BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam sistem komunikasi, suatu pesan yang akan dikirim secara digital biasanya dibuat dalam bentuk sandi atau kode. Dalam pengiriman pesan yang telah diubah dalam bentuk kode sering kali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan (*error*) dalam penerimaan pesan. Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang dapat mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi tersebut diperlukan sistem pengkodean dan pendekodean pesan yang mampu mengkoreksi *error*.

Kode yang digunakan dalam pengkoreksian *error* antara lain adalah kode Hamming untuk mendeteksi dan mengkoreksi kesalahan tunggal (*single error*), kode BHC yang dapat mengkoreksi sampai dua kesalahan (*double error*) secara efektif, kode Reed Solomon yang dapat mengkoreksi *multiple error*. Selain itu juga ada kode Golay yang mampu mengkoreksi sampai *triple error*.

Kode Golay terdiri dari kode Golay biner dan perluasan kode Golay biner yang bekerja atas lapangan berhingga GF_2. Kode Golay [23,12,7]

merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7. Kode ini mampu mengkoreksi sampai tiga *error*. Dalam pendekodean kode Golay [23,12,7] diperlukan algoritma – algoritma untuk mendeteksi dan mengkoreksi sampai tiga *error*. Ada beberapa cara untuk pendekodean kode Golay tersebut, salah satunya dengan menggunakan basis Gröbner. Basis Gröbner adalah basis standar ideal pada ring polinomial

1.2 PERMASALAHAN

Berdasarkan uraian diatas, permasalahan dalam penulisan tugas akhir ini adalah bagaimana menentukan kesalahan pada pendekodean kode Golay biner [23,12,7] dengan basis Gröbner untuk pendeteksian dan pengkoreksian sampai tiga *error*.

1.3 PEMBATASAN MASALAH

Pembahasan tugas akhir ini dipusatkan pada algoritma pendekodean kode Golay biner [23,12,7] dalam pendeteksian dan pengoreksian sampai tiga *error* dengan menggunakan basis Gröbner. Proses pengkodean kode Golay biner [23,12,7] serta pendekodean kode Golay biner [23,12,7] dengan algoritma lain tidak dibahas dalam penulisan tugas akhir ini.

1.4 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah mengoreksi sampai tiga *error* dalam pendekodean kode Golay biner [23,12,7] dengan menggunakan basis Gröbner.

1.5 METODOLOGI PENULISAN

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode literatur, yatu dengan mencari referensi sumber buku, baik melalui media pustaka maupun *download* di internet yang berkaitan dengan sistem pendekodean kode Golay biner [23.12.7].

1.6 SISTEMATIKA PENULISAN

Tugas Akhir ini terdiri dari 4 bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan, dan sistematika penulisan. Bab II berisi teori – teori dasar yang digunakan dalam pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, kode siklik dan kode Golay biner [23,12,7] dan basis Gröbner. Bab III berisi tentang Sistem komunikasi dengan gangguan *channel*, sindrom dalam penentuan pola – pola *error*, basis Gröbner untuk pendekodean dan pendekodean kode Golay biner [23,12,7] dengan basis Gröbner. Bab IV berisi kesimpulan dari seluruh bahasan pada tugas akhir ini.

BAB II

MATERI PENUNJANG

2.1 Ring dan Ring Polinomial

Definisi 2.1.1 [14]

Suatu ring $\langle R,+,\bullet \rangle$ adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi biner yang disajikan dengan tanda jumlahan (+) dan tanda pergandaan ($\bullet$) yang memenuhi aksioma – aksioma di bawah ini :

1). $\langle R,+\rangle$merupakan grup komutatif

2). Terhadap operasi pergandaan memenuhi sifat assosiatif

3). Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

Untuk setiap $x,y,z \in R$ berlaku $x \bullet (y+z) = x \bullet y+x \bullet z$ dan

$(x+y) \bullet z = x \bullet z+y \bullet z$

□

Contoh:

Himpunan semua bilangan bulat Z terhadap operasi jumlahan dan pergandaan, dinotasikan $\langle Z,+, \bullet \rangle$ merupakan ring.

Definisi 2.1.2 [14]

F disebut lapangan (*field)* jika memenuhi aksioma berikut :

1) $\langle F,+,\bullet \rangle$ adalah ring komutatif

2) F terhadap operasi pergandaan "$\bullet$" mempunyai elemen satuan e dan $e \neq 0$

3) Setiap elemen tak nol dari F mempunyai invers terhadap operasi pergandaan

□

Definisi 2.1.3 [14]

Misalkan F lapangan dengan banyaknya elemen berhingga maka F disebut lapangan berhingga (*finite field)*.

□

Contoh:

Z_3 adalah lapangan dengan elemen berhingga, yaitu $\{0, 1, 2\}$.

Definisi 2.1.4 [14]

Diberikan ring R dan S himpunan bagian dari R, maka S disebut ring bagian (sub ring) dari ring R jika S merupakan ring terhadap operasi biner yang sama pada R.

□

Definisi 2.1.5 [14]

Misalkan $I \subseteq R$, R ring, I disebut ideal dari ring R jika memenuhi:

1) I sub ring dari R

2) Untuk setiap $x \in I$, $r \in R$, maka $xr \in I$ dan $rx \in I$

selanjutnya untuk setiap $r \in R$, $Ir = \{xr | x \in I\}$ dengan $Ir \subseteq I$ disebut Ideal kanan dan $rI = \{ rx \mid x \in I\}$ dengan $rI \subseteq I$ disebut Ideal kiri.

□

Contoh:

Didefinisikan $S = \{2k \mid k \in Z\}$ merupakan Ideal dari Z. Ambil $r \in Z$, maka ideal kiri dari *S* adalah

$$rS = \{r(2k) \mid r \in Z\},\ r(2k) = 2(rk) \in S,\ rk \in Z$$

dan ideal kanan dari S adalah

$$Sr = \{(2k)r \mid r \in Z\},\ (2k)r = 2(kr) \in S,\ kr \in Z$$

Definisi 2.1.6 [5]

Diberikan ring komutatif *R* dan *indeterminate x*.

$$R[x] = \{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \mid a_i \in R\}$$

adalah ring polinomial atas *R* dengan *indeterminate x*, dimana n adalah bilangan bulat non negatif dan a_i adalah elemen dari *R*.

□

Dalam definisi ini, *x* tidak menunjukkan sebagai variabel ataupun elemen yang tidak diketahui, tapi untuk menyajikan penempatan yang tepat yang memisahkan elemen ring $a_0, a_1, \ldots, a_n$.

Lapangan berhingga F yang memuat q elemen sering dinotasikan dengan GF(q) yang disebut Galois field (lapangan Galois). q mempunyai bentuk p^n, yaitu q merupakan suatu bilangan prima p atau hasil pemangkatan dari p. Notasi GF(p^n) adalah lapangan dengan karakteristik p. Dalam mengkonstruksi

suatu lapangan berhingga dengan p^n elemen, digunakan suatu polinomial tak tereduksi dengan derajad n dalam $GF_p[x]$.

Teorema 2.1.7 [11]

Jika *F* adalah lapangan berhingga dengan karakteristik p, maka *F* terdiri dari p^n elemen untuk suatu bilangan integer positif n.

Bukti : Lihat [11] dan [15] □

Definisi 2.1.8 [11]

Diberikan lapangan berhingga *F* dan didefinisikan *F** yaitu himpunan elemen – elemen dari *F* yang tidak nol, *F** = F - {0}. Elemen $\alpha \in$ F disebut generator (pembangun) dari *F**, atau disebut primitif elemen (elemen primitif) dari *F* jika

$$\{\alpha^i : i \geq 0\} = F^*$$

Yaitu jika α membangun semua elemen tak nol dalam lapangan *F*.

□

Definisi 2.1.9 [11]

Order suatu elemen tak nol $\alpha \in GF_q$ adalah bilangan bulat positif terkecil t sedemikian hingga $\alpha^t = 1$, ditulis ord(α) = t.

□

Teorema 2.1.10 [11]

Setiap lapangan berhingga $F = GF_q$ mempunyai elemen primitif.

Bukti : Lihat [11] dan [15]□

Contoh:

Diberikan lapangan perluasan GF(2^3) atas GF_2 dan sebuah polinomial *irreducible* $x^3 + x + 1$. Maka GF(2^3) terdiri dari $2^3 = 8$ elemen yaitu {$0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2$}. Jika α adalah elemen primitif dari GF(2^3), akan ditunjukkan bahwa α membangun semua elemen tak nol di dalam GF(2^3).

Polinomial *irreducible* $x^3 + x + 1 \equiv 0 \bmod x^3 + x + 1$, atau $x^3 \equiv x + 1 \bmod x^3 + x + 1$. Maka :

$\alpha^0 = 1$ $\qquad$ $\alpha^4 = x^2 + x$

$\alpha^1 = x$ $\qquad$ $\alpha^5 = x^3 + x^2 = x^2 + x + 1$

$\alpha^2 = x^2$ $\qquad$ $\alpha^6 = x^3 + x^2 + x = x^2 + 1$

$\alpha^3 = x^3 = x + 1$ $\qquad$ $\alpha^7 = x^3 + x = 1$

Terbukti bahwa α membangun semua elemen tak nol di dalam GF(2^3) dan ord(α) = 7 karena $\alpha^7 = 1$.

2.2 Kode Siklik dan Kode Golay

2.2.1 Kode Siklik

Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran siklik. Jika C = (c_0, c_1, ..., c_{n-1}) adalah kodekata dari kode siklik, maka (c_1, c_2, ..., c_{n-1}, c_0) yang merupakan perputaran siklik dari C adalah kodekata juga. Sehingga semua perputaran siklik dari C adalah kodekata.

Definisi 2.2.1.1 [15]

Suatu kode linier (n,k) atas lapangan F adalah subruang berdimensi k dari $V_k(F)$.

□

Contoh:

S_1 = {(0000), (1000), (0100), (1100)}

S_2 = {(0000), (1100), (0011), (1111)}

S_1 dan S_2 adalah kode linier dengan parameter (4,2), sehingga S_1 dan S_2 adalah subruang berdimensi 2 dari $V_4(Z_2)$.

Definisi 2.2.1.2 [15]

Suatu subruang S dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ ...\ a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ ...\ a_{n-1}) \in S$.

□

Definisi 2.2.1.3 [15]

Suatu kode linier C adalah kode siklik jika C adalah subruang siklik

□

Contoh

$S = \{(0000), (1111)\} \subseteq V_4(Z_2)$ adalah kode siklik

S = {(0000000), (1011100), (0101110), (0010111), (1110010), (0111001), (1001011), (1100101)} adalah subruang siklik di $V_7(Z_2)$.

Definisi 2.2.1.4 [10]

Kode siklik adalah kode linier dengan matriks generator

$$G = \begin{bmatrix} koef\ dari\ g(x) \\ koef\ dari\ xg(x) \\ koef\ \ dari\ x^2 g(x) \\ \vdots \\ koef\ dari\ x^{k-1} g(x) \end{bmatrix}$$

Dengan *g(x)* adalah polinomial generator dari kode siklik C(n, k) atas F.

□

Masing – masing kodekata dalam C akan berbentuk *p(x)g(x)*.

Contoh

Misalkan $f(x) = x^7 + 1$. Diberikan kode siklik C(7,4) atas Z_2 dengan generator $g(x) = 1 + x + x^3$. Ruang pesan memuat semua polinomial atas Z_2 denagn derajat paling tinggi 3. Matriks generator untuk C adalah

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{bmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{bmatrix}$$

Akan dikodekan pesan $p(x) = 1 + x^2 + x^3$ akan dikodekan ke dalam C, maka kodekata yang terbentuk

$$p(x)g(x) = (1 + x^2 + x^3)\ (1 + x + x^3\ )$$
$$= (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4-tuple (1011), dikodekan ke kodekata (1011).G = (1111111).

2.2.2 Kode Golay

Kode Golay ditemukan pada tahun 1949 oleh Marcel J.E.Golay. Kode Golay bekerja pada lapangan berhingga (GF) yang ditemukan oleh Evariste Galois (1811 – 1832) seorang ahli matematika berkebangsaan Perancis pada tahun 1930 – an.

Kode Golay merupakan kode yang digunakan untuk mengkoreksi error sampai 3 error dalam sistem komunikasi digital. Kode Golay terdiri dari Kode Golay biner dan perluasan Kode Golay biner yang bekerja atas lapangan berhingga GF2. Kode Golay biner merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7 yang bekerja atas GF2 atau yang biasa disebut juga dengan kode Golay biner [23,12,7]. Kode ini juga dapat mengkoreksi error sampai 3 error.

Dalam kode Golay biner [23,12,7] terdapat 2^{23} kodekata yang mungkin. Tiap kodekata berisi pesan dengan panjang 12, sehingga hanya digunakan 2^{12} kodekata dari 2^{23} kodekata yang mungkin. Setelah pengkodean 12 – digit pesan, terdapat 11 digit redudansi (tambahan) sebagai sisanya. Digit – digit redudansi ini akan memberikan kemampuan pada kodekata untuk mereduksi pengaruh dari channel yang mengalami gangguan yang mana memberikan error – *error* sepanjang proses transmisi pesan.

2.3 Basis Gröbner

Basis Gröbner atau basis standar untuk ideal dari ring polinomial mulai dikenalkan pada tahun 1965 oleh B. Buchberger dan dinamai dari orang yang dihormatinya, yaitu W. Gröbner (1899 – 1980), pembimbing thesisnya. Buchberger juga mengembangkan algoritma pokok untuk menggunakan basis Gröbner.

Setiap himpunan dari polinomial dapat disajikan dalam basis Gröbner. Ada tiga cara untuk mengkonstruksi basis Gröbner, yaitu eliminasi Gauss untuk memecahkan sistem persamaan linier, algoritma *euclidean* untuk menghitung *gcd* dari dua polinomial, dan algoritma simplek untuk pemrograman linier.

Sebelum membicarakan tentang basis Gröbner, terlebih dahulu akan dibahas tentang relasi urutan monomial. Pertama, dibentuk monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dari n-tuple pangkat $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_{\geq 0}^n$. Disini terjadi korespondensi satu – satu antara monomial didalam $K[x_1 ... x_n]$ dan $Z_{\geq 0}^n$. Setiap relasi urutan > yang ditetapkan dalam $\in Z_{\geq 0}^n$ akan memberikan urutan pada monomial, yaitu jika $\alpha > \beta$ maka $x^{\alpha} > x^{\beta}$.

