J M S K
Jurnal Matematika, Statistika, & Komputasi
http://journal.unhas.ac.id/index.php/jmsk
Vol 13, No 2,122-127 , Januari 2017
ISBN:1858-1382

# Proses Decoding Kode Reed Muller Orde Pertama Menggunakan Transformasi Hadamard

Andi Kresna Jaya*

## Abstract

The first order Reed Muller, that is written R(1,*r*), is obtained by construction variation from dual of extended Hamming code. Error from message or image through satellite transmission use R(1,*r*) code will be easier to detected with decoding process. One of the efficient process decoding is Hadamard transformation. A vector message, binary vector tuple-$2^n$, is transformed by Hadamard transformation and output transformation is $\boldsymbol{R}$ real vector tuple-$2^n$ with entries 1 and -1. Then $R$ is transformed with Hadamard Matrix can be $\hat{R}$ real vector.

Key Word: *Kode Reed Muller orde pertama* (R(1,*r*)), *matriks Hadamard, proses decoding, simbol pengecek, transformasi Hadamard, vektor pesan*.

## 1. Pendahuluan

Pesatnya perkembangan ilmu pengetahuan dan teknologi mendorong pertukaran informasi sebanyak-banyaknya dari suatu tempat ke tempat lain. Dalam teknologi informatika, informasi/pesan dikirim berupa data melalui encoder, saluran transmisi dan decoder. Pesan yang terkirim melalui encode berupa barisan karakter biner (0 dan 1) di saluran transmisi dapat saja mengalami gangguan yang menyebabkan kesalahan pada penerimaan pesan. Pada decoder pesan yang diterima diuraikan kembali menjadi pesan asli setelah dideteksi dan dikoreksi kesalahannya.

Kode merupakan hasil proses encoding dari semua pesan-pesan yang siap dikirimkan, sedangkan vektor di dalam Kode disebut kata kode. Kata kode umumnya terdiri dari gabungan dua sub vektor yaitu pesan asli dan simbol cek tambahan. Misalnya dalam bentuk pesan awal :

$$m = m_0 m_1 m_2 \cdots m_{k-1}$$

dengan proses encoding, menjadi :

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

dimana pesan asli pada kata kode $c$ tersebut adalah

$$c_0 c_1 c_2 \cdots c_{k-1} = m_0 m_1 m_2 \cdots m_{k-1}$$

dan

$c_k c_{k+1} \cdots c_{n-1}$ sebagai simbol cek tambahan.

Tulisan ini membahas tentang konstruksi kode R(1,*r*) dan proses decodingnya menggunakan transformasi Hadamard dan memperlihatkan algoritma sederhana dari proses decoding tersebut. Kode ini pertama kali diterapkan oleh pesawat Mariner IX untuk pengiriman gambar hitam putih pada tahun 1972.

* *Staf Pengajar pada Jurusan Matematika F.MIPA Universitas Hasanuddin Makassar*

## 2. Kode linier C($n$,$k$,$d$) dan kode dualnya C$^{\perp}$($n$,$n$-$k$,$d$)

Kode linier C($n$,$k$,$d$) adalah sub ruang berdimensi $k$ dari ruang biner berdimensi $n$ ($GF(2^n)$). Sedangkan $d$ merupakan minimum jarak Hamming atau minimum banyaknya posisi koordinat untuk dua buah vektor kode (kata kode). Untuk menghitung jarak Hamming sebuah kode yang mempunyai $m$ kata kode, harus dilihat semua jarak dari pasangan kata kodenya. Misalkan Kode C adalah sub ruang berdimensi k dari ruang vektor $GF(2^n)$ di mana $k<n$.

$$C = \left\{C_1, C_2, C_3, \cdots, C_m \middle| C_i = c_1 c_2 c_3 \cdots c_n, \quad c_j \in GF(2),\ i = 1,2,3,\cdots,m,\ j = 1,2,3,\cdots,n\right\}$$
$$d = \min\left\{d(C_i, C_k) \middle| C_i \neq C_k, i \neq k\right\}$$

