Proceeding Galuh Mathematics National Conference
Vol. 5 No.1 2025 | Hal 162-167 | ISSN: 3032-2588
https://jurnal.unigal.ac.id/GAMMA-NC/article/view/19161

PENERAPAN STRUKTUR ALJABAR *GALOIS FIELD* PADA *ERROR-CORRECTING CODES*

Muhammad Faris Atstsauri[1*], Putranto Hadi Utomo[2]
Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret
Email: farisatstsauri@student.uns.ac.id

ABSTRAK

Perkembangan teknologi komunikasi digital menuntut sistem transmisi data yang tidak hanya cepat, tetapi juga andal dalam menghadapi gangguan. *Error* dalam pengiriman data dapat menyebabkan informasi yang diterima berbeda dari yang dikirim, sehingga diperlukan sistem yang mampu mendeteksi dan memperbaiki *error* secara otomatis. Salah satu pendekatan matematis yang mendasari pengembangan sistem tersebut adalah teori *error-correcting codes* yang memanfaatkan struktur aljabar *Galois Field*. Penelitian ini bertujuan untuk mengkaji penerapan *Galois Field*, khususnya $GF(2)$ dan $GF(2^m)$, dalam membangun kode linier dan kode siklik. Metode yang digunakan adalah studi literatur dengan menganalisis konsep-konsep dasar aljabar seperti *grup, ring, field*, dan ruang vektor, serta penerapannya dalam pengodean data. Hasil penelitian menunjukkan bahwa matriks generator dan matriks cek paritas dapat dibangun melalui basis dalam $GF(2)$ dan hubungan antara keduanya merepresentasikan struktur ruang kode dan kernel. Dalam $GF(2^m)$, representasi elemen sebagai polinomial dan vektor membuka peluang pengembangan kode siklik seperti Reed–Solomon yang memiliki kemampuan deteksi dan koreksi *error* lebih tinggi. Kebaruan dari penelitian ini terletak pada penyajian terstruktur mengenai hubungan antara struktur aljabar *Galois Field* dan teori *error-correcting codes* yang bertujuan memberikan pemahaman yang utuh terhadap dasar matematis sistem komunikasi digital. Penelitian ini diharapkan menjadi landasan bagi penelitian lanjutan dalam optimalisasi algoritma decoding, serta pengembangan sistem pengodean berbasis kecerdasan buatan untuk mendukung komunikasi digital yang adaptif dan efisien.

Kata Kunci: *Error-Correcting Codes*, *Galois Field, Struktur Aljabar*

Dikirim: Mei 2025; Diterima: Juni 2025; Dipublikasikan: Juni 2025
Cara sitasi: Atstsauri, M., & Utomo, P. H. (2025). Penerapan Struktur Aljabar *Galois Field* pada *Error-Correcting Codes*. *Proceeding Galuh Mathematics National Conference*, *5*(1), 162-167.

PENDAHULUAN

Perkembangan teknologi telah mendorong transformasi komunikasi dari tatap muka menjadi digital melalui media elektronik seperti internet dan telepon seluler. Komunikasi digital modern menuntut sistem transmisi data yang cepat sekaligus andal. Claude Shannon (1948), dalam karya monumentalnya *A Mathematical Theory of Communication*, menyatakan bahwa *"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point."* Pernyataan ini menekankan pentingnya menjaga integritas pesan selama proses transmisi, yang menjadi dasar lahirnya teori informasi.

Dalam praktiknya, komunikasi digital kerap mengalami gangguan yang menyebabkan *error* pada data yang diterima. Untuk mengatasi hal ini, dikembangkan sistem *error-correcting codes* yang mampu mendeteksi dan memperbaiki *error* tanpa perlu pengiriman ulang data. Salah satu pendekatan matematis yang digunakan dalam pengembangan sistem ini adalah struktur aljabar *Galois Field*, yaitu *finite field* (himpunan berhingga) yang memenuhi aksioma *field*. *Galois Field* telah diterapkan luas dalam pengodean dan kriptografi, termasuk pada algoritma *Advanced Encryption Standard* (AES) (Stallings, 2005).

