Contemporary Mathematics and Applications
Vol. 3, No. 2, 2021, pp. 71-79.

Polinomial Pembangun dari Ideal dan Dimensi dari Kode Siklik

Tuhfatul Janan[1], Mohammad Imam Utoyo[2] & Fatmawati[3]

[1]Sekolah Tinggi Agama Islam Muhammadiyah Probolinggo
[2,3]Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga

[1]Corresponding author: tuhfatuljanan4@gmail.com

Abstrak. Dalam penelitian ini, diberikan hubungan antara ideal dan kode siklik serta sifat-sifat polinomial pembangun dari ideal dan dimensi dari kode siklik. Sifat-sifat tersebut antara lain hubungan antara polinomial pembangun dari ideal dengan polinomial monik dengan derajat terkecil di ideal, eksistensi dan ketunggalan dari polinomial pembangun dari ideal, hubungan antara polinomial pembangun dari ideal dengan pembagi monik dari $x^n - 1$, dan hubungan antara derajat dari polinomial pembangun dari ideal dan dimensi dari kode siklik.

Kata kunci: *dimensi, ideal, kode siklik, polinomial pembangun*.

1 Pendahuluan

Teori pengkodean pertama kali ditemukan oleh Shannon pada tahun 1948 dalam jurnalnya yang berjudul "*A Mathematical Theory of Communication*" [4]. Teori pengkodean adalah ilmu yang mempelajari teknik dan metode transmisi data atau informasi melalui saluran komunikasi yang tidak bebas gangguan secara efisien dan akurat. Teori pengkodean telah berkembang begitu pesat dan memiliki aplikasi yang begitu luas, diantaranya minimalisasi gangguan dari perekaman CD, transfer data dari memori ke CPU komputer atau antar CPU komputer, transaksi ATM, dan komunikasi satelit [1]. Dalam perkembangannya, kode siklik pertama kali ditemukan oleh Prange pada tahun 1957 [3]. Kode siklik merupakan bahasan penting dari teori pengkodean karena menjadi dasar dari teori pengkodean modern, seperti kode Hamming, kode Golay, kode BCH, kode Reed-Solomon, dan kode Goppa [2].

2 Polinomial dan Ruang Vektor atas Lapangan

Definisi 2.1 Misalkan F adalah lapangan. Polinomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ dengan $a_i \in F$ dan $0 \leq i \leq n$ disebut polinomial atas F. Himpunan semua polinomial atas F dinotasikan dengan $F[x]$.

Definisi 2.2 Misalkan $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ adalah polinomial dengan $a_n \neq 0$. Bilangan bulat n disebut derajat dari $f(x)$ dan dinotasikan dengan $\deg(f(x))$.

Definisi 2.3 Polinomial $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ disebut monik jika $a_n = 1$.

Definisi 2.4 Misalkan $f(x) \in F[x]$ dengan $\deg(f(x)) \geq 1$. Himpunan sisa dari pembagian semua polinomial di $F[x]$ dengan $f(x)$ dinotasikan dengan $F[x]/f(x)$.

Definisi 2.5 Aturan penjumlahan dan perkalian untuk polinomial $g(x)$ dan $h(x) \in F[x]/f(x)$ didefinisikan sebagai berikut :

$$g(x) \oplus h(x) \coloneqq g(x) + h(x) \bmod f(x),$$
$$g(x) \odot h(x) \coloneqq g(x) \cdot h(x) \bmod f(x).$$

Untuk selanjutnya, penulisan tanda "$\oplus$" dan "$\odot$" secara berturut-turut disederhanakan menjadi "$+$" dan "$\cdot$".

Contoh 2.6 Misalkan $g(x) = x^2 + 1$, $h(x) = x^3 + 1 \in \mathbb{Z}_2[x]/(x^4 - 1)$, maka $g(x) + h(x) = x^3 + x^2$ dan $g(x) \cdot h(x) = x^3 + x^2 + x + 1$.

Definisi 2.7 Misalkan F_q adalah lapangan berhingga dengan q elemen. Ruang vektor $F_q^n \coloneqq \{(v_1, v_2, v_3, \dots, v_n)\ ;\ v_i \in F_q,\ 1 \leq i \leq n\}$ disebut ruang vektor dengan panjang n atas F_q. Untuk selanjutnya, penulisan vektor $\boldsymbol{v} = (v_1, v_2, v_3, \dots, v_n) \in F_q^n$ disederhanakan menjadi $\boldsymbol{v} = v_1 v_2 v_3 \dots v_n \in F_q^n$.