Kode linier tersebut sesungguhnya merupakan range dari transformasi linier dari himpunan pesan asli yang diuraikan dalam bentuk biner sebagai ruang $GF(2^k)$ ke ruang biner $GF(2^n)$. Bentuk transformasi ini bisa disajikan sebagai matriks $G$ berukuran $k \times n$, sehingga kata kode $c$ di C($n$,$k$,$d$) diperoleh sebagai hasil perkalian vektor pesan ***m*** dengan matriks $G$, untuk setiap vektor pesan ***m*** dalam $GF(2^k)$.

Matriks $G$ dikenal sebagi matriks perentang untuk kode linier C($n$,$k$), yang baris-barisnya merupakan vektor-vektor basis dari C($n$,$k$). Matriks perentang dalam bentuk baku dapat ditulis sebagai :

$$G = \left[I_k \vdots A\right]$$

di mana :

$I_k$ adalah entri-entri pada matriks identitas orde $k$.

$A$ adalah matriks berukuran $k \times (n-k)$ yang entri-entrinya 0 dan 1.

Bentuk matriks perentang tidak tunggal karena dengan operasi baris elementer pada $G$ menghasilkan suatu matriks yang juga merupakan perentang yang lain untuk kode C($n$,$k$,$d$).

Kata kode $c$ diperoleh sebagai hasil perkalian vektor pesan $m$ dengan matriks $G$, untuk setiap $m \in GF(2^k)$, yaitu :

$$E : GF(2^k) \to GF(2^n)$$
$$m \mapsto c = mG$$

Misalkan vektor pesan $m$ = (1 0 1) di $GF(2^3)$ maka dengan matriks $G$ diperoleh

$$mG = (101)\begin{pmatrix} 10000 \\ 01010 \\ 00111 \end{pmatrix} = (10111)$$

Selain kode C($n$,$k$), dalam ruang $GF(2^n)$ terdapat juga sub ruang yang merupakan komplemen ortogonal dari kode C yaitu kode linier ($n$,$n$-$k$). Disebut komplemen ortogonal karena perkalian dot (kali dalam) antara vektor di C dan komplemennya adalah 0 (skalar nol). Kode linier yang merupakan komplemen dari C($n$,$k$) dinyatakan sebagai kode dual C dan ditulis dalam bentuk himpunan $C^{\perp} = \left\{b \in GF\left(2^n\right) \middle| b \bullet c = 0, \forall c \in C\right\}$.

Yang menarik di sini adalah matriks perentang dari C$^{\perp}$ merupakan matriks pengecek untuk C, demikian pula sebaliknya. Secara khusus, jika $G = \left[I_k \vdots A\right]$ adalah

matriks perentang C, maka matriks perentang untuk kode dualnya berbentuk $H = \left[A^T \vdots I_{n-k}\right]$.

## 3. Konstruksi kode R(1,*r*) dari Kode Hamming ($2^r$–1, $2^r$–1–*r*,3)

Pandang kode linier dengan matriks pengeceknya adalah ***H***. Kode ini akan dikonstruksi menjadi kode baru baik dengan penambahan atau pengurangan simbol pengecek maupun simbol pesan.

Kode linier C(*n*,*k*) disebut juga kode Hamming(*n*,*k*) jika $n = 2^m - 1$ dan $k = n - m$ dengan matriks pengecek ***H*** adalah matriks berukuran $k \times n$ sedemikian sehingga kolom-kolomnya adalah semua vektor tak nol dalam ruang *GF*($2^m$).

Kode Hamming merupakan kode linier C(*n*,*k*,*d*) dimana $n=2^r-1$ dan $k=n-r$ dengan matriks pengeceknya adalah matriks berukuran $r \times n$ sedemikian sehingga kolom-kolomnya adalah semua vektor dalam *GF*($2^r$) yang tidak nol.

