DEKODING SINDROM KODE *GILBERT-VARSHAMOV* BINER BERJARAK MINIMUM RENDAH

A. SAEPULROHMAN[1], S. GURITMAN[2], B. P. SILALAHI[2]

Abstrak

Dalam sistem komunikasi, kemampuan untuk mengirim dan menerima pesan secara cepat sangat dibutuhkan. Semakin besar sebuah data, semakin lama waktu yang diperlukan untuk pengiriman dan semakin besar pula kemungkinan data hilang dalam proses pengiriman pesan. Oleh karena itu dibutuhkan sebuah cara untuk membuat (kontruksi) sebuah kode yang lebih optimal tanpa merusak informasi yang dikandung oleh data tersebut. Kode *Gilbert-Varshamov* biner adalah salah satu cara penyandian (*encoding*) yang menggunakan tiga parameter dengan panjang kode n, dimensi k dan jarak minimum d yang dinotasikan sebagai kode-$[n, k, d]$. Problem utama dalam penelitian ini adalah mengoptimalkan sebuah kode- $[n, k, d]$ berjarak minimum rendah yang dapat meminimalkan kesalahan sehingga pesan yang diterima sesuai dengan yang dikirim. Jika terjadi kesalahan maka dilakukan proses pemulihan (*decoding*) menjadi pesan asli dengan menggunakan metode dekoding sindrom. Dalam mengimplementasikan proses enkoding dan dekoding dilakukan pengembangan dengan bantuan *software* matematika

Kata Kunci: kode biner, enkoding, dekoding sindrom, matriks cek paritas, matriks generator, teorema *Gilbert-Varshamov*.

PENDAHULUAN

Komunikasi data adalah proses pertukaran pesan dari sumber ke tujuan. Dalam komunikasi, pesan dapat direpresentasikan sebagai barisan simbol biner 0 dan 1 yang dikenal dengan *bitstring*. Simbol biner inilah yang sering disebut dengan kode, yang kemudian memunculkan istilah pengkodean (*coding*). Teori koding (*coding theory*) merupakan ilmu yang mempelajari teknik dan metode pengiriman pesan melalui saluran terganggu (*noisy channel*). Saluran yang terganggu menyebabkan berubahnya beberapa simbol yang dikirim, sehingga mengurangi kualitas informasi yang diterima.

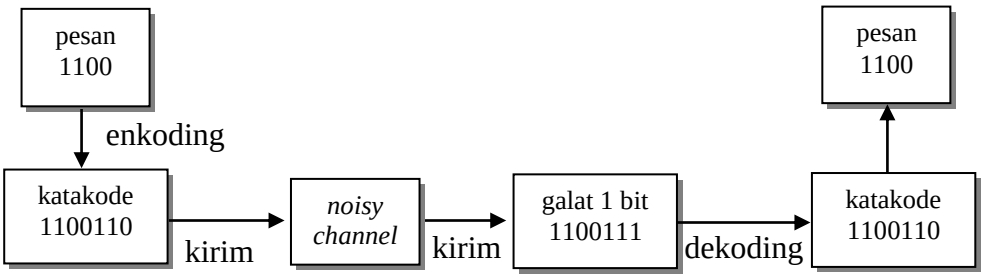
C. E. Shannon telah memformulasikan dasar teori untuk membuat (mengkonstruksi) suatu kode yang berasal dari suatu masalah dalam teori informasi yang dijelaskan dalam artikelnya yang berjudul *A Mathematical Theory of Communication*. Masalah tersebut dapat digambarkan sebagai berikut. Apabila suatu pesan dikirim melalui saluran terganggu (*noisy channel*), seringkali pesan

[1]Mahasiswa S2, Program Studi Matematika Terapan, Sekolah Pascasarjana IPB Dramaga Bogor, 16680 E-mail: asepspl@yahoo.com.
[2]Departemen Matematika, Fakultas Ilmu Pengetahuan Alam, Jalan Meranti Kampus IPB Dramaga Bogor, 16680.

yang diterima berbeda dengan yang dikirim. Saluran (*channel*) tersebut berupa jaringan telepon, jaringan radio berfrekuensi tinggi atau jaringan satelit. Sedangkan gangguan (*noisy*) didefinisikan sesuatu yang dapat menyebabkan pesan yang diterima tidak sama dengan pesan yang dikirim. Gangguan dapat terjadi karena adanya petir, goresan, hujan, meteor, panas matahari, gangguan radio, dan lain-lain. Oleh karena itu dibutuhkan suatu cara (proses) untuk mengkontruksi kode dalam blok biner yang lebih optimal terhapap gangguan yang akan terjadi.

