BAREKENG: Jurnal Ilmu Matematika dan Terapan
June 2021 Vol. 15 No. 2 Page 231–240
P-ISSN: 1978-7227 E-ISSN: 2615-3017
: https://doi.org/10.30598/barekengvol15iss2pp231-240

KODE SIKLIK BERULANG DARI KODE LINEAR $\mathbb{F}_p$ ATAS LAPANGAN HINGGA $\mathbb{F}_{p^l}$ DENGAN l BILANGAN PRIMA TERTENTU

Repeated Cyclic Code of Linear Code $\mathbb{F}_p$ over Finite Field $\mathbb{F}_{p^l}$ with Fixed Prime l

Juli Loisiana Butar-Butar[1*], Yan Batara Putra Siringoringo[2]

[1,2] *Matematika, Fakultas MIPA, Universitas Quality Berastagi*
Sumatera Utara, 22153, Indonesia

Corresponding author e-mail: [1] julois.butrz@gmail.com*

Abstrak

Kode blok adalah skema penyandian yang menggunakan sistem kode-kode pada suatu lapangan hingga dengan panjang yang sama dan tetap. Kode blok linear atau lebih sering disebut kode linear atas suatu lapangan hingga merupakan himpunan kode-kode blok C dengan panjang n yang membentuk suatu subruang bagian atas lapangan hingga $\mathbb{F}_{p^k}$ dengan p adalah bilangan prima dan k bilangan bulat positif. Sedangkan kode linear C dikatakan kode siklik jika setiap elemennya diputar masih terdapat di himpunan kode linear C. Setiap kode blok di kode siklik mempunyai korespondensi dengan semua faktorisasi polinomial tak tereduksi dari polinmial $x^n - 1$. Umumnya, pembahasan mengenai kode siklik pada lapangan hingga hanya dibatasi oleh $\gcd(n, p) = 1$. Hal ini menyebabkan setiap faktor dari polinomial $x^n - 1$ adalah tunggal. Untuk $\gcd(n, p) \neq 1$, memunculkan suatu pendefinisian baru dari konsep kode siklik. Kode siklik ini disebut disebut kode siklik berulang *(repeated cyclic code)*. Penelitian ini mencakup sifat dan struktur ring dari kode linear atas ring rangkaian komutatif hingga, kontruksi kode siklik berulang, algoritma dari kontruksi kode siklik atas lapangan hingga $\mathbb{F}_{p^l}$ dengan l bilangan prima tertentu.

Kata Kunci : *Kode siklik berulang, kode siklik, dual kode siklik, lapangan hingga*

Abstract

Block code is an encoding scheme that uses a system of codes in a finite with same and fixed length. Linear block code or called linear code over a finite field until is a set of blocks code C with length n which forms a subspace over the finite field $\mathbb{F}_{p^k}$ where p is a prime number and k is a positive integer. The linear code C is said to be a cyclic code if each element is rotated there is still in the set linear code C. Each block code in the cyclic code has a correspondence with all irreducible factorization of $x^n - 1$. Generally, the discussion of cyclic codes in the finite field is only to $gcd(n, p) = 1$. This cause each factor of $x^n - 1$ is singular. For $gcd(n, p) \neq 1$, brings up to a new definition of the cyclic code concept. This cyclic code is called repeated cyclic code. This research involves the properties and structures of linear code over finite chain rings, construction of repeated cyclic code, the algorithm of construction of repeated cyclic code over finite field $\mathbb{F}_{p^l}$ with l is a fixed prime number.

Keywords: *Repeated cyclic code, cyclic code, dual cyclic code, finite field.*

Article info:

Submitted: 15th November 2020 *Accepted: 13rd April 2021*

How to cite this article:
J. L. Butar-Butar and Y. B. P. Siringoringo, "KODE SIKLIK BERULANG DARI KODE LINEAR $\mathbb{F}_p$ ATAS LAPANGAN HINGGA $\mathbb{F}_{p^l}$ DENGAN l BILANGAN PRIMA TERTENTU", *BAREKENG: J. Il. Mat. & Ter.*, vol. 15, no. 02, pp. 231-240, Jun. 2021.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Copyright © 2021 Juli Loisiana Butar-Butar, Yan Batara Putra Siringoringo

1. PENDAHULUAN

Teori Pengkodean sangat berguna dalam pengembangan ilmu informasi seperti dalam komputerisasi. Salah satu yang sangat sering digunakan adalah dalam sistem bilangan biner atau $\{0,1\}$ dengan operasi penjumlahan dan perkalian modulo 2 merupakan lapangan $\mathbb{F}_2$. Lebih umum, lapangan hingga dinotasikan dengan $\mathbb{F}_{p^k}$ dengan karateristik bilangan prima p dan $k \in \mathbb{Z}^+$. Batasan yang akan dibahas dalam penelitian ini adalah kode blok linear (*linear block codes*).

Kode Blok adalah skema penyandian yang menggunakan sistem kode-kode pada suatu lapangan hingga dengan panjang yang sama dan tetap. Kode blok linear atau lebih sering disebut kode linear atas suatu lapangan hingga merupakan himpunan kode-kode blok dengan panjang n yang membentuk suatu subruang bagian atas lapangan hingga. 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 merupakan elemen lapangan hingga untuk $i = 1,2, \dots, n$.

Kode linear C dikatakan kode siklik jika untuk setiap $(c_1, c_2, \dots, c_n) \in C$, maka $(c_2, c_3, \dots, c_n, c_1) \in C$. 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 $\mathbb{F}_{q^m}[x]/\langle x^n - 1\rangle$, 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 $x^n - 1$.

Umumnya pembahasan mengenai kode siklik pada lapangan hingga hanya dibatasi oleh $\gcd(n, p) = 1$. Hal ini menyebabkan setiap faktor dari polinomial $x^n - 1$ adalah tunggal. Untuk kasus lain $\gcd(n, p) \neq 1$, memunculkan suatu pendefinisian baru tentang kode siklik yang disebut kode siklik berulang [1]. Lebih lanjut, suatu kode siklik C atas $\mathbb{F}_{q^m}$ dengan panjang kode n disebut kode siklik berulang (*repeated cyclic code*) jika $\gcd(n, p) \neq 1$. Pembahasan tentang kode siklik berulang sangat erat kaitannya dengan faktorisasi berulang polinomial atas lapangan hingga yang telah dibahas di [2] dan [3]. Pembahasan mengenai kode siklik berulang inilah yang menjadi fokus utama penelitian ini.

