



FORUM GURU BESAR
INSTITUT TEKNOLOGI BANDUNG



Orasi Ilmiah Guru Besar Institut Teknologi Bandung



TEORI DESAIN DAN TEORI KODING **Panorama Kombinatorika Aljabar**

Profesor Djoko Suprijanto

**Fakultas Matematika dan Ilmu Pengetahuan Alam
Institut Teknologi Bandung**

**Aula Barat ITB
16 November 2024**

Orasi ilmiah Guru Besar
Institut Teknologi Bandung

TEORI DESAIN DAN TEORI KODING

Panorama Kombinatorika Aljabar

Orasi ilmiah Guru Besar
Institut Teknologi Bandung

TEORI DESAIN DAN TEORI KODING

Panorama Kombinatorika Aljabar

Prof. Djoko Suprijanto

16 November 2024
Aula Barat ITB



Hak cipta © pada penulis dan dilindungi Undang-Undang

Hak penerbitan pada ITB Press

Dilarang memperbanyak sebagian atau seluruh bagian dari buku ini tanpa izin dari penerbit

Orasi ilmiah Guru Besar Institut Teknologi Bandung:

Teori Desain dan Teori Koding: Panorama Kombinatorika Aljabar

Penulis : Prof. Djoko Suprijanto

Reviewer : Prof. Khreshna Imaduddin Ahmad Syuhada

Editor Bahasa : Rina Lestari

Cetakan I : 2024

ISBN : 978-623-297-608-5

e-ISBN : 978-623-297-609-2 (PDF)



📍 Gedung STP ITB, Lantai 1,
Jl. Ganesa No. 15F Bandung 40132
☎ +62 22 20469057
🌐 www.itbpress.id
✉ office@itbpress.id
Anggota Ikapi No. 043/JBA/92
APPTI No. 005.062.1.10.2018

Wandrer's Nachtlid

*Über allen Gipfeln
Ist Ruh,
In allen Wipfeln
Spürest du
Kaum einen Hauch;
Die Vögelein schweigen im Walde.
Warte nur, balde
Ruhest du auch. (Johann Wolfgang von Goethe)*

Dendang Malam Pengembara

*Di puncak segala
Sentosa bertakhta,
Di pucuk segala
Nyaris tiada
Sehembus pun bayu kau rasa;
Senyap burung-burung di hutan.
Sabar, kan segera tiba masa
Engkau pun istirahat sentosa.
--terjemah Agus R. Sarjono, 2013)*

PRAKATA

Bismillahi rahmanirrahim

Alhamdulillah rabilalamin. Allahumma shalli ala Muhammad wa ala ali Muhammad.

Segala puji dan kemuliaan adalah milik Allah yang Mahaagung. Semoga salam dan berkah-Nya senantiasa tercurah kepada manusia mulia, Nabi Muhammad Saw., keluarganya, dan para shahabatnya.

Dalam serba keterbatasan —waktu dan terutama kemampuan— akhirnya kami dapat menuntaskan buku Orasi Ilmiah Guru Besar Institut Teknologi Bandung berjudul *Teori desain dan Teori Koding: Panorama Kombinatorika Aljabar*.

Buku ini terwujud berkat peran dan kontribusi dari banyak pihak. Kami tidak akan melupakan dorongan dari Fakultas Matematika dan Ilmu Pengetahuan Alam Institut Teknologi Bandung, di bawah kepemimpinan Prof. Wahyu Srigutomo, Ph.D.. Dukungan dari Bapak/ Ibu tenaga kependidikan di Departemen Matematika juga senantiasa kami ingat. Terima kasih juga kami sampaikan kepada seluruh rekan dosen di Departemen Matematika yang telah menciptakan suasana yang menyenangkan bagi berlangsungnya kegiatan penelitian.

Kami mengucapkan terima kasih kepada Forum Guru Besar Institut Teknologi Bandung yang telah memberikan kesempatan untuk menyampaikan orasi ilmiah dan kepada penerbit ITB Press yang telah memublikasikan buku orasi ini. Tidak banyak yang kami harapkan dari orasi dan penerbitan buku ini. Seandainya ada yang dapat mengambil manfaat dari buku ini, kami sudah merasa sangat bersyukur dan berterima kasih.

Bandung, 14 Oktober 2024

Djoko Suprijanto

SINOPSIS

Buku ini kami upayakan sebagai semacam kaleidoskop (meski tidak lengkap), yang merekam perjalanan kami, tentu saja berkolaborasi dengan beberapa kolega, dalam melakukan penelitian matematika, khususnya pada dua aspek besar dalam bidang kombinatorika aljabar, yakni teori desain (*design theory*) dan teori koding¹ (*coding theory*), selama hampir 17 tahun (2007-2024) sebagai dosen di Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Teknologi Bandung, sejak 1996. Secara khusus ada dua topik besar yang dieksplorasi di dalam buku ini: versi kontinu dari desain kombinatorial, khususnya *spherical designs* dan *Euclidean designs*, dan teori koding kombinatorial dan teori koding aljabar (*algebraic and combinatorial coding theory*).

¹ Sebagai istilah, teori koding kami maksudkan sebagai padanan dari istilah *coding theory* dalam Bahasa Inggris. Meski istilah ini tidak baku, istilah pengkodean tampaknya lebih sesuai dengan kaidah gramatika dalam Bahasa Indonesia, namun istilah ini sudah telanjur kami gunakan selama bertahun-tahun di berbagai kesempatan, termasuk dalam menamai mata kuliah yang kami tawarkan di program studi Matematika, baik untuk program sarjana maupun program magister. Karena itu, istilah ini tetap kami pertahankan di sini.

DAFTAR ISI

PRAKATA.....	VII
SINOPSIS	IX
DAFTAR ISI.....	XI
DAFTAR GAMBAR.....	XIII
DAFTAR TABEL.....	XV
1. PENDAHULUAN.....	1
1.1 Kombinatorika Aljabar: Masalah Definisi	2
1.2 Teori Delsarte tentang Teori Desain dan Teori Koding.....	3
2. SKEMA ASOSIASI.....	5
2.1 Sejarah Singkat Skema Asosiasi	5
2.2 Grup Permutasi dan Definisi Skema Asosiasi	5
2.3 Beberapa Contoh Skema Asosiasi	9
3. TEORI DESAIN	11
3.1 Teori <i>Spherical Designs</i>	12
3.2 Perumuman <i>Spherical Designs</i>	22
4. TEORI KODING	33
4.1 Kode Linear Atas Lapangan Hingga.....	33
4.2 Kode Linear Atas Ring Hingga.....	38
4.3 Beberapa Hasil Lain Terkait Kode Linear Atas Lapangan dan Ring Hingga	56
5. PENUTUP.....	57
6. UCAPAN TERIMA KASIH	59
DAFTAR PUSTAKA	63
CURRICULUM VITAE	69

DAFTAR GAMBAR

Gambar 1	Bidang Fano	11
Gambar 2	Dari kiri ke kanan berturut-turut adalah tetrahedron regular, kubus, oktahedron regular, dodekahedron regular, okisahedron regular.	15
Gambar 3	<i>Tight Euclidean 4-design</i> dalam $\mathbb{R}^2$	26
Gambar 4	Ilustrasi definisi <i>Euclidean design</i> yang bersifat non-rigid kuat.....	28

DAFTAR TABEL

Tabel 1	Contoh-contoh spherical designs R^3	15
Tabel 2	<i>Spherical t-design</i> pada bola satuan $S^{d-1} \subseteq R^d$	21
Tabel 3	Daftar kode liner biner yang diperoleh dengan beragam metode konstruksi.....	37

1 PENDAHULUAN

Dibandingkan dengan cabang ilmu lainnya, kombinatorika dipandang sebagai cabang ilmu matematika yang relatif muda. Di awal abad ke-20, prasangka terhadap kombinatorika sebagai bukan “*real mathematics*” sangatlah lazim. John Henry Constantine Whitehead (1904-1960) dilaporkan berkata, “*Combinatorics is the slums of topology.*” Robert Kanigel menggambarkan Percy Alexander MacMahon (1854 – 1929), salah seorang matematikawan Inggris yang menemukan bakat luar biasa yang dimiliki oleh sang jenius Srinivasa Ramanujan (1887-1920), dalam ungkapan demikian:

[MacMahon's] expertise lay in combinatorics, a sort of glorified dicethrowing, and in it he had made contributions original enough to be named a Fellow of the Royal Society.

Satu nama besar yang mengangkat marwah kombinatorika adalah Gian Carlo Rota (1932-1999), seorang matematikawan kelahiran Italia yang menghabiskan kariernya di MIT. Lewat artikelnya, *On the Foundations of Combinatorial Theory*,² yang terbit pada 1964, Rota berhasil melakukan sebuah revolusi besar yang menyebabkan kombinatorika masuk ke dalam arus utama matematika modern. Karena karyanya itu pulalah, Rota dianugerahi Steel Prize pada 1964.

Pandangan dunia matematika terhadap kombinatorika semakin berubah setelah pada tahun 1998, dua orang yang memberikan kontribusi yang signifikan dan terkait erat dengan kombinatorika meraih Fields medal. Keduanya adalah Richard Borcherds dan Timothy Gowers. Borcherds dikenal sebagai matematikawan yang bekerja di bidang teori kisi (*lattices theory*), teori grup, juga aljabar berdimensi tak hingga. Sementara itu Gowers dikenal sebagai seorang matematikawan yang bekerja di bidang analisis fungsional dan kombinatorika.

² “On the Foundations of Combinatorial Theory I. Theory of Möbius Functions,” *Z. Wahrscheinlichkeitstheorie* 2 (1964), 340-368. Artikel Rota bagian II hingga IX terbit pada rentang waktu 1970-1974, sementara artikel bagian terakhir, bagian X, terbit pada tahun 1992. Kecuali artikel bagian V yang ditulis oleh George E. Andrews, artikel bagian II hingga bagian X ditulis oleh Rota berkolaborasi dengan beberapa matematikawan lain.

1.1 Kombinatorika Aljabar: Masalah Definisi

Istilah kombinatorika aljabar (*algebraic combinatorics*) untuk pertama kalinya diperkenalkan secara resmi di dunia ilmiah oleh Eiichi Bannai dalam sebuah artikel survei berjudul “*Algebraic Combinatorics*” yang terbit dalam *Sugaku* vol. 31 hal. 126-134, tahun 1979. *Sugaku* adalah jurnal ilmiah resmi yang diterbitkan oleh *the Mathematical Society of Japan*, yang secara khusus menerbitkan artikel survei atau eksposisi dalam bahasa Jepang. Jurnal ini kemudian juga diterjemahkan dan diterbitkan dalam Bahasa Inggris oleh American Mathematical Society, dengan nama *Sugaku Expositions*.³ Beberapa tahun kemudian, tepatnya pada 1984, Eiichi Bannai dan Tatsuro Ito menggunakan istilah yang sama saat mereka menerbitkan sebuah buku berjudul “*Algebraic Combinatorics I: Association Schemes*.”⁴ Sementara istilah serupa di dunia kombinatorika, yaitu *algebraic graph theory* (teori graf aljabar) telah lebih dahulu digunakan oleh Norman Bigg sejak tahun 1974, juga *algebraic coding theory* (teori koding aljabar) oleh Elwyn Berlekamp pada 1968, ketika masing-masing menerbitkan sebuah buku dan menamai bukunya dengan kedua istilah itu. Istilah ini semakin populer sejak kemunculan sebuah jurnal baru, *Journal of Algebraic Combinatorics*⁵ pada 1992, dengan Bannai bertindak sebagai salah seorang *advisory board*. Pada tahun 1993, Chris Godsil juga menerbitkan buku berjudul *Algebraic Combinatorics*,⁶ yang topik pembahasannya sangat serupa dengan karya Bannai dan Ito yang telah terbit pada 1984 itu.

³ Jurnal overview: *Sugaku Expositions contains translations into English of expository articles from the journal Sugaku, published by Iwanami Shoten, publishers for the Mathematical Society of Japan. Published biannually, each issue of Sugaku Expositions contains several expository articles that provide highly informative accounts of a variety of current areas of research.* Selengkapnya tentang jurnal ini, lihat <https://www.ams.org/publications/journals/journalsframework/aboutsuga>.

⁴ E. Bannai dan T. Ito, (1984) *Algebraic combinatorics I: Association schemes*, Benjamin/ Cummings, Menlo Park, California. Buku ini semula direncanakan untuk terbit dalam dua bagian, dengan bagian kedua berjudul *Algebraic combinatorics II: Delsarte theory, codes and designs*. Tetapi buku ini tidak kunjung terbit hingga saat ini, karena tidak sempat dituliskan.

⁵ Lihat <https://link.springer.com/journal/10801>. Sejak akhir tahun 2017 seluruh Editor-in-Chief (berjumlah 4 orang) dan hampir semua editorial board dari jurnal tersebut memutuskan untuk tidak memperpanjang kontrak karena mereka tidak menyukai kebijakan penerbit Springer yang semakin berorientasi bisnis. Dalam kalimat salah seorang mantan Editor-in-Chief jurnal tersebut, Akihiro Munemasa, “It has been becoming more and more clear that commercial journal publishers are charging high subscription fees, profiting from the volunteer labour of the academic community, and adding little value.” Untuk uraian lengkap terkait alasan mengapa para editorial board ramai-ramai mengundurkan diri dari jurnal ini, lihat misalnya <https://www.math.is.tohoku.ac.jp/~munemasa/events/documents/20170810.txt>). Sebagai gantinya, hampir semua editorial board dari jurnal tersebut terlibat dalam pengelolaan jurnal baru, *Algebraic Combinatorics*, yang terbit sejak 2018. Jurnal ini gratis baik bagi penulis maupun pembaca.

⁶ C.D. Godsil, (1993), *Algebraic Combinatorics*, Chapman & Hall.

Tidak ada definisi eksplisit atau definisi baku terkait istilah kombinatorika aljabar ini. Tetapi, yang dimaksud oleh Bannai (1979) dan Bannai dan Ito (1984) dengan kombinatorika aljabar adalah cabang ilmu matematika yang secara filosofis bersifat “teori grup tanpa (menggunakan istilah teknis) grup” (*group theory without groups*), atau teori representasi kombinatorik (*combinatorial representation theory*), atau studi berbagai objek kombinatorika dengan menggunakan pendekatan teori karakter (*a character theoretical study of combinatorial objects*).

Saat ini istilah kombinatorika aljabar mengacu kepada objek matematika yang tidak tunggal. Setidaknya, istilah ini juga digunakan untuk menggantikan istilah kombinatorika enumeratif (*enumerative combinatorics*), yaitu kombinatorika yang terkait langsung ataupun tidak dengan pencacahan (*counting*). Kelompok ini memandang bahwa secara filosofis, kombinatorika aljabar adalah sintesis dari dua hal yang tampak berlawanan: abstraksi sesuatu yang konkret sekaligus konkretisasi sesuatu yang abstrak (*abstraction of the concrete dan concretization of the abstract*)⁷, sebuah frasa yang bersifat umum dan tampaknya tidak membuat yang kurang jelas menjadi lebih jelas.

Jika para juru bicara atau inisiator untuk kelompok pertama di antaranya adalah Eiichi Bannai, Tatsuro Ito, Chris Godsil, dan Paul Terwilliger, maka untuk kelompok kedua adalah Gian-Carlo Rota, Richard Stanley, Marco Schutzenberger dan Dominique Foata. Istilah kombinatorika aljabar di dalam buku ini mengacu pada pengertian kelompok pertama.

1.2 Teori Delsarte tentang Teori Desain dan Teori Koding

Salah satu cabang ilmu kombinatorika yang memegang peran penting dan sentral dalam kombinatorika aljabar adalah skema asosiasi. Adalah Philippe Delsarte, seorang kombinatorialis Belgia yang pertama kali menunjukkan peran sentral dari skema asosiasi dalam kombinatorika aljabar tersebut.

Buku ini diawali dengan uraian tentang skema asosiasi, yang oleh Philippe Delsarte⁸ ditunjukkan dapat digunakan sebagai alat terpadu untuk meninjau beragam objek kombinatorika yang berbeda. Pendekatan Delsarte ini

⁷ Doron Zeilberger, “Enumerative and Algebraic Combinatorics” dalam Timothy Gowers, June-Barrow Green, dan Imre Leader (Editors), (2008), *Princeton Companion to Mathematics*, Princeton University Press, hal 550.

⁸ P. Delsarte, “An algebraic approach to the association schemes of coding theory,” *Phillips Research Reports Supplements*, No. 10 (1973). Artikel ini berasal dari disertasi PhD-nya pada tahun 1973.

belakangan dikenal sebagai Teori Delsarte. Seperti telah disebutkan di awal, Eiichi Bannai dan Tatsuro Ito telah menerbitkan buku berjudul “*Algebraic Combinatorics I: Association Schemes*.” Sebagaimana terbaca dalam catatan kaki nomor 4, buku ini semula direncanakan untuk terbit dalam dua bagian, dengan bagian kedua berjudul “*Algebraic combinatorics II: Delsarte Theory, Codes and Designs*”. Namun bagian kedua ini tidak kunjung terbit hingga saat ini, karena tidak sempat dituliskan. Sebagai gantinya, Eiichi Bannai bersama Etsuko Bannai, Tatsuro Ito, dan Rie Tanaka justru menerbitkan buku lain, “*Algebraic Combinatorics*,” Walter de Gruyter GmbH, Berlin/ Boston, pada 2021. Buku ini memuat dua bab terkait teori Delsarte tentang kode dan desain, dua objek kombinatorika yang penting dalam kombinatorika aljabar.

