

# 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 perbaikan 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

	Halaman
<b>Judul</b>	i
<b>Editor</b>	ii
<b>Tim Penilai Makalah (Reviewer)</b>	iii
<b>Kata Pengantar</b>	iv
<b>Daftar Isi</b>	v
<b>Minimisasi Norm Daerah Hasil (Range Norm) Himpunan Bayangan (Image Set) Matriks Atas Aljabar Max-Plus Interval</b>	1 - 6
Siswanto, Ari Suparwanto, M. Andy Rudhito	
<b>Seputar Modul Komultiplikasi</b>	7 - 11
Laila Dini Anggraini, Indah Emilia Wijayanti	
<b>Graph Cantik</b>	12 - 20
Imam Rofiki	
<b>Graf Model Lalu-Lintas Kendaraan Di Persimpangan Jalan Bersinyal Dengan Palang Pintu Kereta Api</b>	21 - 27
Tomi Tristono	
<b>Konstruksi Kode Varshmov Biner Berjarak Minimum Rendah</b>	28 - 34
Sugi Guritman, Nur Aliatiningtyas, Teduh Wulandari, Muhammad Ilyas	
<b>Invers Matriks Laplace yang Digeneralisasi</b>	35 - 38
Irwan Susanto	
<b>Teorema Pemetaan Kontraktif Pada <math>L^p([0, \infty))</math> Sebagai Ruang Norm -2</b>	39 - 41
Shelvi Ekariani, Hendra Gunawan	
<b>Kekompakan Dan Keterhubungan Dengan Menggunakan Gauge Pada Ruang Topologi</b>	42 - 46
Dewi Kartika Sari, Ch. Rini Indrati	
<b>Dual KÖTHE-TOEPLITZ Pada Ruang Barisan Dengan Elemen Barisan Generalisasi Barisan P-Absolutely Summable Dan Barisan Terbatas</b>	47 - 55
Sumardyono, Soeparna D.W., Supama	
<b>Mollifier Pada Ruang Bernorma <math>\mathbb{R}^n</math></b>	56 - 59
Dwi Nur Yunianti	

	Halaman
<b>Primitif Fungsi Terintegral <math>M_{\text{ALPHA}}</math> Pada Ruang Berdimensi – n Bersifat <math>ACG_{\text{ALPHA}}</math></b> Muslich	60 - 64
<b>Teorema Representasi Riesz Pada Ruang Barisan Yang Dibangkitkan Oleh Fungsi Orlicz Yang Diperluas</b> Nur Khusnussa'adah, Supama	65 - 70
<b>Kriteria Cauchy Dari Suatu Fungsi Bernilai Vektor Pada Suatu Sel Di Dalam Ruang Metrik Kompak Lokal</b> Manuharawati dan Dwi Nur Yuniarti	71 - 75
<b>Bifurkasi <i>Hopf</i> Dan <i>Heteroclinic</i> Pada Model Mangsa-Pemangsa Holling-Tanner Tipe II</b> Ali Kusnanto, M. Buchari Gaib, Paian Sianturi	76 - 80
<b>Analisis dan Kontrol Optimal Model Dinamik Virus Hepatitis B (VHB) dengan Pertumbuhan Logistik Sel Hepatosit</b> Fatmawati, Adise Putra Indanto, Yayuk Wahyuni	81 - 85
<b>Teknik Pemisahan Sinyal Suara menggunakan Deteksi Puncak pada <i>Scattering Plot</i></b> Irwansyah, Dhany Arifianto, Aulia Siti Aisjah	86 - 92
<b>Aplikasi Skema Central Upwind Semidiskrit Order Kedua Pada Persamaan Saint Venant Dimensi-Satu dengan Lebar dan Dasar Saluran Tidak Konstan</b> Noor Hidayat, Suhariningsih, Agus Suryanto	93 - 99
<b>Model Matematika Penyebaran HIV/AIDS dalam Tubuh Manusia dengan Faktor Respon Imun</b> Maulida Syarifah, Fatmawati, Yayuk Wahyuni	100 - 107
<b>Generalisasi Barisan Transisi Pada Kode Gray Biner Menjadi Barisan Transisi Blok</b> Wahidah	108 - 115
<b>Model Matematika Pertumbuhan dan Pemanenan Rumput Gajah Sebagai Pakan Ternak</b> Windarto, Dini Wulandari, Mahfudhotin	116 - 120
<b>Normalized Differentiation Water Index (NDWI) Spot Untuk Delineasi Tubuh Air</b> Wiweka	121 - 125
<b>Kestabilan model SIR-SI host-vector transmisi demam berdarah dengue</b> Jafaruddin, S. W. Indratno, Nuning Nuraini, Asep K Supriatna, E. Soewono	126 - 131

