BAB II
KAJIAN TEORI

Pada Bab II ini berisi kajian teori. Di bab ini akan dijelaskan beberapa definisi mengenai grup, ring, dan lapangan serta teori-teori pengkodean yang mendasari teori kode BCH.

A. Grup

Definisi 2.1 (Fraleigh, 2003 : 20). *Operasi biner* $*$ *pada himpunan S adalah suatu pemetaan fungsi* $S \times S$ *ke* S. *Untuk setiap* $(a, b) \in S \times S$, *elemen* $*((a, b))$ *dari S dilambangkan dengan* $a * b$.

Definisi 2.2 (Fraleigh, 2003 : 37). *Grup* $(G,*)$ *adalah suatu himpunan G yang tertutup dengan operasi biner* $*$, *sedemikian sehingga aksioma-aksioma berikut dipenuhi:*

1. *Untuk setiap* $a, b, c \in G$, *berlaku* $(a * b) * c = a * (b * c)$ *atau sifat asosiatif dari* $*$.
2. *Ada suatu elemen* e *di* G *sedemikian sehingga untuk setiap* $x \in G$, $e * x = x * e = x$, e *adalah elemen identitas untuk* $*$.
3. *Untuk setiap* $a \in G$, *ada suatu elemen* a' *di* G *sedemikian sehingga* $a * a' = a' * a = e$, a' *adalah invers dari* a.

Definisi 2.3 (Fraleigh, 2003 : 39). *Grup G disebut grup abelian jika operasi binernya bersifat komutatif.*

Berikut akan diberikan contoh grup abelian.

Contoh 2.1. Himpunan $Z_2 = \{[0], [1]\}$ adalah suatu grup abelian. Himpunan Z_2 adalah himpunan semua kelas bilangan bulat modulo 2 dengan penjumlahan modulo 2.

Bukti:

$+_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Memperhatikan tabel Cayley Z_2 untuk penjumlahan modulo 2 terlihat bahwa sifat tertutupnya terpenuhi, elemen identitasnya adalah $[0]$, invers terhadap penjumlahan modulo 2 yaitu $-[0] = 0, -[1] = 1$.

Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo 2 bersifat komutatif. ■

B. Ring

Ring adalah suatu struktur aljabar dengan dua operasi biner.

Definisi 2.4 (Fraleigh, 2003 : 167). *Ring* $(R, +, \cdot)$ *adalah suatu himpunan* R *dengan dua operasi biner* $+$ *dan* $\cdot$, *yang kemudian disebut operasi penjumlahan dan perkalian. Kedua operasi tersebut didefinisikan pada* R *sedemikian sehingga aksioma-aksioma berikut dipenuhi:*

1. $(R, +)$ *adalah grup abelian.*
2. *Operasi perkaliannya bersifat asosiatif.*
3. *Untuk setiap* $a, b, c \in R$, *berlaku sifat distributif kiri,* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *dan sifat distributif kanan* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Berikut diberikan contoh dari ring.

Contoh 2.2. Himpunan $Z_2 = \{[0], [1]\}$ adalah suatu ring. Himpunan Z_2 adalah himpunan semua kelas bilangan bulat modulo 2 dengan penjumlahan modulo 2 dan perkalian modulo 2 adalah suatu ring.

Bukti:

$+_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$*_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Memperhatikan tabel Cayley Z_2 untuk penjumlahan modulo 2 terlihat bahwa sifat tertutupnya terpenuhi, elemen nolnya adalah $[0]$, invers terhadap penjumlahan modulo 2 yaitu $-[0] = 0, -[1] = 1$. Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo 2 bersifat komutatif. Himpunan Z_2 terhadap perkalian modulo 2 bersifat tertutup. ■

C. Lapangan

Definisi 2.5 (Gallian, 2006 : 250). *Lapangan adalah suatu ring komutatif dengan elemen kesatuan yang setiap elemen yang bukan nol adalah suatu unit (mempunyai invers terhadap perkalian).*

Berikut adalah contoh dari lapangan.

