SIFAT KODE LINEAR BINER BERDASARKAN BOBOT KODE

Ahmad Ali Hakam Dani[1)]

[1)] Dosen Program Studi Teknik Informatika Universitas Andi Djemma Palopo
[1)] ahmad.ali@unanda.ac.id

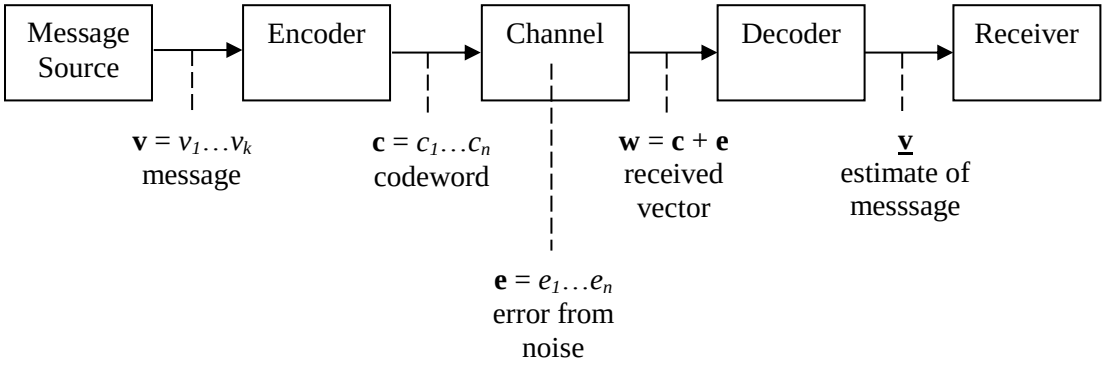
Abstrak
Penelitian ini mendefinisikan konsep kode linear biner. Kode linear biner yang dibahas hanya kode linear yang dibangun dengan melalui matriks generator. Beberapa sifat kode linear biner, khususnya kode linear ortogonal diri dan kode dual diri, ternyata bisa diturunkan hanya dari sifat-sifat bobot, misalnya dari paritas bobot, semua kata kode dalam kode linear.

Kata Kunci: Kode Linear Biner, Matriks Genarator, Ortogonal-diri, Dual-diri.

PENDAHULUAN

Teori pengkodean, dimulai pada tahun 1948 lewat karya Claude Shannon dengan karya tulisnya yang berjudul "A Mathematical Theory of Communication". Meskipun teori pengkodean awalnya muncul untuk menyelesaikan masalah rekayasa (*engineering*), tetapi topik ini sudah berkembang jauh dan bertambah kaya dengan konsep dan teknik yang lebih canggih.

Teori pengoreksi kode dimotivasi oleh kebutuhan komunikasi yang terpercaya. Gambaran umum dari suatu kanal komunikasi (*communication channel*) adalah informasi dikirimkan dari suatu sumber melalui kanal tersebut ke pihak penerima. Sebagai contoh, dalam komunikasi di ruang angkasa, sebuah satelit bisa berperan sebagai sumber informasi, kanalnya adalah ruang angkasa bersama-sama hardware yang mengirim dan menerima informasi sedangkan penerima adalah stasiun bumi.



Gambar 1: Kanal Informasi

Pada sumber, sebuah informasi atau pesan diberi simbol **v**. Jika pesan ini dikirim seperti apa adanya (tidak dimodifikasi), ada kemungkinan penerima akan menerima pesan **w** yang sudah berubah, tidak lagi persis sama dengan **v** (**w** ≠ **v**) dan tidak ada cara untuk mendapatkan **v** dari **w**, padahal pesan yang diinginkan untuk diterima adalah **v** (yang diinginkan: **w** = **v**).

Ide dasar dari Teori Pengecekan Kode adalah memberi sedikit tambahan data (redudansi) terhadap pesan asli. Redundansi pada pesan asli **v**, berupa kata biner dengan panjang *k*, ditambahkan oleh encoder dan pesan **c** (yang telah diberi redudansi sehingga menjadi untaian biner dengan panjang $n > k$) dinamakan kata kode (*codewords*). Jadi yang dikirimkan oleh sumber adalah kata kode **c**.

Suatu kode linear adalah ruang vektor yang dilengkapi dengan fungsi jarak bernilai diskrit. Kode linier yang biasa dibahas adalah kode linear biner, yaitu ruang vektor atas lapangan dengan dua elemen: $F_2 = \{0, 1\}$. Kode linear biner merupakan kode yang paling dominan dipelajari karena lebih mudah dimanipulasi (dibangun, di-*encode*, dan di-*decode*).

Bobot Hamming suatu vektor biner (atau kata kode) **c**, ditulis $w(\mathbf{c})$, adalah banyaknya bit 1 dalam vektor tersebut. Jarak antara dua vektor kode $\mathbf{c}_1$ dan $\mathbf{c}_2$, ditulis $d(\mathbf{c}_1,\mathbf{c}_2)$, adalah banyak bit kedua vektor kode yang berbeda. Jadi jika $\mathbf{c}_1 = 0111$, $\mathbf{c}_2 = 1000$, $\mathbf{c}_3 = 1111$ maka $w(\mathbf{c}_1) = 3$, $w(\mathbf{c}_2) = 1$, $w(\mathbf{c}_3) = 4$ dan $d(\mathbf{c}_1,\mathbf{c}_2) = 4$, $d(\mathbf{c}_1,\mathbf{c}_3) = 1$, $d(\mathbf{c}_2,\mathbf{c}_3) = 3$.