Contoh 2.8 $\mathbb{Z}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$ adalah ruang vektor dengan panjang 2 atas $\mathbb{Z}_2$ dan penulisannya disederhanakan menjadi $\mathbb{Z}_2^2 = \{00, 01, 10, 11\}$. Sedangkan $\mathbb{Z}_3^2 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0)(2,1), (2,2)\}$ adalah ruang vektor dengan panjang 2 atas $\mathbb{Z}_3$ dan penulisannya disederhanakan menjadi $\mathbb{Z}_3^2 = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$.

3 Kode Linier dan Kode Siklik

Definisi 3.1 Ruang bagian dari F_q^n disebut kode linier dengan panjang n atas F_q.

Contoh 3.2 $C = \{000, 001, 010, 011\}$ adalah kode linier dengan panjang 3 atas $\mathbb{Z}_2$ karena C adalah ruang bagian dari $\mathbb{Z}_2^3$.

Definisi 3.3 Dimensi dari kode linier C adalah dimensi dari C sebagai ruang vektor atas F_q dan dinotasikan dengan $\dim(C)$.

Teorema 3.4 Misalkan C adalah kode linier dengan panjang n atas F_q. Jika $\dim(C) = k$, maka $|C| = q^k$. Jadi, $\dim(C) = k = \log_q |C|$.

Bukti. Misalkan $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \dots, \boldsymbol{c}_k\}$ adalah basis untuk C. Maka $C = \{\alpha_1\boldsymbol{c}_1 + \alpha_2\boldsymbol{c}_2 + \alpha_3\boldsymbol{c}_3 + \cdots + \alpha_k\boldsymbol{c}_k : \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k \in F_q\}$. Karena $|F_q| = q$, maka terdapat q pilihan untuk setiap $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_k$. Oleh karena itu, $|C| = q^k$. Jadi, $\dim(C) = k = \log_q|C|$.

Contoh 3.5 Dimensi dari $C = \{000, 001, 010, 011\}$ adalah $\dim(C) = \log_2 4 = 2$.

Definisi 3.6 Kode linier C dengan panjang n dan dimensi k atas F_q disebut kode linier *q-ary* $[n, k]$.

Contoh 3.7 $C_1 = \{000, 001, 010, 011\}$ adalah kode linier 2-*ary* $[3, 2]$ karena C_1 adalah kode linier dengan panjang 3 dan dimensi 2. Sedangkan $C_2 = \{0000, 0001, 1100, 1101, 1102, 0002, 2200, 2201, 2202\}$ adalah kode linier 3-*ary* $[4, 2]$ karena C_2 adalah kode linier dengan panjang 4 dan dimensi 2.

Definisi 3.8 Kode linier C dengan panjang n atas F_q disebut kode siklik jika untuk setiap $(c_0, c_1, c_2, \dots, c_{n-1}) \in C$ mengakibatkan $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$.

Contoh 3.9 $C_1 = \{000, 110, 011, 101\}$ adalah kode siklik 2-*ary* $[3, 2]$ karena C_1 adalah kode linier dengan panjang 3 atas $\mathbb{Z}_2$ dan $000, 110, 011, 101 \in C_1$. Sedangkan $C_2 = \{0000, 1010, 0101, 1111\}$ adalah kode siklik 2-*ary* $[4, 2]$ karena C_2 adalah kode linier dengan panjang 4 atas $\mathbb{Z}_2$ dan $0000, 1010, 0101, 1111 \in C_2$.

4 Hubungan antara Ideal dan Kode Siklik

Didefinisikan transformasi linier yang memetakan ruang vektor F_q^n ke ring polinomial $F_q[x]/(x^n - 1)$ sebagai berikut :

$$\pi : F_q^n \longrightarrow F_q[x]/(x^n - 1), \text{ dengan pengaitan}$$
$$(a_0, a_1, a_2, \dots, a_{n-1}) \mapsto a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \quad (1)$$

Teorema 4.1 Misalkan π adalah transformasi linier yang didefinisikan pada (1). Himpunan bagian tak kosong C dari F_q^n adalah kode siklik jika dan hanya jika $\pi(C)$ adalah ideal dari $F_q[x]/(x^n - 1)$.