Namun dalam [1] dibahas tentang kode siklik berulang kode linear $\mathbb{F}_q$ yang panjangnya $n = p^t n_0$ dengan $t \in \mathbb{Z}^+$ dan $\gcd(n_0, p) = 1$ atas lapangan hingga $\mathbb{F}_{q^m} = \mathbb{F}_{q^l}$ dimana l adalah bilangan prima tertentu dan $q = p^k$. Secara khusus, penelitian ini hanya untuk $k = 1$ atau dengan kata lain $q = p$.

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah studi literatur. Penelitian ini terlebih dahulu dibahas mengenai teori kode siklik atas lapangan hingga. Setelah itu, membahas tentang teori dasar dari kode linear atas ring rantai komutatif hingga yang dibahas berdasarkan [4] dan [5].

Hal yang selanjutnya akan dilakukan adalah menyelidiki sifat dan struktur dari ring $\mathcal{R}_n^{(q)}$ dan $\mathcal{R}_n^{(q^l)}$ yang terdapat dalam [4]. Kode siklik berulang atas ring rangkaian hingga juga dibahas dalam [6]. Dari sifat-sifat dan struktur kedua ring tersebut selanjutnya akan dikontruksi kode siklik berulang kode linear $\mathbb{F}_q$ atas lapangan hingga $\mathbb{F}_{q^l}$.

Dari kontruksi ini, penelitian akan mengambil kondisi khusus. Seperti yang telah dijelaskan di latar belakang, $\mathbb{F}_q$ adalah lapangan hingga dengan karateristik p dan $q = p^k$ dengan k bilangan bulat positif. Pada penelitian, peneliti akan mengambil menentukan $k = 1$ sehingga lapangan hingga yang digunakan adalah $\mathbb{F}_p$. Kontruksi dari kode siklik berulang $\mathcal{C}$ khusus yang diteliti adalah kode linear $\mathbb{F}_p$ atas lapangan hingga $\mathbb{F}_{p^l}$ dengan l adalah suatu bilangan prima tertentu.

Dari kontruksi ini akan dibuat dalam bentuk algoritma untuk mencari elemen pembangun dari kode siklik berulang $\mathcal{C}$ kode linear $\mathbb{F}_p$ atas lapangan hingga $\mathbb{F}_{p^l}$. Faktorisasi polinomial atas lapangan hingga $\mathbb{F}_p$ diperlukan dalam tahapan algoritma ini nantinya. Hal ini karena setiap kode siklik mempunyai suatu polinomial yang membangunnya sebagai suatu ideal dari ring hingga ring $\mathbb{F}_q[x]/(x^n - 1)$.

Selain faktorisasi polinomial $x^n - 1$ atas lapangan hingga, metode lain yang diperlukan dalam algoritma yang akan disusun adalah algoritma perluasan Euclid (*Extended Euclidean Algorithm*) [7] yang gunanya untuk mencari faktor pembagi terbesar antara dua polinomial dan koefisien dari identitas Bézout.

Selanjutnya, akan dikontruksi kode dual dari $\mathcal{C}$, yakni $\mathcal{C}^{\perp}$ dengan sifat yang diperlukan untuk kontruksi ini terdapat dalam [8]. Bagian akhir dari penelitian ini adalah memberikan contoh dari algoritma yang telah disusun dan perhitungan-perhitungan yang dilakukan dalam contoh menggunakan *software* Matlab 2013.

3. HASIL DAN PEMBAHASAN

Penulisan hasil dan Pembahasan dapat dipisahkan dalam sub yang berbeda atau dapat juga digabung menjadi satu sub. Rangkuman hasil yang disajikan dapat dalam bentuk grafik dan angka. Pada bagian hasil dan pembahasan harus bebas dari interpretasi ganda. Pembahasan harus menjawab masalah penelitian, mendukung dan mempertahankan jawaban dengan hasil, membandingkan dengan hasil penelitian yang relevan, nyatakan keterbatasan studi yang dilakukan dan temukan kebaharuan.

3.1 Kontruksi Kode Linear siklik $\mathbb{F}_q$ akar berulang atas $\mathbb{F}_{q^l}$

Sebelum membahas kontruksi dari kode linear berulang terlebih dahulu dibahas mengenai ring yang erat hubungannya dengan polinomial $x^n - 1$. Dibentuk ring $\mathcal{R}_n^{(q)} = \frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle} = \{a(x) + \langle x^n - 1\rangle | a(x) \in \mathbb{F}_q[x], a(x) = 0 \text{ atau } \deg\big(a(x)\big) < n\}$ dan $\mathcal{R}_n^{(q^l)} = \frac{\mathbb{F}_{q^l}[x]}{\langle x^n-1\rangle} = \{a(x) + \langle x^n - 1\rangle | a(x) \in \mathbb{F}_{q^l}[x], a(x) = 0 \text{ atau } \deg\big(a(x)\big) < n\}$ dengan $n = p^t n_0$ dengan $p \nmid n_0$ dan l suatu bilangan prima.

Teorema 1. *Diberikan polinomial* $u_i(X) = \big(a_i(X)\big)^{p^t}$ *dan* $v_i(X) = \big(b_i(X)\big)^{p^t}$ *adalah polinomial di* $\mathbb{F}_q[X]$ *dengan* $a_i(x), b_i(x) \in \mathbb{F}_q[x]$ *memenuhi* $1 = \left(a_i(x)\frac{X^{n_0}-1}{m_i(x)} + b_i(x)m_i(x)\right)^{p^t}$ *dan* $d_i = deg\big(m_i(x)\big)$. *Jika* $\mathcal{K}_i = \mathcal{R}_n^{(q)}\varepsilon_i(x) \trianglelefteq \mathcal{R}_n^{(q)}$ *dan* $\mathcal{I}_i = \mathcal{R}_n^{(q^l)}\varepsilon_i(x) \trianglelefteq \mathcal{R}_n^{(q^l)}$ *dimana* $\varepsilon_i(x) = u_i(x)\frac{x^n-1}{M_i(x)}$, *dan* $\pi_i = m_i(x)\varepsilon_i(x)$ *untuk* $0 \le i \le s$. *Pernyataan berikut berlaku.*

(i) $\mathcal{K}_i$ *adalah ring rantai berhingga dengan ideal maksimal tunggal* $\langle \pi_i\rangle = \mathcal{K}_i\pi_i$, *indeks kenilpotenan dari* π_i *adalah* p^t *dan* $\mathcal{K}_i/\langle \pi_i\rangle \cong \mathbb{F}_q[x]/\langle m_i(x)\rangle \cong \mathbb{F}_{q^{d_i}}$.