Suatu kode (*code*) diciptakan untuk mendeteksi atau mengoreksi terjadinya galat (*error*) akibat saluran terganggu. Dalam hal ini sebelum dikirim, semua pesan akan diubah menjadi katakode (*codeword*) dengan cara menambahkan beberapa simbol ekstra pada simbol pesan. Proses pengubahan pesan menjadi katakode disebut enkoding (*encoding*). Perangkat yang mengubah pesan menjadi katakode disebut enkoder (*encoder*). Dekoding proses yang mengubah barisan simbol yang diterima menjadi katakode yang selanjutnya dipulihkan menjadi pesan asli.

Model komunikasi data dalam proses pengiriman pesan dapat digambarkan seperti pada Gambar 1 dibawah ini



Gambar 1 Sistem pengiriman pesan kode biner

Ilustrasi dari Gambar 1 menjelaskan bahwa suatu pesan dengan simbol 1100 akan dikirim, maka terlebih dahulu pesan tersebut diubah menjadi katakode (*codeword*) 1100110 dengan menambahkan simbol ektra pada pesan. Kemudian katakode tersebut dikirim melalui saluran yang diasumsikan terganggu sehingga terdapat galat pada katakode sebanyak 1 bit. Selanjutnya dekoder akan mendeteksi galat dan mengoreksi menjadi katakode yang akan mendefinisikan pesan asli.

Proses rekontruksi suatu kode biner dibutuhkan untuk melakukan proses dekoding yang berdasarkan pada Tabel Brouwer [3]. Dekoding sindrom kode *Gilbert-Varshamov* biner adalah suatu cara mengubah barisan simbol yang diterima menjadi katakode yang selanjutnya dipulihkan menjadi pesan asli menggunakan tabel tanpa simpanan. Keunggulan dari kode *Gilbert-Varshamov* biner adalah metode yang bersifat universal sehingga dapat diterapakan pada berbagai jenis data. Metode dekoding sindrom memberikan hasil yang cukup memuaskan. Percobaan menggunakan dekoding sindrom kode *Gilbert-Varshamov*

biner dengan bahasa pemograman memberikan hasil bahwa cara pengkodean *Gilbert-Varshamov* dapat mengoreksi kesalahan data dari data semula.

Manfaat dari proses dekoding sindrom kode *Gilbert-Varshamov* adalah mendeteksi terjadinya galat (*error*) dan sekaligus mengoreksi kembali, sehingga menjadi data yang benar. Misalnya suatu data disimpan pada *Compact Disc* (CD), dimana CD merupakan benda yang mudah tergores dan goresan-goresan pada permukaan CD berpotensi merusak isi data yang ada di dalamnya. Tentunya goresan tersebut mengakibatkan terjadinya *error*. Oleh karena itu CD didesain supaya *error* yang terjadi dari goresan-goresan kecil tidak merusak isi data dan data masih dapat dibaca dengan benar. Kemudian manfaat yang lain mendeteksi galat dalam proses komunikasi satelit, transfer data dari memori ke CPU komputer, dan lain sebagainya.

Tujuan dari penelitian ini adalah merekonstruksi kode *Gilbert-Varshamov* biner berjarak minimum rendah untuk kasus *double error correction* ($d = 5, 7, 9, 11, 13, 15$) dan menurunkan algoritma proses enkoding dan dekoding sindrom.

KODE GILBERT-VARSHAMOV BINER

Dalam teori koding dikenal tiga parameter yang terkait dengan konstruksi suatu kode, yaitu panjang, dimensi, dan jarak minimum. Jika C kode dengan panjang n, berdimensi k, dan berjarak minimum d, maka C dapat dinamakan kode-$[n, k, d]$. Kode linear dengan panjang n didefinisikan sebagai subruang C dari $\mathbb{F}_2^n$ dengan $\mathbb{F}_2^n$ notasi ruang vektor standar berdimensi n atas field biner $\mathbb{F}_2 = \{0, 1\}$.

Kode diciptakan untuk melindungi (mendeteksi atau mengoreksi) pesan dari kesalahan saat pengiriman. Untuk mendeteksi terjadi kesalahan pada pesan digunakan konsep bobot Hamming dan jarak Hamming. Misalnya didefinisikan suatu kode dengan panjang n di dalam ruang $\mathbb{F}_2^n$ dengan vektor $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in C$. Bobot Hamming (*Hamming weight*) dari suatu kode adalah banyaknya simbol tak nol dalam vektor $\mathbf{x} \in \mathbb{F}_2^n$, dinotasikan $\mathrm{wt}(\mathbf{x})$, Sedangkan bobot minimum dari suatu kode C didefinisikan

$$\mathrm{wt}(\mathbf{x}) = \min\{\mathrm{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq 0\}. \quad (1)$$

Jarak Hamming (*Hamming distance*) antara dua vektor $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, dinotasikan $d(\mathbf{x}, \mathbf{y})$, adalah banyaknya posisi dijit dari $\mathbf{x}$ dan $\mathbf{y}$ dimana simbol mereka berbeda. Sedangkan jarak minimum dari suatu kode C didefinisikan

$$d(\mathbf{x}, \mathbf{y}) = \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}. \quad (2)$$

