BAB I

PENDAHULUAN

1.1 Latar Belakang

Sekarang ini teknologi untuk berkomunikasi sangatlah mudah. Penyampaian pesan dapat dilakukan dengan media telephone, handphone, internet, dan berbagai macam peralatan penyampai pesan dalam bentuk digital. Suatu pesan dalam dunia digital biasanya dibuat dalam bentuk kode atau sandi. . Kode adalah daftar kata atau simbol yang mengganti secara khusus kata lain. Dalam proses pengiriman pesan yang telah diubah kedalam bentuk kode sering mengalami gangguan (*noise*) sehingga menyebabkan pesan yang diterima keliru.

Kesalahan (*error*) merupakan masalah dalam sistem komunikasi karena dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan suatu sistem yang mampu untuk mengkoreksi *error*. Oleh karena itu, pada sistem komunikasi diperlukan sistem pengkodean.

Kode yang biasa digunakan dalam proses koreksi *error* antara lain kode Hamming yang mampu mengkoreksi satu kesalahan (*single error*), kode BCH yang mampu mengkoreksi dua kesalahan (*double error*), kode Golay yang mampu mengkoreksi tiga kesalahan (*triple error*),dan juga terdapat kode Reed Solomon yang mampu mengkoreksi *multiple error*.

Kode residu kuadratik adalah kode yang dibentuk dari kode BCH dan kode Red Solomon. Untuk memecahkan kode residu kuadratik tersebut dapat

digunakan beberapa metode. Salah satunya adalah melalui algoritma Berlekamp Massey yang dapat mengoreksi letak kesalahan yang terdapat pada kode residu kuadratik tersebut.

1.2 Permasalahan

Berdasarkan apa yang telah diuraikan diatas, permasalahan yang dikemukakan pada tugas akhir kali ini adalah bagaimana menentukan kesalahan peletakan kode residu kuadratik *(QR codes)* dengan menggunakan algorima Berlekamp Massey.

1.3 Pembatasan Masalah

Pembahasan tugas akhir ini hanya dibatasi pada pencarian kesalahan peletakan kode residu kuadratik biner (23, 12, 7) dengan menggunakan algoritma Berlekamp- Massey. Penggunaan algoritma Berlekamp Massey untuk mencari kesalahan peletakan kode residu kuadratik yang lain tidak akan dibahas.

1.4 Tujuan Penulisan

Penulisan tugas akhir ini bertujuan untuk menentuan kesalahan peletakan kode residu kuadratik biner dengan algoritma Berlekamp Massey.

1.5 Sistematika penulisan

Tugas akhir ini terdiri dari empat bab. Bab I berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan dan sistematika penulisan. Bab II berisi tentang teori-teori yang mendasari pembahasan tugas akhir ini yang meliputi ring dan ring polinomial, faktorisasi x^n-1, residu kuadratik dan polinomial pembangkit, serta kode. Bab III berisi tentang sindrom dan kesalahan peletakan *(error locator)*, metode pemecahan kode residu kuadratik biner serta kasus penentuan kesalahan peletakan kode residu kuadratik biner dengan algoritma Berlekamp Massey, dan yang terakhir Bab IV berisi kesimpulan dari pembahasan yang sudah dilakukan pada tugas akhir ini.

BAB II

TEORI PENUNJANG

2.1 RING DAN RING POLINOMIAL

Definisi 2.1.1 [11]

Suatu *ring* $\langle R,+,\bullet \rangle$ adalah himpunan tidak kosong R yang dilengkapi dengan dua operasi biner yang disajikan dengan tanda jumlahan (“+”) dan tanda perkalian $("\bullet")$ yang memenuhi aksioma-aksioma di bawah ini :

i. $\langle R,+ \rangle$ merupakan grup komutatif (grup *abelian*).

ii. Terhadap operasi perkalian memenuhi sifat asosiatif.

iii. Memenuhi sifat distributif kiri dan distributif kanan, yaitu :

untuk setiap $x, y, z \in R$ berlaku :

$x\,(y + z) = x\,y + x\,z$ dan

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

Suatu ring $\langle R,+,\bullet \rangle$ dikatakan ring komutatif jika operasi perkalian $("\bullet")$ pada R bersifat komutatif, yaitu:

Untuk setiap $x, y \in R$ sedemikian sehingga $x \bullet y = y \bullet x$.

