KOMPUTASI, Vol.15, No.2, Juli 2018, pp. 164−171
ISSN: 1693-7554,

DEKODING SINDROM KODE LINEAR GILBERT-VARSHAMOV BINER DENGAN JARAK MINIMUM 15

Asep Saepulrohman
Program Studi Ilmu Komputer – FMIPA Universitas Pakuan
Jl. Pakuan PO BOX 452, Bogor
Telp/Fax (0251) 8375 547
Email: asepspl@unpak.ac.id

Abstrak

Transmisi data merupakan proses untuk melakukan pengiriman data dari salah satu sumber data ke penerima menggunakan media tertentu. Dalam transimisi data, pesan dikirim melalui jaringan internet bisa terjadi perubahan yang mengakibatkan pesan tidak autentik. Pesan dalam bentuk kode linear biner dengan panjang n yang merupakan subruang vektor $\mathbb{F}_2^n$ yang merupakan kode biner. Kode tersebut dapat direpresentasikan dalam bentuk digital sebagai barisan simbol, umumnya digunakan blok simbol biner $\mathbb{F}_2 = \{0,1\}$ yang dikenal dengan bitstring. Kode linear biner didefinisikan sebagai operasi XOR (eXclusive OR) yang berguna untuk mendeteksi dan mengoreksi apabila terjadi kesalahan (error) informasi. Semakin besar sebuah data, semakin lama waktu yang diperlukan semakin besar kemungkinan data yang hilang. Oleh karena itu dibutuhkan cara metode untuk mengkontruksi sebuah kode yang lebih optimal tanpa merusak informasi. Metode yang digunakan menggunakan kode Gilbert-Vashamov biner yang merupakan salah satu cara penyandian (*encoding*) *yang menggunakan tiga parameter yaitu, panjang kode, dimensi, jarak minimum. Mengkonstruksi suatu kode dengan panjang n yang berdimensi k dengan jarak d dinyatakan sebagai kode $[n,k,d]$ yang memiliki beban komputasi cukup berat, dalam hal ini dekoder harus menyediakan memori untuk matrik berukuran $2^{n-k} \times 2^k$. Untuk mengkontruksi kode optimal kuat dilakukan pemilihan kode dasar untuk submatriks generator atau cek paritas dengan menghapus beberapa matriks baris yang tidak sempurna dengan jarak minimum 15 dan dilakukan dengan digunakan paket program konstruksi dengan menggunakan software MAPLE..*

***Kata Kunci**: Kode linear, teorema Gilbert-Varshamov, dekoding sindrom, bobot Hamming.*

Abstract

Data transmission is the process of sending data from one data source to the receiver using certain media. In the transmission of data, messages sent over the internet can cause changes that result in inauthentic messages. Message in the form of binary linear code with length n which is a vector space $\mathbb{F}_2^n$ which is binary code. The code can be represented in digital form as a row of symbols, commonly used binary symbol blocks $\mathbb{F}_2 = \{0,1\}$, known as bitstrings. Binary linear code is defined as an XOR (eXclusive OR) operation that is useful for detecting and correcting when an error occurs (information) information. The larger the data, the longer the time needed, the more likely the missing data. Therefore we need a method to construct a more optimal code without destroying information. The method used uses the Gilbert-Vashamov binary code which is one of the encoding methods that uses three parameters namely, code length, dimensions, minimum distance. Constructing a code of length n dimension k with distance d is expressed as code [n, k, d] which has a heavy computational burden, in this case the decoder must provide memory for a matrix of size $2^{n-k} \times 2^k$. To construct a strong optimal code, a selection of base code for generator submatrix or parity check is done by removing some imperfect matrix lines with a minimum distance of 15 and using a construction program package using certain MAPLE software.

