Prosiding

SEMINAR NASIONAL
MATEMATIKA DAN APLIKASINYA 2013

"Peran Matematika dan Sistem Informasi sebagai Basis Pengembangan IPTEK di Indonesia"

EDITOR

KETUA : Fatmawati

ANGGOTA : Abdulloh Jaelani
Indah Werdiningsih
M.Yusuf S
Toha Saifudin
Nurul Surtika Sari

PENATA LETAK:

Abdulloh Jaelani

DESAIN COVER:

Taufik

PENERBIT:

Departemen Matematika
Fakultas Sains dan Teknologi
Universitas Airlangga
Kampus C, Jl. Mulyorejo, Surabaya

Cetakan pertama September 2013
ISBN No. 978-602-14413-0-5

Tim Penilai Makalah (*Reviewer*):

Eridani, Dr .(Prodi Matematika, FST-Universitas Airlangga)
Moh. Imam Utoyo, Dr. (Prodi Matematika, FST-Universitas Airlangga)
Fatmawati, Dr. (Prodi Matematika, FST-Universitas Airlangga)
Windarto, Dr. (Prodi Matematika, FST-Universitas Airlangga)
Herry Suprajitno, Dr. (Prodi Matematika, FST-Universitas Airlangga)
Miswanto, Dr. (Prodi Matematika, FST-Universitas Airlangga)
Liliek Susilowati, M.Si. (Prodi Matematika, FST-Universitas Airlangga)
Nur Chamidah, M.Si (Prodi Statistik, FST-Universitas Airlangga)
Eto Wuryanto, DEA (Prodi Sistem Informasi, FST-Universitas Airlangga)

KATA PENGANTAR

Prosiding ini merupakan hasil dari Seminar Nasional Matematika dan Aplikasinya 2013 (SNMA 2013) yang diselenggarakan oleh Departemen Matematika Universitas Airlangga pada hari Sabtu, 21 September 2013 yang bertempat di Kampus C, Fakultas Sains dan Teknologi Universitas Airlangga Jl. Mulyorejo Surabaya.

Seminar ini dimaksudkan sebagai sarana untuk publikasi penelitian dan karya tulis, juga dapat digunakan sebagai sarana dan upaya untuk menjalin komunikasi antar praktisi, akademisi dan institusi yang turut serta mengoptimalkan dan memanfaatkan hasil-hasil riset dan inovasi dalam berbagai bidang. Makalah yang dimuat terdiri dari beberapa topik yang terpilih oleh Tim Penilai dan telah dipresentasikan dalam seminar tersebut, yaitu dalam bidang Aljabar dan Graf, Analisis, Matematika Terapan, Riset Operasi dan Komputasi, Statistika, Pendidikan Matematika dan Sistem Informasi.

Makalah yang disusun dalam prosiding ini dicetak sesuai dengan makalah asli yang dikirimkan oleh masing-masing penulis setelah dilakukan perbaikkan atas saran reviewer yang ditunjuk oleh Panitia Seminar. Perubahan yang dilakukan oleh Panitia Seminar hanya terkait dengan format guna keseragaman penulisan dalam prosiding ini.

Walaupun semua makalah yang telah dimuat dalam prosiding telah direview oleh Tim Penilai Makalah, namun tanggung jawab penulisan makalah dalam prosiding ini sepenuhnya ada pada penulis.

Surabaya, September 2013

Tim Editor

DAFTAR ISI

KONSTRUKSI KODE VARSHAMOV BINER BERJARAK MINIMUM RENDAH

Sugi Guritman[1)], Nur Aliatiningtyas[2)], Teduh Wulandari[3)], Muhammad Ilyas[4)]

[1)2)3)4)]*Laboratorium Matematika Murni*
Departemen Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Institut Pertanian Bogor
[1)]guritman@yahoo.co.id
[2)]nur.aliatiningtyas@gmail.com
[3)]teduhw@gmail.com
[4)]reiken7@gmail.com

Abstract— **Misalkan F_2^n menotasikan ruang vektor standar berdimensi *n* atas field biner $F_2 = \{0,1\}$. Kode linear biner dengan panjang *n* didefinisikan sebagai subruang *C* dari F_2^n. Jika *C* berdimensi *k* dengan jarak minimum *d*, maka *C* dinyatakan sebagai kode [*n*,*k*,*d*]. Problem utama dalam aljabar teori koding adalah mengoptimalkan salah satu dari parameter *n*, *k*, dan *d* ketika dua nilai yang lain telah diketahui. Di dalam artikel ini dihasilkan suatu teorema sebagai varian dari teorema *Gilbert-Varshamov bounds*. Kode yang konstruksinya berdasarkan pada teorema ini disebut *kode Varshamov*. Kemudian, kita definisikan *kode optimal* kuat yang metode konstruksinya didasarkan pada kode Varshamov. Eksplorasi komputasi menunjukkan bahwa metode konstruksi tersebut cukup baik diterapkan pada kode berjarak minimum rendah. Dalam hal ini, eksplorasi dilakukan untuk nilai $d \leq 15$, sedangkan untuk $d > 15$ bisa dilakukan tertapi terbatas pada sumberdaya komputasi terkait dengan kompleksitas algoritmenya.**

