Jurnal Matematika Integratif. p-ISSN:1412-6184, e-ISSN:2549-903
Vol. 15, No. 1 (2019), pp. 9-15. doi:10.24198/jmi.v15.n1.20897.9-15

# Kode Siklis dari Sebuah Monomial

Nopendri[1], Intan Muchtadi-Alamsyah[2], Djoko Suprijanto[3], Aleams Barra[4]

[1,2,4]**KK Aljabar, FMIPA, Institut Teknologi Bandung, Indonesia,**
**nopendri301@students.itb.ac.id**
[2]**ntan@math.itb.ac.id**
[4]**barra@math.itb.ac.id**
[3]**KK Matematika Kombinatorika, FMIPA, Institut Teknologi Bandung,**
**djoko@math.itb.ac.id**

**Abstrak**

Kode siklis merupakan salah satu topik riset paling aktif dalam teori koding karena memiliki banyak aplikasi pada sistem penyimpanan data dan komunikasi. Hal ini dikarenakan kode siklis memiliki algoritma *encoding* dan *decoding* yang efisien. Dalam makalah ini, dijelaskan tentang konstruksi kode siklis dari barisan yang dibangun oleh *trace* dari sebuah monomial atas lapangan hingga karakteristik dua. Beberapa contoh dari kode yang diperoleh ditampilkan pada makalah ini.

*Kata kunci*: kode siklis, barisan, *trace*, monomial

**Abstract**

*Cyclic codes have been one of the most active research topics in coding theory because they have many applications in data storage systems and communication systems as they have efficient encoding and decoding algorithms. This paper explain the construction of a family of binary cyclic codes from sequences generated by a trace of a monomial over finite fields of characteristic two. Some examples of the codes are presented in this paper.*

*Keywords*: cyclic codes, sequences, trace, monomials.

## 1. Pendahuluan

Kode siklis banyak digunakan secara luas di berbagai bidang seperti sistem penyimpanan data dan sistem komunikasi dikarenakan memiliki algoritma yang efisien untuk proses *encoding* dan *decoding* [1].

Salah satu masalah utama dalam penelitian teori koding adalah mencari kode-kode yang optimal, yaitu kode-kode yang memiliki jarak minimum $d$ terbesar yang terkait dengan kemampuan memperbaiki kesalahan dalam transfer informasi [2].

Kode siklis dapat dikonstruksi dari sebuah polinom suatu barisan periodik $s$ (lihat Ding [3, 4]). Barisan ini dibangkitkan dari sebuah fungsi pada suatu lapangan hingga. Hasil konstruksi kode dalam makalah tersebut sangat menjanjikan, yakni diperoleh kode optimal berdasarkan koleksi tabel kode linier terbaik di `http://www.codetables.de/`.

*2000 Mathematics Subject Classification*: 11T71, 94B15, 94B05, 94A55
Received: 2019-02-16, Revisions : 2019-05-27, Accepted: 2019-06-18.

Dalam makalah [3] dan [4] tersebut beberapa monomial dan trinomial digunakan untuk mengonstruksi kode siklis atas lapangan hingga. Pada makalah [3] juga dikemukakan definisi barisan baru yang dinotasikan dengan š untuk mengonstruksi kode siklis namun masih menggunakan monomial dan trinomial yang sama. Hal ini akan menghasilkan kode siklis baru yang masih berelasi dengan kode dari definisi $s$. Pada makalah [3], salah satu monomial dari [4] dipakai dalam mengonstruksi kode siklis dari barisan š. Beberapa kode yang diperoleh adalah optimal.

Dalam makalah ini dibahas konstruksi kode siklis dengan barisan š dari salah satu monomial di [3]. Makalah ini membahas barisan untuk polinom pembangun kode siklis dengan menggunakan ide yang mirip dengan [5] namun lebih sederhana dalam pembuktiannya. Juga ditambahkan sedikit informasi tentang jarak minimum. .

## 2. Kode Siklis dan Barisan Periodik

Dalam makalah ini, misalkan $p$ adalah bilangan prima dan $q$ adalah pangkat positif dari $p$.