Selanjutnya tipe khusus dari *ring* akan didefinisikan sebagai berikut.

Definisi 2.1.2 [7]

Himpunan *F* adalah sebuah lapangan *(field)* jika memenuhi syarat-syarat berikut:

i. *F* adalah *ring* komutatif

ii. *F* mempunyai elemen satuan e dan $e \neq 0$

iii. Setiap elemen tak nol dari F mempunyai invers terhadap perkalian.

Lapangan dengan elemen berhingga disebut lapangan berhingga atau disebut lapangan *Galois (Galois Field).* Lapangan berhingga dangan *q* elemen, dinotasikan dengan $GF_{(q)}$ yang menunjukkan *Galois Field* dengan *q* elemen. Dimana *q* haruslah dalam bentuk p^n yaitu bilangan prima atau pangkat prima.

Definisi 2.1.3 [3]

Suatu lapangan berhingga yang terdiri atas *p* kelas-kelas residu sebagai sisa pembagian *(mod p)* dari bilangan bulat dengan *p* adalah bilangan prima disebut *Galois Field* berorde *p* dan dinotasikan GF_p.

Misalkan *R* suatu ring komutatif dengan elemen satuan *e* dan *x* suatu simbol yang disebut *indeterminate*, dengan *f*(*x*), *g*(*x*) adalah polinomial-polinomial dalam *x*,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots$$

Dimana koefisien-koefisiennya berasal dari lapangan *R*.

Definisi 2.1.4 [3]

Suatu polinomial *f*(*x*) di dalam $GF_p[x]$ dikatakan tereduksi atas GF_p jika ditemukan polinomial $\Phi_1(x)$ berderajat $m, \Phi_2(x)$ berderajat *n* di dalam $GF_p[x]$ dengan $m \geq 1, n \geq 1$ sedemikian hingga

$$f(x) = \Phi_1(x)\Phi_2(x)$$

Sehingga, *f(x)* dapat dibagi oleh $\Phi_1(x)$ dan $\Phi_2(x)$. Sebaliknya, jika tidak mungkin menentukan polinomial dari $\Phi_1(x)$ dan $\Phi_2(x)$, maka dikatakan tak tereduksi.

Contoh:

Polinomial $x^3 + 2x^2 + 3x + 4$ atas $GF_5[x]$ adalah polinomial tereduksi atas GF_5 karena $x^3 + 2x^2 + 3x + 4$ dapat dibagi oleh polinomial-polinomial $\Phi_1(x) = x^2 + 3x + 1$ dan $\Phi_2(x) = x + 4$ sedemikian sehingga :

f(x)= $x^3 + 2x^2 + 3x + 4 = (x^2 + 3x + 1)(x + 4)$

Definisi 2.1.5 [3]

Polinomial-polinomial $f_1(x), f_2(x) \in GF_p[x]$ disebut kongruen modulo $\Phi(x)$ jika $f_1(x) - f_2(x)$ dapat dibagi oleh $\Phi(x)$ yang merupakan polinomial dari $GF_p[x]$ dan dinotasikan

$$f_1(x) = f_2(x) [\text{mod } \Phi(x)]$$

Contoh:

Misalkan

$$f_1(x) = x^3 + 3x^2 + 4x + 4$$

$f_1(x) = 2x^2 + x$

Dimanda $f_1(x), f_2(x) \in GF_5[x]$

Karena $f_1(x) - f_2(x) = x^3 + x^2 + 3x + 4$ dapat dibagi oleh $\Phi_1(x) = x^2 + 3x + 1$ atau $\Phi_2(x) = x + 4$ maka $f_1(x) = f_2(x)[\mathrm{mod}\,\Phi_1(x)]$.