	Halaman
<b>Model Estimasi Angka Produktivitas Penuntasan Wajib Belajar Pendidikan Sekolah Dasar Berbasis pada Masyarakat Kelompok Miskin: <i>Studi Kasus di Kabupaten Donggala Sulawesi Tengah</i></b>	132 - 138
Nursalam, Suwari, Jafaruddin, Ariyanto, Heru Suwardi, Jakobis Johanis M	
<b>Peningkatan Unjuk Kerja Pemisahan Bunyi Campuran Melalui Perubahan Konfigurasi Sensor Array Secara Spasial</b>	139 - 143
Muh. Syaifuddin Zuhdi, Dhany Arifianto	
<b>Jaringan Syaraf Tiruan dengan Pembelajaran Algoritma Genetika dan Diversitas untuk Deteksi Kelas Penyakit</b>	144 - 148
Abidatul Izzah, Ratih Kartika Dewi	
<b>Penentuan Harga Opsi Asia Dengan Model Binomial Dipercepat</b>	149 - 156
Surya Amami Pramuditya, Kuntjoro Adji Sidarto	
<b>Penjadwalan Mata Kuliah Sistem Mayor-Minor Di Perguruan Tinggi</b>	157 - 162
Nur Apriandini, Farida Hanum, Amril Aman, Toni Bakhtiar	
<b>Model Pengoptimuman <i>Dispatching</i> Bus Pada Transportasi Perkotaan</b>	163 - 170
Nurisma, Amril Aman, Farida Hanum	
<b>Penerapan Back Propagation Neural Network dan Linier Programming Dalam Perencanaan Pola Tanam-tanaman Pangan di kabupaten Lombok Tengah</b>	171 - 178
Syaharuddin, M. Isa irawan, Habibi RPN, Ripai	
<b>Pemodelan Temporally Weighted Regression Pada Hubungan Angka Insiden DBD Dan Unsur Iklim Di Surabaya</b>	179 - 182
Baharuddin, Brodjol Sutjjo Suprih Ulama, Suhariningsih	
<b>Penggunaan Metode <i>Value at Risk</i> Untuk Menentukan Tingkat Resiko Investasi Melalui Pendekatan Model <i>Financial Series</i></b>	183 - 188
Sediono	
<b>Pendugaan Curah Hujan, Kelembaban, Dan Suhu Di Surabaya Berdasarkan Metode <i>Ordinary Kriging</i></b>	189 - 194
Toha Saifudin, Elly Ana, Nur Chamidah, Beta Ghobia Khalmah	
<b>Studi Pengembangan Bandara Internasional Ngurah Rai Berdasarkan Prediksi Jumlah Penumpang Pesawat Dalam Rangka Mendukung Potensi Pariwisata Di Bali</b>	195 - 200
Kadek Ary W, Vinny Marlinda H, Renanthera Puspita N, Irmanita Azalia, Heri Kuswanto	

