JURNAL MIPA 11 (2) 56 - 61

dapat diakses melalui http://ejournal.unsrat.ac.id/index.php/jmuo

Matriks Maximum Distance Separable (MDS) ukuran $m \times m$ atas $\mathbb{Z}_q$

Septa Windy Nitalessy[a]*, Mans Lumiu Mananohas[a], Rinancy Tumilaar[a], Angelina Patricia Amanda[a], Tesalonika Angela Tumey[a]

[a]Jurusan/Prodi Matematika, Fakultas MIPA, Universitas Sam Ratulangi, Manado, Sulawesi Utara

KATA KUNCI

Matriks
MDS
Entri
Submatriks

ABSTRAK

Kode Maximum Distance Separable (MDS) adalah salah satu kode yang dapat digunakan untuk mendeteksi dan mengoreksi kesalahan dimana matriks pembangunnya [I|A] disusun oleh matriks identitas dan matriks MDS. Dalam pengkodean, matriks MDS dapat mendeteksi dan mengoreksi kesalahan secara optimal. Sebuah matriks atas $\mathbb{Z}_q$ disebut matriks MDS jika dan hanya jika semua determinan submatriks bujur sangkarnya tidak nol. Pada suatu matriks $m \times m$ atas $\mathbb{Z}_q$, entri dan determinan submatriks yang mungkin terbentuk dapat menyatakan keberadaan matriks MDS ukuran $m \times m$ atas $\mathbb{Z}_q$. Hasil yang diperoleh yaitu tidak akan ada matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2+1]-[q-2]$ untuk $\mathbb{Z}_q$ dengan q sembarang. Untuk $\mathbb{Z}_q$ dengan q prima, tidak akan ada matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2+1]-[q-2]-\left[\frac{1}{2}(q-1)\right]$.

KEYWORDS

Matrix
MDS
Entry
Submatrix

ABSTRACT

The Maximum Distance Separable (MDS) code is one of the codes that known as error-correcting code where the generator matrix [I|A] is arranged by the identity matrix and the MDS matrix. In coding, MDS matrix can detect and correct errors optimally. A matrix over the $\mathbb{Z}_q$ is called an MDS matrix if and only if all the determinants of its square submatrix are non-zero. A matrix over $\mathbb{Z}_q$ is called an MDS matrix if and only if all the determinants of its square submatrix are non-zero. In $m \times m$ matrix over $\mathbb{Z}_q$, the analyzed of possible entries and determinants of submatrix can be declare the existence of an MDS matrix of size $m \times m$ over $\mathbb{Z}_q$. The result is there will be no MDS matrix of size $m \times m$ where $m \geq [(q-1)^2+1]-[q-2]$ for $\mathbb{Z}_q$ with any of q. For $\mathbb{Z}_q$ with q prime, there will be no MDS matrix of size $m \times m$ where $m \geq [(q-1)^2+1]-[q-2]-\left[\frac{1}{2}(q-1)\right]$.

TERSEDIA *ONLINE*
01 Agustus 2022

Pendahuluan

Latar Belakang

Kebutuhan manusia terhadap teknologi di era digital sekarang ini sangatlah tinggi, mulai dari proses jual beli, komunikasi, media bertukar infomasi, dan banyak hal lainnya. Proses penyaluran data yang dilakukan oleh pengguna teknologi saat ini tentu saja membutuhan pengamanan data, sebab baik penyalur maupun penerima data tentu saja ingin data atau pesan yang disampaikan terjaga kerahasiaannya. Untuk menjaga kerahasiaan suatu data atau pesan dapat dilakukan dengan menyamarkan data mengunakan pengkodean. Dalam mengubah pesan yang dirahasiakan (*plainteks)* ke pesan hasil penyamaran (*chiperteks)* maupun sebaliknya bisa terjadi kesalahan yang menyebabkan pesan yang disampaikan terjadi kesalahan.

Dalam pengkodean, terdapat kode yang mampu mendeteksi atau mengoreksi kesalahan yang disebut dengan *Error Correcting Code*, salah satu-nya yaitu

*Corresponding author:
Email address: windynitalessy@unsrat.ac.id
Published by FMIPA UNSRAT (2022)

kode linear. Kode linear dapat dibangun oleh suatu matriks tertentu yang disebut matriks generator disusun oleh matrik identitas dan suatu matriks A. Dalam pengkodean untuk mendeteksi kesalahan lebih banyak, kita harus memaksimalkan minimal jarak. Hal ini dapat dilakukan apabila matriks A yang digunakan pada matriks generator merupakan matriks *Maximum Distance Separable* (MDS).