Bentuk paling sederhana dalam *Galos Field* adalah $GF(2)$ yang hanya terdiri dari dua elemen $\{0,1\}$ dan menjadi dasar bagi kode linier seperti Hamming Code. Sementara itu, $GF(2^m)$ memungkinkan representasi elemen dalam bentuk polinomial, yang mendasari konstruksi kode siklik seperti Reed–Solomon yang efektif dalam menangani kesalahan beruntun. Menurut Pless (1998), struktur aljabar seperti ruang vektor, *field*, dan polinomial merupakan fondasi penting dalam membangun sistem *error-correcting* yang efisien dan sistematis.

Penelitian ini bertujuan untuk mengkaji penerapan struktur aljabar *Galois Field* dalam konstruksi kode linier dan kode siklik, serta menganalisis keterkaitan antara konsep aljabar dan sistem pengodean digital. Pembahasan dalam artikel ini mencakup struktur $GF(2)$ dalam pembentukan matriks generator dan matriks cek paritas, dilanjutkan dengan analisis hubungan antara ruang kode dan kernel. Selanjutnya dibahas struktur kode siklik dalam $GF(2^m)$, implementasi Reed–Solomon, serta studi kasus proses encoding dan decoding berbasis sindrom.

METODE PENELITIAN

Penelitian ini merupakan studi literatur yang bertujuan mengkaji penerapan struktur aljabar *Galois Field* dalam sistem *error-correcting codes*, khususnya pada kode linier dan kode siklik seperti Reed–Solomon. Penelitian dilakukan secara konseptual dan teoretis dengan pendekatan deduktif, berfokus pada analisis konsep-konsep aljabar abstrak yang berkaitan dengan teori pengodean.

Tahapan dimulai dengan identifikasi masalah, yaitu bagaimana struktur aljabar seperti *grup, ring, field*, dan khususnya *Galois Field* digunakan dalam pembentukan sistem pengodean yang mampu mendeteksi dan memperbaiki *error*. Fokus utama diarahkan pada peran $GF(2)$ dalam penyusunan kode linier melalui matriks generator G dan matriks pemeriksa paritas H, serta hubungan keduanya dalam konteks kernel dan ruang dual kode. Untuk kode siklik dan Reed–Solomon, penelitian memperluas kajian ke *field extension* $GF(2^m)$, di mana elemen-elemen *field* direpresentasikan sebagai polinomial biner dengan operasi modulo *irreducible polynomial*.

Data dikumpulkan dari berbagai sumber sekunder seperti buku teks aljabar, artikel jurnal internasional, dan referensi akademik yang relevan. Selanjutnya, materi diklasifikasikan berdasarkan tema-tema utama, seperti struktur dasar aljabar, konstruksi *Galois Field*, dan penerapannya dalam teori pengodean. Analisis dilakukan secara deduktif dengan menelusuri keterkaitan antar konsep dan menurunkan formulasi-formulasi matematis seperti transformasi vektor pesan melalui G, verifikasi sindrom dengan H, serta prosedur encoding-decoding berbasis polinomial. Untuk mendukung penjelasan, digunakan representasi matematis formal dan ilustrasi berbasis kasus.

Proceeding Galuh Mathematics National Conference
Vol. 5 No.1 2025 | Hal 162-167 | ISSN: 3032-2588
https://jurnal.unigal.ac.id/GAMMA-NC/article/view/19161

HASIL DAN PEMBAHASAN

Struktur Kode Linear dalam $GF(2)$

Kode linear dalam *Galois Field* $GF(2)$ merupakan subruang vektor dari ruang vektor $GF(2)^n$, dimana setiap *codeword* direpresentasikan sebagai kombinasi linear dari vektor-vektor basis. $GF(2)$ terdiri dari dua elemen, yaitu $\{0, 1\}$, dengan operasi penjumlahan dan perkalian modulo 2. Sifat-sifat $GF(2)$ yang tertutup, asosiatif, dan komutatif (Lidl & Neiderreiter, 1994) menjadikannya fondasi ideal untuk konstruksi *error-correcting codes*.