***Keywords :** Linear code, Gilbert-Varshhamov theorem, Syndrome decoding, Hamming weight*

Received May 18, 2018; Revised May 28, 2018; Accepted June 2, 2018

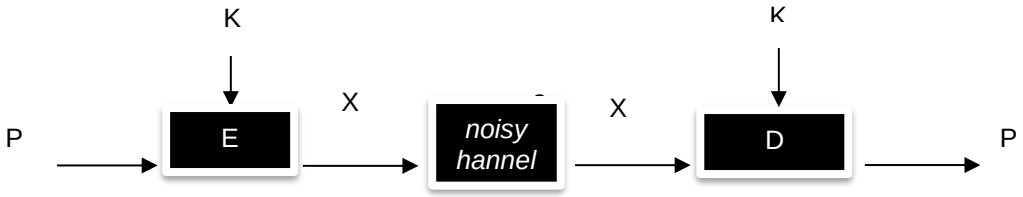
1. Pendahuluan

Dalam sistem komunikasi digital ada beberapa metode untuk mengetahui terjadinya kesalahan (*error*) saat pengiriman data, salah satunya penelitian terdahulu menggunakan metode *Forward Error Correction* (CEF) yang bekerja mengatasi *error* pada penerima [5]. Dari penelitian sebelumnya dikembangkan metode Dekoding Sindrom Gilbert-Varshmov Biner dengan menambahkan bit paritas pada data pesan awal yang kemudian pesan tersebut dikirim berbasis sinyal elektrik, yang memungkinkan sinyalnya bersifat terputus-putus dan menggunakan sistem bilangan biner. Bilangan biner tersebut akan membentuk kode-kode yang merepresentasikan suatu informasi tertentu. Setelah melalui proses digitalisasi informasi yang masuk akan berubah menjadi serangkaian bilangan biner yang membentuk informasi dalam wujud kode digital. Kode digital tersebut nantinya akan mampu dimanipulasi oleh komputer. Teori yang mendasari sistem komunikasi data pertama kali ditemukan pada tahun 1948 oleh Claude E. Shannon telah menerbitkan "*Teori Matematika Komunikasi*". Karya ini mengkaji masalah teori koding (*coding theory*) [6] yang berfokus pada pengiriman data [3]. Informasi yang dikirim berupa pesan yang ditransmisi melalui saluran terganggu (*noisy chanel*), sering kali pesan yang diterima tidak sama dengan pesan yang dikirim. Pada awalnya sistem pengamanan transmisi data sangat dominan digunakan pada bidang militer dan layanan pemerintahan yang berfungsi untuk melindungi hal-hal kebijakan strategis dan melindungi rahasia negara atau banyak dipakai pada bidang intelejen untuk memberikan layanan keamanan negara.

Dalam komunikasi, pesan dapat direpresentasikan dalam bentuk digital sebagai barisan (*block*) simbol, umumnya digunakan blok simbol biner $\mathbb{F}_2 = \{0, 1\}$ yang dikenal dengan *bitstring* [4]. Pendefinisian kode dilakukakan sedemikian sehingga apabila terjadi perubahan beberapa simbol, maka kesalahan tersebut dapat dipulihkan kembali. Dengan demikinan, kode diciptakan untuk mendeteksi dan mengoreksi apabila terjadi galat (*error*) saat pengiriman pesan dalam saluran terganggu. Pesan dalam simbol biner diubah menjadi katakode (*codeword*) dengan cara menambahkan matriks cek paritas [7]. Proses mengubah pesan menjadi katakode disebut enkoding (*encoding*) dan perangkat yang mengubah pesan menjadi katakode disebut enkoder (*encoder*).

Kode merupakan representasi dari himpunan semua pesan, artinya satu katakode mewakili satu pesan. Dengan demikian di dalam setiap bitstring katakode harus mengandung dua makna, yaitu simbol pesan dan simbol cek. Simbol pesan telah diketahui sebagai bentuk biner dari pesan, sedangkan simbol cek merupakan simbol ekstra yang ditempelkan pada pesan. Biasanya nilai simbol cek bergantung pada simbol pesan. Simbol cek didefinisikan dengan tujuan untuk melindungi pesan.

Beberapa tujuan keamanan informasi diantaranya menjaga kerahasian informasi, integritas data (*data integrity*) artinya informasi tidak diganti, autentifikasi entitas atau pesan benar-benar berasal dari sumber informasi, penandaan (*signature*) [5] maksudnya suatu alat yang digunakan untuk memberikan ciri tertentu pada informasi yang ditujukan ke suatu entitas [4]. Secara umum, proses pengiriman pesan dapat digambarkan sebagai berikut.



Gambar 1 Sistem transmisi pesan kode biner

Skema pengiriman pesan kode linear biner menggunakan kunci eksternal pada saat enkripsi dan dekripsi, yaitu

P : Plainteks / pesan awal yang beranggotakan string simbol biner
E : Enkripsi /transformasi plainteks menjadi cipherteks atau E(m)
K : Key/himpunan berhingga ruang kunci
X : Chiperteks / himpunan pesan yang telah diekripsi
D : Dekripsi/proses pengembalian chiperteks menjadi plainteks semula.