Sebuah matriks atas lapangan $\mathbb{F}_q$ disebut dengan matriks MDS jika dan hanya jika semua minor (determinan dari submatriks bujur sangkar) matriks tersebut tidak nol (Duval, S dan Laurent, G. 2018). Artinya matriks MDS memiliki anggota tak nol. Pada penelitian yang dilakukan oleh Muhammad Afifurrahman difokuskan untuk mencari jumlah entri berbeda pada Matriks MDS involutori atas lapangan berhingga khususnya F_{2^m} dengan menganalisis entri matriksnya. Pada penelitian ini dengan melihat keunikan dan fakta yang bisa diperoleh dari analisis entri matriks MDS akan dicari ada tidaknya suatu matriks matriks MDS di $\mathbb{F}_q$ tertentu untuk ukuran $m \times m$ tertentu.

Rumusan Masalah

Berapa nilai r terkecil sehingga tidak akan ada MDS ukuran $m \times m$ atas $\mathbb{Z}_q$untuk $m \geq r$?

Tujuan Penelitian

Penelitian ini bertujuan memperkecil daerah pencarian matriks $m \times m$ yang mungkin membentuk matriks MDS atas $\mathbb{Z}_q$ dimana $m \geq r$ dengan mencari nilai r terkecil.

Batasan Masalah

Penelitian yang dilakukan hanya berfokus pada lapangan $\mathbb{Z}_q$ dan hanya untuk membuktikan keberadaan matriks MDS ukuran $m \times m$ pada m tertentu.

Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini yaitu memperkecil daerah pencarian matriks MDS ukuran $m \times m$ atas $\mathbb{Z}_q$ sehingga bisa membantu menentukan generator matriks untuk digunakan pada kode linear

Material dan Metode

Kode MDS

Definisi 1

Misalkan $\mathbb{F}$ adalah lapangan berhingga dengan p dan q bilangan bulat, Misalkan $x \to M \times x$ merupakan pemetaan dari $\mathbb{F}^p$ ke $\mathbb{F}^q$didefinisikan dengan matriks M berukuran $q \times p$. Kita katakan matriks M adalah matriks MDS jika setiap pasangan $(x, M \times x)$ adalah kode MDS. Sebagai contoh sebuah kode linear dengan dimensi p, panjang $p + q$ dan jarak minimal $q + 1$ (Gupta, K. dan Ray, I., 2013).

Definisi 2

Sebuah kode $[n, k, d]$ dengan $d = n - k + 1$ dikatakan kode jarak terpisahkan terjauh (*maximum distance separable*) atau kode MDS secara singkat (MacWilliams, F. dan Sloane, N., 1977).

Matriks MDS

Definisi 2

Sebuah matriks bujursangkar A adalah matriks MDS jika dan hanya jika semua submatriks bujursangkar dari A merupakan matriks non singular. Semua entri dari matriks MDS adalah elemen tak nol (Gupta, dkk. 2019).

Generator Matriks

Definisi 4

Sebuah kode C $[n, k, d]$ dengan matriks pembangun (generator) $G = [I|A]$, di mana A adalah matriks berukuran $\mathrm{k} \times (\mathrm{n} - \mathrm{k})$, merupakan matriks MDS jika dan hanya jika setiap submatriks bujursangkar dibentuk dari sebarang kolom ke-i dan baris ke-i, untuk sebarang $\mathrm{i} = 1,2, \ldots, \min\{\mathrm{k}, \mathrm{n} - \mathrm{k}\})$ dari A adalah nonsingular.

Modulo

Definisi Modulo

Menurut Lalonde (2013), misalkan $a, n \in \mathbb{Z}$ dan dituliskan $a = qn + r$. Kita melambangkan sisa pembagian r dari $[a]_n$ dan kita menyebutnya sisa pembagian dari $a \ mod \ n$.

Contoh:

Misalkan $a = 17$ dan $n = 5$. Maka

$$a = 17 = 5.3 + 2 = 5n + 2$$

jadi sisa pembagiannya

$$[a]_n = [17]_5 = 2$$

Definisi $\mathbb{Z}_n$

Menurut Lalonde (2013), misalkan $\mathbb{Z}_n$ = {0,1,2, …, $n - 1$} melambangkan himpunan bilangan bulat mod n. Kita dapat menjumlahkan 2 elemen dari $a, b \in \mathbb{Z}_n$ dengan

$$a +_n b = [a + b]_n$$

Contoh:

Misalkan $\mathbb{Z}_4 = \{1,2,3\}$ maka

$$3 +_4 7 = [3 + 7]_4 = [10]_4 = 2$$

Metode Penelitian

Metode yang digunakan adalah metode studi pustaka.

Tahapan Penelitian

1. Memeriksa bentuk matriks 2×2 sebagai submatriks $m \times m$.
2. Menganalisis bentuk matriks 2×2 yang bukan MDS pada $\mathbb{Z}_q$.
3. Menganalisis entri matriks 2×2 yang bukan matriks MDS.
4. Menganalisis kembali bentuk matriks 2×2 yang bukan MDS pada $\mathbb{Z}_q$ dengan q tertentu.
5. Menarik kesimpulan.