Bukti. ($\Leftarrow$) Misalkan $\pi(C)$ adalah ideal dari $F_q[x]/(x^n - 1)$.
Ambil sebarang $\boldsymbol{a}, \boldsymbol{b} \in C$ dan $\alpha \in F_q[x]/(x^n - 1)$. Akibatnya, $\pi(\boldsymbol{a})$, $\pi(\boldsymbol{b}) \in \pi(C)$ sehingga $-\pi(\boldsymbol{b}) \in \pi(C)$. Karena π adalah transformasi linier, maka $\pi(\boldsymbol{a}) - \big(-\pi(\boldsymbol{b})\big) = \pi(\boldsymbol{a}) + \pi(\boldsymbol{b}) = \pi(\boldsymbol{a} + \boldsymbol{b}) \in \pi(C)$ dan $\alpha\pi(\boldsymbol{a}) = \pi(\alpha\boldsymbol{a}) \in \pi(C)$ sehingga $+\boldsymbol{b}$, $\alpha\boldsymbol{a} \in C$. Oleh karena itu, C merupakan kode linier. Selanjutnya, ambil sebarang $\boldsymbol{c} = (c_0, c_1, c_2, \dots, c_{n-1}) \in C$. Dari (1), diperoleh $\pi(\boldsymbol{c}) = \pi(c_0, c_1, c_2, \dots, c_{n-1}) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \pi(C)$. Kemudian, $x\pi(\boldsymbol{c}) = c_0x + c_1x^2 + c_2x^3 + \cdots +$

$c_{n-1}x^n = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-1}x^n - c_{n-1} = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-1}(x^n - 1)$. Karena $x^n - 1 = 0$ di $F_q[x]/(x^n - 1)$, maka diperoleh $x\pi(\boldsymbol{c}) = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-2}x^{n-1} \in \pi(C)$. Oleh karena itu, $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. Jadi, C adalah kode siklik.

($\Longrightarrow$) Misalkan C adalah kode siklik.

(i) Ambil sebarang $\pi(\boldsymbol{d}), \pi(\boldsymbol{e}) \in \pi(C)$ dengan $\pi(\boldsymbol{d}) = \pi(d_0, d_1, d_2, \dots, d_{n-1}) = d_0 + d_1x + d_2x^2 + \cdots + d_{n-1}x^{n-1}$, $\pi(\boldsymbol{e}) = \pi(e_0, e_1, e_2, \dots, e_{n-1}) = e_0 + e_1x + e_2x^2 + \cdots + e_{n-1}x^{n-1}$ dan $(d_0, d_1, d_2, \dots, d_{n-1})$, $(e_0, e_1, e_2, \dots, e_{n-1}) \in C$. Akibatnya, $\pi(\boldsymbol{d}) - \pi(\boldsymbol{e}) = (d_0 + d_1x + d_2x^2 + \cdots + d_{n-1}x^{n-1}) - (e_0 + e_1x + e_2x^2 + \cdots + e_{n-1}x^{n-1}) = (d_0 - e_0) + (d_1 - e_1)x + (d_2 - e_2)x^2 + \cdots + (d_{n-1} - e_{n-1})x^{n-1}$. Karena $(e_0, e_1, e_2, \dots, e_{n-1}) \in C$, maka $-(e_0, e_1, e_2, \dots, e_{n-1}) \in C$. Dengan demikian, $(d_0, d_1, d_2, \dots, d_{n-1}) + \big(-(e_0, e_1, e_2, \dots, e_{n-1})\big) = (d_0, d_1, d_2, \dots, d_{n-1}) - (e_0, e_1, e_2, \dots, e_{n-1}) = (d_0 - e_0,\ d_1 - e_1,\ d_2 - e_2, \dots,\ d_{n-1} - e_{n-1}) \in C$. Oleh karena itu, $\pi(\boldsymbol{d}) - \pi(\boldsymbol{e}) \in \pi(C)$.