Setelah uraian yang serba ringkas tentang skema asosiasi, bagian berikutnya memaparkan uraian tentang desain kombinatorial (*combinatorial designs*) dan desain sferis (*spherical designs*) sebagai versi kontinu (*continuous analogue*) dari desain kombinatorial. Selanjutnya, akan diuraikan pula desain Euclides (*Euclidean designs*), sebagai perumuman dari desain kombinatorial dan desain sferis⁹. Akan kami sampaikan juga beberapa kontribusi kami di bidang ini. Beralih ke bagian berikutnya, kami akan menguraikan teori koding atas lapangan hingga dan ring hingga dan kontribusi kami di dalamnya.

⁹ Untuk selanjutnya kita akan menggunakan istilah aslinya: *spherical designs* dan *Euclidean designs*.

2. SKEMA ASOSIASI

2.1 Sejarah Singkat Skema Asosiasi

Skema asosiasi adalah konsep matematika yang pada awalnya diperkenalkan oleh para ahli statistika lebih dari setengah abad lalu.

Awalnya, Yates (1939) untuk pertama kalinya mendesain suatu desain blok tak-lengkap (*incomplete block design*) untuk kebutuhan eksperimen dalam statistika. Desain ini melahirkan dua pertanyaan bagi para ahli statistika. Dua tahun kemudian, Bose dan Nair (1939) memperkenalkan *balanced incomplete block designs* (BIBD) untuk menjawab dua pertanyaan di atas. Konsep yang melandasi BIBD adalah apa yang sekarang disebut sebagai skema asosiasi. Secara formal, Bose dan Shimamoto (1952) yang memperkenalkan gagasan skema asosiasi, yang sesungguhnya telah muncul secara implisit pada BIBD. Tujuh tahun kemudian, Bose dan Mesner (1959) memperkenalkan konsep aljabar yang terkait dengan skema asosiasi. Aljabar ini sekarang dikenal sebagai Aljabar Bose-Mesner.

Setelah lebih dari tiga puluh tahun tidak ada perkembangan berarti, konsep skema asosiasi mulai berkembang pesat setelah Philippe Delsarte pada disertasi 1973 menunjukkan bahwa skema asosiasi dapat dijadikan sebagai alat terpadu untuk meninjau beragam objek kombinatorika yang berbeda, yang dua di antaranya adalah desain kombinatorial dan kode linear. Sejak saat itu, studi tentang skema asosiasi hidup kembali dan berkembang pesat.

2.2 Grup Permutasi dan Definisi Skema Asosiasi

Dari perspektif aljabar, skema asosiasi dapat dipandang sebagai perumuman dari grup permutasi hingga.

Misalkan $\Omega \neq \emptyset$ adalah himpunan hingga. Grup G beraksi pada himpunan Ω jika terdapat pemetaan $\Omega \times G \rightarrow \Omega$, $(\alpha, g) \mapsto \alpha^g$, yang memenuhi kedua sifat berikut.

1. $\alpha^{gh} = (\alpha^g)^h$, untuk setiap $\alpha \in \Omega$, dan setiap $g, h \in G$.
2. $\alpha^1 = \alpha$, untuk setiap $\alpha \in \Omega$, dengan 1 adalah unsur identitas dari G .

Misalkan G adalah grup yang beraksi pada himpunan hingga Ω . Kita definisikan relasi $\sim$ pada Ω sebagai berikut: untuk setiap $\alpha, \beta \in \Omega$,

$$\alpha \sim \beta \Leftrightarrow \alpha^g = \beta, \text{ untuk suatu } g \in G.$$

Mudah ditunjukkan bahwa $\sim$ merupakan sebuah *relasi ekivalen*. Kelas-kelas ekivalen yang dibentuk dari relasi ekivalen tersebut kita sebut *orbit* dari aksi G pada Ω . Orbit dari aksi G pada Ω kita tuliskan sebagai

$$\alpha^G := \{\alpha^g : g \in G\},$$

untuk $\alpha \in \Omega$.

Grup G dikatakan *beraksi secara transitif* pada himpunan Ω jika untuk setiap $\alpha, \beta \in \Omega$ terdapat $g \in G$ sehingga $\alpha^g = \beta$.

Permutasi pada Ω adalah pemetaan satu-satu dan pada dari Ω ke Ω . Himpunan semua permutasi pada Ω membentuk grup terhadap operasi komposisi. Grup ini disebut *grup simetris*, ditulis $S(\Omega)$. Grup permutasi adalah subgrup dari $S(\Omega)$. Jika $|\Omega| = n$, maka kita juga biasa menuliskan $S(\Omega)$ sebagai $S(n)$ atau S_n .

Misalkan grup permutasi G beraksi secara transitif pada himpunan hingga Ω . Maka G beraksi secara natural pada himpunan $\Omega \times \Omega$ dengan $(\alpha, \beta)^g = (\alpha^g, \beta^g)$. Maka himpunan $\{(\alpha, \alpha) : \alpha \in \Omega\}$ adalah orbit dari aksi G pada himpunan $\Omega \times \Omega$. Tuliskan

1. $R_0 := \{(\alpha, \alpha) : \alpha \in \Omega\}$.

Tentu saja, $\Omega \times \Omega$ dapat didekomposisi ke dalam orbit-orbit $R_0, R_1, R_2, \dots, R_d$ dengan aksi dari grup G . Jadi,

2. $\Omega \times \Omega = R_0 \cup R_1 \cup \dots \cup R_d$, dengan $R_i \cap R_j = \emptyset$, untuk $i \neq j$.

Lebih jauh lagi, dapat ditunjukkan bahwa orbit-orbit tersebut memenuhi hubungan

3. Untuk setiap $i \in [0, d]_{\mathbb{Z}}$, jika kita definisikan

$$R_i^T := \{(\beta, \alpha) : (\alpha, \beta) \in R_i\},$$

maka terdapat $j \in [0, d]_{\mathbb{Z}}$ sehingga $R_i^T = R_j$.

4. Untuk setiap $i, j, k \in [0, d]_{\mathbb{Z}}$, kardinalitas dari himpunan

$$\{\gamma \in \Omega : (\alpha, \gamma) \in R_i, (\gamma, \beta) \in R_j\}$$

tidak bergantung kepada pemilihan $\alpha, \beta \in \Omega$ dengan $(\alpha, \beta) \in R_k$, dan hanya bergantung kepada pemilihan i, j, k .

Skema asosiasi didefinisikan secara aksiomatis sebagai konfigurasi yang memenuhi sifat yang tepat sama dengan sifat-sifat grup permutasi transitif pada (1)-(4) di atas. Secara formal, skema asosiasi didefinisikan demikian.

Definisi (Skema asosiasi) Misalkan X adalah himpunan hingga dan $\mathcal{R} := \{R_0, R_1, \dots, R_d\}$ barisan relasi pada X . Konfigurasi $\mathfrak{X} = (X, \mathcal{R})$ disebut skema asosiasi kelas- d jika memenuhi sifat-sifat berikut:

1. $R_0 := \{(\alpha, \alpha) : \alpha \in \Omega\}$.
2. $X \times X = R_0 \cup R_1 \cup \dots \cup R_d$, dengan $R_i \cap R_j = \emptyset$, untuk $i \neq j$.
3. Untuk setiap $i \in [0, d]_{\mathbb{Z}}$, jika kita definisikan

$$R_i^T := \{(\beta, \alpha) : (\alpha, \beta) \in R_i\},$$

maka terdapat $j \in [0, d]_{\mathbb{Z}}$ sehingga $R_i^T = R_j$.

4. Untuk setiap $i, j, k \in [0, d]_{\mathbb{Z}}$, kardinalitas dari himpunan

$$p_{ij}^k := |\{\gamma \in \Omega : (\alpha, \gamma) \in R_i, (\gamma, \beta) \in R_j\}|$$

tidak bergantung kepada pemilihan $\alpha, \beta \in \Omega$ dengan $(\alpha, \beta) \in R_k$, dan hanya bergantung kepada pemilihan i, j, k .

Skema asosiasi dikatakan *komutatif* jika memenuhi hubungan

5. $p_{ij}^k = p_{ji}^k$, untuk setiap $i, j, k \in [0, d]_{\mathbb{Z}}$.

Skema asosiasi dikatakan *simetris* jika memenuhi hubungan

6. $R_i^T = R_i$, untuk setiap $i \in [0, d]_{\mathbb{Z}}$.

Mudah dibuktikan bahwa setiap skema asosiasi simetris adalah skema asosiasi komutatif.

Untuk setiap $i \in [0, d]_{\mathbb{Z}}$, kita definisikan matriks ketetanggaan A_i dari relasi R_i sebagai berikut.

$$A_i(x, y) := \begin{cases} 1, & \text{jika } (x, y) \in R_i, \\ 0, & \text{jika } (x, y) \notin R_i. \end{cases}$$

Kondisi nomor (1) sampai dengan (6) pada definisi skema asosiasi di atas ekuivalen dengan kondisi (1) sampai dengan (6) di bawah ini:

1. $A_0 = I$, matriks identitas.
2. $A_0 + A_1 + \dots + A_d = J$, matriks yang semua entrinya 1.
3. Untuk setiap $i \in [0, d]_{\mathbb{Z}}$ terdapat $j \in [0, d]_{\mathbb{Z}}$ sehingga berlaku

$$A_i^T = A_j.$$

4. Untuk setiap $i, j \in [0, d]_{\mathbb{Z}}$, berlaku

$$A_i A_j = \sum_{k=0}^d p_{ij}^k A_k.$$

5. Untuk setiap $i, j \in [0, d]_{\mathbb{Z}}$, berlaku

$$A_i A_j = A_j A_i.$$

6. Untuk setiap $i \in [0, d]_{\mathbb{Z}}$ berlaku

$$A_i^T = A_i.$$

Subaljabar $\mathbb{C}[\mathfrak{X}] := \langle A_0, A_1, \dots, A_d \rangle_{\mathbb{C}}$ dari aljabar matriks $\mathbb{C}^{|X| \times |X|}$ disebut aljabar Bose-Mesner dari skema asosiasi $\mathfrak{X}$. Aljabar $\mathbb{C}[\mathfrak{X}]$ merupakan aljabar semisimpel atas $\mathbb{C}$ berdimensi $(d + 1)$. Skema asosiasi $\mathfrak{X}$ adalah skema asosiasi komutatif jika dan hanya jika aljabar Bose-Mesner $\mathbb{C}[\mathfrak{X}]$ komutatif. Dalam kasus ini, aljabar komutatif $\mathbb{C}[\mathfrak{X}]$ memiliki $(d + 1)$ idempoten primitif $E_0, E_1, \dots, E_d$ yang juga merupakan basis dari aljabar $\mathbb{C}[\mathfrak{X}]$. Tanpa mengurangi keumuman, kita dapat memisalkan bahwa $E_0 = \frac{1}{|X|}J$. Jadi, aljabar Bose-Mesner $\mathbb{C}[\mathfrak{X}]$ dari skema asosiasi komutatif $\mathfrak{X}$ memiliki setidaknya dua basis, yaitu $A_0, A_1, \dots, A_d$ dan basis idempoten primitif $E_0, E_1, \dots, E_d$. Misalkan P dan Q merupakan matriks perubahan dari dua basis tersebut, yaitu matriks yang memenuhi hubungan

$$(A_0, A_1, \dots, A_d) = (E_0, E_1, \dots, E_d)P,$$

$$(|X|E_0, |X|E_1, \dots, |X|E_d) = (A_0, A_1, \dots, A_d)Q.$$

P dan Q berturut-turut kita sebut matriks karakteristik pertama dan kedua dari skema asosiasi komutatif $\mathfrak{X}$. Matriks karakteristik pertama disebut juga tabel karakter dari skema $\mathfrak{X}$. Dapat ditunjukkan dengan mudah bahwa matriks karakteristik pertama dan kedua memenuhi hubungan

$$PQ = QP = |X|I,$$

dengan I adalah matriks identitas.

Perkalian Hadamard antara dua matriks A dan B berukuran sama didefinisikan sebagai perkalian entri demi entri yang bersesuaian:

$$(A \circ B)(i, j) = A(i, j)B(i, j),$$

dengan $A = A(i, j)_{i,j=1}^{m,n}$, dan $B = B(i, j)_{i,j=1}^{m,n}$. Karena skema asosiasi komutatif $\mathfrak{X}$ tertutup terhadap perkalian Hadamard, maka terdapat bilangan kompleks q_{ij}^k sehingga

$$(|X|E_i) \circ (|X|E_j) = \sum_{k=0}^d q_{ij}^k (|X|E_k).$$

Telah diketahui bahwa bilangan kompleks q_{ij}^k memenuhi pertaksamaan $q_{ij}^k \geq 0$, artinya q_{ij}^k merupakan bilangan real taknegatif. Pertaksamaan ini disebut *syarat Krein*.

2.3 Beberapa Contoh Skema Asosiasi

Di bawah ini adalah beberapa contoh skema asosiasi yang diperoleh dari suatu grup hingga G .

Contoh 2.1 (Kasus grup) Misalkan G grup hingga yang beraksi secara transitif pada himpunan hingga X . Maka $R_0 := \{(x, x) : x \in X\}, R_1, \dots, R_d$ merupakan orbit dari aksi G pada himpunan $X \times X$, sehingga $\mathfrak{X}(G, X) = (X, \{R_i\}_{i=0}^d)$ merupakan skema asosiasi kelas- d . Skema asosiasi ini komutatif jika dan hanya jika karakter permutasi $\pi = 1_H^G$ dari G pada X bebas-multiplisitas (*multiplicity-free*), yakni jika $\pi = \chi_0 + \chi_1 + \dots + \chi_d$ merupakan dekomposisi dari π ke dalam karakter-karakter tak tereduksi, maka $\chi_i \neq \chi_j$ untuk $i \neq j$.

Contoh 2.2 (Skema asosiasi grup $\mathfrak{X}(G)$) Misalkan G adalah grup hingga dan misalkan pula $C_0 := \{1\}, C_1, \dots, C_d$ adalah kelas-kelas konjugasi dari G . Jika untuk setiap $i \in [0, d]_{\mathbb{Z}}$ kita definisikan relasi R_i dengan

$$(x, y) \in R_i \Leftrightarrow yx^{-1} \in C_i \quad (x, y \in G),$$

maka $\mathfrak{X}(G) = (G, \{R_i\}_{i=0}^d)$ merupakan skema asosiasi. Skema asosiasi ini selalu bersifat komutatif.

Contoh 2.3 (Skema asosiasi Hamming $H(d, q)$) Misalkan $q \geq 2$ bilangan asli, dan F himpunan hingga dengan q unsur, dan $X = F \times F \times \dots \times F = F^d$ (perkalian langsung dari d buah himpunan F). Relasi pada X didefinisikan sebagai:

$$(x, y) \in R_i \Leftrightarrow d_H(x, y) := |\{j : x_j \neq y_j\}| = i,$$

untuk setiap $x = (x_1, x_2, \dots, x_d), y = (y_1, y_2, \dots, y_d) \in X, i \in [0, d]_{\mathbb{Z}}$.

Maka $H(d, q) = (X, \{R_i\}_{i=0}^d)$ merupakan skema asosiasi simetris, yang disebut skema asosiasi Hamming atau skema Hamming.

Contoh 2.4 (Skema asosiasi Johnson $J(v, d)$) Misalkan V adalah himpunan dengan v unsur dan X adalah koleksi subhimpunan dari V dengan d unsur, dengan $d \leq \frac{v}{2}$. (Jadi $|X| = \binom{v}{d}$). Relasi pada X didefinisikan sebagai:

$$(x, y) \in R_i \Leftrightarrow |x \cap y| = d - i,$$

untuk setiap $i \in [0, d]_{\mathbb{Z}}$. Maka $J(v, d) = (X, \{R_i\}_{i=0}^d)$ merupakan skema asosiasi simetris, yang disebut skema asosiasi Johnson atau skema Johnson.

Catatan:

1. Skema asosiasi pada Contoh 2.2 di atas adalah skema asosiasi kasus grup (Contoh 2.1) jika kita meninjau aksi dari grup $G \times G$ pada himpunan G dengan $g^{(g_1, g_2)} = g_1^{-1} g g_2$, untuk setiap $(g_1, g_2) \in G \times G$, dan $g \in G$.
2. Skema asosiasi pada Contoh 2.3 adalah skema asosiasi kasus grup (Contoh 2.1) jika kita meninjau aksi dari grup $G = S_q \wr S_d$ pada himpunan $X = H \backslash G$ dengan $H = S_{q-1} \wr S_d$. Dalam teori coding, simbol $d_H(\mathbf{x}, \mathbf{y}) := |\{j: x_j \neq y_j, j \in [1, n]_{\mathbb{Z}}\}|$ disebut jarak Hamming antara vektor $\mathbf{x}$ dengan vektor $\mathbf{y}$.
3. Skema asosiasi pada Contoh 2.4 adalah skema asosiasi kasus grup (Contoh 2.1) jika kita meninjau aksi dari grup $G = S_v$ pada himpunan $X = H \backslash G$ dengan $H = S_d \times S_{v-d}$.