***Keywords*— Kode Linear Biner, Optimal Kuat, Gilbert-Varshamov Bounds, Konstruksi Kode.**

I. PENDAHULUAN

Teori koding berasal dari suatu problem di teori informasi yang ditulis oleh C.E. Shannon pada tahun 1948 dalam artikelnya yang berjudul *A Mathematical Theory of Communication*. Problem itu dapat digambarkan sebagai berikut. Apabila suatu pesan (informasi) dikirim melalui *saluran terganggu (noisy channel)*, sering kali terjadi bahwa pesan yang diterima tidak sama dengan yang dikirim[1]. Di dalam komunikasi, pesan direpresentasikan dalam bentuk dijitel sebagai blok (barisan) simbol, umumnya menggunakan simbol biner yang dikenal dengan *bitstring*. Saluran biasanya berupa jaringan telepon, jaringan radio berfrekuensi tinggi, jaringan komunikasi satelit, dll. Saluran yang terganggu menyebabkan berubahnya beberapa simbol yang dikirim, sehingga mengurangi kualitas informasi yang diterima.

Suatu *kode* (*code*) dikonstruksi 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 *mengkode* (*enkoding*). Perangkat yang mengubah pesan menjadi katakode disebut *Enkoder*. Kode merupakan himpunan yang anggotanya semua katakode. Pendefinisian kode ini dilakukan sedemikian sehingga apabila terjadinya perubahan beberapa simbol pada katakode, maka galat itu bisa dipulihkan lagi oleh *Dekoder*. Dekoder merupakan perangkat yang mengubah barisan simbol yang diterima menjadi katakode yang selanjutnya dipulihkan menjadi pesan asli. Proses tersebut diringkas dalam bagan berikut ini.

1001	→	1001101	→	ada noisy
Pesan	Enkode	Katakode	Kirim	
				↓
1001	←	1001101	←	1101101
Pesan	Dekode	Katakode	koreksi	galat 1 bit

Di dalam artikel ini diturunkan suatu teorema sebagai varian dari teorema *Gilbert-Varshamov bounds* yang menjadi dasar teori untuk mendefinisikan *kode optimal* kuat beserta metode konstruksinya. Pembahasan meliputi dua seksi. Seksi 2 berisi pengertian kode linear beserta sifat-sifatnya dari sudut pandang aljabar. Seksi 3 memuat bahasan inti dari topik dan tujuan penelitian.

II. MODEL ALJABAR KODE LINEAR

Misalkan $\mathbb{F}_2^n$ menotasikan ruang vektor standar berdimensi *n* atas field biner $\mathbb{F}_2 = \{0,1\}$. *Bobot* (*Hamming weight*) dari suatu vektor $\mathbf{x} \in \mathbb{F}_2^n$, dinotasikan $wt(\mathbf{x})$, adalah banyaknya simbol taknol dalam $\mathbf{x}$. *Jarak* (*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, jelas bahwa $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} + \mathbf{y})$.

[1]Sebagai ilustrasi, pesan yang berupa suara atau gambar menjadi tidak jelas.

Sebagai ilustrasi, di dalam ruang $\mathbb{F}_2^5$, jika $\mathbf{x} = 10011$ dan $\mathbf{y} = 11010$, maka

$$d(\mathbf{x}, \mathbf{y}) = wt(1011 + 11010) = wt(01001) = 2$$

Dalam praktik, pengertian tersebut terkait dengan makna fisik sebagai berikut. Jika pesan **x** dikirim dan berubah menjadi **y** saat diterima, maka $d(\mathbf{x}, \mathbf{y})$ merepresentasikan banyaknya galat yang terjadi. $d(\mathbf{x}, \mathbf{y}) = 0$ berarti tidak terjadi kesalahan saat pengiriman.

Kode linear biner (untuk selanjutnya cukup disebut *kode*) dengan panjang n didefinisikan sebagai *subruang C* dari $\mathbb{F}_2^n$. Anggota suatu kode disebut dengan *katakode*. Walaupun definisinya sederhana, mengkonstruksi suatu kode bukan suatu hal yang sederhana karena harus mempertimbangkan makna praktik yang dijelaskan sebagai berikut.