Hasil dan Pembahasan

Bentuk matriks 2×2 sebagai sub matriks $m \times m$.

Suatu matriks $m \times m$ dimana $m \geq 2$ akan selalu memiliki submatriks 2×2. Berdasarkan Definisi 3 suatu matriks bujursangkar A adalah matriks MDS jika dan hanya jika semua submatriks bujursangkar dari A merupakan matriks nonsingular. Artinya apabila suatu submatriks 2×2 sebagai submatriks $m \times m$ untuk $m \geq 2$ terbukti bukan matriks

nonsingular maka matriks $m \times m$ tersebut bukanlah matriks MDS.

Misalkan submatriks 2×2 entri sebarang bilangan a, b, c, d dengan $a \neq b \neq c \neq d$. Dengan demikian akan diperoleh beberapa bentuk submatriks 2×2 dari kombinasi bilangan a, b, c, d sebagai berikut

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix}, \begin{bmatrix} b & a \\ a & a \end{bmatrix}, \begin{bmatrix} a & b \\ a & a \end{bmatrix}, \begin{bmatrix} a & a \\ b & a \end{bmatrix}, \begin{bmatrix} a & a \\ a & b \end{bmatrix},$$
$$\begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} a & b \\ a & b \end{bmatrix}, \begin{bmatrix} a & b \\ b & a \end{bmatrix}, \begin{bmatrix} a & a \\ b & c \end{bmatrix}, \begin{bmatrix} b & c \\ a & a \end{bmatrix},$$
$$\begin{bmatrix} a & b \\ a & c \end{bmatrix}, \begin{bmatrix} b & a \\ c & a \end{bmatrix}, \begin{bmatrix} a & b \\ c & a \end{bmatrix}, \begin{bmatrix} b & a \\ a & c \end{bmatrix}, \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Analisa bentuk matriks 2×2 yang bukan matriks MDS

Suatu matriks 2×2 sebagai submatriks dari matriks $m \times m$ untuk $m \geq 2$ yang memliki determinan nol merupakan matriks singular. Berdasarkan Definisi 5 matriks tersebut bukanlah matriks MDS. Setelah dicari determinan matriks 2×2 dari kombinasi bilangan a, b, c, d yang telah diuraikan pada Bagian 3.1 diperoleh bahwa terdapat beberapa matriks 2×2 dengan determinan nol, yaitu subm$\begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$, $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$. Artinya kita dapat nyatakan matriks $m \times m$ yang memiliki submatriks 2×2 dengan bentuk tersebut bukanlah matriks MDS.

Analisa entri matriks 2×2 yang bukan matriks MDS

Diketahui himpunan $\mathbb{Z}_q = \{0,1,2,\dots,q-1\}$ dengan anggota tak nol yang dinotasikan sebagai $\mathbb{Z}_q - \{0\} = \{1,2,\dots,q-1\}$. Perlu diingat bahwa nol yang merupkan elemen $\mathbb{Z}_q$ tidak akan pernah digunakan sebagai entri untuk menghasilkanmatriks MDS. Misalkan kombinasi

$$(x,y)_q = \begin{Bmatrix} (x_i, y_i) | x_i \in \mathbb{Z}_q - \{0\}, y_i \in \mathbb{Z}_q - \{0\} \\ dengan\ i = 1,2,3,\dots dan\ q = 1,2,3,\dots. \end{Bmatrix}$$

Selanjutnya banyak anggota tak nol $\mathbb{Z}_q$ dinotasikan sebagai $|\mathbb{Z}_q - \{0\}| = q - 1$.

Misalkan semua kombinasi $(x,y)_q$ yang terbentuk disusun sebagai sub-submatriks 1×2 bentuk $[x_i \quad y_i]$ pada matriks $m \times m$ yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 seperti berikut

$$\begin{bmatrix} x_1 & y_1 & a_{13} & a_{14} & \cdots & a_{m1} \\ x_2 & y_2 & a_{23} & a_{24} & \dots & a_{m2} \\ x_3 & y_3 & a_{33} & a_{34} & \dots & a_{m3} \\ x_4 & y_4 & a_{34} & a_{44} & \dots & a_{m4} \\ x_5 & y_5 & a_{35} & a_{45} & \dots & a_{m5} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_i & y_i & a_{3m} & a_{4m} & \dots & a_{mm} \end{bmatrix}$$

Nantinya pemisalan ini akan digunakan untuk menganalisis entri matriks $m \times m$.

