Jurnal LPPM Bidang Sains dan Teknologi Vol. 8, No. 1, April 2023, 29-35
pISSN: 2407-6074 e-ISSN: 2808-7070

Matriks Maximum Distance Separable Hadamard atas Lapangan Berhingga $\mathbb{Z}_q$

Tesalonika Angela Tumey, Mans Lumiu Mananohas*, Chriestie Montolalu, Septa Windy Nitalessy, Angelina Patricia Amanda, Charles Mongi

Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sam Ratulangi, Manado, 95115

Corresponding author: mansmananohas@unsrat.ac.id

Abstrak

Dalam hal menyamarkan suatu data bisa terjadi suatu kesalahan, sehingga untuk menghindari hal tersebut digunakan kode pengoreksi kesalahan. Kode MDS (*Maximum Distance Separable*) dapat digunakan untuk mengoreksi suatu kesalahan dengan matriks *generator* yang terdiri dari matriks identitas dan suatu matriks A, dimana matriks A merupakan matriks MDS. Suatu matriks dikatakan MDS jika dan hanya jika setiap submatriks bujursangkar memiliki determinan yang tak nol. Dalam penelitian ini digunakan tipe matriks MDS Hadamard atas lapangan berhingga $\mathbb{Z}_q$ dimana $q \leq 7$. Matriks Hadamard atas lapangan berhingga dapat menghemat penggunaan memori sehingga menjadi lebih efisien. Berdasarkan hasil penelitian, dapat disimpulkan tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_q$ di mana $q \leq 7$ sehingga tidak dapat digunakan pada matriks *generator* karena tidak akan menghasilkan performa kode yang optimal untuk mengoreksi suatu kesalahan.

Kata kunci: Matriks MDS Hadamard, submatriks, lapangan berhingga.

Hadamard Maximum Distance Separable Matrix over a Finite Field $\mathbb{Z}_q$

ABSTRACT

In the case of disguising data an error may occur, so an error-correcting code is used to avoid this. MDS code (Maximum Distance Separable) can be used to correct an error with a generator matrix consisting of an identity matrix and a matrix A, where matrix A is the MDS matrix. Matrix A is said to be MDS if and only if each square submatrix has a non-zero determinant. In this research, the Hadamard MDS matrix type is used over a finite field $\mathbb{Z}_q$ where $q \leq 7$. Hadamard matrix on a finite field can save memory usage so it becomes more efficient. Based on the results of the research, it can be concluded that there is no MDS Hadamard matrix measuring 4×4 on a finite field $\mathbb{Z}_q$ where $q \leq 7$ so it cannot be used on the generator matrix because it will not produce optimal code performance to correct an error.

Keywords: Hadamard MDS Matrix, submatrix, finite field.

PENDAHULUAN

Pada zaman sekarang ini untuk menjaga kerahasiaan informasi merupakan hal yang sangat penting. Sebagai contohnya dalam hal pengiriman data baik antara pengirim dan penerima masing-masing tentunya menginginkan kerahasiaan dan perlindungan data. Untuk menjaga kerahasiaan suatu data atau pesan dilakukan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Namun dalam hal menyamarkan suatu data atau pesan bisa terjadi suatu kesalahan pada data atau pesan yang diterima. Oleh karena itu, untuk menghindari hal tersebut digunakan kode pengoreksi kesalahan.

Kode linear merupakan kode yang dapat mengoreksi kesalahan yang terdiri dari kode yang memiliki panjang n, memuat sebanyak k *codeword* serta jarak minimal antar *codeword* d yang dinotasikan sebagai (n, k, d). Kode linear ini dapat memungkinkan agar supaya pengkodean menjadi lebih efisien. Kode linear yang memenuhi batas $d \leq n - k + 1$ (*singleton bound*) adalah kode MDS karena memiliki kemampuan paling terbaik dalam hal

mengoreksi kesalahan dengan matriks generator yang terdiri dari matriks identitas dan suatu matriks A, dimana matriks A merupakan matriks MDS yang dapat menghasilkan performa kode yang optimal baik jarak minimal yang akan menjadi besar ataupun kapasitasnya yang menjadi besar.