(ii) Jika $\mathcal{T}_i = \{\sum_{k=0}^{d_i-1} r_k x^k \varepsilon_i(x) | r_0, r_1, \cdots,, r_{d_i-1} \in \mathbb{F}_q\}$ *maka* $\mathcal{T}_i$ *adalah himpunan Teichmüller dari* $\mathcal{K}_i$, *dan* $|\mathcal{K}_i| = q^{p^t d_i}$.

(iii) Jika $\mathcal{K}_i$ *adalah suatu aljabar-*$\mathbb{F}_q$, *dan* $\{X^k\big(m_i(x)\big)^h\varepsilon_i(x) | k = 0,1,\cdots,d_i-1; h = 0,1,\cdots,p^t-1\}$ *adalah suatu basis-*$\mathbb{F}_q$ *dari* $\mathcal{K}_i$, *maka* $dim_{\mathbb{F}_q}(\mathcal{K}_i) = p^t d_i$.

Bukti.

Definisikan pemetaan $\varphi: \mathbb{F}_q[x] \to \mathcal{K}_i$ sebagai $\varphi\big(r(x)\big) = r(x)\varepsilon_i(x) + \langle x^n - 1\rangle$. Jelas bahwa φ merupakan homomorfisma ring surjektif dari $\mathbb{F}_q[x]$ ke $\mathcal{K}_i$. Ambil sebarang $g(x) \in Ker(\varphi)$ sehingga $\varphi\big(g(x)\big) = g(x)\varepsilon_i(x) + \langle x^n - 1\rangle = 0$ akibatnya $g(x)\varepsilon_i(x) = p(x)(x^n - 1)$ untuk suatu $p(x) \in \mathbb{F}_q[x]$. Karenanya, $g(x)u_i(x)\frac{x^n-1}{M_i(x)} = p(x)(x^n - 1)$ sehingga $g(x) = \frac{p(x)}{u_i(x)}M_i(x)$. Ini berarti, $g(x) \in \langle M_i(x)\rangle$ atau $Ker(\varphi) = \langle M_i(x)\rangle$. Dengan demikian, φ membentuk suatu isomorfisma ring $\bar{\varphi}$ dari $\mathbb{F}_q[x]/\langle M_i(x)\rangle$ ke $\mathcal{K}_i$ yang didefinisikan sebagai $\bar{\varphi}(r(x) + \langle M_i(x)\rangle) = r(x)\varepsilon_i(x)$ untuk setiap $r(x) \in \mathbb{F}_q[x]$. Notasikan $A = \mathbb{F}_q[x]/\langle M_i(x)\rangle$. Karena $M_i(x) = \big(m_i(x)\big)^{p^t}$ dan $m_i(x)$ tak tereduksi di $\mathbb{F}_q[x]$, maka berdasarkan Contoh 2.1 pada [1] , A merupakan ring rantai berhingga dengan ideal maksimal tunggal $\langle m_i(x)\rangle = Am_i(x)$ dan indeks kenilpotenan dari $m_i(x)$ atas ring A adalah p^t, dan himpunan Teichmüller didefinisikan sebagai

$$\mathcal{S}_i = \left\{\sum_{k=0}^{d_i-1} r_k x^k | r_0, r_1, \cdots, r_{d_i-1} \in \mathbb{F}_q\right\}. \quad (1)$$

Akibat hal ini dan isomorfisma ring $\bar{\varphi}$ konklusi pada (i) dan (ii) terbukti. Selanjutnya, (iii) terbukti berdasarkan (i) dan (ii). □

Selanjutnya, untuk menentukan kode siklik $C_i^{(q)}$ berdasarkan [1] memenuhi ketentuan:

1. untuk $0 \le i \le r$ dengan $m_i(x)$ berderajat 1, untuk setiap $m_i(x)$ atas $\mathbb{F}_{q^l}$ kode siklik memenuhi $C_{j_i}^{(q)} = C_{j_i}^{(q^l)}$, dan
2. untuk $r+1 \le i \le s$ dengan $m_i(x)$ berderajat lebih besar dari 1, dinotasikan $m_{i,\lambda}(x) = \prod_{k \in C_{j_i q^\lambda}^{(q^l)}} (x - \zeta^k)$ untuk $\lambda = 0,1,\cdots,l-1$ sehingga $m_i(x) = \prod_{\lambda=0}^{l-1} m_{i,\lambda}(x)$ diperoleh $C_{j_i}^{(q)} = C_{j_i}^{(q^l)} \cup C_{j_i q}^{(q^l)} \cup \cdots \cup C_{j_i q^{l-1}}^{(q^l)}$.

Kontruksi Kode Linear siklik $\mathbb{F}_q$ akar berulang atas $\mathbb{F}_{q^l}$ [9] dengan panjang n. Diidentifikasikan vektor $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_{q^l}^n$ dengan polinomial $a(x) = \sum_{k=0}^{n-1} a_k x^k \in \mathcal{R}_n^{(q^l)}$. $\mathcal{R}_n^{(q)} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ dengan $\langle x^n - 1\rangle$ adalah ideal dari $\mathbb{F}_q[x]$ yang dibangun $x^n - 1$, dan $\mathcal{R}_n^{(q^l)} = \mathbb{F}_{q^l}[x]/\langle x^n - 1\rangle$ dengan $\langle x^n - 1\rangle$ adalah ideal dari $\mathbb{F}_{q^l}[x]$ yang dibangun $x^n - 1$.

Teorema 2. *Diberikan $\emptyset \neq \mathcal{C} \subseteq \mathcal{R}_n^{(q^l)}$. Pernyataan berikut ekuivalen:*

(i) $\mathcal{C}$ adalah kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ dengan panjang n.

(ii) $\mathcal{C}$ adalah $\mathcal{R}_n^{(q)}$-submodul dari $\mathcal{R}_n^{(q^l)}$.

(iii) Terdapat suatu $\mathcal{K}_i$-submodul $\mathcal{C}_i$ dari $\mathcal{I}_i$ untuk setiap $0 \le i \le s$ sedemikian sehingga $\mathcal{C} = \bigoplus_{i=0}^{s} \mathcal{C}_i$.

Bukti.

(i) ⇒ (ii) Karena $\mathcal{C}$ adalah kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ dengan panjang n, maka identifikasi kode huruf $\boldsymbol{c} = c_0 c_1 \cdots c_{n-1} \in \mathcal{C}$ dengan polinomial $c(x) = \sum_{k=0}^{n-1} c_k x^k \in \mathcal{R}_n^{(q^l)}$. Perubahan siklik$c_{n-1} c_0 \cdots c_{n-2}$ diidentifikasi dengan polinomial $c(x)x$. Karena $\mathcal{C}$ siklik, jika $c(x) \in \mathcal{C}$, maka $c(x)x^k \in \mathcal{C}$ untuk setiap $k \in \mathbb{Z}^+ \cup \{0\}$. Karena $\mathcal{C}$ juga linear-$\mathbb{F}_q$, , jika $c(x) \in \mathcal{C}$, maka $c(x)f(x) \in \mathcal{C}$ untuk setiap polinomial $f(x) \in \mathcal{R}_n^{(q)}$. Akibatnya, kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ merupakan $\mathcal{R}_n^{(q)}$-submodul dari $\mathcal{R}_n^{(q^l)}$.