Contoh 2.3. Himpunan $Z_5 = \{[0], [1], [2], [3], [4]\}$ adalah himpunan semua kelas bilangan bulat modulo 5 dengan penjumlahan modulo 5 dan perkalian modulo 5 adalah suatu lapangan.

Bukti:

$+_5$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$*_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Memperhatikan tabel Cayley Z_5 untuk penjumlahan modulo 5 terlihat bahwa sifat tertutupnya terpenuhi, elemen nolnya adalah $[0]$, invers terhadap penjumlahan modulo 5, yaitu $-[0] = 0$, $-[1] = 4$, $-[2] = 3$, $-[3] = 2$, $-[4] = 1$. Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo 5 maupun perkalian modulo 5 bersifat komutatif. Himpunan Z_5 terhadap perkalian modulo 5 bersifat tertutup, elemen kesatuannya adalah $[1]$ dan invers dari setiap elemenennya terhadap perkalian modulo 5, yaitu $[1]^{-1} = [1]$, $[2]^{-1} = [3]$, $[4]^{-1} = [4]$. ■

D. Lapangan Hingga

Definisi 2.6 (Lange, 2011). *Suatu lapangan yang memuat elemen sebanyak berhingga disebut lapangan berhingga. Lapangan hingga yang memuat sebanyak* $\boldsymbol{q}$ *elemen dilambangkan dengan* $\boldsymbol{F_q}$.

Berikut akan diberikan contoh lapangan hingga.

Contoh 2.4. Himpunan $Z_2 = \{[0], [1]\}$ adalah suatu lapangan hingga karena Z_2 adalah suatu lapangan dengan banyak elemen yang berhingga.

E. Lapangan Galois

Definisi 2.7 (Vanstone dan Oorschot, 1989 : 28). *Jika* $\boldsymbol{F}$ *suatu lapangan hingga dengan* $\boldsymbol{q}$ *elemen, dan* $\boldsymbol{q} = \boldsymbol{p}^{\boldsymbol{n}}$ *dengan* $\boldsymbol{p}$ *bilangan prima dan* $\boldsymbol{n}$ *bilangan asli, maka* $\boldsymbol{F}$ *dilambangkan dengan* $\boldsymbol{GF}(\boldsymbol{q})$.

Untuk mengkonstruksi suatu lapangan hingga yang memuat p^n elemen digunakan suatu polinomial tak tereduksi dengan derajat n dalam $GF(p)[x]$. Untuk kasus $n = 2$, akan dibuktikan bahwa selalu ada suatu polinomial kuadrat tidak tereduksi dalam $GF(p)[x]$. Ada p^2 polinomial monik (polinomial dengan derajat $n \geq 1$ dengan koefisien dari x^n adalah 1) berderajat dua dalam $GF(p)[x]$. Jika satu dari p^2 polinomial tersebut yang dapat direduksi, maka polinomial tersebut adalah suatu hasil perkalian dari 2 polinomial monik berderajat 1. Ada tepat p polinomial monik berderajat 1. Menggunakan polinomial-polinomial monik berderajat 1 tersebut didapatkan $\binom{p}{2} + p$ polinomial kuadrat monik yang dapat direduksi, dengan $\binom{p}{2}$ adalah kombinasi 2 dari p. Sehingga banyaknya polinomial kuadrat monik yang tidak tereduksi adalah

$$l_2 = p^2 - \binom{p}{2} - p = \binom{p}{2} > 0, \qquad p \geq 2$$

yang membuktikan keberadaan polinomial kuadrat tidak tereduksi.

