KODE *SELF-DUAL* SIKLIK ATAS RING RANTAI BERHINGGA

Juli Loisiana Butar-Butar
Dosen Fakultas Keguruan dan Ilmu Pengetahuan (FKIP), Universitas Quality Berastagi
Email **:** julois.butrz@gmail.com

Abstrak

Kode siklik *self-dual* adalah kode siklik dimana dualnya sama dengan kode siklik tersebut. Pada penelitian ini akan dibahas syarat perlu dan cukup untuk eksistensi non-trivial dari kode siklik *self-dual* atas ring rantai berhingga. Dengan syarat perlu dan cukup ini, disusun algoritma tentang kontruksi kode siklik *self-dual* atas ring rantai berhingga dengan panjang n. Faktorisasi polinomial $x^n - 1$ atas lapangan hingga $\mathbb{F}_q$ diperlukan dalam tahapan algoritma ini. Hal ini karena setiap pembangun kode siklik *self-dual* atas ring rantai berhingga berkoresponden dengan suatu ideal dari ring hingga ring $\mathbb{F}_q[x]/(x^n - 1)$ yang merupakan faktorisasi dari $x^n - 1$ atas lapangan hingga $\mathbb{F}_q$.

Kata kunci: Kode siklik *self-dual*, ring rantai berhingga

Abstract

The self-dual cyclic code is a cyclic code where its dual is the same as the cyclic code. This paper will discuss the necessary and sufficient conditions for the non-trivial existence a self-dual cyclic code over a finite chain ring. With this necessary and sufficient conditions, an algorithm is constructed about the construction of a self-dual cyclic code over a finite chain ring with length n. The polynomial factorization $x^n - 1$ over finite field $\mathbb{F}_q$ is required in this algorithm steps. This is because each generator element of cyclic self-dual code over finite chain ring corresponds to an ideal from ring to ring $\mathbb{F}_q[x]/(x^n - 1)$ which is a factorization from $x^n - 1$ over finite field to $\mathbb{F}_q$.

Keywords: Self-Dual Cyclic Code, Finite Chain Ring.

Pendahaluan

Sudah cukup umum pembahasan mengenai kode siklik adalah atas lapangan hingga $\mathbb{F}_q = \mathbb{F}_{p^k}$ dengan bilangan prima p karateristik lapangan dan $k \in \mathbb{N}$. Kode atas ring rantai merupakan generalisasi dari kode atas lapangan (Batoul, Guenda, & Gulliver, 2014). Suatu ring dikatakan ring rantai jika semua idealnya membentuk suatu rantai secara inklusi. Ring rantai berhingga merupakan ring lokal berhingga yang ideal maksimalnya merupakan ideal utama.

Dimisalkan C adalah kode linear. Elemen dari kode linear C adalah pasangan terurut n yang dinotasikan dengan $(c_1, c_2, \dots, c_n)$ dengan $c_i \in \mathbb{F}_q$ untuk $i = 1,2, \dots, n$. Kode linear C dikatakan kode siklik (*cyclic code*) jika untuk setiap $(c_1, c_2, \dots, c_n) \in C$, maka $(c_2, \dots, c_n, c_1) \in C$.

Struktur kombinasi kode siklik dengan panjang n dapat dikonversi menjadi suatu bentuk aljabar yang berhubungan dengan faktorisasi polinomial $x^n - 1$.

Kode siklik C atas lapangan hingga $\mathbb{F}_q$ mempunyai bentuk dual yang disimbolkan dengan $C^\perp$ dan didefinisikan sebagai

$$C^\perp = \{v \in R^n | [v, w] = 0, \forall\, w \in C\}.$$

Kode yang memenuhi $C = C^\perp$ disebut *self-dual*.

Adapun yang menjadi tujuan penelitia ini adalah mengkontruksi kode siklik *self-dual* non-trivial atas ring rantai berhingga. Hal

ini dimotivasi berdasarkan (Batoul, Guenda, & Gulliver, 2014) pada struktur kode *self-dual* atas ring dan memberikan syarat perlu dan cukup untuk eksistensi non-trivial dari kode siklik *self-dual* atas ring rantai hingga.