Setiap kode linear $[n, k]$ dalam $GF(2)$ memiliki dimensi k, yang berarti terdapat k vektor basis yang membangun seluruh ruang kode. Basis ini direpresentasikan dalam bentuk matriks generator G berukuran $k \times n$ (Ling & Xing, 2004). Misal, untuk kode $[5,3]$, matriks generator Gdapat ditulis sebagai,

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

Setiap *codeword* $\boldsymbol{c}$ dihasilkan dari perkalian vektor pesan $\boldsymbol{m}$ dengan matriks generator,

$$\boldsymbol{c} = \boldsymbol{m}G$$

Operasi ini dilakukan dalam $GF(2)$, sehingga penjumlahan koefisien menggunakan operasi XOR. Sebagai contoh, misalkan vector pesan $\boldsymbol{m} = (1,0,1)$, maka *codeword* yang dihasilkan adalah

$$\boldsymbol{c} = (1,0,1) \cdot G = (1,0,1,0,0)$$

Proses ini menunjukkan bagaimana struktur aljabar dalam $GF(2)$ memungkinkan pembentukan *codeword* secara sistematis.

Jarak minimum d dalam kode linear menentukan Kemampuan deteksi dan koreksi kesalahan. Untuk kode dengan jarak minimum d, jumlah kesalahan yang dapat dideteksi adalah $d - 1$, sedangkan kesalahan yang dapat dikoreksi adalah $\left\lfloor \frac{d-1}{2} \right\rfloor$. Dalam $GF(2)$, jarak minimum dihitung menggunakan bobot Hamming, yaitu jumlah posisi bit yang bernilai 1.

Matriks Generator dan Cek Paritas

Matriks generator G berukuran $k \times n$ merupakan inti dari kode linear dalam $GF(2)$. Setiap baris G adalah vektor basis yang membangun ruang kode. Matriks generator G mengubah vektor pesan $\boldsymbol{m}$ menjadi *codeword* $\boldsymbol{c}$ melalui operasi $\boldsymbol{c} = \boldsymbol{m}G$. Baris-baris G harus bersifat bebas linear agar dimensi kode menjadi k ini disebut independensi linear (Pless, 1998). Bentuk standar dari G adalah

$$G = [I_K | X]$$

Dimana I_k adalah matriks identitas berukuran $k \times k$ dan X adalah matriks berukuran $k \times (n - k)$. Dalam bentuk ini, kode disebut sistematis karena memisahkan bit Informasi dan bit paritas.

Matriks cek paritas H berukuran $(n - k) \times n$ memvalidasi *codeword* dengan hubungan ortogonal,

$$H \cdot \boldsymbol{c}^T = 0 \quad \forall \boldsymbol{c} \in C.$$

Jika bentuk $G = [I_k | X]$, maka $H = [-X^T | I_{n-k}]$, dalam $GF(2)$, $-X^T = X^T$ (Ling & Xing, 20024). Misal H dari G adalah,

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Proses decoding dari kode linear adalah dengan menghitung sindrom $\boldsymbol{s} = \boldsymbol{r}H^T$, Dimana $\boldsymbol{r}$ merupakan vektor yang diterima. Jika $\boldsymbol{s} \neq 0$, maka terdapat *error*. Misal $\boldsymbol{r} = (1,1,1,0,0,0,1)$ sehingga $\boldsymbol{s} = (0,1,1)$ ini menunjukan *error* terjadi pada posisi ke-2.

Hubungan antara G dan H adalah pada kernel dan dualitas. Ruang kode C adalah kernel dari H, hal ini ditunjukan dari $C = \{\boldsymbol{c} | H\boldsymbol{c}^T = 0\}$. Dualitas ini ditunjukkan oleh fakta bahwa baris-baris dari matriks H membentuk basis untuk ruang dual $C^{\perp}$ dari kode C.