2.1. **Kode Siklis.** Misalkan $GF(q)$ adalah lapangan hingga dengan $q$ unsur. Pandang $(GF(q))^n$ sebagai ruang vektor atas $GF(q)$. Sebuah $q$-ary $[n, k, d]$-*kode linier* $\mathcal{C}$ adalah subruang dari $(GF(q))^n$ dengan dimensi $k$ atas $GF(q)$ dan jarak (minimum) $d$. Sebuah kode linier $\mathcal{C}$ adalah siklis jika untuk setiap vektor $(c_0, c_1, ..., c_{n-1})$ di $\mathcal{C}$, vektor $(c_{n-1}, c_0, c_1, ..., c_{n-2})$ di $\mathcal{C}$. Sebuah kata kode(vektor) $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ di $\mathcal{C}$ dapat direpresentasikan dalam sebuah polinom $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ di gelanggang $\mathcal{R}_n = GF(q)[x]/\langle x^n - 1\rangle$. Sehingga $\mathcal{C} \subseteq (GF(q))^n$ dapat diidentifikasi dengan sebuah subhimpunan dari $\mathcal{R}_n$, dalam hal ini kode siklis adalah sebuah *ideal* dari $\mathcal{R}_n$ dan ideal dari $\mathcal{R}_n$ adalah kode siklis. Ideal dari $\mathcal{R}_n$ adalah utama, sehingga setiap ideal dibangun oleh sebuah polinom $g(x)$, dengan $g(x)$ adalah pembagi $x^n - 1$. Polinom $g$ dinamakan *pembangun* dari kode siklis $\mathcal{C}$. Dimensi dari kode siklis $\mathcal{C}$ ditentukan oleh $\text{der}(g(x))$, derajat polinom pembangun $g$.

2.2. **Barisan Periodik atas Lapangan Hingga.** Misalkan $s^\infty = (s_t)_{t=0}^\infty$ sebuah barisan atas $GF(q)$. Barisan $s^\infty$ dikatakan *periodik* dengan periode $N$ jika terdapat bilangan bulat $N$ sedemikian sehingga $s_t = s_{t+lN}$ untuk setiap $t, l \geq 0$.

Sebuah polinom $c(x) = a_kx^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0$ atas $GF(q)$, dengan $a_k = 1$, dinamakan *polinom karakteristik* dari $s^\infty$ jika untuk setiap $n = 0, 1, 2, \ldots$ berlaku

$$a_ks_{n+k} + a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + ... + a_0s_n = 0.$$

Polinom karakteristik berderajat terkecil dari $s^\infty$ dinamakan *polinom minimal* dari $s^\infty$, dan dinotasikan dengan $\mathbb{M}_s(x)$. Polinom minimal $\mathbb{M}_s(x)$ dari sebuah barisan $s^\infty$ ini adalah tunggal dan membagi $c(x)$. Derajat dari $\mathbb{M}_s(x)$ disebut *linear span* dari $s^\infty$.

2.3. **Kode Siklis dari Barisan.** Salah satu cara mengonstruksi kode siklis atas $GF(q)$ dengan panjang $n$ adalah dengan menggunakan polinom pembangun

$$g(x) = \frac{x^n - 1}{FPB(S^n(x), x^n - 1)},$$

dengan $S^n(x) = \sum_{i=0}^{n-1} s_ix^i \in GF(q)[x]$ dan $(s_i)_{i=0}^\infty$ barisan dengan periode $n$ atas $GF(q)$.

Untuk barisan periodik ada beberapa cara untuk menentukan *linear span* dan polinom minimal.

**Lema 2.1** ([6]). *Misalkan $s^\infty$ adalah barisan dengan periode $L$. Definisikan $S^L(x) = \sum_{t=0}^{L-1} s_tx^t \in GF(q)[x]$, maka polinom minimal $\mathbb{M}_s(x)$ berbentuk*

$$\frac{x^L - 1}{FPB(S^L(x), x^L - 1)}$$

*dan linear span $\mathbb{L}_s$ adalah $L - der(FPB(S^L(x), x^L - 1))$.*

**Lema 2.2** ([7]). *Sebarang barisan $s^\infty$ atas $GF(q)$ dengan periode $q^m-1$ memiliki bentuk ekspansi yang tunggal, yakni*