Motivasi yang lain yang mendasari kode siklik *self-dual* adalah karateristik dari bilangan bulat n yang mana $p^i \neq -1$ untuk semua i dan p adalah ganjil. Hal ini diperlukan untuk menentukan kode siklik *self-dual* non-trivial yang disebutkan oleh (Dinh & López-Permouth, 2004).

Seperti halnya, kode siklik yang berasosiasi dengan faktorisasi polynomial $x^n - 1$, demikian juga halnya dengan kode siklik *self-dual*. Faktorisasi atas lapangan hingga $\mathbb{F}_p$ telah dibahas (Butar-butar & Sinuhaji, 2019). Faktorisasi ini menjadi salah satu langkah dalam algoritma mengkontruksi kode siklik *self-dual* non-trivial atas ring rantai berhingga.

Metode Penelitian

1. Ring Rantai Berhingga

Suatu ring komutatif dikatakan suatu ring rantai jika struktur dari semua idealnya membentuk suatu rantai (Liu & Liu, 2015). Ring R disebut ring lokal jika R memiliki ideal maksimal yang unik. Ring komutatif berhingga adalah ring rantai berhingga jika dan hanya jika itu adalah ring ideal utama lokal (Dinh & López-Permouth, 2004). Untuk kelas dari ring rantai komutatif berhingga, perhatikan kondisi ekuivalen berikut.

Proposisi 2.1.1. Untuk suatu ring komutatif berhingga R kondisi berikut ekuivalen:

i) R adalah ring lokal dan ideal maximal M dari R adalah utama;
ii) R adalah ring ideal utama lokal;
iii) R adalah ring rantai.

Bukti.

i) ⇒ ii). Andaikan I ideal dari R. Jika $I = R$, maka I dibangun oleh identitas 1. Jika $I \subsetneq R$, maka $I \subseteq M$. Karena R adalah ring lokal dan ideal maximal M dari R adalah utama, maka M dibangun oleh satu elemen, katakan $M = \langle a \rangle$. Oleh karenanya, $I = \langle a^k \rangle$ untuk $k \in \mathbb{Z}$. Dengan demikian, R adalah ring ideal utama lokal.

ii) ⇒ iii). Karena R adalah ring ideal utama lokal, maka R memiliki ideal maksimal $M = \langle a \rangle$, dan A, B adalah ideal sejati sejati R. Akibatnya, $A, B \subseteq M$, yang mana terdapat l, m sedemikan hingga $A = \langle a^l \rangle$, $B = \langle a^m \rangle$ dengan l, m lebih kecil atau sama dengan kenilpotenan dari a. Akibatnya, hanya berlaku salah satu $A \subseteq B$ atau $B \subseteq A$. Dengan demikian, R adalah ring rantai.

iii) ⇒ ii). Karena R adalah ring komutatif rantai berhingga, maka jelas bahwa R lokal. Selanjutnya untuk membuktikan ideal maksimal M dari R adalah utama, dengan pengandaian M dibangun lebih dari satu elemen. Dimisalkan b, c terdapat di elemen pembangun dari M dan $b \notin cR$, dan $c \in bR$. Akibatnya, $\langle b \rangle \nsubseteq \langle c \rangle$ dan $\langle c \rangle \nsubseteq \langle b \rangle$, kontradiksi dengan asumsi bahwa R adalah ring rantai. Dengan demikian, M adalah utama. ■

Untuk selanjutnya, dianggap R ring rantai komutatif berhingga dan akan memanfaatkan kondisi dari Proposisi 2.1.1 Dimisalkan a adalah pembangun dari ideal maksimal M sehingga a adalah nilpotent dan indeks kenilpotenannya $e \in \mathbb{Z}$. Ideal-ideal dari R berbentuk rantai

$$\langle 0 \rangle = \langle a^e \rangle \subsetneq \langle a^{e-1} \rangle \subsetneq \cdots \subsetneq \langle a \rangle \subsetneq \langle a^0 \rangle = R.$$

Diberikan $R[x]$ adalah ring dari semua polinomial atas ring R dengan intermedian x. Dimisalkan $\bar{R} = R/M$ dengan $\bar{}: R[x] \to \bar{R}[x]$ didefinisikan sebagai homomorfisma natural yang memetakan $r \mapsto r + M$ dan intermedian x ke x.