(ii) Ambil sebarang $\pi(\boldsymbol{f}) \in \pi(C)$ dengan $\pi(\boldsymbol{f}) = \pi(f_0, f_1, f_2, \dots, f_{n-1}) = f_0 + f_1x + f_2x^2 + \cdots + f_{n-1}x^{n-1}$ dan $(f_0, f_1, f_2, \dots, f_{n-1}) \in C$. Akibatnya, $x\pi(\boldsymbol{f}) = f_{n-1} + f_0x + f_1x^2 + \cdots + f_{n-2}x^{n-1} = \pi(f_{n-1}, f_0, f_1, \dots, f_{n-2}) \in \pi(C)$ dan $x^2\pi(\boldsymbol{f}) = x\big(x\pi(\boldsymbol{f})\big) = f_{n-2} + f_{n-1}x + f_0x^2 + \cdots + f_{n-3}x^{n-1} = \pi(f_{n-2}, f_{n-1}, f_0, \dots, f_{n-3}) \in \pi(C)$. Dengan demikian, berdasarkan induksi, diperoleh $x^i\pi(\boldsymbol{f}) \in \pi(C)$ dengan $i \geq 0$. Oleh karena itu, untuk setiap $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_{n-1}x^{n-1} \in F_q[x]/(x^n - 1)$, diperoleh $h(x)\pi(\boldsymbol{f}) = \sum_{i=0}^{n-1} h_i \left(x^i\pi(\boldsymbol{f})\right) \in \pi(C)$ dan $\pi(\boldsymbol{f})h(x) = \sum_{i=0}^{n-1} \left(x^i\pi(\boldsymbol{f})\right) h_i \in \pi(C)$.

Jadi, $\pi(C)$ adalah ideal dari $F_q[x]/(x^n - 1)$. ■

Contoh 4.2 (i) $C = \{000, 111, 222\}$ adalah kode siklik 3-*ary*, maka $\pi(C) = \{0, 1 + x + x^2, 2 + 2x + 2x^2\}$ adalah ideal dari $F_3[x]/(x^3 - 1)$.

(ii) $I = \{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$ adalah ideal dari $F_2[x]/(x^4 - 1)$, maka $\pi^{-1}(I) = \{0000, 1010, 0101, 1111\}$ adalah kode siklik 2-*ary*.

5 Sifat-Sifat Polinomial Pembangun dari Ideal dan Dimensi dari Kode Siklik

Teorema 5.1 Misalkan I adalah ideal tak nol di $F_q[x]/(x^n - 1)$. Maka $g(x)$ adalah polinomial monik dengan derajat terkecil di I jika dan hanya jika $g(x)$ adalah polinomial pembangun dari I.

Bukti. ($\Longrightarrow$) Misalkan $g(x)$ adalah polinomial monik dengan derajat terkecil di I. Ambil sebarang $f_1(x) \in I$, maka berdasarkan algoritma pembagian, terdapat dengan tunggal $s(x)$, $r(x) \in F_q[x]/(x^n - 1)$ sehingga $f_1(x) = s(x)g(x) + r(x)$ dengan $\deg\big(r(x)\big) < \deg\big(g(x)\big)$ atau $r(x) = 0$. Akibatnya, $r(x) = f_1(x) - s(x)\, g(x)$

sehingga $r(x) \in I$. Karena $g(x)$ adalah polinomial monik dengan derajat terkecil di I, maka $r(x) = 0$. Oleh karena itu, $f_1(x) = s(x)g(x)$. Jadi, $g(x)$ adalah polinomial pembangun dari I.
($\Longleftarrow$) Misalkan $g(x)$ adalah polinomial pembangun dari I. Ambil sebarang $f_2(x) \in I$ dengan $f_2(x) = h(x)\, g(x)$ dan $h(x) \in F_q[x]/(x^n - 1)$. Akibatnya, $\deg\big(g(x)\big) \leq \deg\big(f_2(x)\big)$. Jadi, $g(x)$ adalah polinomial monik dengan derajat terkecil di I. ■

Teorema 5.2 Misalkan I adalah ideal tak nol di $F_q[x]/(x^n - 1)$, maka terdapat dengan tunggal polinomial pembangun dari I.