(ii) ⇒ (iii) Karena $\mathcal{C}$ adalah $\mathcal{R}_n^{(q)}$-submodul dari $\mathcal{R}_n^{(q^l)}$, maka untuk setiap $0 \le i \le s$ dimisalkan $\mathcal{C}_i = \mathcal{C} \cap \mathcal{I}_i$ sehingga $\mathcal{C} \supseteq \sum_{i=0}^{s} \mathcal{C}_i = \bigoplus_{i=0}^{s} \mathcal{C}_i$. Di lain pihak, untuk setiap $c(x) \in \mathcal{C}$ oleh $\mathcal{R}_n^{(q^l)} = \bigoplus_{i=0}^{s} \mathcal{I}_i$ terdapat $c_i(x) \in \mathcal{I}_i$ untuk $0 \le i \le s$ sedemikian sehingga $c(x) = \sum_{i=0}^{s} c_i\,(x)$ dimana $c_i(x) = \varepsilon_i(x) c_i(x)$ berdasarkan Lemma 3.2 pada pada bagian (iii). Dari hal ini dan Lemma 3.2 pada [1] oleh $\mathcal{C}$ adalah submodul-$\mathcal{R}_n^{(q)}$ dari $\mathcal{R}_n^{(q^l)}$ dan $\varepsilon_j \in \mathcal{R}_n^{(q)}$. Karena itu, $c_j(x) \in \mathcal{C} \cap \mathcal{I}_i = \mathcal{C}$ untuk semua $0 \le j \le s$ yang berakibat $\mathcal{C} \subseteq \bigoplus_{i=0}^{s} \mathcal{C}_i$. Dengan demikian, $\mathcal{C} = \bigoplus_{i=0}^{s} \mathcal{C}_i$. Berdasarkan Lemma 3.2 pada [1] pada bagian (iv), $\mathcal{K}_i = \mathcal{R}_n^{(q)} \varepsilon_i(x) = \langle \frac{x^n - 1}{M_i(x)} \rangle \trianglelefteq \mathcal{R}_n^{(q)}$ adalah subring dari $\mathcal{I}_i$. Karena $\mathcal{C}$ adalah submodul-$\mathcal{R}_n^{(q)}$ dari $\mathcal{R}_n^{(q^l)}$, $\mathcal{K}$ subring dari $\mathcal{R}_n^{(q)}$ dan $\mathcal{C}_i = \mathcal{C} \cap \mathcal{I}_i$, dapat dilihat $\mathcal{C}_i$ tertutup atas operasi penjumlahan dan perkalian oleh elemen $\mathcal{K}_i$. Karena itu, $\mathcal{C}_i$ adalah submodul-$\mathcal{K}_i$ dari $\mathcal{I}_i$.

(iii) ⇒ (i) Dimisalkan $0 \le i \le s$. Karena $\mathcal{C}_i$ adalah submodul-$\mathcal{K}_i$ dan $\mathbb{F}_q \subseteq \mathcal{K}_i$, maka $\mathcal{C}_i$ juga adalah subruang-$\mathbb{F}_q$ dari $\mathcal{R}_n^{(q^l)}$Berdasarkan Lemma 3.2 pada [1] pada bagian (iii) berlaku $\varepsilon_i(x) c_i(x)$ untuk setiap $c_i(x) \in \mathcal{C}_i$. Dari hal ini dan $x\varepsilon_i(x) \in \mathcal{K}_i$ disimpulkan bahwa $x c_i(x) = x\varepsilon_i(x) c_i(x) \in \mathcal{C}_i$. Akibatnya, $\mathcal{C}_i$ adalah kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ dengan panjang n. Oleh karena itu, $\bigoplus_{i=0}^{s} \mathcal{C}_i$ kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ dengan panjang n. □

Dengan notasi pada Lemma 1, $\mathcal{C} = \bigoplus_{i=0}^{s} \mathcal{C}_i$, dimana $\mathcal{C}_i = \mathcal{C} \cap \mathcal{I}_i$ untuk $0 \le i < s$, disebut dekomposisi bentuk kanonik dari siklik linear-$\mathbb{F}_q$ dari kode $\mathcal{C}$. Menggunakan dekomposisi bentuk kanonik ini, dapat dihitung dan dikontruksi siklik linear-$\mathbb{F}_q$ dari kode $\mathbb{F}_{q^l}$ dengan panjang n dari submodul-$\mathcal{K}_i$ dari $\mathcal{I}_i$ untuk $0 \le i \le s$.

3.2 Kode Dual dari Kode Siklik Linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$

Jika $\mathcal{C}$ adalah suatu kode siklik linear-$\mathbb{F}_q$ atas $\mathbb{F}_{q^l}$ dengan panjang n, kode dual didefinisikan sebagai

$$C^{\perp} = \left\{ v \in \mathbb{F}_{q^l}^n \middle| \langle c, v \rangle = 0, \forall\, c \in C \right\}. \quad (2)$$

Kode C dikatakan jika *self-orthogonal* $C \subseteq C^{\perp}$dan C dikatakan *self-dual* jika $C = C^{\perp}$. Kode *self-dual* atas ring rantai berhingga dibahas dalam [10].

Dimisalkan b adalah q atau q^l. Untuk sebarang $f(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathcal{R}_n^{(b)}$ dengan $a_i \in \mathbb{F}_b$ didefinisikan $\mu\big(f(x)\big) = \tilde{f}(x) = \sum_{i=0}^{n-1} a_i x^{n-i} = x^n f\left(\frac{1}{x}\right)$. Pemetaan μ adalah suatu homomorfisma ring atas $\mathcal{R}_n^{(b)}$ yang memenuhi $\mu^{-1} = \mu$ karena $\mu^2 = id$ dengan id adalah pemetaan identitas.