Definisi 2.3.1 [3]

Misalkan $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ dan $\beta = (\beta_1, \beta_2, ..., \beta_n)$. $\alpha, \beta \in Z_{\geq 0}^n$

(i) Order *lexicographic* : $\alpha >_{lex} \beta$ *jika* $\alpha - \beta \in Z^n$ atau bagian bukan nol yang lebih kiri dari $\alpha - \beta$ adalah positif.

(ii) Order *graded lex* : $\alpha >_{grlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $\alpha >_{grlex} \beta$ jika $\alpha >_{lex} \beta$ dan $|\alpha| = |\beta|$.

(iii) Order *graded reverse lex* : $\alpha >_{grevlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $|\alpha| = |\beta|$ dan bagian bukan nol yang lebih kanan dari $\alpha - \beta$ adalah negatif.

□

Contoh:

Diketahui f = {$4xy^2z$, $7x^2z^2$, $5x^3$}, maka jika diurutkan :

(i) $5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z$, karena (3, 0, 0) – (2, 0, 2) = (1, 0, –2) dan (2, 0, 2) – (1, 2, 1) = (1, –2, 1).

(ii) $7x^2z^2 >_{grlex} 4xy^2z >_{grlex} 5x^3$, karena $|2,0,2| = |1,2,1| = 4$ dan $7x^2z^2 >_{lex} 4xy^2z$.

(iii) $4xy^2z >_{grevlex} 7x^2z^2 >_{grevlex} 5x^3$, karena $|1,2,1| = |2,0,2| = 4$ dan (1, 2, 1) – (2, 0, 2) = (–1, 2, –1).

Definisi 2.3.2 [3]

$f = \sum_{\alpha} a_\alpha x^\alpha$ polinomial *non zero* di dalam $K[x]$ dan > adalah urutan monomial,

(i) Derajat tertinggi dari *f* adalah *multideg* (*f*) = max ($\alpha \in Z_{\geq 0}^{n}$, $a_\alpha \neq 0$)

(ii) Koefisien pemimpin (*leading coeficient*) dari *f* adalah *lc* (*f*) = $a_{multideg(f)} \in K$

(iii) Monomial pemimpin (*leading monomial*) dari *f* adalah *lm* (*f*) = $x^{multideg(f)}$

(iv) Pemimpin suku (*Leading term*) dari *f* adalah *lt* (*f*) = *lc(f).lm(f)*

□

Contoh:

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ adalah sebuah polynomial di dalam *K*[*x*] dan > adalah urutan lexicographic. Maka:

Multideg (f) = (3,0,0)

Lc (f) = –5

Lm (f) = x^3

Lt (f) = –5 x^3

Definisi 2.3.3 [16]

Diketahui f, g ∈ *K*[*x*], maka *S* – Polinomial dari f dan g merupakan polinomial *S(f,g)* ∈ *K*[*x*], yaitu:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)}.f - \frac{lcm(lm(f), lm(g))}{lt(g)}.g$$

□

Contoh:

Misalkan $I = \langle f_1, f_2 \rangle \subset K[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$.

S-polinomial dari f_1 dan f_2 adalah:

$$S(f_1, f_2) = \frac{x^2y^3}{x^2y}\left(x^2y + x\right) - \frac{x^2y^3}{xy^3}\left(xy^3 - y\right) = xy + xy^2$$

Berikut ini akan diberikan definisi dari basis Gröbner menurut David Cox, John Little dan donal O'Shea:

Definisi 2.3.4 [3]

Diketahui I ideal pada $K[x]$ dan relasi urutan monomial > pada $K[x]$. himpunan $G = \{g_1, g_2, ..., g_t\} \subset K[x]$ disebut basis Gröbner untuk ideal I terhadap relasi > jika $\langle lt(g_1), ..., lt(g_t)\rangle = \langle lt(I)\rangle$.

□

Dalam definisi lain, $G = \{g_1, g_2, ..., g_t\}$ merupakan basis Gröbner untuk I terhadap relasi >, jika setiap anggota di I dapat dibagi oleh paling sedikit satu anggota G.

Contoh:

Pada contoh sebelumnya diketahui bahwa S-polinomial dari f_1 dan f_2 adalah $xy+xy^2$. Dimana

$$xy + xy^2 = 0\left(x^2y + x\right) + 0\left(xy^3 - y\right) + \left(xy + xy^2\right)$$

$xy+xy^2 \in I$, tapi $xy+xy^2$ tak dapat dibagi oleh f_1 maupun f_2, sehingga $xy+xy^2 \notin \langle f_1, f_2\rangle$, sehingga $\langle f_1, f_2\rangle$ bukan basis Gröbner.

Teorema 2.3.5 [16]

Diketahui I Ideal pada $K[x]$, $f \in K[x]$ dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka terdapat dengan tunggal $r \in K[x]$ sisa pembagian f dengan G dengan sifat:

i. tidak ada suku pada r yang habis dibagi oleh suatu lt(g_i) dengan $g_i \in$ G

ii. terdapat $g \in I$ sedemikian sehingga $f = g + r$.

Bukti: Lihat [3] dan [16]. □

Teorema berikut merupakan akibat dari teorema diatas dan definisi basis Gröbner. Sisa pembagian poliniomial f dengan himpunan polinomial F dinotasikan dengan rem(f,F).

Teorema 2.3.6 [16]

Diketahui I ideal pada $K[x]$, $f \in K[x]$, dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka berlaku $f \in I$ jika dan hanya jika rem(f,G) = 0.

Bukti: Lihat [3] dan [16]. □

Teorema (Kriteria Buchberger) 2.3.7 [16]

Diketahui $I = \langle g_1, g_2, ..., g_t \rangle$ ideal pada $K[x]$. Himpunan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I jika dan hanya jika untuk setiap $1 \leq i, j \leq t$ dengan $i \neq j$ berlaku rem($S(g_i, g_j)$,G) = 0.

Bukti: Lihat [3] dan [16]. □

Contoh

Diketahui ideal I = $\langle f_1, f_2 \rangle \subset Q[x, y]$ dengan $f_1 = x^2 - x$ dan $f_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan relasi terurut lexicographic. *S* – polinomial f_1, f_2 adalah:

$$h = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

Selanjutnya $S(f_1, f_2)$ dibagi dengan f_1 dan f_2

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Sehingga sisa pembagian dengan f_1 dan f_2 adalah

$$\text{rem}(S(f_1, f_2), \{f_1, f_2\}) = y^2 - y$$

menurut kriteria Buchberger, karena $\text{rem}(S(f_1, f_2), \{f_1, f_2\}) \neq 0$, maka $\{f_1, f_2\}$ bukan merupakan basis Gröbner untuk I. namun dengan mengikutsertakan sisa pembagian tersebut, yaitu $f_3 = y^2 - y$, pada himpunan pembangun menjadi $G = \{f_1, f_2, f_3\}$ sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2$$

Dengan memperhatikan bahwa:

$S_1 = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1) f_2 + f_3$

$S_2 = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y) f_2 + (-y) f_3$

$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y) f_1 + (-x) f_3$

Karena untuk i = 1, 2, 3 berlaku rem(S_i, G) = 0, maka menurut kriteria Buchberger, himpunan G = $\{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

Polinomial gagal untuk mempunyai solusi umum jika dan hanya jika $1 \in \langle f_1, f_2, \dots, f_s \rangle$. Misal $\langle g_1, g_2, \dots, g_s \rangle$ adalah basis Gröbner dari $I = \langle 1 \rangle$ maka $1 \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \dots, lt(g_s) \rangle$. Ini menunjukkan bahwa 1 dapat dibagi oleh $lt(g_i)$, ambil saja $lt(g_1)$, maka $lt(g_1)$ konstan. Untuk $lt(g_i)$ lainnya adalah kelipatan dari konstanta tersebut. Sehingga $g_2, \dots, g_s$ dapat dihilangkan dari basis Gröbner. Karena $lt(g_i)$ konstan maka g_i sendiri juga kostan, sebab setiap non konstan monomial adalah lebih besar dari 1. Sehingga g_i dapat digandakan dari konstanta tersebut untuk membuat g_i = 1. Jika G = {1} maka G tidak punya *zero*.

Teorema 2.3.8 [6]

G adalah basis Gröbner monik untuk $\langle P \rangle = \langle p_1, p_2, \dots, p_s \rangle \subseteq F[x]$. P adalah sistem persamaan aljabar, P dapat diselesaikan jika dan hanya jika $1 \notin$ G.

Bukti: Lihat [3] dan [6]. □

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam sistem komunikasi, suatu pesan yang akan dikirim secara digital biasanya dibuat dalam bentuk sandi atau kode. Dalam pengiriman pesan yang telah diubah dalam bentuk kode sering kali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan (*error*) dalam penerimaan pesan. Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang dapat mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi tersebut diperlukan sistem pengkodean dan pendekodean pesan yang mampu mengkoreksi *error*.

Kode yang digunakan dalam pengkoreksian *error* antara lain adalah kode Hamming untuk mendeteksi dan mengkoreksi kesalahan tunggal (*single error*), kode BHC yang dapat mengkoreksi sampai dua kesalahan (*double error*) secara efektif, kode Reed Solomon yang dapat mengkoreksi *multiple error*. Selain itu juga ada kode Golay yang mampu mengkoreksi sampai *triple error*.

Kode Golay terdiri dari kode Golay biner dan perluasan kode Golay biner yang bekerja atas lapangan berhingga GF_2. Kode Golay [23,12,7]

merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7. Kode ini mampu mengkoreksi sampai tiga *error*. Dalam pendekodean kode Golay [23,12,7] diperlukan algoritma – algoritma untuk mendeteksi dan mengkoreksi sampai tiga *error*. Ada beberapa cara untuk pendekodean kode Golay tersebut, salah satunya dengan menggunakan basis Gröbner. Basis Gröbner adalah basis standar ideal pada ring polinomial

1.2 PERMASALAHAN

Berdasarkan uraian diatas, permasalahan dalam penulisan tugas akhir ini adalah bagaimana menentukan kesalahan pada pendekodean kode Golay biner [23,12,7] dengan basis Gröbner untuk pendeteksian dan pengkoreksian sampai tiga *error*.

1.3 PEMBATASAN MASALAH

Pembahasan tugas akhir ini dipusatkan pada algoritma pendekodean kode Golay biner [23,12,7] dalam pendeteksian dan pengoreksian sampai tiga *error* dengan menggunakan basis Gröbner. Proses pengkodean kode Golay biner [23,12,7] serta pendekodean kode Golay biner [23,12,7] dengan algoritma lain tidak dibahas dalam penulisan tugas akhir ini.

1.4 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah mengoreksi sampai tiga *error* dalam pendekodean kode Golay biner [23,12,7] dengan menggunakan basis Gröbner.

1.5 METODOLOGI PENULISAN

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode literatur, yatu dengan mencari referensi sumber buku, baik melalui media pustaka maupun *download* di internet yang berkaitan dengan sistem pendekodean kode Golay biner [23.12.7].

1.6 SISTEMATIKA PENULISAN

Tugas Akhir ini terdiri dari 4 bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan, dan sistematika penulisan. Bab II berisi teori – teori dasar yang digunakan dalam pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, kode siklik dan kode Golay biner [23,12,7] dan basis Gröbner. Bab III berisi tentang Sistem komunikasi dengan gangguan *channel*, sindrom dalam penentuan pola – pola *error*, basis Gröbner untuk pendekodean dan pendekodean kode Golay biner [23,12,7] dengan basis Gröbner. Bab IV berisi kesimpulan dari seluruh bahasan pada tugas akhir ini.

BAB II

MATERI PENUNJANG

2.1 Ring dan Ring Polinomial

Definisi 2.1.1 [14]

Suatu ring $\langle R,+,\bullet \rangle$ adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi biner yang disajikan dengan tanda jumlahan (+) dan tanda pergandaan ($\bullet$) yang memenuhi aksioma – aksioma di bawah ini :

1). $\langle R,+\rangle$merupakan grup komutatif

2). Terhadap operasi pergandaan memenuhi sifat assosiatif

3). Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

Untuk setiap $x,y,z \in R$ berlaku $x \bullet (y+z) = x \bullet y+x \bullet z$ dan

$(x+y) \bullet z = x \bullet z+y \bullet z$

□

Contoh:

Himpunan semua bilangan bulat Z terhadap operasi jumlahan dan pergandaan, dinotasikan $\langle Z,+, \bullet \rangle$ merupakan ring.

Definisi 2.1.2 [14]

F disebut lapangan (*field)* jika memenuhi aksioma berikut :

1) $\langle F,+,\bullet \rangle$ adalah ring komutatif

2) F terhadap operasi pergandaan "$\bullet$" mempunyai elemen satuan e dan $e \neq 0$

3) Setiap elemen tak nol dari F mempunyai invers terhadap operasi pergandaan

□

Definisi 2.1.3 [14]

Misalkan F lapangan dengan banyaknya elemen berhingga maka F disebut lapangan berhingga (*finite field)*.

□

Contoh:

Z_3 adalah lapangan dengan elemen berhingga, yaitu $\{0, 1, 2\}$.

Definisi 2.1.4 [14]

Diberikan ring R dan S himpunan bagian dari R, maka S disebut ring bagian (sub ring) dari ring R jika S merupakan ring terhadap operasi biner yang sama pada R.

□

Definisi 2.1.5 [14]

Misalkan $I \subseteq R$, R ring, I disebut ideal dari ring R jika memenuhi:

1) I sub ring dari R

2) Untuk setiap $x \in I$, $r \in R$, maka $xr \in I$ dan $rx \in I$

selanjutnya untuk setiap $r \in R$, $Ir = \{xr | x \in I\}$ dengan $Ir \subseteq I$ disebut Ideal kanan dan $rI = \{ rx \mid x \in I\}$ dengan $rI \subseteq I$ disebut Ideal kiri.

□

Contoh:

Didefinisikan $S = \{2k \mid k \in Z\}$ merupakan Ideal dari Z. Ambil $r \in Z$, maka ideal kiri dari *S* adalah

$$rS = \{r(2k) \mid r \in Z\},\ r(2k) = 2(rk) \in S,\ rk \in Z$$

dan ideal kanan dari S adalah

$$Sr = \{(2k)r \mid r \in Z\},\ (2k)r = 2(kr) \in S,\ kr \in Z$$

Definisi 2.1.6 [5]

Diberikan ring komutatif *R* dan *indeterminate x*.

$$R[x] = \{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \mid a_i \in R\}$$

adalah ring polinomial atas *R* dengan *indeterminate x*, dimana n adalah bilangan bulat non negatif dan a_i adalah elemen dari *R*.