Jelas jarak minimum dari suatu kode linear biner C adalah bobot minimum dari sembarang katakode taknol dengan menggunakan operasi XOR pada dua vektor $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, ditulis

$$d(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} \oplus \mathbf{y}). \tag{3}$$

Masalah utama dalam proses enkoding adalah mengkonstruksi suatu kode. Mengkonstruksi suatu kode berarti mendefinisikan matriks cek paritas **H** atau matriks generator **G**. Matriks cek paritas (*parity check matrix*) adalah matriks yang berukuran $(n-k)$ x n yang semua barisnya merupakan suatu basis untuk $C^{\perp}$(kode dual dari C). Dengan demikian $C^{\perp}$ berdimensi $r = n - k$. Bentuk standar dari matriks cek paritas

$$\mathbf{H} = \left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1k} & 1 & 0 & \cdots & 0 \\ a_{21} & a_{22} & & a_{2k} & 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rk} & 0 & 0 & \cdots & 1 \end{array}\right) \tag{4}$$

atau dapat ditulis $\mathbf{H} = (\mathbf{B^T} \mid \mathbf{I_r})$. Sedangkan matriks generator adalah matriks berkuran k x n yang semua barisnya merupakan basis untuk kode C, ditulis $\mathbf{G} = (\mathbf{I_k} \mid \mathbf{B})$.

Kode *Gilbert-Varshamov* adalah suatu kode-$[n, k, d]$ yang dapat kontruksi menjadi sebuah kode dengan parameter $[n+1, k+1, d]$. Kode C dengan parameter $[n, k, d]$ disebut kode optimal kuat jika $[n, k, d]$ ada dan telah berhasil dibuktikan bahwa $[n+1, k+1, d]$ tidak ada. Berdasarkan problem diatas formulasi rekonstruksi kode berlandaskan pada teorema berikut ini.

Teorema 1 (*The Gilbert-Varshamov bound*) Jika diketahui kode $[n, k, d]$ yang memenuhi ketaksamaan

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{d-2} < 2^{n-k}$$

maka ada (dapat dikonstruksi) kode dengan parameter $[\text{n} + 1, \text{k} + 1, \text{d}]$.

Berdasarkan Teorema 1, dilakukan proses enkoding dengan menggunakan submatriks cek paritas dan submatriks generator yang didasarkan atas pertimbangan efesiensi komputasi, yaitu matriks **B** yang berukuran k x r yang memenuhi sifat-sifat sebagai berikut:

1. Vektor-vektor baris dari **B** berbobot paling sedikit $(d-1)$.
2. Jumlah setiap i vektor baris dari **B** berbobot paling sedikit $(d-i)$ untuk setiap $i = 2, 3, \ldots, s$ dimana $s = \min\{d-1, k\}$.

REKONSTRUKSI

Untuk menyelesaikan proses pemulihan katakode yang diasumsikan terjadi galat pada pesan, maka akan dilakukan proses rekonstruksi kode terlebih dahulu. Proses rekonstruksi dilakukan berdasarkan sifat-sifat kontruksi diatas yang didasarkan pada tabel Brouwer [3]. Ide dasar untuk merekonstruksi suatu kode dimulai dengan mendefinisikan matriks generator **G** atau matrik cek paritas **H** . Misal diberikan bloks simbol pesan dengan panjang k dinotasikan $\mathbf{m} = m_1 m_2 \dots m_k$ akan dienkode menjadi katakode $\mathbf{x} = x_1 x_2 \dots x_k x_{k+1} \dots x_n$ dimana $n \geq k$ dengan

$$\mathbf{x} = \mathbf{mG} \quad \text{atau} \quad \mathbf{Hx}^{\mathrm{T}} = \mathbf{0} \tag{5}$$

Setelah kode-$[n, k, d]$ terkonstruksi, langkah berikutnya adalah mendefinisikan himpunan **V** yang beranggotakan semua vektor baris dari **B** dan semua vektor dari hasil jumlah i vektor baris dari **B** untuk $i = 2, 3, \dots, s$ dimana $s = \min\{d - 1, k\}$, sehingga jelas bahwa $\mathbf{V} \subseteq \mathbb{F}_2^r$. Jika $\mathbf{V} \neq \mathbb{F}_2^r$, maka ada vektor $\mathbf{x} \in \mathbb{F}_2^r$ dan $\mathbf{x} \notin \mathbf{V}$ yang bisa ditambahkan ke baris matriks **B** untuk mendefinisikan matriks $\mathbf{B_1}$ berukuran $(k + 1)$ x r dan matriks cek paritas $\mathbf{H_1}$ akan mendefinisikan kode dengan parameter $[n + 1, k + 1, d]$. Dalam penelitian ini akan ditentukan bahwa strategi konstruksi kode $[n + 1, k + 1, d]$ akan memenuhi teorema *Gilbert-Varshamov bound*.