Setiap lapangan $\mathbb{F}_{p^l}$ dapat direpresentasikan dengan $\frac{\mathbb{F}_p}{\langle \phi(y) \rangle}$ [11]. Untuk mengkontruksi lapangan hingga $\mathbb{F}_{p^l}$ dari $\phi(y)$ suatu polinomial minimal dari ω berderajat l atas $\mathbb{F}_p$ dengan menggunakan aturan $\phi(\omega) = 0$ sehingga sifat setiap elemen $\mathbb{F}_{p^l} = \{a_0 + a_1\omega + \cdots + a_{l-1}\omega^{l-1} \big| a_0, a_1, \ldots, a_{l-1} \in \mathbb{F}_p\}$ dapat ditentukan.

Pada bagian berikut ini disusun algoritma kontruksi kode siklik berulang atas dari kode linear $\mathbb{F}_p$atas lapangan hingga $\mathbb{F}_{q^l}$ berdasarkan sifat-sifat dan contoh dari [1]. Namun pada algoritma berikut diasumsikan bahwa $p = q$.

Algoritma Kontruksi Kode Siklik Berulang dari Kode Linear $\mathbb{F}_p$ atas Lapangan Hingga $\mathbb{F}_{p^l}$ dengan l Bilangan Prima Tertentu

Input : p bilangan prima
n panjang kode siklik dengan $n = p^t n_0$ dimana $t \in \mathbb{Z}^+$, $\gcd(n_0, p) = 1$, dan $\gcd(n, p) \neq 1$
Output : $\mathcal{C}$ kode siklik berulang dari kode linear $\mathbb{F}_q$

Langkah 1 Faktorisasi $x^{n_0} - 1 = \prod_{i=0}^{s} m_i(x)$ [2], dimana $m_i(x)$ adalah polinomial $\mathbb{F}_p[X]$ untuk $i = 0,1,\cdots,s$.

Langkah 2 Tentukan $d_i = \deg\big(m_i(x)\big)$.

Langkah 3 Cari polinomial $\phi(y)$ berderajat l yang merupakan polinomial minimal dari ω atas $\mathbb{F}_p$ dan bentuk $\mathbb{F}_{p^l} = \frac{\mathbb{F}_p[Y]}{\langle \phi(Y) \rangle}$ dimana $\omega = y + \langle \phi(y) \rangle$.

Langkah 4 Cari $\gamma_0, \gamma_1, \cdots, \gamma_{l-1} \in \mathbb{F}_{q^l}$ sehingga $\frac{\phi(y)}{y-\omega} = \sum_{k=0}^{l-1} \gamma_k y^k$.

Langkah 5 Tentukan $\{\theta_0, \theta_1, \cdots, \theta_{l-1}\}$ $\mathbb{F}_q$-basis $\mathbb{F}_{q^l}$ dimana $\theta_j = \frac{\gamma_j}{\phi'(\omega)}$ untuk $j = 0,1,\cdots,l-1$.

Langkah 6 Notasikan ring $\mathcal{R}_n^{(p)} = \mathbb{F}_p[x]/\langle x^n - 1 \rangle$ dan $\mathcal{R}_n^{(p^l)} = \mathbb{F}_{p^l}[x]/\langle x^n - 1 \rangle$. Faktorisasi $x^n - 1 = (x^{n_0} - 1)^{p^t} = \prod_{i=0}^{s} M_i(x)$ dengan $M_i(x) = \big(m_i(x)\big)^{p^t}$ untuk $i = 0,1,\cdots,s$.

Langkah 7 Tentukan $u_i(x), v_i(x) \in \mathbb{F}_p[x]$ sehingga $u_i(x)\frac{x^n-1}{M_i(x)} + v_i(x)M_i(x) = 1$ dengan menggunakan Algoritma *Extended Euclidean* [7] untuk $i = 0,1,\cdots,s$.

Langkah 8 Tentukan $\varepsilon_i(x) = u_i \frac{x^n-1}{M_i(x)}$ untuk $i = 0,1,\cdots,s$.

Langkah 9 Bentuk ring rantai berhingga $\mathcal{K}_i = \mathcal{R}_n^{(p)}\varepsilon_i(x) \trianglelefteq \mathcal{R}_n^{(p)}$ dengan $\langle \pi_i \rangle$ ideal maksimal tunggal dari $\mathcal{K}_i$ dimana $\pi_i = m_i(x)\varepsilon_i(x)$ dengan indeks kenilpotenan π_i adalah p^t, dan $\mathcal{K}_i/\langle \pi_i \rangle \cong \mathbb{F}_q[x]/\langle m_i(x) \rangle = F_{q^{d_i}}$ untuk $i = 0,1,\cdots,s$ dengan ketentuan

- $\mathcal{K}_i = \varepsilon_i(x)\{\sum_{j=0}^{p^t-1} r_j(m_i(x))^j \ | r_j \in \mathbb{F}_p, j = 0,1,\cdots,p^t-1\}$ untuk i dengan $d_i = 1$
- $\mathcal{K}_i = \varepsilon_i(x)\{\sum_{h=0}^{p^t-1}\sum_{k=0}^{s} a_{k,h}x^k \ | a_{k,h} \in \mathbb{F}_p, k = 0,1,\cdots,d_i-1, h = 0,1,\cdots,p^t-1\}$ untuk i dengan $d_i > 1$.

Langkah 10 Faktorisasi polinomial $m_i(x)$ atas $\mathbb{F}_{p^l}$ untuk i dengan $d_i > 1$ sebagai $m_i(x) = \prod_{\lambda=0}^{l-1} m_{i,\lambda}(x)$ dengan $m_{i,\lambda}(x)$ polinomial tak tereduksi monik saling prima di $\mathbb{F}_{p^l}[X]$ dan $\deg\left(m_{i,\lambda}(x)\right) = \frac{d_i}{l}$ untuk semua $\lambda = 0,1,\cdots,l-1$.

Langkah 11 Hitung $M_{i,\lambda}(x) = \left(m_{i,\lambda}(x)\right)^{p^t}$ untuk derajat $m_{i,\lambda}(x)$ lebih besar dari 1 dan $\lambda = 0,1,\cdots,l-1$.

Langkah 12 Tentukan $u_{i,\lambda}(x), v_{i,\lambda}(x) \in \mathbb{F}_{p^l}[x]$ sehingga $u_{i,\lambda}(x)\frac{M_i(x)}{M_{i,\lambda}(x)} + v_{i,\lambda}(x)M_{i,\lambda}(x) = 1$ dengan menggunakan Algoritma *Extended Euclidean* [7] dimana $\deg\left(u_{i,\lambda}(x)\right) < p^t\frac{d_i}{l}$ untuk $i = 0,1,\cdots,s$.

Langkah 13 Tentukan $e_{i,\lambda}(x) = u_i(x)u_{i,\lambda}(x)\frac{x^n-1}{M_{i,\lambda}(x)}$ untuk i dengan $d_i > 1$ dan $\lambda = 0,1,\cdots,l-1$.

