BAB I
PENDAHULUAN

A. Latar Belakang

Teori pendeteksian error dan pengoreksi sandi adalah cabang dari teknik mesin dan matematika yang berhubungan dengan transmisi dan *storage* yang dapat dipercaya. Dalam prakteknya media informasi tidak dapat 100% dipercaya, karena dimungkinkan adanya gangguan frekuensi yang menyebabkan data tidak valid.

Untuk mendeteksi dan memperbaiki kesalahan, harus ditambahkan suatu redundansi. Dengan adanya pemberian redundansi, sekali pun kesalahan dilakukan (sampai ke beberapa tingkatan toleransi), informasi yang asli dapat diperoleh kembali, atau setidaknya kesalahan yang ada dapat diketahui. Oleh karena itu, perlu ditambahkan bit-bit pengecek yang merupakan redundansi pada informasi yang telah diterima. Bit-bit pengecek tersebut dapat ditentukan apabila kita telah mengetahui matriks *parity-check* dari suatu *codeword*.

Pada makalah ini, akan dibahas mengenai cara membentuk suatu matriks *parity-check* untuk suatu (n,k)-kode yang diketahui berdasarkan matriks generator dari kode tersebut. Matriks *parity-check* akan digunakan dalam mendeteksi suatu *single-error* maupun *2-error*. Selain itu, matriks parity-check juga masih akan digunakan pada bab-bab selanjutnya.

B. Rumusan Masalah

Makalah ini membahas 3 masalah sebagai berikut :

1. Apa yang dimaksud dengan Matriks *Parity-Check*?
2. Bagaimana cara mengkonstruksi suatu matriks parity-check untuk suatu (n,k)-kode?
3. Bagaimana penggunaan matriks *parity-check* dalam mendeteksi dan/atau mengoreksi kesalahan suatu informasi yang diterima?

C. Tujuan

Adapun tujuan dari makalah ini adalah :

1. Mengenal dan memahami tentang matriks *parity-check*..
2. Mengetahui cara mengkonstruksi suatu matriks *parity-check* untuk suatu (n,k)-kode.
3. Mengetahui penggunaan matriks *parity-check* dalam mendeteksi dan/atau mengoreksi kesalahan suatu informasi yang diterima.

BAB II
PEMBAHASAN

A. Definisi

"Misal C adalah (n,k) kode atas F. Jika H adalah matriks pembangkit untuk $C^{\perp}$, maka H disebut matriks *parity-check*."

Dari subbab 3.2 telah diketahui bahwa suatu vector $x \in V_n(F)$ adalah suatu *codeword* dari (n,k) kode C jika dan hanya jika $Hx^T = 0$, dimana H adalah matriks generator untuk $C^{\perp}$. $C^{\perp}$ adalah himpunan n-tuple atas F yang orthogonal untuk setiap vector di C. $C^{\perp}$ disebut kode dual dari C.

Ingat bahwa

$$C^{\perp} = \{x \in V_n(F) \colon x \cdot y = 0 \; untuk \; semua \; y \in C\}$$

Jika G adalah matriks generator untuk C dan H adalah matriks generator untuk $C^{\perp}$, maka H disebut matriks *parity-check* untuk C dan G disebut matriks *parity-check* untuk $C^{\perp}$.

B. Langkah-langkah Pengkonstruksian Matriks Parity-Check

Secara khusus, jika G=[I_k A] adalah matriks generator untuk C, maka $H = [-A^T I_{n-k}\ ]$ adalah matrks *parity-check* untuk C sekaligus matriks generator untuk $C^{\perp}$. Dari situ dapat ditentukan suatu kode linear C dengan memberikan salah satu matriks generator G atau matriks *parity-check* H.

Namun ada kemungkinan dimana G' sebagai hasil OBE dari G yang G' ≠ [I_k A], sehingga ada 2 langkah menentukan matrik *parity-check*, yaitu :

1. Menentukan matrik *parity-ckeck* jika G' = [I_k A]
   - 1.1 Jika diketahui suatu kode C (n,k) dan matrik generator dari C yaitu G
   - 1.2 Dengan OBE G di operasikan menjadi G' = [I_k A]
   - 1.3 Sehingga matrik *parity-check* nya yaitu H = [-A^T I_{n-k}]

Contoh 1:

Diketahui suatu kode C (6,3)-kode (dibaca : kode yang berdimensi 3 dengan panjang 6) atas lapangan Z_2 matriks generatornya adalah

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

Tentukan matriks *parity-check*nya!