2. Struktur Kode Siklik atas Ring Rantai Hingga

Perlu diketahui bahwa dalam teori Ring dasar, $\mathbb{F}_p[x]/\langle x^n - 1 \rangle$ merupakan ring polinomial dengan setiap faktor tak tereduksi dari $x^n - 1$ merupakan pembangun dari ideal di $\mathbb{F}_p[x]/\langle x^n - 1 \rangle$. Karena setiap faktor tak tereduksi dari $x^n - 1$ merupakan pembangun dari ideal di $\mathbb{F}_{p^r}[x]/\langle x^n - 1 \rangle$, maka setiap faktor dari

$x^n - 1$ berkorespondesi dengan setiap unsur pembangun dari kode siklik C. Atau dengan kata lain, pembentukan himpunan kode siklik C dengan panjang kode n berhubungan dengan faktorisasi dari polinomial $x^n - 1$.

Dimisalkan R ring rantai hingga dengan ideal maksimal, dan menjadi nilpotensi a. Berdasarkan Proposisi 2.2 dari (Dinh & López-Permouth, 2004), terdapat bilangan prima p dan bilangan bulat l sedemikian hingga $|\bar{R}| = p^l$, $|R| = p^{lt}$, karateristik dari R dan $\bar{R}$ adalah perpangkatan dari p . Pada bagian ini, asumsikan $n \in \mathbb{N}$ yang tidak habis dibagi p sehingga n tidak habis dibagi karateristik dari lapangan residu $\bar{R}$ sehingga $x^n - 1$ polinomial *square-free* di $\bar{R}[x]$. Akibatnya, $x^n - 1$ mempunyai faktorisasi tunggal dan saling prima relatif di $R[x]$ Proposisi 2.7. dari (Dinh & López-Permouth, 2004).

Lebih lanjut, jika $f(x)$ adalah faktor dari $x^n - 1$, dinotasikan $\hat{f}(x) = \frac{x^n-1}{f(x)}$.

Teorema 2.2.1 Andaikan R adalah ring rantai berhingga dengan ideal maksimal $\langle a \rangle$, dan t adalah kenilpotenan dari a. Jika $x^n - 1 = f_1 f_2 \dots f_r$ adalah hasil kali dari faktor tak tereduksi yang saling prima relatif dari $x^n - 1$ di $R[x]$, maka sebarang ideal di $\frac{R[x]}{\langle x^n-1 \rangle}$ adalah jumlahan dari ideal-ideal berbentuk

$$\langle a^j \hat{f}_i + \langle x^n - 1 \rangle \rangle,$$

dimana $0 \le j \le t$, $1 \le i \le r$.

Bukti.

Berdasarkan Teorema Sisa Cina (CRT) diperoleh

$$\frac{R[x]}{\langle x^n - 1 \rangle} = \frac{R[x]}{\bigcap_{i=1}^{r} \langle f_i \rangle} \cong \bigoplus \sum_{i=1}^{r} \frac{R[x]}{\langle f_i \rangle}.$$

Dengan demikian, sebarang ideal I dari $\frac{R[x]}{\langle x^n-1 \rangle}$ adalah berbentuk $\bigoplus \sum_{i=1}^{r} I_i$, dimana I_i adalah ideal dari $\frac{R[x]}{\langle f_i \rangle}$. Berdasarkan Lemma 3.1 pada (Dinh & López-Permouth, 2004) untuk $1 \le i \le r$, $I_i = 0$ atau $I_i = \langle a^k \hat{f}_i + \langle x^n - 1 \rangle \rangle$ di $\frac{R[x]}{\langle x^n-1 \rangle}$. Akibatnya, I adalah penjumlahan dari ideal-ideal yang berbentuk $\langle a^k \hat{f}_i + \langle x^n - 1 \rangle \rangle$. ■

Untuk selanjutnya, untuk mempermudah penotasian, cukup hanya menulis $r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$ untuk untuk koset yang berkoresponden dengan $r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} + \langle x^n - 1 \rangle$ di $\frac{R[x]}{\langle x^n-1 \rangle}$.