Contoh 2.5. Untuk $p = 2$ dan $n = 3$, ada dua polinomial monik pangkat tiga yang tidak tereduksi atas Z_2 yaitu $x^3 + x + 1$ dan $x^3 + x^2 + 1$. Misal ambil $f(x) = x^3 + x + 1$ sehingga elemen-elemen $GF(2^3)$ adalah $[0]$, $[1]$, $[x]$,

$[1+x]$, $[x+x^2]$, $[x^2]$, $[1+x^2]$, $[1+x+x^2]$. Jika $a_0+a_1x+a_2x^2$ dilambangkan dengan $(a_0a_1a_2)$ maka elemen-elemen dari $GF(2^3)$ adalah

0	$= (000)$	$x+x^2$	$= (011)$
1	$= (100)$	x^2	$= (001)$
x	$= (010)$	$1+x^2$	$= (101)$
$1+x$	$= (110)$	$1+x+x^2$	$= (111)$

F. Kata Kode (*Codeword*)

Definisi 2.8 (Ling S. & Xing C., 2004 : 5). *Misal* $A=\{a_1,a_2,\dots,a_q\}$ *adalah himpunan berukuran q, yang kemudian disebut alfabet kode dan elemen-elemennya disebut simbol kode.*

1. *Kata (word) q-er dengan panjang* n *atas* A *adalah suatu barisan* $w=w_1w_2\dots w_n$ *dengan* $w_i\in A$ *untuk setiap* i.
2. *Kode blok q-er dengan panjang* n *atas* A *adalah suatu himpunan tidak kosong* C *yang berisi kata dengan panjang n.*
3. *Suatu elemen* C *disebut kata kode dalam* C.

Biasanya alfabet kode yang digunakan diambil dari lapangan hingga F_q dengan order q. Kode atas alfabet kode $F_2=\{0,1\}$ disebut kode biner.

G. Jarak Hamming

Definisi 2.9 (Ling S. & Xing C., 2004 : 9). *Misal x dan y adalah kata kode dengan panjang* n *atas* A . *Jarak Hamming dari* x *ke* y , *dinotasikan dengan* $d(x,y)$ *adalah banyaknya posisi yang berbeda antara* x *dan* y . *Jika* $x=x_1x_2\dots x_n$ *dan* $y=y_1y_2\dots y_n$, *maka*

$$d(x,y)=d(x_1,y_1)+\dots+d(x_n,y_n)$$

dengan x_i *dan* y_i *dianggap sebagai kata dengan panjang* 1, *dan*

$$d(x_i, y_i) = \begin{cases} 1 & jika\ x_i \neq y_i \\ 0 & jika\ x_i = y_i. \end{cases}$$

Berikut adalah contoh penghitungan jarak Hamming dari dua kata kode.

Contoh 2.6. Jika $A = \{0, 1\}$ dan $x = 01010, y = 01101, z = 11101$ maka

$$d(x, y) = 3$$

$$d(y, z) = 1$$

$$d(z, x) = 4$$

Definisi 2.10 (Vanstone dan Oorschot, 1989 : 7). *Jika C suatu kode-*$[n, M]$ *(kode dengan panjang n memuat M kata kode) maka jarak Hamming d dari kode C adalah*

$$d = min\{d(x, y): \ x, y \in C, x \neq y\}.$$

Dengan kata lain, jarak Hamming dari suatu kode adalah jarak minimum antara dua kata kode yang berbeda, atas semua pasang kata kode.

Contoh 2.7. Misalkan $C = \{c_0, c_1, c_2, c_3\}$ dengan

$c_0 = (00000)$ $\quad$ $c_2 = (01011)$

$c_1 = (10110)$ $\quad$ $c_3 = (11101)$

diperoleh

$d(c_0, c_1) = 3$ $\quad$ $d(c_2, c_3) = 3$

$d(c_0, c_2) = 3$

$d(c_0, c_3) = 4$

$d(c_1, c_2) = 4$

$d(c_1, c_3) = 3$

Jadi C mempunyai jarak $d = 3$.