Kode merupakan representasi dari himpunan semua pesan, artinya satu katakode mewakili satu pesan. Kode diciptakan untuk melindungi (koreksi atau deteksi) pesan dari kesalahan saat pengiriman. Dengan demikian, di dalam setiap *bitstring* katakode harus mengandung dua makna, yaitu *simbol pesan* dan *simbol cek*. Simbol pesan telah diketahui (diberikan) sebagai bentuk biner dari pesan, sedangkan simbol cek merupakan simbol ekstra yang ditempelkan pada pesan. Boasanya nilai simbol cek bergantung pada nilai simbol pesan dalam hubungan sistem persamanan linear. Simbol cek didefinisikan dengan tujuan untuk melindungi pesan dari galat.

Ortogonal dari *C* (baca: *kode dual* dari *C*), notasi $C^\perp$, didefinisikan

$$C^\perp = \{\mathbf{y} \in \mathbb{F}_2^n \ / \ \mathbf{x} \cdot \mathbf{y} = 0 \text{ untuk setiap } \mathbf{x} \in \mathrm{C}\}$$

dengan " · " adalah *produk dalam standar* pada $\mathbb{F}_2^n$ yang didefinisikan sebagai

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i,$$
$$\forall \mathbf{x} = (x_1, x_2, \dots, x_n), \mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n$$

Dengan demikian, jika *C* berdimensi *k*, maka $C^\perp$ berdimensi $r = n - k$.

Suatu matriks **H** berukuran $r \times n$ yang semua barisnya merupakan suatu basis untuk $C^\perp$ disebut *matriks cek paritas* (parity check matrix) dari *C*. Pengertian matriks paritas ini berimplikasi pada pedefinisian kode linear yang berkaitan dengan cara konstruksinya, yaitu

$$C = \{\mathbf{x} \in \mathbb{F}_2^n / \mathbf{H}\mathbf{x}^T = 0\}$$

Dengan kata lain, *C* adalah ker(**H**). Konstruksi kode linear dengan panjang *n* dan berdimensi *k* sama artinya dengan mendefinisikan matriks cek paritas seperti yang dimaksud di atas. Di samping itu, matriks cek paritas berfungsi mengubah pesan menjadi katakode. Dengan kata lain, ia merupakan parameter dalam proses enkode. Enkode kode linear dengan matriks paritas **H** diilustrasikan sebagai berikut.

Diberikan blok *simbol pesan* dengan panjang *k*, misalnya $\mathbf{u} = u_1 u_2 \dots u_k$, akan dikodekan menjadi katakode $\mathbf{x} = x_1 x_2 \dots x_n$ dengan $n \geq k$ dengan menggunakan matriks cek paritas **H** yang telah didefinisikan sebelumnya. Maka, pertama kali didefinisikan

$$x_1 = u_1, x_2 = u_2, \dots, x_k = u_k$$

dan diikuti dengan pendefinisian $r = (n - k)$ *simbol cek* $x_{k+1} x_{k+2} \dots x_n$ yang nilainya bergantung pada nilai simbol pesan. Ketergantungan ini ditentukan oleh **H** dengan menyelesaikan sistem persamaan linear homogen berikut

$$\mathbf{H}\mathbf{x}^T = 0 \Leftrightarrow \mathbf{H}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (1)$$

Demi kemudahan penyelesaian, matriks **H** biasanya diberikan dalam bentuk *standar,* yaitu

$$\mathbf{H} = (\mathbf{A}|\mathbf{I}_r) \qquad (2)$$

dengan **A** adalah matriks biner berukuran $r \times k$, dan $\mathbf{I}_r$ adalah matriks identitas berukuran $r \times r$.

Selain menggunakan matriks cek paritas **H**, untuk mengkonstruksi *C* juga bisa menggunakan *matriks generator* dari *C*, biasanya dinotasikan dengan **G**. Dengan demikian, *semua baris dari G merupakan basis untuk C*. Akibatnya, **G** berukuran $k \times n$ dan setiap katakode merupakan kombinasi linear dari semua vektor baris dari **G**, dengan kata lain

$$C \coloneqq Span(\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\})$$

dimana $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ adalah himpunan semua baris dari **G**. Hubungan antara **H** dan **G** dijelaskan berikut ini.

