MATHEMATICAL SCIENCES AND APPLICATIONS JOURNAL

Volume 05, Number 02 | ISSN: 2986-4180

https://online-journal.unja.ac.id/msa

Article

Implementasi Aljabar Non-Asosiatif dalam pembentukkan Kode Linear Optimal pada Teori Koding

Nabila Nurmala Hasan, Sisilia Sylviani*

Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Sumedang, Jawa Barat 45363, Indonesia

*Corresponding author e-mail: sisilia.sylviani@unpad.ac.id

Article Info

Received July 2025

Accepted November 2025

Published November 2025

Keyword:

Loop algebra

Finite field

Lattice

Module theory

Coding theory

Abstract

This article will discuss a theorem referenced from B.T. Markov's 2012 article titled "МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ" (Mathematical Methods Of Cryptography). The theorem discussed provides a deep connection between non-associative algebraic structures, module theory, and optimal code construction in its application to coding theory. In this theorem, the loop algebra PL over the finite field $\mathbb{F}_q$ (where $q = p^n$ and p is a prime number) is analyzed through module decomposition and left lattice ideals, where the loop L with order $2q - 2$ contains a cyclic subgroup H with order $q - 1$ and each element in loop L\H satisfies three operational conditions that govern the interaction between cyclic subgroup H and loop L\H. The main result of this theorem is the construction of a code that provides optimal linear code parameters useful for detecting errors in available information. This shows that certain loop algebraic structures can produce optimal linear codes in their application to coding theory.

1. Pendahuluan

Saat ini, banyak sekali penelitian tentang pengaplikasian aljabar, grup, ring, maupun modul dalam penerapannya di suatu permasalahan nyata, seperti aljabar nonasosiatif (loop dan quasigroup) akan penerapannya dalam bidang kriptografi dan teori kode. Pada artikel ini, penulis melakukan kajian terkait dengan pengaplikasian aljabar loop di teori kode dalam menghasilkan kode linear optimal. Hal ini diperkenalkan oleh V.T. Markov, pada tahun 2012, dalam tulisannya yang berjudul "МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ" (Metode Matematika dalam Kriptografi)[1].

Sebelumnya, sudah banyak artikel yang membahas tentang penerapan struktur aljabar tertentu pada teori pengkodean atau kriptografi, seperti [2] sebagai artikel *Systematic Literatur Review* yang salah satunya membahas tentang penerapan modul di teori kode, [3] yang membahas pengkodean melalui *skew polinomial rings*, [4] mempelajari kode kesalahan dengan aljabar non asosiatif, [5] merepresentasikan Aljabar Lie pada Teori Koding, serta [6] Komputasi Aljabar dalam Teori Kode dan Kriptografi.

Selain itu, beberapa penelitian juga membahas tentang aljabar non asosiatif dengan struktur yang lebih fleksibel karena tidak memerlukan keasosiatifan dalam struktur aljabarnya, seperti pada [7]; lalu penerapan quasigroups pada [8] dan [9]; lapangan hingga pada [10], [11]; grup abelian [12],[13], [14]; serta aljabar loop [15],[16]; merupakan penerapan suatu struktur aljabar tertentu.

Pada artikel ini, penulis akan membahas kembali sebuah teorema di mana struktur aljabar loop tertentu dapat membuat kode linear optimal dalam teori koding dari artikel yang dirujuk. Bahwa ketika suatu struktur lapangan hingga yaitu aljabar loop yang terbatas yang memuat grup siklik tertentu akan menghasilkan kode linear yang optimal untuk diaplikasikan pada penggunaan di teori kode. Meskipun artikel ini dipublikasikan pada tahun 2012, namun belum ada artikel lain yang membahas terkait dengan teorema ini. Penulis berharap

https://doi.org/10.22437/msa.v5i2.46783

dengan adanya artikel ini dapat menambah wawasan pembaca dari sebuah teorema yang dirujuk dari artikel V.T. Markov.

2. Metode Penelitian

2.1. Grupoid

Definisi 2.1 [1] Grupoid merupakan struktur aljabar paling dasar, di mana merupakan himpunan tak kosong yang diberikan sebuah operasi biner. Grupoid adalah perumuman dari konsep grup karena tidak semua elemennya dapat dipetakan. Dengan *terminology* dari *Category theory*, grupoid adalah pemetaan dari himpunan G (yang kita sebut himpunan transisi) bersama dengan himpunan objek (yang disebut basis).