	Halaman
<b>Pembesaran Citra Wajah berbasis Fungsi Polinomial Menggunakan Metode <i>Least Square Error(LSE)</i></b>	201 - 205
Qurin Ainun, Cahyo Crysdiان	
<b>Pemetaan Pencemaran Air Sungai di Surabaya Berdasarkan Indikator Pencemaran Air Secara Kimia (<i>Chemical Oxygen Demand</i>) Sebagai <i>Early Warning System</i> dengan Metode <i>Mixed Geographically Weighted Regression</i></b>	206 - 213
Rosna Malika, Umi Anifah, Dewi Arfianty ‘azmi, Tahira Eta Adisti, Sutikno	
<b>Laju Kekonvergenan Penduga Fungsi Nilai Harapan Pada Proses Poisson Periodek Majemuk</b>	214 - 221
Ruhayat, I Wayan Mangku, I Gusti Putu Purnaba	
<b>Estimasi Konsentrasi Gas Polutan Karbon Monoksida (CO) Dan Nitrogen Dioksida (NO<sub>2</sub>) Di Surabaya Menggunakan Metode Cokriging</b>	222 - 228
Dian Safrina Putri, Silvia Roshita Dewi, Lauda Septiana, Idayati	
<b>Algoritma Expectation-Maximization (EM) untuk Estimasi Distribusi <i>Mixture</i></b>	229 - 233
Tomy Angga Kusuma, Suparman	
<b>Pemodelan Tingkat Kerawanan Penyakit Demam Berdarah Dengue Di Surabaya Dengan Pendekatan <i>Geographically Weighted Logistic Regression</i></b>	234 - 240
Nur Chamidah, Toha Saifudin, Marisa Rifada, Fitriah Anugrah Gunita	
<b>Perbandingan Kinerja Penduga Robust MVE dan MCD dalam Analisis Diskriminan Kuadratik lebih dari Dua Kelompok</b>	241 - 245
Toha Saifudin	
<b>Peningkatan Hasil Belajar Matematika melalui Strategi Pembelajaran Holobis Kuntul Baris Berjalan Terbalik Dikemas dalam CD Pembelajaran pada Materi Fungsi Invers Kelas XI IPA SMA Negeri 1 Jatibarang.</b>	246 - 251
Nur Rokhman	
<b>Penerapan Algoritma <i>Ant Colony Optimization (Aco)</i> Pada Penjadwalan <i>Vehicle Routing Problem (Vrp)</i> Dengan Batasan Sumber Daya Dan Jarak Tempuh Di Balai Riset Dan Standardisasi Industri Surabaya Penerapan Algoritma <i>Ant Colony Optimization (Aco)</i> Pada Penjadwalan <i>Vehicle</i></b>	252 - 258
Mahfudhotin, Ratnaning Palupi, Vida Nourma Chakim, Hernanda Lasmana <sup>4</sup> , Annisa Ayu Utami, Herry Suprajitno	
<b>Membangun Fungsi Multivariabel Untuk Studi Parameter Fisik Pada Permasalahan Lendutan Balok Beton Cantilever</b>	259 - 263
Wahyo Hendarto Yoh.	