Dalam katakode $\mathbf{x} = x_1 x_2 \dots x_n$ dari Persamaan (1), $x_1 x_2 \dots x_n$ merupakan *simbol pesan* dan $x_{k+1} x_{k+2} \dots x_n$ adalah *simbol cek*. Dengan notasi matriks, barisan simbol pesan ditulis

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \mathbf{I}_k \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix} \qquad (3)$$

Kemudian dari Persamaan (1) dan (2), diturunkan

$$(\mathbf{A}|\mathbf{I}_{n-k})\begin{pmatrix}x_1\\x_2\\\vdots\\x_k\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$$
$$\Leftrightarrow\begin{pmatrix}x_{k+1}\\x_{k+2}\\\vdots\\x_n\end{pmatrix}=\mathbf{A}\begin{pmatrix}x_1\\x_2\\\vdots\\x_k\end{pmatrix} \quad (4)$$
$$\Leftrightarrow\begin{pmatrix}x_{k+1}\\x_{k+2}\\\vdots\\x_n\end{pmatrix}=\mathbf{A}\begin{pmatrix}u_1\\u_2\\\vdots\\u_k\end{pmatrix}$$

Dengan meletakkan Persamaan (3) di atas Persamaan (4), diperoleh
$$\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}=\left(\frac{\mathbf{I}_k}{\mathbf{A}}\right)\begin{pmatrix}u_1\\u_2\\\vdots\\u_k\end{pmatrix}$$
dan hasil transpos kedua ruasnya adalah
$$(x_1x_2\ldots x_n)=(u_1u_2\ldots u_k)(\mathbf{I}_k|\mathbf{A}^T),$$
ditulis
$$\mathbf{x}=\mathbf{uG}, \text{dengan } \mathbf{G}=(\mathbf{I}_k|\mathbf{A}^T). \quad (5)$$

Persamaan 5 menunjukkan bahwa katakode **x** merupakan kombinasi linear dari baris-baris matriks **G**. Dengan demikian, **G** adalah generator matriks dari *C*. Jika **G** mempunyai bentuk standar seperti dalam Persamaan 5, maka diperoleh
$$\mathbf{H}=(\mathbf{A}|\mathbf{I}_{n-k})$$

Dari Persamaan 1 dan 5, diperoleh hubungan **G** dan **H** dalam persamaan berikut
$$\mathbf{GH}^T=\mathbf{HG}^T=\mathbf{O}.$$

Sekarang, misalkan pesan biner $\mathbf{u}=u_1u_2\ldots u_k$, akan dikodekan menjadi katakode $\mathbf{x}=x_1x_2\ldots x_n$ yang selanjutnya dikirim melalui saluran yang diasumsikan terganggu, maka vektor yang diterima $\mathbf{y}=y_1y_2\ldots y_n$ bisa jadi berbeda dari **x**. Dari proses ini, kita definisikan *vektor galat* (*error vector*)
$$\mathbf{e}=e_1e_2\ldots e_n$$

sebagai selisih (perbedaan) antara **x** dan **y**, yaitu $\mathbf{x}=\mathbf{y}-\mathbf{e}$ atau (dalam kasus biner) $\mathbf{x}=\mathbf{y}+\mathbf{e}$.

Diasumsikan saluran yang digunakan *saluran simetrik biner* (*binary symmetric channel*) dengan probabilitas $e_i=0$ (simbol ke-*i* benar) adalah $1-p$ dengan $0\le p\le\frac{1}{2}$, maka probabilitas bahwa $e_i=1$ (simbol ke-*i* salah) adalah p. Dalam proses dekode, dekoder harus memutuskan yang mana diantara $\mathbf{x}\in C$ yang dikirim dan telah berubah menjadi **y**. Ini sama artinya jika dikatakan bahwa Dekoder harus memilih **e** sehingga $\mathbf{x}=\mathbf{y}+\mathbf{e}$. Tentu saja strategi yang harus digunakan adalah memilih **e** yang *paling mungkin*. Strategi itu dikatakan optimum jika ia mampu meminimumkan probabilitas bahwa Dekoder *salah* dalam mengambil keputusan. Mendekode dengan strategi optimum disebut *maximum likelihood decoding*.

[2] $\lfloor x\rfloor$ menotasikan bilangan bulat terbesar $\le x$.

Untuk menjelaskan lebih rinci bahaimana Dekoder bekerja diperlukan dua konsep berikut ini.

Definisi 1 ***Jarak minimum*** *dari suatu kode C didefinisikan*
$$d(C):=min\{d(\mathbf{x},\mathbf{y})/\mathbf{x},\mathbf{y}\in C,\mathbf{x}\neq\mathbf{y}\}.$$
Bobot minimum *dari suatu kode C didefinisikan*
$$wt(C):=min\{wt(\mathbf{x})/\mathbf{x}\in C,\mathbf{x}\neq\mathbf{0}\}.$$

Sifat pada proposisi berikut hanya berlaku untuk kode yang linear

Proposisi 1 *Jarak minimum dari suatu kode linear C adalah bobot minimum dari sembarang katakode taknol.*

Peranan jarak minimum suatu kode dalam proses transfer informasi dinyatakan dalam teorema berikut.