2. Metode Penelitian

Metode penelitian yang digunakan dalam mengkonstruksi kode yang optimal kuat berjarak minimu 15 melalui tahapan sebagai berikut

1. Pengembangan Konsep

   Masalah utama dalam penelitian ini adalah mengoptimalkan sebuah kode-$[n, k, d]$ berjarak minimum rendah yang digunakan untuk meminimalkan kesalahan sehingga pesan yang diterima sesuai dengan yang dikirim berdasakan pada pengembangan teorema *Gilbert-Varshamov* biner. Jika terjadi kesalahan maka dilakukan proses pemulihan (*decoding*) menjadi pesan asli. Kode C dengan parameter $[n, k, d]$ disebut optimal kuat (*strongly optimal codes*) jika kode dengan parameter $[n, k, d]$ ada dan telah dibuktikan bahwa kode dengan parameter $[n + 1, k + 1, d]$ tidak ada [1]. Hal ini sesuai berdasar teorema *Gilbert-Varshamov* di bawah ini.

   Teorema 1. (*The Gilbert-Varshamov bound* [8]) *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 $[n + 1, k + 1, d]$.

2. Perancangan Algoritma

   Prosedur untuk pelacakan kode optimal kuat dengan jarak minimum 15 dilakukan dengan menggunkan *software* MAPLE yang dirancang agar dapat diaplikasikan untuk menemukan jarak optimal.

3. Mengontruksi Kode Optimal Kuat

   Masalah utama dalam penelitian ini adalah mengoptimalkan sebuah kode-$[n, k, d]$ berjarak minimum.Fungsi-fungsi yang berhubungan dengan proses rekonstruksi suatu kode linear biner merupakan pengembangan dari fungsi-fungsi aljabar matriks. Selain itu, proses rekonstruksi melibatkan aspek pengembangan komputasi, sampai kajian eksplorasi untuk memecahkan kode optimal kuat. Untuk mencapai hal tersebut, dilakukan hal sebagai berikut:

   1. Merekonstruksi kode *Gilbert-Varshamov* biner berjarak minimum rendah.
   2. Menyusun algoritma proses enkoding dan dekoding dari hasil merekonstruksi yang mengacu pada tujuan pertama.
   3. Mengimplementasikan algoritma proses pelacakan enkoding dan dekoding dalam bahasa pemrograman yang didasarkan pada tujuan pertama dan kedua.

3. Hasil dan Pembahasan

3.1 Pengembangan Teori

Pada tahap ini akan dilakukan rekonstruksi kode dengan parameter $[n, k, d]$ berjarak minimum rendah dengan mendefinisikan matriks cek paritas (*parity check matrix*), yaitu Berdasarkan Teorema 3 merekonstruksi suatu kode cukup mengkonstruksi bentuk standar matriks $\mathbf{H}$

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1k} & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & 1 & \vdots \\ a_{r1} & \cdots & a_{rk} & 0 & \cdots & 1 \end{array}\right). \quad (1)$$

Berdasarkan Teorema 1 merekonstruksi suatu kode cukup mengkonstruksi bentuk standar matriks $\mathbf{H}$, tetapi atas pertimbangan efisiensi komputasi cukup mengkonstruksi matriks $\mathbf{B}$ berukuran k x r yang memenuhi sifat-sifat:

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

Tahap selanjutnya melakukan proses dekoding untuk mendapatkan pesan asli dengan mengacu pada hasil rekonstruksi. Jika 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 dari suatu kode adalah

banyaknya simbol tak nol dalam vektor $\boldsymbol{x} \in \mathbb{F}_2^n$, dinotasikan $wt(\boldsymbol{x})$, sedangkan jarak Hamming 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 simbolnya berbeda [5]. Jelas jarak minimum dari suatu kode linear biner C adalah bobot minimum dari sembarang katakode taknol dengan menggunakan operasi XOR [8] pada dua vektor $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, ditulis

$$d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} + \mathbf{y}) \quad (2)$$

dan pada tahap terakhir mengimplentasikan algoritma-algoritma ke dalam bahasa pemrograman dengan menggunakan *software* MAPLE.