	Halaman
<b>Optimalisasi Penggunaan Teknologi Informasi Sekolah ( <i>Software</i> KWIKTRIG 3.0.5, CAMTASIA Recorder 8.0 Dan Facebook) Dalam Pembelajaran Trigonometri Siswa SMA</b> Hilda Nurul Hikmah	264 - 269
<b>Pengembangan Instrumen Penelitian Pembelajaran Kalkulus Diferensial Berbasis Pendekatan <i>Open Ended</i> Untuk Meningkatkan Kemampuan Representasi Matematis Mahasiswa STKIP PGRI Pontianak</b> Ichsan	270 - 273
<b>Purwarupa Sistem Administrasi Akademik Untuk Perguruan Tinggi Dengan Model Pembelajaran Jarak Jauh</b> Soetam Rizky Wicaksono, Tri Mariono	274 - 278
<b>Pembelajaran Matematika Saat Ini?</b> Jackson Pasini Mairing	279 - 286
<b>Menumbuhkan Kreativitas Dan Kemampuan Berfikir Tingkat Siswa Melalui Pengembangan Konjektur Matematika</b> I Wayan Puja Astawa	287 – 293
<b>Pengetahuan Konten Pedagogik (<i>Pedagogical Content Knowledge</i>) Pembeda Profesi Guru Dari Yang Lain (Kasus Guru Matematika)</b> Usman HB.	294 – 299
<b>Profil Pemecahan Masalah Geometri Siswa Kelas Akselerasi SMP Ditinjau Dari Tingkat Kemampuan Matematika</b> Imam Rofiki	300 - 312
<b>Meningkatkan <i>Self-Regulated Learning</i> Melalui Pendekatan <i>Problem-Centered Learning</i> Dengan <i>Hands-On-Activity</i> Pada Siswa Kelas VIII SMP Negeri 3 Cipaku Tahun Pelajaran 2011/2012</b> Lala Nailah Zamnah	313 - 319
<b>Profil Berpikir Siswa Sekolah Dasar Yang Menggunakan Numeralia Bahasa Biak Dalam Menyelesaikan Soal Operasi Hitung</b> Mayor M.H. Manurung	320 - 325
<b>Strategi Brain Based Learning Dalam Pembelajaran Matematika Untuk Mengembangkan Kemampuan Berfikir Kritis Dan Kreatif Siswa</b> Ginanjar Abdurrahman, Mukti Sintawati	326 - 330

	Halaman
<b>Rancang Bangun E-Learning untuk Pembelajaran Aritmatika dalam Bahasa Mandarin bagi Siswa Sekolah Dasar Berbasis Web</b> Yulius Hari, Darmanto, Budi Hermawan	331 - 336
<b>Konkrit Perkalian Dan Pembagian Dalam Matematika Gasing</b> Ali Godjali, Josephine Kusuma	337 - 345
<b>Analisis Pekerjaan Siswa Pada Topik Segiempat Berdasarkan Teori <i>Van Hiele</i></b> Bettisari Napitupulu	346 - 353
<b>What Wrong With Math ?</b> Bernaridho Imanuel Hutabarat , Roni F. Sinaga	354 - 357
<b>Abstraksi Konsep Pembagian Pecahan Dengan Topangan</b> Firman Pangaribuan	358 - 363
<b>Studi Analisa Pembelajaran Matematika Melalui Game Pada Anak Usia SD</b> Arik Kurniawati	364 - 368
<b>Imputasi <i>Missing Data</i> Menggunakan Algoritma Pengelompokan Data <i>K-Harmonic Means</i></b> Abidatul Izzah, Nur Hayatin	369 - 373
<b>Analisis dan Perancangan Sistem Informasi Berbasis Web Sebagai Media Promosi dan Informasi Kain Tenun Daerah Flores</b> Gregorius Rinduh Iriane	374 - 378
<b>Analisa Dan Perancangan Aplikasi Augmented Reality Pada Lokasi Pariwisata Flores Berbasis Android</b> Benediktus Y. Bhae, Devi Indriasari, Pranowo	379 - 386
<b>Prototipe Katalog Metadata Informasi Spasial Penginderaan Jauh Berstandar ISO 19115 Menggunakan Software Open Source Geonetwork</b> Samsul Arifin	387 - 391
<b>Pengembangan Aplikasi Penyusuluhan Pertanian Tanaman Hortikutura Berbasis SMS Gateway Pada Dinas Pertanian Dan Perkebunan Provinsi Nusa Tenggara Timur</b> Emerensiana Ngaga, Suyoto, Eddy Julianto	392 - 398
<b>Memprioritaskan Kebutuhan Perangkat Lunak Menggunakan Model Kano Dengan Menampilkan Rancangan Antarmuka Perangkat Lunak</b> Indra Kharisma Raharjana	399 - 405