Proposisi 2 *Suatu kode C dengan panjang n, baik yang linear maupun tak-linear, dengan jarak minimum d mampu mengoreksi* $\left\lfloor\frac{d-1}{2}\right\rfloor$ *galat*[2]*. Jika d genap, C mampu mengoreksi* $\frac{d-2}{2}$ *galat dan sekaligus mendeteksi* $\frac{d}{2}$ *galat.*

III. KONSTRUKSI KODE OPTIMAL KUAT

Sejauh ini telah diperkenalkan ada tiga parameter terkait dengan konstruksi suatu kode,yaitu *panjang, dimensi,* dan *jarak minimum*. Jika *C* adalah kode linear biner yang mempunyai panjang *n*, berdimensi *k*, dan berjarak minimum *d*, maka *C* diberi nama kode $[n,k,d]$. Selanjutnya, *C* dikatakan *baik* jika *n-kecil, k-besar* dan *d-besar*.

Diberikan sembarang dua parameter, misalnya *n* dan *k*, problemnya: “Adakah suatu kode $[n,k,d]$ untuk nilai *d* yang sebesar-besarnya?”. Pertanyaan itu mengarah pada pendefinisian fungsi
$$D(n,k):=\max\{d/\text{kode }[n,k,d]\text{ ada}\}.$$

Dalam hal ini, suatu kode *C* dengan parameter $[n,k,d]$ disebut *optimal-D* (optimal jarak minimum), jika *C* ada (telah berhasil dikonstruksi) dan telah pula dibuktikan bahwa tidak ada kode dengan parameter $[n,k,d+1]$.

Batas bawah dan *batas atas* dari fungsi $D(n,k)$ diartikan sebagai berikut. Misalnya,
$$l\le D(n,k)\le u,$$
artinya telah berhasil dikonstruksi kode dengan parameter $[n,k,d\le l]$ dan telah berhasil pula dibuktikan bahwa tidak ada kode dengan parameter $[n,k,d>u]$, sedangkan ada/tidaknya kode dengan parameter $[n,k,d]$, dengan $l<d\le u$, merupakan *problem terbuka*. Untuk memperbaiki satu langkah batas bawah dari fungsi

$D(n,k)$ berarti kita harus mampu mengkonstruksi kode dengan parameter $[n,k,l+1]$. Perbaikan satu langkah batas atas dari fungsi $D(n,k)$ berarti kita harus mampu membuktikan bahwa tidak ada kode dengan parameter $[n,k,u]$. Informasi terkini (updated) basis data untuk batas fungsi $D(n,k)$ dapat dilihat di dalam Tabel Brouwer [2] dan bisa diakses secara on-line. Jika kita telah berhasil memperbaiki satu saja batas (bawah atau atas) dari Tabel Brouwer, berarti kita telah "memecahkan satu rekor dunia".

Secara analog, kita bisa mendefinisikan fungsi $K(n,d)$ untuk *optimalisasi dimensi* (optimal-K) atau fungsi $N(k,d)$ untuk *optimalisasi panjang kode* (optimal-N) dan sekaligus memformulasikan problemnya:

$$K(n,d) \coloneqq \max\{k/\text{kode } [n,k,d] \text{ ada}\}$$
$$N(k,d) \coloneqq \min\{n/\text{kode } [n,k,d] \text{ ada}\}$$

Berdasarkan formulasi umum problem di atas, kita definisikan *kode optimal kuat* (strongly optimal codes) beserta formulasi problem konstruksinya berlandaskan teorema berikut ini.

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

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

maka ada (*dapat dikonstruksi*) *kode dengan parameter* $[n+1,k+1,d]$.

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 sifat-sifat dasar kode linear, bisa ditunjukkan bahwa jika *C* optimal kuat, maka *C* pasti optimal-D, optimal-K, dan optimal-N. Hal ini tidak berlaku sebaliknya.

Kajian tentang teorema Gilbert-Varshamov bound cukup menarik. Bentuk umum perbaikan teorema tersebut terakhir dilakukan oleh A. Barg dkk. [1]. Namun penerapan per kasus kode (kode dengan nilai parameter tertentu) baik yang batas atas maupun batas bawah masih banyak problem yang belum terpecahkan.

Telah disinggung sebelumya bahwa mengkonstruksi suatu kode berarti mendefinisikan matriks cek paritas **H** atau matriks generatornya **G**. Selain teorema Gilbert-Varshamov bound, berikut ini diberikan beberapa teorema yang paling berperan untuk melandasi konstruksi **H**.