Langkah 14 Bentuk $\mathcal{I}_i = \mathcal{R}_n^{(p^l)}\varepsilon_i(x)$ sebagai modul bebas-$\mathcal{K}_i$ dengan basis-$\mathcal{K}_i$ adalah

- $\mathcal{B}_i = \{\varepsilon_i(x), \varepsilon_i(x)\omega, \cdots, \varepsilon_i(x)\omega^{l-1}\}$untuk i dengan $d_i = 1$.
- $\mathcal{B}_i = \{e_{i,0}(x), e_{i,1}(x), \cdots, e_{i,l-1}(x)\}$ untuk i dengan $d_i > 1$

Langkah 15 Bentuk dual dari basis-$\mathcal{K}_i$ adalah

- $\mathcal{B}_i^{\perp} = \{\varepsilon_{\mu(i)}(x)\theta_0, \varepsilon_{\mu(i)}(x)\theta_1, \cdots, \varepsilon_{\mu(i)}(x)\theta_{l-1}\}$ untuk i dengan $d_i = 1$, dan
- $\mathcal{B}_i^{\perp} = \left\{\tilde{e}_{i,0}(x), \tilde{e}_{i,1}(x), \cdots, \tilde{e}_{i,l-1}(x)\right\}$ untuk i dengan $d_i > 1$.

Langkah 16 Kode siklik linear-$\mathbb{F}_p$ dari kode $\mathcal{C}$ atas $\mathbb{F}_{p^l}$ dengan panjang n dan kode dualnya $\mathcal{C}^{\perp}$ adalah

$$\mathcal{C} = \sum_{i=0}^{p} \mathcal{K}_i\left(\mathcal{B}_i U_i^{tr}\right) \tag{3}$$

dan

$$\mathcal{C}^{\perp} = \sum_{i=0}^{p} \mathcal{K}_i(\mathcal{B}_i^{\perp} V_i^{tr}), \tag{4}$$

dimana $\mathcal{K}_i(\mathcal{B}_i U_i^{tr})$ dan $\mathcal{K}_i(\mathcal{B}_i^{\perp} V_i^{tr})$ adalah submodul-$\mathcal{K}_i$ dari $\mathcal{I}_i$ dibangun oleh masing –masing entri dari vektor-vektor $\mathcal{B}_i U_i^{tr}$ dan $\mathcal{B}_i^{\perp} V_i^{tr}$, dan (U_i, V_i) memenuhi kondisi $(G, G^{\perp})$ pada contoh 2.5 di [1]. **Selesai**.

Untuk lebih jelas memahami tahapan algoritma tersebut perhatikan contoh berikut.

Contoh 1.
Diberikan $p = 2, l = 2, n_0 = 9, n = 2n_0,$ dan $t = 1$. Tentukan kontruksi dari kode siklik berulang dan dualnya.

Penyelesaian:

Faktorisasi $f(x)$ atas $\mathbb{F}_2$ adalah $m_0(x) = x + 1,\ m_1(x) = x^2 + x + 1,\ m_2(x) = x^6 + x^3 + 1$ dengan $d_0 = 1, d_1 = 2, d_2 = 6$.

Dimisalkan $\phi(y) = y^2 + y + 1$ adalah polinomial minimal dari ω tak tereduksi atas $\mathbb{F}_2$ dan $\mathbb{F}_{2^2} = \frac{\mathbb{F}_2[y]}{\langle\phi(y)\rangle} = \{a + b\omega | a, b \in \mathbb{F}_2\} = \{[0], [1], [\omega], [\omega + 1]\}$ dimana $\omega = y + \langle\phi(y)\rangle$ memenuhi $\omega^2 = \omega + 1$. Karena ω akar dari $\phi(y)$, maka $\frac{\phi(y)}{y-\omega} = (\omega + 1) + y$, yang mengakibatkan $\gamma_0 = \omega + 1$ dan $\gamma_1 = 1$. Diperoleh bahwa $\phi'(\omega) = 1$, sehingga $\theta_0 = \frac{\gamma_0}{\phi'(\omega)} = \omega + 1$, $\theta_1 = \frac{\gamma_1}{\phi'(\omega)} = 1$.

Dinotasikan ring $\mathcal{R}_{18}^{(3)} = \mathbb{F}_3[x]/\langle x^{18} - 1\rangle$ dan $\mathcal{R}_{18}^{(2^2)} = \mathbb{F}_{2^2}[x]/\langle x^{18} - 1\rangle$ sehingga $x^{18} - 1 = \prod_{i=0}^{2} M_i(x)$ dengan $M_i(x) = \left(m_i(x)\right)^2$. Akibatnya, $M_0(x) = x^2 + 1,\ M_1(x) = x^4 + x^2 + 1,\ M_2(x) = x^{12} + x^6 + 1$ sehingga diperoleh:

$$\begin{aligned} k_0(x) &= \frac{x^{18}-1}{m_0(x)} \\ &= x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1, \\ k_1(x) &= \frac{x^{18} - 1}{m_1(x)} \\ &= x^{14} + x^{12} + x^8 + x^6 + x^2 + 1, \\ k_2(x) &= \frac{x^{18}-1}{m_2(x)} = x^6 + 1. \end{aligned}$$

Dengan menggunakan Algoritma *Extended Euclidean* untuk $k_i(x)$ dan $M_i(x)$ untuk $i = 0,1,2$ diperoleh

$$u_0(x) = 1,\ u_1(x) = x^2, \text{ dan } u_2(x) = x^6.$$

Selanjutnya, diperoleh $\varepsilon_i(x) = u_i(x)k_i(x)$ untuk $i = 0,1,2$

$$\varepsilon_0(x) = x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1,$$
$$\varepsilon_1(x) = x^{16} + x^{14} + x^{10} + x^8 + x^4 + x^2,$$
$$\varepsilon_2(x) = x^{12} + x^6.$$

Dibentuk ring rantai berhingga $\mathcal{K}_i = \mathcal{R}_{18}^{(2)}\varepsilon_i(x) \trianglelefteq \mathcal{R}_{18}^{(2)}$ dengan $\langle \pi_i \rangle$ ideal maksimal tunggal dari $\mathcal{K}_i$ dengan $\pi_i = m_i(x)\varepsilon_i(x)$.

$$\pi_0(x) = \sum_{i=0}^{17} x^i,$$
$$\pi_1(x) = x^{18} + x^{17} + x^{15} + x^{14} + x^{12} \quad x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + x^2,$$
$$\pi_2(x) = x^{18} + x^{15} + x^9 + x^6.$$

dengan indeks kenilpotenan π_i adalah 2 untuk $i = 0,1,2$ sehingga diperoleh

- $\mathcal{K}_0 = \varepsilon_0(x)\{a + b \cdot m_0(x) | a, b \in \mathbb{F}_2\}$
- $\mathcal{K}_i = \varepsilon_i(x)\{\sum_{k=0}^{2} a_k x^k + \left(\sum_{k=0}^{2} b_k x^k\right) m_i(x) | a_k, b_k \in \mathbb{F}_2, k = 0,1\}$ untuk $i = 1,2$.