Penyelesaian:

Dengan menggunakan operasi baris elementer (OBE), kita bentuk G menjadi $[I_k\ A]$, yaitu

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} = [I_3\, A]$$

Dengan $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ dan $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$A^T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$, sehingga $A^T = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

Maka matriks *parity-check*-nya adalah

$$H = [-A^T I_{n-k}\ ] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

2. Menentukan matrik *parity-ckeck* jika $G \neq [I_k\ A]$
   - 2.1 Jika diketahui suatu kode C (n,k) dan matrik generator dari C yaitu G
   - 2.2 Dengan OBE G di operasikan menjadi $G' \neq [I_k\ A]$
   - 2.3 Kolom-kolom pada G’ misal kita beri nomor urutan dari depan
   - 2.4 Ubah urutan kolom sehingga menjadi $G'' = [I_k\ A]$
   - 2.5 Dengan $G'' = [I_k\ A]$ matrik *parity check* $H' = [-A^T\ I_{n-k}]$
   - 2.6 Kolom-kolom H’ ubah sesuai nomor urutnya seperti pada langkah 2.3
   - 2.7 Dari langkah 2.6 di dapat matrik *parity-check* dari G kode C yaitu H

Contoh 2 :

Diketahui suatu kode C (7,4)-kode (dibaca : kode yang berdimensi 4 dengan panjang 7) atas lapangan Z_3 matriks generatornya adalah

$$G = \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & 2 & 0 & 2 & 0 \\ 1 & 1 & 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Tentukan matriks *parity-check*nya!

Penyelesaian:

Dengan menggunakan operasi baris elementer (OBE), kita bentuk G menjadi $[I_k\ A]$, yaitu

$$G' = \begin{bmatrix} 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \neq [I_k\ A]$$

Karena G' $\neq$ $[I_k\ A]$, maka kita buat nomor urut tiap kolom nya. Sehingga menjadi :

$$G' = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Ubah urutan kolom sedemikian sehingga matrik G' menjadi $[I_k\ A]$, sehingga urutannya menjadi 5, 3, 2, 7, 1, 4, dan 6.

$$G' = \begin{array}{c} \begin{matrix} 5 & 3 & 2 & 7 & 1 & 4 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 \end{bmatrix} \end{array} = [I_k\ A]$$

Dengan $A = \begin{array}{c} \begin{matrix} 1 & 4 & 6 \end{matrix} \\ \begin{bmatrix} 0 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 2 & 2 \\ 2 & 1 & 0 \end{bmatrix} \end{array}$ dan $I_4 = \begin{array}{c} \begin{matrix} 5 & 3 & 2 & 7 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$

$$A^T = \begin{bmatrix} 0 & 0 & 2 & 2 \\ 2 & 1 & 2 & 1 \\ 1 & 2 & 2 & 0 \end{bmatrix} \text{ dan } -A^T = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 0 \end{bmatrix}$$

Maka didapat H’ yaitu :

$$H' = [-A^T I_{n-k}\,] = \begin{array}{c} \begin{matrix} 5 & 3 & 2 & 7 & 1 & 4 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{matrix} \\ \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 2 & 0 & 1 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Kemudian matrik H’ urutan kolomnya dikembalikan seperti semula

$$H = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 & 1 & 0 & 2 \\ 0 & 1 & 1 & 0 & 2 & 1 & 0 \end{bmatrix} \end{array}$$

H merupakan matrik *parity-check* dari kode C(7,4) atas lapangan Z_3 dengan generator G.

C. Penggunaan Matriks Parity-Check

Misalkan $m = (m_1 m_2 \dots m_k)$ adalah *k*-tupel pesan yang akan diletakkan dalam *codeword* c yang panjangnya *n*. selanjutnya, andaikan bahwa symbol-simbol informasi yang dikirim muncul pada k komponen pertama dari c, maka c memiliki bentuk sebagai berikut

$$c = (m_1 m_2 \dots m_k x_1 x_2 \dots x_{n-k})$$

x_i biasanya disebut sebagai symbol pengecek yang menyediakan redundansi yang diperlukan agar dapat mendeteksi dan mengoreksi kesalahan, dengan $1 \le i \le n - k$. Diberikan m_i dengan $1 \le i \le k$, dan x_i dengan $1 \le i \le n - k$. c adalah suatu *codeword* dan Hc^T harus merupakan vector nol, maka dapat ditentukan secara unik dari persamaan

$$Hc^T = 0$$

Oleh karena itu, simbol pengecek x_i dapat ditentukan jika kita diberikan matriks *parity-check* H untuk kode tersebut.

