Majalah Ilmiah Matematika dan Statistika 17 Nomor 2 2017, 61 – 66
https://jurnal.unej.ac.id/index.php/MIMS/index ISSN 1411-6669

SIFAT ALJABAR KODE KUADRATIK RESIDU YANG DIPERLUAS

Kusbudiono dan Bagus Juliyanto
Jurusan Matematika Fakultas MIPA Universitas Jember

Abstract. In code theory one of the important code types is binary code. At binary field till, there is a residu quadratic and a permutation defined with residu quadratic can form a code called residu quadratic code. This code can be extended. In this paper, we discuss the propertis of group of it.

Keywords: Extension, residu quadratic code, properties of algebra
MSC 2020 (https://zbmath.org/classification)

1. Pendahuluan

Dalam penjumlahan (+) dan perkalian (*) yang memenuhi aksioma-aksioma berikut:

1. $(F,+)$ adalah grup komutatif, yang memenuhi
   Untuk semua $r,s \in F$ maka $r + s \in F$ (tertutup)
   Untuk semua $r, s \in F$ maka $r + s = s + r$ (komutatif)
   Terdapat elemen $0 \in F$ yang untuk setiap $r \in F$ maka $r + 0 = r$
   Untuk setiap $r \in F$, ada elemen $-r \in F$ berlaku $r + (-r) = 0$ (invers)
   Untuk semua $r, s, t \in F$ maka $r + (s + t) = (r + s) + t$ (assosiatif)
2. $(F\text{-}\{0\})$ adalah grup komutatif
3. Untuk setiap $r, s, t \in F$ maka $r * (s + t) = (r * s) + (r * t)$ (distributif).

2. Hasil dan Pembahasan

Suatu kode $C(n, k)$ yang linier merupakan subruang dari ruang vektor linier dimensi n atas $GF(2)$ (*Galoys Field* modulo 2). Oleh karena itu ada kemungkinan untuk menemukan k katakode yang saling bebas, misal $g_1, g_2, \ldots, g_{k-1}$ di C, sedemikian sehingga agar setiap katakode v di C merupakan kombinasi linier dari k katakode tersebut,

$$v = u_0g_0 + u_1g_1 + \ldots + u_{k-1}g_{k-1}$$

$u_i \in \{0, 1\}$ untuk $0 \le i \le k\text{-}1$.

Misalkan k katakode yang saling bebas linier disusun sebagai baris dari matriks k x n, seperti berikut ini:

$$G = \begin{bmatrix} \overline{g_0} \\ g_1 \\ . \\ . \\ . \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n-1} \\ . & & & & . \\ . & & & \ddots & . \\ . & & & & . \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

dimana $g_i = \{g_{1,0}, g_{i,2}, \ldots g_{i,n-1}\}$ untuk $0 \le i \le k$. Jika $u = \{u_0, u_1, \ldots, u_{k-1}\}$ adalah pesan yang dienkoding, hubungannya dengan katakode dapat diberikan sebagai berikut:

$$V = UG$$

$$= \begin{bmatrix} u_0 & u_1 & \cdots & u_{k-1} \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix}$$

$$= u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1}$$

Selanjutnya akan didefinisikan kode siklis yang diberikan oleh Ratna.[3] dan generator dari suatu kode siklis yang diberikan oleh Pless.[2]

Definisi 2.1 Suatu kode linier *C(n, k)* dapat dikatakan kode siklis jika setiap pergeseran siklis (permutasi) dari vektor kode di *C* juga merupakan vektor di *C*.

Contoh :

C = {(000000), (1011100), (0010111), (1110010), (0111001), (1001011), (1100101)}.

Definisi 2.2 Misal x^{n+1} adalah polinomial yang dapat dinyatakan sebagai $x^{n+1} = g(x)h(x)$ dimana *g(x)* adalah polinomial berderajat *n-k*. *g(x)* disebut generator polinomial sebagai faktor dari x^{n+1}. Artinya setiap faktor dari x^{n+1} dengan derajat *n-k* membangun suatu kode siklik (*n, k*).

