Tugas Teori Persandian

" Step-by-Step Decoding "

Kelompok VI

Okto Mukhotim	08305144029
Evy Damayanti	08305144036
Rerir Roddi A	08305144041
Setiawan Hidayat	08305144046

MATEMATIKA SWADANA 2008

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI YOGYAKARTA

2011

A. Pendahuluan

Dengan semakin berkembangnya teknologi, komunikasi digital menjadi sangat penting dalam segala aspek kehidupan. Segala macam peralatan komunikasi seperti telephone, hand phone, internet, dan berbagai macam peralatan penyampai pesan dalam bentuk digital dipergunakan. Untuk mengurangi tingkat kesalahan penyampaian, pesan – pesan tersebut diubah dalam bentuk kode. Namun demikian, kesalahan (error) mungkin saja terjadi pada saat pengiriman pesan, sehingga pesan yang disampaikan berbeda dari yang seharusnya. Untuk itu, dibuatlah suatu sistem yang dapat mendeteksi, bahkan mengoreksi kesalahan dalam pengiriman pesan tersebut.

Dalam makalah ini akan dibahas mengenai teknik lain dalam menguraikan isi kode yang disebut step-by-step decoding yang berdasar pada standard array decoding. Dalam step-by-step decoding hanya dibutuhkan korespondensi satu-satu antara syndrome dan bobot dari coset leader.

B. Pembahasan

Step by Step Decoding

Step-by-step decoding merupakan suatu teknik decoding yang berdasarkan standard array decoding. Dengan step-by-step decoding,hanya dibutuhkan membentuk suatu korespondensi satu-satu antara syndrome dan bobot dari coset leader. Tabel berikut diperoleh dari pembahasan bab sebelumnya

Coset Leader	Syndrome	Weight of coset Leader
000000	000	0
000001	101	1
000010	011	1
000100	110	1
001000	001	1
010000	010	1
100000	100	1
001100	111	2

Selanjutnya, vektor yang diterima dapat dikodekan menggunakan algoritma berikut ini. Notasi e_i menunjukkan biner n-tuple yang elemen tak nol nya hanyalah elemen ke i.

Algoritmanya sebagai berikut :

Buatlah korespondensi satu- satu antara syndrome dan bobot dari coset leader yang terkait. Korespondensi-korespondensi tersebut ditentukan oleh matrik parity check yang terpilih.
H adalah matrik parity check, dan $r = (r_1 r_2 ... r_n)$ adalah kata yang diterima.

- set i = 1
- Hitung Hr^T dan hitung bobot w dari coset leader yang terkait
- Jika w = 0, hentikan langkah dan r adalah codeword yang dikirimkan.
- Jika $H(r+e_i)^T$ mempunyai bobot yang lebih kecil dari Hr^T, maka set $r = r+e_i$
- set i = i + 1, ulangi langkah 2

Contoh 1

Diberikan (6,3) code pada tabel 2, dengan H matrik parity check . Korespondensi satu-satu antara syndrome dan bobot dari coset leader yang terkait dapat dilihat pada tabel di atas.misal r adalah vektor yang diterima

$$r = (1\ 1\ 1\ 0\ 0\ 0)$$

$Hr^T = (1\ 1\ 1)^T$

Diperoleh dari :

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

r= (1 1 1 0 0 0)

$$r^T = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$Hr^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = (1\ 1\ 1)^T$$

$Hr^T = (1\ 1\ 1)^T$ yang bersesuaian dengan coset leader dengan bobot 2. Karena $w \neq 0$ maka lanjutkan langkah selanjutnya.

$$r + e_1 = (1\ 1\ 1\ 0\ 0\ 0) + (1\ 0\ 0\ 0\ 0\ 0) = (0\ 1\ 1\ 0\ 0\ 0)$$

$$H(r + e_1)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = (0\ 1\ 1)^T$$

$H(r + e_1)^T = (0\ 1\ 1)^T$ yang bersesuaian dengan coset leader dengan bobot 1, dibandingkan dengan bobot sebelumnya maka mengalami penurunan dari 2 menjadi satu sehingga perbaharui r.

$$\mathbf{r = r + e_1}$$

Beralih ke komponen kedua pada r

$$r + e_2 = (0\ 1\ 1\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0\ 0) = (0\ 0\ 1\ 0\ 0\ 0)$$

$$H(r + e_2)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = (0\ 0\ 1)^T$$

$H(r + e_2)^T = (\ 0\ 0\ 1\ )^T$ yang bersesuaian dengan coset leader dengan bobot 1, karena bobotnya sama atau tidak mengalami perubahan maka nilai r tetap yaitu r = (0 1 1 0 0 0)