Teorema 2 *[5]Jika **H** adalah matriks cek paritas dari suatu kode dengan panjang n, maka kode tersebut mempunyai dimensi* $(n-r)$ *jika dan hanya jika ada r kolom dari **H** yang bebas linear tetapi tidak ada* $(r+1)$ *kolom dari **H** yang bebas linear* (*artinya r adalah rank dari **H***).

Teorema 3 *[5]Jika **H** adalah matriks cek paritas dari suatu kode dengan panjang n, maka kode tersebut mempunyai jarak minimum d jika dan hanya jika ada d kolom dari **H** yang tidak bebas linear dan setiap* $d-1$ *kolom dari **H** yang bebas linear.*

Teorema 4 (*The Singleton bound*) *[5]Jika C adalah kode dengan parameter* $[n,k,d]$, *maka* $(n-k)\geq(d-1)$.

Sebelum kita turunkan teorema yang melandasi konstruksi kode optimal kuat, ada baiknya berikut ini dibahas terlebih dahulu bukti teorema Gilbert-Varshamov.

Bukti. (Teorema Gilbert-Varshamov)

Misalkan diketahui kode *C* memiliki parameter $[n,k,d]$. Berdasarkan Teorema 3 ada matriks paritas **H** berordo $(n-k)\times n$ ditulis

$$\mathbf{H}=(\mathbf{c}_1\ \mathbf{c}_2\ \ldots\ \mathbf{c}_n)$$

yang setiap $d-1$ vektor dari $\{\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n\}$ adalah bebas linear dalam ruang $\mathbb{F}_2^{n-k}$. Ide dasar pembuktian adalah jika ada vekto $\mathbf{x}\in\mathbb{F}_2^{n-k}$r yang bukan *i* kombinasi linear dari vektor-vektor kolom **H** untuk $i=1,2,\ldots,d-2$, maka

$$\mathbf{H}'=(\mathbf{c}_1\ \mathbf{c}_2\ \ldots\ \mathbf{c}_n\ \mathbf{x})$$

adalah matriks berordo $(n-k)\times(n+1)$ yang setiap $d-1$ vektor dari himpunan $\{\mathbf{c}_1,\mathbf{c}_2,\ldots,\mathbf{c}_n,\mathbf{x}\}$ adalah bebas linear dalam ruang $\mathbb{F}_2^{n-k}$. Dalam hal ini **H**' merupakan matriks paritas untuk kode $[n+1,k+1,d]$. Syarat adanya vektor $\mathbf{x}\in\mathbb{F}_2^{n-k}$ terjadi ketika dipenuhi ketaksamaan

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

dengan ruas kiri menyatakan banyaknya vektor-vektor sebagai hasil *i* kombinasi linear dari vektor-vektor kolom **H** untuk $i=1,2,\ldots,d-2$, sedangkan ruas kanan menyatakan banyaknya vektor-vektor tak-nol dalam $\mathbb{F}_2^{n-k}$. □

Selnutnya teorema utama yang akan digunakan untuk konstruksi suatu kode dinyatakan berikut ini sebagai varian dari teorema Gilbert-Varshamov.

Teorema 5 *Jika matriks **B** berukuran* $k\times r$ *dikonstruksi berdasarkan sifat bahwa:*

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

$$\mathbf{H}=(\mathbf{B}^T|\mathbf{I}_r)$$

Merupakan matriks paritas untuk kode C dengan parameter $[k+r,k,\geq d]$. *Dalam hal ini matriks generator dari C adalah*

$$\mathbf{G}=(\mathbf{I}_k|\mathbf{B})$$

Bukti. Misalkan telah dikonstruksi matriks **B** berukuran $k \times r$ sebagaimana disyaratkan oleh teorema, akan ditunjukkan bahwa **H** merupakan matriks paritas untuk kode $C - [k + r, k, \geq d]$. Hal pertama yang mudah dilihat dari struktur **H** adalah C mempunyai panjang $(k + r)$ dan berdimensi k, sehingga tinggal ditunjukkan C memiliki jarak minimum $\geq d$.