Misalkan *g(x)* adalah generator polinomial dari kode siklik *C*. diketahui bahwa *g(x)* membagi x^{n-1} sehingga $x^{n-1} = g(x)h(x)$. Jika *g(x)* mempunyai derajat *n – k*, maka *C* mempunyai dimensi *k* dan *h(x)* berderajat *k* karena *h(x)* membagi x^{n-1}.

Suatu generator *e(x)* dari sebuah ideal di *Rn* disebut generator idempoten jika *e(x)* adalah idempoten, yaitu $e^2(x) = e(x)$. Generator ini bertindak sebagai unit karena jika *a(x)* di dalam $\langle e(x) \rangle$ maka $a(x) = b(x)e(x)$ dan $a(x)b(x) = b(x)e^2(x) = b(x)e(x) = a(x)$. Selanjutnya akan diberikan lemma dari Pless.[2] tentang generator idempoten.

Lemma 2.3 Suatu polinomial biner *f(x)* adalah suatu idempoten di *Rn* jika hanya jika himpunan *S* dari pangkat *x* yang terjadi dengan koefisien tidak nol di *f(x)* adalah gabungan koset siklotomik untuk *n*.

Kode kuadratik residu dapat didefinisikan atas sebuah *field* hingga umum, tetapi pada tulisan ini hanya dibatasi pada kode kuadratik residu biner. Kode-kode ini adalah kode siklik dan akan dibangun dengan generator idempotennya. Pandang *field* hingga *GF(p)* dimana *p* adalah prima ganjil dan *G* adalah grup perkalian dari elemen tidak nol dalam *GF(p),* maka *G* mempunyai order $p - 1$. Misalkan *Q* adalah subgrup dari kuadrat-kuadrat di *G*. Anggota-anggota dari *Q* disebut kuadratik residu, dan *Q* mempunyai order $(p - 1)/2$.

Kode siklik adalah kode-kode yang mentransformasikan pada dirinya sendiri dengan suatu pergeseran siklik. Pada kode kuadratik residu juga ditransformasikan pada dirinya sendiri dengan permutasi $i \rightarrow ai \pmod{p}$ dimana *a* adalah suatu kuadratik residu.

Jika *a* adalah sembarang bilangan bulat kurang dari *n* dan *gcd(a, n)* = 1, maka permutasi μ_a yang didefinisikan dengan $\mu_a(i) = ai \pmod{n}$ membawa koset siklotomik pada koset siklotomik. Jika $a \equiv 2^i \pmod{n}$, maka permutasi μ^a mentransformasi suatu kode siklik pada dirinya sendiri. Anggap *a* bukan pangkat dari 2 (mod *n*) maka permutasi μ_a mentransformasi kode siklik pada suatu kode siklik lain yang ekivalen, dan teorema berikut akan menunjukkan bahwa kode yang ekivalen tersebut juga kode siklik.

Teorema 2.4 Jika *C* kode silik dengan panjang *n*, maka permutasi μ_a yang didefinisikan dengan $\mu_a(i) = ai \pmod{n}$, $i = 1, 2, \ldots, n - 1$ dimana *gcd(a, n)* = 1 mentransformasi *C* ke suatu kode siklik *C*' atau pada *C* itu sendiri.

Bukti:

Misalkan *e(x)* adalah generator idempoten kode silik *C*, jika *S* = {i sedemikian hingga *xi* mempunyai koefisien 1 di *e(x),* maka *S* adalah gabungan dari koset siklotomik (lemma 2.3). Sehingga vektor *e(x)* memiliki "1" pada penggabungan koset siklotomik yang sama, maka $e(x)\mu_a = e(x)$ dan $e(x)\ \mu_a^{-1} = e(x)$. Dengan $\mu_a\ \sigma\ \mu_a^{-1} = \sigma$ (akibar defini μ_a) maka $e(x)\ \mu_a^{-1}\ \sigma\ \mu_a = e(x)\ \mu_a$ dan $(e(x)\ \sigma\ )\ \mu_a = e(x)\ \mu_a$. Hal ini berarti μ_a mentransformasi *e(x)* pada *e(x)* sendiri. Dan karena *e(x)* adalah generator idempoten *C* maka μ_a mentransformasi *C* pada *C* itu sendiri.