Di samping contoh-contoh skema asosiasi yang berasal dari grup hingga, kita juga dapat mengonstruksi berbagai contoh skema asosiasi yang tidak berasal dari grup. Contoh-contoh ini dapat kita lihat misalnya di dalam buku karya Rosemary Bailey¹⁰, tetapi tidak kita diskusikan di sini.

Struktur skema asosiasi ini kita manfaatkan untuk mengobservasi eksistensi *tight Euclidean t-designs* dan untuk mengonstruksi kode linear atas lapangan hingga. Karena keterbatasan ruang, peran krusial dari skema asosiasi dalam hubungannya dengan eksistensi *tight Euclidean t-design* tidak kami deskripsikan di sini¹¹, tetapi kami tampilkan secara eksplisit dalam konstruksi kode linear atas lapangan hingga, ketika kami memaparkan hasil penelitian terkait konstruksi kode linear atas lapangan hingga dari graf Johnson, yang berasal dari skema (asosiasi) Johnson.

¹⁰ Lihat R.A. Bailey, (2004), *Association Schemes: Designed Experiments, Algebra and Combinatorics*, Cambridge University Press.

¹¹ Untuk deskripsi lengkap, silahkan tinjau D. Suprijanto, "On tight Euclidean 6-designs: an experimental result," *ITB Journal of Science* **43** A(1) (2011), 19-42.

3. TEORI DESAIN

Kita awali dengan pengertian desain kombinatorial. Misalkan $X \neq \emptyset$, dan $|X| = v$. Misalkan $\mathcal{B} \subseteq \binom{X}{k}$, koleksi subhimpunan dari X dengan kardinalitas k . *Desain kombinatorial* dengan parameter $(v, k, \lambda) - t$ adalah konfigurasi $(X, \mathcal{B})$ yang memenuhi hubungan:

1. Setiap anggota dari $\mathcal{B}$, disebut *blok*, terdiri atas tepat k titik (yakni anggota dari X); dan
2. Setiap t titik termuat tepat dalam λ blok.

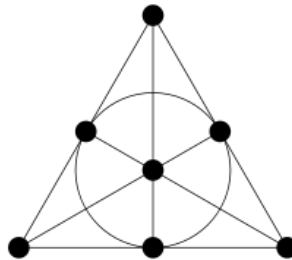
Dalam ekspresi lain, konfigurasi $(X, \mathcal{B})$ disebut desain kombinatorial dengan parameter $(v, k, \lambda) - t$ jika memenuhi persamaan

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{X}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B),$$

untuk setiap polinom $f(x_1, x_2, \dots, x_v)$ berderajat kurang dari atau sama dengan t , dengan fungsi polinom didefinisikan sebagai berikut: untuk setiap $i \in X$,

$$x_i(B) := \begin{cases} 1, & i \in B, \\ 0, & i \notin B. \end{cases}$$

Contoh yang sangat populer untuk desain kombinatorial adalah bidang Fano, yang merupakan desain kombinatorial dengan parameter $(7, 3, 1) - 2$.



Gambar 1 Bidang Fano

Teori desain kombinatorial telah berkembang cukup jauh. Untuk mengetahui perkembangan terakhir dan objek-objek kombinatorika yang terkait dengannya, lihat misalnya (C.J. Colbourn dan J.H. Diniz (ed.), 2007), dan berbagai artikel ilmiah yang terbit di beragam jurnal kombinatorika seperti *Journal of Combinatorial Designs*, *Journal of Combinatorial Theory Serie*

A, Algebraic Combinatorics dll.. Sekarang, marilah kita tinjau ilustrasi di bawah ini.

Tinjaulah kubus Q yang terdiri atas 8 titik dengan koordinat

$$Q := \left\{ \left(\pm \frac{1}{3}, \pm \frac{1}{3}, \pm \frac{1}{3} \right) \right\},$$

termuat di dalam bola satuan $S^2 \subseteq \mathbb{R}^3$. Q adalah penaksiran yang baik untuk S^2 dalam arti bahwa

$$\frac{1}{4\pi} \int_{S^2} f(\mathbf{x}) d\sigma = \frac{1}{8} \sum_{\mathbf{x} \in Q} f(\mathbf{x}),$$

untuk setiap polinom $f(\mathbf{x}) \in \text{Pol}(\mathbb{R}^3)$ berderajat paling tinggi 3. Q disebut *spherical 3-design* dalam bola satuan $S^2 \subseteq \mathbb{R}^3$. Contoh kubus Q di atas membawa kita pada gagasan tentang *spherical designs*.

3.1 Teori Spherical Designs

Konsep *spherical design* dapat dipandang sebagai analogi kontinu (*continuous analogue*) dari konsep desain kombinatorial. Secara informal, pertanyaan kita dapat kita formulasikan sebagai berikut. Apakah subhimpunan hingga yang baik untuk mengaproksimasi sebuah bola satuan sebagai keseluruhan. Kita akan definisikan bola yang kita maksud di bawah nanti. Bola satuan yang kita maksud adalah himpunan yang kita definisikan sebagai

$$S^{n-1} := \{(x_1, x_2, \dots, x_n) : x_1^2 + x_2^2 + \dots + x_n^2 = 1\}.$$

Secara formal, *spherical design* kita definisikan seperti di bawah ini.

Definisi (Spherical t-design) Himpunan hingga $X \subseteq S^{n-1}$ disebut **spherical t-design** jika memenuhi persamaan

$$\frac{1}{|S^{n-1}|} \int_{S^{n-1}} f(\mathbf{x}) d\sigma(\mathbf{x}) = \frac{1}{|X|} \sum_{\mathbf{x} \in X} f(\mathbf{x}),$$

untuk setiap polinom $f(\mathbf{x}) = f(x_1, x_2, \dots, x_n)$ berderajat kurang dari atau sama dengan t , dengan $|S^{n-1}|$ menyatakan luas permukaan bola S^{n-1} .

Definisi di atas menunjukkan bahwa X merupakan sebuah *spherical t-design* jika nilai dari integral permukaan atas bola satuan atas sebarang

polinom berderajat kurang dari atau sama dengan t , setelah dibagi dengan luas permukaan bola satuan tersebut, dapat dihitung secara eksak sebagai rata-rata dari nilai polinom tersebut di setiap di X . Dalam hal ini, kita katakan bahwa X adalah himpunan hingga yang dapat mengaproksimasi bola satuan S^{n-1} secara baik. Parameter t pada *spherical t-designs* disebut *strength* dan merupakan parameter yang sangat penting bagi suatu desain.

Spherical design pertama kali diperkenalkan oleh tiga kombinatorialis terkemuka di dunia, Delsarte, Goethals, dan Seidel pada tahun 1977¹² sebagai versi kontinu dari konsep desain kombinatorial yang sudah ada sebelumnya. Untuk melihat keserupaan konsep tersebut, bandingkanlah ekspresi matematis pada kedua definisi *spherical design* dan desain kombinatorial.

Erat kaitannya dengan konsep *spherical design* adalah konsep *distance set*. Misalkan $X \subseteq S^{n-1}$ adalah himpunan hingga tak kosong. Definisikan himpunan

$$A(X) = \{\langle x, y \rangle : x, y \in X, x \neq y\},$$

dengan $\langle x, y \rangle$ adalah perkalian dalam Euclides. Himpunan X disebut *s-distance set* jika $|A(X)| = s$.

Mudah dibuktikan bahwa gabungan dari *spherical design* adalah juga *spherical design*. Karena itu tidak ada batas atas dari kardinalitas suatu himpunan hingga agar membentuk *spherical design*. Dan perhatian para peneliti beralih kepada batas bawah dari kardinalitas suatu himpunan hingga yang merupakan *spherical design*. Di antara hasil-hasil penting dari Delsarte, Goethals, dan Seidel ini adalah dua teorema berikut.

Teorema 3.1 (Delsarte-Goethals-Seidel, 1977) *Pernyataan-pernyataan di bawah ini berlaku.*

1. Jika X adalah **spherical t-design** dalam bola satuan S^{n-1} , maka

$$|X| \geq \binom{n-1 + \left\lceil \frac{t}{2} \right\rceil}{\left\lceil \frac{t}{2} \right\rceil} + \binom{n-2 + \left\lceil \frac{t}{2} \right\rceil}{\left\lceil \frac{t}{2} \right\rceil - 1}.$$

2. Jika X adalah **s-distance set** dalam bola satuan S^{n-1} , maka

$$|X| \leq \binom{n-1+s}{s} + \binom{n-2+s}{s-1}.$$

¹² P. Delsarte, G.-M. Goethals, and J.J. Seidel, (1977), "Spherical codes and designs," *Geom. Dedicata* **6**, 363-388.

3. Jika X adalah **spherical t -design** sekaligus juga **s – distance set** dalam bola satuan S^{n-1} , maka

$$t \leq 2s.$$

4. Jika X adalah himpunan dalam bola satuan S^{n-1} yang memenuhi hipotesis dan juga memenuhi persamaan dari salah satu dari pernyataan-pernyataan (1), (2), (3), maka persamaan dalam dua pernyataan sisanya juga dipenuhi oleh X . Jika ini terjadi, maka t merupakan bilangan genap dan $t = 2s$. (Dalam hal ini X kita katakan **tight spherical $2s$ -design**).

Untuk himpunan $X \subseteq S^{n-1}$ yang *antipodal*, yakni bersifat $X = -X$, Delsarte, Goethals, dan Seidel juga membuktikan teorema berikut.

Teorema 3.2 (Delsarte-Goethals-Seidel, 1977) Pernyataan-pernyataan di bawah ini berlaku.

1. Jika X adalah **antipodal spherical t -design** dalam bola satuan S^{n-1} , maka

$$|X| \geq 2 \cdot \binom{n-1 + \left\lfloor \frac{t}{2} \right\rfloor}{\left\lfloor \frac{t}{2} \right\rfloor}.$$

2. Jika X adalah **antipodal s – distance set** dalam bola satuan S^{n-1} , maka

$$|X| \leq 2 \cdot \binom{n-2+s}{s-1}.$$

3. Jika X adalah **antipodal spherical t -design** sekaligus juga **s – distance set** dalam bola satuan S^{n-1} , maka

$$t \leq 2s - 1.$$

4. Jika X adalah himpunan antipodal dalam bola satuan S^{n-1} yang memenuhi hipotesis dan juga memenuhi persamaan dari salah satu dari pernyataan-pernyataan (1), (2), (3), maka persamaan dalam dua pernyataan sisanya juga dipenuhi oleh X . Jika ini terjadi, maka t merupakan bilangan ganjil dan $t = 2s - 1$. (Dalam hal ini X kita katakan **antipodal tight spherical $(2s - 1)$ -design**).

Dua teorema di atas menunjukkan bahwa *tight spherical designs* maupun *tight distance sets* adalah dua objek ekstremal.

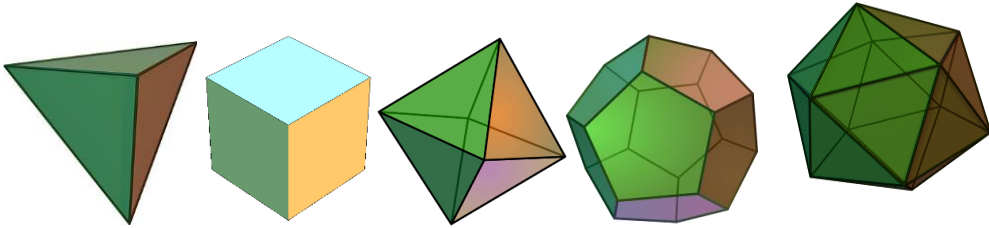
Berikut adalah beberapa contoh sederhana dari *spherical designs*.

1. n –gon regular pada bola satuan $S^1 \subseteq \mathbb{R}^2$ adalah *spherical t – design*, untuk $1 \leq t \leq n - 1$.
2. *Spherical designs* pada bola satuan $S^2 \subseteq \mathbb{R}^3$.

Tabel 1 Contoh-contoh spherical designs $\mathbb{R}^3$

No.	X	X	Strength t
1.	Tetrahedron regular	4	2
2.	Kubus	8	3
3.	Oktahedron regular	6	3
4.	Dodekahedron regular	20	5
5	Ikosahedron regular	12	5

Gambar dari kelima *spherical designs* tersebut di atas adalah demikian.



Gambar 2 Dari kiri ke kanan berturut-turut adalah tetrahedron regular, kubus, oktahedron regular, dodekahedron regular, okisahedron regular.

Eksistensi *spherical designs* telah dibuktikan sekitar 40 tahun lalu oleh Seymour dan Zaslavsky (Seymour dan Zaslavsky, 1984).

Teorema 3.3 (Seymour-Zaslavsky, 1984) Terdapat *spherical t-designs* X pada bola satuan $S^n \subseteq \mathbb{R}^{n+1}$, untuk sembarang t dan n dan kardinalitas $|X|$ yang cukup besar.

Teorema Seymour-Zaslavsky ini sangat penting dalam kajian tentang *spherical designs*. Kita deskripsikan secara agak detail algoritma pembuktian teorema tersebut di atas.

Misalkan Ω adalah ruang topologis lintasan-terhubung dengan ukuran hingga positif μ yang memenuhi $\mu(S) \geq 0$, untuk setiap himpunan terukur S dan $\mu(U) > 0$, untuk setiap himpunan buka tak-kosong U . Misalkan $f_1, f_2, \dots, f_m: \Omega \rightarrow \mathbb{R}^p$ adalah fungsi-fungsi kontinu dan terintegralkan. Himpunan rata-rata dari $f_1, f_2, \dots, f_m$ adalah subhimpunan hingga $X \subseteq \Omega$ yang untuk setiap bilangan bulat $j \in [1, m]_{\mathbb{Z}}$ memenuhi persamaan

$$\frac{1}{\mu(\Omega)} \int_{\Omega} f_j d\mu = \frac{1}{|X|} \sum_{u \in X} f_j(u).$$

Seymour-Zaslavsky membuktikan sifat berikut.

Teorema 3.4 (Seymour-Zaslavsky, 1984) Misalkan Ω, μ , dan $f_1, f_2, \dots, f_m$ seperti yang tertulis di atas. Maka himpunan rata-rata X dari fungsi-fungsi $f_1, f_2, \dots, f_m$ dijamin adanya. Kardinalitas dari X dapat bernilai sama dengan sembarang bilangan positif, dengan sejumlah hingga pengecualian. Lebih dari itu, himpunan X dapat dipilih sehingga vektor-vektor dalam himpunan $\{f_1(u), f_2(u), \dots, f_m(u)\}$, untuk $u \in X$, semuanya berbeda.

Jika kita memilih himpunan $\Omega = S^{n-1}$ dengan ukuran Haar σ , dan kita pilih sebuah himpunan basis $\{f_1, f_2, \dots, f_m\}$ dari $P_t(S^{n-1})$, maka himpunan rata-rata X menjadi *spherical t -design*.

Meski bukti eksistensi *spherical design* dengan sembarang parameter telah diberikan oleh Seymour-Zaslavsky lebih dari 40 tahun lalu, tetapi bukti yang mereka berikan sangatlah sulit dan tidak konstruktif. Karena itu bukti alternatif terkait dengan eksistensi *spherical designs* ini masih menanti untuk diselesaikan.

Masalah terbuka 3.5: Berikan bukti alternatif (dan jika memungkinkan bersifat konstruktif dan lebih mudah) untuk eksistensi **spherical designs** dengan sembarang parameter.

Seperti telah disampaikan di atas, bukti dari Seymour-Zaslavsky tentang eksistensi *spherical design* itu tidak konstruktif. Teorema itu hanya membuktikan eksistensi *spherical design* tanpa memberikan metode untuk mengonstruksi *spherical design* tersebut. Karena itu masalah bagaimana mengonstruksi *spherical design* adalah tantangan tersendiri yang perlu diselesaikan.

3.1.1 Konstruksi Spherical Designs

Masalah utama yang akan kita diskusikan di sini adalah sebagai berikut.

Masalah utama: Untuk sembarang bilangan bulat positif t dan d , berikankah metode konstruksi eksplisit dari *spherical t -designs* pada bola satuan S^d .

Masalah ini dapat kita reduksi menjadi masalah eksistensi *interval t -designs* dengan fungsi bobot Gegenbauer untuk integral seperti berikut.

Misalkan $w_\alpha(x) := (1 - x^2)^\alpha$, dengan $\alpha = \frac{d-2}{2}$, adalah fungsi bobot Gegenbauer pada interval $[-1, 1]$.