H. Bobot Hamming

Definisi 2.11 (Ling S. & Xing C., 2004 : 46). *Misal x suatu kata kode dalam F_q^n. Bobot Hamming dari x, disimbolkan $wt(x)$, didefinisikan sebagai banyaknya koordinat tak nol di x. Untuk setiap elemen x dari F_q bobot Hamming didefinisikan sebagai berikut:*

$$wt(x) = d(x,0) = \begin{cases} 1 & jika\, x \neq 0 \\ 0 & jika\, x = 0. \end{cases}$$

Jika $x \in F_q^n$ dengan $x = (x_1, x_2, \dots, x_n)$ maka bobot Hamming dari x juga secara ekuivalen didefinisikan sebagai

$$wt(x) = wt(x_1) + wt(x_2) + \cdots + wt(x_n)$$

Definisi 2.12 (Ling S. & Xing C., 2004 : 48). *Jika C suatu kode maka bobot (Hamming) minimum dari C, dilambangkan dengan $wt(C)$ adalah bobot terkecil dari kata kode tak nol dari C.*

Berikut diberikan contoh penghitungan bobot Hamming dari suatu kode.

Contoh 2.8. Misal ada suatu kode biner linear $C = \{0000, 1000, 0100, 1100\}$.

$$wt(1000) = 1$$
$$wt(0100) = 1$$
$$wt(1100) = 2.$$

Sehingga $wt(C) = 1$.

I. Kode Linear

Definisi 2.13 (Ling S. & Xing C., 2004 : 45). *Suatu kode linear $\boldsymbol{C}$ dengan* *panjang* $\boldsymbol{n}$ *atas* $\boldsymbol{F_q}$ *adalah suatu subruang vektor dari ruang vektor* $\boldsymbol{F_q^n}$ *dengan* $\boldsymbol{F_q^n}$ *adalah himpunan semua vektor dengan panjang* $\boldsymbol{n}$ *yang entri-entrinya adalah elemen* $\boldsymbol{F_q}$

$$\boldsymbol{F_q^n} = \{(\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}) : \boldsymbol{v_i} \in \boldsymbol{F_q}\}.$$

Definisi 2.14 (Ling S. & Xing C., 2004 : 46). *Kode* $\boldsymbol{C}(\boldsymbol{n}, \boldsymbol{k})$ *adalah kode linear* $\boldsymbol{C}$ *dengan panjang* $\boldsymbol{n}$ *berdimensi* $\boldsymbol{k}$ *atas* $\boldsymbol{F_q}$ *.*

Contoh 2.9. Berikut ini adalah kode linear:

(i) $C = \{(\lambda, \lambda, \ldots, \lambda) : \lambda \in F_q\}$. Kode ini disebut *repetition code*.

(ii) $C = \{000, 001, 010, 011\}$ dengan $q = 2$.

(iii) $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$ dengan $q = 2$.

(iv) $C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$ dengan $q = 3$.

J. Matriks Generator

Matriks yang digunakan untuk membentuk suatu kode linear adalah matriks generator.

Definisi 2.15 (Vanstone dan Oorschot, 1989 : 51). *Suatu Matriks Generator* G *untuk kode* C (n, k) *adalah matriks* $k \times n$ *yang barisnya merupakan basis ruang vektor dari* C.

Kata kode dari suatu kode linear C (atas lapangan F) dengan matriks generator G adalah semua kombinasi linear (atas F) dari baris-baris G. Kemudian C disebut kode yang dibangun oleh matriks G.

Operasi baris elementer yang dilakukan pada G akan memberikan matriks-matriks yang juga membangun C. Misalnya, jika dapat ditemukan suatu matriks generator yang berbentuk $G = [I_k A]$ dengan I_k adalah matriks identitas $k \times k$ dan A adalah suatu matriks $k \times (n - k)$, maka simbol informasi berada di posisi k pertama dari suatu kata kode. Matriks G dengan bentuk tersebut disebut matriks generator dengan bentuk standar. Tidak dapat dijamin bahwa akan selalu ada G untuk C. Meski demikian, menukar posisi koordinat dari suatu kode C menghasilkan ruang bagian C' yang memiliki bobot dan jarak Hamming yang sama dengan C. Sehingga C dan C' adalah kode yang sama, yang kemudian mendorong adanya definisi berikut, dengan *matriks permutasi* adalah suatu matriks identitas dengan baris atau kolom yang ditukar.