Pertama dianalisis secara khusus untuk $\mathbb{Z}_1 = \{0\}$ dan $\mathbb{Z}_2 = \{0,1\}$. Pada $\mathbb{Z}_1$ dan $\mathbb{Z}_2$ tidak mungkin berbentuk matriks MDS. Matriks MDS harus memiliki entri tak nol yang berarti $\mathbb{Z}_1$ tidak mungkin membentuk matriks MDS dan pada $\mathbb{Z}_2$ dengan elemen tak nol-nya yaitu $\{1\}$ hanya dapat membentuk matriks $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ dengan determinan nol (0) dimana merupakan bentuk matriks $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ yang bukan matriks MDS. Maka analisis yang dilakukan lebih fokus pada $\mathbb{Z}_q$ dengan $q \geq 3$.

Selanjutnya dilakukan analisis berdasarkan bentuk matriks 2×1 yang memiliki determinan nol (0) berdasarkan Langkah 3.2 Bentuk matriks yang akan dianalisis yaitu $\begin{bmatrix} a & a \\ a & a \end{bmatrix}, \begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} a & b \\ a & b \end{bmatrix}$.

a. Analisis bentuk submatriks $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$ dan $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$

Preposisi 1. Tidak akan terdapat matriks MDS atas $\mathbb{Z}_q$ untuk $m \times m$ dimana $m \geq (q-1)^2 + 1$.

Bukti.

Banyaknya kombinasi $(x,y)_q$ yang mungkin terbentuk pada setiap $\mathbb{Z}_q$ yaitu sebanyak $n(x,y) = |\mathbb{Z}_q - \{0\}|^2 = (q-1)^2$.

Mengingat Teorema *Pigeon Hole* akan terdapat setidaknya 2 kombinasi $(x,y)_q$ yang sama untuk matriks MDS ukuran $m \times m$ dengan $m \geq (q-1)^2 + 1$ yang disusun secara vertikal sejajar pada setiap baris ke-i kolom ke-1 dan ke-2. Perhatikan matriks berikut

$$\begin{bmatrix} x_1 & y_1 & a_{13} & a_{14} & \cdots & a_{(m-1)1} & a_{m1} \\ x_2 & y_2 & a_{23} & a_{24} & \dots & a_{(m-1)2} & a_{m2} \\ x_3 & y_3 & a_{33} & a_{34} & \dots & a_{(m-1)3} & a_{m3} \\ x_4 & y_4 & a_{34} & a_{44} & \dots & a_{(m-1)4} & a_{m4} \\ x_5 & y_5 & a_{35} & a_{45} & \dots & a_{(m-1)5} & a_{m5} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_i & y_i & a_{3(m-1)} & a_{4(m-1)} & \dots & a_{(m-1)(m-1)} & a_{m(m-1)} \\ x_{i+1} & x_{i+1} & a_{m(m-1)} & a_{5(m-1)} & \dots & a_{(m-1)m} & a_{mm} \end{bmatrix}$$

Misalkan submatriks $[x_1 \quad y_1], \dots, [x_i \quad y_i]$ berasal dari $(q-1)^2$ kombinasi $(x,y)_q$ berbeda, maka untuk submatriks $[x_{i+1} \quad y_{i+1}]$ diisi oleh salah satu kombinasi $(x,y)_q$ yang sudah pasti sama dengan salah satu dari $(q-1)^2$ kombinasi $(x,y)_q$ berbeda yang merupkan salah satu submatriks $[x_1 \quad y_1], [x_2 \quad y_2], .., atau\ [x_i \quad y_i]$. Misalkan matriks yang diambil sebagai $[x_{i+1} \quad y_{i+1}]$ yaitu $[x_i \quad y_i]$ maka akan terbentuk matriks $m \times m$ sebagai berikut:

$$\begin{bmatrix} x_1 & y_1 & a_{13} & a_{14} & \cdots & a_{(m-1)1} & a_{m1} \\ x_2 & y_2 & a_{23} & a_{24} & \dots & a_{(m-1)2} & a_{m2} \\ x_3 & y_3 & a_{33} & a_{34} & \dots & a_{(m-1)3} & a_{m3} \\ x_4 & y_4 & a_{34} & a_{44} & \dots & a_{(m-1)4} & a_{m4} \\ x_5 & y_5 & a_{35} & a_{45} & \dots & a_{(m-1)5} & a_{m5} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_i & y_i & a_{3(m-1)} & a_{4(m-1)} & \dots & a_{(m-1)(m-1)} & a_{m(m-1)} \\ x_i & x_i & a_{m(m-1)} & a_{5(m-1)} & \dots & a_{(m-1)m} & a_{mm} \end{bmatrix}$$