Bukti. Karena $F_q[x]/(x^n - 1)$ adalah ring ideal utama, maka I adalah ideal utama, yaitu terdapat $g(x) \in I$ sebagai polinomial pembangun dari I. Selanjutnya, misalkan $g_1(x)$ dan $g_2(x)$ adalah polinomial pembangun dari I dengan $g_1(x) \neq g_2(x)$. Berdasarkan Teorema 5.1, $g_1(x)$ dan $g_2(x)$ adalah polinomial monik dengan derajat terkecil di I sehingga $\deg\big(g_1(x)\big) = \deg\big(g_2(x)\big)$. Akibatnya, terdapat $\alpha \in F_q$ sehingga $\alpha\big(g_1(x) - g_2(x)\big)$ juga polinomial monik di I dengan $\deg\Big(\alpha\big(g_1(x) - g_2(x)\big)\Big) < \deg\big(g_1(x)\big) = \deg\big(g_2(x)\big)$. Hal ini menimbulkan kontradiksi. Oleh karena itu, $g_1(x) = g_2(x)$. Jadi, terdapat dengan tunggal polinomial pembangun dari I. ■

Teorema 5.3 Misalkan I adalah ideal tak nol di $F_q[x]/(x^n - 1)$. Maka $g(x)$ adalah polinomial pembangun dari I jika dan hanya $g(x)$ adalah pembagi monik dari $x^n - 1$.

Bukti. ($\Longrightarrow$) Misalkan $g(x)$ adalah polinomial pembangun dari I. Maka berdasarkan algoritma pembagian, terdapat dengan tunggal $s_1(x), r_1(x) \in F_q[x]/(x^n - 1)$ sehingga $x^n - 1 = s_1(x)\, g(x) + r_1(x)$ dengan $\deg\big(r_1(x)\big) < \deg\big(g(x)\big)$ atau $r_1(x) = 0$. Akibatnya, $r_1(x) = (x^n - 1) - s_1(x)g(x)$ sehingga $r_1(x) \in I$. Karena $g(x)$ adalah polinomial pembangun dari I, maka berdasarkan Teorema 5.1, $g(x)$ adalah polinomial monik dengan derajat terkecil di I. Oleh karena itu, $r_1(x) = 0$ sehingga $x^n - 1 = s_1(x)g(x)$. Jadi, $g(x)$ adalah pembagi monik dari $x^n - 1$.
($\Longleftarrow$) Misalkan $g(x)$ adalah pembagi monik dari $x^n - 1$. Asumsikan $h(x)$ adalah polinomial pembangun dari I. Maka terdapat $s_2(x) \in F_q[x]/(x^n - 1)$ sehingga $h(x) \equiv s_2(x)\, g(x) \pmod{x^n - 1}$. Akibatnya, $g(x)$ membagi $h(x)$. Selanjutnya, berdasarkan Teorema 5.1, $h(x)$ adalah polinomial monik dengan derajat terkecil di I. Oleh karena itu, $g(x) = h(x)$. Jadi, $g(x)$ adalah polinomial pembangun dari I. ■

Contoh 5.4 (i) $I_1 = \{0, 1 + x + x^2, 2 + 2x + 2x^2\}$ adalah ideal dari $F_3[x]/(x^3 - 1)$ dan $1 + x + x^2$ adalah polinomial monik dengan derajat terkecil di I_1, maka $1 + x + x^2$ adalah polinomial pembangun dari I_1 dan pembagi monik dari $x^3 - 1$.

(ii) $I_2 = \{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$ adalah ideal dari $F_2[x]/(x^4 - 1)$ dan $1 + x^2$ adalah polinomial monik dengan derajat terkecil di I_2, maka $1 + x^2$ adalah polinomial pembangun dari I_2 dan pembagi monik dari $x^4 - 1$.

Teorema 5.5 Misalkan I adalah ideal di $F_q[x]/(x^n - 1)$ dan $g(x)$ adalah polinomial pembangun dari I. Jika $g(x)$ berderajat $n - k$, maka kode siklik yang bersesuaian berdimensi k.