3. Kode Siklik Dual

Kode *self-dual* atas ring dan lapangan adalah salah satu bagian yang paling penting dan banyak dipelajari teori pengkodean (Dougherty, Gildea, Taylor, & Tylyshchak, 2016). Pada bagian ini, hanya membahas kode *self-dual* siklik atas ring rantai berhingga dan kontruksi kode siklik *self-dual* atas ring rantai berhingga dibahas dalam (Dougherty S. T., 2010). Diberikan R adalah ring rantai berhingga dan dimisalkan M adalah ideal maksimal dari R. Karena R adalah utama, terdapat generator $\gamma \in R$ dari M . Sehingga γ nilpoten dengan indeks nilpotensi bilangan bulat e . Ideal R terbentuk seperti rantai berikut

$$\langle 0 \rangle = \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \cdots \subsetneq \langle \gamma \rangle \subsetneq R.$$

Karenanya nilradikal R adalah $\langle \gamma \rangle$, sehingga semua elemen dari $\langle \gamma \rangle$ adalah nilpotent. Karena itu elemen $\frac{R}{\langle \gamma \rangle}$ adalah unit. Karena $\langle \gamma \rangle$ ideal maksimal, maka ring residu $\frac{R}{\langle \gamma \rangle}$ adalah lapangan yang dinotasikan dengan K. Morfisma ring surjektif natural didefinisikan sebagai $(-)$ sebagai berikut

$$-: R \to K$$
$$a \mapsto \bar{a} = a (\mathrm{mod}\, \gamma)$$

Misalkan $|R|$ adalah nilai cardinal dari R, dan R^* adalah grup perkalian dari semua unit di R. Karena K lapangan dan ideal maksimal $\langle \gamma \rangle \subsetneq R$, maka karateristik K adalah bilangan prima p sehingga $|K| = q = p^r$ untuk suatu r bilangan bulat. Akibatnya,

$$\begin{aligned} |R| &= |K| \cdot |\langle \gamma \rangle| \\ &= |K| \cdot |K|^{e-1} \\ &= |K|^e \\ &= p^{er}. \end{aligned}$$

Suatu kode C dengan panjang n atas R adalah subset dari R . Kode C diasumsikan linear. Menggunakan

perkalian inner $[\boldsymbol{v},\boldsymbol{w}] = \sum v_i w_i$. Kode dual $C^{\perp}$ dari C didefiniskan sebagai

$$C^{\perp} = \{v \in R^n | [v,w] = 0, \forall\, w \in C\}.$$

Kode C dikatakan *self-dual* jika $C = C^{\perp}$.

Untuk polinomial $f(x)$ berderajat r dimisalkan $f^*(x)$ menunjukkan polinomial resiprokal $x^r f(x^{-1})$. Teorema berikut memberikan struktur dual dari kode siklik pada ring rantai berhingga.

Teorema 2.3.1 (Teorema Struktur Dual) Diberikan R ring rantai berhingga dengan karateristik p, ideal maksimal γ, dan indeks nilpoten e . Dimisalkan n bilangan bulat sehingga $\gcd(p,n) = 1$ dan $f_1 f_2 \cdots f_l$ adalah hasil kali faktorisasi tak tereduksi dari $x^n - 1$.

Jika $C = \langle \hat{F}_1, \gamma\hat{F}_2, \dots, \gamma^{e-1}\hat{F}_e \rangle$ dengan $\hat{F}_j = \frac{x^{n-1}}{F_j}$ untuk $0 < j \le e$ adalah kode siklik dengan panjang n atas ring R, maka $C^{\perp} = \langle \hat{F}_0^*, \gamma\hat{F}_e^*, \dots, \gamma^{e-1}\hat{F}_2^* \rangle$, dimana $F_0, F_1, \cdots, F_{e-1}$ adalah polinomial yang saling prima relatif yang membagi $x^n - 1$.

Bukti

Karena $|K| = \left|\frac{R}{\langle\gamma\rangle}\right| = p^r$ untuk suatu r bilangan bulat dan $|R| = p^{er}$, maka berdasarkan Proposisi 2.2 pada (Dinh & López-Permouth, 2004) diperoleh

$$\begin{aligned} |C| &= (|K|)^{\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}} \\ &= p^{r\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}}. \end{aligned}$$

Berdasarkan proposisi 2.11 pada (Dinh & López-Permouth, 2004) terdapat l dengan $l + er = ern$ sehingga

$$l + r\sum_{i=0}^{e-1}(e-i)\deg F_{i+1} = ern.$$

Oleh karenanya,

$$\begin{aligned} l &= ern - r\sum_{i=0}^{e-1}(e-i)\deg F_{i+1} \\ &= r\sum_{i=1}^{e} i \deg F_{i+1}. \end{aligned}$$

Dinotasikan $C^* = \langle \hat{F}_0^*, \gamma\hat{F}_e^*, \dots, \gamma^{e-1}\hat{F}_2^* \rangle$. Untuk $i,j \in \{0,1,\cdots,e-1\}$. Ada dua kemungkinan, yaitu $i + 1 = e - j + 1$ dan $i + 1 \neq e - j + 1$.