Beralih ke komponen 3

$$r + e_3 = (0\ 1\ \ 1\ 0\ 0\ 0\ ) + (\ 0\ 0\ 1\ 0\ 0\ 0\ ) = (\ 0\ 1\ 0\ 0\ 0\ 0\ )$$

$$H(r + e_3)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = (\ 0\ 1\ 0\ )^T$$

$H(r + e_3)^T = (\ 0\ 1\ 0\ )^T$ yang bersesuaian dengan coset leader dengan bobot 1, karena bobotnya sama atau tidak mengalami perubahan maka nilai r tetap yaitu r = (0 1 1 0 0 0)

Selanjutnya

$$r + e_4 = (\ 0\ 1\ 1\ 0\ 0\ 0\ ) + (\ 0\ 0\ 0\ 1\ 0\ 0\ ) = (\ 0\ 1\ 1\ 1\ 0\ 0\ )$$

$$H(r + e_4)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = (\ 1\ 0\ 1\ )^T$$

$H(r + e_4)^T = (\ 1\ 0\ 1\ )^T$ yang bersesuaian dengan coset leader dengan bobot 1, karena bobotnya sama atau tidak mengalami perubahan maka nilai r tetap yaitu r = (0 1 1 0 0 0)

Selanjutnya

$$r + e_5 = (0\ 1\ 1\ 0\ 0\ 0) + (0\ 0\ 0\ 0\ 1\ 0) = (0\ 1\ 1\ 0\ 1\ 0)$$

$$H(r + e_5)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = (0\ 0\ 0)^T$$

$H(r + e_5)^T = (0\ 0\ 0)^T$ yang bersesuaian dengan coset leader dengan bobot 0. Set $r = r + e_5 =$ (0 1 1 0 1 0), ini adalah kata yang dikirimkan.

Contoh 2

$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, H adalah suatu matriks parity-check untuk suatu (6,3) kode biner.

Diketahui :

Coset Leader	**Syndrome**	**Weight of coset Leader**
000000	000	0
000001	011	1
000010	110	1
000100	101	1
001000	001	1
010000	010	1
100000	100	1
001100	111	2

Misal , r = (0 1 0 1 0 1)

$$Hr^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = (1\ 0\ 0)^T$$

$Hr^T = (1\ 1\ 1)^T$ yang bersesuaian dengan coset leader dengan bobot 1. Karena $w \neq 0$ maka lanjutkan langkah selanjutnya.

$$r + e_1 = (0\ 1\ 0\ 1\ 0\ 1) + (1\ 0\ 0\ 0\ 0\ 0) = (1\ 1\ 0\ 1\ 0\ 1)$$

$$H(r + e_1)^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = (0\ 0\ 0)^T$$

$H(r + e_1)^T = (0\ 0\ 0)^T$ yang bersesuaian dengan coset leader dengan bobot 0. Set $r = r + e_1$ = (1 1 0 1 0 1) ini adalah kata yang dikirimkan.

Untuk mengetahui bagaimana algoritma step by step decoding bekerja. Akan dijealskan suatu lexicographic ordering pada vector. Misal, vektor $(a_1a_2\ldots a_n)$ mendahului $(b_1b_2\ldots b_k)$ pada lexicographic ordering jika $a_{k+1}=1$, $b_{k+1}=0$ untuk k, $0 \leq k \leq n-1$ dan $a_i = b_i$ untuk semua $i \leq k$

Contoh : (1 0 1 1 1 0) mendahului (1 0 1 1 0 1). Dapat dilihat perbedaannya mulai elemen ke 5, dimana pada vektor pertama a=1 dan vektor kedua a = 0

Contoh :

Lexicographic ordering pada semua 3-tuple atas Z_2 adalah sebagai berikut

1 1 1
1 1 0
1 0 1
1 0 0
0 1 1
0 1 0
0 0 1
0 0 0

C. Kesimpulan

1. Untuk operasi pada $H\,(r + e_n)^T$ yang menghasilkan bobot sama dengan bobot sebelumnya maka komponen r (vektor yang diterima) tetap dengan sebelumnya.
2. Untuk operasi pada $H\,(r + e_n)^T$ yang menghasilkan bobot berbeda dengan bobot sebelumnya maka komponen r (vektor yang diterima) berbeda dengan sebelumnya.

Daftar pustaka

http://eprints.undip.ac.id/5626/1/AURORA_NUR_AINI.pdf

Vanstone, Scott A. and Paul C. van Orshot.1989. *An Introduction to Error Correcting Codes with Application*. Norwell: Kluwer Academic Publisher.