Selanjutnya, faktorisasi m_1 dan m_2 atas $\mathbb{F}_{2^2}$ sehingga

$$m_1(x) = x^2 + x + 1 = (x + \omega)\big(x + (\omega + 1)\big) = m_{1,0}(x)m_{1,1}(x),$$
$$m_2(x) = x^6 + x^3 + 1 = (x^3 + \omega)\big(x^3 + (\omega + 1)\big) = m_{2,0}(x)m_{2,1}(x).$$

Selanjutnya, menghitung $M_{i,\lambda}(x) = \left(m_{i,\lambda}(x)\right)^2$ untuk $i = 1,2$ dan $\lambda = 0,1$ sehingga

$$M_{1,0}(x) = (x + \omega)^2 = x^2 + (\omega + 1),$$
$$M_{1,1}(x) = (x + (\omega + 1))^2 = x^2 + \omega,$$
$$M_{2,0}(x) = (x^3 + \omega)^2 = x^6 + (\omega + 1),$$
$$M_{2,1}(x) = (x^3 + (\omega + 1))^2 = x^6 + \omega.$$

Akibatnya, diperoleh

$$k_{1,0}(x) = \frac{M_1(x)}{M_{1,0}(x)} = \frac{x^4 + x^2 + 1}{x^2 + (\omega + 1)} = x^2 + \omega,$$
$$k_{1,1}(x) = \frac{M_1(x)}{M_{1,1}(x)} = \frac{x^4 + x^2 + 1}{x^2 + \omega} = x^2 + (\omega + 1),$$
$$k_{2,0}(x) = \frac{M_2(x)}{M_{2,0}(x)} = \frac{x^{12} + x^6 + 1}{x^6 + (\omega + 1)} = x^6 + \omega,$$
$$k_{2,1}(x) = \frac{M_2(x)}{M_{2,1}(x)} = \frac{x^{12} + x^6 + 1}{x^6 + \omega} = x^6 + (\omega + 1).$$

Selanjutnya, menentukan $u_{i,\lambda}(x) \in \mathbb{F}_{p^l}[x]$ dengan menggunakan Algoritma *Extended Euclidean* antara $k_{i,\lambda}$ dan $M_{i,\lambda}$ untuk $i = 1,2$ dan $\lambda = 0,1$ sehingga diperoleh

$$u_{1,0}(x) = 1, u_{1,1}(x) = 1, u_{2,1}(x) = 1, \text{ dan } u_{2,2}(x) = 1.$$

Akibatnya diperoleh $e_{i,\lambda}(x) = u_i(x)u_{i,\lambda}(x)\frac{x^{18}-1}{M_{i,\lambda}(x)}$ untuk $i = 1,2$ dan $\lambda = 0,1$

$$e_{1,0}(x) = \omega x + (\omega + 1)x^4 + x^6 + \omega x^8 + (\omega + 1)x^{10} + x^{12} + \omega x^{14} + (\omega + 1)x^{16} + x^{18},$$
$$e_{1,1}(x) = (\omega + 1)x + \omega x^4 + x^6 + (\omega + 1)x^8 + \omega x^{10} + x^{12}\ (\omega + 1)x^{14} + \omega x^{16} + x^{18},$$
$$e_{2,0}(x) = \omega x^6 + (\omega + 1)x^{12} + x^{18},$$
$$e_{2,1}(x) = (\omega+1)x^6 + \omega x^{12} + x^{18}.$$

Kemudian dibentuk $\mathcal{I}_i = \mathcal{R}_n^{(q^l)}\varepsilon_i(x)$ sebagai modul bebas-$\mathcal{K}_i$ dengan basis-$\mathcal{K}_i$ adalah

- $\mathcal{B}_0 = \{\varepsilon_0(x), \varepsilon_0(x)\omega\}$,
- $\mathcal{B}_1 = \{e_{1,0}(x), e_{1,1}(x)\}$, dan
- $\mathcal{B}_2 = \{e_{2,0}(x), e_{2,1}(x)\}$.

Karena $\varepsilon_{\mu(i)}(x) = \tilde{\varepsilon}_i(x) = \varepsilon_i(x)$ dan $\mu(i) = i$ untuk semua $i = 0,1,2$, dan ehingga bentuk dual dari basis-$\mathcal{K}_i$ adalah

- $\mathcal{B}_0^{\perp} = \{\varepsilon_0(x)\theta_0, \varepsilon_0(x)\theta_1\} = \{(\omega + 1)\varepsilon_0(x), \varepsilon_0(x)\}$

- $\mathcal{B}_i^{\perp} = \{\tilde{e}_{i,0}(x), \tilde{e}_{i,1}(x)\}$ untuk $i = 1,2$ dengan
  $\tilde{e}_{1,0}(x) = \omega x^{17} + (\omega+1)x^{14} + x^{12} + \omega x^{10} + (\omega+1)x^8 + x^6 + \omega x^4 + (\omega+1)x^2 + 1,$
  $\tilde{e}_{1,1}(x) = (\omega+1)x^{17} + \omega x^{14} + x^{12} + (\omega+1)x^{10} + \omega x^8 + x^6 + (\omega+1)x^4 + \omega x^2 + 1,$
  $\tilde{e}_{2,0}(x) = \omega x^{12} + (\omega+1)x^6 + 1,$
  $\tilde{e}_{2,1}(x) = (\omega+1)x^{12} + \omega x^6 + 1.$

Selanjutnya, kode linear-$\mathbb{F}_2$ siklik $\mathcal{C}$ dan dualnya $\mathcal{C}^{\perp}$ adalah

$$\mathcal{C} = \sum_{i=0}^{p} \mathcal{K}_i\left(\mathcal{B}_i U_i^{tr}\right) \text{ dan } \mathcal{C}^{\perp} = \sum_{i=0}^{p} \mathcal{K}_i(\mathcal{B}_i^{\perp} V_i^{tr})$$

(i) $U_i = (1, \alpha_i(x))$dan $V_i = (-\tilde{\alpha}_i(x), 1)$ dengan $\alpha_i(x) = \sum_{k=0}^{d_i-1} a_{0,k}\, x^k + \left(\sum_{k=0}^{d_i-1} a_{1,k}\right) m_i(x)$ dan

$\tilde{\alpha}_i(x) = \sum_{k=0}^{d_i-1} a_{0,k}\, x^{18-k} + \left(\sum_{k=1}^{d_i-1} a_{1,k} x^{18-k}\right) \tilde{m}_i(x)$, $a_{h,k} \in \mathbb{F}_2$, $h = 0,1$ dan $0 \le k \le d_i - 1$.