- Jika $i + 1 = e - j + 1$ atau $i = e - j$, maka $\left(\gamma^i \hat{F}_{i+1}\right)\left(\gamma^j \hat{F}_{e-j+1}^*\right)^* = 0$.
- Jika $i + 1 \neq e - j + 1$ atau $i \neq e - j$, maka

$$(x^n - 1) | \left(\gamma^i \hat{F}_{i+1}\right)\left(\gamma^j \hat{F}_{e-j+1}^*\right)^*.$$

Akibatnya, $\left(\gamma^i \hat{F}_{i+1}\right)\left(\gamma^j \hat{F}_{e-j+1}^*\right)^* = 0$ di $\frac{R[x]}{\langle x^n-1\rangle}$.

Karenanya, $C^* \subseteq C^{\perp}$.

Karena $\left|\langle \hat{F}_0^* \rangle\right| = (|K|)^{e\deg F_0}$ dan untuk $i = 1,2,\cdots,e-1$, diperoleh

$$\begin{aligned} \left|\gamma^j \hat{F}_{e-j+1}^*\right| &= \left(\frac{|R|}{|\langle\gamma^{e-i}\rangle|}\right)^{n-\deg \hat{F}_{e+1-i}^*} \\ &= \left(\frac{|K|^e}{|K|^i}\right)^{\deg \hat{F}_{e+1-i}^*} \\ &= (|K|)^{(e-i)\deg F_{e+1-i}}. \end{aligned}$$

Akibatnya,

$$\begin{aligned} |C^*| &= \left|\langle \hat{F}_0^* \rangle\right| \cdot \left|\langle \gamma\hat{F}_e^* \rangle\right| \cdots \left|\langle \gamma^{e-1}\hat{F}_2^* \rangle\right| \\ &= (|K|)^{e\deg F_0}(|K|)^{(e-1)\deg F_e} \\ &\quad \cdots (|K|)^{\deg F_2} \\ &= (|K|)^{\sum_{i=1}^{e} i \deg F_{i+1}} \\ &= (p^r)^{\sum_{i=1}^{e} i \deg F_{i+1}} \\ &= |C^{\perp}|. \end{aligned}$$

Karena $C^* \subseteq C^{\perp}$ dan $|C^*| = |C^{\perp}|$, maka $C^* = C^{\perp}$. ■

Sifat berikut ini memberikan kondisi yang memenuhi syarat perlu dan cukup untuk eksistensi dari kode *self-dual* siklik.

Teorema 2.3.2 Diberikan R ring rantai berhingga dengan ideal maksimal γ, indeks nilpoten e genap, dan lapangan residu K dimana $|R| = p^{er}$ dan $|K| = p^r$. Kode siklik *self-dual* non-trivial dengan panjang n atas R ada jika dan hanya jika $(p^r)^i \neq -1 (\mathrm{mod}\, n)$ untuk semua bilangan positif i.

Bukti.

Dimisalkan C_v dinotasikan sebagai koset siklotomik modulo n yang memuat v dan α adalah akar ke- n primitive dari unit. Misalkan $g(x)$ adalah faktor tak tereduksi dasar monik dari $x^n - 1$. Akibatnya, terdapat suatu koset siklotomik C_u sedemikan sehingga

$$g(x) = \prod_{i \in C_u} (x - \alpha^i)$$

sehingga

$$g^*(x) = \prod_{i \in C_u} \alpha^i \prod_{i \in C_{u-n}} \left(x - \alpha^i\right)$$

$$= u \prod_{i \in C_{u-n}} (x - \alpha^i)$$

dimana $u = \prod_{i \in C_u} \alpha^i$ adalah suatu elemen invertibel di R. Karenanya, berdasarkan Proposisi 4.3 pada (Batoul, Guenda, & Gulliver, 2014), kode siklik *self-dual* nontrivial dengan panjang n ada jika dan hanya jika terdapat faktor tak tereduksi dasar $f(x)$ dari $f(x)$ dari $x^n - 1$ sedemikian hingga $f(x)$, $f^*(x)$ tidak berasosiasi, jika dan hanya jika $C_u \neq C_{n-u}$ untuk semua kode siklotomik C_u, jika dan hanya jika $p^i \not\equiv -1 (\mathrm{mod}\, n)$ untuk semua i. ■