Matriks MDS (*Maximum Distance Separable*) merupakan matriks bujursangkar yang memiliki submatriks-submatriks yang *non-singular* atau submatriksnya memiliki determinan yang tak nol. Akibatnya, matriks MDS memiliki entri yang tak nol (Gupta dkk, 2019). Salah satu tipe dari matriks MDS adalah matriks Hadamard atas lapangan berhingga. Matriks Hadamard atas lapangan berhingga adalah matriks berbentuk khusus dengan ukuran $2^n \times 2^n$ atas lapangan berhingga (Sajadieh dkk, 2012). Keuntungan matriks Hadamard atas lapangan berhingga adalah dapat menghemat penggunaan memori sehingga menjadi lebih efisien. Lapangan berhingga adalah lapangan yang memiliki berhingga banyaknya elemen. Contohnya adalah $\mathbb{Z}_q$ dengan q adalah bilangan prima (Vanstone dan Oorschot, 1989).

Pada penelitian yang dilakukan oleh Li dan Wang (2016) dengan judul penelitian "*On the Construction of Lightweight Circulant Involutory MDS Matrices"* difokuskan meneliti tentang konstruksi *Lightweight Hadamard Involutory* dan *Non-Involutory* atas $GL(m, \mathbb{F}_2)$. Pada penelitian ini akan meneliti tentang Matriks *Maximum Distance Separable* Hadamard berukuran 4×4 atas Lapangan Berhingga $\mathbb{Z}_q$ untuk $q \leq 7$.

METODOLOGI PENELITIAN

Waktu dan Tempat

Penelitian ini dilaksanakan mulai bulan Oktober 2021 sampai Januari 2022 dengan tempat penelitian di rumah atau *work from home* dikarenakan pandemi COVID-19.

Metode Penelitian

Metode yang digunakan adalah metode studi pustaka yang berupa mengumpulkan referensi-referensi seperti buku, jurnal maupun sumber-sumber lainnya.

Tahapan Penelitian

1. Menganalisis submatriks dari matriks Hadamard atas lapangan berhingga berukuran 4×4.
2. Menganalisis pertukaran entri pada matriks $Had(a, b, c, d)$
3. Matriks MDS Hadamard atas lapangan berhingga $\mathbb{Z}_q$ dimana $q \leq 7$ berdasarkan sifat-sifat yang telah diperoleh.
4. Menarik kesimpulan.

HASIL DAN PEMBAHASAN

Menganalisis submatriks dari matriks Hadamard atas lapangan berhingga berukuran 4×4

Matriks Hadamard atas lapangan berhingga berukuran 4×4 memiliki bentuk sebagai berikut:

$$Had(a, b, c, d) = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}, \forall a, b, c, d \in \mathbb{Z}_q, q \leq 7$$

Berdasarkan persamaan ini, telah diperiksa untuk submatriks $1 \times 1, 2 \times 2$ dan 3×3 yang selanjutnya akan dianalisis untuk determinannya. Untuk menghitung banyaknya submatriks $1 \times 1, 2 \times 2$ dan 3×3 dapat menggunakan rumus kombinasi.

1) Submatriks berukuran 1×1

Untuk submatriks berukuran 1×1 memiliki sebanyak $C_3^4 \times C_3^4 = 4 \times 4 = 16$ submatriks. Dari 16 submatriks yang diperoleh hanya akan digunakan 4 submatriks berdasarkan bentuk yang berbeda yaitu $[a], [b], [c], [d]$ selanjutnya dengan menggunakan perhitungan

rumus determinan matriks maka diperoleh hasil determinannya adalah a, b, c dan d. Sehingga jelas bahwa untuk $a, b, c, d \neq 0$ karena semua entri dari matriks MDS adalah elemen tak nol.