Perhatikan akan terbentuk submatriks $\begin{bmatrix} x_i & y_i \\ x_i & y_i \end{bmatrix}$ dimana merupakan submatriks bentuk $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$. Untuk kombinasi $(x,y)_q$ terdapat kondisi dimana $x_i = y_i$ seperti $(1,1), (2,2), .., dan\ (q-1, q-1)$, pada kasus ini submatriks yang terbentuk nantinya akan berbentuk $\begin{bmatrix} x_i & x_i \\ x_i & x_i \end{bmatrix}$ yang merupakan submatriks bentuk $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$. Oleh karena matriks $m \times m$ dimana $m = (q-1)^2 + 1$ akan membentuk setidaknya satu submatiks berbentuk $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$ atau $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ dimana

submatriks tersebut merupakan submatriks dengan determinan nol (0) maka untuk $m \geq (q-1)^2+1$ sudah pasti ditemukan lebih dari 1 submatriks yang terbentuk dengan determinan nol (0). Dapat disimpulkan bahwa untuk matriks $m \times m$ dimana $m \geq (q-1)^2+1$ tidak mungkin terdapat matriks MDS atas $\mathbb{Z}_q$.

b Analisis bentuk submatriks $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$

Preposisi 2. Tidak akan terdapat matriks MDS atas $\mathbb{Z}_q$ ukuran $m \times m$ dimana $m \geq [(q-1)^2+1]-[q-2]$

Bukti.

Banyaknya kombinasi $(x,y)_q$ yang mungkin terbentuk pada setiap $\mathbb{Z}_q$ yaitu sebanyak $n(x,y) = \left|\mathbb{Z}_q - \{0\}\right|^2 = (q-1)^2$.

Perhatikan untuk bentuk matriks $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$ disusun oleh submatriks $[a \quad a]$ dan $[b \quad b]$, kemudian perhatikan juga untuk kombinasi $(x,y)_q$ yang akan disususn sebgai sub-submatriks 1×2 bentuk $[x_i \quad y_i]$ pada matriks $m \times m$ yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 terdapat kondisi dimana $x_i = y_i$ yang artinya akan membentuk submatriks 1×2 bentuk $[x_i \quad x_i]$. Submatriks 1×2 dengan kondisi tersebut apabila disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 sudah pasti menghasilkan submatriks 2×2 bentuk $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$, misalnya $\begin{bmatrix} x_1 & x_1 \\ x_2 & x_2 \end{bmatrix}$.

Mengacu pada Preposisi 1 artinya atas $\mathbb{Z}_q$ matriks $m \times m$ terbesar yang masih mungkin membentuk matriks MDS yaitu saat $m = (q-1)^2$. Perhatikan matriks $m \times m$ dimana $m = (q-1)^2$ yang setiap baris ke-i kolom 1 dan 2 disusun kombinasi $(x,y)_q$ berbeda seperti berikut ini.

$$\begin{bmatrix}
1 & 1 & a_{13} & \cdots & a_{1[(q-1)^2]} \\
1 & 2 & a_{23} & \cdots & a_{2[(q-1)^2]} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & q-1 & a_{[(q-1)]3} & \cdots & a_{[(q-1)][(q-1)^2]} \\
2 & 1 & a_{[(q-1)+1]3} & \cdots & a_{[(q-1)+1][(q-1)^2]} \\
2 & 2 & a_{[(q-1)+2]3} & \cdots & a_{[(q-1)+2][(q-1)^2]} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
2 & q-1 & a_{[2(q-1)]3} & \cdots & a_{[2(q-1)][(q-1)^2]} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
q-1 & 1 & a_{[(q-2)(q-1)]3} & \cdots & a_{[(q-2)(q-1)][(q-1)^2]} \\
q-1 & 2 & a_{[((q-2)(q-1))+1]3} & \cdots & a_{[((q-2)(q-1))+1][(q-1)^2]} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
q-1 & q-1 & a_{[(q-1)^2]3} & \cdots & a_{[(q-1)^2][(q-1)^2]}
\end{bmatrix}$$

Berdasarkan analisis yang dilakukan apabila terdapat lebih dari satu submatriks 1×2 bentuk $[x_i \quad x_i]$ akan membentuk submatriks 2×2 bentuk $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$seperti

$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 3 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ q-1 & q-1 \end{bmatrix}, \begin{bmatrix} q-2 & q-2 \\ q-1 & q-1 \end{bmatrix}$.

Submatriks $[x_i \quad x_i]$ dibentuk dari kombinasi $(x,x)_q = \begin{Bmatrix} (x_i,x_i) | (x_i,x_i) \in (x,y)_q \; dimana \; x_i = y_i \\ dengan \; i = 1,2,3,\ldots dan \; q = 1,2,3,\ldots. \end{Bmatrix}$

Artinya hanya boleh paling banyak satu dari kombinasi $(x,x)_q$ yang boleh dijadikan submatrik $[x_i \quad x_i]$ yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 agar tidak membentuk suatu submatriks dengan determinan nol. Banyaknya kombinasi $(x,x)_q$ pada $\mathbb{Z}_q - \{0\}$ sama dengan banyaknya anggota $\mathbb{Z}_q - \{0\}$ yaitu sebanyak $q-1$.