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it},\ \forall t \geq 0,$$

*dengan $c_i \in GF(q^m)$. Misalkan himpunan indeks $I = \{i | c_i \neq 0\}$, maka polinom minimal $\mathbb{M}_s(x)$ dari $s^\infty$ adalah*

$$\mathbb{M}_s(x) = \prod_{i \in I} (x - \alpha^i).$$

## 3. Konstruksi Kode Siklis dari Barisan Periodik

Pada bagian ini akan dibahas kode siklis dari suatu barisan di $GF(2)$ yang didefinisikan oleh

$$\check{s}_t = \mathrm{Tr}(f(\alpha^t + 1) - f(\alpha^t)), \tag{1}$$

dengan $f(x) = x^{2^m-2} \in GF(2^m)[x]$, $m$ bilangan bulat positif, $\alpha$ adalah suatu akar primitif di $GF(2^m)$, dan $\mathrm{Tr}(x)$ adalah fungsi *trace* dari $GF(q^m)$ ke $GF(q)$. Pandang koset 2-siklotomik modulo $2^m-1$ yang didefinisikan sebagai $C_j = \{j, j2^1, j2^2, ..., j2^{m_j-1}\}$ dengan $m_j$ adalah bilangan bulat terkecil sedemikian sehingga $j2^{m_j} \equiv j \mod (2^m-1)$. Bilangan $m_j$ disebut panjang dari $C_j$, dan $j$ sebagai bilangan terkecil di $C_j$ disebut pemuka koset. Dinotasikan $\Gamma$ sebagai himpunan semua pemuka koset, $\Lambda = \Gamma \setminus \{2^{m-1}-1\}$, dan $B_j = \{i | i \in C_j \text{ dan } 0 \leq i \leq 2^{m-1}-1\}$. Beberapa lema berikut diperlukan untuk pembuktian hasil utama makalah ini.

**Lema 3.1** ([5]). *Untuk setiap $j \in \Gamma \setminus \{0\}$, diperoleh $j$ ganjil dan $1 \leq j \leq 2^{m-1}-1$.*

**Lema 3.2** ([8]). *Koset 2-siklotomik $C_j$ modulo $2^m-1$ dengan $|C_j| = m_j$ ada jika dan hanya jika $m_j | m$. Untuk $FPB(j, 2^m-1) = 1$ maka $m_j = m$.*

**Lema 3.3** ([5]). *Untuk setiap $j \in \Gamma$ dan $i \in B_j$, terdapat secara tunggal $0 \leq k_{ij} \leq m_j - 1$, sedemikian sehingga*

$$2.i.2^{k_{ij}} \equiv j \mod (2^m-1).$$

**Lema 3.4.** *Barisan dengan definisi (1) adalah periodik dengan periode $N = 2^m-1$.*

Bukti. Misalkan $k$ bilangan bulat positif dan $\alpha \in GF(2^m) \setminus \{0\}$.

$$\begin{aligned}\check{s}_{t+kN} &= \mathrm{Tr}_1^m(f(\alpha^{t+kN}+1) - f(\alpha^{t+kN})) = \mathrm{Tr}_1^m(f(\alpha^{kN}\alpha^t+1) - f(\alpha^{kN}\alpha^t)) \\ &= \mathrm{Tr}_1^m(f(\alpha^t+1) - f(\alpha^t)) = \check{s}_t.\end{aligned}$$

**Lema 3.5** ([9]). *Jika $a$ dan $b$ bilangan bulat positif, $b \leq a$, dengan representasi basis 2 (secara berurutan) $a = a_r 2^r + a_{r-1}2^{r-1} + ... + a_1 2 + a_0$ dan $b = b_r 2^r + b_{r-1}2^{r-1} + ... + b_1 2 + b_0$ maka*

$$\binom{a}{b} = \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}} ... \binom{a_0}{b_0} \pmod 2.$$

3.1. **Hasil Utama.** Dari Lema 3.2, misalkan $m = m_j.l_j$ dengan $l_j$ bilangan bulat tunggal, definisikan

$$\chi_j = l_j.|B_j| \mod 2.$$

Teorema dan akibat berikut merupakan hasil utama dari makalah ini.

**Teorema 3.6.** *Misalkan $m \geq 3$ dan $\check{s}^{\infty}$ adalah barisan seperti pada (1) , dengan $f(x) = x^{2^m-2}$ atas $GF(2^m)$, maka polinom minimal dari $\check{s}^{\infty}$ adalah*

$$\mathbb{M}_{\check{s}}(x) = \prod_{j\in\Lambda, \chi_j=1} m_{\alpha^j}(x), \tag{2}$$

*dengan $m_a(x)$ adalah polinom minimal dari $a \in GF(2^m)$ dan linier span dari $\check{s}^{\infty}$ adalah $\mathbb{L}_{\check{s}} = 2^{m-1} - m$.*