$X = \{x_1, x_2, \dots, x_M\}$ merupakan *interval t-design* pada $[-1,1]$ terhadap fungsi bobot $w_\alpha(x)$, jika persamaan di bawah ini dipenuhi

$$\frac{1}{\int_{-1}^1 w_\alpha(x) dx} \int_{-1}^1 f(x) w_\alpha(x) dx = \frac{1}{|X|} \sum_{x \in X} f(x),$$

untuk sembarang polinom $f(x)$ berderajat kurang dari atau sama dengan t .

Selanjutnya, untuk setiap $i \in [1, M]_{\mathbb{Z}}$, misalkan S_i menyatakan bola satuan dalam ruang Euclides $\mathbb{R}^d$ dengan radius $\sqrt{1 - x_i^2}$ dan berpusat di titik $(x_i, 0, 0, \dots, 0) \in \mathbb{R}^{d+1}$, dengan koordinat pertama adalah x_i . Maka seluruh bola S_i terletak pada bola satuan S^d .

Sekarang, untuk setiap $i \in [1, M]_{\mathbb{Z}}$, misalkan X_i menyatakan *spherical t-design* pada bola S_i . Kita asumsikan bahwa $|X_i| = K$, untuk setiap $i \in [1, M]_{\mathbb{Z}}$. Maka,

$$\bigcup_{i=1}^M X_i$$

merupakan *spherical t-design* dengan kardinalitas $K \times M$ dalam bola satuan S^d . Secara formal, konstruksi *spherical designs* dengan cara seperti ini dibuktikan oleh Rabau dan Bajnok pada tahun 1991.

Teorema 3.6 (Rabau-Bajnok, 1991) Misalkan $Y \subseteq S^{d-1}$ *spherical t-design* dan misalkan $V \subseteq [-1,1]$ *interval t-design* pada interval $[-1,1]$ terhadap fungsi bobot $w_\alpha(x) := (1 - x^2)^\alpha$, dengan $\alpha = \frac{d-2}{2}$. Maka himpunan

$$X := \left\{ \left(y\sqrt{(1 - v^2)}, v \right) : y \in Y, v \in V \right\}$$

merupakan *spherical t-design* pada bola satuan S^d .

Salah satu konstruksi *spherical designs* eksplisit terbaru diberikan oleh Gerg Kuperberg (2005).

Teorema 3.7 (Kuperberg, 2005) 2^s titik berbentuk $\pm z_1 \pm z_2 \pm \dots \pm z_s$ membentuk formula kuadratur tipe-**Chebyshev** berderajat $(2s + 1)$ pada interval $[-1,1]$ dengan bobot konstan jika dan hanya jika $\sqrt{z_i}$ adalah akar-akar dari polinom.

$$Q(x) = x^s - \frac{x^{s-1}}{3} + \frac{x^{s-2}}{45} - \cdots + \frac{(-1)^s}{1 \cdot 3 \cdot 15 \cdots (4^s - 1)}.$$

Untuk selanjutnya, himpunan 2^s titik berbentuk $\pm z_1 \pm z_2 \pm \cdots \pm z_s$ dalam Teorema 3.7 di atas kita sebut saja **himpunan Kuperberg**.

Dengan menerapkan Teorema Rabau-Bajnok, Kuperberg sesungguhnya telah mengonstruksi *spherical designs* untuk sembarang *strength* ganjil $(2s + 1)$ pada bola satuan $S^2 \subseteq \mathbb{R}^3$. Empat tahun kemudian, dalam sebuah artikel surveinya, (Bannai-Bannai, 2009) meyakini bahwa metode Kuperberg dapat diperumum untuk mengonstruksi *spherical designs* dengan sembarang *strength* ganjil di ruang Euclides yang lebih besar.

Masalah terbuka 3.8 (Bannai-Bannai, 2009): *Gunakan metode Kuperberg untuk mengonstruksi **spherical designs** dengan sembarang **strength** $(2k + 1)$ pada bola satuan $S^{d-1} \subseteq \mathbb{R}^d$, untuk $d \geq 4$.*

Percobaan pertama, dan satu-satunya sejauh ini, untuk menjawab tantangan Bannai dan Bannai telah kami lakukan secara parsial bersama Muhammad Samy Baladram¹³. Observasi yang kami lakukan pada dasarnya bersifat numerik. Berikut adalah hasil-hasil yang kami peroleh terkait dengan konstruksi *spherical designs* dengan menggunakan metode yang ditemukan oleh Kuperberg.

Teorema 3.9 (Baladram-Suprijanto, 2014) *Misalkan s bilangan bulat positif dan $\mathbf{a} = (a_1, a_2, \dots, a_s) \in \mathbb{R}^s$. Misalkan Y adalah himpunan Kuperberg dengan 2^s titik berbentuk $\pm a_1 \pm a_2 \pm \cdots \pm a_s$. Maka himpunan Kuperberg Y membentuk **interval 3-desain** pada interval $[-1, 1]$ terhadap fungsi bobot Gegenbauer $w(x) := (1 - x^2)^{\frac{d-2}{2}}$ jika dan hanya jika $\|\mathbf{a}\| = \frac{1}{\sqrt{d+1}}$.*

Berdasarkan teorema di atas kita peroleh akibat di bawah ini.

Akibat 3.10 (Baladram-Suprijanto, 2014) *Misalkan Y adalah **tight spherical 3-design** pada bola satuan S^{d-1} . Maka berlaku:*

¹³ Muhammad Samy Baladram, Ph.D. menyelesaikan masalah ini dalam tugas akhirnya di Program Studi Matematika, Program Sarjana, di bawah bimbingan saya. Kini yang bersangkutan adalah Assistant Professor di Tohoku University, Sendai, Jepang.

1. himpunan

$$Y' = \left\{ \left(y \sqrt{1 - \frac{1}{d+1}}, \pm \frac{1}{\sqrt{d+1}} \right) : y \in Y \right\}$$

merupakan **tight spherical 3-design** pada bola satuan S^d .

2. himpunan

$$Y' = \left\{ \left(y \sqrt{1 - (\pm a \pm a)^2}, \pm a \pm a \right) : a = \frac{1}{2} \sqrt{\frac{2}{d+1}} \text{ dan } y \in Y \right\}$$

merupakan **spherical 3-design** pada bola satuan S^d .

Teorema 3.11 (Baladram-Suprijanto, 2014) Himpunan Y yang terdiri atas 2^2 titik berbentuk $\pm a_1 \pm a_2$, dengan $a_i > 0$, yang memenuhi **interval 5-design** pada selang $[-1,1]$ terhadap bobot Gegenbauer

$$w(x) := (1 - x^2)^{\frac{d-2}{2}}$$

eksis hanya untuk $d = 1, 2$, atau 3 .

Secara eksperimental, kami juga membuktikan syarat perlu dan syarat cukup bagi himpunan Kuperberg untuk membentuk **interval 5-design** seperti berikut.

Teorema 3.12 (Baladram-Suprijanto, 2014) Himpunan Kuperberg Y yang terdiri atas 2^3 titik berbentuk $\pm \sqrt{z_1} \pm \sqrt{z_2} \pm \sqrt{z_3}$ membentuk **interval 5-design** pada selang $[-1,1]$ terhadap bobot Gegenbauer

$$w(x) := (1 - x^2)^{\frac{d-2}{2}}$$

jika dan hanya jika z_i merupakan akar-akar dari persamaan

$$Q(x) = x^3 - \frac{x^3}{d+1} + \frac{dx}{2(d+1)^2(d+3)} - p$$

dengan p adalah bilangan real yang terletak pada selang buka

$$\left(\frac{18d^2 - 27d + 5d^3 + \sigma_2 - 108}{\sigma_1}, \frac{27d - 18d^2 - 5d^3 + \sigma_2 + 108}{\sigma_1} \right)$$

dan $\sigma_1 = 54d^6 + 648d^5 + 3078d^4 + 7344d^3 + 9234d^2 + 5832d + 1458$,

$$\sigma_2 = \sqrt{2} (d + 3)^{\frac{3}{2}} \sqrt{-d^3 + 18d^2 - 108d + 216}.$$

Lebih dari itu, interval 5-design ini eksis hanya untuk $d \in [1, 6]_{\mathbb{Z}}$.

Analog dengan yang terjadi pada *interval 5-design*, kami juga berhasil membuktikan hal serupa untuk *interval 7-design*.

Teorema 3.13 (Baladram-Suprijanto, 2014) Himpunan Y yang terdiri atas 2^3 titik berbentuk $\pm a_1 \pm a_2 \pm a_3$, dengan $a_i > 0$, yang memenuhi **interval 7-design** pada selang $[-1, 1]$ terhadap bobot Gegenbauer

$$w(x) := (1 - x^2)^{\frac{d-2}{2}}$$

eksis hanya untuk $d = 1$ atau 2 .

Sekali lagi, secara eksperimental, kami juga membuktikan syarat perlu dan syarat cukup bagi himpunan Kuperberg untuk membentuk *interval 7-design* seperti berikut.

Teorema 3.14 (Baladram-Suprijanto, 2014) Himpunan Kuperberg Y yang terdiri atas 2^4 titik berbentuk $\pm \sqrt{z_1} \pm \sqrt{z_2} \pm \sqrt{z_3} \pm \sqrt{z_4}$ membentuk **interval 7-design** pada selang $[-1, 1]$ terhadap bobot Gegenbauer

$$w(x) := (1 - x^2)^{\frac{d-2}{2}}$$

jika dan hanya jika z_i merupakan akar-akar dari persamaan

$$Q(x) = x^4 - \frac{x^3}{d+1} + \frac{dx^2}{2d^3 + 10d^2 + 14d + 6} - \frac{(d^2 - d)x}{6d^5 + 66d^4 + 252d^3 + 420d^2 + 318d + 90} + p$$

dengan p adalah bilangan real yang terletak pada selang buka seperti tertulis pada tabel di bawah ini:

d	p
2	(0, 0.000001628808061)
3	(0.000001440015579, 0.000002166860188)
4	(0.000001923319464, 0.000001951463832)

Lebih dari itu, secara eksperimental kami juga melakukan observasi terkait dengan bagaimana mengonstruksi *interval design* dengan

menggunakan himpunan Kuperberg, yakni bagaimana akar-akar dari persamaan

$$x^s - a_1x^{s-1} + a_2x^{s-2} - a_3x^{s-3} + \dots + (-1)^{s-1}a_{s-1}x + (-1)^sa_s = 0$$

dapat menjadi *interval t-design*. Semua akar dari persamaan di atas haruslah bilangan real. Tetapi, untuk *strength* dan dimensi ruang Euclides yang besar, persamaan di atas memiliki solusi berupa bilangan kompleks, yang tentu tidak kita inginkan. Untuk mengatasi hal itu, kita melakukan manipulasi terhadap persamaan di atas dengan memperluasnya menjadi

$$x^{s+k} - a_1x^{s-1+k} + \dots + (-1)^{s-1}a_{s-1}x^{k-1} + (-1)^{s-1}p_1x^{k-1} + \dots + (-1)^{s+k-1}p_{k-1}x + (-1)^{s+k}p_k = 0.$$

Himpunan solusi dari persamaan di atas memberikan *spherical* $(2s + 1)$ -*design* dengan 2^{s+k} titik. Karena semua nilai dari a_i telah diketahui, maka kita harus mencari cara untuk memilih p_i , dengan $0 < p_i < 1$, sehingga akar dari persamaan di atas seluruhnya merupakan bilangan real. Dengan memanfaatkan Teorema Sturm¹⁴, kita sampai pada kesimpulan bahwa untuk setiap dimensi d , terdapat bilangan bulat positif $k \leq s$ sehingga akar-akar dari persamaan terakhir di atas membentuk *interval* $(2s + 1)$ -*design* dengan 2^{s+k} titik. Akibatnya, kita peroleh *spherical designs* dengan parameter seperti diberikan pada tabel berikut.

Tabel 2 *Spherical t-design* pada bola satuan $S^{d-1} \subseteq \mathbb{R}^d$

	<i>t</i>						
<i>d</i>	3	5	7	9	11	13	15
2	2	2^2	2^3	2^4	2^5	2^6	2^7
3	2	2^2	2^4	2^5			
4	2	2^3	2^4	2^5			
5	2^3						
6	2^3						
7							
8							

Observasi eksperimental di atas membawa kita pada konjektur (dugaan) berikut.

Konjektur 3.14 (Bannai-Baladram-Suprijanto, 2023) Untuk setiap bilangan bulat positif d dan s , terdapat himpunan Kuperberg yang terdiri atas 2^{s+k} titik, untuk $k \leq s$, membentuk **interval** $(2s + 1)$ -**design** terhadap bobot Gegenbauer.

¹⁴ C5 Yap, Fundemental Problems in Algorithmic Algebra, Oxford University Press, 20060.

Masalah terbuka 3.15 *Terkait dengan Konjektur di atas, tunjukkan eksistensi himpunan Kuperberg yang membentuk **interval** $(2s + 1)$ -**design** terhadap bobot **Gegenbauer** yang terdiri atas 2^{s+k} titik, untuk $k = k(s)$ (artinya, tidak harus $k \leq s$).*

3.2 Perumuman *Spherical Designs*

Ada setidaknya dua arah perumuman dari konsep *spherical designs*: (1) dengan mengganti ruang Euclides $\mathbb{R}^n$ dengan ruang simetrik kompak lainnya; atau (2) dengan mengganti bola satuan S^{n-1} dengan sejumlah hingga bola konsentrik. Perluasan dalam arah pertama membawa kita pada konsep desain dalam ruang simetrik kompak, sementara perluasan dalam arah kedua membawa kita kepada gagasan *Euclidean designs*. Kita akan deskripsikan perluasan dalam arah pertama secara ringkas dan perluasan dalam arah kedua secara agak mendalam.

3.2.1 Desain dalam Ruang Simetrik Kompak

Ada beberapa perluasan dari konsep *spherical designs*, yang sebelumnya didefinisikan pada bola satuan di ruang Euclides, ke ruang-ruang lainnya seperti ruang projektif, ruang Grassmann, dan mungkin pula pada ruang hiperbolik.

3.2.1.1 Desain pada Ruang Simetrik Kompak dengan Rank 1

Sebelum mengkaji *spherical codes* dan *spherical designs* pada tahun 1977, dua tahun sebelumnya Delsarte, Goethals, dan Seidel¹⁵ telah lebih dahulu mengkaji sistem garis pada ruang $\mathbb{R}^n$ dan ruang $\mathbb{C}^n$. Karena garis di ruang $\mathbb{R}^n$ dan ruang $\mathbb{C}^n$ dapat dipandang sebagai titik dalam ruang projektif atas $\mathbb{R}$ dan $\mathbb{C}$, maka kita dapat memandang bahwa artikel Delsarte, Goethals, dan Seidel tersebut mengkaji subhimpunan hingga dalam suatu ruang projektif.

Telah diketahui bahwa bola satuan S^{n-1} merupakan salah satu ruang simetrik kompak dengan rank 1. Klasifikasi lengkap dari ruang simetrik kompak dengan rank 1 telah diketahui, dan terdiri atas:

¹⁵ P. Delsarte, G.-M. Goethals, and J.J. Seidel, (1975), "Bounds for systems of lines and Jacobi polynomials," *Philips Research Reports* **30**, Boukamp Volume 91*-105*.

1. S^{n-1} , dan
2. ruang projektif $P^{n-1}(\mathbb{R})$, dengan $\mathbb{R}$ himpunan bilangan real,
3. ruang projektif $P^{n-1}(\mathbb{C})$, dengan $\mathbb{C}$ himpunan bilangan kompleks,
4. ruang projektif $P^{n-1}(\mathbb{H})$, dengan $\mathbb{H}$ himpunan quaternion,
5. ruang projektif $P^{n-1}(\mathbb{O})$, dengan $\mathbb{O}$ himpunan oktonion.

Banyak teori yang berlaku di ruang bola satuan S^{n-1} juga berlaku di ruang-ruang projektif tersebut di atas. Kajian tentang teori desain dalam ruang-ruang projektif tersebut telah mulai dilakukan oleh Bannai dan Hoggar dalam beberapa karya mereka (Hoggar, 1982), (Hoggar, 1984), (Bannai-Hoggar, 1985), (Bannai-Hoggar, 1989), (Hoggar, 1990). Hingga saat ini, perkembangan di sekitar kajian ini masih sangat lambat dan menanti kontribusi dari banyak pihak.

3.2.1.2 Design pada Ruang Simetrik Kompak dengan Rank > 1

Perluasan atas konsep *spherical designs* juga telah dilakukan pada ruang simetrik kompak dengan rank lebih dari 1. Salah satu ruang tersebut adalah yang disebut ruang Grassmann. Konsep *t-designs* dalam ruang Grassmann diperkenalkan oleh (Bachoc, Coulangenon, dan Nebe, 2002). Sifat-sifat dasar tentang desain dalam ruang Grassmann tersebut juga telah mereka kaji. Sifat-sifat lanjut dari *t-designs* dalam ruang Grassmann ini telah dikaji juga oleh (Bachoc, Bannai, dan Coulangenon, 2004). Meski demikian, masalah klasifikasi lengkap atas *tight t-designs* dalam ruang Grassmann ini masih merupakan masalah terbuka hingga kini.