Berdasarkan (Chen, Ling, & Zhang, 2014), jika indeks nilpotensi e genap, maka kode siklik *self-dual* $\langle \prod_{i \in I} f_i^{\frac{e}{2}} \rangle$ disebut kode *self-dual* trivial.

Namun hasil berikut menyediakan kriteria sederhana untuk eksistensi dari kode siklik *self-dual* non-trivial.

Teorema 2.3.2 Diberikan R ring rantai berhingga dengan ideal maksimal γ, indeks nilpoten e genap, dan lapangan residu K dimana $|R| = p^{er}$ dan $|K| = p^r$. Kode siklik *self-dual* nontrivial dengan panjang n ganjil atas R ada jika dan hanya jika $ord_n(p^r)$ adalah ganjil.

Bukti

⇐) Dibuktikan dengan mengadaikan tidak terdapat kode siklik *self-dual* nontrivial. Karena tidak terdapat kode siklik *self-dual* nontrivial, maka berdasarkan Teorema 2.3.2 terdapat bilangan bulat i sedemikian hingga $(p^r)^i \equiv -1 \pmod{n}$. Akibatnya berdasarkan bagian (i) pada Lemma 4.5 pada (Batoul, Guenda, & Gulliver, 2014) diperoleh $ord_n(p^r)$ genap.

⇒) Karena terdapat kode siklik *self-dual* nontrivial, maka berdasarkan Teorema 4 tidak terdapat bilangan i sedemikian hingga $p^{ri} \equiv -1 \pmod{n}$. Akan ditunjukkan bahwa $ord_n(p^r)$ adalah ganjil dengan menggasumsikan kasus berikut.

(i) Jika n adalah prima ganjil, maka berdasarkan bagian (ii) Lemma 4.5 pada (Batoul, Guenda, & Gulliver, 2014) diperoleh $ord_n(p^r)$ adalah ganjil.

(ii) $n = q^\alpha$, asumsikan $ord_{q^\alpha}(p^r)$ adalah genap, pertama akan dibuktikan implikasi berikut

$ord_{q^\alpha}(p^r)$ adalah genap ⇒ $ord_q(p^r)$ adalah genap

Asumsikan $ord_{q^\alpha}(p^r)$ genap dan $ord_q(p^r)$ ganjil. Akibatnya terdapat $i > 0$ ganjil sedemikian hingga $p^{ri} \equiv 1 \pmod{q} \Leftrightarrow p^{ri} = 1 + kq$. Karena $(1 + kq)^{q^{\alpha-1}} \equiv 1 + kq^\alpha \pmod{q^{\alpha+1}}$, maka $p^{riq^{\alpha-1}} = (1 + kq)^{q^{\alpha-1}} \equiv 1 \pmod{q^\alpha}$. Oleh karenanya,

$p^{riq^{\alpha-1}} \equiv 1 \pmod{q^\alpha}$	(1)

Keadaan pada persamaan (1) terjadi hanya jika i ganjil dan $q^{\alpha-1}$ ganjil, maka $ord_{q^\alpha}(p^r)$ ganjil karena $iq^{\alpha-1}$ habis dibagi $ord_{q^\alpha}(p^r)$. Namun, hal ini kontradiksi dengan asumsi $ord_{q^\alpha}(p^r)$ genap. Dengan demikian, asumsi salah. Seharusnya, $ord_{q^\alpha}(p^r)$ ganjil.