Definisi 2.1.6 [3]

Setiap elemen tak nol θ dari GF_{p^n} memenuhi persamaan:

$\theta^{p^n-1} = 1$

Elemen tak nol θ dikatakan elemen primitif dari lapangan jika hasil dari semua θ dengan pangkat kurang dari p^n-*1* berbeda.

Contoh:

Polinomial $p(x) = x^2 + x + 2$ merupakan polinomial primitif dari GF_{3^2} . Sebagai pengganti $x^2 + 1$ polinomial irreduksibel atas GF_{3^2} maka diperoleh sembilan kelas yaitu:

[0], [1], [2], [x], [x + 1], [x + 2], [2x], [2x + 1], [2x + 2].

Disisi lain, diberikan $p(x) = x^2 + x + 2$ maka elemen-elemen tidak nolnya adalah:

$$\begin{aligned}
&\left[x^0\right] = 1\\
&\left[x^1\right] = [x]\\
&\left[x^2\right] = [-x-2] = [2x+1]\\
&\left[x^3\right] = [2x+1][x] = \left[2x^2 + x\right] = [2x+2]\\
&\left[x^4\right] = [2x+2][x] = \left[2x^2 + 2x\right] = [2[2x+1] + 2x] = [6x+2] = [2]
\end{aligned}$$

$$[x^5] = [2][x] = [2x]$$
$$[x^6] = [2x][x] = [2x^2] = [[2][2x+1]] = [4x+2] = [x+2]$$
$$[x^7] = [x+2][x] = [x^2+2x] = [[2x+1]+2x] = [4x+1] = [x+1]$$
$$[x^8] = [x+1][x] = [x^2+x] = [[2x+1]+x] = [3x+1] = [1]$$

2.2 FAKTORISASI $x^n - 1$

Diberikan x^n-1 yang membagi $x^{q^m} - 1$ dimana $m \equiv q \bmod n$. Dengan pembuat nol dari x^n-1 yang merupakan akar ke-n yang berada dalam lapangan perluasan F_{q^m}. Misalkan α yang merupakan elemen primitif atas F_{q^m}. Jika n membagi $q^m - 1$ atau ekivalen dengan $q^m \equiv 1 \bmod n$, untuk m adalah integer positif, maka $1, \beta, \beta^2, ... \beta^{n-1}$ adalah n pembuat nol yang berbeda satu sama lain dari x^n-1, dimana $\beta = \alpha^{(q^m-1)/n}$. Sehingga diperoleh fatorisasi dari x^n-1 melalui faktor linier atas F_{q^m} sebagai berikut:

$$x^n - 1 = \prod_{i=0}^{n-1} x - \beta^i$$

Definisi 2.2.1 [5]

Perkalian *q (mod n)* dalam himpunan di GF_q disebut koset siklotomi mod n.

Koset siklotomi atas GF_q yang mengandung s adalah

$$C_s = \{s, qs, q^2 s, ..., q^{m_s - 1} s\}$$

Dimana *m* adalah integer positif terkecil sedemikian sehingga $q^{m_s} \equiv s \bmod n$ dan *s* adalah angka terkecil didalam C_s. *s* disebut koset siklotomi representatif modulo *n*.

Contoh:

Diberikan $n = 23$ dan $m = \frac{n-1}{2}$ berada di GF_2, maka:

$q^{m_s} \equiv s \bmod n$
$2^{11} \equiv s \bmod 23$
$2048 \equiv s \bmod 23$
$2048 - s = k \cdot 23$

s yang memenuhi adalah 1, maka 1 adalah koset siklotomik representatif modulo 23.

2.3 RESIDU KUADRATIK DAN POLINOMIAL PEMBANGKIT

Terdapat 2 bilangan bulat *a* dan *b*, terdapat bilangan bulat tertentu yang lain yaitu *n*, *a* disebut kongruensi dengan *b* modulo *n* jika (*a*-*b*) adalah kelipatan dari n. Dinotasikan dengan $a \equiv b (\bmod n)$. Jika $a \equiv b (\bmod n)$ maka *a*-*b* = *kn*, dimana k merupakan bilangan bulat.