Misalkan diberikan $(G,*)$ merupakan grupoid dengan operasi biner, dan a merupakan anggota dari grupoid G. Didefinisikan pemetaan sebagai berikut:

$$L(a): G \to G, \quad R(a): G \to G$$

di mana fungsi pemetaannya adalah

$$xL(a) = x - a, \qquad xR(a) = a - x, \qquad \forall x \in G.$$

2.2. Grup Siklik, Modul

Definisi 2.2 [4] Misalkan grup G dengan operasi biner $*$, G dikatakan grup siklik jika $\exists a \in G \ni G = \{a^n | n \in \mathbb{Z}\} = \langle a \rangle$ di mana a disebut generator/pembangun.

Definisi 2.3 [17] Misalkan R ring satuan. Modul R atau modul atas R merupakan *additive* dari Grup Abelian (komutatif) M dengan aksi kiri $R \times M \to M$, didefinisikan dengan $(\lambda, x) \mapsto \lambda x$ sedemikian sehingga

(1) $\forall \lambda \in R$ berlaku $\lambda(x + y) = \lambda x + \lambda y, \forall x, y \in M$
(2) $\forall \lambda, \mu \in R$ berlaku $(\lambda + \mu)x = \lambda x + \mu x, \forall x \in M$
(3) $\forall \lambda, mu \in R$ berlaku $\lambda(\mu x) = (\lambda\mu)x, \forall x \in M$
(4) $\forall x \in M$ berlaku $1_R x = x$.

2.3. Kuasigrup

Definisi 2.4 [1][9] Misalkan $(\boldsymbol{G},*)$ merupakan grupoid, dikatakan kuasigrup jika pemetaan $\boldsymbol{L}(\boldsymbol{a})$ dan $\boldsymbol{R}(\boldsymbol{a})$ adalah bijeksi untuk $\boldsymbol{a} \in \boldsymbol{G}$ sebarang. Pemetaan bijeksi atau fungsi bijektif adalah fungsi yang memenuhi syarat injektif dan surjektif, di mana injektif memetakan elemen tepat ke satu elemen di kodomain, dan surjektif ketika setiap elemen di kodomain memiliki prapeta di domain.

Sebuah grupoid $\boldsymbol{G}$ disebut grupoid primitive dengan elemen pembagi jika terdapat dua operasi biner

$$\boldsymbol{l}: \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G} \text{ dan } \boldsymbol{r}: \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}$$

sedemikian sehingga

$$\boldsymbol{l}(\boldsymbol{a}, \boldsymbol{b}) \cdot \boldsymbol{a} = \boldsymbol{b} \text{ d an } \boldsymbol{a} \cdot \boldsymbol{r}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{b}$$

untuk semua $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{G}$. Sebuah grupoid primitif $\boldsymbol{G}$ dengan pembagian disebut kuasigrup jika persamaan $\boldsymbol{ax} = \boldsymbol{b}$ dan $\boldsymbol{ya} = \boldsymbol{b}$ memiliki solusi unik/tunggal.

2.4. Loop / Magnifier, Subloop

Definisi 2.5 [1] Suatu grupoid $(\boldsymbol{G},*)$ disebut $\boldsymbol{magnifier/loop}$ jika $(\boldsymbol{G},*)$ adalah grup semu/kuasigrup dengan elemen satuan/unit. Artinya, untuk setiap elemen $\boldsymbol{a}$ dari $\boldsymbol{loop}$ $(\boldsymbol{G},*)$ terdapat elemen $\boldsymbol{a^{\lambda}}$ dan $\boldsymbol{a^{\rho}}$ yang memenuhi kondisi $\boldsymbol{a^{\lambda}} \cdot \boldsymbol{a} = \boldsymbol{1}$ dan $\boldsymbol{a} \cdot \boldsymbol{a^{\rho}} = \boldsymbol{1}$. Dalam strukturnya, loop memenuhi syarat grup tetapi tidak bersifat asosiatif.