Konstruksi kode baru dari kode Hamming ($2^r$–1, $2^r$–1–*r*,3) dapat dilihat pada diagram berikut:

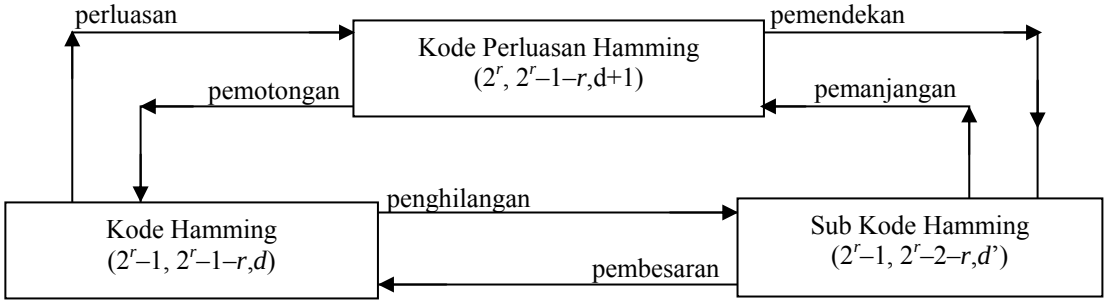


Diagram 1. Variasi kode dari kode Hamming

Misalkan $\boldsymbol{H_r}$ adalah matriks pengecek kode Hamming. $\boldsymbol{H_r}$ memuat $2^r - 1$ vektor kolom terurut *r* yang tidak nol. Kode dualnya adalah kode linier ($2^r$-1,*r*) dengan matriks perentangnya adalah matriks pengecek kode Hamming. Konstruksi kode dual Hamming mempunyai kata kode yang berbobot $2^r$-1, kecuali vektor nol.

Konstruksi kode baru dari kode dual Hamming dengan penambahan simbol pesan akan diperoleh kode Reed Muller orde pertama. Dual dari variasi konstruksi kode Hamming pada diagram di atas merupakan konstruksi dari dual kode Hamming. Diagram konstruksinya dapat dilihat pada diagram berikut:

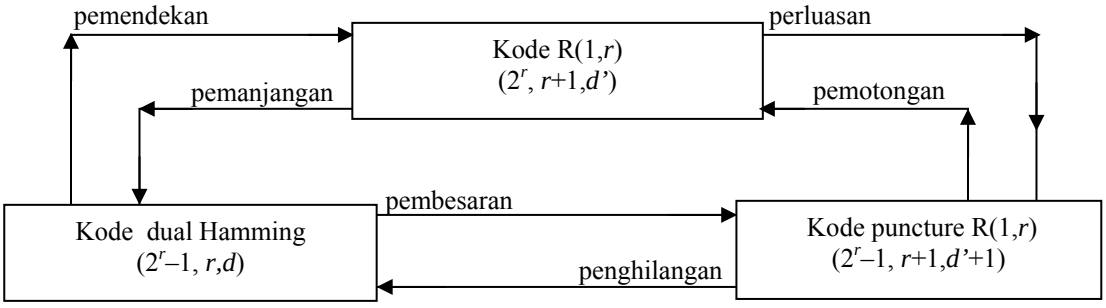


Diagram 2. Variasi kode dari kode dual Hamming

Kode Reed Muller orde pertama R(1,*r*) adalah kode linier ($2^r$,*r*+1,$2^{r-1}$) yang merupakan sub ruang vektor dengan matriks perentang adalah:

$$\hat{H}_r = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ & & & & 0 \\ & Hr & & & 0 \\ & & & & \vdots \\ & & & & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ \hline Hr : 0 \end{bmatrix}$$

$\boldsymbol{H_r}$ adalah matriks pengecek kode Hamming atau matriks perentang kode dual Hamming. Matriks perentang untuk kode reed muller orde pertama memuat vektor-vektor kolom yang tidak nol berdimensi *r* +1.