Definisi 2.16 (Vanstone dan Oorschot, 1989:52). *Dua kode-(n, k) C dan C' atas lapangan F dikatakan kode ekuivalen jika ada matriks generator G dan G' untuk C dan C' dan suatu matriks permutasi P dengan ukuran $n \times n$ sedemikian sehingga $G' = GP$.*

Matriks P menukar kolom G, sehingga menukar posisi koordinat di C yang menghasilkan kode C'.

Contoh 2.10. Misal C adalah suatu kode-$(4, 3)$ yang dibangun oleh matriks generator $\tilde{G}$

$$\tilde{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

C' adalah kode-$(4, 3)$ dengan matriks generator

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Dapat ditunjukkan bahwa C dan C' adalah kode ekuivalen sebagai berikut. Dengan operasi baris pada $\tilde{G}$

$$\tilde{G} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} \\ r_2 + r_1 \to r_2 \\ r_3 + r_1 \to r_3 \end{matrix}$$

didapatkan matriks generator lain untuk C yaitu

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Dipilih matriks permutasi yang akan menghasilkan $G' = GP$

$$G' = GP$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} a_9 + a_{13} & a_{10} + a_{14} & a_{11} + a_{15} & a_{12} + a_{16} \\ a_5 + a_{13} & a_6 + a_{14} & a_7 + a_{15} & a_8 + a_{16} \\ a_1 & a_2 & a_3 & a_4 \end{bmatrix}$$

didapatkan

$$P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Perkalian antara matriks G dan matriks P menukar kolom 1 dan 3 dari G, sehingga menukar koordinat 1 dan 3 dari setiap kata kode dari C. Kedua kode tersebut ekuivalen, tetapi tidak identik.

Definisi 2.17 (Vanstone dan Oorschot, 1989 : 54). *Jika C adalah suatu* *kode-*(n,k) *atas lapangan* F *maka komplemen ortogonal* $C^{\perp} = \{\, x \in Vn(F) : x \cdot y = 0$ *untuk semua* $y \in C\}$.

Himpunan $C^{\perp}$ adalah himpunan n-tupel atas F yang ortogonal terhadap setiap vektor di C. Kode $C^{\perp}$ selanjutnya disebut sebagai kode dual dari C.

Definisi 2.18 (Vanstone dan Oorschot, 1989 : 55). *Jika* $G = [I_k A]$ *adalah matriks generator untuk* C, *maka* $H = [-A^T I_{n-k}]$ *adalah matriks generator untuk* $C^{\perp}$.

Contoh 2.11. Kode C adalah kode-$(6,3)$ atas Z_2 yang dibangun oleh

$$\tilde{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Dengan melakukan operasi baris elementer yang sesuai terhadap $\tilde{G}$, didapatkan matriks G yang membangun kode yang sama, dengan

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} = [I_3 A], \qquad A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Matriks generator yang membangun komplemen ortogonal $C^{\perp}$ dari C adalah

$$H = [-A^T I_3] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

K. Matriks *Parity Check*

Definisi 2.19 (Ling S. & Xing C., 2004 : 52). *Matriks Parity Check* H *untuk suatu kode linear* C *adalah matriks generator untuk kode* $C^{\perp}$.

Jika G adalah matriks generator untuk C dan H adalah matriks generator untuk $C^{\perp}$, maka H adalah matriks *parity check* untuk C dan G adalah matriks *parity check* untuk $C^{\perp}$.

Contoh 2.12. Jika $H = [1\ 1\ 1\ 1\ 1]$ adalah matriks *parity check* untuk kode-$(5,4)$ C atas Z_2 maka matriks generator untuk C adalah

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

L. Syndrome

Definisi 2.20 (Ling S. & Xing C., 2004 : 59). *Jika C adalah suatu kode linear dengan panjang n atas F_q dan $u \in F_q^n$ adalah sebarang vektor dengan panjang n, maka koset dari C yang ditentukan oleh u adalah himpunan*

$$C + u = \{v + u : v \in C\}.$$

Grup F_q^n dengan operasi penjumlahan vektor adalah suatu grup abelian berhingga dan kode linear C atas F_q dengan panjang n adalah suatu subgrup dari F_q^n sehingga $C + u = u + C$.