Berdasarkan [15] himpunan tak kosong L dengan operasi biner disebut loop jika memenuhi kondisi berikut:

1) $a * b \in L, \forall a, b \in L$
2) $\exists e \in L \ni a * e = e * a = a \; \forall a \in L$
3) $\forall (a, b) \in L \times L \; \exists (x, y) \in L \times L \ni a * x = b$ dan $y * a = b$.

Definisi 2.6 [15] Misalkan H himpunan tak kosong dan $H \subseteq L$. H disebut subloop dari L jika H adalah loop dengan operasi biner sama pada L.

2.5. Loop Moufang

Definisi 2.7 [1] Sebuah $loop$ $(L,\cdot)$ dengan elemen satuan 1 disebut $magnifier\ Moufang$/loop Moufang jika memenuhi identitas $(xy)(zx) = [x(yz)]x, \forall x, y, z \in L$. Teorema 1 menjelaskan sifat-sifat dari elemen di loop Moufang.

Teorema 1. Berikut merupakan identitas-identitas yang berlaku untuk semua elemen di loop Moufang

1) $y^{\lambda} = y^{\rho}$, sehingga berlaku $y^{\lambda} = y^{\rho} = y^{-1}$
2) $(xy)x = x(yx)$
3) $(xy)(zx) = x[(yz)x]$
4) $(xy)y^{-1} = x$
5) $[(yx)z]x = y[(x(zx)]$
6) $[(xz)x]y = x[z(xy)]$
7) $(xx)y = x(xy)$
8) $(xy)y = x(yy)$

Lemma 1. Misalkan $(L,\cdot)$ adalah suatu loop Moufang, maka untuk sembarang $x, y \in L$ berlaku

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Teorema 2. [12] Misalkan $(L,\cdot)$ adalah sebuah loop Moufang, jika untuk $x, y, z \in L$ memenuhi $x(yz) = (xy)z$, maka x, y, z membentuk sebuah subgrup di L.

Akibat 1. Setiap loop Mufang $(M,\cdot)$ adalah diasosiatif, yaitu setiap dua elemen membentuk subgrup di M.
Akibat 2. Setiap loop Moufang $(M,\cdot)$ adalah sebuah loop dengan tumpukkan/pangkat asosiatif.

Perhatikan bahwa sebuah kelas dari loop disebut **loop Paige**. Loop Paige didefinisikan oleh loop Moufang M yang non-asosiatif, terbatas, dan sederhana [1]. Misalkan $\mathbb{F}_q$ adalah sebuah lapangan hingga. Untuk $\alpha, \beta \in F_q^3$ didefinisikan operasi $\cdot$ dan $\times$ seperti berikut

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3$$
$$\alpha \times \beta = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1)$$

Aljabar Zorn $Z(q)$ adalah himpunan dari matriks $2 \times 2\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$, di mana $a, b \in \mathbb{F}_q$ dan $\alpha, \beta \in \mathbb{F}_q^3$ yang didefinisikan dengan operasi berikut:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha\delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}$$

Semua elemen $\mathbb{Z}(q)$ dengan determinan $M = ab - \alpha\beta = 1$ membentuk loop Paige $M^*(q)$ dengan elemen identitas/netral, yaitu $e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix}$. Sedemikian sehingga, didapat kesimpulan bahwa $|M^*(q)| = q^3(q^4 - 1)$ jika q genap, dan $|M^*(q)| = q^3(q^4 - 1)/2$ jika q ganjil.

Teorema 3. [1] Misalkan $S \subseteq Z$ himpunan order dari semua elemen magnifier $M^*(q)$ dan T adalah himpunan order dari elemen-elemen $L(q)$. Maka $S = T$ dan urutan elemen $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in M^*(q)$ bertepatan dengan urutan elemen $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in L_2(q)$pada $(\alpha, \beta) = (0,0)$ dengan urutan elemen $\begin{pmatrix} a & 1 \\ \alpha \cdot \beta & b \end{pmatrix} \in L_2(q)$ di mana $\alpha \neq 0$.