Bukti. Dari Lema 3.4, barisan (1) memenuhi Lema 2.2, maka dapat dicari ekspansi barisan dalam bentuk akar primitif $\alpha$. Dari definisi barisan, diperoleh

$$\check{s}_t = \mathrm{Tr}_1^m(f(\alpha^t+1) - f(\alpha^t)) = \mathrm{Tr}_1^m((\alpha^t+1)^{2^m-2} - (\alpha^t)^{2^m-2}) \tag{3}$$

Dengan menggunakan formula binomial $(u+v)^n = \sum_{i=0}^{n} \binom{n}{i} u^{n-i}v^i$, dimana $\binom{n}{i} = \frac{n!}{i!(n-i)!}$, bentuk (3) dapat diperluas menjadi

$$\check{s}_t = \mathrm{Tr}_1^m\left(\left(\sum_{i=0}^{2^m-1}\binom{2^m-2}{i}\alpha^{it}\right) - \alpha^{t(2^m-2)}\right) \tag{4}$$

Untuk meninjau bentuk $\binom{2^m-2}{i} \mod 2$, diperlukan Lema 3.5. Bentuk $2^m-2$ dapat direpresentasikan dalam $2^m - 2 = 1.2^{m-1} + ... + 1.2^1 + 0.2^0$ dan bentuk $i$ dapat direpresentasikan dalam bentuk $i = i_{m-1}.2^{m-1} + ... + i_1.2^1 + i_0.2^0$. Sehingga dengan Lema 3.5 diperoleh

$$\binom{2^m-2}{i} = \binom{1}{i_r}\binom{1}{i_{r-1}}...\binom{1}{i_1}\binom{0}{i_0} = \binom{0}{i_0} \pmod 2.$$

Karena $0 \leq i \leq 2^m-2$, $\binom{2^m-2}{i} \mod 2 = 1 \Leftrightarrow i_0 = 0 \Leftrightarrow i = i_{m-1}.2^{m-1}+...+i_1.2^1+0.2^0 \Leftrightarrow i \mod 2 = 0$, bentuk (4) menjadi

$$\begin{aligned}\check{s}_t &= \mathrm{Tr}_1^m\left(\left(\sum_{i=0}^{2^{m-1}-1}\alpha^{2it}\right) - \alpha^{t(2^m-2)}\right) = \mathrm{Tr}_1^m\left(\sum_{i=0}^{2^{m-1}-1}\alpha^{2it}\right) - \mathrm{Tr}_1^m\left(\alpha^{t(2^m-2)}\right)\\ &= \mathrm{Tr}_1^m\left(\sum_{j\in\Gamma}\sum_{i\in B_j}\alpha^{2it}\right) - \mathrm{Tr}_1^m\left(\alpha^{t(2^m-2)}\right) = \left(\sum_{j\in\Gamma}\sum_{i\in B_j}\mathrm{Tr}_1^m(\alpha^{2it})\right) - \left(\sum_{i=0}^{m-1}\alpha^{t(2^m-2)2^i}\right)\end{aligned} \tag{5}$$

Karena $FPB(2^m-2, 2^m-1) = 1$, berdasarkan kasus khusus pada Lema 3.2 koset 2-siklotomik $C_{2^m-2}$ memiliki panjang $m$. Kemudian berdasarkan sifat fungsi *trace* dan sifat

yang terdapat dalam Lema 3.3 maka bentuk (5) diatas menjadi

$$\begin{aligned}
\check{s}_t &= \left(\sum_{j\in\Gamma}\sum_{i\in B_j}[\mathrm{Tr}_1^m(\alpha^{2it})]^{2^{k_{ij}}}\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right)\\
&= \left(\sum_{j\in\Gamma}\sum_{i\in B_j}\mathrm{Tr}_1^m(\alpha^{2i2^{k_{ij}}t})\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right)\\
&= \left(\sum_{j\in\Gamma}\sum_{i\in B_j}\sum_{u=0}^{m_j-1}\sum_{h=0}^{l_j-1}(\alpha^{jt})^{2^{u+m_jh}}\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right)\\
&= \left(\sum_{j\in\Gamma}\sum_{i\in B_j}\sum_{u=0}^{m_j-1}\alpha^{jt2^u}\sum_{h=0}^{l_j-1}1\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right) \qquad (6)\\
&= \left(\sum_{j\in\Gamma}\sum_{u=0}^{m_j-1}\alpha^{jt2^u}\sum_{i\in B_j}\sum_{h=0}^{l_j-1}1\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right)\\
&= \left(\sum_{j\in\Gamma}\sum_{i\in C_j}(\alpha^{it})\sum_{i\in B_j}\sum_{h=0}^{l_j-1}1\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right)\\
&= \left(\sum_{j\in\Gamma}\chi_j\left(\sum_{i\in C_j}(\alpha^{it})\right)\right) - \left(\sum_{i\in C_{2^m-2}}(\alpha^{it})\right).
\end{aligned}$$