Untuk kasus sederhana n = k+1 (simbol pengecek tunggal) pada contoh berikut ini, H merupakan *parity-bit*.

Contoh 3:

Misalkan H = $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ adalah suatu matriks *parity-check* untuk suatu (6,3) kode biner C. *codeword* yang mana yang membawa informasi m = (101)?

Hal ini tentu saja tergantung dari basis yang dipilih untuk membangun C. Andaikan kita ingin agar informasi yang dikirim muncul pada 3 komponen pertama dari *codeword*, kita harus menemukan bit-bit pengecek x_1, x_2, x_3 sehingga c = (1 0 1 x_1 x_2 x_3) merupakan suatu *codeword*. Dengan demikian

$$Hc^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0 \text{ Menghasilkan}$$

$1 + 1 + x_1 = 0$ atau $x_1 = 0$

$1 + x_2 = 0$ atau $x_2 = 1$

$1 + x_3 = 0$ atau $x_3 = 1$

$Hc^T = 0$ digunakan untuk menentukan bit-bit pengecek x_i dari kode c = $(m_1 m_2 m_3 x_1 x_2 x_3)$ yang dikorespondensikan dengan pesan $m = (m_1 m_2 m_3)$ sehingga memenuhi system

$$\begin{aligned} m_1 + \quad\quad m_3 &= x_1 \\ m_1 + m_2 \quad\quad &= x_2 \\ m_2 + m_3 &= x_3 \end{aligned}$$

Setiap bit pengecek x_i adalah suatu fungsi dari beberapa subruang dari bit-bit pesan m_j dan sebaliknya baris ke- *i* dari H menetapkan suatu subruang dari bit-bit kode yang menunjukkan suatu *parity-check* genap.

Dapat juga ditentukan *codeword* c yang dikorespondensikan dengan pesan m= (101) dengan menemukan matriks generator G untuk C dimana G=[I_3 A]. sehingga dapat dengan mudah dipenuhi dari H yang diberikan, dengan $H = [-A^T I_3]$.

Kemudian G = [I_3 A] = $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

Sehingga c = mG = (101011)

Teorema 3.5.

" Jika H adalah matriks *parity-check* untuk (n,k) kode C atas F. Maka setiap himpunan dari s-1 kolom dari H bebas linear jika dan hanya jika C punya jarak paling kecil s."

Bukti :

Pertama, andaikan bahwa setiap himpunan dari s-1 kolom dari matriks H bebas linear atas lapangan F. misalkan $c = c_1 c_2 \dots c_n$ adalah *codeword* tak nol, dan misalkan $h_1 h_2 \dots h_n$ adalah kolom dari matriks H. kemudian, Karena H adalah matriks *parity-check*, maka $Hc^T = 0$. Hasil kali matriks vector ini dapat ditulis dalam bentuk $Hc^T = \sum_{i=1}^{n} c_i h_i = 0$.

Jika w(c) ≤ s-1, kemudian kita mempunyai suatu kombinasi linear nontrivial kurang dari s kolom matriks H yang jumlahnya sama dengan 0. Hal ini tidak mungkin, karena pada pengandaian sebelumnya setiap himpunan s-1 atau kurang dari s-1 kolom matriks H bebas linear. Oleh sebab itu w(c)≥ s, dan karena c adalah suatu sebarang *codeword* tak nol dan C adalah suatu kode linear, maka menurut theorem 3.1 bahwa w(C)≥s, mengimplikasikan bahwa C mempunyai jarak minimal s.

Untuk membuktikan kebalikannya, andaikan bahwa C mempunyai jarak minimal s. misalkan bahwa beberapa himpunan dari $t \leq s$ -1 kolom dari matriks H yang bebas linear. Missal kolom tersebut adalah $h_{i_1} h_{i_2} \dots h_{i_n}$. Kemudian ada scalar $\lambda_{i_j} \in F$ yang tidak semuanya nol, sedemikian sehingga $\sum_{j=1}^{t} \lambda_{i_j} h_{i_j} = 0$.