(ii) $U_i = \left(m_i(x), m_i(x)\beta_i(x)\right)$ dan $V_i = \begin{pmatrix} -\tilde{\beta}_i(x) & 1 \\ \tilde{m}_i(x) & 0 \end{pmatrix}$,

$\beta_i(x) = \sum_{k=0}^{d_i-1} a_k x^k$ dan $\tilde{\beta}_i(x) = a_0 + \sum_{k=1}^{d_i-1} a_k x^{18-k}$, $a_k \in \mathbb{F}_2$ dan $0 \le k \le d_i - 1$.

(iii) $U_i = (m_i(x)\beta_i(x), 1)$ dan $V_i = (1, -\tilde{m}_i(x)\tilde{\beta}_i(x))$, untuk $\beta_i(x)$ dan $\tilde{\beta}_i(x)$ sama dengan (ii).

(iv) $U_i = (0, m_i(x))$ dan $V_i = \begin{pmatrix} 1 & -\tilde{m}_i(x)\tilde{\beta}_i(x) \\ 0 & \tilde{m}_i(x) \end{pmatrix}$, untuk $\beta_i(x)$ dan $\tilde{\beta}_i(x)$ sama dengan (ii).

(v) $U_i = \begin{pmatrix} m_i(x) & 0 \\ 0 & m_i(x) \end{pmatrix}$ dan $V_i = \begin{pmatrix} \tilde{m}_i(x) & 0 \\ 0 & \tilde{m}_i(x) \end{pmatrix}$.

(vi) $U_i = \begin{pmatrix} 1 & \beta_i(x) \\ 0 & m_i(x) \end{pmatrix}$ dan $V_i = \left(-\tilde{m}_i(x)\tilde{\beta}_i(x), \tilde{m}_i(x)\right)$, untuk $\beta_i(x)$ dan $\tilde{\beta}_i(x)$ sama dengan (ii).

(vii) $U_i = \begin{pmatrix} \beta_i(x) & 1 \\ m_i(x) & 0 \end{pmatrix}$ dan $V_i = \left(\tilde{m}_i(x), -\tilde{m}_i(x)\tilde{\beta}_i(x)\right)$, untuk $\beta_i(x)$ dan $\tilde{\beta}_i(x)$ sama dengan (ii).

(viii) $U_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ dan $V_i = 0$, atau $U_i = 0$ dan $U_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. ■

Dengan menggunakan algoritma dapat ditentukan kontruksi dari kode siklik berulang $\mathcal{C}$ dan dualnya $\mathcal{C}^{\perp}$ atas lapangan hingga $\mathbb{F}_{p^l}$.

4. KESIMPULAN

Umumnya, kode siklik atas lapangan hingga $\mathbb{F}_q$ dengan panjang n dibatasi untuk $\gcd(n, q) = 1$. Dengan membuat aturan $\gcd(n, q) \neq 1$ membuat suatu pendefinisian baru untuk kode siklik berulang. Algoritma kontruksi kode siklik berulang dengan panjang n atas kode linear $\mathbb{F}_p$ atas lapangan hingga $\mathbb{F}_{p^l}$ disusun berdasarkan sifat-sifat dan struktur dari ring $\mathcal{R}_n^{(q)}$ dan $\mathcal{R}_n^{(q^l)}$ dengan mengambil kasus $q = p$ untuk $n = p^t n_0$, $p \nmid n_0$ dan l suatu bilangan prima. Saran selanjutnya, penelitian dikembangkan untuk kontruksi kode siklik berulang atas lapangan hingga $\mathbb{F}_q$ dengan $q \neq p$.

UCAPAN TERIMA KASIH

Penelitian ini didanai oleh DRPM Dikti skema Penelitian Dosen Pemula tahun pendanaan 2020 dengan nomor kontrak 256/LL1/PG/2020.

DAFTAR PUSTAKA

[1] Y. Cao and Y. Gao, "Repeated root cyclic F_q-linear codes over F_{q^l}.," *Journal Finite Fields and Their Applications*, vol. 31, p. 202–227., 2014.

[2] J. L. Butar-butar and F. Sinuhaji, ". Faktorisasi Polinomial Square-Free dan bukan Square-Free atas Lapangan Hingga Zp," *Jurnal Teori dan Aplikasi Matematika (JTAM)*, vol. 3, no. 2, pp. 132-142, 2019.

[3] J. L. Butar-butar and F. Sinuhaji, "Faktorisasi Polinomial dengan Gabungan Algoritma SFF dan Algoritma Berlekamp atas Lapangan Hingga," in *SiManTap: Seminar Nasional Matematika dan Terapan*, Pematangsiantar, 2019.

[4] A. Sălăgean, "Repeated-root cyclic and negacyclic codes over a finite chain ring," *Journal Discrete Applied Mathematics,* vol. 152, no. 2, pp. 413-419, 2006.

[5] X. Liu and H. Liu, "LCD codes over finite chain rings," *Finite Fields and Their Applications,* vol. 34, pp. 1-19, 2015.

[6] A. T. Fotue and C. Mouaha, "Contraction of cyclic codes over finite chain rings," *Journal Discrete Mathematics,* vol. 341, no. 6, pp. 1722-1731, 2018.

[7] A. Iliev and N. Kyurkchiev, "A Note on Euclidean and Extended Euclidean Algorithms for Greatest Common Divisor for Polynomials," *International Journal of Pure and Applied Mathematics,* vol. 118, no. 3, pp. 713-721., 2018.

[8] W. C. Huffman, "Cyclic F_q -linear F_{q^t} -codes," *Int. J. Inf. Coding Theory,* vol. 1, no. 3, pp. 249-284, 2010.

[9] W. C. 2. Huffman, " On the theory of F_q-linear F_(q^t)-codes," vol. 7, no. 3, p. 57–90, 2013.

[10] J. L. Butar-Butar, "Kode Self-Dual Siklik atas Ring Rantai Berhingga," *Jurnal Curere,* vol. 4, no. 1, pp. 60-66, 2020.

[11] J. Doliskani and É. Schost, "Taking roots over high extensions of finite fields," *Mathematics of Computation,* vol. 83, no. 285, pp. 435-446, 2014.