# 4. Proses Decoding Kode Reed Muller Orde Pertama

## 4.1. Proses Decoding Konvensional

Proses decoding adalah proses menerjemahkan vektor kode yang diterima menjadi pesan dalam bentuk aslinya setelah dikoreksi dan dideteksi kesalahannya. Misalnya setiap vektor $\boldsymbol{c}$ yang dikirimkan oleh transmiter diterima sebagai vektor $\boldsymbol{r}$ oleh receiver.

Strategi penguraian vektor pesan yang diterima secara umum bisa digambarkan sebagai berikut:

Misalkan vektor pesan yang diterima adalah $\boldsymbol{r}$ dimana $\boldsymbol{r}$ sama dengan sebuah vektor hasil encoding $\boldsymbol{c}$', maka vektor $\boldsymbol{r}$ tidak akan dikoreksi tapi langsung diterjemahkan sebagai m sebagai bentuk pesan awal sebelum diubah menjadi $\boldsymbol{c}$' pada encoding, walaupun sebenarnya vektor kode yng dikirimkan belum tentu $\boldsymbol{c}$'.

Jika $\boldsymbol{r}$ tidak sama dengan salah satu dari vektor kode, maka vektor $\boldsymbol{r}$ akan dikoreksi menjadi satu dan hanya satu vektor kode $\boldsymbol{c}$ di **C** yang paling dekat dengan $\boldsymbol{r}$. Selanjutnya $\boldsymbol{c}$ diuraikan kembali menjadi $\boldsymbol{m}$. Jika lebih dari satu vektor kode berjarak sama dengan vektor $\boldsymbol{r}$, kesalahan hanya dapat terdeteksi tanpa dilakukan koreksi.

## 4.2. Proses Decoding Dengan Transformasi Hadamard

Untuk memahami proses decoding dengan menggunakan transformasi Hadamard ini diperlukan matriks Hadamard. Matriks Hadamard (dinotasikan $H_n$) adalah matriks bujur sangkar ordo-*n* dengan entri 1 dan -1 dan berlaku $H_n . H_n^T = n . I_n$. Matriks Hadamard ordo 2*n* dengan $n=2^r-1$ dapat dikonstruksi dari hasil kali kronecker dari *r* buah matriks Hadamard $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Selanjutnya akan dibentuk vektor $\boldsymbol{R}$ terurut $2^r$ sebagai vektor dengan entri 1 dan $-1$ yang diperoleh dari $\boldsymbol{r}$ vektor biner terurut $2^r$. Untuk setiap komponen vektor $\boldsymbol{r}$ yang diasosiasikan dengan suatu vektor biner terurut-*r* yang berbeda. Suatu vektor $\boldsymbol{u}$ terurut-*r* mendefinisikan skalar $r(\boldsymbol{u})$ adalah komponen dari $\boldsymbol{r}$ yang berasosiasi dengan $\boldsymbol{u}$ sehingga komponen pada posisi yang sama di R adalah $\boldsymbol{R}(\boldsymbol{u}) = (-1)^{r(\boldsymbol{u})}$.

Pada posisi yang sama dari vektor R yang diasosiasikan dengan **u** vektor terurut-*r*, transformasi Hadamard dilakukan untuk mendapatkan vektor $\hat{R}$ yang komponennya diasosiasikan dengan vektor ***u*** dinyatakan dengan rumus:

$$\hat{R}(u) = \sum_{v \in GF(2^r)} (-1)^{u.v} R(v)$$

Komponen dari vektor $\hat{R}$ yang terbesarlah yang akan menentukan pada posisi mana dari vektor ***r*** yang akan dikoreksi.

