkan karakteristik deteksi dan koreksi eror yang berbeda, bergantung pada pemilihan vektor generator. Analisis menggunakan metrik *Lee distance* memperlihatkan bahwa variasi generator berpengaruh langsung terhadap nilai jarak minimum kode yang menentukan kemampuan deteksi dan koreksi eror. Hasil penelitian ini menjawab tujuan utama penelitian, yaitu membuktikan bahwa penilihan struktur generator yang tepat pada kode linear berbasis *Galois ring* dapat meningkatkan performa kode. Temuan ini mendukung teori Holdman dan Keef (2016) sebelumnya bahwa *Galois ring* memberikan fleksibilitas lebih tinggi dibandingkan *finite field* biner dalam perancangan kode linear pada sistem non-biner. Kode linear berbasis $GR(2^3)$ dengan metrik *Lee distance* berpotensi diterapkan pada sistem komunikasi dan penyimpanan data non-biner yang membutuhkan ketahanan eror lebih baik. Penelitian selanjutnya dapat diarahkan pada penggunaan panjang kode dan dimensi yang lebih besar, serta perbandingan performa kode linear berbasis *Galois ring* dengan kode linear pada *finite field* dalam konteks aplikasi komunikasi modern.

## DAFTAR PUSTAKA

Astola, H., & Tabus, I. (2016). On the linear programming bound for linear Lee codes. *SpringerPlus, 5*, Article 246. https://doi.org/10.1186/s40064-016-1863-8

Astsauri, M. F., & Utomo, P. H. (2025). Penerapan struktur aljabar Galois field pada *error-correcting codes*. In *Proceedings of the Galuh Mathematics National Conference*.

Bariffi, J., & Weger, V. (2023). Better bounds on the minimal Lee distance. *arXiv*. https://arxiv.org/abs/2307.06079

Choukroun, Y., & Wolf, L. (2024). Learning linear block error correction codes. *IEEE Journal on Selected Areas in Communications, 42*(1), 98–110.

Dinh, H. Q., Kewat, P. K., & Mondal, N. K. (2022). Lee distance distribution of repeated-root constacyclic codes over GR($2^e$, m) and related MDS codes. *Journal of Applied Mathematics and Computing, 68*(6), 3861–3872.

Du, X. (2023). Performance analysis of several common error correction codes. *Applied and Computational Engineering, 14*(1), 211–219.

Gassner, N., Greferath, M., Rosenthal, J., & Weger, V. (2022). Bounds for coding theory over rings. *Entropy, 24*(10), Article 1406.

Holdman, G. R., & Keef, P. (2016). *Error-correcting codes over Galois rings*. Springer.

Irwansyah, I., & Suprijanto, D. (2022). Linear codes over a general family of rings and MacWilliams-type relations. *Discrete Mathematics Letters, 11*, 53–60.

Jose, L., Lavanya, G., & Sharma, A. (2025). Linear codes over a mixed-alphabet ring and their Gray images with applications to projective and locally repairable codes. *Manuscript submitted for publication*.

Kim, B., & Lee, Y. (2017). Lee weights of cyclic self-dual codes over Galois rings of characteristic $p^2$. *Finite Fields and Their Applications, 45*, 107–130.

Mohan Cruz, J., et al. (2020). On the covering radius of codes over $\mathbb{Z}_{(p^k)}$. *Manuscript submitted for publication*.

Qi, W. (2024). The polycyclic codes over $\mathbb{F}$_q. *AIMS Mathematics, 9*(11), 29707–29717.

Suprijanto, D. (2023). Linear codes and cyclic codes over finite rings and their generalizations: A survey. *Electronic Journal of Graph Theory and Applications, 11*(2).

Tao, Y. (2023). Research and application of several error correction codes in communication. In *Highlights in Science, Engineering and Technology: ACME* (Vol. 2023).

Tiwari, R., et al. (2024). Additive conjucyclic codes over a class of Galois rings. *Journal of Applied Mathematics and Computing, 70*, 235–250.

Wang, Y., & Zhou, H. (2025). Counting polynomials with distinct zeros in Galois ring GR($p^2$, r). *Discrete Mathematics, 348*(1), Article 113789.

Wang, Z., Li, N., Zeng, X., & Tang, X. (2025). The Lee weight distributions of linear codes over $\mathbb{Z}_4$. *arXiv*.

Wang, Z., Li, N., Zeng, X., & Tang, X. (2025). The Lee weight distributions of several classes of linear codes over $\mathbb{Z}_4$. *Manuscript in preparation*.

Zeng, X., Li, N., & Tang, X. (2024). Generalized toric codes on twisted tori for quantum error correction. *Quantum Information Processing, 23*(6), Article 210.