Jika C adalah sebuah kode linear, maka himpunan semua vektor **w** yang tegak lurus terhadap semua vektor $\mathbf{c} \in C$ diberi lambang $C^{\perp}$. Jadi

$$C^{\perp} = \{\mathbf{w} \in F_2^n \mid \forall \mathbf{c} \in C.\ \mathbf{w} \cdot \mathbf{c} = 0 \pmod 2\}.$$

Jika $C^{\perp} \subseteq C$, maka C disebut kode ortogonal-diri (*self-orthogonal*) sedangkan jika $C^{\perp} = C$, maka C disebut kode dual-diri (*self-dual*).

Berdasarkan uraian diatas maka penulis berusaha untuk mengkaji konsep kode linier biner yang dituangkan dalam penelitian yang berjudul Sifat Kode Linier Biner Berdasarkan Bobot Kode.

1) Kode Biner

Di sini hanya dibahas ruang vektor biner

$$F_2^n = \{x_1x_2\ldots x_n \mid x_i \in F_2\}$$

yaitu himpunan semua untaian biner (*binary string*) $x_1x_2\ldots x_n$ yang panjangnya n dengan operasi tambah dan kali modulo 2. Untuk selanjutnya, untaian ini disebut kata biner dan komponen x_i disebut *bit* ke-i.

Sembarang $C \subseteq F_2^n$ disebut *kode biner* dan setiap vektor $\mathbf{c} = c_1c_2\ldots c_n \in C$ disebut *kata kode* (*codeword*). Jika ukuran (banyak unsur) C adalah M, maka kode C tersebut disebut kode (n, M).

Jika $C \subseteq F_2^n$ juga merupakan subruang dari F_2^n (jadi, C tertutup terhadap penjumlahan dan merupakan ruang vektor), maka kode C disebut *kode linear*. Kode linear biner dimensi k berisi tepat sebanyak 2^k kata kode dan biasa dinyatakan sebagai kode $[n, k]$. Banyak kata kode di dalam kode linier biner C adalah $M = 2^k$ (Hufman, 2003).

2) Matriks Generator dan Matriks Cek Paritas

Cara yang paling umum digunakan untuk mendapatkan kode linear adalah dengan matriks generator atau matriks cek paritas. Sebuah matriks generator untuk kode C $[n, k]$ adalah semua matriks **G** berukuran $k \times n$ yang baris-barisnya membentuk sebuah basis dari C. Pada umumnya terdapat banyak matriks generator pada sebuah kode linear $[n, k]$. Setiap kata kode **c** dalam kode linier C bisa diperoleh dari hasil kali sebuah vektor $\mathbf{v} \in F_2^k$ dengan **G**. Sesungguhnya kode C adalah ruang vektor yang dibangkitkan oleh semua baris-baris dari matriks **G**. Dengan kata lain,

$$C = \{\mathbf{vG} \in F_2^n \mid \mathbf{v} \in F_2^k\}.$$

Ini adalah konstruksi ruang vektor berdimensi-n atas lapangan F yang paling mudah dan paling praktis.

Misalnya dari $\mathbf{v}_1 = 1011$, $\mathbf{v}_2 = 0101$ dan matriks generator

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

diperoleh kata kode $\mathbf{c}_1 = \mathbf{v}_1\mathbf{G} = 1011000$, $\mathbf{c}_2 = \mathbf{v}_2\mathbf{G} = 0101101 \in C$.

Dalam teori *Error-Correcting Codes*, implementasi perubahan vektor biner **v** (dengan panjang kata *k*) menjadi kata kode **c** (dengan panjang kata $n > k$) disebut *encoding*. Biasanya **c** dikirim sebagai bagian dari data dan diterima sebagai **w** (= **c**, jika tak ada gangguan yang menyebabkan perubahan pada **c**). Proses sebaliknya, merubah vektor **w** (yang diterima dari proses pengiriman) kembali menjadi **v**, disebut proses decoding.

Dalam ilustrasi di atas, matriks generator **G** berbentuk baku, yaitu berbentuk

$$\mathbf{G} = [\mathrm{I}_k \mid \mathrm{A}].$$

Dalam bentuk baku ini, setiap *k* kolom-kolom bebas linier pertama pada matriks generator **G** bersesuaian dengan sebanyak *k* bit pertama dari **c** yang disebut *bit informasi* pada *C*. Sisanya, sebanyak $r = n - k$ bit dari **c**, disebut bit *redundansi* dan *r* disebut redundansi dari *C* (Hufman, 2003).