Definisi 2.21 (Ling S. & Xing C., 2004 : 60). *Suatu kata atau kata kode dengan bobot (Hamming) terkecil dalam suatu koset disebut coset leader.*

Definisi 2.22 (Ling S. & Xing C., 2004 : 62). *Misal C adalah suatu kode linear-$[n, k, d]$ atas F_q dan H adalah matriks parity check untuk C, untuk setiap $u \in F_q^n$. Syndrome dari kode u adalah $S(u) = uH^T$.*

Contoh 2.13. Suatu kode-$(6,3)$ C dengan matriks generator dan matriks *parity check*

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$C = \{000000,\ 110100,\ 011010,\ 101001,\ 101110,\ 011101,\ 110011,$
$000111\}$

Tabel 2.1 *Standard Array* kode-(6,3) C

Coset Leader 000000	000000	110100	011010	101001	101110	011101	110011	000111
000001	000001	110101	011011	101000	101111	011100	110010	000110
000010	000010	110110	011000	101011	101100	011111	110001	000101
000100	000100	110000	011110	101101	101010	011001	110111	000011
001000	001000	111100	010010	100001	100110	010101	100011	001111
010000	010000	100100	001010	111001	111110	001101	100011	010111
100000	100000	010100	111010	001001	001110	111101	010011	100111
001100	001100	111000	010110	100101	100010	010001	111111	001011

Semua vektor yang berbobot 1 merupakan coset leader, sehingga leader yang terletak di baris terakhir tidak langsung terlihat dengan jelas. Leader ini dapat diperoleh setelah menghitung semua vektor berbobot 2 dari ketujuh leader yang telah didapatkan.

Untuk menghitung syndrome, digunakan $S(u) = uH^T$ sehingga:

$$S(000000) = [000000]\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [000] \quad S(000001) = [000001]\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [101]$$

$$S(000010) = [000010]\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [011] \quad S(000100) = [000100]\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = [110]$$

$$S(001000) = [001000]\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix} = [001] \quad S(010000) = [010000]\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix} = [010]$$

$$S(100000) = [100000]\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix} = [100] \quad S(001100) = [001100]\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix} = [111]$$

Tabel 2.2 *Coset leader* dan *Syndrome* kode-$(6,3)$ C

Coset Leader	*Syndrome*
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
001100	111

M. Ring Polinomial

Definisi 2.23 (Ling S. & Xing C., 2004 : 22). *Misal F adalah suatu lapangan. Himpunan*

$$F[x] = \left\{\sum_{i=0}^{n} a_i x^i : a_i \in F, n \geq 0\right\}$$

disebut ring polinomial atas F. Suatu elemen dari $F[x]$ disebut suatu polinomial atas F. Dalam polinomial $f(x) = \sum_{i=0}^{n} a_i x^i$, bilangan bulat n disebut derajat dari $f(x)$, dilambangkan dengan $deg(f(x))$, jika $a_n \neq 0$.

Polinomial tak nol $f(x) = \sum_{i=0}^{n} a_i x^i$ berderajat n disebut polinomial monik jika $a_n = 1$. Polinomial $f(x)$ yang berderajat positif disebut *reducible* (atas F)

jika ada dua polinomial $g(x)$ dan $h(x)$ atas F sedemikian sehingga $deg(g(x)) < deg(f(x))$, $deg(h(x)) < deg(f(x))$ dan $f(x) = g(x)h(x)$. Jika syarat-syarat tersebut tidak dipenuhi, polinomial $f(x)$ berderajat positif tersebut disebut *irreducible* atas F.