Bukti. Didefinisikan $A \coloneqq \{g(x)f(x) : f(x) \in F_q[x]/(x^n - 1), \deg(f(x)) \leq k - 1\}$. Diperoleh $A \subseteq < g(x) >$. Selanjutnya, ambil sebarang $g(x)\, h(x) \in < g(x) >$ dengan $h(x) \in F_q[x]/(x^n - 1)$, maka berdasarkan algoritma pembagian terdapat dengan tunggal $s(x)$, $r(x) \in I$ sehingga $g(x)h(x) = s(x)(x^n - 1) + r(x)$ dengan $\deg(r(x)) < n$. Kemudian, diperoleh $r(x) = g(x)h(x) - s(x)(x^n - 1)$. Karena $x^n - 1 = 0$ di $F_q[x] / (x^n - 1)$, maka $r(x) = g(x)\, h(x)$. Akibatnya, karena $\deg(g(x)) = n - k$, maka $\deg(h(x)) < k$. Oleh karena itu, $r(x) = g(x)h(x) \in A$. Hal ini menunjukkan bahwa $< g(x) > \subseteq A$. Dengan demikian, $A = < g(x) >$. Di sisi lain, karena $|F_q| = q$, maka terdapat q pilihan untuk setiap $f(x)$ dengan $\deg(f(x)) \leq k - 1$. Akibatnya, $|A| = q^k$. Jadi, berdasarkan Teorema 3.4, dimensi dari kode siklik yang bersesuaian adalah $\log_q |A| = \log_q q^k = k$. ■

Contoh 5.6 Tabel 1 – 4 berikut menunjukkan faktorisasi dari $x^n - 1$, polinomial pembangun dan derajatnya, kode siklik *q-ary* dengan $q = 2, 3, 4, 5$ beserta dimensinya.

Tabel 1 Kode siklik 2-*ary* dengan $n \leq 5$.

n	**Faktorisasi** $x^n - 1$	**Polinomial Pembangun** $(g(x))$	$\deg(g(x))$	**Kode Siklik** (C)	$\dim(C)$
1	$1 + x$	1	0	$\mathbb{Z}_2$	1
		$1 + x$	1	$\{0\}$	0
2	$(1 + x)^2$	1	0	$\mathbb{Z}_2^2$	2
		$1 + x$	1	$\{00, 11\}$	1
		$(1 + x)^2$	2	$\{00\}$	0
3	$(1 + x)$ $(1 + x + x^2)$	1	0	$\mathbb{Z}_2^3$	3
		$1 + x$	1	$\{000, 110, 011, 101\}$	2
		$1 + x + x^2$	2	$\{000, 111\}$	1
		$(1 + x)$ $(1 + x + x^2)$	3	$\{000\}$	0

4	$(1+x)^4$	1	0	$\mathbb{Z}_2^4$	4
		$1+x$	1	$\{0000, 1100, 0110, 0011, 1001, 1010, 0101, 1111\}$	3
		$(1+x)^2$	2	$\{0000, 1010, 0101, 1111\}$	2
		$(1+x)^3$	3	$\{0000, 1111\}$	1
		$(1+x)^4$	4	$\{0000\}$	0
5	$(1+x)$ $(1+x+x^2+x^3+x^4)$	1	0	$\mathbb{Z}_2^5$	5
		$1+x$	1	$\{00000, 11000, 01100, 00110, 00011, 10001, 10100, 01010, 00101, 10010, 01001, 11110, 01111, 10111, 11011, 11101\}$	4
		$1+x+x^2+x^3+x^4$	4	$\{00000, 11111\}$	1
		$(1+x)$ $(1+x+x^2+x^3+x^4)$	5	$\{00000\}$	0

Tabel 2 Kode siklik 3-*ary* dengan $n \leq 3$.

$\boldsymbol{n}$	**Faktorisasi** $\boldsymbol{x^n - 1}$	**Polinomial Pembangun** $\boldsymbol{(g(x))}$	$\boldsymbol{\deg(g(x))}$	**Kode Siklik** $\boldsymbol{(C)}$	$\boldsymbol{\dim(C)}$
1	$2+x$	1	0	$\mathbb{Z}_3$	1
		$2+x$	1	$\{0\}$	0
2	$(1+x)$ $(2+x)$	1	0	$\mathbb{Z}_3^2$	2
		$1+x$	1	$\{00, 11, 22\}$	1
		$2+x$	1	$\{00, 21, 12\}$	1
		$(1+x)$ $(2+x)$	2	$\{00\}$	0
3	$(2+x)^3$	1	0	$\mathbb{Z}_3^3$	3
		$2+x$	1	$\{000, 210, 120\}$	2
		$(2+x)^2$	2	$\{000, 111, 222\}$	1
		$(2+3)^3$	3	$\{000\}$	0