Untuk setiap kode linier [*n*, *k*] terdapat matriks **H** dengan ukuran $(n-k)\times n$ dan disebut matriks cek paritas untuk kode [*n*, *k*] yang didefenisikan

$$C = \left\{ \mathbf{x} \in F_2^n \mid \mathbf{H}\mathbf{x}^T = \mathbf{0} \right\} \qquad (2.1)$$

Baris-baris dari **H** juga bebas linier (Hufman, 2003).

Bentuk baku dari matriks cek paritas yang diambil dari bentuk baku dari matriks generator adalah (Hufman, 2003).

$$\mathbf{H} = [\mathbf{A}^T \mid \mathbf{I}_{n-k}]$$

3) Dual dari Kode

Matriks generator **G** untuk kode *C* adalah matriks sederhana dengan baris-baris yang bebas linier dan yang membangkitkan *C*. Baris-baris dari matriks cek paritas **H** juga saling bebas linier dan merupakan matriks generator dari suatu kode linier, yang disebut dual dari kode C. Kode dual dari *C* diberi notasi $C^{\perp}$.

Jika *C* adalah kode [*n*, *k*], dari ukuran matriks **H** terlihat bahwa $C^{\perp}$ adalah sebuah kode [*n*, $n - k$]. Cara mendefenisikan dual dari kode di atas ekuivalen dengan cara menggunakan hasil kali dalam.

Hasil kali dalam antara vektor $\boldsymbol{x} = x_1, x_2, \ldots, x_n$ dengan vektor $\mathbf{y} = y_1, y_2, \ldots, y_n$ di dalam F_2^k adalah

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i \mathrm{y}_i \pmod 2$$

Berdasarkan persamaan (2.1), kita melihat bahwa $C^{\perp}$ dapat juga didefenisikan menjadi (Kschischang, 2007).

$$C^{\perp} = \{ \mathbf{x} \in F_2^n \mid \text{untuk setiap } \mathbf{c} \in C, \mathbf{x} \cdot \mathbf{c} = 0 \pmod 2 \} \qquad (2.2)$$

Selanjutnya dikenal kode dual-diri (*self-dual*) dan kode ortogonal-diri (*self-orthogonal*).

Definisi

Kode C disebut kode *ortogonal-diri* jika $C^{\perp} \subseteq C$ dan disebut kode *dual-diri* jika $C^{\perp} = C$.

Jadi, kode dual-diri otomatis kode ortogonal-diri.

4) Bobot dan Jarak Kode

Invarian penting dari sebuah kode adalah jarak minimum diantara kata kode. Sebelum jarak minimum kode didefinisikan, lebih dulu didefinisikan jarak *Hamming* d(**x,y**) antara dua vektor **x, y** $\in F_2^n$, yaitu banyaknya koordinat yang berbeda dari **x** dan **y**. Selanjutnya, jarak minimum kode C didefinisikan sebagai (Welsh dan Hill, 2007)

$$d(\mathrm{C}) = \min \{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C\,, \mathbf{x} \neq \mathbf{y}\}.$$

Bobot suatu vektor biner adalah banyaknya bit 1 dalam vektor tersebut. Misalnya, bobot dari vektor $\mathbf{x} = 0011111 \in F^7$ adalah 5, yang secara simbolik ditulis

$$wt(\mathbf{x}) = 5$$

atau

$$wt(0011111) = 5.$$

Misalkan $C \in F_2{}^n$ adalah sebuah kode biner dengan ukuran $|C| = M$ dan A_i menyatakan banyak kata kode dalam C yang bobotnya i, $0 \le i \le n$. Barisan

$$A_0, A_1, \ldots, A_n$$

disebut *distribusi bobot* dari C.

Dalam kode linear, jarak minimum kode juga disebut bobot minimum kode. Jika diketahui bobot minimum d dari kode $[n, k]$, maka kita juga dapat menulis kode tersebut menjadi kode $[n, k, d]$ (Welsh dan Hill, 2007).

HASIL DAN PEMBAHASAN

1) Sifat-Sifat Kode Linier Biner

Teorema 1: Memiliki sifat-sifat sebagai berikut:

(i) *Jika* $\mathbf{x}, \mathbf{y} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$,

(ii) *Jika* $\mathbf{x}, \mathbf{y} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x} \cap \mathbf{y}) \equiv \mathbf{x} \cdot \mathbf{y} \pmod 2$

(iii) *Jika* $\mathbf{x} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x} \pmod 2$

Bukti:

(i) *Jika* $\mathbf{x}, \mathbf{y} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$,

Perhatikan, $wt(\mathbf{x} + \mathbf{y}) = \mathrm{N}_{\mathbf{x}} + \mathrm{N}_{\mathbf{v}}$ di mana

$\mathrm{N}_{\mathbf{x}}$ = banyaknya bit 1 dalam **x** sedangkan untuk **y** di posisi yang sama, bitnya adalah 0,

$\mathrm{N}_{\mathbf{y}}$ = banyaknya bit 1 dalam **y** sedangkan untuk **x** di posisi yang sama, bitnya adalah 0.