3.2.2 Euclidean Designs

Sebagai perumuman atas konsep *spherical t-designs* dalam arah kedua, (Neumaier dan Seidel, 1988) dan (Delsarte dan Seidel, 1989) mendefinisikan apa yang mereka namakan *Euclidean t-designs*. Jika *spherical t-designs* meninjau himpunan hingga titik yang terletak pada sebuah bola satuan konsentrik, maka *Euclidean t-designs* meninjau himpunan hingga titik yang terletak pada sejumlah hingga bola konsentrik.

Misalkan $X \subseteq \mathbb{R}^n$ adalah himpunan hingga. Misalkan $\{\|u\|: u \in X\} = \{r_1, r_2, \dots, r_p\}$. Untuk $i \in [1, p]_{\mathbb{Z}}$, misalkan $S_i := \{x \in \mathbb{R}^n: \|x\| = r_i\}$ adalah bola berjari-jari r_i , dan misalkan pula $X_i = X \cap S_i$. Misalkan $w: X \rightarrow \mathbb{R}^+$ adalah

fungsi bobot, dengan $w(X_i) = \sum_{x \in X_i} w(x)$. Himpunan hingga berbobot (X, w) adalah *Euclidean t-design* jika persamaan

$$\sum_{i=1}^p \frac{w(X_i)}{|S_i|} \int_{S_i} f(x) d\sigma(x) = \sum_{x \in X} w(x) f(x)$$

dipenuhi untuk semua polinom $f(x)$ berderajat kurang dari atau sama dengan t .

Neumaier dan Seidel (1988) juga membuktikan kondisi yang ekuivalen dengan definisi *Euclidean t-design* yang dalam banyak hal sangat memudahkan kita dalam kalkulasi.

Teorema 3.16 (Neumaier-Seidel, 1988) Misalkan (X, w) adalah himpunan hingga berbobot dalam $\mathbb{R}^n$. Maka pernyataan-pernyataan berikut ekuivalen.

1. (X, w) adalah *Euclidean t-design*.
2. $\sum_{x \in X} w(x) \|x\|^{2j} \varphi(x) = 0$ dipenuhi untuk setiap bilangan bulat $l \in [1, t]_{\mathbb{Z}}$ dan $j \in \left[1, \left\lfloor \frac{t-1}{2} \right\rfloor\right]_{\mathbb{Z}}$, dan $\varphi \in \text{Harm}_l(\mathbb{R}^n)$.
3. Setiap momen dari X berderajat kurang dari atau sama dengan t invarian terhadap setiap transformasi orthogonal.

Seperti dalam kasus *spherical designs*, gabungan dari dua *Euclidean design* adalah juga *Euclidean design*, sehingga para peneliti memberikan perhatian pada batas bawah dari kardinalitas himpunan hingga agar membentuk *Euclidean design*. Batas bawah yang natural untuk itu telah ditemukan oleh Moller (1979).

Teorema 3.17 (Moller, 1979) Misalkan (X, w) adalah **Euclidean t-design**. Maka berlaku dua pernyataan di bawah ini.

1. Jika $t = 2e$, maka $|X| \geq \dim(P_e(S))$.
2. Jika $t = 2e + 1$, maka $|X| \geq \begin{cases} 2 \dim(P_e^*(S)), & \text{jika } e \text{ genap dan } 0 \in X \\ 2 \dim(P_e^*(S)), & \text{jika tidak demikian.} \end{cases}$

Jika *Euclidean t-designs* (X, w) mencapai batas bawah dalam teorema di atas, dan $\dim(P_e(S)) = \dim(P_e(\mathbb{R}^n))$ atau $\dim(P_e^*(S)) = \dim(P_e^*(\mathbb{R}^n))$, maka (X, w) dikatakan *tight Euclidean t-designs*.

Jika dalam kasus *spherical design*, Delsarte, Goethal, dan Seidel (1977) telah membuktikan bahwa *spherical design* tertentu memiliki struktur skema asosiasi polinom- Q , maka *Euclidean design* -yang merupakan perumuman dari *spherical design*- juga memiliki hubungan dengan konfigurasi koheren -yang merupakan perumuman dari skema asosiasi. Bannai dan Bannai telah membuktikan kedua sifat di bawah ini.

Teorema 3.18 (Bannai-Bannai, 2010) Misalkan (X, w) adalah **Euclidean t -design**. Misalkan fungsi bobot $w(x)$ bernilai konstan pada setiap bola konsentrik X_k , dengan $k \in [1, p]_{\mathbb{Z}}$, dan $s_{i,k} + s_{k,j} \leq t - 2(p - 2)$, untuk setiap $i, j, k \in [1, p]_{\mathbb{Z}}$. Maka X memiliki struktur sebagai konfigurasi koheren.

Teorema 3.19 (Bannai-Bannai, 2010) Misalkan (X, w) adalah **antipodal Euclidean t -design**. Misalkan fungsi bobot $w(x)$ bernilai konstan pada setiap bola konsentrik X_k , dengan $k \in [1, p]_{\mathbb{Z}}$, dan $s_{i,k} + s_{k,j} - \delta_{i,k} - \delta_{k,j} \leq t - 2(p - 2)$, untuk setiap $i, j, k \in [1, p]_{\mathbb{Z}}$. Maka X memiliki struktur sebagai konfigurasi koheren.

Catatan: Telah dibuktikan bahwa fungsi bobot untuk *tight Euclidean design* pada p bola konsentrik bernilai konstan untuk setiap bola konsentrik X_k .

Mudah untuk diperiksa bahwa jika (X, w) adalah Euclidean t -design, maka (X', w') adalah juga Euclidean t -design, dengan $X' = \{ax : x \in X\}$ dan $w'(ax) = \lambda w(x)$, untuk $x \in X$ dan $a, \lambda > 0$.

3.2.2.1 Eksistensi Euclidean designs

Berbeda dengan *spherical design*, sejak pertama kali diperkenalkan oleh Neumaier dan Seidel (1988) (juga Delsarte dan Seidel (1989)), eksistensi *Euclidean designs*, khususnya eksistensi *tight Euclidean design*, diyakini tidak ada selain yang trivial saja.

Konjektur 3.20 (Delsarte-Neumaier-Seidel, 1988-1989) Tidak ada **tight Euclidean $2e$ -designs**, untuk $e \geq 2$, selain simpleks regular.

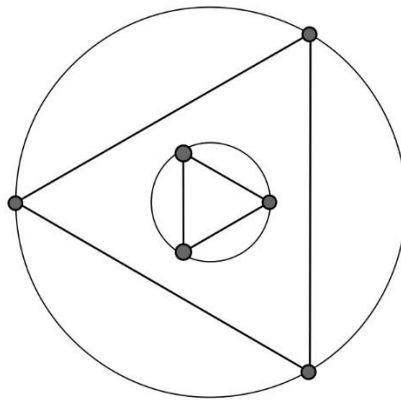
Konjektur Delsarte-Neumaier-Seidel ini membuat penelitian di bidang *Euclidean designs* tidak berkembang dan bahkan terhenti. Hingga sebelum tahun 2006, artikel terkait dengan topik *Euclidean design* praktis hanya ada dua saja, yaitu artikel yang ditulis oleh (Neumaier dan Seidel, 1988) yang terbit pada 1988 dan yang ditulis oleh (Delsarte dan Seidel, 1989) yang terbit setahun

setelahnya, pada 1989. Konjektur Delsarte-Neumaier-Seidel ini “bertahan” lebih dari limabelas tahun, hingga pada tahun 2006 (Bannai dan Bannai, 2006) memberikan contoh penyangkal atas konjektur tersebut.

Contoh penyangkal atas konjektur Delsarte-Neumaier-Seidel: Tinjaulah himpunan $X = X_1 \cup X_2$, dengan

- $X_1 = \left\{ (1,0), \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right), \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) \right\}$,
- $X_2 = \left\{ (-r, 0), \left(\frac{r}{2}, \frac{\sqrt{3}r}{2}\right), \left(\frac{r}{2}, -\frac{\sqrt{3}r}{2}\right) \right\}$,
- Fungsi bobot $w(x) = \begin{cases} 1, & x \in X_1, \\ \frac{1}{r^3}, & x \in X_2. \end{cases}$

Jika $r \neq 1$, maka X merupakan *tight Euclidean 4-design*.



Gambar 3 *Tight Euclidean 4-design* dalam $\mathbb{R}^2$

Karya (Bannai dan Bannai, 2006) ini membangkitkan kembali minat para peneliti di bidang kombinatorika aljabar, khususnya *Euclidean designs*, dan menandai semangat baru dalam penelitian di bidang ini. Pertanyaan yang muncul secara logis adalah, bagaimana dengan *eksistensi tight Euclidean designs* dengan *strength* ganjil. Jika eksistensinya dijamin, pertanyaan berikutnya adalah bagaimana dengan konstruksi contoh-contoh eksplisitnya, juga bagaimana dengan klasifikasi lengkapnya? Untuk menjawab hal ini, kami (Bannai, Bannai, dan Suprijanto, 2007) memperkenalkan gagasan tentang rigiditas dari *Euclidean designs*.

3.2.2.2 Rigiditas dari *Euclidean Designs*

Konsep rigiditas dari *Euclidean designs* terinspirasi dari konsep serupa yang telah diperkenalkan sebelumnya oleh Bannai (Bannai, 1987) untuk *spherical designs*. *Spherical t-design* dikatakan non-rigid jika tidak dapat dideformasi secara lokal dan tetap mempertahankan strukturnya sebagai *spherical t-design*.

Definisi (Non-rigid spherical designs) *Spherical t-design* $X := \{\mathbf{x}_i: 1 \leq i \leq N\} \subseteq S^{n-1}$ dikatakan **non-rigid** atau dapat dideformasi dalam ruang $\mathbb{R}^n$ jika untuk setiap $\epsilon > 0$ terdapat *spherical t-design* lain, katakanlah $Y := \{\mathbf{y}_i: 1 \leq i \leq N\} \subseteq S^{n-1}$, sehingga kedua kondisi di bawah dipenuhi:

1. Untuk setiap $i \in [1, N]_{\mathbb{Z}}$ berlaku $\|\mathbf{x}_i - \mathbf{y}_i\| < \epsilon$; dan
2. Tidak terdapat transformasi ortogonal $g \in O(n)$ yang memenuhi $g(\mathbf{x}_i) = \mathbf{y}_i$, untuk setiap $i \in [1, N]_{\mathbb{Z}}$.

Dimotivasi oleh definisi di atas, pada 2007 kami memperkenalkan konsep rigiditas untuk *Euclidean designs* yang bergantung kepada grup yang dibangun oleh transformasi ortogonal, *scaling*, dan juga *adjustment* pada fungsi bobot. Kita gunakan notasi $O^*(n) = \langle O(n), g_\lambda, g^\mu \rangle$ untuk grup yang dibangun oleh grup ortogonal $O(n)$, *scaling* g_λ pada X dan *adjustment* g^μ pada fungsi bobot yang didefinisikan berturut-turut sebagai berikut:

$$\begin{cases} g_\lambda: (X, w) \ni \mathbf{x} \rightarrow \mathbf{x}' = \lambda \mathbf{x} \in (X', w'), \\ w'(\mathbf{x}') = w(\mathbf{x}). \end{cases}$$

$$\begin{cases} g^\mu: (X, w) \ni \mathbf{x} \rightarrow \mathbf{x}' = \mathbf{x} \in (X', w'), \\ w'(\mathbf{x}') = \mu w(\mathbf{x}). \end{cases}$$

Definisi (Non-rigid Euclidean designs) *Euclidean t-design* $X = (\{\mathbf{x}_i\}_{i=1}^N, w) \in \mathbb{R}^n$ dikatakan **non-rigid** atau dapat dideformasi jika untuk setiap $\epsilon > 0$ terdapat *Euclidean t-design* lain, katakanlah $Y := (\{\mathbf{y}_i\}_{i=1}^N, w') \in \mathbb{R}^n$, sehingga kedua kondisi di bawah dipenuhi:

1. Untuk setiap $i \in [1, N]_{\mathbb{Z}}$ berlaku $\|\mathbf{x}_i - \mathbf{y}_i\| < \epsilon$ dan $\|w(\mathbf{x}_i) - w'(\mathbf{y}_i)\| < \epsilon$
2. Tidak terdapat transformasi ortogonal $g \in O^*(n)$ yang memenuhi $g(\mathbf{x}_i) = \mathbf{y}_i$, untuk setiap $i \in [1, N]_{\mathbb{Z}}$.

Telah diketahui secara meluas bahwa *tight spherical t-design* bersifat rigid, karena jarak yang mungkin untuk sembarang dua vektor dalam desain tersebut berhingga buah banyaknya dan ditentukan hanya oleh dimensi n dan *strength t*. Pertanyaan yang natural adalah bagaimana sifat rigiditas dari *tight*

spherical t-design jika dipandang sebagai *Euclidean t-design*. Kita miliki sifat berikut.

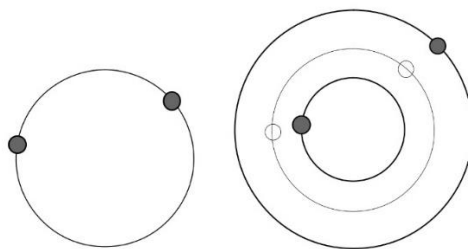
Lema 3.21 (Bannai-Bannai-Suprijanto, 2007) *Setiap tight spherical 2e-design bersifat rigid jika dipandang sebagai Euclidean 2e-design, untuk $e \geq 2$.*

Sebagai contoh lain, *tight Euclidean 4-design* yang dikonstruksi oleh Bannai dan Bannai (2006) sebagai contoh penyangkal atas konjektur Delsarte-Neumaier-Seidel merupakan contoh dari non-rigid *Euclidean design*. Hal ini dapat kita jelaskan demikian. Jika kita gerakkan semua titik yang terletak pada bola konsentrik kedua, $X_2(r)$, secara simultan dengan mengubah jari-jari r menjadi r' sementara semua titik yang terletak pada bola konsentrik pertama, X_1 , kita biarkan seperti semula, maka desain yang baru tetaplah merupakan *Euclidean design* dengan parameter yang sama. Tetapi transformasi semacam ini tidak termuat di dalam $O^*(n)$, karena $X(r)$ dan $X(r')$ tidaklah sama untuk $r \neq r'$. Karena itu *Euclidean design* ini bersifat non-rigid.

Dalam deformasi yang dijelaskan di atas, semua titik yang terletak pada satu bola konsentrik seluruhnya bergerak ke satu bola konsentrik baru. Pertanyaan yang natural adalah, apa yang terjadi jika dua titik pada bola konsentrik yang sama bergerak ke dua bola konsentrik (baru) yang berbeda? Pertanyaan ini membawa kita kepada gagasan tentang non-rigiditas kuat (*strong non-rigidity*), kasus khusus dari non-rigiditas.

Definisi (Non-rigiditas kuat) Euclidean t-design $X = (\{x_i\}_{i=1}^N, w) \in \mathbb{R}^n$ dikatakan **non-rigid** kuat (*strongly non-rigid*) jika untuk setiap $\epsilon > 0$ terdapat *Euclidean t-design* lain, katakanlah $Y := (\{y_i\}_{i=1}^N, w') \in \mathbb{R}^n$, sehingga kedua kondisi di bawah dipenuhi:

1. Untuk setiap $i \in [1, N]_{\mathbb{Z}}$ berlaku $\|x_i - y_i\| < \epsilon$ dan $\|w(x_i) - w'(y_i)\| < \epsilon$; dan
2. Terdapat $i, j \in [1, N]_{\mathbb{Z}}$ yang bersifat $\|x_i\| = \|x_j\|$ tetapi $\|y_i\| \neq \|y_j\|$.



Gambar 4 Ilustrasi definisi *Euclidean design* yang bersifat non-rigid kuat

Jelas bahwa setiap *Euclidean t-design* yang non-rigid kuat adalah *Euclidean t-design* yang non-rigid, karena syarat (2) di atas berimplikasi bahwa transformasi

$$\mathbf{x}_i \mapsto \mathbf{y}_i, \text{ untuk setiap } i \in [1, N]_{\mathbb{Z}}$$

tidak termuat di dalam grup $O^*(n)$.

Konsep non-rigid kuat ini mengantarkan kita kepada satu sifat penting berikut.

Teorema 3.22 (Bannai-Bannai-Suprijanto, 2007) *Tight Euclidean t-design berikut bersifat non-rigid kuat:*

1. **Tight spherical 2-design** dalam S^{n-1} dipandang sebagai **tight Euclidean 2-design**.
2. **Antipodal tight spherical 3-design** dalam S^1 dipandang sebagai **tight Euclidean 3-design**.
3. **Tight Euclidean 4-design** dalam ruang $\mathbb{R}^2$ yang pada dua bola konsentrik.
4. **Antipodal tight 5-design** dalam ruang $\mathbb{R}^2$ yang pada dua bola konsentrik.

Sebagai akibat dari teorema di atas, kita peroleh eksistensi tak-hingga banyak *tight Euclidean design* yang tidak trivial di bawah ini.