□

Dalam definisi ini, *x* tidak menunjukkan sebagai variabel ataupun elemen yang tidak diketahui, tapi untuk menyajikan penempatan yang tepat yang memisahkan elemen ring $a_0, a_1, \ldots, a_n$.

Lapangan berhingga F yang memuat q elemen sering dinotasikan dengan GF(q) yang disebut Galois field (lapangan Galois). q mempunyai bentuk p^n, yaitu q merupakan suatu bilangan prima p atau hasil pemangkatan dari p. Notasi GF(p^n) adalah lapangan dengan karakteristik p. Dalam mengkonstruksi

suatu lapangan berhingga dengan p^n elemen, digunakan suatu polinomial tak tereduksi dengan derajad n dalam $GF_p[x]$.

Teorema 2.1.7 [11]

Jika *F* adalah lapangan berhingga dengan karakteristik p, maka *F* terdiri dari p^n elemen untuk suatu bilangan integer positif n.

Bukti : Lihat [11] dan [15] □

Definisi 2.1.8 [11]

Diberikan lapangan berhingga *F* dan didefinisikan *F** yaitu himpunan elemen – elemen dari *F* yang tidak nol, *F** = F - {0}. Elemen $\alpha \in$ F disebut generator (pembangun) dari *F**, atau disebut primitif elemen (elemen primitif) dari *F* jika

$$\{\alpha^i : i \geq 0\} = F^*$$

Yaitu jika α membangun semua elemen tak nol dalam lapangan *F*.

□

Definisi 2.1.9 [11]

Order suatu elemen tak nol $\alpha \in GF_q$ adalah bilangan bulat positif terkecil t sedemikian hingga $\alpha^t = 1$, ditulis ord(α) = t.

□

Teorema 2.1.10 [11]

Setiap lapangan berhingga $F = GF_q$ mempunyai elemen primitif.

Bukti : Lihat [11] dan [15]□

Contoh:

Diberikan lapangan perluasan GF(2^3) atas GF_2 dan sebuah polinomial *irreducible* $x^3 + x + 1$. Maka GF(2^3) terdiri dari $2^3 = 8$ elemen yaitu {$0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2$}. Jika α adalah elemen primitif dari GF(2^3), akan ditunjukkan bahwa α membangun semua elemen tak nol di dalam GF(2^3).

Polinomial *irreducible* $x^3 + x + 1 \equiv 0 \bmod x^3 + x + 1$, atau $x^3 \equiv x + 1 \bmod x^3 + x + 1$. Maka :

$\alpha^0 = 1$ $\qquad$ $\alpha^4 = x^2 + x$

$\alpha^1 = x$ $\qquad$ $\alpha^5 = x^3 + x^2 = x^2 + x + 1$

$\alpha^2 = x^2$ $\qquad$ $\alpha^6 = x^3 + x^2 + x = x^2 + 1$

$\alpha^3 = x^3 = x + 1$ $\qquad$ $\alpha^7 = x^3 + x = 1$

Terbukti bahwa α membangun semua elemen tak nol di dalam GF(2^3) dan ord(α) = 7 karena $\alpha^7 = 1$.

2.2 Kode Siklik dan Kode Golay

2.2.1 Kode Siklik

Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran siklik. Jika C = (c_0, c_1, ..., c_{n-1}) adalah kodekata dari kode siklik, maka (c_1, c_2, ..., c_{n-1}, c_0) yang merupakan perputaran siklik dari C adalah kodekata juga. Sehingga semua perputaran siklik dari C adalah kodekata.

Definisi 2.2.1.1 [15]

Suatu kode linier (n,k) atas lapangan F adalah subruang berdimensi k dari $V_k(F)$.

□

Contoh:

S_1 = {(0000), (1000), (0100), (1100)}

S_2 = {(0000), (1100), (0011), (1111)}

S_1 dan S_2 adalah kode linier dengan parameter (4,2), sehingga S_1 dan S_2 adalah subruang berdimensi 2 dari $V_4(Z_2)$.

Definisi 2.2.1.2 [15]

Suatu subruang S dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ ...\ a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ ...\ a_{n-1}) \in S$.

□

Definisi 2.2.1.3 [15]

Suatu kode linier C adalah kode siklik jika C adalah subruang siklik

□

Contoh

$S = \{(0000), (1111)\} \subseteq V_4(Z_2)$ adalah kode siklik

S = {(0000000), (1011100), (0101110), (0010111), (1110010), (0111001), (1001011), (1100101)} adalah subruang siklik di $V_7(Z_2)$.

Definisi 2.2.1.4 [10]

Kode siklik adalah kode linier dengan matriks generator

$$G = \begin{bmatrix} koef\ dari\ g(x) \\ koef\ dari\ xg(x) \\ koef\ \ dari\ x^2 g(x) \\ \vdots \\ koef\ dari\ x^{k-1} g(x) \end{bmatrix}$$

Dengan *g(x)* adalah polinomial generator dari kode siklik C(n, k) atas F.

□

Masing – masing kodekata dalam C akan berbentuk *p(x)g(x)*.

Contoh

Misalkan $f(x) = x^7 + 1$. Diberikan kode siklik C(7,4) atas Z_2 dengan generator $g(x) = 1 + x + x^3$. Ruang pesan memuat semua polinomial atas Z_2 denagn derajat paling tinggi 3. Matriks generator untuk C adalah

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{bmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{bmatrix}$$

Akan dikodekan pesan $p(x) = 1 + x^2 + x^3$ akan dikodekan ke dalam C, maka kodekata yang terbentuk

$$p(x)g(x) = (1 + x^2 + x^3)\ (1 + x + x^3\ )$$
$$= (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4-tuple (1011), dikodekan ke kodekata (1011).G = (1111111).

2.2.2 Kode Golay

Kode Golay ditemukan pada tahun 1949 oleh Marcel J.E.Golay. Kode Golay bekerja pada lapangan berhingga (GF) yang ditemukan oleh Evariste Galois (1811 – 1832) seorang ahli matematika berkebangsaan Perancis pada tahun 1930 – an.

Kode Golay merupakan kode yang digunakan untuk mengkoreksi error sampai 3 error dalam sistem komunikasi digital. Kode Golay terdiri dari Kode Golay biner dan perluasan Kode Golay biner yang bekerja atas lapangan berhingga GF2. Kode Golay biner merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7 yang bekerja atas GF2 atau yang biasa disebut juga dengan kode Golay biner [23,12,7]. Kode ini juga dapat mengkoreksi error sampai 3 error.

Dalam kode Golay biner [23,12,7] terdapat 2^{23} kodekata yang mungkin. Tiap kodekata berisi pesan dengan panjang 12, sehingga hanya digunakan 2^{12} kodekata dari 2^{23} kodekata yang mungkin. Setelah pengkodean 12 – digit pesan, terdapat 11 digit redudansi (tambahan) sebagai sisanya. Digit – digit redudansi ini akan memberikan kemampuan pada kodekata untuk mereduksi pengaruh dari channel yang mengalami gangguan yang mana memberikan error – *error* sepanjang proses transmisi pesan.

2.3 Basis Gröbner

Basis Gröbner atau basis standar untuk ideal dari ring polinomial mulai dikenalkan pada tahun 1965 oleh B. Buchberger dan dinamai dari orang yang dihormatinya, yaitu W. Gröbner (1899 – 1980), pembimbing thesisnya. Buchberger juga mengembangkan algoritma pokok untuk menggunakan basis Gröbner.

Setiap himpunan dari polinomial dapat disajikan dalam basis Gröbner. Ada tiga cara untuk mengkonstruksi basis Gröbner, yaitu eliminasi Gauss untuk memecahkan sistem persamaan linier, algoritma *euclidean* untuk menghitung *gcd* dari dua polinomial, dan algoritma simplek untuk pemrograman linier.

Sebelum membicarakan tentang basis Gröbner, terlebih dahulu akan dibahas tentang relasi urutan monomial. Pertama, dibentuk monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dari n-tuple pangkat $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_{\geq 0}^n$. Disini terjadi korespondensi satu – satu antara monomial didalam $K[x_1 ... x_n]$ dan $Z_{\geq 0}^n$. Setiap relasi urutan > yang ditetapkan dalam $\in Z_{\geq 0}^n$ akan memberikan urutan pada monomial, yaitu jika $\alpha > \beta$ maka $x^{\alpha} > x^{\beta}$.

Definisi 2.3.1 [3]

Misalkan $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ dan $\beta = (\beta_1, \beta_2, ..., \beta_n)$. $\alpha, \beta \in Z_{\geq 0}^n$

(i) Order *lexicographic* : $\alpha >_{lex} \beta$ *jika* $\alpha - \beta \in Z^n$ atau bagian bukan nol yang lebih kiri dari $\alpha - \beta$ adalah positif.

(ii) Order *graded lex* : $\alpha >_{grlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $\alpha >_{grlex} \beta$ jika $\alpha >_{lex} \beta$ dan $|\alpha| = |\beta|$.

(iii) Order *graded reverse lex* : $\alpha >_{grevlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $|\alpha| = |\beta|$ dan bagian bukan nol yang lebih kanan dari $\alpha - \beta$ adalah negatif.

□

Contoh:

Diketahui f = {$4xy^2z$, $7x^2z^2$, $5x^3$}, maka jika diurutkan :

(i) $5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z$, karena (3, 0, 0) – (2, 0, 2) = (1, 0, –2) dan (2, 0, 2) – (1, 2, 1) = (1, –2, 1).

(ii) $7x^2z^2 >_{grlex} 4xy^2z >_{grlex} 5x^3$, karena $|2,0,2| = |1,2,1| = 4$ dan $7x^2z^2 >_{lex} 4xy^2z$.

(iii) $4xy^2z >_{grevlex} 7x^2z^2 >_{grevlex} 5x^3$, karena $|1,2,1| = |2,0,2| = 4$ dan (1, 2, 1) – (2, 0, 2) = (–1, 2, –1).

Definisi 2.3.2 [3]

$f = \sum_{\alpha} a_\alpha x^\alpha$ polinomial *non zero* di dalam $K[x]$ dan > adalah urutan monomial,

(i) Derajat tertinggi dari *f* adalah *multideg* (*f*) = max ($\alpha \in Z_{\geq 0}^{n}$, $a_\alpha \neq 0$)

(ii) Koefisien pemimpin (*leading coeficient*) dari *f* adalah *lc* (*f*) = $a_{multideg(f)} \in K$

(iii) Monomial pemimpin (*leading monomial*) dari *f* adalah *lm* (*f*) = $x^{multideg(f)}$

(iv) Pemimpin suku (*Leading term*) dari *f* adalah *lt* (*f*) = *lc(f).lm(f)*

□

Contoh:

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ adalah sebuah polynomial di dalam *K*[*x*] dan > adalah urutan lexicographic. Maka:

Multideg (f) = (3,0,0)

Lc (f) = –5

Lm (f) = x^3

Lt (f) = –5 x^3

Definisi 2.3.3 [16]

Diketahui f, g ∈ *K*[*x*], maka *S* – Polinomial dari f dan g merupakan polinomial *S(f,g)* ∈ *K*[*x*], yaitu:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)}.f - \frac{lcm(lm(f), lm(g))}{lt(g)}.g$$

□

Contoh:

Misalkan $I = \langle f_1, f_2 \rangle \subset K[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$.

S-polinomial dari f_1 dan f_2 adalah:

$$S(f_1, f_2) = \frac{x^2y^3}{x^2y}\left(x^2y + x\right) - \frac{x^2y^3}{xy^3}\left(xy^3 - y\right) = xy + xy^2$$

Berikut ini akan diberikan definisi dari basis Gröbner menurut David Cox, John Little dan donal O'Shea:

Definisi 2.3.4 [3]

Diketahui I ideal pada $K[x]$ dan relasi urutan monomial > pada $K[x]$. himpunan $G = \{g_1, g_2, ..., g_t\} \subset K[x]$ disebut basis Gröbner untuk ideal I terhadap relasi > jika $\langle lt(g_1), ..., lt(g_t)\rangle = \langle lt(I)\rangle$.

□

Dalam definisi lain, $G = \{g_1, g_2, ..., g_t\}$ merupakan basis Gröbner untuk I terhadap relasi >, jika setiap anggota di I dapat dibagi oleh paling sedikit satu anggota G.

Contoh:

Pada contoh sebelumnya diketahui bahwa S-polinomial dari f_1 dan f_2 adalah $xy+xy^2$. Dimana

$$xy + xy^2 = 0\left(x^2y + x\right) + 0\left(xy^3 - y\right) + \left(xy + xy^2\right)$$

$xy+xy^2 \in I$, tapi $xy+xy^2$ tak dapat dibagi oleh f_1 maupun f_2, sehingga $xy+xy^2 \notin \langle f_1, f_2\rangle$, sehingga $\langle f_1, f_2\rangle$ bukan basis Gröbner.

Teorema 2.3.5 [16]

Diketahui I Ideal pada $K[x]$, $f \in K[x]$ dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka terdapat dengan tunggal $r \in K[x]$ sisa pembagian f dengan G dengan sifat:

i. tidak ada suku pada r yang habis dibagi oleh suatu lt(g_i) dengan $g_i \in$ G

ii. terdapat $g \in I$ sedemikian sehingga $f = g + r$.

Bukti: Lihat [3] dan [16]. □

Teorema berikut merupakan akibat dari teorema diatas dan definisi basis Gröbner. Sisa pembagian poliniomial f dengan himpunan polinomial F dinotasikan dengan rem(f,F).

Teorema 2.3.6 [16]

Diketahui I ideal pada $K[x]$, $f \in K[x]$, dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka berlaku $f \in I$ jika dan hanya jika rem(f,G) = 0.

Bukti: Lihat [3] dan [16]. □

Teorema (Kriteria Buchberger) 2.3.7 [16]

Diketahui $I = \langle g_1, g_2, ..., g_t \rangle$ ideal pada $K[x]$. Himpunan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I jika dan hanya jika untuk setiap $1 \leq i, j \leq t$ dengan $i \neq j$ berlaku rem($S(g_i, g_j)$,G) = 0.