Tetapi $\mathrm{N}_{\mathbf{x}}$ = banyaknya bit 1 dalam **x** sedangkan untuk **y** di posisi yang sama, bitnya adalah 0 adalah sama dengan banyak bit 1 dalam **x** dikurangi banyaknya bit 1 dalam yang dimiliki bersama oleh **x** dan **y**, yaitu

$$\mathrm{N}_{\mathbf{x}} = wt(\mathbf{x}) - wt(\mathbf{x} \cap \mathbf{y}).$$

Secara analog,

$$\mathrm{N}_{\mathbf{y}} = wt(\mathbf{y}) - wt(\mathbf{x} \cap \mathbf{y}).$$

Jadi

$$\begin{aligned} wt(\mathbf{x} + \mathbf{y}) = \mathrm{N}_{\mathbf{x}} + \mathrm{N}_{\mathbf{y}} &= wt(\mathbf{x}) - wt(\mathbf{x} \cap \mathbf{y}) + wt(\mathbf{y}) - wt(\mathbf{x} \cap \mathbf{y}) \\ &= wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}). \end{aligned}$$

(ii) *Jika* $\mathbf{x}, \mathbf{y} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x} \cap \mathbf{y}) \equiv \mathbf{x} \cdot \mathbf{y} \pmod 2$
Menurut definisi $\mathbf{x} \cap \mathbf{y}$, $wt(\mathbf{x} \cap \mathbf{y})$ adalah banyaknya bit-1, katakan n bit-1, pada posisi yang sama dalam vektor $\mathbf{x}$ dan $\mathbf{y}$. Sedangkan $\mathbf{x} \cdot \mathbf{y}$ adalah jumlah hasil kali sebanyak n bit-1 tersebut setelah dikenakan kongruensi modulo 2. Tetapi jumlah hasil kali sebanyak n buah bit-1 adalah n. Ini membuktikan bahwa $wt(\mathbf{x} \cap \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} \pmod 2$.

(iii) *Jika* $\mathbf{x} \in \boldsymbol{F}_2^n$, *maka* $wt(\mathbf{x}) \equiv \mathbf{x} \cdot \mathbf{x} \pmod 2$
Jelas karena menurut definisi bobot dan definisi vektor $\mathbf{x} \cap \mathbf{y}$

$$wt(\mathbf{x} \cap \mathbf{x}) = wt(\mathbf{x}) = \mathbf{x} \cdot \mathbf{x}.$$ □

Teorema 2: *Misalkan C sebuah* [*n, k, d*] *kode dari* $\boldsymbol{F}_2$, *maka:*

(i) $A_0(C) + A_1(C) + \ldots + A_n(C) = 2^k$.

(ii) $A_0(C) = 1$ *dan jika* $d > 1$, *maka* $A_1(C) = \ldots = A_{d-1}(C) = 0$.

(iii) *Jika C adalah sebuah kode biner ortogonal-diri, maka setiap kata kode memiliki bobot genap, dan* $C^{\perp}$ *memuat kata kode* $\mathbf{1} = 11\ldots1$.

Bukti:

(i) $A_0(C) + A_1(C) + \ldots + A_n(C) = 2^k$.
$A_i(C)$ menyatakan banyak kode yang bobotnya i dalam kata kode C. Jadi $A_0(C) + A_1(C) + \ldots + A_n(C)$ menyatakan banyak semua kata kode dengan bobot 0 sampai dengan n, yaitu banyak semua kata kode dalam C. Karena banyaknya kata kode dalam C adalah 2^k, terbukti

$$\sum_{i=1}^{n} A_i(C) = 2^k$$

(ii) $A_0(C) = 1$ *dan jika* $d > 1$, *maka* $A_1(C) = \ldots = A_{d-1}(C) = 0$.
Karena C kode linier, maka C memuat $\mathbf{0}$, satu-satunya kata kode dengan bobot nol, yaitu $A_0(C) = 1$. Langsung dari definisi bobot minimum kode C, yaitu d adalah bobot terkecil dari kata kode $\mathbf{x} \neq \mathbf{0}$. Artinya tak ada kata kode $\mathbf{x} \neq \mathbf{0}$ dengan bobot 1, 2, ..., $d - 1$, yaitu $A_1(C) = \ldots = A_{d-1}(C) = 0$.

(iii) *Akan dibuktikan, setiap kata kode memiliki bobot genap, dan* $C^{\perp}$ *memuat kata kode* $\mathbf{1} = 11\ldots1$.
Telah kita ketahui bahwa sebuah kode ortogonal-diri apabila $C^{\perp} \subseteq C$. Ini berarti ada paling sedikit satu kata kode $\mathbf{c}_0 \in C^{\perp} \subseteq C$ yang tegak lurus (ortogonal) terhadap setiap $\mathbf{c} \in C$. Jadi untuk sembarang $\mathbf{c} \in C$.

$$\mathbf{c} \cdot \mathbf{c}_0 = 0.$$

Pada khususnya, jika dipilih $\mathbf{c} = \mathbf{c}_0$,

$$\mathbf{c}_0 \cdot \mathbf{c}_0 = 0.$$

Dari Teorema 4(*ii*)

$$wt(\mathbf{c}_0) \equiv wt(\mathbf{c}_0 \cap \mathbf{c}_0) \equiv \mathbf{c}_0 \cdot \mathbf{c}_0 \pmod 2 = 0 \pmod 2.$$