2.6. Elemen Primitif

Definisi 2.8 [18] Diketahui $\mathbb{F}_q^* = \mathbb{F}_q/\{0\}$ dan memenuhi kondisi berikut:

(i) Grup $\mathbb{F}_q^*$ merupakan grup siklik dengan orde $q - 1$ di bawah perkalian pada $\mathbb{F}_q$.

(ii) Jika γ adalah generator pada siklik grup tersebut, maka
$$\mathbb{F}_q = \{0, 1 = \gamma^0, \gamma, \gamma^2, \dots, \gamma^{q-2}\}$$
dan $\gamma^i = 1$ jika dan hanya jika $(q - 1)|i$ atau dapat dikatakan $q - 1$ habis membagi i.

Setiap generator γ di $\mathbb{F}_q^*$ disebut elemen primitif dari $\mathbb{F}_q$. Ketika elemen non-nol dari lapangan hingga $\mathbb{F}_q$ diekspresikan sebagai pangkat γ, maka perkalian dalam lapangan tersebut dapat dilakukan sesuai dengan aturan $\gamma^i\gamma^j = \gamma^{i+j} = \gamma^s$, di mana $0 \leq s \leq q - 2$ dan $i + j \equiv s \ (mod\ q - 1)$.

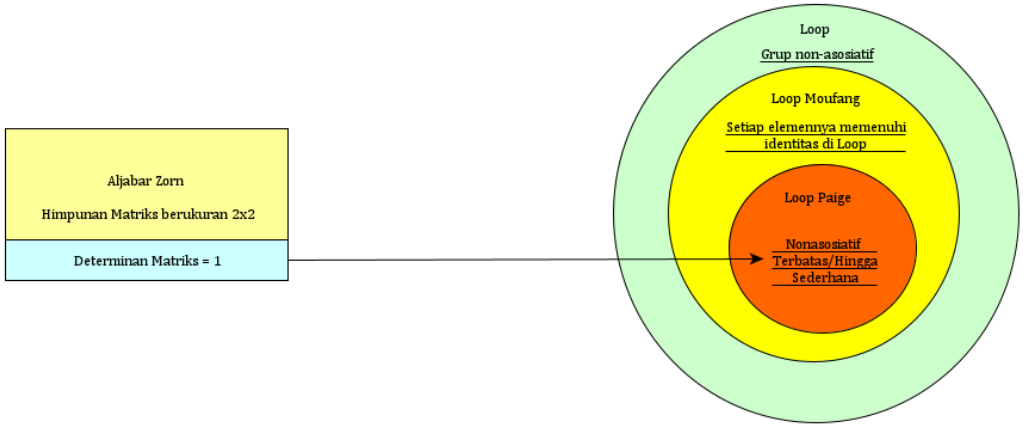
2.7. G-graded

Definisi 2.9 [1][19] Sebuah ring disebut $G - graded$ jika terdapat m sedemikian sehingga $\{R_\sigma : \sigma \in G\}$ dari subgrup-subgrup aditif (penjumlahan) R_σ dari grup aditif R sedemikian sehingga

$$R = \bigoplus_{\sigma \in G} R_\sigma, R_\sigma R_\tau \subseteq R_{\sigma\tau} \text{ untuk semua } \sigma, \tau \in G.$$

Lemma 2. Misalkan $R = \bigoplus_{\sigma \in G} R_\sigma - G$ adalah $G - grade$, kemudian

1) $1 \in R_e, R_e$ adalah subring dari ring R
2) Elemen invers r^{-1} terhadap elemen homogen yang dapat dibalik, maka r juga homogen.



Gambar 1. Ilustrasi Loop, Loop Moufang, Loop Paige, dan Aljabar Zorn.

Definisi 2.10 [20] $G - grade$ R merupakan grade ketat jika dan hanya jika $1 \in R_\sigma R_{\sigma^{-1}}$ untuk setiap $\sigma \in G$.

Akibat 3. Keserataan $R_e R_\sigma = R_\sigma R_e = R_\sigma$ yaitu R_σ adalah R_e bimodul adalah benar, dengan R adalah sebuah aljabar non-komutatif berdimensi terbatas/hingga atas lapangan F.

2.8. Basis Multiplikatif

Definisi 2.11 [1] Suatu basis multiplikatif dari aljabar berdimensi hingga R adalah basis B sedemikian sehingga $B \cup \{0\}$ tertutup terhadap perkalian.