Proses ekstensi kode dari $[n,\ k, d]$ ke $[n + 1, k + 1, d]$ dilakukan tahap demi tahap sampai diperoleh suatu kode C dengan parameter $[n', k', d]$ yang sudah tidak bisa diperluas lagi. Ketika diperoleh informasi bahwa telah dibuktikan bahwa kode dengan parameter $[n' + 1, k' + 1, d]$ tidak ada, maka C merupakan kode optimal kuat yang telah berhasil dikonstruksi. Akan tetapi, ketika diperoleh informasi bahwa ada kode dengan parameter $[n' + 1, k' + 1, d]$, berarti kita telah gagal mengkonstrusi kode optimal kuat. Dalam hal ini, kita harus melakukan rekonstruksi dengan strategi memilih kode dasar $[n,\ k, d]$ yang lain yang berpeluang besar dapat diperluas menjadi kode optimal kuat C.

Selanjutnya yang akan dijelaskan dibawah ini untuk kasus *double error correcting* $(d = 7)$. Kode-kode optimal kuat yang disusun berdasar urutan dari dimensi terendah di antranya [11, 2, 7], [15, 5, 7], [23, 12, 7], dan [27, 14, 7], [31, 17, 7]. Sedangkan untuk $k > 17$ masih menjadi *problem terbuka*. Metode dan strategi yang diterapkan untuk mengkonstruksi kode-kode optimal kuat akan dijelaskan dibawah ini

1. Konstruksi kode dengan parameter [11, 2, 7]

Konstruksi dimulai dengan mendefinisikan matriks **B** yang berukuran 2 x 9 berikut

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Dari matriks tersebut akan digunakan sebagai dasar matriks yang diperluas menjadi matriks B_1 yang mendifinisikan optimal kuat berikutnya.

2. Konstruksi kode dengan parameter [15, 5, 7]

Matriks B_1 diperoleh dengan cara menambahkan satu vektor nol pada kolom matriks B, selanjutnya menambahkan tiga vektor 10 bit yang memenuhi syarat strategi algoritma konstruksi. Tanpa memperhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukan ada 36 macam matriks B_1 yang berukuran 5 x 10, kemudian dengan dihilangkan matriks-matriks yang saling ekuivalen ternyata diperoleh 1 kode optimal kuat yang berbobot genap, yaitu

$$\mathrm{B}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3. Konstruksi kode dengan parameter [23, 12, 7]

Matriks B_3 diperoleh dengan cara menambahkan tujuh vektor 11 bit yang memenuhi syarat strategi algoritma konstruksi. Tanpa memperhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukan ada 1 macam matriks yang berukuran 12 x 11 yang tidak saling ekuivalen dan merupakan kode optimal kuat, yaitu

$$B_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

4. Konstruksi kode dengan parameter [27, 14, 7]

Dengan cara yang serupa, kode linear dengan paremater [27, 14, 7] diperoleh dengan menghapus beberapa baris dari matriks B_3 dan dilakukan rekonstruksi ulang. Hasil komputasi menunjukkan ada 291 macam matriks B_4 yang berukuran 14 x 13, kemudian dengan dihilangkan matriks-matriks yang saling ekuivalen ternyata diperoleh 8 kode optimal kuat, salah satunya

$$B_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

5. Konstruksi kode dengan parameter [31, 17, 7]

Percobaan untuk memperluas B_4 ke matriks berikutnya untuk mendapapatkan kode optimal kuat $[31, 17, 7]$ adalah gagal dikonstruksi. Sedangkan untuk kode dengan ukuran yang lebih besar masih menjadi masalah terbuka (*open problem*). Dalam hal ini B_4 hanya mampu diperluas ke lebih dari 299 macam kode optimal–D $[30, 16, 7]$. Namun demikian, strategi rekontruksi berhasil mendefinisikan sedikitnya 2 optimal kuat $[31, 17, 7]$ yang direpresentasikan oleh matriks berukuran 17 x 14. Karena bisa diperluas sampai kode $[31, 17, 7]$, berarti pada penelitian ini berhasil memperbaiki batas bawah problem terbuka diatas.

DEKODING SINDROM

Misal diketahui simbol pesan biner $\mathbf{m} = m_1 m_2 \ldots m_k$ akan dienkode menjadi katakode $\mathbf{x} = x_1 x_2 \ldots x_n$ dengan $n > k$ yang selanjutnya dikirim melalui saluran terganggu, maka vektor yang diterima $\mathbf{y} = y_1 y_2 \ldots y_n$ boleh jadi pesan yang dikirim berbeda dengan yang diterima. Dari proses ini diasumsikan terdapat vektor galat (*error vector*)

$$\mathbf{e} = e_1 e_2 \ldots e_n \tag{6}$$

yang didefinisikan sebagai selisih antara vektor **x** dan vektor **y,** yaitu $\mathbf{x} = \mathbf{y} - \mathbf{e}$ atau dalam kasus biner dapat ditulis

$$\mathbf{x} = \mathbf{y} \oplus \mathbf{e}. \tag{7}$$

Jika vektor $e_i = 0$ berarti simbol untuk posisi ke- i bernilai benar dan $e_i = 1$ maka simbol untuk posisi ke- i bernilai salah.