Oleh karena pada matriks $m \times m$ dengan $m = (q-1)^2$ atas $\mathbb{Z}_q$ masih terdapat kemungkinan untuk terbentuk matriks dengan determinan nol (0) seperti pada analisis diatas. Maka batas pada Preposisi 1 dapat diperkecil dengan ruas kanan dikurang banyak kombinasi $(x,y)_q$ yang tidak boleh berada dalam satu matriks sebagai submatrik 1×2 yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 yaitu sebanyak $(q-1)-1 = q-2$ yang diperoleh dari pernyataan bahwa dari kombinasi $(x,y)_q$ terdapat sebanyak $q-1$ kombinasi $(x,x)_q$ hanya boleh terdapat paling banyak satu kombinasi $(x,x)_q$ yang boleh dijadikan submatrik 1×2 yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2. Maka dapat disimpulkan bahwa tidak akan terdapat matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2+1]-[q-2]$.

Analisa kembali bentuk matriks 2×2 yang bukan MDS pada $\mathbb{Z}_q$ dengan q tertentu.

Mengacu pada 4.1 dan 4.2 masih terdapat submatriks lainnya yang dapat terbentuk jadi akan dianalisis semua bentuk submatriks 2×2 selain $\begin{bmatrix} a & a \\ a & a \end{bmatrix}, \begin{bmatrix} a & a \\ b & b \end{bmatrix}, \begin{bmatrix} a & b \\ a & b \end{bmatrix}$. Apabila suatu matriks $m \times m$ memiliki submatriks singular dengan determinan nol (0) malas sudah dipastkan bahwa matriks tersebut bukan matriks MDS. Maka selanjutnya akan dianalisis submatriks yang dapat terbentuk dengan pemisalan bahwa submatriks tersebut memiliki determinan nol untuk mengidentifikasi pada ukuran $m \times m$ manakah yang tidak adakan terbentuk matriks MDS, yang selanjutnya diperoleh syarat entri yaitu $a^2 = b^2$, $a^2 = bc$, $a^2 = ab$, $ab = ac$, $ad = bc$. Akan diperhatikan syarat-syarat tersebut atas $\mathbb{Z}_q$ dimana $q > 2$.

Perhatikan permetaan $\mathbb{Z}_q - \{0\} \times \mathbb{Z}_q - \{0\}$ dan di temukan bahwa $\mathbb{Z}_q$ dengan q prima sangat unik dimana $\mathbb{Z}_q$ dengan q prima merupakan lapangan berhingga, yang memperlihatkan bahwa setiap elemen $\mathbb{Z}_q$ muncul tepat satu kali di setiap baris dan kolom. Selanjutnya Analisa akan dilakukan untuk $\mathbb{Z}_q$ dengan q pima.

a. Analisis submatriks dengan determinan $a^2 = b^2$

Lemma 1. Pada setiap $\mathbb{Z}_q$, untuk menghasilkan $a^2 = b^2$ dengan bentuk matriks $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ dipenuhi saat $a^2 = (-a)^2$.

Bukti.

Jika kita misalkan bahwa $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ bukan Matriks MDS, maka:

$$det\begin{bmatrix} a & b \\ b & a \end{bmatrix} = 0$$
$$(a+b)(a-b) = 0$$
$$(a+b) = 0\ atau\ (a-b) = 0$$
$$a = -b\ atau\ a = b$$

Untuk $a = b$ akan menghasilkan bentuk $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$. Sudah dibahas sebelumnya. Maka untuk menghasilkan $a^2 = b^2$ dengan bentuk matriks $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ dipenuhi saat $a^2 = (-a)^2$. Pada hal ini $(-a)$ menyatakan invers penjumlahan dari a atas $\mathbb{Z}_q$. Misal,

$$a = 1 \rightarrow (-a) = q - 1$$
$$a = 2 \rightarrow (-a) = q - 2$$
$$\vdots$$
$$a = q - 1 \rightarrow (-a) = q - (q-1) = 1$$

Preposisi 3. Untuk $\mathbb{Z}_q$ dengan q prima, tidak akan terdapat matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2] - \left[\frac{1}{2}(q-1)\right]$.

Bukti.

Berdasarkan Lemma 1 dengan memperhatikan hasil perkalian pada $\mathbb{Z}_q$ dan syarat entri $a^2 = b^2$ diperoleh tabel penguraian sebagai berikut.