3. Hasil dan Pembahasan

Pada bagian ini, akan diberikan pembuktian dari Teorema yang menunjukkan bahwa suatu struktur aljabar yang dikonstruksikan dapat menghasilkan kode linear yang optimal dalam pemakaiannya di Teori Koding yang dibuktikan oleh V.T. Markov, dkk [1]. Di mana akan dikonstruksikan berdasarkan struktur aljabar nonasosiatif dengan bentuk kode koreksi kesalahan pada Teori Koding, yang bersifat optimal, melalui struktur ideal kiri/modul dalam aljabar loop.

Teorema

Misalkan $P = \mathbb{F}_q$ dengan $q = p^n$. Misalkan L −aljabar loop orde $2q - 2$ yang memuat grup siklik abelian H dengan orde $q - 1$. Misalkan $\exists b \in L - H$ yang memiliki tiga kondisi berikut:

1) $\forall l \in L - H, \exists h_l \in H, \forall h \in H$ berlaku $lh = b(h_l h)$
2) $\forall l \in L - H, \exists s_l \in H, \forall h \in H$, berlaku $l(bh) = s_l h$
3) $\forall a \in H, \exists h_a \in H, \forall h \in H$ berlaku $a(bh) = h_a h$

Jika $char(P) \neq 2$ maka lattice dari ideal kiri aljabar loop PL dari L atas P yang memuat $\phi(q-1)$ struktur yang berbentuk:

$$\mathcal{L}_i \subseteq \mathcal{M}_i^-, \qquad \mathcal{M}_i^+ \subseteq \mathcal{N}_i$$

Di mana $i \in \{1, 2, \dots, q-1\}$ dan $\mathcal{C}(\mathcal{M}_i)$ merupakan kode linear optimal dengan parameter $[2q-5, 2q-3, 3]_q$. Selain itu, semua ideal yang muncul dalam struktur ini berpasangan berbeda. Jika $char(P) = 2$, maka lattice dari ideal kiri PL yang memuat $\phi(q-1)$ mengikuti kondisi berikut

$$\mathcal{L}_i \subseteq \mathcal{M}_i \subseteq \mathcal{N}_i$$

Di mana $\in \{1, 2, \dots, q-1\}$ dan $\mathcal{C}(\mathcal{M}_i)$ merupakan kode linear optimal $[2q-5, 2q-3, 3\}_q$. Selain itu, semua ideal yang muncul dalam struktur ini berpasangan berbeda.

Bukti:

Diketahui

1) Loop $L = H \cup bH$ di mana $H = \langle a \rangle_{q-1}$
2) Aljabar loop $\mathbb{F}_q L$ adalah ruang vector atas $\mathbb{F}_q$ dengan basis L
3) Ideal di $\mathbb{F}_q H$

Karena H siklik, $\mathbb{F}_q H \cong \mathbb{F}_q[x]/(x^{q-1} - 1)$. Idealnya berbentuk $\big(g(x)\big)$ dengan $g(x) \mid x^{q-1} - 1$.

Karena H grup siklik berorde $q-1$, koversi bentuk $H = \langle a \rangle_{q-1}$, sehingga $PH \cong \mathbb{F}_p[x]/(x^{q-1} - 1)$ dan semua ideal dari PH berbentuk $([g(x)])$, di mana $g(x) \mid x^{q-1} - 1$ ($x^{q-1} - 1$ merupakan faktor dari polinomial $g(x)$. Perlu diperhatikan bahwa $P^* = P/\{0\}$ dengan $|P^*| = q - 1$, maka bentuk polinomial $x^{q-1} - 1$ dapat diuraikan/difaktorkan dalam P menjadi (berbagai) pengali linear yang berbeda.