Ini membuktikan $wt(\mathbf{c}_0)$ adalah genap.
Demikian pula untuk sembarang $\mathbf{c} \in C$ berlaku

$$wt(\mathbf{c} \cap \mathbf{c}_0) \equiv \mathbf{c} \cdot \mathbf{c}_0 \pmod 2 = 0 \pmod 2,$$

yaitu $wt(\mathbf{c} \cap \mathbf{c}_0)$ adalah genap.
Selanjutnya dengan menerapkan Teorema 4(*i*)

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$$

dengan $\mathbf{x} = \mathbf{c} + \mathbf{c}_0$ dan $\mathbf{y} = \mathbf{c}_0$, dperoleh

$$wt(\mathbf{c}) = wt(\mathbf{c} + \mathbf{c}_0) + wt(\mathbf{c}_0) - 2wt([\mathbf{c} + \mathbf{c}_0] \cap \mathbf{c}_0).$$

Karena tak ada bit-1 bersama antara $\mathbf{c} + \mathbf{c}_0$ dan $\mathbf{c}_0$, maka menurut definisi

$$[\mathbf{c} + \mathbf{c}_0] \cap \mathbf{c}_0 = \mathbf{0}.$$

Jadi

$$wt(\mathbf{c}) = wt(\mathbf{c} + \mathbf{c}_0) + wt(\mathbf{c}_0)$$

Karena $wt(\mathbf{c} + \mathbf{c}_0)$ dan $wt(\mathbf{c}_0)$ telah dibuktikan genap, maka $wt(\mathbf{c})$ juga genap.

Akhirnya untuk membuktikan $\mathbf{1} \in C^{\perp}$, perhatikan bahwa untuk setiap $\mathbf{c} \in C$ berlaku

$$\mathbf{c} \cdot \mathbf{1} = wt(\mathbf{c}) \equiv 0 \bmod 2,$$

sebab $wt(\mathbf{c})$ genap. Jadi $\mathbf{1} \in C^{\perp}$. □

Contoh 1:
Misalkan C kode biner dengan matriks generator.

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

Sehingga diperoleh kode biner C sebagai berikut:
C = {000000, 000011, 001100, 001111, 110000, 110011, 111100, 111111}
Ditribusi bobot dari kode C adalah $A_0 = A_6 = 1$ dan $A_2 = A_4 = 3$. Sedangkan yang distribusi bobot yang lain bernilai nol, yaitu $A_1 = A_3 = 0$ (biasanya koefisien distribusi dengan nilai 0 tidak ditulis).

Kode biner di atas merupakan kode biner dual-diri dan juga otomatis ortogonal-diri, berdasarkan Teorema 5, maka setiap kata kode memiliki bobot genap, dan $C^{\perp}$ memuat kata kode $\mathbf{1} = 11\ldots1$.

Lemma: *Misalkan C adalah sebuah kode biner* [n, k] *yang ortogonal-diri maka untuk setiap* $\mathbf{x}, \mathbf{y} \in C$ *berlaku* $\mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod 2$.

Bukti:
Misalkan $\mathbf{x}, \mathbf{y} \in C$, maka $\mathbf{x} + \mathbf{y} \in C$ sehingga menurut Teorema 5(*iii*), $\mathbf{x} + \mathbf{y}$ berbobot genap, yaitu $wt(\mathbf{x} + \mathbf{y}) \equiv 0 \pmod 2$.
Dari lain pihak, $\mathbf{x} + \mathbf{y}$, yaitu vektor dengan bit-1 pada posisi di mana $\mathbf{x}$ dan $\mathbf{y}$ berbeda, adalah komplemen dari vektor $\mathbf{x} \cap \mathbf{y}$, yaitu vektor dengan bit-1 pada posisi di mana $\mathbf{x}$ dan $\mathbf{y}$ sama. Ini berarti $\mathbf{x} \cap \mathbf{y} = \mathbf{1} + \mathbf{x} + \mathbf{y}$. Karena setiap unsur dalam kode ortogonal diri berbobot genap, maka $wt(\mathbf{1}) = n$ (panjang kata) adalah genap. Jadi $wt(\mathbf{1} + \mathbf{x} + \mathbf{y}) = n - \text{wt}(\mathbf{x} + \mathbf{y})$ adalah genap. □

Contoh 2:
Misalkan terdapat kode C yang ortogonal-diri, yaitu
C = {000000, 000011, 001100, 001111, 110000, 110011, 111100, 111111},
maka misalkan $\mathbf{x}$ = 000011 □ C dan $\mathbf{y}$ = 001111 □ C, sehingga berdasarkan Lemma diatas

$$\mathbf{x} \cdot \mathbf{y} = 000011 \cdot 001111 = 2 \equiv 0 \pmod 2,$$

atau $\mathbf{x} \cdot \mathbf{y}$ adalah genap.