Untuk menunjukan bahwa suatu kode siklik adalah kode kuadratik residu, akan diberikan beberapa teorema-teorema yang akan digunakan untuk mengidentifikasi suatu kode siklik adalah kode kuadratik residu dengan mengasumsikan *gcd(a, n)* = 1.

Teorema 2.5 Untuk suatu permutasi μ_a yang didefinisikan sebagai $\mu_a = ai \pmod{n}$ mempertahankan perkalian polinomial.

Bukti:

Dari teorema diketahui bahwa μ_a mengirimkan sebarang kode siklik pada kode siklik lain. Sehingga benar μ_a mempertahankan perkalian polinomial di *Rn*. Untuk mengetahui hal itu misalkan

$$b(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$$

dan

$c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$

maka

$b(x)c(x) = (b_0c_0 + b_1c_{n-1} + \ldots + b_{n-1}c_1) + (b_0c_1 + b_1c_0 + \ldots + b_{n-1}c_2)x + \ldots + (b_0c_{n-1} + b_1c_{n-2} + \ldots + b_{n-1}c_0)x^{n-1}$.

Misalkan $b'(x)$, $c'(x)$, dan $(b(x)c(x))'$masing-masing adalah peta dari $b(x)$, $c(x)$, dan $b(x)c(x)$ dibawa μ_a, maka

$b'(x)c'(x) =$

Dari teorema di atas dan fakta bahwa suatu kode siklik dengan suatu permutasi dapat dikirim menjadi suatu kode siklik lain timbul akibat berikut.

Akibat 2.6 Jika μ_a mengirimkan suatu kode siklik C dengan idempoten $e(x)$ pada suatu kode C', maka C' adalah siklik dengan idempoten $e(x)$ μ_a.

Bukti:

Dari Teorema 2.4 dan 2.5 jelas, karena idempoten adalah unit perkalian dari kode. Misalkan Q_1 dan Q_2 adalah kode kuadratik residu, Q_1 dan Q_2 biasanya diperluas dengan menjumlahkan suatu parity chek keseluruhan. Untuk itu diberikan koordinat baru ∞. Koordinat-koordinat itu sekarang diberi nama ∞, 0, 1, . . ., p-1, ini dilakukan karena koordinat-koordinat baru itu adalah titik-titik garis proyektif dan akan ditunjukkan bahwa transformasi garis proyektif di dalam grup masing-masing perluasan kode kuadratik residu yang merupakan salah satu sifat dari kode tersebut. Dan untuk perluasan kode Q_1 dan Q_2 dinotasikan dengan Q_1' dan Q_2'. Selanjutnya akan diberikan teorema berikut untuk menunjukkan sifat di atas.

Sebelum membahas teorema yang dimaksud, akan didefinisikan suatu grup linier proyektif khusus yaitu suatu grup tranformasi dari garis proyektif yang mempunyai $p + 1$ titik yaitu ∞, 0, 1, . . ., $p - 1$ untuk p prima. Didefinisikan $PSL_2(p)$ suatu grup permutasi pada ∞, 0, 1, ..., $p - 1$ untuk p prima adalah dibentuk dengan permutasi elemen-elemen i pada $GF(p)$ berikut:

$\sigma : i \rightarrow i + 1 \pmod p$, $\quad \infty \rightarrow \infty$

μ a: $i \rightarrow ai \pmod p$, untuk $a \in Q$ $\quad \infty \rightarrow \infty$

ρ: $i \rightarrow -1/i \pmod p$, $i \neq 0$, $\quad 0 \rightarrow \infty, \infty \rightarrow 0$

Diketahui bahwa $PSL^2(p)$ mempunyai order $(p -1)p(p + 1)/2$ dan dengan teorema Gleason dan Prange dalam Pless.[2] akan ditunjukkan bahwa $PSL_2(p)$ terletak di dalam grup Q_1' dan Q_2'.