Akibat 3.23 (Bannai-Bannai-Suprijanto, 2007) Terdapat tak hingga banyak *tight Euclidean design* dengan parameter seperti berikut:

1. 2-design dalam $\mathbb{R}^n$ yang pada $p = 2, 3, \dots, n + 1$ bola konsentrik.
2. Antipodal 3-design dalam $\mathbb{R}^2$ yang pada dua bola konsentrik.
3. 4-design dalam $\mathbb{R}^2$ yang pada 3 dan 4 bola konsentrik.
4. Antipodal 5-design dalam $\mathbb{R}^2$ yang pada 3 dan 4 bola konsentrik.

Akibat di atas membuktikan eksistensi tak-hingga banyak *tight Euclidean t-design* yang tidak trivial, bertentangan dengan konjektur dari Delsarte-Neumaier-Seidel. Berbeda dengan Bannai dan Bannai (2006), di sini kita membuktikan kekeliruan konjektur Delsarte-Neumaier-Seidel tersebut dengan cara yang elementer. Lebih dari itu, terkait dengan eksistensi *tight Euclidean t-design*, kami percaya pada dugaan berikut.

Konjektur 3.24 (Bannai-Bannai-Suprijanto, 2007) Jika tight Euclidean 2e-design atau antipodal tight Euclidean $(2e+1)$ -design yang disuport oleh lebih dari $\left\lceil \frac{e+\epsilon_S}{2} \right\rceil + 1$ bola konsentrik dijamin adanya, maka terdapat tak hingga banyak tight

Euclidean 2e-design atau antipodal tight Euclidean $(2e+1)$ -design, berturut-turut.

3.2.2.2 Konstruksi dan Klasifikasi *Euclidean Designs*

Seperti yang terjadi pada *spherical designs*, salah satu masalah utama dalam penelitian di bidang *Euclidean designs* adalah bagaimana mengonstruksi contoh eksplisit dan, jika mungkin, mengklasifikasi *Euclidean designs* pada p bola konsentrik. Karena secara umum masalah ini sangat sulit, para peneliti memulainya dengan melakukan klasifikasi pada *tight Euclidean designs*. Sejauh ini, *tight Euclidean designs* yang telah diketahui adalah sebagai berikut:

1. Dalam ruang $\mathbb{R}^2$, (Bajnok, 2006) telah mengonstruksi *tight Euclidean t -design* pada p bola konsentrik, untuk sembarang *strength* t yang mungkin.
2. Dalam ruang $\mathbb{R}^n$, (Bannai, Bannai, dan Suprijanto, 2007) telah membuktikan bahwa konfigurasi (X, w) adalah *Euclidean 2-design* jika dan hanya jika X adalah himpunan dengan $n + 1$ unsur dan juga merupakan himpunan perkalian-dalam-1, yakni $\{u \cdot v : u, v \in X, u \neq v\} = \{\alpha\}$, untuk suatu konstanta negatif $\alpha < 0$.
3. Dalam ruang $\mathbb{R}^n$, Et. Bannai (2006) telah membuktikan bahwa *tight Euclidean 3-design* serupa dengan himpunan $X = \{\pm r_i e_i : 1 \leq i \leq n\}$, dengan $w(r_i e_i) = \frac{1}{m_i^2}$, untuk $i \in [1, n]_{\mathbb{Z}}$.
4. Misalkan (X, w) adalah *tight Euclidean 4-design* pada dua bola konsentrik. Misalkan $X = X_1 \cup X_2$, dengan $|X_1| \leq |X_2|$. Et. Bannai (2009) telah membuktikan hasil-hasil di bawah ini:
 - Jika $|X_1| = \{0\}$, maka X_2 adalah *tight spherical 4-design*.
 - Jika $|X_1| = n + 1$, maka $n = 2, 4, 5, 6, 22$ dan X_2 memiliki struktur sebagai *tight (kombinatorial) 4-design* di dalam skema Johnson $J(n + 1, 2)$.
 - Jika $|X_1| = n + 2$, maka $n = 4$ dan X_2 memiliki struktur sebagai skema Hamming $H(2, 3)$.
 - Jika $|X_1| \geq n + 3$ dan $n < 78$, maka $|X_1| = 33$ dan X_2 memiliki struktur sebagai *tight (kombinatorial) 4-design* di dalam skema Hamming $J(11, 3)$.

- Jika $|X_1| \geq n + 3$ dan $n \geq 78$, maka klasifikasi masih merupakan masalah terbuka.
5. Misalkan (X, w) adalah *tight Euclidean 5-design* pada dua bola konsentrik. Misalkan $X = X_1 \cup X_2$, dengan $|X_1| \leq |X_2|$. Et. Bannai (2006) telah membuktikan hasil-hasil di bawah ini:
 - Jika $|X_1| = \{0\}$, maka X_2 adalah *tight spherical 5-design*.
 - Jika $0 \notin X$, maka $n = 2, 3, 5, 6$.
 6. Misalkan (X, w) adalah *tight Euclidean 7-design* pada dua bola konsentrik. Misalkan $X = X_1 \cup X_2$, dengan $|X_1| \leq |X_2|$. (Bannai dan Bannai, 2008) telah membuktikan bahwa $0 \notin X$ dan $n = 2, 4, 7$.
 7. (Bajnok, 2006) telah mengonstruksi *tight Euclidean 6-design* (X, w) di ruang Euclides $\mathbb{R}^2$ sebagai berikut:
 - $X = \left\{ b_{kj} = \left(r_k \cos \left(\frac{2j+kl}{5} \pi \right), r_k \sin \left(\frac{2j+kl}{5} \pi \right) \right) : j \in [1,5]_{\mathbb{Z}}, k \in [1,2]_{\mathbb{Z}} \right\}$; dan
 - $w(b_{kj}) = \frac{1}{r_k^5}$, dengan $k \in [1,2]_{\mathbb{Z}}$.
 (Suprijanto, 2011) menunjukkan bahwa *tight Euclidean 6-design* di atas adalah satu-satunya di ruang Euclides $\mathbb{R}^n$, dengan $n \in [2,8]_{\mathbb{Z}}$.
 8. (Bannai, Bannai, dan Shigezumi, 2012) mengonstruksi *tight Euclidean 6-design* di ruang Euclides $\mathbb{R}^{22}$ pada dua bola konsentrik dengan kardinalitas $\binom{22+3}{3}$, dan rasio jari-jari $\frac{r_2}{r_1} = \sqrt{11}$, dan rasio fungsi bobot $\frac{w_2}{w_1} = \frac{1}{729}$. Ini adalah satu dari dua *tight Euclidean 6-design* yang berada di ruang Euclides $\mathbb{R}^n$, dengan $n \in [2,438]_{\mathbb{Z}}$.
 9. (Bajnok, 2007) juga telah mengonstruksi *tight Euclidean 7-design* pada tiga bola konsentrik.
 10. Misalkan (X, w) adalah *tight Euclidean 9-design* pada dua bola konsentrik. Misalkan $X = X_1 \cup X_2$, dengan $|X_1| \leq |X_2|$. (Bannai dan Bannai, 2011) telah melakukan klasifikasi lengkap dengan membuktikan beberapa fakta sebagai berikut.
 - Jika $X_1 = \{0\}$, maka $n = 2$, dan $(X \setminus \{0\}, w)$ serupa dengan *tight Euclidean 9-design* (Y, w) dengan $Y = Y_1 \cup Y_2$, dan Y_1 dan Y_2 adalah 8-gon regular berbentuk
 - $Y_1 = \left\{ r_1 (\cos \theta_k, \sin \theta_k) : \theta_k = \frac{2k\pi}{8}, k \in [0,7]_{\mathbb{Z}} \right\}$,

$$- Y_2 = \left\{ r_1(\cos \theta_k, \sin \theta_k) : \theta_k = \frac{(2k+1)\pi}{8}, k \in [0,7]_{\mathbb{Z}} \right\}.$$

- Jika $n \geq 3$, maka tidak terdapat tight Euclidean 9-design.

11. Hasil terbaru sejauh ini terkait dengan *tight Euclidean t-design*, dengan $t \geq 11$ ganjil, telah diberikan oleh (Bannai dan Bannai, 2014) yang berhasil membuktikan bahwa terdapat hanya sejumlah hingga *tight Euclidean t-design* pada dua bola konsentrik.

Sejauh ini, hasil-hasil yang terkait dengan konstruksi *tight Euclidean t-design* pada $p \geq 3$ bola konsentrik masih menanti penyelidikan lebih lanjut. Lebih dari itu, klasifikasi lengkap dari *tight Euclidean t-designs*, untuk t ganjil maupun t genap, masih jauh dari tuntas, bahkan pun untuk desain yang termuat pada dua ($p = 2$) bola konsentrik. Masih banyak sekali masalah terbuka yang menanti untuk diselesaikan.

Masalah terbuka 3.25 *Konstruksi atau klasifikasi tight Euclidean t-designs pada $p \geq 2$ bola konsentrik.*

4. TEORI KODING

Kemunculan derau (*noise*) dalam setiap saluran komunikasi merupakan hal yang tidak terhindarkan dalam kehidupan kita. Teori Koding (*error-correcting codes*) lahir sebagai respons atas masalah ini. Adalah Claude Elwood Shannon yang pada tahun 1948 melahirkan karya (Shannon, 1948) yang menandai lahirnya cabang ilmu ini. Di dalam karya tersebut, Shannon membuktikan eksistensi kode yang baik, yang dapat digunakan dalam proses komunikasi, terlepas dari saluran komunikasi yang tersedia. Tetapi, bukti yang diberikan oleh Shannon itu tidaklah konstruktif. Dia hanya membuktikan eksistensi kode tanpa memberikan konstruksi eksplisit dari kode tersebut. Karena itu, konstruksi kode yang baik merupakan salah satu masalah utama dalam bidang penelitian Teori Koding ini.

Teori Koding telah tumbuh menjadi cabang ilmu yang sangat penting karena ilmu ini merupakan irisan dari berbagai disiplin ilmu lain, termasuk teori informasi, sains komputer, teknik elektro, di samping matematika sendiri. Bahkan di dalam bidang matematika sendiri, Teori Koding melibatkan berbagai cabang ilmu, termasuk Aljabar, Kombinatorika, Teori Bilangan, Analisis, dan juga Teori Peluang.

4.1 Kode Linear Atas Lapangan Hingga

Misalkan $\mathbb{F}_q$ adalah lapangan hingga. Kode C dengan panjang n adalah subhimpunan tak-kosong dari ruang vektor $\mathbb{F}_q^n$, dan kode linear C dengan panjang n adalah subruang dari ruang vektor $\mathbb{F}_q^n$ atas lapangan $\mathbb{F}_q$. Kode linear C berdimensi k kita tuliskan sebagai kode- $[n, k]$. Matriks pembangkit dari C adalah matriks berukuran $k \times n$ yang baris-barisnya merupakan basis dari kode C . Bobot $wt(c)$ dari katakode $c \in C$ didefinisikan sebagai banyaknya entri tak nol dari c . Bobot minimum $wt(C)$ dari kode C didefinisikan

$$wt(C) = \min\{wt(x) : x \in C, x \neq 0\}.$$

Selain panjang kode dan dimensi, parameter lain yang penting bagi sebuah kode linear adalah jarak minimum $d = d(C)$ yang didefinisikan sebagai berikut.

$$d = d(C) = \min\{d_H(x, y) : x, y \in C, x \neq y\},$$

dengan $d_H(\mathbf{x}, \mathbf{y}) := |\{j: x_j \neq y_j\}|$. Mudah dibuktikan bahwa untuk kode linear, bobot jarak minimum dari kode C tepat sama dengan bobot minimum dari kode C . Jadi, $d(C) = wt(C)$. Kode linear C dengan panjang n , dimensi k , dan jarak minimum d ditulis kode- $[n, k, d]$. Pencacah bobot W dari kode linear C didefinisikan sebagai

$$W(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i,$$

dengan A_i menyatakan banyaknya katakode berbobot i di dalam C .

Ruang vektor $\mathbb{F}_q^n$ dilengkapi dengan perkalian dalam Euclides yang natural. Dual dari kode C , ditulis $C^\perp$, didefinisikan sebagai himpunan vektor dalam $\mathbb{F}_q^n$ yang ortogonal dengan setiap katakode di C . Kode linear C dikatakan swa-dual jika $C = C^\perp$. Sebuah kode linear C disebut tipe II jika C swa-dual dan *doubly even*, yakni setiap katakode di dalamnya berbobot kelipatan 4.

Jarak minimum $d = d(C)$ dari sebuah kode C sangatlah penting karena parameter ini berbanding lurus dengan kemampuan kode tersebut dalam mendeteksi dan mengoreksi kesalahan, sebagaimana diberikan oleh teorema di bawah ini.

Teorema 4.1 *Kode linear dengan jarak minimum d dapat mengoreksi hingga $\left\lfloor \frac{d-1}{2} \right\rfloor$ digit kesalahan jika kode tersebut digunakan dalam transmisi informasi.*

Kode linear C berdimensi k dan jarak minimum d kita tuliskan sebagai kode- $[n, k, d]$. Sebuah kode linear dikatakan ekstremal atau hampir ekstremal jika jarak minimumnya tepat sama atau berselisih satu dengan batas atas dari jarak minimum yang mungkin untuk kode linear tersebut, sebagaimana diberikan oleh Grassl (2024).

Salah satu masalah penting dalam penelitian di bidang Teori Koding diberikan seperti di bawah ini.

Masalah fundamental dalam Teori Koding *Jika diberikan dua parameter dari kode linear, yaitu panjang kode n dan dimensi kode k , bagaimana mengonstruksi kode linear yang memiliki jarak minimum d setinggi mungkin.*

4.1.1 Konstruksi Kode Linear dari Skema Asosiasi Johnson

Sejauh ini ada beragam metode konstruksi yang telah diperkenalkan oleh banyak peneliti. Meski demikian, tidak ada satupun metode konstruksi yang dapat digunakan untuk memperoleh kode linear dengan jarak minimum yang optimal untuk seluruh panjang kode dan dimensi kode yang diberikan. Salah satu yang telah kami coba adalah bagaimana mengonstruksi kode linear dari graf Johnson.

Untuk menyegarkan ingatan, marilah kita tinjau kembali skema Johnson. Misalkan V adalah himpunan dengan v unsur dan X adalah koleksi subhimpunan dari V dengan k unsur, dengan $k \leq \frac{v}{2}$. (Jadi $|X| = \binom{v}{k}$). Relasi pada X didefinisikan sebagai:

$$(x, y) \in R_i \Leftrightarrow |x \cap y| = k - i,$$

untuk setiap $i \in [0, k]_{\mathbb{Z}}$. Maka $J(v, k) = (X, \{R_i\}_{i=0}^k)$ merupakan skema asosiasi simetris yang disebut skema asosiasi Johnson atau skema Johnson dan graf $\Gamma = (X, R_1)$ disebut graf Johnson. Kami gunakan empat buah metode konstruksi untuk mendapatkan kode linear dengan jarak minimum yang optimal.

Untuk sembarang bilangan real $r, s, t \in \mathbb{F}_q$, definisikan matriks

$$Q(r, s, t) := rI + sA + t\bar{A},$$

dengan I matriks identitas, A matriks ketetanggaan dari graf Γ , dan $\bar{A} = J - I - A$.

Matriks insidensi $M = (M(i, j))$ dari graf $\Gamma = (X, R_1)$ didefinisikan sebagai $M(i, j) = 1$ jika titik i menempel pada sisi e_j , dan $M(i, j) = 0$ jika titik i tidak menempel pada sisi e_j .

Kita perkenalkan juga beberapa notasi dan definisi. Graf garis dari Γ , ditulis $L\Gamma$, didefinisikan sebagai graf dengan himpunan titik $V(L\Gamma) = E(\Gamma)$, dan sembarang dua titik dalam $V(L\Gamma)$ bertetangga jika dan hanya jika kedua sisi yang bersesuaian memiliki titik yang sama. Telah diketahui bahwa matriks ketetanggaan dari graf garis $L\Gamma$ berbentuk $M^T M - 2I$, dengan M adalah matriks insidensi dari graf Γ . Perkalian tensor $T\Gamma = \Gamma \times \Gamma$ dari graf Γ adalah graf dengan himpunan titik $V(\Gamma \times \Gamma) = V(\Gamma) \times V(\Gamma)$, dan sembarang dua titik

$(u_1, u_2), (v_1, v_2) \in V(\Gamma \times \Gamma)$ bertetangga jika dan hanya jika $\{u_1, v_1\}, \{u_2, v_2\} \in E(\Gamma)$.

Kami coba mengonstruksi kode linear dengan menggunakan dua belas matriks pembangkit, yang empat di antaranya seperti di bawah ini:

1. A , dengan A adalah matriks ketetanggaan dari graf Γ ;
2. $(A | M)$, dengan M adalah matriks insidensi dari graf Γ ;
3. $P(r, s, t) = (I | Q(r, s, t))$, dengan I matriks identitas dan $Q(r, s, t)$ seperti didefinisikan di atas;

$$4. B(r, s, t) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha & \beta & \cdots & \beta \\ & 0 & & & \gamma & & & \\ \vdots & I & & \vdots & Q(r, s, t) & & & \\ & 0 & & & \gamma & & & \end{pmatrix}, \text{ dengan } \alpha, \beta, \gamma \text{ suatu unsur di } \mathbb{F}_q.$$

Delapan matriks pembangkit lainnya diperoleh dari keempat matriks pembangkit di atas, dengan menggantikan graf Γ dengan graf garis $L\Gamma$ dan graf tensor $T\Gamma$. Secara umum, untuk sembarang graf Γ kita memiliki sifat berikut.