Andaikan ada $\mathbf{v} \in C$ dengan $wt(\mathbf{v}) < d$ dan dituliskan $\mathbf{v} = (\mathbf{v}_m, \mathbf{v}_c)$ dengan $\mathbf{v}_m$ *vektor pesan* dengan $wt(\mathbf{v}_m) = i$ dan $\mathbf{v}_c$ *vektor cek* dengan $\boldsymbol{wt}(\mathbf{v}_c) = j$, maka berlaku

$$i + j < d \Leftrightarrow j < d - i \Rightarrow wt(\mathbf{v}_c) < d - i \qquad \text{(i)}$$

dan

$$\begin{aligned} &\mathbf{H}\mathbf{v}^T = \mathbf{0}^T \\ &\Leftrightarrow (\mathbf{B}^T|\mathbf{I}_r)\begin{pmatrix}\mathbf{v}_m^T \\ \mathbf{v}_c^T\end{pmatrix} = \mathbf{0}^T \\ &\Leftrightarrow \mathbf{B}^T\mathbf{v}_m^T + \mathbf{I}_r\mathbf{v}_c^T = \mathbf{0}^T \\ &\Leftrightarrow \mathbf{B}^T\mathbf{v}_m^T = \mathbf{v}_c^T \end{aligned} \qquad \text{(ii)}$$

Karena $wt(\mathbf{v}_m) = i$, dan berdasarkan Syarat 2 dari konstruksi **B**, maka

$$\mathrm{wt}(\mathbf{B}^T\mathbf{v}_m^T) \geq d - i \qquad \text{(iii)}$$

Perhatikan bahwa Ekspresi i, ii dan iii menunjukkan suatu kontradiksi sehingga dapat disimpulkan bahwa C berbobot minimum $\geq d$, atau dengan kata lain C memiliki jarak minimum $\geq d$. □

Berdasarkan Teorema 5, untuk mengkonstruksi kode $C - [k + r, k, d]$ berarti cukup mengkonstruksi matriks **B** berukuran $k \times r$ yang memenuhi sifat-sifat:

1. Semua vektor baris dari **B** berbeda, dan
2. Jumlah setiap i vektor baris dari **B** berbobot paling sedikit $(d - i)$ untuk $i = 1,2,3, \dots, s$ dengan $s = \min\{d - 1, k\}$ dan $(d - 1) \leq r$.

Dalam penelitian ini, kedua syarat konstruksi matriks **B** tersebut telah diwujudkan dalam algoritme-algoritme dan telah diprogram atas bantuan perangkat lunak MAPLE (terlalu panjang untuk dicantumkan dalam artikel ini). Kemudian, kita padukan hal tersebut dengan Teorema Gilbert-Varshamov untuk mendefinisikan langkah-langkah komputasi kode optimal kuat sebagaimana dideskripsikan berikut ini:

1. Ditetapkan suatu nilai n dan d, kemudian dikonstruksi *kode dasar* $[n, k, d]$ dengan sifat nilai k cukup kecil, konstruksinya cukup mudah dan Optimal-D.
2. Begitu kode $[n, k, d]$ telah terkonstruksi, langkah berikutnya adalah mendefinisikan himpunan V yang beranggotakan semua vektor baris dari **B** dan semua vektor sebagai hasil jumlah i vektor baris dari **B** untuk $i = 2,3, \dots, s$ dengan $s = \min\{d - 1, k\}$. Maka jelas bahwa $V \subseteq \mathbb{F}_2^r$. Jika $V \neq \mathbb{F}_2^r$, maka ada vektor $\mathbf{x} \in \mathbb{F}_2^r$ dan $\mathbf{x} \notin V$ yang bisa ditambahkan ke baris matriks **B** untuk mendefinisikan matriks **B'** berukuran $(k + 1) \times r$ dan matriks cek paritas
$$\mathbf{H}' = ((\mathbf{B}')^T|\mathbf{I}_r)$$
akan mendefinisikan kode dengan parameter $[n + 1, k + 1, d]$.
3. 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 mengkonstruksi 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.

Penerapan komputatif dari prosedur di atas untuk kasus $d = 5$ diberikan berikut ini.

Ilustrasi 1 *Berdasarkan tabel Brower, untuk kasus* ***double error correcting*** $(d = 5)$ *, kode-kode optimal kuat mempunyai parameter* (*terurut dari dimensi terendah*)*:* $[8,2,5], [11,4,5], [17,9,5]$ *dan* $[23,14,5]$. *Sedangkan kode optimal kuat untuk* $k > 14$ *masih* ***problem terbuka*** *dengan batas bawah* $k = 23$ (*berarti kode Optimal-D dengan parameter* $[33,23,5]$ *telah berhasil dikonstruksi*)*. Akan dijelaskan bahaimana metode dan strategi di atas diterapkan untuk mengkonstruksi kode-kode tersebut. Dimulai dari kode* $[8,2,5]$, *kode dengan parameter ini sangat mudah dikonstruksi, yaitu dengan mendefinisikan matriks* ***B*** *berukuran* 2×6 *berikut*