Teorema 2.7 Grup Q_1' atau Q_2' memuat $PSL_2(p)$

Bukti:

Diketahui bahwa σ dan μ a didalam $G(Qi)$', i = 1, 2, karena transformasi ini didalam $G(Qi)$

dan transformasi itu mempertahankan koordinat ∞. Untuk menunjukkan bahwa ρ mentransformasi perluasan kode kuadratik residu pada dirinya sendiri untuk kode-kode tertentu rumit, maka hanya dilihat pada saat $\rho = 7$. Berikut ini adalah daftar $e_1(x)$ dan semua pergeserannya dengan parity chek tambahan. Ini mencakup suatu matrik generator bagi Q_1. Sebut baris-baris itu $r_0, r_1, \ldots, r_6$,

	∞	0	1	2	3	4	5	6
r_0	1	0	1	1	0	1	0	0
r_1	1	0	0	1	1	0	1	0
r_2	1	0	0	0	1	1	0	1
r_3	1	1	0	0	0	1	1	0
r_4	1	0	1	0	0	0	1	1
r_5	1	1	0	1	0	0	0	1
r_6	1	1	1	0	1	0	0	0

Dengan mengaplikasikan ρ pada kolom-kolom matriks ini, akan didapatkan matriks berikut, dimana **h** adalah vektor satuan.

	∞	0	1	2	3	4	5	6		
r_0	0	1	0	0	1	0	1	1	=	$r_0 + h$
r_1	0	1	0	1	1	1	0	0	=	$r_6 + r_0$
r_2	0	1	1	1	0	0	1	0	=	$r_3 + r_0$
r_3	1	1	0	0	0	1	1	0	=	$r_2 + r_0 + h$
r_4	0	1	1	0	0	1	0	1	=	$r_5 + r_0$
r_5	1	1	1	0	1	0	0	0	=	$r_4 + r_0 + h$
r_6	1	1	0	1	0	0	0	1	=	$r_1 + r_0 + h$

Ingat bahwa 1, 2 dan 4 adalah residu. Ada suatu pola yang muncul yang berlaku umum. Ketika $p \equiv -1 \pmod 8$, misalkan M adalah matriks dengan baris-baris r_i, $i = 0, \ldots, p-1$, dimana $r_0 = e_1(x)$ dan r_i, untuk $i \neq 0$, sama dengan pergeseran ke-i dari $e_1(x)$. Misalkan M', dengan baris-baris r_i', matriks yang dihasilkan dari pengaplikasian ρ ke M. Maka terlihat bahwa $r_0' = r_0 + \mathbf{h}$, $r_1' = r_{-1/I} + r_0$ jika i adalah sebuah residu dan $r_i' = r_{-1/i} + r_0 + \mathbf{h}$ jika i bukan residu. Akibatnya M' ekivalen denga M', sehingga ρ mentransformasi Q_1' kepada dirinya sendiri, analog untuk Q_2'.

3. Kesimpulan

Berdasarkan pembahasan tentang salah satu sifat aljabar dari kode kuadratik, maka dapat ditarik kesimpulan sebagai berikut:

1. Grup kode adalah suatu himpunan permutasi yang mentransformasi suatu kode pada kode itu sendiri.
2. Kode kuadratik residu adalah suatu kode yang diransformasi pada dirinya sendiri oleh suatu permutasi : $i \rightarrow ai$, dengan a suatu kuadratik residu.
3. Grup kode dari perluasan kode kuadratik residu memuat suatu grup linier proyektif khusus ($PSL^2(p)$).

Daftar Pustaka

[1] Fraleigh, J.B., (1971), *A First Course in Abstract Algebra*, Fourth Edition, Addison-Wesley Publishing Company, New York

[2] Pless, V., (1989), *Introduction to The Theory of Error-Correcting Codes*, Second Edition, John Wiley and Sons, New York.

[3] Ratna D.S, dan Sunarsini, (1995), *Kode Red-Solomon (RS) dan Penerapannya untuk Koreksi Data*, Laporan Penelitian, Institut Teknologi Sepuluh Nopember, Surabaya