Teorema 3: *Misalkan C adalah sebuah kode biner* [n, k] *yang ortogonal-diri dan C_0 merupakan subimpunan dari C yang terdiri atas semua kata kode dengan bobot habis dibagi* 4, *maka berlaku*:
(i) $C = C_0$, *atau*

(ii) *C_0 adalah sebuah subkode* $[n, k-1]$ *dari* C *dan* $C = C_0 \cup C_1$, *maka untuk setiap kata kode* $\mathbf{x}$ *yang bobotnya tidak habis dibagi empat*

$$C_1 = \mathbf{x} + C_0 = \{\mathbf{x} + \mathbf{c} \mid \mathbf{c} \in C_0\},$$

Lebih jauh, C_1 *adalah koset dari* C_0 *dan terdiri atas semua kata kode dari* C *yang bobotnya tidak habis dibagi empat.*

Bukti:

Akan dibuktikan jika (*i*) tidak benar ($C \neq C_0$), maka (*ii*) berlaku $C = C_0 \cup C_1$, di mana C_1 adalah subhimpunan dari C yang memuat semua kata kode dengan bobot bukan kelipatan 4.

Berdasarkan Teorema 5, semua kata kode dalam C memiliki bobot genap. Jadi jika (*i*) tidak benar ($C \neq C_0$), maka terdapat kata kode C yang memiliki bobot genap tetapi bukan kelipatan 4.

Pilih sembarang kata kode $\mathbf{x} \in C$ yang memiliki bobot genap tetapi bukan kelipatan 4. Misalkan $\mathbf{y}$ adalah kata kode lain yang bobotnya genap tetapi bukan kelipatan 4.

Berdasarkan Teorema 4(*i*),

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}) \equiv 2 + 2 - 2wt(\mathbf{x} \cap \mathbf{y}) \pmod 4.$$

Teorema di atas dibawa ke dalam modulo 4 sehingga

$$wt(\mathbf{x} + \mathbf{y}) \equiv 2wt(\mathbf{x} \cap \mathbf{y}) \pmod 4$$

Selanjutnya berdasarkan Teorema 4(*ii*),

$$wt(\mathbf{x} \cap \mathbf{y}) \equiv \mathbf{x} \cdot \mathbf{y} \pmod 2.$$

Berdasarkan Lemma, dimana $\mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod 2$. Sehingga diperoleh $wt(\mathbf{x} + \mathbf{y})$ merupakan kelipatan 4, artinya $\mathbf{x} + \mathbf{y} \in C_0$. Hasil ini menunjukkan bahwa $\mathbf{y} \in \mathbf{x} + C_0$ dan $C_1 = \mathbf{x} + C_0$ terdiri dari semua kata kode dari C yang bobotnya tidak habis dibagi empat. □

Contoh 3:

Misalnya terdapat matriks generator $\mathbf{G}$

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

maka dapat diperoleh kode C

C = {0000000, 0001011, 0010110, 0100101,
0101100, 0111000, 0110011, 0011101,
1010001, 1100010, 1110100, 1001100,
1000111, 1101001, 1011010, 1111111}

Distribusi bobotnya adalah $A_0 = A_7 = 1$, $A_3 = 8$ dan $A_4 = 6$. Kode diatas kode yang ortogonal-diri. Disini, banyak kata kode C_0 adalah $A_4 = 6$ dan

$$C_1 = \mathbf{x} + C_0 = \{\mathbf{x} + \mathbf{c} \mid \mathbf{c} \in C_0\},$$

misalnya $\mathbf{x} =$ 1100010 dan $\mathbf{c} =$ 1110100 $\in C_0$, maka

$$C_1 = 1100010 + 1110100 = 0010110 \in C,$$

sehingga C_1 adalah kata kode dari C yang bobotnya tidak habis dibagi empat, maka $C = C_0 \cup C_1$.

Teorema 4: *Misalkan C adalah sebuah kode* [*n, k*] *dan* C_e *adalah sebuah bit dari kata kode dalam C yang bobotnya genap, maka berlaku:*

(i) $C = C_e$, *atau*

(ii) C_e *adalah sebuah subkode* [*n, k – 1*] *dari C dan* $C = C_e \cup C_o$, *maka untuk setiap kata kode* **x** *yang bobotnya ganjil*

$$C_o = \mathbf{x} + C_e = \{\mathbf{x} + \mathbf{c} \mid \mathbf{c} \in C_e\},$$

Lebih jauh, C_o *adalah koset dari* C_e *dan terdiri dari semua kata kode dari C yang bobotnya ganjil.*

Bukti:

Akan dibuktikan jika (*i*) tidak benar ($C \neq C_e$), maka (*ii*) berlaku ($C = C_e \cup C_o$, di mana C_o adalah subhimpunan dari *C* yang memuat semua kata kode dengan bobot ganjil.

Berdasarkan Teorema 5, semua kata kode dalam *C* memiliki bobot genap. Jadi jika (*i*) tidak benar ($C \neq C_e$), maka terdapat kata kode $\mathbf{x} \in C$ yang memiliki bobot ganjil. Misalkan pula **y** kata kode lain yang bobotnya ganjil. Maka berdasarkan Teorema 4(*i*),

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$$

dimana $wt(\mathbf{x})$ dan $wt(\mathbf{y})$ adalah ganjil, maka dalam operasi $wt(\mathbf{x}) + wt(\mathbf{y})$ akan menghasilkan genap sehingga $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y})$ genap.