Dalam proses dekoding, dekoder harus memutuskan yang mana diantara $\mathbf{x} \in C$ yang dikirim dan telah berubah menjadi $\mathbf{y} \in \hat{C}$. Untuk menjelaskan bagaimana

dekoder bekerja diperlukan konsep jarak minimum dan bobot minimum pada persamaan (2) dan (3). Peranan jarak minimum suatu kode dalam proses transfer informasi digunakan untuk menentukan banyaknya galat. Suatu kode C dengan panjang n, baik yang linear atau taklinear dengan jarak minimum d mampu mengoreksi $\frac{d-1}{2}$ galat dan jika d genap, C mampu mengoreksi $\frac{d-2}{2}$ galat dan sekaligus mendeteksi $\frac{d}{2}$ galat yang mengacu pada journal [8].

Dekoding sindrom merupakan metode untuk menentukan banyaknya galat pada katakode. Sindrom **S** dari kode **y** didefinisikan sebagai vektor

$$\mathbf{S} = \mathbf{H}\mathbf{y}^{\mathbf{T}}, \tag{8}$$

dimana **H** matriks cek paritas dan **y** katakode yang diterima yang tersimpan pada mesin dekoder. Suatu cara bagaimana menggambarkan mesin dekoder bekerja adalah dengan menggunakan tabel simpanan atau tanpa simpanan. Katakode yang mempunyai galat yang tersimpan pada tabel simpanan ditentukan dengan menggunakan dekoding sindrom, sindrom **S** dari kode $\hat{C}$ dapat ditulis

$$\mathbf{S} = \mathbf{H}\hat{C}^{\mathrm{T}} = [\mathbf{B}^{\mathrm{T}} | \mathrm{I}\,] \begin{bmatrix} \hat{\mathbf{m}} \\ \hat{\mathbf{x}} \end{bmatrix} = \mathbf{B}^{\mathrm{T}}\hat{\mathbf{m}} \oplus \hat{\mathbf{x}} = \begin{pmatrix} \mathbf{B}^{\mathrm{T}}\hat{\mathbf{m}} \\ \hat{\mathbf{x}} \end{pmatrix}. \tag{9}$$

Dari persamaan definsisi sindrom dan persamaan (9) dapat diturunkan beberapa sifat sindrom, yaitu:

1. Karena **H** berukuran r x n dimana $r = n - k$ dan katakode yang diterima $\hat{C}$ berukuran 1 x n ($\hat{C}^{\mathrm{T}}$ berukuran n x 1), maka **S** berukuran r x 1.
2. Bobot minimum dari sindrom, ditulis $s = wt(\mathbf{S})$ menentukan keaslian dari katakode yang dikirim. Jika $s = 0$, maka katakode yang dikirim sama dengan yang diterima.
3. Galat yang muncul bisa terjadi pada simbol pesan yang dinotasikan e_u atau simbol ekstra yang dinotasikan e_p, sehingga katakode C dapat ditentukan

$$C = \hat{C} \oplus \boldsymbol{e} = (\mathrm{Ru}|\mathrm{Rp}) \oplus \begin{pmatrix} \mathrm{e}_u \\ e_p \end{pmatrix} = \left(\mathrm{Ru} \oplus \mathrm{e}_u \,\middle|\, \mathrm{Rp} \oplus e_p \right).$$

Sifat 3 menyatakan bahwa "$\mathrm{Ru} + \mathrm{e}_u$ dan $\mathrm{Rp} + e_p$ merupakan simbol pesan dan simbol ekstra bergalat". Ilustrasikan posisi galat ada di posisi mana, perhatikan kasus kode linear biner dengan panjang kode $d = 7$ dibawah ini.

Tabel 2
Nilai galat pada simbol pesan dan simbol ekstra

$\boldsymbol{e_u}$	$\boldsymbol{e_p}$	$\mathbf{wt}(\mathbf{S})$
0	0	0
0	1	1
0	2	2

0	3	3
1	0	≥ 6
1	1	≥ 5
1	2	≥ 4
2	0	≥ 5
2	1	≥ 4
3	0	≥ 4

Berdasar Tabel 2 jalas nilai galat yang muncul pasti pada katakode yang diterima terjadi pada *simbol ekstra* karena setiap minimal ada 1 galat pada simbol pesan, maka bobot dari sindromnya bernilai lebih besar dari t atau $(wt(\mathbf{S}) \geq t)$. Dengan demikian dapat diturunkan sebuah proposisi yang menjelaskan tentang nilai galat.