Lema 4.2 *Jika G adalah matriks pembangkit dari kode linear C , dengan parameter $[n, k, d]$, maka berlaku $d \leq \min\{wt(g_i) : 1 \leq i \leq k\}$, dengan g_i adalah baris-baris pada matriks G .*

Sabagai akibat dari sifat di atas, terkait keempat metode konstruksi yang diberikan pada (1), (2), (3), dan (4) di atas, kita peroleh sifat di bawah ini.

Akibat 4.3 *Misalkan $\Gamma = (X, R_1)$ adalah graf Johnson dengan $|X| = v$ dan $|R_1| = \epsilon$, dan misalkan pula $\delta(\Gamma)$ adalah derajat titik terkecil pada graf Γ . Maka berlaku:*

1. *kode linear dengan matriks pembangkit A memiliki parameter $[n, k, d]$ dengan $d \leq \delta(\Gamma)$.*
2. *kode linear dengan matriks pembangkit $(A | M)$ memiliki parameter $[n + \epsilon, k, d]$ dengan $d \leq \delta(\Gamma)$.*
3. *kode linear dengan matriks pembangkit $P(r, s, t)$ memiliki parameter $[2v, v, d]$ dengan $d \leq v + 1$.*
4. *kode linear dengan matriks pembangkit $B(r, s, t)$ memiliki parameter $[2v + 2, v + 1, d]$ dengan $d \leq v + 2$.*

Hasil-hasil konstruksi kode linear biner yang kami peroleh adalah seperti tertulis di dalam tabel di bawah ini.

Tabel 3 Daftar kode liner biner yang diperoleh dengan beragam metode konstruksi.

No	$\langle i, n, k, r, s, t, \alpha, \beta, \gamma \rangle$	Parameter $[n, k, d]$	BA	BB	Tipe	(A_d, A_{d+1}, A_{d+2})
1.	$\langle 4, 3, 1, 0, 1, 0, 1, 1, 1 \rangle$	$[8, 4, 3]$	4	4	<i>n-ex</i>	$(3, 7, 4)$
2.	$\langle 4, 3, 1, 0, 1, 0, 1, 1, 1 \rangle$	$[8, 4, 3]$	4	4	<i>n-ex</i>	$(4, 6, 4)$
3.	$\langle 4, 3, 1, 0, 1, 0, 0, 1, 1 \rangle$	$[8, 4, 3]$	4	4	<i>n-ex</i>	$(7, 7, 0)$
4.	$\langle 3, 4, 1, 0, 1, 0 \rangle$	$[8, 4, 4]$	4	4	<i>s-d, ex</i>	$(14, 0, 0)$
5.	$\langle 9, 3, 1 \rangle$	$[9, 4, 4]$	4	4	<i>ex</i>	$(9, 0, 6)$
6.	$\langle 1, 2, 5, 2 \rangle$	$[10, 4, 4]$	4	4	<i>ex</i>	$(5, 0, 10)$
7.	$\langle 4, 4, 1, 0, 1, 0, 1, 1, 1 \rangle$	$[10, 5, 3]$	4	4	<i>n-ex</i>	$(4, 6, 8)$
8.	$\langle 4, 3, 1, 0, 1, 0, 0, 1, 0 \rangle$	$[10, 5, 3]$	4	4	<i>n-ex</i>	$(4, 14, 8)$
9.	$\langle 3, 2, 5, 1, 0, 1, 0 \rangle$	$[10, 5, 4]$	4	4	<i>ex</i>	$(10, 16, 0)$
10.	$\langle 4, 3, 1, 0, 1, 0, 1, 1, 0 \rangle$	$[10, 5, 4]$	4	4	<i>ex</i>	$(18, 0, 8)$
11.	$\langle 5, 2, 4, 2 \rangle$	$[12, 4, 6]$	6	6	<i>ex</i>	$(12, 0, 3)$
12.	$\langle 4, 5, 1, 0, 1, 0, 1, 1, 1 \rangle$	$[12, 6, 3]$	4	4	<i>n-ex</i>	$(5, 10, 0)$
13.	$\langle 4, 5, 1, 0, 1, 0, 0, 1, 0 \rangle$	$[12, 6, 3]$	4	4	<i>n-ex</i>	$(5, 10, 16)$
14.	$\langle 4, 5, 1, 0, 1, 0, 1, 1, 0 \rangle$	$[12, 6, 4]$	4	4	<i>ex</i>	$(5, 16, 0)$
15.	$\langle 3, 4, 2, 0, 1, 1 \rangle$	$[12, 6, 4]$	4	4	<i>s-d, n-ex</i>	$(15, 10, 32)$
16.	$\langle 4, 4, 2, 0, 0, 1, 0, 1, 1 \rangle$	$[14, 7, 3]$	4	4	<i>n-ex</i>	$(6, 15, 0)$
17.	$\langle 3, 7, 1, 0, 1, 0 \rangle$	$[14, 7, 4]$	4	4	<i>ex</i>	$(21, 0, 0)$
18.	$\langle 4, 4, 2, 0, 1, 1, 1, 1, 0 \rangle$	$[14, 7, 4]$	4	4	<i>ex</i>	$(21, 0, 32)$
19.	$\langle 1, 6, 2 \rangle$	$[15, 4, 8]$	8	8	<i>ex</i>	$(15, 0, 0)$
20.	$\langle 3, 8, 1, 0, 1, 0 \rangle$	$[16, 8, 4]$	5	5	<i>s-d, n-ex, T-II</i>	$(28, 0, 0)$
21.	$\langle 4, 7, 1, 0, 1, 0, 0, 1, 1 \rangle$	$[16, 8, 4]$	5	5	<i>s-d, n-ex, T-II</i>	$(28, 0, 0)$
22.	$\langle 4, 7, 1, 0, 1, 0, 1, 1, 0 \rangle$	$[16, 8, 4]$	5	5	<i>n-ex</i>	$(28, 0, 0)$
23.	$\langle 9, 5, 1 \rangle$	$[25, 16, 4]$	4	4	<i>ex</i>	$(100, 0, 600)$
24.	$\langle 8, 4, 2, 0, 0, 1, 1, 1, 1 \rangle$	$[26, 13, 6]$	7	7	<i>n-ex</i>	$(54, 64, 135)$
25.	$\langle 8, 4, 2, 1, 1, 0, 1, 1, 0 \rangle$	$[26, 13, 6]$	7	7	<i>n-ex</i>	$(70, 0, 471)$
26.	$\langle 8, 4, 2, 0, 0, 1, 1, 1, 0 \rangle$	$[26, 13, 6]$	7	7	<i>n-ex</i>	$(102, 0, 247)$
27.	$\langle 1, 8, 2 \rangle$	$[28, 6, 12]$	12	12	<i>ex</i>	$(28, 0, 0)$
28.	$\langle 4, 6, 2, 0, 0, 1, 1, 1, 1 \rangle$	$[32, 16, 7]$	8	8	<i>n-ex</i>	$(35, 465, 120)$
29.	$\langle 4, 6, 2, 0, 0, 1, 1, 1, 0 \rangle$	$[32, 16, 7]$	8	8	<i>n-ex</i>	$(120, 380, 120)$
30.	$\langle 4, 6, 2, 0, 0, 1, 0, 1, 0 \rangle$	$[32, 16, 7]$	8	8	<i>n-ex</i>	$(155, 465, 0)$
31.	$\langle 4, 6, 2, 0, 0, 1, 0, 1, 1 \rangle$	$[32, 16, 8]$	8	8	<i>s-d, n-ex</i>	$(620, 0, 0)$
32.	$\langle 12, 4, 1, 0, 1, 0, 0, 1, 1 \rangle$	$[34, 17, 7]$	8	8	<i>n-ex</i>	$(32, 300, 320)$
33.	$\langle 12, 4, 1, 1, 0, 1, 0, 1, 0 \rangle$	$[34, 17, 7]$	8	8	<i>n-ex</i>	$(32, 620, 320)$
34.	$\langle 12, 4, 1, 1, 0, 1, 0, 1, 1 \rangle$	$[34, 17, 8]$	8	8	<i>ex</i>	$(332, 640, 0)$
35.	$\langle 3, 6, 3, 1, 0, 1 \rangle$	$[40, 20, 8]$	9	10	<i>s-d, n-ex, T-II</i>	$(285, 0, 0)$
36.	$\langle 3, 6, 3, 0, 1, 0 \rangle$	$[40, 20, 8]$	9	10	<i>s-d, n-ex</i>	$(285, 0, 1024)$

Catatan terkait tabel:

- $i = 1$ berarti kode diperoleh dengan metode konstruksi (1) dari graf Γ .
- $i = 2$ berarti kode diperoleh dengan metode konstruksi (2) dari graf Γ .
- $i = 3$ berarti kode diperoleh dengan metode konstruksi (3) dari graf Γ .
- $i = 4$ berarti kode diperoleh dengan metode konstruksi (4) dari graf Γ .
- $i = 5$ berarti kode diperoleh dengan metode konstruksi (1) dari graf LG .
- $i = 6$ berarti kode diperoleh dengan konstruksi metode (2) dari graf LG .
- $i = 7$ berarti kode diperoleh dengan konstruksi metode (3) dari graf LG .
- $i = 8$ berarti kode diperoleh dengan konstruksi metode (4) dari graf LG .

- $i = 1$ berarti kode diperoleh dengan metode konstruksi (1) dari graf TT .
- $i = 2$ berarti kode diperoleh dengan metode konstruksi (2) dari graf TT .
- $i = 3$ berarti kode diperoleh dengan metode konstruksi (3) dari graf TT .
- $i = 4$ berarti kode diperoleh dengan metode konstruksi (4) dari graf TT .
- “ex” dan “n-ex” berturut-turut berarti ekstremal dan hampir ekstremal. “s-d” berarti swa-dual. “T-II” berarti tipe II. “BA” dan “BB” berarti batas atas dan batas bawah dari jarak minimum seperti diberikan oleh (Grassl, 2024).

Dengan metode seperti yang dijelaskan di atas, kami juga memperoleh puluhan kode linear lain dengan jarak minimum yang baik, dengan panjang beragam atas lapangan $\mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$, dan $\mathbb{F}_7$. Untuk hasil-hasil lengkapnya, silahkan lihat (Suprijanto dan Nugraha, 2016).

4.2 Kode Linear Atas Ring Hingga

Kode atas ring hingga diperkenalkan kembali oleh Ian F. Blake pada tahun 1970-an (Blake, 1972), (Bake, 1975) setelah sebelumnya (Assmus dan Mattson, 1963) mengatakan bahwa ring hingga merupakan alfabet yang mungkin untuk kode linear. Blake (1972) memperkenalkan suatu cara untuk mengonstruksi kode atas ring $\mathbb{Z}_m$ dari kode siklis atas lapangan hingga $\mathbb{F}_p$, dengan p adalah faktor prima dari m . Blake (1975) juga mengobservasi struktur dari kode linear atas $\mathbb{Z}_{p^r}$. (Spiegel, 1977), (Spiegel, 1978) kemudian memperumum hasil-hasil dari Blake tentang kode linear atas $\mathbb{Z}_m$, untuk sembarang bilangan positif m . Meski demikian, studi tentang kode linear atas ring hingga baru menarik perhatian banyak peneliti setelah Hammons, Kumar, Calderbank, Sloane, dan Sole (1994)¹⁶ menelurkan karyanya, dengan salah satu hasil utama adalah bagaimana beberapa keluarga dari kode tak-linear yang dikenal baik dalam bidang Teori Koding terkait erat dengan kode linear atas ring $\mathbb{Z}_4$. Sejak karya Hammons, dkk. (1994) ini, banyak peneliti melakukan penelitian tentang kode linear atas beragam ring hingga.

Sementara itu, investigasi tentang kode siklis atas lapangan hingga telah dimulai lebih dahulu oleh Prange pada tahun 1957 dan 1958 dengan dua laporan penelitian AFCRL (Prange, 1957), (Prange, 1958). Kode siklis merupakan kelas kode yang sangat penting karena dua hal: secara teoretis,

¹⁶ Karya ini juga mendapat penghargaan *IEEE Information Theory Society Best Paper Award* tahun 1994.

kode siklis kaya akan struktur matematis, dan secara praktis, kode ini mudah diimplementasikan dalam skema dekoding.

4.2.1 Kode Siklis Atas Ring Hingga

Pada bagian ini akan kita uraikan serba ringkas kode siklis atas ring hingga $B_{k,q}$ yang didefinisikan sebagai

$$B_{k,q} := \frac{\mathbb{F}_q[v_1, v_2, \dots, v_k]}{\langle v_i^2 - v_i \rangle_{i=1}^k}.$$

Kita awali dengan sekilas sejarah.

Kode siklis atas ring hingga tampaknya dieksplorasi secara ekstensif untuk kali pertama oleh (Calderbank dan Sloane, 1995) pada tahun 1995, walaupun kajian yang lebih awal telah dilakukan oleh (Shankar, 1979) pada tahun 1979, di mana Chinese Remainder Theorem digunakan untuk menyelidiki suatu kelas dari kode siklis, tepatnya kode BCH, atas ring $\mathbb{Z}_m$. Dalam karyanya itu, Calderbank dan Sloane menurunkan beberapa sifat dasar terkait dengan struktur dari kode siklis dengan panjang n atas ring hingga $\mathbb{Z}_{p^r}$, dengan p bilangan prima yang tidak membagi n , dan r bilangan bulat positif. Sayangnya, sebagaimana diakui sendiri oleh penulisnya, hasil-hasil utama di dalam artikel (Calderbank dan Sloane, 1995) diverifikasi dengan menggunakan teori representasi atau aljabar komutatif, dan buktinya tidak diberikan di dalam artikel tersebut. Belakangan, Kanwar dan Lopez-Permouth (1997) membuktikan ulang hasil-hasil yang ada di dalam (Calderbank dan Sloane, 1995) dengan menggunakan pendekatan yang lebih elementer. Norton dan Salangean-Mandache (2000) memperluas teorema-teorema yang didapat oleh (Calderbank dan Sloane, 1995) dan (Kanwar dan Lopez-Permouth, 1997) ke dalam kode siklis atas ring rantai hingga. Pada 2004, Dinh dan Lopez-Permouth (Dinh dan Lopez-Permouth, 2004) menurunkan sifat-sifat struktural dari kode siklis dan kode negasiklis atas ring rantai hingga dalam setting yang lebih umum. Pendekatan mereka berbeda dengan yang digunakan oleh (Norton dan Salangean-Mandache, 2000). Lebih dari itu, hasil-hasil dalam (Dinh dan Lopez-Permouth, 2004) juga lebih detail dibandingkan dengan hasil-hasil yang didapat dalam (Norton dan Salangean-Mandache, 2000).

Kemudian, (Abualrub dan Siap, 2007) menurunkan sifat-sifat struktural dari kode siklis atas ring non-rantai $\mathbb{Z}_2 + u\mathbb{Z}_2$ dengan $u^2 = 0$, dan $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$ dengan $u^3 = 0$. Lebih belakangan lagi, pada 2014, (Cengellenmis, Derti, dan Dougherty, 2014) menyelidiki struktur dari kode linear atas ring $B_{2,q}$ ((Cengellenmis, Derti, dan Dougherty, 2014) menggunakan notasi A_k).

Marilah kita tinjau lebih dahulu serba singkat struktur aljabar dari $B_{k,q}$. Sebagai contoh, untuk $k = 1$ maka $B_{1,q} = \mathbb{F}_q + v\mathbb{F}_q$, dengan $q = p^r$ adalah bilangan bulat pangkat prima. Kita tuliskan juga $B_{0,q} = \mathbb{F}_q$. Ring $B_{k,q}$ dapat dipandang sebagai ruang vektor atas $\mathbb{F}_q$ berdimensi 2^k dengan basis berupa unsur-unsur berbentuk $\prod_{i \in H} w_i$, dengan $H \in 2^{[1,k]\mathbb{Z}}$ dan $w_i \in \{v_i, 1 - v_i\}$, untuk $i \in [1,k]\mathbb{Z}$ (Irwansyah dkk, 2018a). Juga, ring $B_{k,q}$ isomorf dengan $\mathbb{F}_q^{2^k} = \mathbb{F}_{p^r}^{2^k}$, melalui Teorema Sisa Cina (Chinese Remainder Theorem) (Irwansyah, dkk., 2018b).

Setiap unsur $a \in B_{k,q}$ dapat dituliskan sebagai

$$a = \sum_{S \in 2^{[1,k]\mathbb{Z}}} a_S v_S,$$

untuk suatu $a_S \in \mathbb{F}_{p^r}$, dengan $v_S := \prod_{i \in S} v_i$ dan $v_\emptyset := 1$.