Berikut akan dianalisis terkait dimensi dan jarak sebagai atribut utama dalam koreksi kesalahan pada kode. Dimensi menentukan banyaknya informasi yang dapat dibawa dari sebuah kode. Sedangkan, jarak dihitung untuk mengetahui kemampuan kode dalam mendeteksi atau mengkoreksi kesalahan. Perhitungan dimensi dan jarak bertujuan untuk menunjukkan tingkat efisiensi dan kekuatan kode pada $\mathcal{C}(\mathcal{V}_i)$ dan $\mathcal{C}(\mathcal{W}_i)$. Untuk setiap primitif $\alpha_i \in P, i = 1, \dots, \varphi(q-1)$, kita mendefinisikan ideal $\mathcal{V}_i$ dan $\mathcal{W}_i$ yang dibentuk sebagai sebuah kode.

$$\begin{aligned} \mathcal{V}_i &= ([(x-1)(x-\alpha_i)])\rho \lhd PH, \mathcal{W}_i \\ &= ([(x-\alpha_i)]) \lhd PH \end{aligned} \qquad (1)$$

Sehingga $\dim(\mathcal{V}_i) = q - 1 - 2 = q - 3$, dan $\dim(\mathcal{W}_i) = q - 1 - 1 = q - 2$. Dapat diperoleh bahwa $d\big(\mathcal{C}(\mathcal{W}_i)\big) = 2$. Untuk menentukan jarak $\mathcal{C}(\mathcal{V}_i)$ perhatikan bahwa vektor v termasuk dalam $\mathcal{C}(\mathcal{V}_i)$ jika dan hanya jika

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha_i & \alpha_i^2 & \dots & \alpha_i^{q-2} \end{pmatrix} v = 0 \qquad (2)$$

Karena orde $\alpha_i = q - 1$, maka rank yang dijamin dari matriks verifikasi (2) adalah 2. Oleh karena itu, jarak minimumnya adalah $d\big(\mathcal{C}(\mathcal{V}_i)\big) = 3$. Dengan $\mathcal{V}_i$, $\mathcal{W}_i$, dan $b \in L \backslash H$ konstruksi bentuk sebagai berikut

$$\mathcal{L}_i = e\mathcal{V}_i + b\mathcal{V}_i, \ \mathcal{N}_i = e\mathcal{W}_i + b\mathcal{W}_i \qquad (3)$$

Sehingga dapat dibangun kode linear yang diperluas dari bentuk $\mathcal{V}_i$ dan $\mathcal{W}_i$, yang diberikan oleh persamaan (3). Berdasarkan sifat 1,2,3 pada teorema, dapat diverifikasi bahwa $\mathcal{L}_i$ dan $\mathcal{N}_i$ adalah ideal di PL. Oleh karena itu, karena $b \in L \backslash H$, maka $L = H \cup bH$, dan akibatnya $PL = PH + bPH$. Sehingga,

$$\dim(\mathcal{L}_i) = 2(q-3) = 2q-6$$
$$\dim(\mathcal{N}_i) = 2(q-2) = 2q-4$$
$$d\big(\mathcal{C}(\mathcal{L}_i)\big) = d\big(\mathcal{C}(\mathcal{V}_i)\big) = 3$$
$$d\big(\mathcal{C}(\mathcal{N}_i)\big) = d\big(\mathcal{C}(\mathcal{W}_i)\big) = 2.$$

Kita nyatakan bentuknya dengan

$$\sigma^+ = ev_i + bv_i$$
$$\sigma^- = ev_i - bv_i$$

di mana $v_i \in \mathcal{W}_i \backslash \mathcal{V}_i$ (jika $char\ P = 2$, maka $\sigma_i^+ = \sigma_i^-$), dan membangun $\mathcal{M}_i^+, \mathcal{M}_i^- \leq_P PL$ (jika $char\ P = 2$, maka $\mathcal{M}_i^+ = \mathcal{M}_i^- = \mathcal{M}$). Jadi dapat dikonstruksi

$$\mathcal{M}_i^+ = \mathcal{L}_i + P\sigma_i^+,\ \mathcal{M}_i^- = \mathcal{L}_i + P\sigma_i^- \qquad (4)$$

Dimensi $\mathcal{M}_i^{\pm}$ adalah $2q-5$ karena $\sigma_i^{\pm} \neq \mathcal{L}_i$. Oleh karena itu, karena $d(v_i, \mathcal{V}_i) \geq 2$, maka

$$d\big(\sigma_i^{\pm}, \mathcal{L}_i\big) \geq 4 > d\big(\mathcal{C}(\mathcal{L}_i)\big) = 3 \qquad (5)$$

Selanjutnya, kita membutuhkan pernyataan berikut untuk melengkapi pembuktian.