Terbukti $wt(\mathbf{x} + \mathbf{y})$ adalah genap, artinya $\mathbf{x} + \mathbf{y} \in C_e$. Hasil ini menunjukkan bahwa $\mathbf{y} \in \mathbf{x} + C_e$ dan $C_o = \mathbf{x} + C_e$ terdiri dari semua kata kode dari *C* yang bobotnya ganjil. □

Contoh 4:

Misalnya terdapat kode biner *C* sebagai berikut:

C = {0000000, 0001011, 0010110, 0100101,
0101100, 0111000, 0110011, 0011101,
1010001, 1100010, 1110100, 1001100,
1000111, 1101001, 1011010, 1111111}

Distribusi bobotnya adalah $A_0 = A_7 = 1$, $A_3 = 8$ dan $A_4 = 6$. Banyak kata kode C_e atau banyak kata kode yang memiliki bobot genap adalah $A_4 = 6$ dan

$$C_o = \mathbf{x} + C_e = \{\mathbf{x} + \mathbf{c} \mid \mathbf{c} \in C_e\},$$

misalnya **x =** 1010001 dan **c =** 1101001 $\in C_e$, maka

$$C_o = 1010001 + 1101001 = 0111000 \in C,$$

sehingga C_o adalah kata kode dari *C* yang bobotnya ganjil, maka $C = C_e \cup C_o$.

Teorema 5: *Misalkan C adalah sebuah kode linier biner.*

(i) Jika C adalah ortogonal-diri dan mempunyai matriks generator yang setiap barisnya mempunyai bobot yang habis dibagi empat, maka setiap kata kode dalam C mempunyai bobot yang habis dibagi empat.

(ii) Jika setiap kata kode dalam C mempunyai bobot yang habis dibagi empat, maka C adalah ortogonal-diri.

Bukti:

(i) Misalkan **x** dan **y** adalah baris-baris dari matriks generator. Berdasarkan teorema 4(*i*),

$$wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \cap \mathbf{y}) \equiv 0 + 0 - 2wt(\mathrm{x} \cap \mathbf{y}) \pmod 4$$

karena

$$wt(\mathrm{x} \cap \mathbf{y}) \equiv 0 \pmod 2,$$

maka

$$wt(\mathrm{x} \cap \mathbf{y}) \equiv 0 \text{ atau } 2 \pmod 4.$$

Sehingga

$$2wt(\mathrm{x} \cap \mathbf{y}) \equiv 0 \pmod 4$$

Jadi

$$wt(\mathbf{x} + \mathbf{y}) \equiv 0 \pmod 4.$$

(ii) Misalkan $\mathbf{x}, \mathbf{y} \in C$. Berdasarkan teorema 4($i$) dan ($ii$),

$$\begin{aligned} 2(\mathbf{x} \cdot \mathbf{y}) &\equiv 2wt(\mathbf{x} \cap \mathbf{y}) \\ &\equiv 2wt(\mathbf{x} \cap \mathbf{y}) - wt(\mathbf{x}) - wt(\mathbf{y}) \\ &\equiv -wt(\mathbf{x} + \mathbf{y}) \\ &\equiv 0 \pmod 4 \end{aligned}$$

Jadi

$$\mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod 2$$ □

Contoh 5:
Misalnya terdapat matriks generator dari kode C

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

maka diperoleh kode C

C = {0000000, 10101010, 11001100, 11110000,
11111111, 01010101, 00110011, 00001111,
10100101, 11000011, 10011001, 10010110,
01100110, 01011010, 00111100, 01101001}

Distribusi bobotnya adalah $A_0 = A_8 = 1$ dan $A_4 = 14$. Jadi, diperoleh kode C yang semua kata kodenya memiliki bobot yang habis dibagi empat yang sesuai dengan Teorema 8. Sehingga berdasarkan Teorema 8, jika setiap kata kode C mempunyai bobot yang habis dibagi empat, maka kode C adalah ortogonal-diri.

Teorema 6: *Misalkan C adalah sebuah kode biner dengan matriks generator yang setiap barisnya memiliki bobot genap, maka setiap kata kode dalam C juga memiliki bobot genap.*

Bukti:

Misalkan $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i$ adalah baris-baris dari matriks generator $\mathbf{G}$ yang bobotnya genap. Selanjuntya terdapat kode pesan $\mathbf{v} = v_1 v_2 \ldots v_i \in \mathbf{V}$. Sebagaimana yang telah kita ketahui bersama bahwa dalam menentukan kata kode $\mathbf{c} = c_1 c_2 \ldots c_i \in C$ yang diperoleh dari matrik generator adalah dengan cara sebagi berikut

$$\mathbf{c} = \mathbf{vG} = \sum_{i=1}^{k} \mathrm{v}_i \mathrm{G}$$

dalam proses *encoding* tersebut, jelas kita peroleh kata kode $\mathbf{c} = c_1 c_2 \ldots c_i \in C$ yang memiliki bobot genap. □