Contoh 2.14

i. Polinomial $f(x) = x^4 + 2x^6 \in Z_3[x]$ adalah suatu polinomial berderajat 6 yang dapat direduksi karena $f(x) = x^4(1 + 2x^2)$.
ii. Polinomial $g(x) = 1 + x + x^2 \in Z_2[x]$ adalah polinomial berderajat 2 yang tidak tereduksi karena jika $g(x)$ tereduksi maka $g(x)$ akan memiliki faktor linear x atau $x + 1$, yaitu 0 atau 1 akan menjadi akar dari $g(x)$, akan tetapi $g(0) = g(1) = 1 \in Z_2$.
iii. Dengan argumen yang sama dengan poin ii, $1 + x + x^3$ dan $1 + x^2 + x^3$ keduanya tidak tereduksi atas Z_2 karena keduanya tidak memiliki faktor linear.

N. Polinomial Minimal

Definisi 2.24 (Togneri dan deSilva, 2006 : 339)

(i) *Misal F dan G adalah dua lapangan. Lapangan G adalah suatu extension field dari F jika ada suatu isomorfisme ring dari F ke himpunan bagian G.*

(ii) *Polinomial dengan derajat $n \geq 1$ dan koefisien dari x^n adalah 1 disebut polinomial monik.*

(iii) *Jika F suatu lapangan dan α adalah elemen dari F atau extension field dari F, $m(x) \in F[x]$ adalah suatu polinomial monik tidak tereduksi dengan $m(\alpha) = 0$ dan tidak ada polinomial lain dengan derajat yang lebih kecil dari $m(x)$ yang memenuhi $m(\alpha) = 0$, maka $m(x)$ adalah polinomial minimum dari α atas F.*

(iv) *Jika $m(x)$ adalah polinomial minimum dari α atas F, maka $m(x)$ adalah*

faktor dari polinomial lain $p(x)$ *yang memenuhi* $p(\alpha) = 0$.

(v) *Misal* n *saling prima dengan* q, *yaitu* $(n, q) = 1$. *Koset siklotomik dari* q *(atau* q*-koset siklotomik) modulo* n *memuat* i *didefinisikan oleh*

$$C_i = \{(i \cdot q^j (mod\, n)) \in Z_n : j = 0,1, \dots\}.$$

Himpunan bagian $\{i_1, \dots, i_t\}$ dari Z_n disebut himpunan lengkap dari representatif koset siklotomik dari q modulo n jika $C_{i_1}, \dots, C_{i_t}$ berbeda dan $\bigcup_{j=1}^{t} C_{i_j} = Z_n$.

Teorema 2.1. *Jika* α *adalah elemen primitif (generator grup perkalian) dari* F_{q^m} *maka polinomial minimal dari* α^i *terhadap* F_q *adalah*

$$m_i(x) = \prod_{j \in C_i} (x - \alpha^j)$$

dengan C_i *adalah koset siklotomik unik dari q modulo* $q^m - 1$ *yang memuat* i.

Bukti

Langkah 1: α^i adalah akar dari $m_i(x)$ karena $i \in C_i$.

Langkah 2: Misal $m_i(x) = a_o + a_i x + \cdots + a_r x^r$ dengan $a_k \in F_{q^m}$ dan $r = |C_i|$. Dengan memangkatkan setiap koefisien dengan q didapatkan

$$a_0^q + a_1^q x + \cdots + a_r^q x^r = \prod_{j \in C_i} (x - \alpha^{qj}) = \prod_{j \in C_{qi}} (x - \alpha^j)$$

$$= \prod_{j \in C_i} (x - \alpha^j) = m_i(x)$$

Di dalam rumus di atas $C_i = C_{qi}$ sehingga $a_k = a_k^q$ untuk semua $0 \le k \le r$. Artinya, $m_i(x)$ adalah suatu polinomial atas F_q.