Buatlah vector c yang panjangnya λ_{i_j} pada posisi i_j, $1 \leq j \leq t$, dan nol untuk yang lain. c adalah vector tak nol karena $Hc^T = 0$. Tetapi $w(c) = t \leq s - 1$. Hal ini berkontradiksi dengan pengandaian bahwa setiap *codeword* tak nol pada C mempunyai bobot minimal s.

Contoh 3:

diberikan matriks $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$ atas lapangan F = Z_3 ,

Kolom-kolom pada matriks H adalah kolom tak nol dan tidak ada dua kolom yang merupakan perkalian scalar satu sama lain. Oleh karena itu H adalah matriks *parity-check* untuk (5,2) kode C atas lapangan F yang jarak minimalnya 3. Dengan mudah dapat dikonstruksikan C jika telah diketahui matriks generator G untuk C.

Selanjutnya dibentuk matriks *parity-check* lain dari matriks H, yaitu H' dengan H'=[I_3 A].

Dengan menggunakan operasi baris pada H, didapatkan

$$H' = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} = [I_3\ A], \qquad A = \begin{bmatrix} 1 & 2 \\ 0 & 2 \\ 1 & 0 \end{bmatrix}$$

$$G = [-A^T I_2] = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Untuk memastikan, dapat dihitung $HG^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 1 \\ 2 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$

Karena $HG^T = 0$ dan G memuat 2 baris yang bebas linear, maka G harus membangun komplemen orthogonal untuk ruang yang dibangun oleh H. dengan demikian, G adalah matriks generator untuk C. C akan memuat 9 codeword. Jika dibuat daftar *codeword* dan bobotnya sebagai berikut

Codeword	**Bobot**
00000	0
20210	3
11001	3
10120	3
22002	3
01211	4
21121	5
12212	5
02122	4

Dapat dengan mudah dipastikan bahwa setiap pasang codeword mempunyai jarak minimal 3. Jika kode C atas Z_2, maka konstruksikan H menjadi lebih sederhana jika hanya membutuhkan jarak 3 kode. Pada kasus ini, kolom-kolom pada H hanya perlu dibuat menjadi tak nol dan berbeda.

Contoh 4:

Andaikan kita ingin membentuk suatu matriks *parity-check* H untuk mengoreksi error tunggal suatu (7,4) kode C atas Z_2. Karena C adalah suatu (7,4) kode, maka $C^\perp$ adalah (7,3) kode dan H adalah matriks 3×7. Jika C mempunyai jarak 3, maka H harus berbeda dan tak nol. Ada tepat 7 3-tupel yang tak nol atas Z_2 dan masing-masing menjadi kolom pada matriks H. sehingga $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$

Dari sini, dapat dibentuk matriks generator dari C.

Karena H=[I_3 A], maka $A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

kemudian $G = [-A^T I_4] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

Andaikan kita ingin membentuk matriks *parity check* untuk mengoreksi kode error ganda. Kode tersebut harus mempunyai jarak minimal 5. Dan menurut theorema 3.5, tidak ada matriks *parity-check* yang berkolom 4 yang bebas linear.

Contoh 5:

Tunjukkan matriks H yang diberikan dibawah ini atas lapangan F = Z_7. Elemen pembangkit dari Z_7 adalah 3, dengan $Z_7/_{\{0\}} = \{3^i : 0 \le i \le 5\}$

$$H = \begin{bmatrix} 3^0 & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 \\ 3^0 & 3^2 & 3^4 & 3^6 & 3^8 & 3^{10} \\ 3^0 & 3^3 & 3^6 & 3^9 & 3^{12} & 3^{15} \\ 3^0 & 3^4 & 3^8 & 3^{12} & 3^{16} & 3^{20} \end{bmatrix} = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

Kita klaim bahwa H adalah matriks *parity-check* untuk (6,2)-kode C atas Z_7 dan C mempunyai jarak 5.harus dibuktikan bahwa tidak ada matriks H yang mempunyai 4 kolom yang bebas linear.