Proceeding Galuh Mathematics National Conference
Vol. 5 No.1 2025 | Hal 162-167 | ISSN: 3032-2588
https://jurnal.unigal.ac.id/GAMMA-NC/article/view/19161

Kode Siklik

Kode siklik merupakan kelas khusus dari kode linear yang tidak berubah oleh pergeseran siklik, sehingga setiap pergeseran satu posisi menghasilkan *codeword* lain dalam himpunan kode. Jika $\boldsymbol{c} = (c_0, c_1, \dots, c_{n-1})$ adalah sebuah *codeword*, maka pergeseran sikliknya $\boldsymbol{c'} = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$ juga merupakan *codeword*. Sifat ini memungkinkan implementasi *encoder* dan *decoder* yang efisien menggunakan register geser. Dalam aljabar, kode siklik dapat direpresentasikan sebagai ideal dalam *ring* polinomial $GF(2)[x]/(x^n - 1)$ (Lidl & Neiderreiter, 1994). Setiap *codeword* c direpresentasikan sebagai polinomial,

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

dan operasi pergeseran siklik ekuivalen dengan perkalian polinomial dengan x modulo $x^n - 1$.

Untuk membangun kode siklik yang lebih kompleks, sering digunakan *finite field extension* yaitu $GF(2^m)$ Representasi elemen $GF(2^m)$ sebagai polinomial dengan koefisien di $GF(2)$ memungkinkan operasi aritmetika yang terstruktur. Misalnya, untuk $GF(2^3)$ dengan polinomial primitif $p(x) = x^3 + x + 1$, elemen-elemennya dapat direpresentasikan seperti yang ditampilkan dalam Tabel 1.

Tabel 1. Representasi Elemen $GF(2^3)$

Notasi Polinomial	Pangkat α	Biner
0	0	000
1	α^0	001
α	α^1	010
α	α^2	100
$\alpha + 1$	α^3	011
$\alpha^2 + \alpha$	α^4	110
$\alpha^2 + \alpha + 1$	α^5	111

Kode siklik sepenuhnya ditentukan oleh generator polinomial $g(x)$ yang membagi $x^n - 1$. Generator polinomial memiliki bentuk $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ dengan $r = n - k$. *Codeword* $c(x)$ harus memenuhi

$$c(x) \equiv 0 \bmod g(x)$$

Langkah-langkah encoding kode siklik dengan parameter $[n, k]$ adalah sebagai berikut,

1. Representasi pesan sebagai polinomial $m(x)$ (derajat $< k$).
2. Kalikan $m(x)$ dengan x^{n-k}, sehingga diperoleh $m(x)x^{n-k}$. Langkah ini menyisipkan ruang untuk bit-bit paritas.
3. Hitung sisa pembagian $m(x)x^{n-k}$ oleh polinomial generator $g(x)$ sebagai polinomial paritas $p(x)$.
4. *Bentuk codeword* $c(x)$ dengan menjumlahkan hasil perkalian dan sisa pembagian,
$$c(x) = m(x)x^{n-k} + p(x).$$

Sebagai ilustrasi misalkan diberikan kode $[7,4]$ dengan polinomial generator $g(x) = x^3 + x + 1$, dan pesan $m(x) = x^2 + 1$, yang dalam bentuk biner adalah "101". Pertama-tama, pesan $m(x)$ dikalikan dengan x^3, sehingga diperoleh $x^5 + x^3$. Kemudian, dilakukan pembagian polinomial ini dengan $g(x)$, dan sisa pembagiannya adalah $x + 1$. Maka, *codeword* yang dihasilkan adalah $x^5 + x^3 + x + 1$, atau dalam bentuk biner "1010011". Dengan demikian, *codeword* "1010011" merupakan representasi dari pesan "101" yang telah diencoding menggunakan metode kode siklik.