Langkah 3: Elemen α adalah suatu elemen primitif, sehingga $\alpha^j \neq \alpha^k$ untuk dua elemen yang berbeda j dan k dari C_i. Sehingga $m_i(x)$ tidak memiliki akar berganda. Kemudian jika $f(x) \in F_q[x]$ dan $f(\alpha^i) = 0$. Berlaku $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ untuk $f_k \in F_q$ maka untuk sebarang $j \in C_i$ ada suatu bilangan bulat l sedemikian sehingga $j \equiv iq^l (\bmod\, q^m - 1)$. Sehingga

$$\begin{aligned} f(\alpha^j) = f\left(\alpha^{iq^l}\right) &= f_0 + f_1\alpha^{iq^l} + \cdots + f_n\alpha^{niq^l} \\ &= f_0^{q^l} + f_1^{q^l}\alpha^{iq^l} + \cdots + f_n^{q^l}\alpha^{niq^l} \\ &= \left(f_0 + f_1\alpha^i + \cdots + f_n\alpha^{ni}\right)^{q^l} \\ &= f(\alpha^i)^{q^l} = 0. \qquad \blacksquare \end{aligned}$$

Langkah yang ketiga mengimplikasikan bahwa $m_i(x)$ adalah pembagi dari $f(x)$.

Ketiga langkah tadi menunjukkan bahwa $m_i(x)$ adalah polinomial minimal dari α^i.

O. Matriks Vandermonde

Definisi 2.25 (Pretzel, 1992 : 203). *Suatu matriks Vandermonde V berukuran $n \times n$ didefinisikan sebagai berikut:*

Baris pertama dari V dapat dipilih secara sebarang:

$$\lambda_{1,} \lambda_2, \ldots, \lambda_n$$

Kemudian keseluruhan matriks adalah

$$V = V(\lambda_1, \ldots, \lambda_n) = \begin{bmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ {\lambda_1}^2 & {\lambda_2}^2 & \cdots & {\lambda_n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ {\lambda_1}^n & {\lambda_2}^n & \cdots & {\lambda_n}^n \end{bmatrix}.$$

Contoh 2.15. Kode BCH (4,3) dengan polynomial generator yang dibentuk dari polynomial primitif $x^4 + x^3 + 1$ atas $GF(16)$ memiliki matriks *parity check* $V = V_{4,3}$. Kolom-kolom matriks tersebut merepresentasikan elemen-elemen tak nol dari $GF(16)$.

Tabel 2.3 Elemen-Elemen $GF(16)$

Bentuk Pangkat	Bentuk Polinomial
0	0
α	α
α^2	α^2
α^3	α^3
α^4	$\alpha^3 + 1$
α^5	$\alpha^3 + \alpha + 1$
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$
α^7	$\alpha^2 + \alpha + 1$
α^8	$\alpha^3 + \alpha^2 + \alpha$
α^9	$\alpha^2 + 1$
α^{10}	$\alpha^3 + \alpha$
α^{11}	$\alpha^3 + \alpha^2 + 1$
α^{12}	$\alpha + 1$
α^{13}	$\alpha^2 + \alpha$
α^{14}	$\alpha^3 + \alpha^2$
$\alpha^{15} = 1$	1

Dengan memilih elemen primitif $\alpha = 2$ diperoleh kolom-kolomnya adalah

$$\begin{bmatrix} 2^i \\ 2^{2i} \\ 2^{3i} \\ 2^{4i} \\ 2^{5i} \\ 2^{6i} \end{bmatrix}$$

jika i berjalan dari 14 sampai 1 maka matriks lengkapnya adalah

$$\begin{bmatrix} 12 & 6 & 3 & 13 & 10 & 5 & 14 & 7 & 15 & 11 & 9 & 8 & 4 & 2 & 1 \\ 6 & 13 & 5 & 7 & 11 & 8 & 2 & 12 & 3 & 10 & 14 & 15 & 9 & 4 & 1 \\ 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 \\ 13 & 7 & 8 & 12 & 10 & 15 & 4 & 6 & 5 & 11 & 2 & 3 & 14 & 9 & 1 \\ 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 \\ 5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1 \end{bmatrix}.$$