2) Submatriks berukuran 2×2

Untuk submatriks berukuran 2×2 memiliki sebanyak $C_2^4 \times C_2^4 = 6 \times 6 = 36$ submatriks. Dari 36 submatriks yang diperoleh hanya akan digunakan 11 submatriks berdasarkan hasil determinan yang berbeda yaitu

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

Selanjutnya dengan menggunakan perhitungan rumus determinan matriks maka diperoleh hasil determinan sebagai berikut:

a. $\det \begin{bmatrix} a & b \\ b & a \end{bmatrix} = a^2 - b^2 \neq 0 \leftrightarrow (a+b)(a-b) \neq 0$
b. $\det \begin{bmatrix} a & c \\ c & a \end{bmatrix} = a^2 - c^2 \neq 0 \leftrightarrow (a+c)(a-c) \neq 0$
c. $\det \begin{bmatrix} a & d \\ d & a \end{bmatrix} = a^2 - d^2 \neq 0 \leftrightarrow (a+d)(a-d) \neq 0$
d. $\det \begin{bmatrix} b & c \\ c & b \end{bmatrix} = b^2 - c^2 \neq 0 \leftrightarrow (b+c)(b-c) \neq 0$
e. $\det \begin{bmatrix} b & d \\ d & b \end{bmatrix} = b^2 - d^2 \neq 0 \leftrightarrow (b+d)(b-d) \neq 0$
f. $\det \begin{bmatrix} c & d \\ d & c \end{bmatrix} = c^2 - d^2 \neq 0 \leftrightarrow (c+d)(c-d) \neq 0$
g. $\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = ad - cb \neq 0$
h. $\det \begin{bmatrix} c & a \\ d & b \end{bmatrix} = cb - ad \neq 0$
i. $\det \begin{bmatrix} a & d \\ b & c \end{bmatrix} = ac - db \neq 0$
j. $\det \begin{bmatrix} d & a \\ c & b \end{bmatrix} = db - ac \neq 0$
k. $\det \begin{bmatrix} a & d \\ c & b \end{bmatrix} = ab - dc \neq 0$

Sehingga diperoleh bahwa:

a) Penjumlahan dua bilangan yang tak nol

$$(a+b) \neq 0$$
$$(a+c) \neq 0$$
$$(a+d) \neq 0$$
$$(b+c) \neq 0$$
$$(b+d) \neq 0$$
$$(c+d) \neq 0$$

Oleh karena itu, diperoleh sifat sebagai berikut

$$x + y \neq 0, \forall x, y \in \{a, b, c, d\} \subseteq \mathbb{Z}_q$$

b) Selisih dua bilangan yang tak nol

$$(a-b) \neq 0 \leftrightarrow a \neq b$$
$$(a-c) \neq 0 \leftrightarrow a \neq c$$
$$(a-d) \neq 0 \leftrightarrow a \neq d$$
$$(b-c) \neq 0 \leftrightarrow b \neq c$$
$$(b-d) \neq 0 \leftrightarrow b \neq d$$
$$(c-d) \neq 0 \leftrightarrow c \neq d$$

Oleh karena itu, diperoleh sifat sebagai berikut

$$a \neq b \neq c \neq d \neq 0$$

c) Selisih dari perkalian dua bilangan yang tak nol

$$ad - cb \neq 0$$
$$cb - ad \neq 0$$
$$ac - db \neq 0$$
$$db - ac \neq 0$$

$$ab - dc \neq 0$$

Oleh karena itu, diperoleh sifat sebagai berikut

$$wz - xy \neq 0, \forall w, x, y, z \in \{a, b, c, d\} \subseteq \mathbb{Z}_q$$

3) Submatriks berukuran 3×3

Untuk submatriks berukuran 3×3 memiliki sebanyak $C_1^4 \times C_1^4 = 4 \times 4 = 16$ submatriks. Dari 16 submatriks yang diperoleh hanya akan digunakan 4 submatriks berdasarkan bentuk yang berbeda yaitu