	Halaman
<b>Rancangan Framework Business Intelligent pada Perguruan Tinggi</b> Henderi , Edi Winarko	406 - 410
<b>Analisis Dan Perancangan Sistem Pendukung Keputusan Penilaian Gabungan Kelompok Tani Berbasis Web</b> Ernawati, Yudi Dwiandiyanta, Patrisius Batarius	411 - 417
<b>Konsep Pemampatan Intra-Frame Urutan Citra Gerak Tari Hegong Menggunakan Alihragam Gelombng Singkat</b> Febriyanti Alwisye Wara, Alb. Joko Santoso, B. Yudi Dwiandiyanta	418 - 423
<b>Simulasi Sistem Antrian Pembuatan Surat Ijin Mengemudi (SIM) Di Satpas Polres Jember</b> Fitria Lusianik, Mahendrawathi ER	424 - 429
<b>Sistem Informasi Manajemen Bea siswa (SIMABEA) Berbasis Sistem Pendukung Keputusan dengan Menggunakan Metode Analytic Hierarchy Process (AHP) dan ELECTRE</b> Haryanto, Firli Irhamni, Bain Khusnul Khotimah	430 - 434
<b>Implementasi Sistem Pendukung Keputusan Dengan Metode Fuzzy Dalam Menentukan Lahan Potensi Tanaman Pangan Di Propinsi Jawa Timur</b> Hario Laskito Ardi, Kartono, Purbandini	435 - 441
<b>Aplikasi Sistem Pendeteksi Diabetes Menggunakan Multilayer Dengan Pelatihan Feedward Neural Network</b> Nur Maulidyah, Bilqies Kimmilah, Friday Yosi Prilnambilanti, Fadillah, Shitta Dewi Puspitasari, Aina Nur Af'ida, Melinda Weridianti Yusuf	442 - 445
<b>Rancang Bangun Sistem Pakar Fuzzy Untuk Diagnosa Demam Berdarah</b> Indah Werdiningsih, Badrus Zaman	446 - 451
<b>Rancang Bangun Sistem Informasi Geografis (SIG) Berbasis Web Untuk Memantau Kualitas SLTP Di Kabupaten Gresik</b> M. Ainul Yaqin, Muhammad Bisri Musthafa	452 - 457
<b>Visualisasi 3D Rupa Bumi Berbasis Data GDEM Aster 30 Meter</b> Mochamad Agung Tarecha, Cahyo Crysdian	458 - 465
<b>Analisis Dan perancangan Sistem Untuk mendukung Pengambilan Keputusan Pemberian Beasiswa Di Universitas Katolik Widya Mandiri Kupang</b> Sisilia Daeng Bakka Mau, Ernawati, Pranowo	466 - 472