Tabel 1. Tabel Matriks yang dihasilkan oleh kombinasi $(\boldsymbol{a}, \boldsymbol{b})$ atas $\mathbb{Z}_{\boldsymbol{q}}$ yang memenuhi $\boldsymbol{a^2 = b^2}$

$\boldsymbol{a}$	$\boldsymbol{b = -a}$	$\boldsymbol{a^2 = b^2}$	Matriks yang dihasilkan
1	$q-1$	$1^2 = (q-1)^2$	$\begin{bmatrix} 1 & q-1 \\ q-1 & 1 \end{bmatrix}$
2	$q-2$	$2^2 = (q-2)^2$	$\begin{bmatrix} 2 & q-2 \\ q-2 & 2 \end{bmatrix}$
⋮	⋮	⋮	⋮
$\boldsymbol{q-2}$	2	$(q-2)^2 = 2^2$	$\begin{bmatrix} q-2 & 2 \\ 2 & q-2 \end{bmatrix}$
$\boldsymbol{q-1}$	1	$(q-1)^2 = 1^2$	$\begin{bmatrix} q-3 & 3 \\ 3 & q-3 \end{bmatrix}$

Berdasarkan tabel diatas pasangan kombinasi (a,b) yang dihasilkan pada $\mathbb{Z}_q$ dengan q yang memenuhi syarat entri $a^2 = b^2$ selanjutnya akan dinotasikan sebagai

$$(a,b)_q = \left\{ \begin{matrix} (a_i, b_i) | (a_i, b_i) \in (x,y)_q, \\ a_i = p\ dan\ b_i = q - p \\ dengan\ p, q = 1,2,3, \ldots \end{matrix} \right\}.$$

Banyaknya kombinasi $(a,b)_q$ yaitu sebanyak $\mathbb{Z}_q - \{0\} = q - 1$. Berdasarkan Tabel 4.2.1 diperoleh:

- saat $a = p\ dan\ b = q - p$ diperoleh boooooooentuk matriks $\begin{bmatrix} p & q-p \\ q-p & p \end{bmatrix}$, dengan submatriks 1×2 yang terbentuk yaitu $[p \quad q-p]$ dan $[q-p \quad p]$.
- saat $a = q - p\ dan\ b = p$ diperoleh bentuk matriks $\begin{bmatrix} q-p & p \\ p & q-p \end{bmatrix}$, dengan submatriks 1×2 yang terbentuk yaitu $[q-p \quad p]$ dan $[p \quad q-p]$.

Perhatikan bahwa dari fakta diatas diperoleh bahwa untuk kondisi (a,b) akan sama dengan (b,a) maka banyaknya submatriks 2×2 dengan submatriks 1×2 berbeda yang dapat terbentuk yaitu setengah dari banyaknya kombinasi $(a,b)_q$ yaitu sebanyak $\frac{1}{2}(q-1)$. Sekarang perhatikan untuk setiap 2×2 yang terbentuk:

$$\begin{bmatrix} p & q-p \\ q-p & p \end{bmatrix}$$

dengan sepasang submatriks 1×2 yang terbentuk yaitu $[q-p \quad p]$ dan $[p \quad q-p]$, Banyak submatriks submatriks 1×2 yang terbentuk yaitu sebanyak dua kali banyak submatriks 2×2 yang terbentuk yaitu sebanyak $2 \times \left[\frac{1}{2}(q-1)\right] = q - 1$. Untuk submatriks $[q-p \quad p]$ dan $[p \quad q-p]$ hanya tepat satu yang boleh disusun pada setiap baris ke-i kolom 1 dan 2 agar tidak diperoleh submatriks yang bukan MDS dan membentuk matriks MDS, karena terdapat sebanyak $q-1$ matriks pasang martiks 1×2 yang terbentuk maka banyak kombinasi $(a,b)_q$ yang boleh terdapat dalam satu matriks yang disusun secara vertikal sejajar pada setiap baris ke-i kolom 1 dan 2 sebanyak $\frac{1}{2}(q-1)$. Mengacu pada Preposisi 2, atas $\mathbb{Z}_q$ matriks $m \times m$ masih mungkin membentuk matriks MDS yaitu saat $m < [(q-1)^2 + 1] - [q-2]$. Matriks $m \times m$ dengan $m = [(q-1)^2] - [q-2]$ yang setiap baris ke-i kolom 1 dan 2 disusun kombinasi $(x,y)_q$ dengan hanya satu kombinasi $(x,x)_q$ sudah pasti memiliki submatriks dengan kombinasi $(a,b)_q$ karena $(a,b)_q \in (x,y)_q$ artinya untuk memperkecil batas pencarian matriks MDS ruas kanan dapat dikurangi dengan $\frac{1}{2}(q-1)$ yang diperoleh dari pernyataan bahwa hanya boleh terdapat setengah dari submatriks 1×2 dari kombinasi $(a,b)_q$. Maka dapat disimpulkan bahwa untuk $\mathbb{Z}_q$ dengan q prima, tidak akan terdapat matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2] - \left[\frac{1}{2}(q-1)\right]$.

b. Analisis submatriks syarat $\boldsymbol{a^2 = ab}$ dan $\boldsymbol{ab = ac}$

Untuk $a^2 = ab$

Dengan memperhatikan hasil perkalian $\mathbb{Z}_q \times \mathbb{Z}_q$ untuk q prima tidak mungkin terdapat hasil berupa $a^2 = ab$ sebab setiap elemen $\mathbb{Z}_q$ muncul tepat satu kali di setiap baris dan kolom dan a^2 tidak mungkin sama dengan ab jika $a \neq b$.