Definisi 2.3.1 [2]

Diberikan bilangan bulat positif *m* dan bilangan bulat *n*,dengan $\gcd(m, n) = 1$, Jika $x^2 \equiv n \bmod m$ mempunyai solusi maka dikatakan *n* residu kuadratik modulo *m*, sedangkan jika tidak memenuhi maka dikatakan non-residu kuadratik modulo *m*.

Contoh:

Diberikan $5^2 \equiv 2 \bmod 23$ karena 23 membagi 25-2. Maka 2 merupakan residu kuadratik modulo 23.

Definisi 2.3.2 [5]

Diberikan g(x) yang merupakan polinomial monik dengan derajat minimal sedemikian hingga g(x) membagi $x^n - 1$. Maka polinomial g(x) disebut polinomial pembangkit.

Contoh:

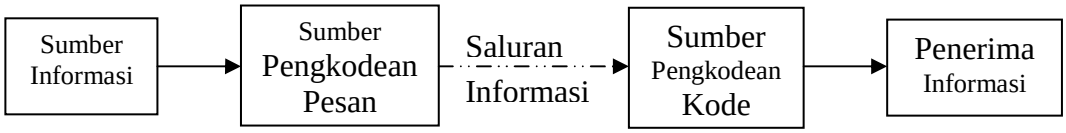
Misalkan $g(x) = 1 + x + x^3$ merupakan polinomial monik Dan $g(x)$ juga merupakan polinomial monik yang membagi $x^7 - 1$ maka $g(x) = 1 + x + x^3$ adalah polinomial pembangkit.

2.4 KODE

Kode adalah daftar kata atau simbol yang mengganti secara khusus kata lain. Kode juga merupakan blok dari simbol alphabet yang terbatas. Alphabet yang sering digunakan adalah himpunan barisan biner yaitu simbol 0 dan 1.

Dalam pengiriman pesan yang telah diubah dalam bentuk kode seringkali mengalami gangguan (*noise*) sehingga menyebabkan kesalahan penerimaan pesan. Kesalahan (*error*) merupakan masalah pada sistem komunikasi sebab dapat mengurangi kinerja dari sistem. Untuk mengatasi masalah tersebut diperlukan satu sistem yang dapat mengoreksi *error*. Oleh

karena itu, pada sistem komunikasi diperlukan sisem pengkodean. Berikut diberikan bagan proses pengiriman pesan:



Gambar 2.1 Diagram Pengiriman Pesan

Saluran pengkodean/pengkodean berfungsi untuk menjaga informasi atau data digital dari *error* yang mungkin terjadi selama proses transmisi.

2.4.1 KODE BLOK

Kode Blok merupakan kode yang membagi barisan pesan menjadi blok-blok dengan panjang *n* dan masing-masing blok dipetakan ke input saluran dengan panjang *M*. Pemetaan ini bebas dari-blok-blok sebelumnya, yaitu tidak ada memori dari satu blok ke blok lain.

Misal A adalah himpunan simbol yang mempunyai elemen sebanyak *q*. Sebagai contoh, A = $\{a_1, a_2, a_3, ..., a_q\}$ adalah himpunan yang mempunyai *q* elemen.

Definisi 2.4.1.1 [15]

Kode Blok *C* dengan panjang blok *n* berisi *M* elemen atas A adalah himpunan *n*-tupel yang berjumlah *M* dengan masing-masing koordinat dari *n*-tupel diambil dari simbol dalam A, dinotasikan dengan kode *C* [*n*, *M*] atas A.

Definisi 2.4.1.2 [15]

Elemen-elemen dari kode blok *C*[*n*, *M*] atas A disebut kodekata (*codeword*) dan elemen-elemen *n*-tupel (blok dengan panjang *n*) yang tidak berada dalam kode blok *C*[*n*, *M*] disebut kata (*word*).