Proposisi 3 Jika $\mathbf{wt}(\mathbf{S}) \leq t$, maka nilai $e_u = 0$ (vektor nol), sehingga kode $C = [\mathrm{Ru}|\mathrm{X}]$ dengan $X = \mathrm{Rp} \oplus \mathbf{S}$.

Proposisi (3) mengisyaratkan bahwa bobot sindrom yang terdapat pada katakode yang diterima dapat dikategorikan menjadi 3 bagian, yaitu

1. Jika $wt(\mathbf{S}) = 0$, maka katakode yang dikirim sama dengan katakode yang diterima $\mathbf{y} \in C$.
2. Jika $\mathbf{wt}(\mathbf{S}) \leq t$, maka terjadi galat dipastikan pada simbol ekstra atau tidak ada galat diposisi simbol pesan (artinya $e_u = 0$)**,** dengan demikian katakode yang diterima adalah
$$C = \begin{pmatrix} \mathrm{Ru} \\ \mathrm{Rp} \oplus e_p \end{pmatrix}.$$
3. Jika $\mathbf{wt}(\mathbf{S}) > t$, maka $e_u \neq 0$ artinya bobot simbol pesan $\mathbf{wt}(e_u)$ paling sedikit 1, kemudian dilacak galatnya diposisi simbol pesan dan simbol ekstra dari 1 sampai dengan t, ditulis
$$\mathrm{S} = (\mathrm{Ru}|\mathrm{I}_r)\begin{pmatrix} e_u \\ e_p \end{pmatrix} = \left(\mathrm{B}^{\mathrm{T}} e_u \oplus e_p\right).$$
Selanjutnya, menampilkan koleksi semua himpunan katakode yang diasumsikan memiliki galat disiombolkan M dan banyaknya m,
$$m = \binom{k}{i} \quad ; 1 \leq i \leq t$$
Jika j menyatakan posisi ke- j dari katakode bergalat, maka untuk $1 \leq j \leq m$ akan ditentukan posisi galat dari koleksi semua himpunan katakode yang mempunyai galat yang disimbolkan $L = M[j]$, kemudian diambil katakode yang memiliki galat pada tabel Look Up yang disimbolkan N, kemudian dihitung simbol paritas. Karena sindrom **S** dari e didefinisikan
$$\mathbf{S} = \mathbf{H}e^{\mathrm{T}} = (\ \mathbf{B^T} \mid \mathbf{I}_r\ )\left(\frac{e_u}{e_p}\right) = \mathbf{B^T}\ e_u \oplus e_p$$

Jika $\mathrm{N} = \mathbf{B}^{\mathbf{T}}\, e_u$ maka diperoleh simbol paritas $e_p = \mathrm{N} \oplus \mathbf{S}$ dan simbol pesan yang diterima dapat dihitung

$$C_u = \mathrm{Ru} \oplus e_u \text{ dan } C_p = \mathrm{Rp} \oplus e_p$$

Sehingga diperoleh katakode yang dikirim adalah

$$C = (\, C_u \mid C_p \,).$$

Hasil dari penjelasan diatas, kemudian diturunkan dua buah algoritma dekoding sindrom dengan menggunakan tabel simpanan dan tanpa tabel simpanan.

Algoritma 1. (Dekoding katakode yang diterima dengan tabel simpanan)

Input : C katakode yang dikirim, Cu simbol pesan dari katakode yang dikirim, Cp simbol ekstra dari katakode yang dikirim, Ru simbol pesan yang diterima (panjang 1 sampai k), Rp simbol ekstra yang diterima (panjang $k+1$ sampai n), X vektor nol (panjang 1 sampai $r = n - k$), S menyatakan sindrom, Ep vektor galat simbol paritas, Eu vektor galat simbol pesan, M koleksi semua himpunan katakode yang memiliki galat, m banyaknya anggota dari M, L list posisi himpunan katakode yang memiliki galat, N mengambil list posisi katakode bergalat pada tabel simpanan, Ls memetakan katakode bergalat.

Output : Vektor hC katakode tanpa galat

1. $t \coloneqq \frac{d-1}{2}$ dimana t batas maksimal mengoreksi kesalahan.
2. Katakode yang diterima $[Ru|Rp]$
   a. $Ru \coloneqq [\mathrm{op}(1..\mathrm{k}, \mathrm{R})]$ dimana Ru menyatakan simbol pesan, dinotasikan dengan op(1..k, R), operands dari pernyataan R yang diterima yang memiliki panjang 1 sampai k yang digunakan dalam *software* MAPLE.
   b. $Rp \coloneqq [\mathrm{op}(\mathrm{k}+1..n, \mathrm{R})]$ dimana Ru menyatakan simbol pesan yang diterima yang memiliki panjang k+1 sampai n.
3. Jika $1 < i < k$, hitung
   a. Jika $Ru = 1$, hitung $\mathrm{X} := \mathrm{X} \oplus \mathrm{B[i]}$
   b. Hitung sindrom $\mathrm{S} \coloneqq \mathrm{X} \oplus \mathrm{Rp}$
   c. kemudian tentukan bobot sindromnya $\mathrm{s} \coloneqq \mathrm{wt(S)}$.
4. Tentukan bobot sindromnya
   a. Jika $\mathrm{s} = 0$ maka tidak terdapat galat pada katakode yang diterima.
   b. Jika $\mathrm{s} \leq t$, maka dipastikan $Eu = 0$ sehingga katakode yang dikirim memiliki galat pada simbol paritasnya, ditulis $C = [\mathrm{Ru|X}]$.
   c. Jika $\mathrm{s} \geq t$ maka dipastikan $Eu \neq 0$ dimana $wt(Eu)$ paling sedikit memiliki galat 1 pada simbol pesan.
5. Dilakukan pelacakan nilai galatnya dari 1 sampai t dengan menampilkan koleksi himpunan katakode terebut, disiombolkan M dan banyaknya katakode dinotasikan m,