Untuk $ab = ac$

Sama halnya dengan bagian a) Dengan memperhatikan hasil perkalian $\mathbb{Z}_q \times \mathbb{Z}_q$ untuk q prima tidak mungkin terdapat hasil berupa $ab = ac$ sebab setiap elemen $\mathbb{Z}_q$ muncul tepat satu kali di

setiap baris dan kolom dan ab tidak mungkin sama ac jika $b \neq c$.

Analisis ini tidak bepengaruh pada daerah pencarian.

Pengambilan kesimpulan.

Setelah menganalisis entri submatriks 2×2 yang mungkin dihasilkan oleh matriks $m \times m$ atas $\mathbb{Z}_q$ dengan memperhatian kombinasi submatriks 1×2 yang nantinya akan disusun secara vertikal sejajar untuk menentukan batas nilai r terkecil sehingga tidak akan ada matriks MDS ukuran $m \times m$ atas lapangan $\mathbb{Z}_q$ untuk $m \geq r$ maka diperoleh bahwa:

- Untuk $\mathbb{Z}_q$ dengan q sembarang, mengacu pada analisis submatriks bentuk $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$, $\begin{bmatrix} a & b \\ a & b \end{bmatrix}$ dimana determinannya nol (0) seperti pada Preposisi 1 dan Preposisi 2, maka tidak akan terdapat matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2]$.

Untuk $\mathbb{Z}_q$ dengan q prima, mengacu pada analisis submatriks bentuk $\begin{bmatrix} b & a \\ a & a \end{bmatrix}, \begin{bmatrix} a & b \\ a & a \end{bmatrix}, \begin{bmatrix} a & a \\ b & a \end{bmatrix}, \begin{bmatrix} a & a \\ a & b \end{bmatrix}, \begin{bmatrix} a & a \\ b & c \end{bmatrix}, \begin{bmatrix} b & c \\ a & a \end{bmatrix}, \begin{bmatrix} a & b \\ a & c \end{bmatrix}, \begin{bmatrix} a & b \\ b & a \end{bmatrix}, \begin{bmatrix} a & b \\ c & a \end{bmatrix}, \begin{bmatrix} b & a \\ a & c \end{bmatrix}$ dengan pemisalan determinan nol (0) seperti pada Preposisi 3, maka tidak akan ada matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2] - \left[\frac{1}{2}(q-1)\right]$.

Kesimpulan

Berdasarkan analisis entri yang dilakukan hasil penelitian yang diperoleh yaitu bahwa:

1. Untuk $\mathbb{Z}_q$ dengan q sembarang, tidak akan terdapat matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2]$.
2. Untuk $\mathbb{Z}_q$ dengan q prima, tidak akan ada matriks MDS ukuran $m \times m$ dimana $m \geq [(q-1)^2 + 1] - [q-2] - \left[\frac{1}{2}(q-1)\right]$.

Daftar Pustaka

Afifurrahman, M. 2021. Information Theory (cs.IT): On the Number of Different Entries in involutory MDS Matrices over Finite Fields of Characteristic Two. *AIP Conference Proceedings 2423 060002*. 10.1063/5.0075414

Duval, S dan Laurent, G. 2018. MDS Matrices with Lightweight Circuits. *IAXR Transactions on Symetric Cryptology*. **2018(2): 48-78**. 10.13154/tosc.v2018i2.48-78

Gupta, K. dan Ray, I., 2013. On constructions of involutory MDS matrices, Progress incryptology-AFRICACRYPT, **7918:** 43-60.

Gupta, K., Pandey, S., Ray, Indranil Ghosh R. dan Samanta, S, 2019. Cryptographically Significant Mds Matrices Over Finite Fields: A Brief Survey and Some Generalized Results. *Advances in Mathematics of Communications*. **13(4)**: 779-843.

Lalonde, S.M. 2013. *Notes on Abstract Algebra*. Dartmouth College, Hanover Amerika Serikat.

MacWilliams, F. dan Sloane, N., 1977. *The Theory of Error Correcting Codes*. Amsterdam-New York-Oxford North-Holland Publishing Co

Wolf, J. 2008. *An Introduction to Error Correcting Codes Part 1*. New York: Springer.