Lemma 1. Jika $v_i \in \mathcal{W}_i$, maka $(\alpha - e)v_i \in \mathcal{V}_i$ untuk setiap $\alpha \in H$

Bukti:
Vektor v_i berkorespondensi dengan $[v_i(x)] \in \mathbb{F}_q[x]/(x^{q-1}-1)$. ... $\alpha = a^k$, maka $(\alpha - e)$ berkorespondensi dengan $[x^k - 1]$. Perlu dicatat bahwa $\big[v_i(x)\big(x^k-1\big)\big] \in ([(x-1)(x-\alpha_i)]) = \mathcal{V}_i$ karena $(x-1)|\ \big(x^k-1\big)$.
Akan ditunjukkan bahwa $\mathcal{M}_i^+ \lhd PL$. Karena $\mathcal{L}_i \lhd PL$, maka cukuplah menunjukkan bahwa $\alpha\sigma_i^+ \in \mathcal{M}_i,\ l\sigma_i \in \mathcal{M}_i$ untuk semua $\alpha \in H, l \in L\backslash H$. Dengan lemma 1 dan sifat 3 kita peroleh dari kondisi

$$\alpha\sigma_i = \alpha(ev_i + bv_i) = \alpha v_i + b(h_\alpha v_i)$$
$$\alpha\sigma_i = (\alpha - e)v_i + ev_i + b\big((h_\alpha - e)v_i + ev_i\big)$$
$$\alpha\sigma_i = \sigma_i + (\alpha - e)v_i + b\big((h\alpha - e)v_i\big) \equiv \sigma_i\ (mod\ \mathcal{L}_i)$$

ketika mempertibangkan σ^-, kita memperoleh bahwa

$$\alpha\sigma_i^- \equiv \sigma_i^-(mod\ \mathcal{L}_i)$$
$$l\sigma_i^- \equiv -\sigma_i^-\ (mod\ \mathcal{L}_i)$$

dengan $\alpha \in H, l \in L\backslash H$.

Selanjutnya, akan ditunjukkan bahwa semua ideal $\mathcal{M}_i^{\pm}$ berbeda.

Misalkan $\mathcal{M}_i^+ + \mathcal{M}_i^- = \mathcal{N}_i$ dan $\mathcal{M}_i^{\pm} + \mathcal{M}_j^{\pm} \supseteq \mathcal{L}_i + \mathcal{L}_j = eS + bS$ di mana $S = (a-e) \lhd PH$, maka

$$\dim(S) = q-2$$

Dengan demikian, kita peroleh

$$dim(\mathcal{N}_i) = \dim\big(\mathcal{L}_i + \mathcal{L}_j\big) = 2q-4 > \dim\big(\mathcal{M}_i^{\pm}\big)$$

4. Kesimpulan

Teorema yang dibahas tidak hanya memberikan pemahaman tentang aljabar loop dan teori modul, tetapi juga memberikan metode secara eksplisit untuk membangun kode linear yang optimal dalam penerapannya di teori koding dengan parameter yang terukur. Perumuman teorema ini ke struktur non-asosiatif lain dan medan dengan karakteristrik yang berbeda, yang membuka peluang penelitian lanjutan. Keberlanjutan teorema ini menjangkau bidang teori pengkodean, kriptografi, dan aljabar komputasional. Potensi struktur kode seperti pada artikel ini dapat berguna untuk menentukan kecepatan dan efisiensi transmisi jaringan, ketahanan data yang haurs efisien dalam mengkoreksi kesalahan/*error* untuk mencegah kerusakan data, serta keamanan data.