$$m = \text{Jumlah (M)} = \binom{k}{i};\ 1 \leq i \leq t\ ,$$

untuk $1 \leq j \leq m$ akan ditentukan posisi galat dari koleksi semua himpunan katakode yang mempunyai galat yang disombolkan $L = M[j]$, kemudian diambil katakode yang memiliki galat pada tabel simpanan yang disimbolkan N = LUTab[op(L)] (program MAPLE pada lampiran tesis [4]), kemudian dihitung simbol paritas. Sindrom **S** dari e didefinisikan

$$\mathbf{S} = \mathbf{H}e^{\mathrm{T}} = (\ \mathbf{B^T}\ |\ \mathbf{I}_r\ )\left(\frac{e_u}{e_p}\right) = \mathbf{B^T}\ Ep \oplus Ep.$$

Karena $\mathrm{N} = \mathbf{B^T} \oplus Ep$ maka diperoleh simbol paritas $Ep = \mathrm{N} \oplus \mathbf{S}$. Kemudian bobot dari Ep, jika $l = \mathbf{wt}(Ep)$, untuk $l + 1 \leq t$ maka tentukan nilai-nilai dibawah ini yang pada penelitian ini menggunakan parameter yang terdapat *software* MAPLE.

a. $Ls = \mathrm{map}(x{-}{>}\ x = 1, L)$ (parameter untuk melakuan pencarian katakode bergalat yang tandai oleh $x = 1$).
b. $Eu = [0,0, \ldots 0];\ 1 \leq i \leq k$ (vektor nol untuk simbol pesan)
c. $Eu = [op(Ls), Eu)]$
d. $Cu = Ru \oplus Eu\ ;\ 1 \leq i \leq k$
e. $Cp = Rp \oplus Ep\ ;$ k+1$\leq i \leq r$
f. $C = [op(Cu), op(Cp)]$.

Algoritma 2. (Dekoding katakode yang diterima tanpa tabel simpanan)

Input : C katakode yang dikirim, Cu simbol pesan dari katakode yang dikirim, Cp simbol ekstra dari katakode yang dikirim, Ru simbol pesan yang diterima (panjang 1 sampai k), Rp simbol ekstra yang diterima (panjang $k + 1$ sampai n), X vektor nol (panjang 1 sampai $r = n - k$), S menyatakan sindrom, Ep vektor galat simbol paritas, Eu vektor galat simbol pesan, M koleksi semua himpunan katakode yang memiliki galat, m banyaknya anggota dari M, L list posisi himpunan katakode yang memiliki galat, N mengambil list posisi katakode bergalat pada tabel simpanan, Ls memetakan katakode bergalat.

Output : Vektor hC katakode tanpa galat

1. $t \coloneqq \frac{d-1}{2}$ dimana t batas maksimal mengoreksi kesalahan.
2. Katakode yang diterima $[Ru|Rp]$
   a. diterima yang memiliki panjang 1 sampai *k*, dinotasikan dengan op(1..k, R), operands dari pernyataan yang digunakan dalam *software* MAPLE.
   b. $Rp \coloneqq [\mathrm{op}(\mathrm{k} + 1..n, \mathrm{R})]$ dimana Ru menyatakan simbol pesan yang diterima yang memiliki panjang $k + 1$ sampai *n*.
3. Jika $1 < i < k$, hitung
   d. Jika $Ru = 1$, hitung X:= X $\oplus$ B[i]
   e. Hitung sindrom S $\coloneqq$ X $\oplus$ Rp
   f. kemudian tentukan bobot sindromnya s $\coloneqq$ wt(S).
4. Tentukan bobot sindromnya
   d. Jika $\mathrm{s} = 0$ maka tidak terdapat galat pada katakode yang diterima.

e. Jika s $\leq t$, maka dipastikan $Eu = 0$ sehingga katakode yang dikirim memiliki galat pada simbol paritasnya, ditulis $C = [\text{Ru}|\text{X}]$.
f. Jika s $\geq t$ maka dipastikan $Eu \neq 0$ dimana $wt(Eu)$ paling sedikit memiliki galat 1 pada simbol pesan.