Contoh :

Kode blok *C*[4, 3] = {(0000), (0110), (1010)} atas A = {0, 1} yaitu kode dengan 3 kodekata, setiap kodekata terdiri 4-tupel (mempunyai panjang 4).

Himpunan S = {(0111), (1111)} merupakan kata karena elemen 4-tupel S tidak berada di dalam kode blok C[4, 3].

Definisi 2.4.1.3 [15]

Jarak Hamming (*Hamming distance*) *d*(*x*, *y*) antara dua kodekata *x* dan *y* adalah jumlah posisi koordinat yang berbeda antara dua kodekata *x* dan *y*.

Contoh :

Diberikan kode *C* [5,2] atas A = {0, 1} yaitu :

x = 00110 dan *y* = 01001

Jarak Hamming *d*(*x*,*y*) = *d*(00110,01001) = 4 karena ada 4 posisi koordinat yang berbeda diantara kedua kodekata tersebut.

Definisi 2.4.1.4 [15]

Diberikan kode blok *C* yang merupakan kode [*n*, *M*], jarak Hamming (*Hamming Distance*) dari kode *C* didefinisikan

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

Jarak Hamming suatu kode sering disebut sebagai jarak (*distance*) saja. Untuk mencari jarak hamming dari kode *C*[*n*, *M*] harus dihitung jarak dari $\binom{M}{2}$ pasang kodekata untuk menemukan pasangan dengan jarak minimum. Dimana $\binom{M}{2}$ merupakan kombinasi 2 dari M.

Contoh :

$C = \{\mathbf{c_0}, \mathbf{c_1}, \mathbf{c_2}\}$, *C* adalah kode [4, 3] atas {*x*, *y*} dengan

$\mathbf{c_0} = (xxxx)$, $\mathbf{c_1} = (yxyy)$, $\mathbf{c_2} = (yyxy)$

Harus dicari jarak dari $\binom{3}{2} = 3$ pasang jarak dari kodekata yaitu :

$\mathrm{d}(\mathbf{c_0}, \mathbf{c_1}) = 3$ $\mathrm{d}(\mathbf{c_0}, \mathbf{c_2}) = 3$ $\mathrm{d}(\mathbf{c_1}, \mathbf{c_2}) = 2$

Sehingga diperoleh $d(C) = 2$

2.4.2 KODE LINIER

Definisi 2.4.2.1 [15]

Kode blok *C* [*n*, *M*] dikatakan linier jika kombinasi linier dari dua kode kata juga merupakan kode kata di dalam kode blok.

Misalkan c_1 dan c_2 adalah dua kodekata di dalam kode Blok (n, k). Jika diambil a_1 dan a_2 adalah dua nilai sebarang di dalam GF_q, maka kode (n, k) adalah kode linier jika dan hanya jika a_1c_1 dan a_2c_2 juga merupakan kodekata. Beberapa kode yang termasuk ke dalam kode linier antara lain kode Hamming, Red Solomon, siklik, dan Golay.

Misal himpunan semua pesan yang akan ditransmisikan adalah himpunan k-tupel yang komponen-komponennya berasal dari lapangan berhingga F dengan q elemen (GF_q). Maka $V_k(F)$ adalah himpunan semua k-tupel atas lapangan F yang terdri atas q^k elemen. Himpunan ini adalah suatu ruang vektor yang mengacu kepada "ruang pesan" dan tiap elemennya mengacu kepada "pesan".

Dalam rangka untuk mendeteksi dan mengoreksi *error*, maka perlu menambahkan beberapa digit redundansi (tambahan). Dari sini pesan k-tupel akan diperbesar ke n-tupel dimana $n \geq k$ sehingga akan disediakan suatu korespondensi satu – satu antara q^k pesan dan q^k n-tupel di $V_n(F)$ yang merupakan himpunan n-tupel atas lapangan F dengan q^n elemen.

Contoh :

Misal suatu ruang pesan terdiri dari himpunan semua bilangan biner dengan panjang 5. Kemudian akan ditransmisikan huruf alfabet sebagai bilangan biner berdimensi 5. Walaupun ruang pesan tersebut terdiri dari 2^5 bilangan biner berdimensi 5, namun hanya akan digunakan 26 saja, karena huruf alfabet hanya berjumlah 26.