Bukti: Lihat [3] dan [16]. □

Contoh

Diketahui ideal I = $\langle f_1, f_2 \rangle \subset Q[x, y]$ dengan $f_1 = x^2 - x$ dan $f_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan relasi terurut lexicographic. *S* – polinomial f_1, f_2 adalah:

$$h = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

Selanjutnya $S(f_1, f_2)$ dibagi dengan f_1 dan f_2

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Sehingga sisa pembagian dengan f_1 dan f_2 adalah

$$\text{rem}(S(f_1, f_2), \{f_1, f_2\}) = y^2 - y$$

menurut kriteria Buchberger, karena $\text{rem}(S(f_1, f_2), \{f_1, f_2\}) \neq 0$, maka $\{f_1, f_2\}$ bukan merupakan basis Gröbner untuk I. namun dengan mengikutsertakan sisa pembagian tersebut, yaitu $f_3 = y^2 - y$, pada himpunan pembangun menjadi $G = \{f_1, f_2, f_3\}$ sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2$$

Dengan memperhatikan bahwa:

$S_1 = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1) f_2 + f_3$

$S_2 = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y) f_2 + (-y) f_3$

$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y) f_1 + (-x) f_3$

Karena untuk i = 1, 2, 3 berlaku rem(S_i, G) = 0, maka menurut kriteria Buchberger, himpunan G = $\{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

Polinomial gagal untuk mempunyai solusi umum jika dan hanya jika $1 \in \langle f_1, f_2, \dots, f_s \rangle$. Misal $\langle g_1, g_2, \dots, g_s \rangle$ adalah basis Gröbner dari $I = \langle 1 \rangle$ maka $1 \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \dots, lt(g_s) \rangle$. Ini menunjukkan bahwa 1 dapat dibagi oleh $lt(g_i)$, ambil saja $lt(g_1)$, maka $lt(g_1)$ konstan. Untuk $lt(g_i)$ lainnya adalah kelipatan dari konstanta tersebut. Sehingga $g_2, \dots, g_s$ dapat dihilangkan dari basis Gröbner. Karena $lt(g_i)$ konstan maka g_i sendiri juga kostan, sebab setiap non konstan monomial adalah lebih besar dari 1. Sehingga g_i dapat digandakan dari konstanta tersebut untuk membuat g_i = 1. Jika G = {1} maka G tidak punya *zero*.

Teorema 2.3.8 [6]

G adalah basis Gröbner monik untuk $\langle P \rangle = \langle p_1, p_2, \dots, p_s \rangle \subseteq F[x]$. P adalah sistem persamaan aljabar, P dapat diselesaikan jika dan hanya jika $1 \notin$ G.

Bukti: Lihat [3] dan [6]. □

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam sistem komunikasi, suatu pesan yang akan dikirim secara digital biasanya dibuat dalam bentuk sandi atau kode. Dalam pengiriman pesan yang telah diubah dalam bentuk kode sering kali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan (*error*) dalam penerimaan pesan. Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang dapat mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi tersebut diperlukan sistem pengkodean dan pendekodean pesan yang mampu mengkoreksi *error*.

Kode yang digunakan dalam pengkoreksian *error* antara lain adalah kode Hamming untuk mendeteksi dan mengkoreksi kesalahan tunggal (*single error*), kode BHC yang dapat mengkoreksi sampai dua kesalahan (*double error*) secara efektif, kode Reed Solomon yang dapat mengkoreksi *multiple error*. Selain itu juga ada kode Golay yang mampu mengkoreksi sampai *triple error*.

Kode Golay terdiri dari kode Golay biner dan perluasan kode Golay biner yang bekerja atas lapangan berhingga GF_2. Kode Golay [23,12,7]

merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7. Kode ini mampu mengkoreksi sampai tiga *error*. Dalam pendekodean kode Golay [23,12,7] diperlukan algoritma – algoritma untuk mendeteksi dan mengkoreksi sampai tiga *error*. Ada beberapa cara untuk pendekodean kode Golay tersebut, salah satunya dengan menggunakan basis Gröbner. Basis Gröbner adalah basis standar ideal pada ring polinomial

1.2 PERMASALAHAN

Berdasarkan uraian diatas, permasalahan dalam penulisan tugas akhir ini adalah bagaimana menentukan kesalahan pada pendekodean kode Golay biner [23,12,7] dengan basis Gröbner untuk pendeteksian dan pengkoreksian sampai tiga *error*.

1.3 PEMBATASAN MASALAH

Pembahasan tugas akhir ini dipusatkan pada algoritma pendekodean kode Golay biner [23,12,7] dalam pendeteksian dan pengoreksian sampai tiga *error* dengan menggunakan basis Gröbner. Proses pengkodean kode Golay biner [23,12,7] serta pendekodean kode Golay biner [23,12,7] dengan algoritma lain tidak dibahas dalam penulisan tugas akhir ini.

1.4 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah mengoreksi sampai tiga *error* dalam pendekodean kode Golay biner [23,12,7] dengan menggunakan basis Gröbner.

1.5 METODOLOGI PENULISAN

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode literatur, yatu dengan mencari referensi sumber buku, baik melalui media pustaka maupun *download* di internet yang berkaitan dengan sistem pendekodean kode Golay biner [23.12.7].

1.6 SISTEMATIKA PENULISAN

Tugas Akhir ini terdiri dari 4 bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan, dan sistematika penulisan. Bab II berisi teori – teori dasar yang digunakan dalam pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, kode siklik dan kode Golay biner [23,12,7] dan basis Gröbner. Bab III berisi tentang Sistem komunikasi dengan gangguan *channel*, sindrom dalam penentuan pola – pola *error*, basis Gröbner untuk pendekodean dan pendekodean kode Golay biner [23,12,7] dengan basis Gröbner. Bab IV berisi kesimpulan dari seluruh bahasan pada tugas akhir ini.

BAB II

MATERI PENUNJANG

2.1 Ring dan Ring Polinomial

Definisi 2.1.1 [14]

Suatu ring $\langle R,+,\bullet \rangle$ adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi biner yang disajikan dengan tanda jumlahan (+) dan tanda pergandaan ($\bullet$) yang memenuhi aksioma – aksioma di bawah ini :

1). $\langle R,+\rangle$merupakan grup komutatif

2). Terhadap operasi pergandaan memenuhi sifat assosiatif

3). Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

Untuk setiap $x,y,z \in R$ berlaku $x \bullet (y+z) = x \bullet y+x \bullet z$ dan

$(x+y) \bullet z = x \bullet z+y \bullet z$

□

Contoh:

Himpunan semua bilangan bulat Z terhadap operasi jumlahan dan pergandaan, dinotasikan $\langle Z,+, \bullet \rangle$ merupakan ring.

Definisi 2.1.2 [14]

F disebut lapangan (*field)* jika memenuhi aksioma berikut :

1) $\langle F,+,\bullet \rangle$ adalah ring komutatif

2) F terhadap operasi pergandaan "$\bullet$" mempunyai elemen satuan e dan $e \neq 0$

3) Setiap elemen tak nol dari F mempunyai invers terhadap operasi pergandaan

□

Definisi 2.1.3 [14]

Misalkan F lapangan dengan banyaknya elemen berhingga maka F disebut lapangan berhingga (*finite field)*.

□

Contoh:

Z_3 adalah lapangan dengan elemen berhingga, yaitu $\{0, 1, 2\}$.

Definisi 2.1.4 [14]

Diberikan ring R dan S himpunan bagian dari R, maka S disebut ring bagian (sub ring) dari ring R jika S merupakan ring terhadap operasi biner yang sama pada R.

□

Definisi 2.1.5 [14]

Misalkan $I \subseteq R$, R ring, I disebut ideal dari ring R jika memenuhi:

1) I sub ring dari R

2) Untuk setiap $x \in I$, $r \in R$, maka $xr \in I$ dan $rx \in I$

selanjutnya untuk setiap $r \in R$, $Ir = \{xr | x \in I\}$ dengan $Ir \subseteq I$ disebut Ideal kanan dan $rI = \{ rx \mid x \in I\}$ dengan $rI \subseteq I$ disebut Ideal kiri.

□

Contoh:

Didefinisikan $S = \{2k \mid k \in Z\}$ merupakan Ideal dari Z. Ambil $r \in Z$, maka ideal kiri dari *S* adalah

$$rS = \{r(2k) \mid r \in Z\},\ r(2k) = 2(rk) \in S,\ rk \in Z$$

dan ideal kanan dari S adalah

$$Sr = \{(2k)r \mid r \in Z\},\ (2k)r = 2(kr) \in S,\ kr \in Z$$

Definisi 2.1.6 [5]

Diberikan ring komutatif *R* dan *indeterminate x*.

$$R[x] = \{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \mid a_i \in R\}$$

adalah ring polinomial atas *R* dengan *indeterminate x*, dimana n adalah bilangan bulat non negatif dan a_i adalah elemen dari *R*.

□

Dalam definisi ini, *x* tidak menunjukkan sebagai variabel ataupun elemen yang tidak diketahui, tapi untuk menyajikan penempatan yang tepat yang memisahkan elemen ring $a_0, a_1, \ldots, a_n$.

Lapangan berhingga F yang memuat q elemen sering dinotasikan dengan GF(q) yang disebut Galois field (lapangan Galois). q mempunyai bentuk p^n, yaitu q merupakan suatu bilangan prima p atau hasil pemangkatan dari p. Notasi GF(p^n) adalah lapangan dengan karakteristik p. Dalam mengkonstruksi

suatu lapangan berhingga dengan p^n elemen, digunakan suatu polinomial tak tereduksi dengan derajad n dalam $GF_p[x]$.

Teorema 2.1.7 [11]

Jika *F* adalah lapangan berhingga dengan karakteristik p, maka *F* terdiri dari p^n elemen untuk suatu bilangan integer positif n.

Bukti : Lihat [11] dan [15] □

Definisi 2.1.8 [11]

Diberikan lapangan berhingga *F* dan didefinisikan *F** yaitu himpunan elemen – elemen dari *F* yang tidak nol, *F** = F - {0}. Elemen $\alpha \in$ F disebut generator (pembangun) dari *F**, atau disebut primitif elemen (elemen primitif) dari *F* jika

$$\{\alpha^i : i \geq 0\} = F^*$$

Yaitu jika α membangun semua elemen tak nol dalam lapangan *F*.

□

Definisi 2.1.9 [11]

Order suatu elemen tak nol $\alpha \in GF_q$ adalah bilangan bulat positif terkecil t sedemikian hingga $\alpha^t = 1$, ditulis ord(α) = t.

□

Teorema 2.1.10 [11]

Setiap lapangan berhingga $F = GF_q$ mempunyai elemen primitif.

Bukti : Lihat [11] dan [15]□

Contoh:

Diberikan lapangan perluasan GF(2^3) atas GF_2 dan sebuah polinomial *irreducible* $x^3 + x + 1$. Maka GF(2^3) terdiri dari $2^3 = 8$ elemen yaitu {$0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2$}. Jika α adalah elemen primitif dari GF(2^3), akan ditunjukkan bahwa α membangun semua elemen tak nol di dalam GF(2^3).

Polinomial *irreducible* $x^3 + x + 1 \equiv 0 \bmod x^3 + x + 1$, atau $x^3 \equiv x + 1 \bmod x^3 + x + 1$. Maka :

$\alpha^0 = 1$ $\qquad$ $\alpha^4 = x^2 + x$

$\alpha^1 = x$ $\qquad$ $\alpha^5 = x^3 + x^2 = x^2 + x + 1$

$\alpha^2 = x^2$ $\qquad$ $\alpha^6 = x^3 + x^2 + x = x^2 + 1$

$\alpha^3 = x^3 = x + 1$ $\qquad$ $\alpha^7 = x^3 + x = 1$

Terbukti bahwa α membangun semua elemen tak nol di dalam GF(2^3) dan ord(α) = 7 karena $\alpha^7 = 1$.

2.2 Kode Siklik dan Kode Golay

2.2.1 Kode Siklik

Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran siklik. Jika C = (c_0, c_1, ..., c_{n-1}) adalah kodekata dari kode siklik, maka (c_1, c_2, ..., c_{n-1}, c_0) yang merupakan perputaran siklik dari C adalah kodekata juga. Sehingga semua perputaran siklik dari C adalah kodekata.

Definisi 2.2.1.1 [15]

Suatu kode linier (n,k) atas lapangan F adalah subruang berdimensi k dari $V_k(F)$.

□

Contoh:

S_1 = {(0000), (1000), (0100), (1100)}

S_2 = {(0000), (1100), (0011), (1111)}

S_1 dan S_2 adalah kode linier dengan parameter (4,2), sehingga S_1 dan S_2 adalah subruang berdimensi 2 dari $V_4(Z_2)$.

Definisi 2.2.1.2 [15]

Suatu subruang S dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ ...\ a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ ...\ a_{n-1}) \in S$.

□

Definisi 2.2.1.3 [15]

Suatu kode linier C adalah kode siklik jika C adalah subruang siklik

□

Contoh

$S = \{(0000), (1111)\} \subseteq V_4(Z_2)$ adalah kode siklik

S = {(0000000), (1011100), (0101110), (0010111), (1110010), (0111001), (1001011), (1100101)} adalah subruang siklik di $V_7(Z_2)$.

Definisi 2.2.1.4 [10]

Kode siklik adalah kode linier dengan matriks generator

$$G = \begin{bmatrix} koef\ dari\ g(x) \\ koef\ dari\ xg(x) \\ koef\ \ dari\ x^2 g(x) \\ \vdots \\ koef\ dari\ x^{k-1} g(x) \end{bmatrix}$$

Dengan *g(x)* adalah polinomial generator dari kode siklik C(n, k) atas F.

□

Masing – masing kodekata dalam C akan berbentuk *p(x)g(x)*.

Contoh

Misalkan $f(x) = x^7 + 1$. Diberikan kode siklik C(7,4) atas Z_2 dengan generator $g(x) = 1 + x + x^3$. Ruang pesan memuat semua polinomial atas Z_2 denagn derajat paling tinggi 3. Matriks generator untuk C adalah

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{bmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{bmatrix}$$

Akan dikodekan pesan $p(x) = 1 + x^2 + x^3$ akan dikodekan ke dalam C, maka kodekata yang terbentuk

$$p(x)g(x) = (1 + x^2 + x^3)\ (1 + x + x^3\ )$$
$$= (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4-tuple (1011), dikodekan ke kodekata (1011).G = (1111111).

2.2.2 Kode Golay

Kode Golay ditemukan pada tahun 1949 oleh Marcel J.E.Golay. Kode Golay bekerja pada lapangan berhingga (GF) yang ditemukan oleh Evariste Galois (1811 – 1832) seorang ahli matematika berkebangsaan Perancis pada tahun 1930 – an.