Tabel 3 Kode siklik 4-*ary* dengan $n \leq 3$.

n	**Faktorisasi** $x^n - 1$	**Polinomial Pembangun** $(g(x))$	**deg**$(g(x))$	**Kode Siklik** (C)	**dim**(C)
1	$3 + x$	1	0	$\mathbb{Z}_4$	1
		$3 + x$	1	$\{0\}$	0
2	$(1 + x)$ $(3 + x)$	1	0	$\mathbb{Z}_4^2$	2
		$1 + x$	1	$\{00, 11, 22, 33\}$	1
		$3 + x$	1	$\{00, 31, 13, 22\}$	1
		$(1 + x)$ $(3 + x)$	2	$\{00\}$	0
3	$(3 + x)$ $(1 + x + x^2)$	1	0	$\mathbb{Z}_4^3$	3
		$3 + x$	1	$\{000, 310, 031, 103, 301, 130, 013, 211, 121, 112, 022, 202, 220, 323, 332, 233\}$	2
		$1 + x + x^2$	2	$\{000, 111, 222, 333\}$	1
		$(3 + x)$ $(1 + x + x^2)$	3	$\{000\}$	0

Tabel 4 Kode siklik 5-*ary* dengan $n \leq 3$.

n	**Faktorisasi** $x^n - 1$	**Polinomial Pembangun** $(g(x))$	**deg**$(g(x))$	**Kode Siklik** (C)	**dim**(C)
1	$4 + x$	1	0	$\mathbb{Z}_5$	1
		$4 + x$	1	$\{0\}$	0
2	$(1 + x)$ $(4 + x)$	1	0	$\mathbb{Z}_5^2$	2
		$1 + x$	1	$\{00, 11, 22, 33, 44\}$	1
		$4 + x$	1	$\{00, 41, 14, 32, 23\}$	1
		$(1 + x)$ $(4 + x)$	2	$\{00\}$	0
3	$(4 + x)$ $(1 + x + x^2)$	1	0	$\mathbb{Z}_5^3$	3
		$4 + x$	1	$\{000, 410, 041, 104, 140, 014, 401, 212, 221, 122, 320, 032, 203, 230, 023, 302, 113, 311, 131, 442, 244, 424, 433, 343, 334\}$	2

		$1 + x + x^2$	2	$\{000, 111, 222, 333, 444\}$	1
		$(4 + x)$ $(1 + x + x^2)$	3	$\{000\}$	0

6 Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut :

1. Hubungan antara ideal dan kode siklik adalah himpunan bagian tak kosong C dari F_q^n adalah kode siklik jika dan hanya jika $\pi(C)$ adalah ideal di $F_q[x]/(x^n - 1)$.
2. Sifat-sifat polinomial pembangun dari ideal dan dimensi dari kode siklik adalah :
   a. Polinomial $g(x)$ adalah polinomial monik dengan derajat terkecil di ideal tak nol I dari $F_q[x]/(x^n - 1)$ jika dan hanya jika $g(x)$ adalah polinomial pembangun dari I.
   b. Terdapat dengan tunggal polinomial pembangun dari ideal tak nol I dari $F_q[x]/(x^n - 1)$.
   c. Polinomial $g(x)$ adalah polinomial pembangun dari ideal tak nol I dari $F_q[x]/(x^n - 1)$ jika dan hanya jika $g(x)$ adalah pembagi monik dari $x^n - 1$.
   d. Jika polinomial pembangun dari ideal tak nol I dari $F_q[x]/(x^n - 1)$ berderajat $n - k$, maka kode siklik yang bersesuaian berdimensi k.

7 Daftar Pustaka

[1] Hankerson, D.R., Horman, D.G., Leonard, D.A., Lindner, C.C., Phelps, K.T., Rodger, C.A. & Wall, J.R., 2000, *Coding Theory and Cryptography : The Essentials Second Edition*, Marcel Dekker, Inc.

[2] Ling, S. & Xing, C., 2004, *Coding Theory A First Course*, Cambridge University Press, hal 133.

[3] Prange, E., 1957, *Cyclic Error-Correcting Codes in Two Symbols*, AFCRC-TN-57, hal. 103.

[4] Shannon, C.E., 1948, *A Mathematical Theory of Communication*, Bell System Technical Journal, Vol. 27, hal. 379-423, 623-656.