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

Matriks ini kemudian dipakai sebagai matriks dasar untuk diperluas menjadi matriks ***B'*** *berordo* 4×7 *yang mendefinisikan kode optimal kuat* $[11,4,5]$. *Proses perluasan dari* ***B*** *ke* ***B'*** *dilakukan dengan menambah satu kolom nol pada* ***B****, dilanjutkan menambah dua vektor 7 bit yang memenuhi syarat strategi. Tanpa memerhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukkan ada 108 macam* ***B'****, salah satunya*

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

Dengan langkah analog, $\boldsymbol{B'}$ *bisa diperluas ke* $\boldsymbol{B''}$ *berordo* 9×8 *yang mendefinisikan kode optimal kuat* $[17,9,5]$ *. Tanpa memerhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukkan ada 132 macam* $\boldsymbol{B''}$*, salah satunya*

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

Percobaan untuk memperluas $\boldsymbol{B''}$ *ke* $\boldsymbol{B'''}$ *untuk mendapatkan kode optimal kuat* $[23,14,5]$ *adalah* ***gagal****. Dalam hal ini* $\boldsymbol{B''}$ *hanya mampu diperluas ke lebih dari 1000 kode Optimal-D* $[22,13,5]$*. Namun demikian, strategi rekonstruksi berhasil mendefinisikan sedikitnya satu kode optimal kuat* $[23,14,5]$ *yang direpresentasikan oleh matriks* $\boldsymbol{B'''}$ *berordo* 14×9 *berikut*

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

Selanjutnya, usaha untuk memperluas $\boldsymbol{B'''}$ *berhasil sampai diperoleh matriks* $\boldsymbol{B}^{iv}$ *berordo* 23×10

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

yang mendefinisikan kode $C - \{33,23,5]$*. Nilai parameter dari C ini menyamai dengan nilai parameter terbaik dari kode yang ada di Tabel Brouwer yang dikonstruksi dengan metode yang lain. Di samping itu, kode ini juga* ***belum*** *bisa disebut optimal kuat karena eksistensi dari kode* $[34,24,5]$ *masih* ***problem terbuka****.*

Penerapan metode konstruksi kode optimal kuat yang telah disampaikan dalam artikel ini (serupa dengan Ilustrasi 1) juga memberikan hasil yang baik ketika diujicobakan untuk kasus $d = 7, d = 9, d = 11, d = 13$ dan $d = 15$. Walaupun tidak sampai pada pemecahan problem terbuka (rekor dunia), namun hasil konstruksi telah menyamai hasil yang ada di Tabel Brouwer, kecuali untuk $d = 9$ setingkat di bawah hasil Tabel Brouwer.

Catatan: *Eksplorasi hanya dilakukan untuk nilai d ganjil, karena eksistensi kode* $[n, k, d]$ *berjarak minimum ganjil dengan teknik puncturing (lihat [2]) akan mengakibatkan eksistensi kode* $[n - 1, k, d - 1]$ *berjarak minimum genap.*

IV. SIMPULAN DAN SARAN

- Dalam artikel ini telah dikembangkan suatu metode komputatif untuk menkonstruksi kode optimal kuat sebagai varian dari metode konstruksi kode Gilbert-Varshamov.
- Penerapan metode yang bersangkutan hanya diberlakukan untuk nilai d $\leqslant$ 15 dan memberikan hasil yang cukup baik, sedangkan untuk d > 15 bisa dilakukan tetapi terbatas pada sumberdaya komputasi terkait dengan kompleksitas algoritmenya. Untuk itu perlu

dikembangkan algoritme yang lebih baik yang berlandaskan pada Teorema 5.

- Pemilihan kode dasar sangat menentukan keberhasilan untuk diperluas menjadi kode optimal kuat. Dengan demikian, perlu adanya kajian baik yang bersifat teoretik maupun komputatif untuk menetapkan kriteria pemilihan kode dasar.

DAFTAR PUSTAKA

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

[2] Brouwer, A.E. "Bounds on the ize of linear codes", Handbook of Coding theory, ed.: V.Pless and W.C.Huffman. Elsevier, 1998. ISBN: 0-444-50088-X. Available at: http://www.win.tue.nl/math/dw/voorlincod.html

[3] Bouyukliev, I. Guritman, S. dan Vavrek, V. "Some bounds for the minimum length of binary linear codes of dimension nine", IEEE Trans. Inform. Theory, vol. 46, no. 3, pp. 1053-1056, May 2000.

[4] Hashim, A.A. "Improvement on Varshamov-Gilbert lower bound on minimum Hamming distance of linear codes", Proc. Inst. Elec. Engrs., 125, pp. 104-106, 1978.

[5] MacWilliams, F.J. dan Sloane, N.J.A. "The theory of error-correcting codes", 2nd reprint, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam – New York – Oxford, 1983, xx+762 pp. ISBN: 0-444-85009-0 and 0-444-85010-4.