HADAMARD TRANSFORM: SUATU PROSES *DECODING* PADA KODE REED MULLER ORDE PERTAMA

Luthfi Nur Azizah[1)], Salmaini Safitri Syam[2)]
[1] Pascasarjana Pendidikan Matematika, Universitas Negeri Yogyakarta
email: luthfinurazizah.2017@student.uny.ac.id
[2] Pascasarjana Pendidikan Matematika, Universitas Negeri Yogyakarta
email: salmaini_syam.2017@student.uny.ac.id

Abstract

Order pertama kode Reed Muller dinotasikan dengan $R(1,r)$ merupakan sub ruang yang dibangun oleh vektor $v_1, v_2 \dots v_r$. Pesan yang dikirimkan oleh transmitter dapat mengalami gangguan dan menyebabkan adanya kesalahan atau kerusakan. Adanya kemungkinan kesalahan tersebut, dapat dideteksi melalui proses decoding. Hadamard Transform merupakan salah satu proses decoding yang efisien untuk mendeteksi kesalahan pada order pertama kode Reed Muller. Suatu vektor biner r dengan 2^r-tuple akan ditransformasikan dengan Hadamard Transform dan menghasilkan pesan asli yaitu $\hat{R}$. Komponen pada $\hat{R}$ berhubungan dengan r-tuple yang akan dinyatakan dengan bilangan bulat 1 dan -1.

Keywords: *Order pertama kode Reed Muller, proses decoding, Hadamard Transform, vektor biner*

1. PENDAHULUAN

Seiring perkembangan ilmu pengetahuan dan teknologi, informasi atau pesan dapat dengan mudah diakses. Pengiriman informasi atau pesan tersebut dapat dilakukan melalui *encoder*, saluran transmisi maupun *decoder*. Proses pengiriman pesan yang dikirimkan oleh transmitter dapat mengalami gangguan dan menyebabkan adanya kesalahan atau kerusakan. Adanya kemungkinan kesalahan tersebut, dapat dideteksi melalui proses decoding. Pesan yang dikirim tersebut merupakan sebuah kode yang di dalanya memuat vector atau disebut sebagai kata kode. Pada umumnya, kata kode terdiri dari gabungan dua sub vektor yaitu pesan asli dan simbol cek tambahan.

Adapun contoh bentuk awal dari suatu pesan adalah:

$$p = p_0 p_1 p_2 \cdots p_{k-1}$$

Kemudian melalui proses encoding, maka pesan tersebut akan menjadi

$$c = c_0 c_1 c_2 \dots c_{k-1} c_k c_{k+1} \dots c_{n-1}$$

Dengan pesan asli pada kata kode tersebut adalah

$$c_0 c_1 c_2 \dots c_{k-1} = p_0 p_1 p_2 \dots p_{k-1}$$

Pada tulisan ini akan dibahas tentang salah satu kelas khusus dalam kode linear yaitu kode Reed Muller. Kode Reed Muller merupakan salah satu kode koreksi kesalahan tertua (Khalifa, 2008, p. 729). Kode ini ditemukan oleh D. E. Muller pada tahun 1954 dan algoritma decoding pertama dibuat oleh I. S. Reed, pada tahun 1954. Kode Reed-Muller digunakan oleh Mariner 9 untuk mengirim foto hitam dan putih Mars pada tahun 1972. Salah satu keuntungan utama Kode Reed-Muller adalah relatif sederhana untuk menyandikan pesan dan memecahkan kode yang diterima transmisi (Shukina, 2013, p. 30).

Salah satu pertanyaan penting tentang analisis algoritma decoding adalah memperkenalkan definisi yang memadai dari kompleksitas algoritma (Ashikhmin1 & Litsyn, 1996, p. 187). Dalam mengkonstruksi kode Reed Muller ($R(1,r)$) dan proses decodingnya menggunakan sebuah transformasi yang disebut Hadamard Transform.

Hadamard Transform merupakan salah satu proses decoding yang efisien untuk mendeteksi kesalahan pada order pertama kode Reed Muller. Suatu vektor biner r dengan 2^r-tuple akan ditransformasikan dengan Hadamard Transform dan menghasilkan pesan asli yaitu $\hat{R}$. Komponen pada $\hat{R}$ berhubungan dengan r-tuple yang akan dinyatakan dengan bilangan bulat 1 dan -1.

2. KAJIAN LITERATUR

A. *First Order Reed-Muller Codes*

Misalkan H_r merupakan matriks *parity check* untuk kode Hamming biner $(2^r, 2^r - 1 - r)$ tentang matriks *parity check*. Kolom $2^r - 1$ terdiri dari semua kemungkinan r −tuple bukan nol. Menentukan $B_r = [H_r, 0]$, dengan H_r adalah kolom adjoin yang memuat 0. Misalkan, $v_1, v_2 \ldots v_r$ merupakan baris dari B_r, dan misalkan 1 merupakan vektor baris dengan panjang 2^r yang semua anggotanya terdiri dari 1 (Vanstone, 1989, p. 115).