Kode Golay merupakan kode yang digunakan untuk mengkoreksi error sampai 3 error dalam sistem komunikasi digital. Kode Golay terdiri dari Kode Golay biner dan perluasan Kode Golay biner yang bekerja atas lapangan berhingga GF2. Kode Golay biner merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7 yang bekerja atas GF2 atau yang biasa disebut juga dengan kode Golay biner [23,12,7]. Kode ini juga dapat mengkoreksi error sampai 3 error.

Dalam kode Golay biner [23,12,7] terdapat 2^{23} kodekata yang mungkin. Tiap kodekata berisi pesan dengan panjang 12, sehingga hanya digunakan 2^{12} kodekata dari 2^{23} kodekata yang mungkin. Setelah pengkodean 12 – digit pesan, terdapat 11 digit redudansi (tambahan) sebagai sisanya. Digit – digit redudansi ini akan memberikan kemampuan pada kodekata untuk mereduksi pengaruh dari channel yang mengalami gangguan yang mana memberikan error – *error* sepanjang proses transmisi pesan.

2.3 Basis Gröbner

Basis Gröbner atau basis standar untuk ideal dari ring polinomial mulai dikenalkan pada tahun 1965 oleh B. Buchberger dan dinamai dari orang yang dihormatinya, yaitu W. Gröbner (1899 – 1980), pembimbing thesisnya. Buchberger juga mengembangkan algoritma pokok untuk menggunakan basis Gröbner.

Setiap himpunan dari polinomial dapat disajikan dalam basis Gröbner. Ada tiga cara untuk mengkonstruksi basis Gröbner, yaitu eliminasi Gauss untuk memecahkan sistem persamaan linier, algoritma *euclidean* untuk menghitung *gcd* dari dua polinomial, dan algoritma simplek untuk pemrograman linier.

Sebelum membicarakan tentang basis Gröbner, terlebih dahulu akan dibahas tentang relasi urutan monomial. Pertama, dibentuk monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dari n-tuple pangkat $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_{\geq 0}^n$. Disini terjadi korespondensi satu – satu antara monomial didalam $K[x_1 ... x_n]$ dan $Z_{\geq 0}^n$. Setiap relasi urutan > yang ditetapkan dalam $\in Z_{\geq 0}^n$ akan memberikan urutan pada monomial, yaitu jika $\alpha > \beta$ maka $x^{\alpha} > x^{\beta}$.

Definisi 2.3.1 [3]

Misalkan $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ dan $\beta = (\beta_1, \beta_2, ..., \beta_n)$. $\alpha, \beta \in Z_{\geq 0}^n$

(i) Order *lexicographic* : $\alpha >_{lex} \beta$ *jika* $\alpha - \beta \in Z^n$ atau bagian bukan nol yang lebih kiri dari $\alpha - \beta$ adalah positif.

(ii) Order *graded lex* : $\alpha >_{grlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $\alpha >_{grlex} \beta$ jika $\alpha >_{lex} \beta$ dan $|\alpha| = |\beta|$.

(iii) Order *graded reverse lex* : $\alpha >_{grevlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $|\alpha| = |\beta|$ dan bagian bukan nol yang lebih kanan dari $\alpha - \beta$ adalah negatif.

□

Contoh:

Diketahui f = {$4xy^2z$, $7x^2z^2$, $5x^3$}, maka jika diurutkan :

(i) $5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z$, karena (3, 0, 0) – (2, 0, 2) = (1, 0, –2) dan (2, 0, 2) – (1, 2, 1) = (1, –2, 1).

(ii) $7x^2z^2 >_{grlex} 4xy^2z >_{grlex} 5x^3$, karena $|2,0,2| = |1,2,1| = 4$ dan $7x^2z^2 >_{lex} 4xy^2z$.

(iii) $4xy^2z >_{grevlex} 7x^2z^2 >_{grevlex} 5x^3$, karena $|1,2,1| = |2,0,2| = 4$ dan (1, 2, 1) – (2, 0, 2) = (–1, 2, –1).

Definisi 2.3.2 [3]

$f = \sum_{\alpha} a_\alpha x^\alpha$ polinomial *non zero* di dalam $K[x]$ dan > adalah urutan monomial,

(i) Derajat tertinggi dari *f* adalah *multideg* (*f*) = max ($\alpha \in Z_{\geq 0}^{n}$, $a_\alpha \neq 0$)

(ii) Koefisien pemimpin (*leading coeficient*) dari *f* adalah *lc* (*f*) = $a_{multideg(f)} \in K$

(iii) Monomial pemimpin (*leading monomial*) dari *f* adalah *lm* (*f*) = $x^{multideg(f)}$

(iv) Pemimpin suku (*Leading term*) dari *f* adalah *lt* (*f*) = *lc(f).lm(f)*

□

Contoh:

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ adalah sebuah polynomial di dalam *K*[*x*] dan > adalah urutan lexicographic. Maka:

Multideg (f) = (3,0,0)

Lc (f) = –5

Lm (f) = x^3

Lt (f) = –5 x^3

Definisi 2.3.3 [16]

Diketahui f, g ∈ *K*[*x*], maka *S* – Polinomial dari f dan g merupakan polinomial *S(f,g)* ∈ *K*[*x*], yaitu:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)}.f - \frac{lcm(lm(f), lm(g))}{lt(g)}.g$$

□

Contoh:

Misalkan $I = \langle f_1, f_2 \rangle \subset K[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$.

S-polinomial dari f_1 dan f_2 adalah:

$$S(f_1, f_2) = \frac{x^2y^3}{x^2y}\left(x^2y + x\right) - \frac{x^2y^3}{xy^3}\left(xy^3 - y\right) = xy + xy^2$$

Berikut ini akan diberikan definisi dari basis Gröbner menurut David Cox, John Little dan donal O'Shea:

Definisi 2.3.4 [3]

Diketahui I ideal pada $K[x]$ dan relasi urutan monomial > pada $K[x]$. himpunan $G = \{g_1, g_2, ..., g_t\} \subset K[x]$ disebut basis Gröbner untuk ideal I terhadap relasi > jika $\langle lt(g_1), ..., lt(g_t)\rangle = \langle lt(I)\rangle$.

□

Dalam definisi lain, $G = \{g_1, g_2, ..., g_t\}$ merupakan basis Gröbner untuk I terhadap relasi >, jika setiap anggota di I dapat dibagi oleh paling sedikit satu anggota G.

Contoh:

Pada contoh sebelumnya diketahui bahwa S-polinomial dari f_1 dan f_2 adalah $xy+xy^2$. Dimana

$$xy + xy^2 = 0\left(x^2y + x\right) + 0\left(xy^3 - y\right) + \left(xy + xy^2\right)$$

$xy+xy^2 \in I$, tapi $xy+xy^2$ tak dapat dibagi oleh f_1 maupun f_2, sehingga $xy+xy^2 \notin \langle f_1, f_2\rangle$, sehingga $\langle f_1, f_2\rangle$ bukan basis Gröbner.

Teorema 2.3.5 [16]

Diketahui I Ideal pada $K[x]$, $f \in K[x]$ dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka terdapat dengan tunggal $r \in K[x]$ sisa pembagian f dengan G dengan sifat:

i. tidak ada suku pada r yang habis dibagi oleh suatu lt(g_i) dengan $g_i \in$ G

ii. terdapat $g \in I$ sedemikian sehingga $f = g + r$.

Bukti: Lihat [3] dan [16]. □

Teorema berikut merupakan akibat dari teorema diatas dan definisi basis Gröbner. Sisa pembagian poliniomial f dengan himpunan polinomial F dinotasikan dengan rem(f,F).

Teorema 2.3.6 [16]

Diketahui I ideal pada $K[x]$, $f \in K[x]$, dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka berlaku $f \in I$ jika dan hanya jika rem(f,G) = 0.

Bukti: Lihat [3] dan [16]. □

Teorema (Kriteria Buchberger) 2.3.7 [16]

Diketahui $I = \langle g_1, g_2, ..., g_t \rangle$ ideal pada $K[x]$. Himpunan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I jika dan hanya jika untuk setiap $1 \leq i, j \leq t$ dengan $i \neq j$ berlaku rem($S(g_i, g_j)$,G) = 0.

Bukti: Lihat [3] dan [16]. □

Contoh

Diketahui ideal I = $\langle f_1, f_2 \rangle \subset Q[x, y]$ dengan $f_1 = x^2 - x$ dan $f_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan relasi terurut lexicographic. *S* – polinomial f_1, f_2 adalah:

$$h = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

Selanjutnya $S(f_1, f_2)$ dibagi dengan f_1 dan f_2

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Sehingga sisa pembagian dengan f_1 dan f_2 adalah

$$\text{rem}(S(f_1, f_2), \{f_1, f_2\}) = y^2 - y$$

menurut kriteria Buchberger, karena $\text{rem}(S(f_1, f_2), \{f_1, f_2\}) \neq 0$, maka $\{f_1, f_2\}$ bukan merupakan basis Gröbner untuk I. namun dengan mengikutsertakan sisa pembagian tersebut, yaitu $f_3 = y^2 - y$, pada himpunan pembangun menjadi $G = \{f_1, f_2, f_3\}$ sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2$$

Dengan memperhatikan bahwa:

$S_1 = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1) f_2 + f_3$

$S_2 = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y) f_2 + (-y) f_3$

$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y) f_1 + (-x) f_3$

Karena untuk i = 1, 2, 3 berlaku rem(S_i, G) = 0, maka menurut kriteria Buchberger, himpunan G = $\{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

Polinomial gagal untuk mempunyai solusi umum jika dan hanya jika $1 \in \langle f_1, f_2, \dots, f_s \rangle$. Misal $\langle g_1, g_2, \dots, g_s \rangle$ adalah basis Gröbner dari $I = \langle 1 \rangle$ maka $1 \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \dots, lt(g_s) \rangle$. Ini menunjukkan bahwa 1 dapat dibagi oleh $lt(g_i)$, ambil saja $lt(g_1)$, maka $lt(g_1)$ konstan. Untuk $lt(g_i)$ lainnya adalah kelipatan dari konstanta tersebut. Sehingga $g_2, \dots, g_s$ dapat dihilangkan dari basis Gröbner. Karena $lt(g_i)$ konstan maka g_i sendiri juga kostan, sebab setiap non konstan monomial adalah lebih besar dari 1. Sehingga g_i dapat digandakan dari konstanta tersebut untuk membuat g_i = 1. Jika G = {1} maka G tidak punya *zero*.

Teorema 2.3.8 [6]

G adalah basis Gröbner monik untuk $\langle P \rangle = \langle p_1, p_2, \dots, p_s \rangle \subseteq F[x]$. P adalah sistem persamaan aljabar, P dapat diselesaikan jika dan hanya jika $1 \notin$ G.

Bukti: Lihat [3] dan [6]. □

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam sistem komunikasi, suatu pesan yang akan dikirim secara digital biasanya dibuat dalam bentuk sandi atau kode. Dalam pengiriman pesan yang telah diubah dalam bentuk kode sering kali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan (*error*) dalam penerimaan pesan. Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang dapat mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi tersebut diperlukan sistem pengkodean dan pendekodean pesan yang mampu mengkoreksi *error*.

Kode yang digunakan dalam pengkoreksian *error* antara lain adalah kode Hamming untuk mendeteksi dan mengkoreksi kesalahan tunggal (*single error*), kode BHC yang dapat mengkoreksi sampai dua kesalahan (*double error*) secara efektif, kode Reed Solomon yang dapat mengkoreksi *multiple error*. Selain itu juga ada kode Golay yang mampu mengkoreksi sampai *triple error*.

Kode Golay terdiri dari kode Golay biner dan perluasan kode Golay biner yang bekerja atas lapangan berhingga GF_2. Kode Golay [23,12,7]

merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7. Kode ini mampu mengkoreksi sampai tiga *error*. Dalam pendekodean kode Golay [23,12,7] diperlukan algoritma – algoritma untuk mendeteksi dan mengkoreksi sampai tiga *error*. Ada beberapa cara untuk pendekodean kode Golay tersebut, salah satunya dengan menggunakan basis Gröbner. Basis Gröbner adalah basis standar ideal pada ring polinomial

1.2 PERMASALAHAN

Berdasarkan uraian diatas, permasalahan dalam penulisan tugas akhir ini adalah bagaimana menentukan kesalahan pada pendekodean kode Golay biner [23,12,7] dengan basis Gröbner untuk pendeteksian dan pengkoreksian sampai tiga *error*.

1.3 PEMBATASAN MASALAH

Pembahasan tugas akhir ini dipusatkan pada algoritma pendekodean kode Golay biner [23,12,7] dalam pendeteksian dan pengoreksian sampai tiga *error* dengan menggunakan basis Gröbner. Proses pengkodean kode Golay biner [23,12,7] serta pendekodean kode Golay biner [23,12,7] dengan algoritma lain tidak dibahas dalam penulisan tugas akhir ini.

1.4 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah mengoreksi sampai tiga *error* dalam pendekodean kode Golay biner [23,12,7] dengan menggunakan basis Gröbner.

1.5 METODOLOGI PENULISAN

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode literatur, yatu dengan mencari referensi sumber buku, baik melalui media pustaka maupun *download* di internet yang berkaitan dengan sistem pendekodean kode Golay biner [23.12.7].

1.6 SISTEMATIKA PENULISAN

Tugas Akhir ini terdiri dari 4 bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan, dan sistematika penulisan. Bab II berisi teori – teori dasar yang digunakan dalam pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, kode siklik dan kode Golay biner [23,12,7] dan basis Gröbner. Bab III berisi tentang Sistem komunikasi dengan gangguan *channel*, sindrom dalam penentuan pola – pola *error*, basis Gröbner untuk pendekodean dan pendekodean kode Golay biner [23,12,7] dengan basis Gröbner. Bab IV berisi kesimpulan dari seluruh bahasan pada tugas akhir ini.

BAB II

MATERI PENUNJANG

2.1 Ring dan Ring Polinomial

Definisi 2.1.1 [14]

Suatu ring $\langle R,+,\bullet \rangle$ adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi biner yang disajikan dengan tanda jumlahan (+) dan tanda pergandaan ($\bullet$) yang memenuhi aksioma – aksioma di bawah ini :

1). $\langle R,+\rangle$merupakan grup komutatif

2). Terhadap operasi pergandaan memenuhi sifat assosiatif

3). Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

Untuk setiap $x,y,z \in R$ berlaku $x \bullet (y+z) = x \bullet y+x \bullet z$ dan

$(x+y) \bullet z = x \bullet z+y \bullet z$

□

Contoh:

Himpunan semua bilangan bulat Z terhadap operasi jumlahan dan pergandaan, dinotasikan $\langle Z,+, \bullet \rangle$ merupakan ring.