3.2 Perancangan Algoritma

Algoritma 1. (Prosedur memberi galat pada pesan katakode yang dikirim)

Input : Integer n dengan $n > 0$, jarak minimum d, list kode C

Output : Vektor C_n sebagai katakode yang telah diberi galat

1. $t := \frac{d-1}{2}$ dimana t batas maksimal mengoreksi kesalahan.
2. $\mathrm{S} := \binom{n}{0}$ dimana S banyaknya kode dalam ruang vektor standar $\mathbb{F}_2^n$.
3. Jika 1 < i < t, hitung $\mathrm{S} := \binom{n}{i}$ diperoleh $\mathrm{S} := [\mathrm{op}(\mathrm{S}), \mathrm{op}(\mathrm{T})]$:
4. Kemudian hitung
   a. $\mathrm{U} := \binom{\mathrm{S}}{1}$
   b. $\mathrm{V} :=$ ({op(op(U))},n) dimana V menguubah U ke bentuk biner
   c. $C_n := Add(C, \mathrm{V}, n)$
5. return(C_n).

Selanjutnya, mengisi tabel Look Up yang berfungsi menyimpan semua katakode dengan susunan semua barisnya adalah semua koset dari suatu kode. Baris pertama dari tabel Look Up adalah kode itu sendiri dengan meletakan katakode nol pada posisi paling kiri dan diikuti koset-koset yang lain pada baris ke-2 sampai dengan baris ke- 2^{n-k} dengan meletakan pimpinan koset pada posisi paling kiri.

Algoritma 2. (Mengisi *Table Look Up*)

Input : Matriks B yang berukuran k x r, dengan $r = n - k$.

Output : Vektor V sebagai katakode yang memiliki galat yang tersimpan pada tabel Look Up

1. Jika 1 < *i* < *t,* hitung
   a. $\mathrm{M} := \binom{n}{0}$ dimana M list semua katakode yang tersimpan dalam tabel Look Up.
   b. $\mathrm{m} := \mathrm{nops}\ \mathrm{M}$ dimana m banyaknya list dari katakode.
2. Jika 1 < *j* < m, hitung
   a. $\mathrm{X} := \mathrm{M}[j]$ dimana X menyatakan katakode yang meiliki error yang terletak ke-j.
   b. $\mathrm{V} := [\mathrm{seq}(0, \mathrm{i} = 1..\mathrm{r})]$ dimana V menyatakan vektor nol yang memiliki panjang 1 sampai r.
3. Jika 1 < *l* < *i*, hitung
   a. $\mathrm{u} := \mathrm{X}[l]$ dimana u menyatakan posisi-posisi error dari X.
   c. $\mathrm{V} := \mathrm{Add}(\mathrm{V}, \mathrm{B}[u], r)$ dimana V hasil penjumlahan dari vektor nol dengan katakode yang bergalat pada matriks B dengan panjang 1 sampai r .

3.3 Konstruksi Kode Linear Optimal Kuat

Konstruksi kode linear [7] tersebut diujicobakan untuk kode linear biner dengan jarak minimum untuk kasus *double error correcting* $(d = 5, 7, 9, 11)$. Proses konstruksi menggunakan bantuan *software* MAPLE yang mengacu pada Tabel Brouwer [2] diperoleh hasil eksplorasi konstruksi kode optimal untuk berikut

d	Kode 1	Kode 2	Kode 3	Kode 4	Kode 5
5	[8, 2, 5]	[11, 4, 5]	[17, 9, 5]	[23, 14, 5]	Open problem
7	[11, 2, 7]	[15, 5, 7]	[23, 12,7]	[27, 14,7]	[31, 17, 7]
9	[14, 2, 9]	[17, 3, 9]	[20, 5, 9]	[23, 7, 9]	[27, 10, 9]

11	[17, 2, 11]	[20, 3, 11]	[23, 5, 9]	[26, 7, 11]	[33, 11, 11]

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

$$B_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

3. **Konstruksi kode dengan parameter [22, 11, 7]**
   Matriks B_2 diperoleh dengan cara menambahkan satu vektor nol pada kolom matriks B_1, selanjutnya menambahkan enam vektor 11 bit yang memenuhi syarat strategi algoritma konstruksi. Tanpa memperhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukan ada 12 macam matriks yang berukuran 11 x 11, kemudian dengan dihilangkan matriks-matriks yang saling ekuivalen ternyata diperoleh 2 kode optimal *varshamov* yang berbobot genap, salah satunya adalah

$$B_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

4. **Konstruksi kode dengan parameter [23, 12, 7]**
   Matriks B_3 diperoleh dengan cara menambahkan satu 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

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

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

Dengan cara yang serupa, kode lonear 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