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

Selanjutnya dengan menggunakan perhitungan rumus determinan matriks maka diperoleh hasil determinan sebagai berikut:

a. $\det\begin{bmatrix} a & d & c \\ d & a & b \\ c & b & a \end{bmatrix} = a\begin{bmatrix} a & b \\ b & a \end{bmatrix} - d\begin{bmatrix} d & b \\ c & a \end{bmatrix} + c\begin{bmatrix} d & a \\ c & b \end{bmatrix}$
$= a(a^2 - b^2) - d(da - bc) + c(db - ac)$
$= a^3 - ab^2 - d^2a + dbc + cdb - c^2a$

b. $\det\begin{bmatrix} b & d & c \\ c & a & b \\ d & b & a \end{bmatrix} = b\begin{bmatrix} a & b \\ b & a \end{bmatrix} - d\begin{bmatrix} c & b \\ d & a \end{bmatrix} + c\begin{bmatrix} c & a \\ d & b \end{bmatrix}$
$= b(a^2 - b^2) - d(ca - bd) + c(cb - ad)$
$= ba^2 - b^3 - dca + d^2b + c^2b - cad$

c. $\det\begin{bmatrix} b & a & c \\ c & d & b \\ d & c & a \end{bmatrix} = b\begin{bmatrix} d & b \\ c & a \end{bmatrix} - a\begin{bmatrix} c & b \\ d & a \end{bmatrix} + c\begin{bmatrix} c & d \\ d & c \end{bmatrix}$
$= b(da - bc) - a(ca - bd) + c(c^2 - d^2)$
$= bda - b^2c - a^2c + abd + c^3 - cd^2$

d. $\det\begin{bmatrix} b & a & d \\ c & d & a \\ d & c & b \end{bmatrix} = b\begin{bmatrix} d & a \\ c & b \end{bmatrix} - a\begin{bmatrix} c & a \\ d & b \end{bmatrix} + d\begin{bmatrix} c & d \\ d & c \end{bmatrix}$
$= b(db - ac) - a(cb - ad) + d(c^2 - d^2)$
$= b^2d - bac - acb + a^2d + dc^2 - d^3$

Menganalisis pertukaran entri pada matriks $Had(a, b, c, d)$

Untuk pertukaran entri pada matriks $Had(a, b, c, d)$ dilakukan dengan menggunakan kombinasi. Sehingga terdapat $4! = 24$ banyaknya kombinasi seperti berikut ini

$$\begin{gathered}(a,b,c,d),(a,b,d,c),(a,c,b,d),(a,c,d,b),\\(a,d,b,c),(a,d,c,b),(b,a,c,d),(b,a,d,c),\\(b,c,a,d),(b,c,d,a),(b,d,a,c),(b,d,c,a)\\(c,a,b,d),(c,a,d,b),(c,b,a,d),(c,b,d,a),\\(c,d,a,b),(c,d,b,a),(d,a,b,c),(d,a,c,b),\\(d,b,a,c),(d,b,c,a),(d,c,a,b),(d,c,b,a)\end{gathered}$$

1. $Had(a, b, c, d) = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$

$= a\begin{bmatrix} a & d & c \\ d & a & b \\ c & b & a \end{bmatrix} - b\begin{bmatrix} b & d & c \\ c & a & b \\ d & b & a \end{bmatrix} + c\begin{bmatrix} b & a & c \\ c & d & b \\ d & c & a \end{bmatrix} - d\begin{bmatrix} b & a & d \\ c & d & a \\ d & c & b \end{bmatrix}$

$= a(a^3 - ab^2 - d^2a + dbc + cdb - c^2a) - b(ba^2 - b^3 - dca + d^2b + c^2b - cad) + c(bda - b^2c - a^2c + abd + c^3 - cd^2)$
$- d(b^2d - bac - acb + a^2d + dc^2 - d^3)$

2. $Had(a,b,d,c) = \begin{bmatrix} a & b & d & c \\ b & a & c & d \\ d & c & a & b \\ c & d & b & a \end{bmatrix}$