Proses decoding diawali dengan menerima polinomial $r(x)$, yang merupakan representasi *codeword* yang mungkin telah mengalami gangguan. Decoding kode siklik melibatkan perhitungan Sindrom $S(x) = r(x) \ mod \ g(x)$. Kemudian diidentifikasi *error* jika $S(x) \neq 0$, gunakan algoritma seperti Peterson-Gorenstein-Zierler untuk menemukan lokasi *error.*

Reed Solomon

Kode Reed–Solomon adalah salah satu *error-correcting codes* paling kuat yang bekerja pada $GF(2^m)$ dan termasuk dalam kelas kode siklik. Kode ini umum digunakan dalam penyimpanan data dan komunikasi digital karena kemampuannya mengoreksi simbol *error* secara efisien. Dengan parameter $n = 2^m - 1$, $k = n - 2t$, dan jarak minimum $d = 2t + 1$, Reed-Solomon mampu mengoreksi hingga t simbol *error* (Pless, 1998; Blahut, 2003).

Untuk $k = 3$, $t = 2$, dan $GF(2^3)$, proses encoding dimulai dengan merepresentasikan pesan sebagai polinomial $m(x) = \alpha^2 x^2 + x + \alpha$. Setelah dikalikan dengan x^4, diperoleh $\alpha^2 x^6 + x^5 + \alpha x^4$. Pembagian dengan polinomial generator menghasilkan sisa $p(x) = \alpha^5 x^3 + \alpha^5 x^2 + \alpha^2 x + \alpha$. Maka, *codeword* akhir adalah $c(x) = \alpha^2 x^6 + x^5 + \alpha x^4 + \alpha^5 x^3 + \alpha^5 x^2 + \alpha^2 x + \alpha$ dengan representasi vektor $c = [\alpha, \alpha^2, \alpha^5, \alpha^5, \alpha, 1, \alpha^2]$

Proses decoding kode Reed–Solomon dimulai dengan menghitung sindrom dari vektor yang diterima $r(x) = c(x) + e(x)$, di mana polinomial *error* $e(x) = \alpha x + \alpha^4 x^2$. Dengan $t = 2$, diperoleh sindrom $S_1 = 1$, $S_2 = 1$, $S_3 = \alpha^6$, $S_4 = 0$. *Poyinomial locator* $\Lambda(x) = 1 + \Lambda_1 x + \Lambda_2 x^2$ ditentukan melalui sistem linier berbasis sindrom dan menghasilkan $\Lambda(x) = 1 + \alpha^4 x + \alpha^3 x^2$ Akar dari $\Lambda(X^{-1})$ memberikan dua lokasi *error*, yaitu α dan α^2.

Magnitudo kesalahan dihitung menggunakan sistem linier lain berdasarkan posisi *error* dan sindrom awal, menghasilkan $Y_1 = \alpha$ dan $Y_2 = \alpha^4$. Maka polinomial *error* yang terbentuk adalah $e(x) = \alpha x + \alpha^4 x^2$ Koreksi dilakukan dengan $c(x) = r(x) + e(x)$, sehingga *codeword* asli berhasil dipulihkan. Prosedur ini mengikuti pendekatan Peterson-Gorenstein-Zierler (PGZ) yang umum digunakan dalam decoding Reed-Solomon (Blahut, 2003).

Hasil penelitian menunjukkan bahwa struktur *Galois Field* dalam $GF(2)$ dan $GF(2^m)$ memungkinkan perumusan sistem pengkodean yang efisien melalui operasi linear dan polinomial. Matriks generator dan pemeriksa paritas dalam $GF(2)$ mencerminkan relasi kernel dan ruang dual kode, sementara pada Reed–Solomon, elemen $GF(2^m)$ memungkinkan koreksi kesalahan simbol sesuai dengan $d = 2t + 1$. Kendala yang dihadapi adalah kompleksitas notasi $GF(2^m)$ dan minimnya referensi lokal terkait decoding, sehingga sintesis teori dilakukan dengan rujukan utama dari Pless (1998), Blahut (2003), dan Lidl & Niederreiter (1994).

KESIMPULAN

Penelitian ini membahas penerapan struktur aljabar *Galois Field* dalam pengembangan sistem pengkodean koreksi kesalahan, khususnya pada kode linier dan kode siklik. Berdasarkan hasil kajian, dapat disimpulkan bahwa struktur $GF(2)$ menyediakan kerangka kerja yang efisien untuk membentuk kode linier melalui pemanfaatan matriks generator dan matriks cek paritas. Hubungan antara ruang kode dan kernel dari matriks cek paritas menunjukkan struktur aljabar yang kuat dalam mendeteksi dan mengoreksi *error* bit tunggal.