5) Beberapa Kode Linier Biner

Kode Hamming

Keluarga kode Hamming berbentuk kode $[2^r - 1, 2^r - 1 - r, r]$, dimana r merupakan jarak minimum kode. Salah satu keluarga kode Hamming yaitu kode Hamming [7, 4, 3] yang bentuk matriks generatornya adalah

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

Distribusi bobotnya adalah $A_0 = A_7 = 1$, $A_3 = 8$ dan $A_4 = 6$.
Sedangkan bentuk matriks cek paritasnya adalah

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

Kode Hamming [8, 4, 4] disebut kode biner Hamming yang diperluas, kode yang diperoleh dari kode Hamming [7, 4, 3] dengan menambah bit paritas. Bentuk matriks generator dari kode Hamming [8, 4, 4] adalah

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

Kode Golay

Kode Golay [24, 12, 8] bisa dikonstruksi dengan matriks generator

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

Kode Golay [24, 12, 8], biasa diberi simbol G_{24} dan merupakan kode dual-diri. Distribusi bobotnya adalah $A_0 = A_{24} = 1$, $A_{12} = 2576$, $A_8 = A_{16} = 759$ (Clark dan Marley, 2005).

Kode Golay [23, 11, 7] bisa diperoleh dari kode Golay [24, 12, 8]. Kode Golay [23, 11, 7], biasa diberi simbol G_{23} diperoleh dengan membuang satu bit pada posisi tetap (tidak penting, posisi yang mana pun akan tetap menghasilkan kode G_{23}). Bentuk matriks generatornya adalah (Clark dan Marley, 2005)

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

Sedangkan distribusi bobot dari kode Golay [23, 11, 7] adalah
$A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$.

Kode Reed Muller

Keluarga kode-kode Reed Muller $R(r, m)$ memiliki panjang kata kode $n = 2^m$ dengan dimensi $k = C_0^m + C_1^m + ... + C_r^m$. Rumus untuk mendapatkan matriks generator dari kode Reed Muller $R(r, m)$ adalah (Raaphorst, 2003)

$$G_{R(r,m)} = \begin{bmatrix} G_{R(r,m-1)} & G_{R(r,m-1)} \\ 0 & G_{R(r-1,m-1)} \end{bmatrix}$$

$$G_{R(0,m)} = \{11...1\}$$

dengan panjang bit 1 adalah 2^m.

$$G_{R(m,m)} = \begin{bmatrix} G_{R(m,m)} \\ 00...01 \end{bmatrix}$$

dengan panjang bit 0 adalah $2^m - 1$.
Selanjutnya kode $R(m - 2, m)$ ekuivalen dengan kode Hamming yang diperluas.

KESIMPULAN

Adapun kesimpulan dalam penulisan ini adalah:

1. Sebuah kode C adalah kode linier biner jika merupakan ruang vektor atas lapangan dengan dua elemen, yaitu atas $F_2^n = \{x_1x_2...x_n \mid x_i \in F_2\}$. Karena F_2^n sendiri merupakan ruang vektor berdimensi n, kode linear $C \subseteq F_2^n$ yang berdimensi k (dilambangkan sebagai kode $[n, k]$) merupakan subruang dari F_2^n.
2. Beberapa sifat kode linier biner bisa diketahui berdasarkan bobot kodenya, dan sebaliknya dari beberapa sifat dari kode linear biner bisa menentukan sifat dari distribusi bobot kode. Misalnya jika kode biner C ortogonal-diri maka kode tersebut memiliki bobot genap dan terdapat vektor $\mathbf{x}$ dan $\mathbf{y} \in C$, dimana
$$\mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod 2.$$
Selanjutnya bobot kode biner juga akan bernilai genap jika baris-baris dari matriks generatornya juga bernilai genap.

3. Jika terdapat baris-baris yang saling bebas linier dari **G** yang merupakan matriks generator dari kode linier *C*, maka kita dapat mengkonstruksinya menjadi matriks cek paritas **H** untuk kode linier *C*.

DAFTAR PUSTAKA

Fraleigh, John B. (1989). *A First Course in Abstract Algebra*. Fifth Edition. University of Rhode Island.

Clark, K. dan Marley. (2005). *The Perfect Code*: *Golay Codes*. Switzerland. http://www.fi.muni.cz/usr/gruska/crypto04/GolayCodes.pdf, diakses tgl 29 Oktober 2010.

Hufman, W. Cary. (2003). *Fundamentals of Error-Correcting Codes*. Cambride University Press. USA.

Kschischang, Frank. (2007). *Error Control Codes.* University of Toronto.

Lint, J.H. Van. (1996). *Algebraic Coding Theory*. Eindhoven University of Technology. Eindhoven. Netherlands.

Raaphorst, Sebastian. (2003). *Reed-Muller Codes*. Carleton University. http://www/cs.toronto.edu/academic/mat5127paper.pdf, diakses tgl 29 Oktober 2010.

Welsh, D. and Hill, R. (2007). *Coding Theory*. Manchester of University. England. http://maths.manchester.ac.uk, diakses tgl 16 September 2010.