(iii) Jika $n = p_1 p_2$ dengan $\gcd(p_1, p_2) = 1$, maka karena $ord_n(p) = \mathrm{lcm}\big(ord_{p_1}(p^r), ord_{p_2}(p^r)\big)$ genap, maka salah satu dari $ord_{p_1}(p^r)$ atau $ord_{p_2}(p^r)$ haruslah genap. Asumsikan $ord_{p_1}(p^r)$. Akibatnya, terdapat $1 \leq k \leq ord_{p_1}(p^r)$ sedemikian hingga $p^{rk} \equiv -1 \pmod{p_1}$. Akibatnya, $p^{rk}(n - p_2) \equiv -(n - p_2) \bmod n$ dengan $k \leq ord_{p_1}(p^r)$. Oleh karenanya, C_{n-p_2} dapat dibalikkan. Namun hal ini tidak mungkin berdasarkan Teorema 2.3.2.

(iv) Jika $n = p_1^{\alpha_1} p_2^{\alpha_2}$ dengan $\gcd(p_1, p_2) = 1$, maka karena

$ord_n(p^r) = \text{lcm}\left(ord_{p_1^{\alpha_1}}(p^r), ord_{p_2^{\alpha_2}}(p^r)\right)$. Jika $ord_{p_1^{\alpha_1}p_2^{\alpha_2}}(p^r)$ genap, maka salah satu dari $ord_{p_1^{\alpha_1}}(p^r)$ atau $ord_{p_2^{\alpha_2}}(p^r)$ haruslah genap. Seperti pada kasus (iii), hal ini tidak mungkin. ■

Berdasarkan sifat-sifat di atas kode siklik *self-dual* non-trivial atas ring rantai berhingga dapat dikontruksi. Kontruksi kode siklik *self-dual* non-trivial dapat dilihat dalam algoritma berikut.

Algoritma : kontruksi kode siklik *self-dual* non-trivial atas ring rantai berhingga

Input : n = panjang kode siklik *self-dual*

K = lapangan residu ring dari rantai berhingga dengan karateritik prima p sehingga $|K| = p^r$ untuk r bilangan bulat atau $K = \mathbb{F}_{p^r}$.

Output : C = kode siklik *self-dual*

1. Hitung $t = ord_n(p)$.
2. Jika t genap, maka tidak ada C kode siklik *self-dual*. Lanjut ke langkah 8.

   Jika tidak, maka C kode siklik *self-dual* ada. Lanjut ke langkah 3.
3. Faktorisasi polinomial $x^n - 1$ atas $\mathbb{F}_{p^r}$ ke bentuk perkalian polinomial tak tereduksi dasar atas $\mathbb{F}_{p^r}$ sehingga $x^n - 1 = f_1(x)f_2(x)\cdots f_l(x)$.
4. Cari beberapa f_j^* dari f_j untuk $j \in \{1,2,\cdots,l\}$.
5. Jika $f_j^* = f_i$ untuk $i \in \{1,2,\cdots,l\}\backslash\{j\}$, maka f_j tidak *self* resiprokal.
6. Bentuk $g = \prod_{\substack{m=1 \\ m\neq j}}^{l} f_m$.
7. Bentuk kode siklik *self-dual* $C = \{f_j^* g, tf_j f_j^*\}$.
8. Selesai.

Proses kontruksi ini bertujuan untuk mengetahui eksitensi kode siklik *self-dual* dan unsur pembangunnya. Untuk lebih jelas perhatikan beberapa contoh kode siklik *self-dual* non-trivial.

Contoh 1. Kode siklik dengan panjang 13 atas $\mathbb{F}_9$.

Diperoleh $t = ord_{13}(3) = 3$ adalah ganjil. Faktorisasi $x^{13} - 1$ atas $\mathbb{F}_9$ adalah

$$x^{13} - 1 = (x-1)(x^3 + 6x^2 + 2x + 8)(x^3 + 7x^2 + 3x + 8)(x^3 + 4x^2 + 7x + 8)(x^3 + 2x^2 + 7x + 8).$$

Misalkan $f(x) = (x^3 + 6x^2 + 2x + 8)$ sehingga diperoleh

$$\begin{aligned} f^*(x) &= x^3 f(x^{-1}) \\ &= x^3(x^{-3} + 6x^{-2} + 2x^{-1} + 8) \\ &= 1 + 6x + 2x^2 + 8x^3 \\ &= -(x^3 + 7x^2 + 3x + 8). \end{aligned}$$