$= a\begin{bmatrix} a & c & d \\ c & a & b \\ d & b & a \end{bmatrix} - b\begin{bmatrix} b & c & d \\ d & a & b \\ c & b & a \end{bmatrix} + d\begin{bmatrix} b & a & d \\ d & c & b \\ c & d & a \end{bmatrix} - c\begin{bmatrix} b & a & c \\ d & c & a \\ c & d & b \end{bmatrix}$

$= a(a^3 - ab^2 - c^2a + cdb + dbc - d^2a) - b(ba^2 - b^3 - cad + c^2b + d^2b - dca) + d(bca - b^2d - a^2d + abc + d^3 - dc^2) - c(b^2c - bad - adb + a^2c + cd^2 - c^3)$

3. $Had(b,a,c,d) = \begin{bmatrix} b & a & c & d \\ a & b & d & c \\ c & d & b & a \\ d & c & a & b \end{bmatrix}$

$= b\begin{bmatrix} b & d & c \\ d & b & a \\ c & a & b \end{bmatrix} - a\begin{bmatrix} a & d & c \\ c & b & a \\ d & a & b \end{bmatrix} + c\begin{bmatrix} a & b & c \\ c & d & a \\ d & c & b \end{bmatrix} - d\begin{bmatrix} a & b & d \\ c & d & b \\ d & c & a \end{bmatrix}$

$= b(b^3 - ba^2 - d^2b + dac + cda - c^2b) - a(ab^2 - a^3 - dcb + d^2a + c^2a - cbd) + c(adb - a^2c - b^2c + bad + c^3 - cd^2) - d(a^2d - abc - bca + b^2d + dc^2 - d^3)$

4. $Had(b,a,d,c) = \begin{bmatrix} b & a & d & c \\ a & b & c & d \\ d & c & b & a \\ c & d & a & b \end{bmatrix}$

$= b\begin{bmatrix} b & c & d \\ c & b & a \\ d & a & b \end{bmatrix} - a\begin{bmatrix} a & c & d \\ d & b & a \\ c & a & b \end{bmatrix} + d\begin{bmatrix} a & b & d \\ d & c & a \\ c & d & b \end{bmatrix} - c\begin{bmatrix} a & b & c \\ d & c & b \\ c & d & a \end{bmatrix}$

$= b(b^3 - ba^2 - c^2b + cad + dca - d^2b) - a(ab^2 - a^3 - cdb + c^2a + d^2a - dbc) + d(acb - a^2d - b^2d + bac + d^3 - dc^2) - c(a^2c - abd - bda + b^2c + cd^2 - c^3)$

5. $Had(c,d,a,b) = \begin{bmatrix} c & d & a & b \\ d & c & b & a \\ a & b & c & d \\ b & a & d & c \end{bmatrix}$

$= c\begin{bmatrix} c & b & a \\ b & c & d \\ a & d & c \end{bmatrix} - d\begin{bmatrix} d & b & a \\ a & c & d \\ b & d & c \end{bmatrix} + a\begin{bmatrix} d & c & a \\ a & b & d \\ b & a & c \end{bmatrix} - b\begin{bmatrix} d & c & b \\ a & b & c \\ b & a & d \end{bmatrix}$

$= c(c^3 - cd^2 - b^2c + bda + abd - a^2c) - d(dc^2 - d^3 - bac + b^2d + a^2d - acb) + a(dbc - d^2a - c^2a + cdb + a^3 - ab^2) - b(d^2b - dca - cad + c^2b + ba^2 - b^3)$

6. $Had(c,d,b,a) = \begin{bmatrix} c & d & b & a \\ d & c & a & b \\ b & a & c & d \\ a & b & d & c \end{bmatrix}$

$= c\begin{bmatrix} c & a & b \\ a & c & d \\ b & d & c \end{bmatrix} - d\begin{bmatrix} d & a & b \\ b & c & d \\ a & d & c \end{bmatrix} + b\begin{bmatrix} d & c & b \\ b & a & d \\ a & b & c \end{bmatrix} - a\begin{bmatrix} d & c & a \\ b & a & c \\ a & b & d \end{bmatrix}$