	Halaman
<b>Data Mining Dengan Metode Soft Clustering Untuk Menganalisa Karakteristik Pelanggan PDAM Kota Surabaya</b> Taufik	473 - 478
<b>Ekstraksi Ciri Sinyal Electromyograph Statik Pada Ekstensi-Fleksi Telapak Tangan</b> Triana Rahmawati, Indah Soesanti, Bondhan Winduratna	479 - 484
<b>Optimalisasi Cluster Data Dengan Menggunakan K-Means Clustering Berbobot</b> Bain Khusnul Khotimah	485 - 490
<b>Segmentasi Citra Biomedis Menggunakan Metode Level Set Local Image Fitting</b> Lianita Febrihani, Pranowo, B. Yudi Dwiandiyanta	491 - 495
<b>Penggunaan Algoritma Decision Tree Untuk Mendeteksi Penyakit Diabetes</b> Aditya Prakoso, M.A Danang, Rinaldhi Cahyono, Lukman Hakim, Aditya Suharjono, Rizqy Galan Pradipta	496 - 498
<b>Diagnosis Penyakit Demam Berdarah Melalui metode Feedward Neural Network</b> Faisal A, A Choliq F, Aldinovi Tito P, Hendra Dwi, Andrianto GP, Ahmadi Soffi S	499 - 502
<b>Diagnosa Penyakit Avian Influenza Pada Ayam Menggunakan Metode Feedforward</b> K. Wanda P, Delia Putri F, Kiki M W , Dika P H , Nur Hesti P , Masteria W	503 - 507
<b>Analisa Metode Fuzzy Untuk Diagnosa Penyakit Mata (Studi Kasus Rumah Sakit DR.T.C. Hillers Maumere)</b> Imelda Dua Reja, Alb. Joko Santoso, Ernawati	508 - 512
<b>Pengenalan Kain Sumba Menggunakan Jaringan Syaraf Tiruan Backpropagation</b> Yustina Rada, Albert Joko Santoso, Patricia Ardanasari	513 - 516
<b>Sistem Rekomendasi Pembelajaran Menggunakan Teknik Collaborative Filtering</b> Andharini Dwi Cahyani	517 - 520
<b>Penggunaan Korelasi Polikhorik dan Pearson untuk Variabel Ordinal dalam Model Persamaan Struktural</b> Anita Kesumahati, Zainal Abidin	521 - 525
<b>Rancang Bangun Sistem Pendukung Keputusan Optimasi Alokasi Pasokan Untuk Rantai Pasok Cabai Merah Besar Dengan Metode Fuzzy Multiobjective Optimization Linear Programming (Studi Kasus Koperasi Tani Made Makmur Surabaya)</b> Ayuningtyas Puspa Karina, Eto Wuryanto, Purbandini	526 - 533
<b>Interval Kepercayaan Rata-rata Respon Model Linier Campuran Berdasarkan Estimator Best Linear Unbiased Prediction</b> Suliyanto	534 - 536

# KONSTRUKSI KODE VARSHAMOV BINER BERJARAK MINIMUM RENDAH

Sugi Guritman<sup>1)</sup>, Nur Aliatiningtyas<sup>2)</sup>, Teduh Wulandari<sup>3)</sup>, Muhammad Ilyas<sup>4)</sup>

<sup>1)2)3)4)</sup>Laboratorium Matematika Murni  
Departemen Matematika  
Fakultas Matematika dan Ilmu Pengetahuan Alam  
Institut Pertanian Bogor  
<sup>1)</sup>guritman@yahoo.co.id  
<sup>2)</sup>nur.aliatiningtyas@gmail.com  
<sup>3)</sup>teduhw@gmail.com  
<sup>4)</sup>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 tetapi terbatas pada sumberdaya komputasi terkait dengan kompleksitas algoritmenya.

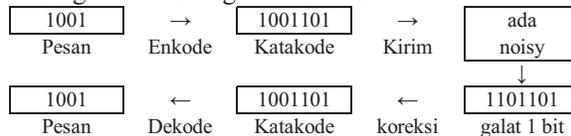
**Keywords**— Kode Linear Biner, Optimal Kuat, Gilbert-Varshamov Bounds, Konstruksi Kode.

## 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<sup>1)</sup>. Di dalam komunikasi, pesan direpresentasikan dalam bentuk dijital 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 (encoding)*. 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.



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 dijital dari  $\mathbf{x}$  dan  $\mathbf{y}$  dimana simbol mereka berbeda, jelas bahwa  $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} + \mathbf{y})$ .

<sup>1)</sup>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  $\mathbf{x}$  dikirim dan berubah menjadi  $\mathbf{y}$  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 persamaan linear. Simbol cek didefinisikan dengan tujuan untuk melindungi pesan dari galat.