Definisi 2.1.2 [14]

F disebut lapangan (*field)* jika memenuhi aksioma berikut :

1) $\langle F,+,\bullet \rangle$ adalah ring komutatif

2) F terhadap operasi pergandaan "$\bullet$" mempunyai elemen satuan e dan $e \neq 0$

3) Setiap elemen tak nol dari F mempunyai invers terhadap operasi pergandaan

□

Definisi 2.1.3 [14]

Misalkan F lapangan dengan banyaknya elemen berhingga maka F disebut lapangan berhingga (*finite field)*.

□

Contoh:

Z_3 adalah lapangan dengan elemen berhingga, yaitu $\{0, 1, 2\}$.

Definisi 2.1.4 [14]

Diberikan ring R dan S himpunan bagian dari R, maka S disebut ring bagian (sub ring) dari ring R jika S merupakan ring terhadap operasi biner yang sama pada R.

□

Definisi 2.1.5 [14]

Misalkan $I \subseteq R$, R ring, I disebut ideal dari ring R jika memenuhi:

1) I sub ring dari R

2) Untuk setiap $x \in I$, $r \in R$, maka $xr \in I$ dan $rx \in I$

selanjutnya untuk setiap $r \in R$, $Ir = \{xr | x \in I\}$ dengan $Ir \subseteq I$ disebut Ideal kanan dan $rI = \{ rx \mid x \in I\}$ dengan $rI \subseteq I$ disebut Ideal kiri.

□

Contoh:

Didefinisikan $S = \{2k \mid k \in Z\}$ merupakan Ideal dari Z. Ambil $r \in Z$, maka ideal kiri dari *S* adalah

$$rS = \{r(2k) \mid r \in Z\},\ r(2k) = 2(rk) \in S,\ rk \in Z$$

dan ideal kanan dari S adalah

$$Sr = \{(2k)r \mid r \in Z\},\ (2k)r = 2(kr) \in S,\ kr \in Z$$

Definisi 2.1.6 [5]

Diberikan ring komutatif *R* dan *indeterminate x*.

$$R[x] = \{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \mid a_i \in R\}$$

adalah ring polinomial atas *R* dengan *indeterminate x*, dimana n adalah bilangan bulat non negatif dan a_i adalah elemen dari *R*.

□

Dalam definisi ini, *x* tidak menunjukkan sebagai variabel ataupun elemen yang tidak diketahui, tapi untuk menyajikan penempatan yang tepat yang memisahkan elemen ring $a_0, a_1, \ldots, a_n$.

Lapangan berhingga F yang memuat q elemen sering dinotasikan dengan GF(q) yang disebut Galois field (lapangan Galois). q mempunyai bentuk p^n, yaitu q merupakan suatu bilangan prima p atau hasil pemangkatan dari p. Notasi GF(p^n) adalah lapangan dengan karakteristik p. Dalam mengkonstruksi

suatu lapangan berhingga dengan p^n elemen, digunakan suatu polinomial tak tereduksi dengan derajad n dalam $GF_p[x]$.

Teorema 2.1.7 [11]

Jika *F* adalah lapangan berhingga dengan karakteristik p, maka *F* terdiri dari p^n elemen untuk suatu bilangan integer positif n.

Bukti : Lihat [11] dan [15] □

Definisi 2.1.8 [11]

Diberikan lapangan berhingga *F* dan didefinisikan *F** yaitu himpunan elemen – elemen dari *F* yang tidak nol, *F** = F - {0}. Elemen $\alpha \in$ F disebut generator (pembangun) dari *F**, atau disebut primitif elemen (elemen primitif) dari *F* jika

$$\{\alpha^i : i \geq 0\} = F^*$$

Yaitu jika α membangun semua elemen tak nol dalam lapangan *F*.

□

Definisi 2.1.9 [11]

Order suatu elemen tak nol $\alpha \in GF_q$ adalah bilangan bulat positif terkecil t sedemikian hingga $\alpha^t = 1$, ditulis ord(α) = t.

□

Teorema 2.1.10 [11]

Setiap lapangan berhingga $F = GF_q$ mempunyai elemen primitif.

Bukti : Lihat [11] dan [15]□

Contoh:

Diberikan lapangan perluasan GF(2^3) atas GF_2 dan sebuah polinomial *irreducible* $x^3 + x + 1$. Maka GF(2^3) terdiri dari $2^3 = 8$ elemen yaitu {$0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2$}. Jika α adalah elemen primitif dari GF(2^3), akan ditunjukkan bahwa α membangun semua elemen tak nol di dalam GF(2^3).

Polinomial *irreducible* $x^3 + x + 1 \equiv 0 \bmod x^3 + x + 1$, atau $x^3 \equiv x + 1 \bmod x^3 + x + 1$. Maka :

$\alpha^0 = 1$ $\qquad$ $\alpha^4 = x^2 + x$

$\alpha^1 = x$ $\qquad$ $\alpha^5 = x^3 + x^2 = x^2 + x + 1$

$\alpha^2 = x^2$ $\qquad$ $\alpha^6 = x^3 + x^2 + x = x^2 + 1$

$\alpha^3 = x^3 = x + 1$ $\qquad$ $\alpha^7 = x^3 + x = 1$

Terbukti bahwa α membangun semua elemen tak nol di dalam GF(2^3) dan ord(α) = 7 karena $\alpha^7 = 1$.

2.2 Kode Siklik dan Kode Golay

2.2.1 Kode Siklik

Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran siklik. Jika C = (c_0, c_1, ..., c_{n-1}) adalah kodekata dari kode siklik, maka (c_1, c_2, ..., c_{n-1}, c_0) yang merupakan perputaran siklik dari C adalah kodekata juga. Sehingga semua perputaran siklik dari C adalah kodekata.

Definisi 2.2.1.1 [15]

Suatu kode linier (n,k) atas lapangan F adalah subruang berdimensi k dari $V_k(F)$.

□

Contoh:

S_1 = {(0000), (1000), (0100), (1100)}

S_2 = {(0000), (1100), (0011), (1111)}

S_1 dan S_2 adalah kode linier dengan parameter (4,2), sehingga S_1 dan S_2 adalah subruang berdimensi 2 dari $V_4(Z_2)$.

Definisi 2.2.1.2 [15]

Suatu subruang S dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ ...\ a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ ...\ a_{n-1}) \in S$.

□

Definisi 2.2.1.3 [15]

Suatu kode linier C adalah kode siklik jika C adalah subruang siklik

□

Contoh

$S = \{(0000), (1111)\} \subseteq V_4(Z_2)$ adalah kode siklik

S = {(0000000), (1011100), (0101110), (0010111), (1110010), (0111001), (1001011), (1100101)} adalah subruang siklik di $V_7(Z_2)$.

Definisi 2.2.1.4 [10]

Kode siklik adalah kode linier dengan matriks generator

$$G = \begin{bmatrix} koef\ dari\ g(x) \\ koef\ dari\ xg(x) \\ koef\ \ dari\ x^2 g(x) \\ \vdots \\ koef\ dari\ x^{k-1} g(x) \end{bmatrix}$$

Dengan *g(x)* adalah polinomial generator dari kode siklik C(n, k) atas F.

□

Masing – masing kodekata dalam C akan berbentuk *p(x)g(x)*.

Contoh

Misalkan $f(x) = x^7 + 1$. Diberikan kode siklik C(7,4) atas Z_2 dengan generator $g(x) = 1 + x + x^3$. Ruang pesan memuat semua polinomial atas Z_2 denagn derajat paling tinggi 3. Matriks generator untuk C adalah

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{bmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{bmatrix}$$

Akan dikodekan pesan $p(x) = 1 + x^2 + x^3$ akan dikodekan ke dalam C, maka kodekata yang terbentuk

$$p(x)g(x) = (1 + x^2 + x^3)\ (1 + x + x^3\ )$$
$$= (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4-tuple (1011), dikodekan ke kodekata (1011).G = (1111111).

2.2.2 Kode Golay

Kode Golay ditemukan pada tahun 1949 oleh Marcel J.E.Golay. Kode Golay bekerja pada lapangan berhingga (GF) yang ditemukan oleh Evariste Galois (1811 – 1832) seorang ahli matematika berkebangsaan Perancis pada tahun 1930 – an.

Kode Golay merupakan kode yang digunakan untuk mengkoreksi error sampai 3 error dalam sistem komunikasi digital. Kode Golay terdiri dari Kode Golay biner dan perluasan Kode Golay biner yang bekerja atas lapangan berhingga GF2. Kode Golay biner merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7 yang bekerja atas GF2 atau yang biasa disebut juga dengan kode Golay biner [23,12,7]. Kode ini juga dapat mengkoreksi error sampai 3 error.

Dalam kode Golay biner [23,12,7] terdapat 2^{23} kodekata yang mungkin. Tiap kodekata berisi pesan dengan panjang 12, sehingga hanya digunakan 2^{12} kodekata dari 2^{23} kodekata yang mungkin. Setelah pengkodean 12 – digit pesan, terdapat 11 digit redudansi (tambahan) sebagai sisanya. Digit – digit redudansi ini akan memberikan kemampuan pada kodekata untuk mereduksi pengaruh dari channel yang mengalami gangguan yang mana memberikan error – *error* sepanjang proses transmisi pesan.

2.3 Basis Gröbner

Basis Gröbner atau basis standar untuk ideal dari ring polinomial mulai dikenalkan pada tahun 1965 oleh B. Buchberger dan dinamai dari orang yang dihormatinya, yaitu W. Gröbner (1899 – 1980), pembimbing thesisnya. Buchberger juga mengembangkan algoritma pokok untuk menggunakan basis Gröbner.

Setiap himpunan dari polinomial dapat disajikan dalam basis Gröbner. Ada tiga cara untuk mengkonstruksi basis Gröbner, yaitu eliminasi Gauss untuk memecahkan sistem persamaan linier, algoritma *euclidean* untuk menghitung *gcd* dari dua polinomial, dan algoritma simplek untuk pemrograman linier.

Sebelum membicarakan tentang basis Gröbner, terlebih dahulu akan dibahas tentang relasi urutan monomial. Pertama, dibentuk monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dari n-tuple pangkat $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_{\geq 0}^n$. Disini terjadi korespondensi satu – satu antara monomial didalam $K[x_1 ... x_n]$ dan $Z_{\geq 0}^n$. Setiap relasi urutan > yang ditetapkan dalam $\in Z_{\geq 0}^n$ akan memberikan urutan pada monomial, yaitu jika $\alpha > \beta$ maka $x^{\alpha} > x^{\beta}$.

Definisi 2.3.1 [3]

Misalkan $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ dan $\beta = (\beta_1, \beta_2, ..., \beta_n)$. $\alpha, \beta \in Z_{\geq 0}^n$

(i) Order *lexicographic* : $\alpha >_{lex} \beta$ *jika* $\alpha - \beta \in Z^n$ atau bagian bukan nol yang lebih kiri dari $\alpha - \beta$ adalah positif.

(ii) Order *graded lex* : $\alpha >_{grlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $\alpha >_{grlex} \beta$ jika $\alpha >_{lex} \beta$ dan $|\alpha| = |\beta|$.

(iii) Order *graded reverse lex* : $\alpha >_{grevlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $|\alpha| = |\beta|$ dan bagian bukan nol yang lebih kanan dari $\alpha - \beta$ adalah negatif.

□

Contoh:

Diketahui f = {$4xy^2z$, $7x^2z^2$, $5x^3$}, maka jika diurutkan :

(i) $5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z$, karena (3, 0, 0) – (2, 0, 2) = (1, 0, –2) dan (2, 0, 2) – (1, 2, 1) = (1, –2, 1).

(ii) $7x^2z^2 >_{grlex} 4xy^2z >_{grlex} 5x^3$, karena $|2,0,2| = |1,2,1| = 4$ dan $7x^2z^2 >_{lex} 4xy^2z$.

(iii) $4xy^2z >_{grevlex} 7x^2z^2 >_{grevlex} 5x^3$, karena $|1,2,1| = |2,0,2| = 4$ dan (1, 2, 1) – (2, 0, 2) = (–1, 2, –1).

Definisi 2.3.2 [3]

$f = \sum_{\alpha} a_\alpha x^\alpha$ polinomial *non zero* di dalam $K[x]$ dan > adalah urutan monomial,

(i) Derajat tertinggi dari *f* adalah *multideg* (*f*) = max ($\alpha \in Z_{\geq 0}^{n}$, $a_\alpha \neq 0$)

(ii) Koefisien pemimpin (*leading coeficient*) dari *f* adalah *lc* (*f*) = $a_{multideg(f)} \in K$

(iii) Monomial pemimpin (*leading monomial*) dari *f* adalah *lm* (*f*) = $x^{multideg(f)}$

(iv) Pemimpin suku (*Leading term*) dari *f* adalah *lt* (*f*) = *lc(f).lm(f)*

□

Contoh:

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ adalah sebuah polynomial di dalam *K*[*x*] dan > adalah urutan lexicographic. Maka:

Multideg (f) = (3,0,0)

Lc (f) = –5

Lm (f) = x^3

Lt (f) = –5 x^3

Definisi 2.3.3 [16]

Diketahui f, g ∈ *K*[*x*], maka *S* – Polinomial dari f dan g merupakan polinomial *S(f,g)* ∈ *K*[*x*], yaitu:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)}.f - \frac{lcm(lm(f), lm(g))}{lt(g)}.g$$

□

Contoh:

Misalkan $I = \langle f_1, f_2 \rangle \subset K[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$.

S-polinomial dari f_1 dan f_2 adalah:

$$S(f_1, f_2) = \frac{x^2y^3}{x^2y}\left(x^2y + x\right) - \frac{x^2y^3}{xy^3}\left(xy^3 - y\right) = xy + xy^2$$

Berikut ini akan diberikan definisi dari basis Gröbner menurut David Cox, John Little dan donal O'Shea:

Definisi 2.3.4 [3]

Diketahui I ideal pada $K[x]$ dan relasi urutan monomial > pada $K[x]$. himpunan $G = \{g_1, g_2, ..., g_t\} \subset K[x]$ disebut basis Gröbner untuk ideal I terhadap relasi > jika $\langle lt(g_1), ..., lt(g_t)\rangle = \langle lt(I)\rangle$.

□

Dalam definisi lain, $G = \{g_1, g_2, ..., g_t\}$ merupakan basis Gröbner untuk I terhadap relasi >, jika setiap anggota di I dapat dibagi oleh paling sedikit satu anggota G.