$= c(c^3 - cd^2 - a^2c + adb + bad - b^2c) - d(dc^2 - d^3 - abc + a^2d + b^2d - bca) + b(dac - d^2b - c^2b + cda + b^3 - ba^2) - a(d^2a - dcb - cbd + c^2a + ab^2 - a^3)$

7. $Had(d,c,a,b) = \begin{bmatrix} d & c & a & b \\ c & d & b & a \\ a & b & d & c \\ b & a & c & d \end{bmatrix}$

$= d\begin{bmatrix} d & b & a \\ b & d & c \\ a & c & d \end{bmatrix} - c\begin{bmatrix} c & b & a \\ a & d & c \\ b & c & d \end{bmatrix} + a\begin{bmatrix} c & d & a \\ a & b & c \\ b & a & d \end{bmatrix} - b\begin{bmatrix} c & d & b \\ a & b & d \\ b & a & c \end{bmatrix}$

$= d(d^3 - dc^2 - b^2d + bca + abc - a^2d) - c(cd^2 - c^3 - bad + b^2c + a^2c - adb) + a(cbd - c^2a - d^2a + dcb + a^3 - ab^2) - b(c^2b - cda - dac + d^2b + ba^2 - b^3)$

8. $Had(d,c,b,a) = \begin{bmatrix} d & c & b & a \\ c & d & a & b \\ b & a & d & c \\ a & b & c & d \end{bmatrix}$

$= d\begin{bmatrix} d & a & b \\ a & d & c \\ b & c & d \end{bmatrix} - c\begin{bmatrix} c & a & b \\ b & d & c \\ a & c & d \end{bmatrix} + b\begin{bmatrix} c & d & b \\ b & a & c \\ a & b & d \end{bmatrix} - a\begin{bmatrix} c & d & a \\ b & a & d \\ a & b & c \end{bmatrix}$

$= d(d^3 - dc^2 - a^2d + acb + bac - b^2d) - c(cd^2 - c^3 - abd + a^2c + b^2c - bda) + b(cad - c^2b - d^2b + dca + b^3 - ba^2) - a(c^2a - cdb - dbc + d^2a + ab^2 - a^3)$

Dilakukan kombinasi yang lainnya dan diperoleh 24 matriks Hadamard tersebut memiliki determinan yang sama. Hal ini membuktikan apabila dilakukan pertukaran entri pada matriks $Had(a,b,c,d)$ akan menghasilkan determinan yang sama.

Matriks MDS Hadamard atas lapangan berhingga $\mathbb{Z}_q$ dimana $q \leq 7$ berdasarkan sifat-sifat yang telah diperoleh

Proposisi 1. Tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_2$ dan $\mathbb{Z}_3$.

Bukti.
Berdasarkan sifat yang telah diperoleh $a \neq b \neq c \neq d \neq 0$, sehingga mengakibatkan bahwa tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_2$ dan $\mathbb{Z}_3$ yang masing-masing memiliki 2 dan 3 elemen.

Proposisi 2. Tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_5$.

Bukti.
Himpunan $\mathbb{Z}_5 = \{0,1,2,3,4\}$ dengan anggota tak nol yang dinotasikan sebagai $\mathbb{Z}_5 - \{0\}$. Berdasarkan sifat $x + y \neq 0, \forall x, y \in \{a,b,c,d\} \subseteq \mathbb{Z}_5 - \{0\}$, diperoleh jika $a = 1$ maka $b,c,d \neq 4$, jika $a = 2$ maka $b,c,d \neq 3$, jika $a = 3$ maka $b,c,d \neq 2$, jika $a = 4$ maka $b,c,d \neq 1$. Perhatikan bahwa pasti ada setidaknya dua elemen yang tidak bisa dipilih secara bersamaan yaitu 1 dan 4, serta 2 dan 3. Oleh karena suatu matriks Hadamard berukuran 4×4 harus memenuhi syarat $a \neq b \neq c \neq d \neq 0$ maka harus ada setidaknya 4 elemen berbeda yang dapat dipilih secara bersamaan dan hal ini kontradiksi dengan analisis pada $\mathbb{Z}_5$ dimana dari 4 elemen pada $\mathbb{Z}_5 - \{0\}$ terdapat dua pasangan elemen yang tidak dapat dipilih secara bersamaan artinya elemen yang dapat dipilih secara bersamaan hanya 2 elemen yaitu 1 atau 4 dan 2 atau 3 yang mana kurang dari 4 elemen. Sehingga jelas terbukti bahwa tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_5$.