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

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

dengan “ $\cdot$ ” 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  $\mathbf{H}$  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  $\ker(\mathbf{H})$ . 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 encode. Encode kode linear dengan matriks paritas  $\mathbf{H}$  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  $\mathbf{H}$  yang telah didefinisikan sebelumnya. Maka, pertama kali didefinisikan

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

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

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

Demi kemudahan penyelesaian, matriks  $\mathbf{H}$  biasanya diberikan dalam bentuk *standar*, yaitu

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

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

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

$$C := \text{Span}(\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k\})$$

dimana  $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k\}$  adalah himpunan semua baris dari  $\mathbf{G}$ . Hubungan antara  $\mathbf{H}$  dan  $\mathbf{G}$  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

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

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

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

Dengan meletakkan Persamaan (3) di atas Persamaan (4), diperoleh

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathbf{I}_k \\ \mathbf{A} \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}$$

dan hasil transpos kedua ruasnya adalah

$$\begin{aligned}
(x_1 x_2 \dots x_n) &= (u_1 u_2 \dots u_k) (\mathbf{I}_k | \mathbf{A}^T), \\
\text{ditulis} \\
\mathbf{x} &= \mathbf{uG}, \text{ dengan } \mathbf{G} = (\mathbf{I}_k | \mathbf{A}^T). \quad (5)
\end{aligned}$$

Persamaan 5 menunjukkan bahwa katakode  $\mathbf{x}$  merupakan kombinasi linear dari baris-baris matriks  $\mathbf{G}$ . Dengan demikian,  $\mathbf{G}$  adalah generator matriks dari  $C$ . Jika  $\mathbf{G}$  mempunyai bentuk standar seperti dalam Persamaan 5, maka diperoleh

$$\mathbf{H} = (\mathbf{A} | \mathbf{I}_{n-k})$$

Dari Persamaan 1 dan 5, diperoleh hubungan  $\mathbf{G}$  dan  $\mathbf{H}$  dalam persamaan berikut

$$\mathbf{GH}^T = \mathbf{HG}^T = \mathbf{0}.$$

Sekarang, misalkan pesan biner  $\mathbf{u} = u_1 u_2 \dots u_k$ , akan dikodekan menjadi katakode  $\mathbf{x} = x_1 x_2 \dots x_n$  yang selanjutnya dikirim melalui saluran yang diasumsikan terganggu, maka vektor yang diterima  $\mathbf{y} = y_1 y_2 \dots y_n$  bisa jadi berbeda dari  $\mathbf{x}$ . Dari proses ini, kita definisikan *vektor galat (error vector)*

$$\mathbf{e} = e_1 e_2 \dots e_n$$

sebagai selisih (perbedaan) antara  $\mathbf{x}$  dan  $\mathbf{y}$ , 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  $0 \leq p \leq \frac{1}{2}$ , 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  $\mathbf{y}$ . Ini sama artinya jika dikatakan bahwa Dekoder harus memilih  $\mathbf{e}$  sehingga  $\mathbf{x} = \mathbf{y} + \mathbf{e}$ . Tentu saja strategi yang harus digunakan adalah memilih  $\mathbf{e}$  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*.

<sup>2</sup> $\lfloor x \rfloor$  menotasikan bilangan bulat terbesar  $\leq x$ .

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 tak nol.*

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  $\lfloor \frac{d-1}{2} \rfloor$  galat<sup>2</sup>. 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  $k$ , masalahnya: "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,

$$l \leq D(n, k) \leq u,$$

artinya telah berhasil dikonstruksi kode dengan parameter  $[n, k, d \leq l]$  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  $l < d \leq u$ , 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 masalahnya:

$$K(n, d) := \max\{k/\text{kode } [n, k, d] \text{ ada}\}$$

$$N(k, d) := \min\{n/\text{kode } [n, k, d] \text{ ada}\}$$

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*

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

*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 sebelumnya bahwa mengkonstruksi suatu kode berarti mendefinisikan matriks cek paritas  $\mathbf{H}$  atau matriks generatornya  $\mathbf{G}$ . Selain teorema Gilbert-Varshamov bound, berikut ini diberikan beberapa teorema yang paling berperan untuk melandasi konstruksi  $\mathbf{H}$ .