Contoh:

Pada contoh sebelumnya diketahui bahwa S-polinomial dari f_1 dan f_2 adalah $xy+xy^2$. Dimana

$$xy + xy^2 = 0\left(x^2y + x\right) + 0\left(xy^3 - y\right) + \left(xy + xy^2\right)$$

$xy+xy^2 \in I$, tapi $xy+xy^2$ tak dapat dibagi oleh f_1 maupun f_2, sehingga $xy+xy^2 \notin \langle f_1, f_2\rangle$, sehingga $\langle f_1, f_2\rangle$ bukan basis Gröbner.

Teorema 2.3.5 [16]

Diketahui I Ideal pada $K[x]$, $f \in K[x]$ dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka terdapat dengan tunggal $r \in K[x]$ sisa pembagian f dengan G dengan sifat:

i. tidak ada suku pada r yang habis dibagi oleh suatu lt(g_i) dengan $g_i \in$ G

ii. terdapat $g \in I$ sedemikian sehingga $f = g + r$.

Bukti: Lihat [3] dan [16]. □

Teorema berikut merupakan akibat dari teorema diatas dan definisi basis Gröbner. Sisa pembagian poliniomial f dengan himpunan polinomial F dinotasikan dengan rem(f,F).

Teorema 2.3.6 [16]

Diketahui I ideal pada $K[x]$, $f \in K[x]$, dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka berlaku $f \in I$ jika dan hanya jika rem(f,G) = 0.

Bukti: Lihat [3] dan [16]. □

Teorema (Kriteria Buchberger) 2.3.7 [16]

Diketahui $I = \langle g_1, g_2, ..., g_t \rangle$ ideal pada $K[x]$. Himpunan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I jika dan hanya jika untuk setiap $1 \leq i, j \leq t$ dengan $i \neq j$ berlaku rem($S(g_i, g_j)$,G) = 0.

Bukti: Lihat [3] dan [16]. □

Contoh

Diketahui ideal I = $\langle f_1, f_2 \rangle \subset Q[x, y]$ dengan $f_1 = x^2 - x$ dan $f_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan relasi terurut lexicographic. *S* – polinomial f_1, f_2 adalah:

$$h = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

Selanjutnya $S(f_1, f_2)$ dibagi dengan f_1 dan f_2

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Sehingga sisa pembagian dengan f_1 dan f_2 adalah

$$\text{rem}(S(f_1, f_2), \{f_1, f_2\}) = y^2 - y$$

menurut kriteria Buchberger, karena $\text{rem}(S(f_1, f_2), \{f_1, f_2\}) \neq 0$, maka $\{f_1, f_2\}$ bukan merupakan basis Gröbner untuk I. namun dengan mengikutsertakan sisa pembagian tersebut, yaitu $f_3 = y^2 - y$, pada himpunan pembangun menjadi $G = \{f_1, f_2, f_3\}$ sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2$$

Dengan memperhatikan bahwa:

$S_1 = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1) f_2 + f_3$

$S_2 = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y) f_2 + (-y) f_3$

$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y) f_1 + (-x) f_3$

Karena untuk i = 1, 2, 3 berlaku rem(S_i, G) = 0, maka menurut kriteria Buchberger, himpunan G = $\{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

Polinomial gagal untuk mempunyai solusi umum jika dan hanya jika $1 \in \langle f_1, f_2, \dots, f_s \rangle$. Misal $\langle g_1, g_2, \dots, g_s \rangle$ adalah basis Gröbner dari $I = \langle 1 \rangle$ maka $1 \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \dots, lt(g_s) \rangle$. Ini menunjukkan bahwa 1 dapat dibagi oleh $lt(g_i)$, ambil saja $lt(g_1)$, maka $lt(g_1)$ konstan. Untuk $lt(g_i)$ lainnya adalah kelipatan dari konstanta tersebut. Sehingga $g_2, \dots, g_s$ dapat dihilangkan dari basis Gröbner. Karena $lt(g_i)$ konstan maka g_i sendiri juga kostan, sebab setiap non konstan monomial adalah lebih besar dari 1. Sehingga g_i dapat digandakan dari konstanta tersebut untuk membuat g_i = 1. Jika G = {1} maka G tidak punya *zero*.

Teorema 2.3.8 [6]

G adalah basis Gröbner monik untuk $\langle P \rangle = \langle p_1, p_2, \dots, p_s \rangle \subseteq F[x]$. P adalah sistem persamaan aljabar, P dapat diselesaikan jika dan hanya jika $1 \notin$ G.

Bukti: Lihat [3] dan [6]. □

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam sistem komunikasi, suatu pesan yang akan dikirim secara digital biasanya dibuat dalam bentuk sandi atau kode. Dalam pengiriman pesan yang telah diubah dalam bentuk kode sering kali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan (*error*) dalam penerimaan pesan. Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang dapat mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi tersebut diperlukan sistem pengkodean dan pendekodean pesan yang mampu mengkoreksi *error*.

Kode yang digunakan dalam pengkoreksian *error* antara lain adalah kode Hamming untuk mendeteksi dan mengkoreksi kesalahan tunggal (*single error*), kode BHC yang dapat mengkoreksi sampai dua kesalahan (*double error*) secara efektif, kode Reed Solomon yang dapat mengkoreksi *multiple error*. Selain itu juga ada kode Golay yang mampu mengkoreksi sampai *triple error*.

Kode Golay terdiri dari kode Golay biner dan perluasan kode Golay biner yang bekerja atas lapangan berhingga GF_2. Kode Golay [23,12,7]

merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7. Kode ini mampu mengkoreksi sampai tiga *error*. Dalam pendekodean kode Golay [23,12,7] diperlukan algoritma – algoritma untuk mendeteksi dan mengkoreksi sampai tiga *error*. Ada beberapa cara untuk pendekodean kode Golay tersebut, salah satunya dengan menggunakan basis Gröbner. Basis Gröbner adalah basis standar ideal pada ring polinomial

1.2 PERMASALAHAN

Berdasarkan uraian diatas, permasalahan dalam penulisan tugas akhir ini adalah bagaimana menentukan kesalahan pada pendekodean kode Golay biner [23,12,7] dengan basis Gröbner untuk pendeteksian dan pengkoreksian sampai tiga *error*.

1.3 PEMBATASAN MASALAH

Pembahasan tugas akhir ini dipusatkan pada algoritma pendekodean kode Golay biner [23,12,7] dalam pendeteksian dan pengoreksian sampai tiga *error* dengan menggunakan basis Gröbner. Proses pengkodean kode Golay biner [23,12,7] serta pendekodean kode Golay biner [23,12,7] dengan algoritma lain tidak dibahas dalam penulisan tugas akhir ini.

1.4 TUJUAN PENULISAN

Tujuan penulisan tugas akhir ini adalah mengoreksi sampai tiga *error* dalam pendekodean kode Golay biner [23,12,7] dengan menggunakan basis Gröbner.

1.5 METODOLOGI PENULISAN

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode literatur, yatu dengan mencari referensi sumber buku, baik melalui media pustaka maupun *download* di internet yang berkaitan dengan sistem pendekodean kode Golay biner [23.12.7].

1.6 SISTEMATIKA PENULISAN

Tugas Akhir ini terdiri dari 4 bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan, dan sistematika penulisan. Bab II berisi teori – teori dasar yang digunakan dalam pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, kode siklik dan kode Golay biner [23,12,7] dan basis Gröbner. Bab III berisi tentang Sistem komunikasi dengan gangguan *channel*, sindrom dalam penentuan pola – pola *error*, basis Gröbner untuk pendekodean dan pendekodean kode Golay biner [23,12,7] dengan basis Gröbner. Bab IV berisi kesimpulan dari seluruh bahasan pada tugas akhir ini.

BAB II

MATERI PENUNJANG

2.1 Ring dan Ring Polinomial

Definisi 2.1.1 [14]

Suatu ring $\langle R,+,\bullet \rangle$ adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi biner yang disajikan dengan tanda jumlahan (+) dan tanda pergandaan ($\bullet$) yang memenuhi aksioma – aksioma di bawah ini :

1). $\langle R,+\rangle$merupakan grup komutatif

2). Terhadap operasi pergandaan memenuhi sifat assosiatif

3). Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

Untuk setiap $x,y,z \in R$ berlaku $x \bullet (y+z) = x \bullet y+x \bullet z$ dan

$(x+y) \bullet z = x \bullet z+y \bullet z$

□

Contoh:

Himpunan semua bilangan bulat Z terhadap operasi jumlahan dan pergandaan, dinotasikan $\langle Z,+, \bullet \rangle$ merupakan ring.

Definisi 2.1.2 [14]

F disebut lapangan (*field)* jika memenuhi aksioma berikut :

1) $\langle F,+,\bullet \rangle$ adalah ring komutatif

2) F terhadap operasi pergandaan "$\bullet$" mempunyai elemen satuan e dan $e \neq 0$

3) Setiap elemen tak nol dari F mempunyai invers terhadap operasi pergandaan

□

Definisi 2.1.3 [14]

Misalkan F lapangan dengan banyaknya elemen berhingga maka F disebut lapangan berhingga (*finite field)*.

□

Contoh:

Z_3 adalah lapangan dengan elemen berhingga, yaitu $\{0, 1, 2\}$.

Definisi 2.1.4 [14]

Diberikan ring R dan S himpunan bagian dari R, maka S disebut ring bagian (sub ring) dari ring R jika S merupakan ring terhadap operasi biner yang sama pada R.

□

Definisi 2.1.5 [14]

Misalkan $I \subseteq R$, R ring, I disebut ideal dari ring R jika memenuhi:

1) I sub ring dari R

2) Untuk setiap $x \in I$, $r \in R$, maka $xr \in I$ dan $rx \in I$

selanjutnya untuk setiap $r \in R$, $Ir = \{xr | x \in I\}$ dengan $Ir \subseteq I$ disebut Ideal kanan dan $rI = \{ rx \mid x \in I\}$ dengan $rI \subseteq I$ disebut Ideal kiri.

□

Contoh:

Didefinisikan $S = \{2k \mid k \in Z\}$ merupakan Ideal dari Z. Ambil $r \in Z$, maka ideal kiri dari *S* adalah

$$rS = \{r(2k) \mid r \in Z\},\ r(2k) = 2(rk) \in S,\ rk \in Z$$

dan ideal kanan dari S adalah

$$Sr = \{(2k)r \mid r \in Z\},\ (2k)r = 2(kr) \in S,\ kr \in Z$$

Definisi 2.1.6 [5]

Diberikan ring komutatif *R* dan *indeterminate x*.

$$R[x] = \{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \mid a_i \in R\}$$

adalah ring polinomial atas *R* dengan *indeterminate x*, dimana n adalah bilangan bulat non negatif dan a_i adalah elemen dari *R*.

□

Dalam definisi ini, *x* tidak menunjukkan sebagai variabel ataupun elemen yang tidak diketahui, tapi untuk menyajikan penempatan yang tepat yang memisahkan elemen ring $a_0, a_1, \ldots, a_n$.

Lapangan berhingga F yang memuat q elemen sering dinotasikan dengan GF(q) yang disebut Galois field (lapangan Galois). q mempunyai bentuk p^n, yaitu q merupakan suatu bilangan prima p atau hasil pemangkatan dari p. Notasi GF(p^n) adalah lapangan dengan karakteristik p. Dalam mengkonstruksi

suatu lapangan berhingga dengan p^n elemen, digunakan suatu polinomial tak tereduksi dengan derajad n dalam $GF_p[x]$.

Teorema 2.1.7 [11]

Jika *F* adalah lapangan berhingga dengan karakteristik p, maka *F* terdiri dari p^n elemen untuk suatu bilangan integer positif n.

Bukti : Lihat [11] dan [15] □

Definisi 2.1.8 [11]

Diberikan lapangan berhingga *F* dan didefinisikan *F** yaitu himpunan elemen – elemen dari *F* yang tidak nol, *F** = F - {0}. Elemen $\alpha \in$ F disebut generator (pembangun) dari *F**, atau disebut primitif elemen (elemen primitif) dari *F* jika

$$\{\alpha^i : i \geq 0\} = F^*$$

Yaitu jika α membangun semua elemen tak nol dalam lapangan *F*.

□

Definisi 2.1.9 [11]

Order suatu elemen tak nol $\alpha \in GF_q$ adalah bilangan bulat positif terkecil t sedemikian hingga $\alpha^t = 1$, ditulis ord(α) = t.

□

Teorema 2.1.10 [11]

Setiap lapangan berhingga $F = GF_q$ mempunyai elemen primitif.

Bukti : Lihat [11] dan [15]□

Contoh:

Diberikan lapangan perluasan GF(2^3) atas GF_2 dan sebuah polinomial *irreducible* $x^3 + x + 1$. Maka GF(2^3) terdiri dari $2^3 = 8$ elemen yaitu {$0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2$}. Jika α adalah elemen primitif dari GF(2^3), akan ditunjukkan bahwa α membangun semua elemen tak nol di dalam GF(2^3).

Polinomial *irreducible* $x^3 + x + 1 \equiv 0 \bmod x^3 + x + 1$, atau $x^3 \equiv x + 1 \bmod x^3 + x + 1$. Maka :

$\alpha^0 = 1$ $\qquad$ $\alpha^4 = x^2 + x$

$\alpha^1 = x$ $\qquad$ $\alpha^5 = x^3 + x^2 = x^2 + x + 1$

$\alpha^2 = x^2$ $\qquad$ $\alpha^6 = x^3 + x^2 + x = x^2 + 1$

$\alpha^3 = x^3 = x + 1$ $\qquad$ $\alpha^7 = x^3 + x = 1$

Terbukti bahwa α membangun semua elemen tak nol di dalam GF(2^3) dan ord(α) = 7 karena $\alpha^7 = 1$.

2.2 Kode Siklik dan Kode Golay

2.2.1 Kode Siklik

Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran siklik. Jika C = (c_0, c_1, ..., c_{n-1}) adalah kodekata dari kode siklik, maka (c_1, c_2, ..., c_{n-1}, c_0) yang merupakan perputaran siklik dari C adalah kodekata juga. Sehingga semua perputaran siklik dari C adalah kodekata.

Definisi 2.2.1.1 [15]

Suatu kode linier (n,k) atas lapangan F adalah subruang berdimensi k dari $V_k(F)$.

□

Contoh:

S_1 = {(0000), (1000), (0100), (1100)}

S_2 = {(0000), (1100), (0011), (1111)}

S_1 dan S_2 adalah kode linier dengan parameter (4,2), sehingga S_1 dan S_2 adalah subruang berdimensi 2 dari $V_4(Z_2)$.