Contoh di atas menggambarkan bahwa q^k n-tupel membentuk subruang berdimensi k dari $V_n(F)$.

Definisi 2.4.2.2 [15]

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

Definisi 2.4.2.3 [15]

Bobot Hamming dari suatu vektor $v \in V_n(F)$ dinotasikan dengan wt (v) merupakan banyaknya koordinat tak nol di v.

Contoh :

Diberikan dua buah kode kata yaitu (01010) dan (1110), maka:

wt (01010) = 2

wt (1110) = 3

Definisi 2.4.2. 4 [15]

Bobot Hamming dari kode C(n, k) adalah :

$$wt(\mathrm{C}) = \min\{wt(\boldsymbol{x}): \boldsymbol{x} \in \mathrm{C}, \boldsymbol{x} \neq 0\}$$

Jarak minimum dari kode linier C(n, k) sama dengan jarak minimum dari kode Blok, yaitu minimum dari jarak masing-masing kodekata pada kode tersebut. Untuk kode linier C(n, k) jarak minimumnya akan sama dengan bobot dari kode tersebut.

Teorema 2.4.2.5 [15]

Misal d adalah jarak suatu kode C(n, k), maka $d = wt$(C).

Bukti :

Dari definisi jarak suatu kode C yang diberikan oleh d = min{d(x, y): $x, y \in$ C, $x \neq y$}. Maka $d(x, y) = wt(x - y)$ karena komponen i dari $x - y$ tak nol jika dan hanya jika komponen i dari x dan y, dimana $x \neq y$ dan $x, y \in F$. Karena C kode Linier, maka C adalah subruang dari V_n(F) dan tertutup terhadap penjumlahan, $x - y \in$ C. Oleh karena itu,

d = min {$wt(z)$: $z \in$ C, $z \neq 0$} = wt(C).

■

Contoh :

Diberikan

S_1 = {(0000), (1000), (0010), (1010)}

S_2 = {(0000), (0011), (0110), (0101)}.

S_1 dan S_2 adalah subruang dari $V_4(Z_2)$

$dS_1 = 1$, dan wt (S_1) = 1

$dS_2 = 2$, dan wt (S_2) = 2

Jadi, jarak dan bobot Hamming dari S_1 dan S_2 masing–masing adalah sama.

2.4.3 KODE SIKLIK

Salah satu kelas dari kode linier adalah kelas kode siklik. Kode siklik adalah bagian dari kode linier yang mengikuti sifat perputaran

siklik. Jika $C=(C_{n-1}, C_{n-2},.. C_0)$ adalah kodekata dari suatu kode siklik, maka $(C_{n-2}, C_{n-3},.. ,C_0, C_{n-1})$ yang merupakan perputaran siklik dari C adalah juga kodekata, karena itu, semua perputaran siklik dari *C* adalah kodekata.

Definisi 2.4.3.1 [15]

Suatu subruang *S* dari $V_n(F)$ adalah subruang siklik jika $(a_1\ a_2\ a_3\ ...a_{n-1}\ a_n) \in S$ maka $(a_n\ a_1\ a_2\ a_3\ ...\ a_{n-1}) \in S$

Definisi 2.4.3.2 [15]

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

Contoh:

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

S = {(0000),(1001),(1100),(0110),(0011),(0111),(1011),
(1101),(1110)} bukan subruang siklik di $V_4(Z_2)$

Definisi 2.4.3.3 [15]

Misalkan $g(x)$ pembagi monik dari $f(x) = x^n - 1$ atas F dengan derajat $n - k$, maka $g(x)$ adalah polinomial pembangkit untuk subruang siklik dari $V_n(F)$ dengan dimensi *k.*

Contoh:

Diberikan kode siklik C(7,4) dengan $g(x) = 1 + x + x^3$.