**Teorema 2** [5] *Jika  $\mathbf{H}$  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  $\mathbf{H}$  yang bebas linear tetapi tidak ada  $(r + 1)$  kolom dari  $\mathbf{H}$  yang bebas linear (artinya  $r$  adalah rank dari  $\mathbf{H}$ ).*

**Teorema 3** [5] *Jika  $\mathbf{H}$  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  $\mathbf{H}$  yang tidak bebas linear dan setiap  $d - 1$  kolom dari  $\mathbf{H}$  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  $\mathbf{H}$  berordo  $(n - k) \times n$  ditulis

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

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

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

adalah matriks berordo  $(n - k) \times (n + 1)$  yang setiap  $d - 1$  vektor dari himpunan  $\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n, \mathbf{x}\}$  adalah bebas linear dalam ruang  $\mathbb{F}_2^{n-k}$ . Dalam hal ini  $\mathbf{H}'$  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

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

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

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

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

1. *Semua vektor baris dari  $\mathbf{B}$  berbeda, dan*
2. *Jumlah setiap  $i$  vektor baris dari  $\mathbf{B}$  berbobot paling sedikit  $(d - i)$  untuk  $i = 1, 2, 3, \dots, s$  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  $\mathbf{B}$  berukuran  $k \times r$  sebagaimana disyaratkan oleh teorema, akan ditunjukkan bahwa  $\mathbf{H}$  merupakan matriks paritas untuk kode  $C - [k+r, k, \geq d]$ . Hal pertama yang mudah dilihat dari struktur  $\mathbf{H}$  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  $wt(\mathbf{v}_c) = j$ , maka berlaku

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

dan

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

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

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

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  $\geq d$ .  $\square$

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

1. Semua vektor baris dari  $\mathbf{B}$  berbeda, dan
2. Jumlah setiap  $i$  vektor baris dari  $\mathbf{B}$  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  $\mathbf{B}$  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  $\mathbf{B}$  dan semua vektor sebagai hasil jumlah  $i$

vektor baris dari  $\mathbf{B}$  untuk  $i = 2, 3, \dots, s$  dengan  $s = \min\{d-1, k\}$ . Maka jelas bahwa  $V \subseteq \mathbb{F}_2^n$ . Jika  $V \neq \mathbb{F}_2^n$ , maka ada vektor  $\mathbf{x} \in \mathbb{F}_2^n$  dan  $\mathbf{x} \notin V$  yang bisa ditambahkan ke baris matriks  $\mathbf{B}$  untuk mendefinisikan matriks  $\mathbf{B}'$  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  $\mathbf{B}$  berukuran  $2 \times 6$  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  $\mathbf{B}'$  berordo  $4 \times 7$  yang mendefinisikan kode optimal kuat  $[11, 4, 5]$ . Proses perluasan dari  $\mathbf{B}$  ke  $\mathbf{B}'$  dilakukan dengan menambah satu kolom nol pada  $\mathbf{B}$ , dilanjutkan menambah dua vektor 7 bit yang memenuhi syarat strategi. Tanpa memerhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukkan ada 108 macam  $\mathbf{B}'$ , 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,  $\mathbf{B}'$  bisa diperluas ke  $\mathbf{B}''$  berordo  $9 \times 8$  yang mendefinisikan kode optimal kuat  $[17,9,5]$ . Tanpa memerhatikan relasi ekuivalensi, hasil eksplorasi komputatif menunjukkan ada 132 macam  $\mathbf{B}''$ , salah satunya

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

Percobaan untuk memperluas  $\mathbf{B}''$  ke  $\mathbf{B}'''$  untuk mendapatkan kode optimal kuat  $[23,14,5]$  adalah **gagal**. Dalam hal ini  $\mathbf{B}''$  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  $\mathbf{B}'''$  berordo  $14 \times 9$  berikut

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

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

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

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  $d \leq 15$  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.