Definisi 2.2.1.2 [15]

Suatu subruang S dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ ...\ a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ ...\ a_{n-1}) \in S$.

□

Definisi 2.2.1.3 [15]

Suatu kode linier C adalah kode siklik jika C adalah subruang siklik

□

Contoh

$S = \{(0000), (1111)\} \subseteq V_4(Z_2)$ adalah kode siklik

S = {(0000000), (1011100), (0101110), (0010111), (1110010), (0111001), (1001011), (1100101)} adalah subruang siklik di $V_7(Z_2)$.

Definisi 2.2.1.4 [10]

Kode siklik adalah kode linier dengan matriks generator

$$G = \begin{bmatrix} koef\ dari\ g(x) \\ koef\ dari\ xg(x) \\ koef\ \ dari\ x^2 g(x) \\ \vdots \\ koef\ dari\ x^{k-1} g(x) \end{bmatrix}$$

Dengan *g(x)* adalah polinomial generator dari kode siklik C(n, k) atas F.

□

Masing – masing kodekata dalam C akan berbentuk *p(x)g(x)*.

Contoh

Misalkan $f(x) = x^7 + 1$. Diberikan kode siklik C(7,4) atas Z_2 dengan generator $g(x) = 1 + x + x^3$. Ruang pesan memuat semua polinomial atas Z_2 denagn derajat paling tinggi 3. Matriks generator untuk C adalah

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{bmatrix} 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 1 \end{bmatrix}$$

Akan dikodekan pesan $p(x) = 1 + x^2 + x^3$ akan dikodekan ke dalam C, maka kodekata yang terbentuk

$$p(x)g(x) = (1 + x^2 + x^3)\ (1 + x + x^3\ )$$
$$= (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4-tuple (1011), dikodekan ke kodekata (1011).G = (1111111).

2.2.2 Kode Golay

Kode Golay ditemukan pada tahun 1949 oleh Marcel J.E.Golay. Kode Golay bekerja pada lapangan berhingga (GF) yang ditemukan oleh Evariste Galois (1811 – 1832) seorang ahli matematika berkebangsaan Perancis pada tahun 1930 – an.

Kode Golay merupakan kode yang digunakan untuk mengkoreksi error sampai 3 error dalam sistem komunikasi digital. Kode Golay terdiri dari Kode Golay biner dan perluasan Kode Golay biner yang bekerja atas lapangan berhingga GF2. Kode Golay biner merupakan kode dengan panjang 23, dimensi 12 dan jarak minimum 7 yang bekerja atas GF2 atau yang biasa disebut juga dengan kode Golay biner [23,12,7]. Kode ini juga dapat mengkoreksi error sampai 3 error.

Dalam kode Golay biner [23,12,7] terdapat 2^{23} kodekata yang mungkin. Tiap kodekata berisi pesan dengan panjang 12, sehingga hanya digunakan 2^{12} kodekata dari 2^{23} kodekata yang mungkin. Setelah pengkodean 12 – digit pesan, terdapat 11 digit redudansi (tambahan) sebagai sisanya. Digit – digit redudansi ini akan memberikan kemampuan pada kodekata untuk mereduksi pengaruh dari channel yang mengalami gangguan yang mana memberikan error – *error* sepanjang proses transmisi pesan.

2.3 Basis Gröbner

Basis Gröbner atau basis standar untuk ideal dari ring polinomial mulai dikenalkan pada tahun 1965 oleh B. Buchberger dan dinamai dari orang yang dihormatinya, yaitu W. Gröbner (1899 – 1980), pembimbing thesisnya. Buchberger juga mengembangkan algoritma pokok untuk menggunakan basis Gröbner.

Setiap himpunan dari polinomial dapat disajikan dalam basis Gröbner. Ada tiga cara untuk mengkonstruksi basis Gröbner, yaitu eliminasi Gauss untuk memecahkan sistem persamaan linier, algoritma *euclidean* untuk menghitung *gcd* dari dua polinomial, dan algoritma simplek untuk pemrograman linier.

Sebelum membicarakan tentang basis Gröbner, terlebih dahulu akan dibahas tentang relasi urutan monomial. Pertama, dibentuk monomial $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dari n-tuple pangkat $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_{\geq 0}^n$. Disini terjadi korespondensi satu – satu antara monomial didalam $K[x_1 ... x_n]$ dan $Z_{\geq 0}^n$. Setiap relasi urutan > yang ditetapkan dalam $\in Z_{\geq 0}^n$ akan memberikan urutan pada monomial, yaitu jika $\alpha > \beta$ maka $x^{\alpha} > x^{\beta}$.

Definisi 2.3.1 [3]

Misalkan $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ dan $\beta = (\beta_1, \beta_2, ..., \beta_n)$. $\alpha, \beta \in Z_{\geq 0}^n$

(i) Order *lexicographic* : $\alpha >_{lex} \beta$ *jika* $\alpha - \beta \in Z^n$ atau bagian bukan nol yang lebih kiri dari $\alpha - \beta$ adalah positif.

(ii) Order *graded lex* : $\alpha >_{grlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $\alpha >_{grlex} \beta$ jika $\alpha >_{lex} \beta$ dan $|\alpha| = |\beta|$.

(iii) Order *graded reverse lex* : $\alpha >_{grevlex} \beta$ jika $|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|$ atau $|\alpha| = |\beta|$ dan bagian bukan nol yang lebih kanan dari $\alpha - \beta$ adalah negatif.

□

Contoh:

Diketahui f = {$4xy^2z$, $7x^2z^2$, $5x^3$}, maka jika diurutkan :

(i) $5x^3 >_{lex} 7x^2z^2 >_{lex} 4xy^2z$, karena (3, 0, 0) – (2, 0, 2) = (1, 0, –2) dan (2, 0, 2) – (1, 2, 1) = (1, –2, 1).

(ii) $7x^2z^2 >_{grlex} 4xy^2z >_{grlex} 5x^3$, karena $|2,0,2| = |1,2,1| = 4$ dan $7x^2z^2 >_{lex} 4xy^2z$.

(iii) $4xy^2z >_{grevlex} 7x^2z^2 >_{grevlex} 5x^3$, karena $|1,2,1| = |2,0,2| = 4$ dan (1, 2, 1) – (2, 0, 2) = (–1, 2, –1).

Definisi 2.3.2 [3]

$f = \sum_{\alpha} a_\alpha x^\alpha$ polinomial *non zero* di dalam $K[x]$ dan > adalah urutan monomial,

(i) Derajat tertinggi dari *f* adalah *multideg* (*f*) = max ($\alpha \in Z_{\geq 0}^{n}$, $a_\alpha \neq 0$)

(ii) Koefisien pemimpin (*leading coeficient*) dari *f* adalah *lc* (*f*) = $a_{multideg(f)} \in K$

(iii) Monomial pemimpin (*leading monomial*) dari *f* adalah *lm* (*f*) = $x^{multideg(f)}$

(iv) Pemimpin suku (*Leading term*) dari *f* adalah *lt* (*f*) = *lc(f).lm(f)*

□

Contoh:

$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ adalah sebuah polynomial di dalam *K*[*x*] dan > adalah urutan lexicographic. Maka:

Multideg (f) = (3,0,0)

Lc (f) = –5

Lm (f) = x^3

Lt (f) = –5 x^3

Definisi 2.3.3 [16]

Diketahui f, g ∈ *K*[*x*], maka *S* – Polinomial dari f dan g merupakan polinomial *S(f,g)* ∈ *K*[*x*], yaitu:

$$S(f,g) = \frac{lcm(lm(f), lm(g))}{lt(f)}.f - \frac{lcm(lm(f), lm(g))}{lt(g)}.g$$

□

Contoh:

Misalkan $I = \langle f_1, f_2 \rangle \subset K[x, y]$ dengan $f_1 = x^2y + x$ dan $f_2 = xy^3 - y$.

S-polinomial dari f_1 dan f_2 adalah:

$$S(f_1, f_2) = \frac{x^2y^3}{x^2y}\left(x^2y + x\right) - \frac{x^2y^3}{xy^3}\left(xy^3 - y\right) = xy + xy^2$$

Berikut ini akan diberikan definisi dari basis Gröbner menurut David Cox, John Little dan donal O'Shea:

Definisi 2.3.4 [3]

Diketahui I ideal pada $K[x]$ dan relasi urutan monomial > pada $K[x]$. himpunan $G = \{g_1, g_2, ..., g_t\} \subset K[x]$ disebut basis Gröbner untuk ideal I terhadap relasi > jika $\langle lt(g_1), ..., lt(g_t)\rangle = \langle lt(I)\rangle$.

□

Dalam definisi lain, $G = \{g_1, g_2, ..., g_t\}$ merupakan basis Gröbner untuk I terhadap relasi >, jika setiap anggota di I dapat dibagi oleh paling sedikit satu anggota G.

Contoh:

Pada contoh sebelumnya diketahui bahwa S-polinomial dari f_1 dan f_2 adalah $xy+xy^2$. Dimana

$$xy + xy^2 = 0\left(x^2y + x\right) + 0\left(xy^3 - y\right) + \left(xy + xy^2\right)$$

$xy+xy^2 \in I$, tapi $xy+xy^2$ tak dapat dibagi oleh f_1 maupun f_2, sehingga $xy+xy^2 \notin \langle f_1, f_2\rangle$, sehingga $\langle f_1, f_2\rangle$ bukan basis Gröbner.

Teorema 2.3.5 [16]

Diketahui I Ideal pada $K[x]$, $f \in K[x]$ dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka terdapat dengan tunggal $r \in K[x]$ sisa pembagian f dengan G dengan sifat:

i. tidak ada suku pada r yang habis dibagi oleh suatu lt(g_i) dengan $g_i \in$ G

ii. terdapat $g \in I$ sedemikian sehingga $f = g + r$.

Bukti: Lihat [3] dan [16]. □

Teorema berikut merupakan akibat dari teorema diatas dan definisi basis Gröbner. Sisa pembagian poliniomial f dengan himpunan polinomial F dinotasikan dengan rem(f,F).

Teorema 2.3.6 [16]

Diketahui I ideal pada $K[x]$, $f \in K[x]$, dan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I, maka berlaku $f \in I$ jika dan hanya jika rem(f,G) = 0.

Bukti: Lihat [3] dan [16]. □

Teorema (Kriteria Buchberger) 2.3.7 [16]

Diketahui $I = \langle g_1, g_2, ..., g_t \rangle$ ideal pada $K[x]$. Himpunan G = $\{g_1, g_2, ..., g_t\} \subset K[x]$ merupakan basis Gröbner untuk I jika dan hanya jika untuk setiap $1 \leq i, j \leq t$ dengan $i \neq j$ berlaku rem($S(g_i, g_j)$,G) = 0.

Bukti: Lihat [3] dan [16]. □

Contoh

Diketahui ideal I = $\langle f_1, f_2 \rangle \subset Q[x, y]$ dengan $f_1 = x^2 - x$ dan $f_2 = x - y$. Akan dicari basis Gröbner G untuk I dengan menggunakan relasi terurut lexicographic. *S* – polinomial f_1, f_2 adalah:

$$h = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

Selanjutnya $S(f_1, f_2)$ dibagi dengan f_1 dan f_2

$$xy - x = 0(x^2 - x) + (y - 1)(x - y) + (y^2 - y)$$

Sehingga sisa pembagian dengan f_1 dan f_2 adalah

$$\text{rem}(S(f_1, f_2), \{f_1, f_2\}) = y^2 - y$$

menurut kriteria Buchberger, karena $\text{rem}(S(f_1, f_2), \{f_1, f_2\}) \neq 0$, maka $\{f_1, f_2\}$ bukan merupakan basis Gröbner untuk I. namun dengan mengikutsertakan sisa pembagian tersebut, yaitu $f_3 = y^2 - y$, pada himpunan pembangun menjadi $G = \{f_1, f_2, f_3\}$ sehingga diperoleh:

$$S_1 = S(f_1, f_2) = \frac{x^2}{x^2}(x^2 - x) - \frac{x^2}{x}(x - y) = xy - x$$

$$S_2 = S(f_2, f_3) = \frac{xy^2}{x}(x - y) - \frac{xy^2}{y^2}(y^2 - y) = xy - y^3$$

$$S_3 = S(f_1, f_3) = \frac{x^2y^2}{x^2}(x^2 - x) - \frac{x^2y^2}{y^2}(y^2 - y) = x^2y - xy^2$$

Dengan memperhatikan bahwa:

$S_1 = xy - x = (y - 1)(x - y) + (y^2 - y) = (y - 1) f_2 + f_3$

$S_2 = xy - y^3 = (y)(x - y) + (-y)(y^2 - y) = (y) f_2 + (-y) f_3$

$S_3 = x^2y - xy^2 = (y)(x^2 - x) + (-x)(y^2 - y) = (y) f_1 + (-x) f_3$

Karena untuk i = 1, 2, 3 berlaku rem(S_i, G) = 0, maka menurut kriteria Buchberger, himpunan G = $\{x^2 - x, x - y, y^2 - y\}$ merupakan basis Gröbner untuk ideal $I = \langle x^2 - x, x - y \rangle$.

Polinomial gagal untuk mempunyai solusi umum jika dan hanya jika $1 \in \langle f_1, f_2, \dots, f_s \rangle$. Misal $\langle g_1, g_2, \dots, g_s \rangle$ adalah basis Gröbner dari $I = \langle 1 \rangle$ maka $1 \in \langle lt(I) \rangle = \langle lt(g_1), lt(g_2), \dots, lt(g_s) \rangle$. Ini menunjukkan bahwa 1 dapat dibagi oleh $lt(g_i)$, ambil saja $lt(g_1)$, maka $lt(g_1)$ konstan. Untuk $lt(g_i)$ lainnya adalah kelipatan dari konstanta tersebut. Sehingga $g_2, \dots, g_s$ dapat dihilangkan dari basis Gröbner. Karena $lt(g_i)$ konstan maka g_i sendiri juga kostan, sebab setiap non konstan monomial adalah lebih besar dari 1. Sehingga g_i dapat digandakan dari konstanta tersebut untuk membuat g_i = 1. Jika G = {1} maka G tidak punya *zero*.

Teorema 2.3.8 [6]

G adalah basis Gröbner monik untuk $\langle P \rangle = \langle p_1, p_2, \dots, p_s \rangle \subseteq F[x]$. P adalah sistem persamaan aljabar, P dapat diselesaikan jika dan hanya jika $1 \notin$ G.

Bukti: Lihat [3] dan [6]. □