Berdasarkan definisi $B_j$, untuk $i \in B_j$ memenuhi $0 \le i \le 2^{m-1}-1 \iff 0 \le 2i \le 2^m-2$. Notasikan $D_j$ sebagai himpunan anggota koset 2-siklotomik $C_j$ yang genap, maka terdapat bijeksi dari $B_j$ ke $D_j$ yang mengakibatkan $|B_j| = |D_j|$. Dari [3] diperoleh $\chi_j = \nu_j$ dengan $\nu_j = \frac{m.|D_j|}{m_j} \mod 2$. Sehingga dari hasil (6) dan dari Lema 4.1 di [3] diperoleh *linier span* $\mathbb{L}_{\check{s}} = \frac{(2^m-1)+1}{2} - m = 2^{m-1} - m$.

Dari definisi koset 2-siklotomik, himpunan $C_{2^m-2} = C_{2^{m-1}-1}$. Berdasarkan Lema 3.1, $C_{2^{m-1}-1}$ merupakan anggota pemuka koset $\Gamma$ yang terbesar. Hal ini mengakibatkan bentuk (6) menjadi

$$\check{s}_t = \left(\sum_{j\in\Gamma}\chi_j\left(\sum_{i\in C_j}(\alpha^{it})\right)\right) - \left(\sum_{i\in C_{2^{m-1}-1}}(\alpha^{it})\right) = \left(\sum_{j\in\Lambda}\chi_j\left(\sum_{i\in C_j}(\alpha^{it})\right)\right). \qquad (7)$$

Kesimpulan yang diinginkan untuk polinom minimal $\mathbb{M}_{\check{s}}(x)$ berasal dari (7) dan Lema 2.2. □

**Akibat 3.7.** *Kode biner $\mathcal{C}_{\check{s}}$ yang didefinisikan dari barisan pada Teorema 3.6 memiliki parameter $[2^m-1, 2^{m-1}-1+m, d]$ dan polinom pembangun $\mathbb{M}_{\check{s}}(x)$ dari (2). Jika $m$ ganjil, maka jarak minimum $d$ genap.*

Bukti.Dimensi dari $\mathcal{C}_{\check{s}}$ diturunkan dari Teorema 3.6 dan dari definisi kode $\mathcal{C}_{\check{s}}$. Untuk $m$ ganjil, berdasarkan Teorema 3.6 diperoleh

$$m_1(x) = m_{\alpha^0}(x) = \prod_{j\in C_0=\{0\}}(x-(\alpha^0)^j) = x-1,$$

dan $\chi_0 = l_0|B_0| = 1$. Sehingga, $m_1(x) = x-1$ adalah pembagi dari $\mathbb{M}_{\check{s}}(x) = \prod_{j\in\Lambda,\chi_j=1} m_{\alpha^j}(x)$. Dengan demikian, $\forall c \in \mathcal{C}_{\check{s}}$ berbobot genap. □

Teorema 3.6 memberikan informasi polinom minimal sebuah barisan periodik $\check{s}$. Polinom minimal tersebut dapat menjadi polinom pembangun kode siklis $\mathcal{C}$ dengan $n = 2^m - 1$ dan dimensi $k = 2^m - 1 + m$. Kode yang diperoleh dari konstruksi ini bisa optimal dan bisa tidak optimal. Sementara itu, Akibat 3.7 memberikan informasi jarak (minimum) untuk kasus $m$ tertentu. Hal ini bisa dilihat pada contoh-contoh berikut.