Lebih lanjut, representasi elemen $GF(2^m)$ sebagai polinomial memungkinkan pembentukan kode siklik seperti Reed–Solomon yang unggul dalam mengoreksi burst *error.* Dengan memanfaatkan sifat siklik dan operasi polinomial dalam *finite field*, sistem encoding dan decoding dapat dibangun secara efisien menggunakan metode berbasis sindrom. Studi kasus pada algoritma Reed–Solomon menunjukkan bagaimana *error locator* polinomial dan magnitudo *error* dapat digunakan untuk memulihkan codeword yang rusak.

Secara keseluruhan, struktur Galois *Field* memberikan dasar matematis yang kuat untuk membangun sistem komunikasi digital yang tangguh terhadap kesalahan. Hubungan antara konsep

abstrak aljabar dengan aplikasi nyata dalam pengodean memperkuat pentingnya pendekatan teoritis dalam pengembangan teknologi komunikasi.

REKOMENDASI

Penelitian ini menunjukkan bahwa struktur aljabar Galois Field memiliki peran penting dalam membentuk sistem pengodean yang efisien, namun kompleksitas matematisnya menjadi tantangan tersendiri dalam proses decoding, terutama pada kode siklik seperti Reed–Solomon. Oleh karena itu, disarankan agar penelitian selanjutnya mengeksplorasi pendekatan numerik, seperti simulasi Monte Carlo, untuk menguji dan mengoptimalkan performa algoritma decoding dalam kondisi kanal transmisi yang tidak ideal (Muchtarulloh *et al*., 2025).

Selain itu, integrasi teknologi berbasis kecerdasan buatan dalam konteks pendidikan matematika dapat dimanfaatkan untuk membantu visualisasi struktur Galois Field secara lebih interaktif. Pendekatan ini telah terbukti efektif dalam desain pembelajaran inovatif dan berpotensi mendukung pengembangan alat bantu belajar dalam teori pengodean (Shatila *et al*., 2025).

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Universitas Sebelas Maret (UNS) dan Program Studi Matematika FMIPA UNS atas dukungan dan fasilitas yang diberikan dalam pelaksanaan penelitian ini. Penulis juga menghargai masukan dari para *reviewer* yang telah membantu meningkatkan kualitas artikel ini.

DAFTAR PUSTAKA

Apriansyah, A., Fauziah, & Hayati, N. (2019*). Implementasi Algoritma Reed Solomon Codes pada Proses Encoding QR Code pada Sistem Absensi. Jurnal Infomedia*, 4(2).

Berlekamp, E. R. (1968). *Algebraic coding theory*. McGraw-Hill.

Lidl, Rudolf and Harald Neiderreiter. (1994). *Introduction to Finite field and Their Applications*. United Kingdom: Cambridge University Press.

Ling, S., and C. Xing. (2004). *Coding Theory*, Cambridge University Press, New York.

Muhtarulloh, F., Sari, A. F., & Huda, A. F. (2025). Estimasi Harga Opsi Saham melalui Simulasi Monte Carlo Menggunakan Model Volatilitas Stokastik Heston. *Teorema: Teori dan Riset Matematika*, 10(1), 1-10.

Blahut, R. E. (2003)**.** *Algebraic Codes for Data Transmission*. Cambridge: Cambridge University Press.

Pless, Vera. (1998) *Introduction to The Theory of Error Corecting Codes, Third Edition*. New York: John Wiley and Sons.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27, 379–423, 623–656.

Shatila, A. G., Buchori, A., & Purwosetiyono, F. X. D. (2025). Analisis Kebutuhan Desain Pembelajaran Inovatif Berbasis Media AI Untuk Meningkatkan Kemampuan Pemecahan Masalah. *Teorema: Teori dan Riset Matematika*, 10(1), 11-20.

Stallings, W.(2005). *Cryptography and Network Security, 4th ed*., Prentice Hall.