Definisi 2.1
(Order Pertama Kode Reed Muller)
Order pertama kode *Reed Muller* dinotasikan $R(1,r)$, yang merupakan sub ruang yang dibangun oleh vektor $v_1, v_2 \ldots v_r$
$R(1,r)$ adalah kode biner dengan matrik generator

$$G = \begin{bmatrix} 1 \\ \hline B_r \end{bmatrix} = \begin{bmatrix} 1 \\ \hline H_r 0 \end{bmatrix}$$

Pada kode $R(1,r)$, untuk memecahkan kode penerimaan vektor r dapat menggunakan suatu transformasi yang disebut dengan ***Hadamard transform*** vektor R diturunkan dari r. *Hadamard transform* berhubungan dengan tipe matriks khusus yang disebut dengan ***Hadamard matrix***. Sebelum mengetahui *Hadamard transform* dan prosedur pemecahan untuk $R(1,r)$, terlebih dulu kita harus mengetahui tentang *Hadamard matrix.*

B. Matriks Hadamard

Definisi 2.2
(Matriks Hadamard)
Matriks Hadamard H_n dari order n adalah sebuah matriks $n \times n$ dengan entri bilangan bulat $+1$ dan -1 yang barisnya merupakan pasangan orthogonal sebagai bilangan real.

Diberikan sebuah Matriks Hadamard H_n pada order n, pengkonstruksian matrik adalah sebagai berikut

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

Dua Matriks Hadamard setara jika apabila dilakukan permutasi baris dan kolom dengan mengalikan beberapa baris atau kolom dengan -1 (Yildiz, 2011, p. 12). Dalam mengkonstruksi Matriks Hadamard dapat dilakukan dengan Perkalian Kronecker atau Proper Order.

Definisi 2.3
(Perkalian Kronecker)
Misalkan $A = [a_{ij}]$ dan $B = [b_{ij}]$ merupakan matriks persegi yang masing-masing berada pada order m dan n. *Perkalian Kronecker* pada A dan B dinotasikan dengan $A \times B$, yang merupakan matriks $mn \times mn$

$$A \times B = [a_{ij}\, B]$$

Diperoleh dengan mengganti entri (i,j) pada A dengan matrik $a_{ij}\, B$, matrik B dengan masing-masing entri dikalikan dengan a_{ij}.

Definisi 2.4
(Proper Order)
Proper order P_r, pada r-tuple biner adalah order yang didefinisikan secara rekursif dengan aturan
(1) $P_1 = [0,1]$
(2) Jika $P_i = [b_1, b_2, \cdots b_{2^i}]$ maka $P_{i+1} = [b_1 0,\ b_2 0, \cdots b_{2^i} 0,\ b_1 1,\ b_2 1, \cdots b_{2^i} 1]$
untuk $1 \le i \le r - 1$

C. Transformasi Hadamard

Definisi 2.5
(Transformasi Hadamard)
Transformasi Hadamard dari 2^r-tuple R adalah 2^r-tuple $\hat{R}$ ketika komponen dari $\hat{R}$ berhubungan dengan r-tuple $u \in V_r$ adalah

$$\hat{R} = \sum_{v \in V_r} (-1)^{u \cdot v} R(v)$$

Dengan komponen R menjadi bilangan bulat $+1$ dan -1, komponen $\hat{R}$ akan menjadi bilangan bulat, karena $R(v) = (-1)^{r(v)}$
Sehingga :

$$\hat{R} = \sum_{v \in V_r} (-1)^{u \cdot v + r(v)}$$

3. ALGORITMA DECODING ORDER PERTAMA KODE RED MULLER

Algoritma dalam membaca order pertama kode Reed Muller adalah sebagai berikut (Vanstone, 1989, p. 125)

- Misalkan r merupakan vektor penerimaan biner dengan panjang 2^r
- Misalkan kolom pada B_r merupakan *proper ordering* P_r
- Misalkan H sebagai matrik Hadamard $H = H(2^r)$

a. Substitusi R dan $\hat{R}$ ke $R(u) = (-1)^{r(u)}$ dan $\hat{R} = RH$
b. Menemukan komponen $\hat{R}(u)$ pada R yang besarnya maksimum, misalnya
$$u = (u_1, \cdots u_r)^T$$
c. Jika $\hat{R}(u) > 0$, maka membaca kode r sebagai $\sum_{i=1}^{r} u_i v_i$
d. Jika $\hat{R}(u) \leq 0$, maka membaca kode r sebagai $1 + \sum_{i=1}^{r} u_i v_i$

4. PROSES DECODING PADA KODE REED MULLER ORDE PERTAMA

Proses decoding dengan menggunakan transformasi Hadamard memerlukan matriks Hadamard.