Berikut ini adalah ilustrasi proses decoding untuk R(1,*r*=5).
Misalnya diberikan matriks perentang untuk R(1,5) adalah:

$$\tilde{H}_5 = \begin{bmatrix} 1111111111 & 1111111111 & 1111111111 & 11 \\ 0101010101 & 0101010101 & 0101010101 & 01 \\ 0011001100 & 1100110011 & 0011001100 & 11 \\ 0000111100 & 0011110000 & 1111000011 & 11 \\ 0000000011 & 1111110000 & 0000111111 & 11 \\ 0000000000 & 0000001111 & 1111111111 & 11 \end{bmatrix} = \begin{bmatrix} 1 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix}$$

- Jika kata kode yang diterima adalah vektor dengan panjang 32, yang berbentuk ***r*** = (01110110011101100111011001110110), maka vektor hasil transformasinya adalah $\hat{R}$ = (-8,8,8,24,-8,8,8,-8,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0). Karena komponen terbesar pada posisi keempat berasosiasi dengan kolom keempat dari matriks perentang, maka hasil decoding adalah ***c*** = (01100110011001100110011001100110 0110). Hasil akhir decoding adalah ***m*** = (011000).
- Jika kata kode yang diterima adalah vektor dengan panjang 32, yang berbentuk ***r*** = (01101101100111011001111000011100), maka hasil transformasinya adalah $\hat{R}$ =(4,4,-4,-8,8,0,12,-4,-4,-4,0,8,0,0,-4,-4,-4,4,0,0,0,-6,-4,12,4,2,0,8,0,0,4,8). Karena komponen terbesar lebih dari satu, yaitu pada posisi ke-7 dan ke-24, proses decoding hanya mendeteksi bahwa telah terjadi kesalahan ganda pada kata kode yang diterima.
- Jika kata kode yang diterima adalah vektor dengan panjang 32 adalah ***r*** = (11111111000000001111111100000000), maka vektor hasil transformasinya adalah (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,-32,0,0,0,0,0,0,0,0). Karena komponen terbesar pada posisi 25 berasosiasi dengan kolom ke-25 dari matriks perentang, maka hasil decoding adalah ***r*** = (11111111000000001111111100000000). Hasil akhir decoding adalah ***m*** = (100011).

# 5. Penutup

Kode Reed Muller R(1,*r*) diperoleh dari konstruksi kode dual Hamming dengan proses penambahan simbol pesan atau merupakan kode dual perluasan hamming yang merupakan bentuk kode linier C($2^r$, $r$+1, $2^{r-1}$).

Proses decoding kode R(1,*r*) untuk sembarang kata pesan yang diterima akan ditransformasi linier dua kali. Pertama dengan mengubah vektor biner tersebut menjadi vektor riil, kemudian vektor riil itu ditransformasi lagi dengan menggunakan transformasi

Hadamard. Vektor yang diperoleh dari transformasi Hadamard inilah yang memberi informasi letak kesalahan pada kata pesan semula.

Jika vektor hasil transformasi hadamard itu mempunyai komponen lebih dari satu, maka vektor pesan hanya diketahui mengalami kesalahan pada posisi-posisi tersebut tapi tidak dapat dilakukan koreksi terhadap pesan yang diterima.

Kemampuan mengoreksi kesalahan tersebut serupa dengan proses decoding menggunakan sifat koset dari grup kode ataupun dengan strategi maksimum decoding. Untuk itu disarankan penelitian lebih lanjut mengenai proses decoding untuk ketiga cara ini.

# Daftar Pustaka

[1] Hillman Abraham, Gerald A., 1994, *"Abstract Algebra"*, A First Undergraduate Course. PWS Publishing Co.
[2] J.B. Fraleigh., 1994, *"A First Course in Abstract Algebra"*, Addison Wesley.
[3] F.J. Mac Williams, N.J.A. Sloane, 1993, *"The theory of Error Correcting Codes"*. Volume 16. North Holland mathematics Library.