Proposisi 3. Tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_7$.

Bukti.
Himpunan $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ dengan anggota tak nol yang dinotasikan sebagai $\mathbb{Z}_7 - \{0\}$**.** Berdasarkan sifat $x + y \neq 0, \forall x, y \in \{a,b,c,d\} \subseteq \mathbb{Z}_7 - \{0\}$, diperoleh bahwa jika $a = 1$ maka $b,c,d \neq 6$, jika $a = 2$ maka $b,c,d \neq 5$, jika $a = 3$ maka $b,c,d \neq 4$, jika $a = 4$ maka $b,c,d \neq 3$, jika $a = 5$ maka $b,c,d \neq 2, \text{jika } a = 6 \text{ maka } b,c,d \neq 1$. Perhatikan bahwa pasti ada setidaknya dua elemen yang tidak bisa dipilih secara bersamaan yaitu 1 dan 6, 2 dan 5, serta 3 dan 4. Oleh karena suatu matriks Hadamard berukuran 4×4 harus memenuhi syarat $a \neq b \neq c \neq d \neq 0$ maka harus ada setidaknya 4 elemen berbeda yang dapat dipilih secara bersamaan dan hal ini kontradiksi dengan analisis pada $\mathbb{Z}_7$ dimana dari 6 elemen pada $\mathbb{Z}_7 - \{0\}$ terdapat tiga pasangan elemen yang tidak dapat dipilih secara bersamaan artinya elemen yang dapat dipilih secara bersamaan hanya 3 elemen yaitu 1 atau 6, 2 atau 5 dan 3 atau 4 yang mana kurang dari 4 elemen. Sehingga jelas terbukti bahwa tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_7$.

KESIMPULAN

Berdasarkan hasil penelitian, maka diperoleh kesimpulan bahwa tidak ada matriks MDS Hadamard berukuran 4×4 atas lapangan berhingga $\mathbb{Z}_q$ dimana untuk $q \leq 7$ sehingga tidak dapat digunakan pada matriks generator karena tidak akan menghasilkan performa kode yang optimal untuk mengoreksi suatu kesalahan.

DAFTAR PUSTAKA

Bezeer, R.A. 2015. *A First Course in Linear Algebra Version* 3.50. Congruent Press, Washington.

Gupta, K.C., S.K. Pandey, I.G. Ray, dan S. Samanta. 2019. Cryptographically Significant MDS Matrices Over Finite Fields: A Brief Survey And Some Generalized Results. Advances in Mathematics of Communications. **13(4)** : 779-843.

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

Harvile, D.A. 1997. *Matrix Algebra From a Statistician's perspective*. Springer Verlag, New York.

Imrona, M. 2002. Aljabar Linier Elementer. Sekolah Tinggi Teknologi Telkom, Bandung.

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

Li, Y. dan M. Wang. 2016. *On the Construction of Lightweight Circulant Involutory MDS Matrices*. FSE 2016, Bochum.

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

Sajadieh, M., M. Dakhilalian, H. Mala dan B. Omoomi. 2012. On construction of involutory MDS matrices from Vandermonde Matrices in GF(2^q). Design, Codes Cryptography. **64** : 287-308.

Vanstone, S.A. dan P.C.V. Oorschot. 1989. *An Introduction To Error Correcting Codes With Applications*. Springer, New York.

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