Daftar Pustaka

1. V. T. Markov, A. V. Mikhalev, A. V. Gribov, P. A. Zolotykh, S. S. S. 2012. Quasigroups and rings in coding theory and cryptography. *Math-Net Ru*, (4), 31–52. Retrieved from https://www.mathnet.ru/php/getRefFromDB.phtml?jrnid=pdm&paperid=387&output=htm&option_lang=eng
2. Ludkowski, S. V. 2023. Nonassociative Algebras, Rings and Modules over Them. *Mathematics*, *11*(7). https://doi.org/10.3390/math11071714.
3. Boucher, D., & Ulmer, F. 2009. Coding with skew polynomial rings. *Journal of Symbolic Computation*, *44*(12), 1644–1656. https://doi.org/10.1016/j.jsc.2007.11.008.
4. Mendelsohn, A., & Ling, C. 2024. Learning with Errors from Nonassociative Algebras. *Cryptology {ePrint} Archive*, 2024/2058. Retrieved from https://eprint.iacr.org/2024/2058
5. Xu, X. 2012. Representations of Lie algebras and coding theory. *Journal of Lie Theory*, *22*(3), 647–682.
6. Reprint, S. I. 2024. *Computational Algebra , Coding Theory and Cryptography*. (H. Bordbar, Ed.). Switzerland: axioms. Retrieved from mdpi.com/journal/axioms
7. Schafer, R. D. 2008. An Introduction to Nonassociative Algebras. *The National Science Foundation*. Retrieved from https://www.gutenberg.org/ebooks/25156
8. Güneri, C., Özbudak, F., Özkaya, B., Saçıkara, E., Sepasdar, Z., & Solé, P. 2017. Structure and performance of generalized quasi-cyclic codes.

Finite Fields and their Applications, *47*, 183–202. https://doi.org/10.1016/j.ffa.2017.06.005.
9. Chiriac, L., & Bobeica, N. 2023. Reprint of: On topological quasigroups and multiple identities. *Topology and its Applications*. https://doi.org/10.1016/j.topol.2023.108759.
10. Ciaglia, F. M., Di Cosmo, F., Facchi, P., Ibort, A., Konderak, A., & Marmo, G. 2023. Groupoid and algebra of the infinite quantum spin chain. *Journal of Geometry and Physics*. https://doi.org/10.1016/j.geomphys.2023.104901.
11. Pumpluen, S. 2025. Using Cyclic (f, σ)-Codes Over Finite Chain Rings To Construct Zp- And Fq[[t]]-Lattices, 1–22. Retrieved from http://arxiv.org/abs/2501.10838
12. Drápal, A., & Vojtěchovský, P. 2023. Abelian congruences and solvability in Moufang loops. *Journal of Algebra*. https://doi.org/10.1016/j.jalgebra.2023.03.001.
13. Johnson, B. P. 2012. Commutative Rings Graded by Abelian Groups. *DigitalCommons @ University of Nebraska - Lincoln*.
14. Baer, R. 1940. Abelian groups that are direct summands of every containing abelian group. *Bulletin of the American Mathematical Society*, *46*(10), 800–806. https://doi.org/10.1090/S0002-9904-1940-07306-9.
15. Muzakki, A. 2013. Loop dan Loop Smarandache Beserta Sifat-sifatnya. *MATHunesa*, *3*(2).
16. Hartwig, B., & Terwilliger, P. 2007. The Tetrahedron algebra, the Onsager algebra, and the sl2 loop algebra. *Journal of Algebra*, *308*(2), 840–863. https://doi.org/10.1016/j.jalgebra.2006.09.011.
17. Martasari, S., Made Arnawa, I., & Noliza Bakar, N. 2020. Sifat-Sifat Modul Noetherian. *Jurnal Matematika UNAND*, *9*(2), 121–129. https://doi.org/10.25077/jmu.9.2.121-129.2020.
18. Huffman, W. C., & Pless, V. 2003. *Fundamentals of Error-Correcting Codes*. *Fundamentals of Error-Correcting Codes*. https://doi.org/10.1017/cbo9780511807077.
19. Perling, M., & Kumar, S. D. 2007. Primary decomposition over rings graded by finitely generated Abelian groups. *Journal of Algebra*, *318*(2), 553–561. https://doi.org/10.1016/j.jalgebra.2007.06.032.
20. Eagon, J., Miller, E., & Ordog, E. 2019. Minimal resolutions of monomial ideals. *Journal of Pure and Applied Algebra*, *229*(3), 107901. https://doi.org/10.1016/j.jpaa.2025.107901.