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

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

Dari kode dengan paremater [27, 14, 7] lakukan pencarian kode optimal kuat dengan menghapus beberapa baris dari matriks B_4 dan dilakukan rekonstruksi ulang. Hasil komputasi menunjukkan ada 299 macam matriks B_5 yang berukuran 17 x 14, kemudian dengan dihilangkan matriks-matriks yang saling ekuivalen ternyata diperoleh 2 kode optimal kuat, salah satunya

$$B_5 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Agar diperoleh kode otptimal baru yang belum diperoleh para peneliti sebelumnya, dilakukan cara perluasan matriks dengan ordo yang lebih besar, namun matriks tersebut gagal dikonstruksi. Rekonstruksi hanya mampu diperluas dengan ukuran 17 x 14 yang merepresentasi kode optimal kuat dengan parameter [31, 17, 7], sedangkan untuk kode dengan ukuran yang lebih besar masih menjadi masalah terbuka (*open problem*) yang menjadi pengembangan peneliti berikutnya.

4. Kesimpulan

Konstruksi sebuah kode linear biner optimal kuat berjarak minimum 15 sangat dipengaruhi oleh metode komputasi yang digunakan. Kajian pengembangan secara teoritik yang digunakan dalam penelitian ini banyak melibatkan aspek aljabar, kajian tentang teorema *Gilbert-Varshamov*, pengembangan metode komputasi, dan kajian eksplorasi untuk memecahkan probelm terbuka tentang kode optimal kuat (*bound of linear codes*) yang didasarkan pada Tabel Brouwer [2]. Harapan tertinggi dari penelitian ini adalah memperbaiki batas bawah fungsi $D(n,k)$, kode linear biner yang berhasil dikonstruksi hanya sampai $k = 17$ dengan parameter kode optimal kuat [31, 17, 7], sedangkan untuk kode dengan parameter yang lebih besar masih gagal dikonstruksi. Hal merupakan masalah terbuka (*open problem*) [9] bagi peneliti berikutnya. Kegagalan dalam menentukan kode optimal kuat disebabkan oleh

1. Pemilihan kode dasar untuk submatriks generator atau cek paritas yang kurang tepat, dalam hal ini diwakili oleh matrisk B.
2. Proses perluasan dalam merekonstruksi kode-kode optimal kuat berikutnya dengan menghapus beberapa baris matriks yang tidak sempurna.
3. Terbatasnya memori komputer yang digunakan dalam proses komputasi dalam pelacakan kode optimal kuat.

References

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

[2] A. E. Brouwer. Bounds on the size of linear codes, in Handbook of Coding Theory, ed. : V. Pless, W. Cary Huffman. ISBN: 0-444-50088-X Elsevier, Amsterdam. Online version of the tables: http://www.win.teu.nl/math/dw/voolincod.html. 1997.

[3] C. Ding. Linear Codes From Some 2-Designs. in *IEEE Transactions on Information Theory*. vol. 61(6).pp. 3265-3275. 2015.

[4] Erez Druk, Yuval I. Linear-time encodable codes meeting the gilbert-varshamov bound and their cryptographic applications. *Proceedings of the 5th conference on Innovations in theoretical computer science.* ACM. 2014.

[5] H. M. Shabour, “Performance Enhancement of the Controller Area Network Protocol Using Reed-Solomon Codes,” *International Conference on Computing, Electrical and Electronic Engineering IEEE*, pp. 512–517, 2013

[6] Pancholi, V.R., Patel, B.P. Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing. *IJIRST-International Journalfor Innovative Research in Science & Technology*. 13(10).pp:240-244. 2015
[7] S. Ling and C. Xing. *Coding Theory-A First Course.* New York:Cambrige. 2004.
[8] S. Guritman, N. Aliantningtyas and T. Wulandari. *Konstruksi Kode Linear Biner Optimal Kuat Berjarak Minimum Rendah*. Departemen Matematika FMIPA Institut Pertanian Bogor. 2010.
[9] S. Guritman. *Aljabar Linear*. Departemen Matematika FMIPA Institut Pertanian Bogor. 2012.
[10] S. Saepulrohman. *Decoding Kode Gilbert-Varshamov Biner Berjarak Minimum Rendah [tesis]*. Departemen Matematika FMIPA Institut Pertanian Bogor. 2015.
[11] Thomas S. Shores. *Apllied Linear Algebra and Matrix Analysis*. USA: Department of Mathematics University of Nebraska Lincoln, NE 68588-0130 Springer. 2000.
[12] Yehuda Lindell. *Introduction to Coding Theory*. Israel: Department of Cumputer Science Bar-Ilan University. 2010.