5. Dilakukan pelacakan nilai galatnya dari 1 sampai t dengan menampilkan koleksi himpunan katakode terebut, disiombolkan M dan banyaknya katakode dinotasikan m,
$$m = \text{Jumlah (M)} = \binom{k}{i};\ 1 \leq i \leq t\ ,$$
untuk $1 \leq j \leq m$ akan ditentukan posisi galat dari koleksi semua himpunan katakode yang mempunyai galat yang disombolkan $L = M[j]$, kemudian diberikan N sebagai vektor nol $\text{N} = [0, 0, 0, \dots, 0];\ 1 \leq i \leq r$ dan untuk $1 \leq h \leq i$ maka akan menentukan posisi galat ke-h yang dinotasikan $g = L(h)$, kemudian update nilai N dengan menjumlahkan nilai vektor nol N yang awal dengan $B(g)$ dan lakukan terus menerus sampai memenuhi ketentuan diatas.
6. Selanjutnya, hitung simbol paritas $Ep = \text{N} \oplus \mathbf{S}$ dan tentukan nilai bobot dari Ep , dinotasikan $l = \text{wt}(Ep)$, maka untuk $l + 1 \leq t$ lakukan pencarian posisi katakode bergalat L yang ditandai oleh $x = 1$ dan menggunakan map (parameter dalam MAPLE) untuk melakukan pencarian
$$Ls = \text{map}(x{-}{>}\ x = 1, L),$$
kemudian update nilai $Eu = \text{subsop}[op(Ls), Eu)]$, dimana $Eu = [0,0, \dots 0];\ 1 \leq i \leq$, sehingga simbol pesan yang diterima
$$Cu = Ru \oplus Eu\ ;\ 1 \leq i \leq k,$$
dan simbol paritas
$$Cp = Rp \oplus Ep\ ;\ k + 1 \leq i \leq r,$$
sehingga diperoleh pesan yang dikirim sama dengan yang diterima, yaitu $C = [\text{op}(Cu), \text{op}(Cp)]$.

SIMPULAN

Dalam penelitian ini telah dilakukan proses enkoding dan dekoding dengan menggunakan teorema *Gilbert-Varshamov* menghasilkan beberapa simpulan sebagai berikut:

1. Berhasil merekonstruksi kode linear biner yang didasarkan pada teorema *Gilbert-Varshamov* yang berjarak minimum rendah $d = 5, 7, 9, 11, 13, 15$ Sedangkan untuk kode optimal kuat dengan $d = 5$ yang berhasil dikontruksi hanya sampai kode $[23, 14, 5]$ dan untuk $k > 14$ gagal dikontruksi, tetapi mampu memperbaiki batas bawah problem terbuka.
2. Berhasil menurunkan algoritma dekoding untuk menentukan proses pelacakan posisi galat pada katakode yang diterima dengan metode tanpa

tabel simpanan, yaitu metode yang lebih baik dari metode tabel simpanan karena hanya menampilkan bagian-bagian katakode yang bergalat, sehingga berpengaruh dalam kecepatan aspek pelacakan.

3. Penelitian ini berkontribusi untuk mendeteksi terjadinya galat pada sistem komunikasi data dan sekaligus mengoreksi kembali, sehingga menjadi data yang benar.

DAFTAR PUSTAKA

[1] Hashim AA. 1978. Improvement on Varshamov-Gilbert lower bound on minimum Hamming distance of linear codes. *Proc. Inst. Elec. Engrs*. 125: 104−106.

[2] Barg A, Guritman S, Simonis J. 2000. Strengthening the Gilbert-Varshamov bound. *Linear Algebra and its Applications.* 307: 119−129.

[3] Brouwer AE. 1998. *Bounds on the size of linear codes in Handbook of Coding theory*. Ed 5th. Elsevier.

[4] Saepulrohman A. 2015. *Dekoding Kode Gilbert-Varshamov Biner Berjarak Minimum Rendah* [tesis]. Bogor: Program Pascasarjana, Institut Pertanian Bogor.

[5] MacWilliams FJ, Sloane NJA. 1983. *The theory of error-correcting codes*. Amsterdam: North-Holland Publishing Co.

[6] Bouyukliev I, Guritman S, Vavrek V. 2000. Some bounds for the minimum length of binary linear codes of dimension nine. *IEEE Trans. Inform. Theory*. 46(3): 1053−1056.

[7] Ling S, Xing C. 2004. *Coding Theory - A First Course.* New York: Cambridge.

[8] Dodunekov SM, Guritman S, Simonis J. 1999. Some new results on the minimum length of binary linear codes of dimension nine. *IEEE Trans. Inform. Theory.* 45: 2543−2546.

[9] Yehuda L. 2010. *Introduction to Coding Theory*. Israel: Department of Computer Science Bar-Ilan University.