Karena $g(x) = x^3 + x + 1$ merupakan pembagi $x^7 - 1$, maka $g(x)$ adalah polinomial pembangkit untuk subruang siklik dari $V_7(Z_2)$ dengan dimensi 4.

Definisi 2.4.3.4 [15]

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 $g(x)$ berderajat *n-k* adalah polinomial pembangkit dari kode siklik (*n*,*k*) atas *F*. Masing-masing kode kata dalam C berbentuk $p(x)g(x)$.

Contoh:

Diberikan kode siklik C(7,4) dengan $g(x) = 1 + x + x^3$ dengan $f(x) = x^7 - 1$ diperoleh matriks generator adalah

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

Akan dikodekan pesan $p(x) = 1 + x + x^3$ ke dalam kode siklik C maka diperoleh kode kata sebagai berikut:

$$p(x)g(x) = (1 + x + x^3)(1 + x + x^3)$$
$$= (1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7)$$
$$= (1111111)$$

Dalam bentuk vektor, $p(x)$ adalah pesan 4 tuple (1011) dan dikodekan de dalam bentuk kode kata menjadi (1111111).

2.4.4 KODE RESIDU KUADRATIK

Kode residu kuadratik $D, \overline{D}, R, \overline{R}$ adalah kode siklik dengan panjang *n* (yang merupakan bilangan prima) atas lapangan *GF(q)*, dimana *q* juga merupakan bilangan prima yang merupakan residu kuadratik modulo *n*. Pada tugas akhir ini hanya akan dibicarakan mengenai kode residu kuadratik dengan *q=2*.

Kode *D* dan *R* adalah kode yang ekivalen, dengan parameter $\left[n, \frac{1}{2}(n+1), d\right]$, sementara itu $\overline{D}$ dan $\overline{R}$ juga merupakan kode yang ekivalen, dengan parameter $\left[n, \frac{1}{2}(n-1), d\right]$. Sedemikian sehingga $\overline{D} \subset D$ dan $\overline{R} \subset R$. Contoh dari kode residu kuadratik antara lain adalah kode Hamming biner (7,4,3), kode Golay biner (23,12,7) dan kode Golay terner (11,6,5)

Diberikan suatu kode dengan panjang *n*, dimana *n* adalah bilangan prima ganjil ($n = \pm 1 (\mathrm{mod}\, 8)$) atas lapangan GF_q, dimana *q* adalah residu kuadratik yang memenuhi $q^{\frac{n-1}{2}} \equiv 1 \bmod n$. Akan

didefinisikan kode residu kuadratik dengan panjang *n* atas lapangan $GF_{(q)}$.

Definisi 2.4.4.1 [5]

Diberikan R_0 merupakan himpunan residu kuadratik di lapangan GF_n, dengan:

$$R_0 = \left\{ j^2 \pmod n \middle| \, j \in GF_n, \, j \neq 0 \right\},$$

Dan R_1 merupakan himpunan non-kuadratik di GF_n, dengan:

$R_1 = GF_n^* \setminus R_0$, dimana $GF_n^* = GF_n - \{0\}$

Contoh:

Diberikan n = 23, maka

$$\begin{aligned} R_0 &= \left\{ j^2 \pmod{23} \middle| \, j \in GF_{23}, \, j \neq 0 \right\} \\ &= \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \end{aligned}$$, dan

$$\begin{aligned} R_1 &= \left(GF_{23} - \{0\}\right) \setminus R_0 \\ &= \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\} \end{aligned}$$

Karena $q \in R_0$, maka himpunan R_0 tertutup terhadap perkalian oleh *q*. Oleh karena itu R_0 adalah gabungan potongan koset siklotomik modulo *n*. Sehingga:

$$g_0(x) = \prod_{i \in R_0} (x - \beta^i) \ , \quad \text{Dan} \quad g_1(x) = \prod_{i \in R_1} (x - \beta^i) .$$

Dimana koefisien-koefisien dari polinomial-polinomial diatas berada didalam GF_q, dan β adalah akar primitif ke-n dari unit dari suatu lapangan yang mengandung GF_q.