Misalnya untuk mengkonstruksi sebuah matrik generator untuk $R(1,3)$ menggunakan

$$B_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

Matrik generator yang sesuai dengan B_3 adalah

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

Dengan menggunakan *proper ordering* P_3 dapat dikonstruksikan Matriks Hadamard

$$H = H(2^3)$$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Misalkan terdapat $r = (0111\ 0110)$ yang diterima oleh alat pembaca sandi. Selanjutnya, dari r, dapat diturunkan menjadi R. Komponen ke-i di B_3 berkaitan dengan komponen ke-i di r.
Untuk menentukan R, perlu diperhatikan kembali antara vektor pada B_3 dengan setiap komponen pada r yang didefinisikan seperti pada algoritma (a) yaitu

$$R(u) = (-1)^{r(u)}$$

Berikut langkah untuk menentukan komponen pada R.

$$R(100) = (-1)^{r(100)} = (-1)^0 = 1$$
$$R(010) = (-1)^{r(010)} = (-1)^1 = -1$$
$$R(001) = (-1)^{r(001)} = (-1)^1 = -1$$
$$R(110) = (-1)^{r(110)} = (-1)^1 = -1$$
$$R(011) = (-1)^{r(011)} = (-1)^0 = 1$$
$$R(101) = (-1)^{r(101)} = (-1)^1 = -1$$
$$R(111) = (-1)^{r(111)} = (-1)^1 = -1$$
$$R(000) = (-1)^{r(000)} = (-1)^0 = 1$$

Sehingga, diperoleh

$$R = (1, -1, -1, -1, 1, -1, -1, 1)$$

Selanjutnya, dengan perkalian vektor matriks, akan ditentukan $\hat{R}$, di mana $\hat{R} = RH$.

$$\hat{R} = (1 \ -1 \ -1 \ -1 \ \ 1 \ -1 \ -1 \ \ 1) \times$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

$$\hat{R} = (-2 \ \ 2 \ \ 2 \ \ 6 \ -2 \ \ 2 \ \ 2 \ -2)$$

Kemudian, dilanjutkan pada algoritma (b) yaitu menemukan komponen $\hat{R}(u)$ pada R yang besarnya maksimum, misalnya

$$u = (u_1, \cdots u_r)^T$$

Komponen terbesar dari $\hat{R}$ berada pada kolom ke 4. Komponen ini bersesuaian pula dengan kolom ke 4 dari B_3, sehingga diperoleh $u = (110)^T$.

Karena entri $\hat{R}\big((110)\big) = 6$ dan 6>0, maka kode r dapat dibaca sesuai dengan algoritma (c) yaitu sebagai berikut.

$$c = \sum_{i=1}^{3} u_i v_i = 1 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3$$
$$= 1 \cdot (0101\ 0101) + 1 \cdot (0011\ 0011) + 0 \cdot (0000\ 1111)$$
$$= (0110 \ \ 0110)$$

Berdasarkan proses decoding yang telah dilakukan, maka diperoleh hasil $c = (0110 \ \ 0110)$ dengan kata kode yang diterima dalam bentuk $r = (0111 \ \ 0110)$.

5. KESIMPULAN

Adanya kemungkinan kesalahan pada Order pertama kode Reed Muller $R(1, r)$, dapat dideteksi melalui proses decoding. *Hadamard Transform* merupakan salah satu proses decoding yang efisien untuk mendeteksi kesalahan pada order pertama kode Reed Muller. Hasil dari proses ini akan memberikan $\hat{R}$ yang berupa vektor.

Dalam membaca kode Reed Muller terdapat dua kemungkinan, yaitu (1) jika $\hat{R}(u) > 0$, maka membaca kode r sebagai $c = \sum_{i=1}^{r} u_i v_i$ atau (2) jika $\hat{R}(u) \leq 0$, maka membaca kode r sebagai $c = 1 + \sum_{i=1}^{r} u_i v_i$.

.

6. REFERENSI

Ashikhmin1, A. E., & Litsyn, S. N. (1996). Fast Decoding Algorithms for First Order Reed-Muller and Related Codes. *Designs, Codes and Cryptography*, *7*(3), 187–214. https://doi.org/https://doi.org/10.1023/A:1018057506207

Khalifa, O. O. et al. (2008). Reed-Muller codec simulation performance. *Journal of Computer Science*, *4*(10), 792–798. https://doi.org/10.3844/jcssp.2008.792.798

Shukina, O. (2013). *Implementation and comparison of the Golay and first order Reed-Muller codes*. Florida Atlantic University. Retrieved from https://fau.digital.flvc.org/islandora/object/fau%3A4226/datastream/OBJ/view/Implementation_and_comparison_of_the_Golay_and_first_order_Reed-Muller_codes.pdf

Vanstone, S. A. & O. (1989). *An Introduction to Error Correcting Codes With Applications*. Massachusetts: Kluwer Academic Publisher.

Yildiz, B. ; et al. (2011). *Coding Theory Lecture Notes*. Retrieved from https://www.math.uci.edu/~nckaplan/teaching_files/kaplancodingnotes.pdf