Misalkan $g(x) = -(x-1)(x^3 + 4x^2 + 7x + 8)(x^3 + 2x^2 + 7x + 8)$ sehingga $x^{13} - 1 = f(x)f^*(x)g(x)$. Sehingga kode siklik *self-dual* adalah

$$\begin{aligned} C &= \langle f^* g, 3ff^* \rangle \\ &= \langle 17x^{10} + 8x^9 + 6x^8 + 24x^7 + 15x^6 + 20x^5 + 9x^4 + 4x^3 + x^2 + 7x + 14, \\ &\quad 24x^6 + 2x^4 + 15x^3 + 2x^2 + 24 \rangle \end{aligned}$$

atau dengan kode angka adalah

$$C = \left\langle \begin{bmatrix} 0 \\ 0 \\ 17 \\ 8 \\ 6 \\ 24 \\ 15 \\ 20 \\ 9 \\ 4 \\ 1 \\ 7 \\ 14 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 24 \\ 0 \\ 2 \\ 15 \\ 2 \\ 24 \end{bmatrix} \right\rangle.$$

Kedua vektor di atas merupakan unsur pembangun dari kode siklik *self-dual*.

Contoh 2. Kode siklik dengan panjang 6 atas $\mathbb{F}_{49}$.

Diperoleh $t = ord_6(7) = 1$ adalah ganjil. Faktorisasi $x^6 - 1$ atas $\mathbb{F}_{49}$ adalah

$$x^6 - 1 = (x-1)(x+18)(x-18)$$

$$(x+19)(x-19).$$

Untuk $f(x) = x - 18 = x + 31$ dengan $f^*(x) = -18(x-19) = 31(x+30) = 31x + 48$ sehingga

$$x^6 - 1 = g(x)f(x)f^*(x)$$

dengan

$$g(x) = -18(x-1)(x+18)(x+19)$$
$$= 31(x+48)(x+18)(x+19).$$

Sehingga kode siklik *self-dual* adalah

$$C = \langle f^*g, 7ff^* \rangle$$
$$= \langle 31x^4 + 19x^3 + 18x + 30, 31x^2 + 29x + 18 \rangle$$

atau dengan kode angka adalah

$$C = \left\langle \begin{bmatrix} 0 \\ 0 \\ 31 \\ 19 \\ 18 \\ 30 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 31 \\ 29 \\ 18 \end{bmatrix} \right\rangle.$$

Kedua vektor di atas merupakan unsur pembangun dari kode siklik *self-dual*.

Kesimpulan

Kode siklik atas ring rantai berhingga dengan lapangan residu merupakan lapangan hingga $\mathbb{F}_{p^k}$ dapat diperoleh dari faktorisasi polinomial $x^n - 1$ dengan n adalah panjang kode siklik. Dengan adanya syarat perlu dan syarat cukup dari kode siklik *self-dual* sehingga dapat diketahui eksistensinya. kode siklik *self-dual*. Proses kontruksi kode siklik *self-dual* non-trivial atas ring rantai berhingga untuk mencari unsur pembangun kode siklik *self-dual*.

Daftar Pustaka

Batoul, A., Guenda, K., & Gulliver, T. (2014). On self-dual cyclic codes over finite chain rings. *Designs, codes and cryptography*, *70*(3), 347-358.

Butar-butar, J. L., & Sinuhaji, F. (2019). . Faktorisasi Polinomial Square-Free dan bukan Square-Free atas Lapangan Hingga Zp. *Jurnal Teori dan Aplikasi Matematika (JTAM)*, *3*(2), 132-142.

Chen, B., Ling, S., & Zhang, G. (2014). Self-dual cyclic codes over finite chain rings. *arXiv preprint arXiv:1405.2602.*, 1-15.

Dinh, H., & López-Permouth, S. (2004). Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, *50*(8), 1728-1744.

Dougherty, S. T. (2010). Constructions of self-dual codes over finite commutative chain rings. *IJICoT*, *1*(2), 171-190.

Dougherty, S., Gildea, J., Taylor, R., & Tylyshchak, A. (2016). Constructions of self-dual and formally self-dual codes from group rings. *arXiv preprint arXiv:1604.07863.*, 1-20.

Jia, Y., Ling, S., & Xing, C. (2011). On self-dual cyclic codes over finite fields. *IEEE Transactions on Information Theory*, *57*(4), 2243-2251.

Liu, X., & Liu, H. (2015). LCD codes over finite chain rings. *Finite Fields and Their Applications*, *34*, 1-19.