**Contoh 3.8.** *Untuk $m = 3$ dan dipilih polinom tak-tereduksi untuk $GF(2^3)$ adalah $x^3 + x + 1$, maka dari definisi barisan (1) diperoleh barisan $\check{s} = \{1, 1, 1, 1, 1, 1, 1, \dots\}$ atas $GF(2)$. Kemudian berdasarkan Lema 2.2 diperoleh ekspansi dari barisan $\check{s}$ tersebut terhadap (pangkat dari) $\alpha$ dengan koefisien $\{c_0 = 1, c_1 = 0, c_2 = 0, c_3 = 0, c_4 = 0, c_5 = 0, c_6 = 0\}$. Sehingga dengan Teorema 3.6 diperoleh polinom minimal $\mathbb{M}_{\check{s}}(x) = x + 1$ dan linier span $\mathbb{L}_{\check{s}} = 1$.Polinom tersebut menjadi polinom pembangun dari kode siklis $\mathcal{C}$ dengan parameter $[7, 6, 2]$.Berdasarkan tabel pada* `http://www.codetables.de/`*, diketahui batas bawah adalah 2 dan batas atas adalah 2 bagi jarak (minimum) kode linier dengan $n = 7$ dan $k = 6$. Sehingga kode ini merupakan kode yang optimal (memenuhi batas atas dan batas bawah bagi jarak(minimum)).*

Dengan menggunakan software `Sage` dan GAP dapat dihitung polinom pembangun beserta parameter kode siklis $\mathcal{C}_{\check{s}}$ seperti pada contoh diatas. Sehingga diperoleh sebagaimana dalam contoh-contoh berikut.

**Contoh 3.9.** *Untuk $m = 4$ dan polinom tak-tereduksi untuk $GF(2^4)$ adalah $x^4 + x + 1$. Maka polinom pembangun kode siklis adalah $x^4 + x^3 + 1$ dan parameter $\mathcal{C} = [15, 11, 3]$. Kode ini merupakan kode yang optimal.*

**Contoh 3.10.** *Untuk $m = 5$ dan polinom tak-tereduksi untuk $GF(2^5)$ adalah $x^5 + x^2 + 1$. Maka polinom pembangun kode siklis adalah $x^{11} + x^9 + x^5 + x^3 + x + 1$ dan parameter $\mathcal{C} = [31, 20, 6]$. Kode ini merupakan kode yang optimal.*

**Contoh 3.11.** *Untuk $m = 6$ dan polinom tak-tereduksi untuk $GF(2^6)$ adalah $x^6 + x^4 + x^3 + x + 1$. Maka polinom pembangun kode siklis adalah $x^{26} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{14} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^4 + x + 1$ dan parameter $\mathcal{C} = [63, 37, 6]$. Kode siklis ini tidak optimal karena untuk kode linier yang optimal dari panjang 63 dan dimensi 37 atas $GF(2)$ memiliki jarak (minimum) $d$ yang memenuhi $10 \leq d \leq 12$.*

## 4. Simpulan

Pada makalah ini dikonstruksi sebuah keluarga kode siklis dari barisan periodik š dari monomial $f(x) = x^{2^m - 2}$ di $GF(2^m)$ dan telah diberikan contoh dari kode siklis dan parameternya. Secara umum kode ini memiliki parameter $[2^m - 1, 2^{m-1} - 1 + m, d]$. Beberapa contoh yang diberikan merupakan kode optimal.

**Ucapan Terimakasih.**

Penelitian ini didanai sebagian oleh Hibah P3MI 2017.

## Daftar Pustaka

[1] Huffman, W.C., Pless, V., 2003, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, New York.

[2] MacWilliams, F., Sloane, N., 1977, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, New York.

[3] Ding, C., 2013, Cyclic Codes from Some Monomials and Trinomials, *SIAM J. Discrete Mathematics*, Vol. 27, No. 4, hal. 1977-1994.

[4] Ding, C., Zhou, Z., 2014, Binary Cyclic Codes from Explicit Polynomials over $GF(2^m)$, *Discrete Mathematics*, Vol. 321, hal. 76-89.

[5] Si, W., Ding, C., 2012, A Simple Stream Cipher with Proven Properties, *Cryptogr. Commun.*, Vol. 4, No. 2, hal. 79-104.

[6] Lidl, R., Niederreiter, H., 1994, *Introduction to Finite Fields and Their Applications*, Cambridge Univ.Press, Cambridge.
[7] Antweiler, M., Bomer,L., 1992, Complex Sequences over $GF(p^M)$ with a Two-Level Autocorrelation Function and a Large Linear Span, *IEEE Trans. Inform. Theory*, Vol. 38, No.1, hal. 120-130.
[8] Gupta, K.C., Maitra, S., 2001, Primitive Polynomials over GF(2) - A Cryptologic Approach, *Third International Conference, ICICS 2001, Xian, China, 13-16 November 2001*, hal. 23-34.
[9] Lucas, E., 1878, Théorie des fonctions numériques simplement périodiques, *Am. J. Math*, Vol. 1, hal. 229-231.