Ambil 4 kolom sebarang dari matriks H dan kita bentuk matriks D

$D = \begin{bmatrix} 3^i & 3^j & 3^k & 3^l \\ 3^{2i} & 3^{2j} & 3^{2k} & 3^{2l} \\ 3^{3i} & 3^{3j} & 3^{3k} & 3^{3l} \\ 3^{4i} & 3^{4j} & 3^{4k} & 3^{4l} \end{bmatrix}$ dimana $i < j < k < l$

Jika kolom-kolom pada matriks D bebas linear, maka determinan D tidak sama dengan nol dan sebaliknya.

det(D) = $3^i 3^j 3^k 3^l \begin{vmatrix} 1 & 1 & 1 & 1 \\ 3^i & 3^j & 3^k & 3^l \\ 3^{2i} & 3^{2j} & 3^{2k} & 3^{2l} \\ 3^{3i} & 3^{3j} & 3^{3k} & 3^{3l} \end{vmatrix}$

det(D) = $3^{i+j+k+l} \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 3^j - 3^i & 3^k - 3^i & 3^l - 3^i \\ 0 & 3^j(3^j - 3^i) & 3^k(3^k - 3^i) & 3^l(3^l - 3^i) \\ 0 & 3^{2j}(3^j - 3^i) & 3^{2k}(3^k - 3^i) & 3^{2l}(3^l - 3^i) \end{vmatrix}$

$$= 3^{i+j+k+l}(3^j - 3^i)(3^k - 3^i)(3^l - 3^i)\begin{vmatrix} 1 & 1 & 1 \\ 3^j & 3^k & 3^l \\ 3^{2j} & 3^{2k} & 3^{2l} \end{vmatrix}$$

$$= 3^{i+j+k+l}(3^j - 3^i)(3^k - 3^i)(3^l - 3^i)(3^k - 3^j)(3^l - 3^j)(3^l - 3^k)$$

$$= 3^{i+j+k+l}\prod_{x>y}(3^x - 3^y)$$

Dimana hasil kali atas $x, y \in \{i, j, k, l\}, x > y$. Karena $3^x - 3^y \neq 0$ untuk $x \neq y$, sehingga det(D)$\neq$ 0 dan tidak ada matriks H yang mempunyai 4 kolom yang bebas linear. Oleh karena itu, H adalah matriks *parity-check* untuk (6,2)-kode atas Z_7 dengan jarak minimal 5. Kode C akan mempunyai 7^2 *codeword*.

BAB III
PENUTUP

Kesimpulan

Studi dari *error-correcting codes* adalah salah satu cabang dari teori persandian, lebih umum dari ilmu pengetahuan yang berhubungan dengan penyajian data, termasuk *data compression* dan *cryptography*. Sasaran dari *data compression* adalah untuk mengubah bentuk data ke dalam suatu penyajian yang lebih padat namun mengutamakan isi informasi dari data asli, untuk memungkinkan penggunaan ruang simpan dan media transmisi yang lebih efisien.

Penambahan redundansi pada suatu data yang diterima ditentukan oleh matriks *parity-check*. Adapun cara membentuk suatu matriks *parity-check* dari suatu kode yang berdimensi *k* dengan panjang *n* adalah dengan mengolah matriks generatornya menggunakan operasi baris elementer sehingga didapatkan bentuk $[I_{n-k}\ A]$, dengan I adalah matriks identitas berordo *n-k*. Selanjutnya, membentuk matriks *parity-check* dengan bentuk $\left[-A^T I_{n-k}\ \right]$.

Matriks *parity-check* digunakan untuk menentukan kode asli yang dikirim dengan mengkonstruksi kembali matriks generatornya, yang selanjutnya akan digunakan untuk menyusun *codeword* yang dicari.

Selain itu, matriks parity-check digunakan dalam mengoreksi kode dengan *single-error* atau *2-error*.

Daftar Pustaka

Vanstone, Scott A. dan Paul C. van Oorschot. 1989. *An Introduction to Error Correcting Codes with Applications.* London:Kluwer Academic Publishers.

Tugas Mata Kuliah Teori Persandian

MAKALAH

”Matriks Parity-Check”

Disusun Oleh:

Kelompok 1

Esti Nur Kurniawati	07305141020
Devriyadi saputra S.	08305141001
Ade Latif	08305141007
Tri Harjianto	08305141009
Billy Arifa Tengger	08305141010

JURUSAN PENDIDIKAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI YOGYAKARTA

2011