Kita definisikan lebih dahulu kode siklis atas ring hingga secara formal. Misalkan R adalah ring komutatif. Himpunan tak kosong C dikatakan kode dengan panjang n atas ring R jika $C \subseteq R^n$. Jika C adalah submodul dari R^n maka C disebut kode linear. Misalkan $f(x) \in R[x]$. Korespondensi di bawah ini dapat membantu kita untuk mengubah struktur kombinatorika dari kode siklis ke dalam struktur aljabar:

$$\pi: R^n \ni (c_0, c_1, \dots, c_{n-1}) \mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \frac{R[x]}{\langle f(x) \rangle}.$$

Kode linear $C \subseteq R^n$ dikatakan polisiklis atas R jika $\pi(C)$ merupakan ideal dalam $\frac{R[x]}{\langle f(x) \rangle}$.

- Jika $f(x) = x^n - 1$, maka C disebut kode siklis.
- Jika $f(x) = x^n + 1$, maka C disebut kode negasiklis.
- Jika $f(x) = x^n + \lambda$, dengan λ unsur unit di R , maka C disebut kode konstasiklis.

Dengan mendefinisikan operator pergeseran λ -konstasiklis T_λ pada R^n seperti berikut

$$T_\lambda(c_0, c_1, \dots, c_{n-2}, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}),$$

maka definisi di atas ekivalen dengan definisi di bawah ini:

- C disebut kode siklis jika $T_1(C) = C$.
- C disebut kode negasiklis jika $T_{-1}(C) = C$.
- C disebut kode λ -konstasiklis jika $T_\lambda(C) = C$.

Kode linear C disebut kuasi-siklis dengan indeks l jika $T^l(C) = C$, untuk suatu bilangan bulat positif l .

Ingat kembali pemetaan Gray yang didefinisikan dari $B_{k,q}$ (Irwansyah, dkk., 2018a), (Irwansyah, dkk., 2028b) sebagai berikut:

$$\varphi: B_{k,q} \ni a = \sum_{i=1}^{2^k} \alpha_{S_i} v_{S_i} \mapsto \left(\sum_{S \subseteq S_1} \alpha_S, \sum_{S \subseteq S_2} \alpha_S, \dots, \sum_{S \subseteq S_{2^k}} \alpha_S \right) \in \mathbb{F}_{p^r}^{2^k}.$$

Pemetaan φ bersifat bijektif. Pemetaan ini juga secara natural dapat diperluas menjadi pemetaan dari $B_{k,q}^n$ sebagai berikut:

$$\bar{\varphi}: B_{k,q} \ni (a_1, a_2, \dots, a_n) \mapsto (\varphi(a_1), \varphi(a_2), \dots, \varphi(a_n)) \in \mathbb{F}_{p^r}^{n \cdot 2^k}.$$

Kita peroleh karakterisasi dari kode siklis dan kode kuasi-siklis atas $B_{k,q}$.

Teorema 4.4 (Irwansyah-Suprijanto, 2018b) *Kode linear C dengan panjang n atas $B_{k,q}$ adalah kuasi siklis dengan indeks l jika dan hanya jika $C = \bar{\varphi}^{-1}(C_1, C_2, \dots, C_{2^k})$ dan setiap kode linear C_i dengan panjang n atas $\mathbb{F}_{p^r}$ adalah kuasi siklis dengan indeks l , untuk atas setiap $1 \leq i \leq 2^k$.*

Karena kode siklis tak lain adalah kode kuasi-siklis dengan indeks atas $l = 1$, maka sebagai konsekuensi dari teorema di atas kita peroleh karakterisasi dari kode siklis atas $B_{k,q}$ berikut.

Teorema 4.5 (Irwansyah-Suprijanto, 2018b) *Kode linear C dengan panjang n atas $B_{k,q}$ adalah kode siklis jika dan hanya jika $C = \bar{\varphi}^{-1}(C_1, C_2, \dots, C_{2^k})$ dan setiap kode linear C_i dengan panjang n atas $\mathbb{F}_{p^r}$ adalah kode siklis, untuk atas setiap $1 \leq i \leq 2^k$.*

Dalam bentuk polinom pembangkit, kita peroleh sifat-sifat berikut.

Akibat 4.6 (Irwansyah-Suprijanto, 2018b) Misalkan kode linear $C = \bar{\varphi}^{-1}(C_1, C_2, \dots, C_{2^k})$ dengan panjang n atas $B_{k,q}$ adalah kuasi-siklis dengan indeks l dan kode linear $C_1, C_2, \dots, C_{2^k}$ dengan panjang n atas $\mathbb{F}_{p^r}$ adalah kuasi siklis dengan indeks l . Jika $C_i = \langle g_{1_i}(x), g_{2_i}(x), \dots, g_{m_i}(x) \rangle$, untuk atas setiap $1 \leq i \leq 2^k$, maka

$$C = \left\langle v_{s_1} g_{1_1}(x), \dots, v_{s_{2^k}} g_{1_1}(x), \dots, v_{s_1} g_{m_1}(x), \dots, v_{s_{2^k}} g_{m_1}(x), \dots, v_{s_1} g_{m_{2^k}}(x), \dots, v_{s_{2^k}} g_{m_{2^k}}(x) \right\rangle.$$

Kembali, akibat di bawah ini merupakan kasus khusus dari sifat di atas, untuk $l = 1$.

Akibat 4.7 (Irwansyah-Suprijanto, 2018b) Misalkan kode linear $C = \bar{\varphi}^{-1}(C_1, C_2, \dots, C_{2^k})$ dengan panjang n atas $B_{k,q}$ adalah siklis dan kode linear $C_1, C_2, \dots, C_{2^k}$ dengan panjang n atas $\mathbb{F}_{p^r}$ adalah siklis. Jika $C_i = \langle g_i(x) \rangle$, untuk atas setiap $1 \leq i \leq 2^k$, maka

$$C = \left\langle v_{s_1} g_1(x), v_{s_2} g_1(x), \dots, v_{s_{2^k}} g_1(x), \dots, v_{s_1} g_{2^k}(x), v_{s_2} g_{2^k}(x), \dots, v_{s_{2^k}} g_{2^k}(x) \right\rangle.$$

4.2.1.1 Kode Siklis Miring Atas Ring Hingga $B_{k,2}$ dan $B_{k,q}$

Sekarang, marilah kita tinjau “satu langkah” generalisasi dari gagasan kode siklis. Kita awali dengan beberapa fakta dasar dari apa yang disebut ring polinom-miring (*skew-polynomial ring*).

Misalkan θ adalah automorfisma pada $\mathbb{F}_{p^r}$. Tinjaulah himpunan polinom formal

$$\mathbb{F}_{p^r}[x; \theta] := \{a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} : a_i \in \mathbb{F}_{p^r}\}$$

dengan koefisien ditulis di sebelah kiri variabel x . $\mathbb{F}_{p^r}[x; \theta]$ membentuk ring terhadap operasi penjumlahan biasa dan perkalian dengan aturan dasar

$$xa := \theta(a)x.$$

Aturan dasar perkalian ini kita perluas secara natural terhadap semua unsur dalam $\mathbb{F}_{p^r}[x; \theta]$ dengan sifat asosiatif dan distributif. $\mathbb{F}_{p^r}[x; \theta]$ disebut ring polinom-miring atas $\mathbb{F}_{p^r}$, dan setiap unsur di dalamnya disebut polinom-miring. Keluarga ring polinom ini telah diperkenalkan oleh Ore, hampir

seabad lalu. Dapat dengan mudah diperiksa bahwa $\mathbb{F}_{p^r}[x; \theta]$ merupakan ring non-komutatif, kecuali jika θ merupakan automorfisma identitas pada $\mathbb{F}_{p^r}$.

Diberikan automorfisma θ pada $\mathbb{F}_{p^r}$ dan elemen unit $\lambda \in \mathbb{F}_{p^r}$. Kode linear C dikatakan konstasiklis- (θ, λ) miring dengan panjang n jika C tertutup terhadap operasi pergeseran konstasiklis- (θ, λ) konstasiklis- $T_{\theta, \lambda}$ pada $\mathbb{F}_{p^r}$ yang didefinisikan sebagai berikut:

$$T_{\theta, \lambda}: \mathbb{F}_{p^r} \ni (v_0, v_1, \dots, v_{n-1}) \mapsto (\theta(\lambda v_{n-1}), \theta(v_0), \dots, \theta(v_{n-2})) \in \mathbb{F}_{p^r}.$$

Khususnya, jika $\lambda = 1$ atau $\lambda = -1$, maka kode tersebut berturut-turut disebut kode siklis miring atau kode negasiklis miring.

Konsep kode siklis miring atau kode siklis- θ atas lapangan hingga pertama kali digagas oleh Boucher, Geiselman, dan Ulmer pada 2007 (Boucher, Geiselman, dan Ulmer, 2007). Telah diketahui bahwa setiap kode siklis atas lapangan hingga berkorespondensi satu-satu dengan pembagi dari polinom $x^n - 1$. Serupa dengan yang terjadi pada kode siklis, setiap kode siklis miring juga berkorespondensi satu-satu dengan pembagi kanan dari $x^n - 1$. Karena polinom-miring tidak selalu memiliki faktorisasi tak-tereduksi yang tunggal, maka polinom $x^n - 1$ dimungkinkan untuk memiliki pembagi kanan yang lebih banyak. Artinya, kita memiliki kode siklis miring yang banyak, dan akibatnya kita memiliki kesempatan lebih besar untuk dapat memperoleh kode dengan parameter yang baik. Inilah salah satu motivasi dari (Boucher, Geiselman, dan Ulmer, 2007) memperkenalkan gagasan ini. Pada tahun 2008 dan 2009, (Boucher, Sole, dan Ulmer, 2008) dan juga (Boucher dan Ulmer, 2009), menginvestigasi lebih lanjut dari kode siklis miring atas ring hingga. Baru-baru ini, kami (Irwansyah, dkk., 2016) dan (Irwansyah, dkk., 2018a) bersama beberapa kolega telah menyelidiki kode siklis miring atas ring $B_{2,q}$ dan $B_{k,q}$.

Kode siklis miring atas ring $B_{k,2}$

Kita awali dengan fakta-fakta dasar terkait dengan kode atas $B_{k,2}$.

Karena $B_{k,2}$ merupakan kasus khusus dari $B_{k,q}$, maka setiap elemen dari $B_{k,2}$ dapat dituliskan secara tepat sama dengan setiap elemen di $B_{k,q}$. Untuk $A, B \in [1, k]_{\mathbb{Z}}$, kita miliki hubungan $v_A v_B = v_{A \cup B}$, sehingga

$$\sum_{B \in 2^{[1,k]\mathbb{Z}}} \alpha_B v_B \cdot \sum_{C \in 2^{[1,k]\mathbb{Z}}} \beta_C v_C = \sum_{D \in 2^{[1,k]\mathbb{Z}}} \left(\sum_{B \cup C = D} \alpha_B \beta_C \right) v_D.$$

Telah ditunjukkan dalam (Cengellenmis, Dertli, dan Dougherty, 2014) bahwa satu-satunya elemen unit dalam ring $B_{k,2}$ adalah 1. Telah ditunjukkan pula oleh (Cengellenmis, Dertli, dan Dougherty, 2014) bahwa ideal $\langle w_1, w_2, \dots, w_k \rangle$, dengan $w_i \in \{v_i, 1 + v_i\}$, merupakan ideal maksimal dengan kardinalitas 2^{2^k-1} . Fakta ini juga memberikan informasi lain bahwa ring $B_{k,2}$ memiliki 2^k ideal maksimal. Karena itu, ring $B_{k,2}$ merupakan ring lokal.

Ring $B_{k,2}$ merupakan ring ideal utama. Khususnya, misalkan $I = \langle \alpha_1, \alpha_2, \dots, \alpha_s \rangle$ adalah ideal dalam $B_{k,2}$. Maka I merupakan ideal utama yang dibangun oleh elemen yang merupakan penjumlahan dari semua perkalian dari α_i , yakni

$$I = \left\langle \sum_{\substack{A \subseteq [1,s]\mathbb{Z}, \\ A \neq \emptyset}} \prod_{i \in A} \alpha_i \right\rangle.$$

Kita definisikan himpunan automorfisma dalam ring $B_{k,2}$. Pertama, kita definisikan lebih dahulu pemetaan Θ_i dengan

$$\Theta_i(v_j) := \begin{cases} v_i + 1, & i = j, \\ v_j, & i \neq j. \end{cases}$$

Untuk $S \subseteq [1, k]\mathbb{Z}$, automorfisma Θ_S didefinisikan sebagai

$$\Theta_S := \prod_{i \in S} \Theta_i.$$

Ingat bahwa Θ_S merupakan involusi pada ring $B_{k,2}$. Kita akan menggunakan involusi ini untuk mendefinisikan kode siklis- Θ_S .

Pemetaan Gray telah didefinisikan untuk semua ring komutatif berorde 4 (lihat (Dougherty, Gaborit, Harada, Munemasa, dan Sole, 1999), untuk deskripsi dari empat pemetaan Gray ini). Untuk ring $B_{k,2} = \mathbb{F}_2 + v\mathbb{F}_2$, kita memiliki pemetaan Gray $\phi_1: B_{k,2} \rightarrow \mathbb{F}_2^2$ yang didefinisikan sebagai $\phi_1(a + bv_1) = (a, a + b)$. Secara eksplisit, untuk $B_{k,2}$ pemetaan Gray berbentuk:

$$0 \mapsto 00,$$

$$1 \mapsto 11,$$

$$v \mapsto 01,$$

$$1 + v \mapsto 10.$$

Kita perluas pemetaan ini secara induktif demikian. Setiap elemen dalam ring $B_{k,2}$ dapat dituliskan sebagai $\alpha + \beta v_k$, dengan $\alpha, \beta \in B_{k-1,2}$. Maka untuk $k \geq 2$, kita definisikan pemetaan $\phi_k: B_{k,2} \rightarrow B_{k-1,2}^2$ dengan

$$\phi_k(\alpha + \beta v_k) = (\alpha, \alpha + \beta).$$

Maka pemetaan Gray $\Phi_k: B_{k,2} \rightarrow \mathbb{F}_2^{2^k}$ kita definisikan sebagai

$$\Phi_1(\gamma) = \phi_1(\gamma), \Phi_2(\gamma) = \phi_1(\phi_2(\gamma)) \text{ dan}$$

$$\Phi_k(\gamma) = \phi_1 \left(\phi_2 \left(\dots \left(\phi_{k-2} \left(\phi_{k-1}(\phi_k(\gamma)) \right) \right) \dots \right) \right).$$

Jelas bahwa $\Phi_k(1) = \mathbf{1}$, vektor dengan semua entri 1. Dapat dengan mudah kita periksa juga bahwa pemetaan Gray Φ_k merupakan pemetaan linear dan bersifat bijektif.

Kita juga mendefinisikan pemetaan lain yang nanti akan kita gunakan untuk mengonstruksi pembangkit untuk kode siklis- Φ_s . Misalkan $p, k \in \mathbb{Z}^+$, dengan $p < k$. Misalkan $\Omega_p = \{p+1, p+2, \dots, k\}$ dan $s = 2^{k-p}$. Maka, kita peroleh $|2^{\Omega_p}| = s$. Kita dapat mendefinisikan pemetaan Gray sebagai berikut:

$$\Psi_{k,p}: B_{k,2} \rightarrow B_{p,2}^s.$$

Kita nyatakan koordinat dari $B_{p,2}^s$ dengan urutan leksikografik dari subhimpunan Ω_p , dan menyatakannya dengan $B_1, B_2, \dots, B_s$. Tuliskan $B_1 = \emptyset$ dan $B_s = \Omega_p$. Maka kita peroleh hubungan

$$\Psi_{k,p} \left(\sum_{B \subseteq \Omega_p} \alpha_B w_B \right) = \left(\sum_{D \subseteq B_1} \alpha_D, \sum_{D \subseteq B_2} \alpha_D, \dots, \sum_{D \subseteq B_s} \alpha_D \right).$$

Untuk $p = 0$, pemetaan $\Psi_{k,0}$ tepat sama dengan pemetaan Ψ_k dalam (Cengellenmis, Dertli, dan Dougherty, 2014). Masih di dalam (Cengellenmis, Dertli, dan Dougherty, 2014), telah dibuktikan bahwa pemetaan Ψ_k dan Φ_k adalah konjugate, dalam pengertian bahwa peta dari mereka bersifat ekuivalen secara permutasi.

Kita tegaskan di sini bahwa representasi elemen dalam $B_{k,2}$ dapat diubah dengan mengganti v_i dengan $1 + v_i$. Dengan cara seperti itu, misalkan $u_i \in \{v_i, 1 + v_i\}$, untuk setiap i . Maka kita memiliki definisi alternatif untuk $\Psi_{k,p}$ sebagai

$$\bar{\Psi}_{k,p} \left(\sum_{B \subseteq \Omega_p} \alpha_B y_B \right) = \left(\sum_{D \subseteq B_1} \alpha_D, \sum_{D \subseteq B_2} \alpha_D, \dots, \sum_{D \subseteq B_s} \alpha_D \right),$$

dengan $y_B = \prod_{i \in B} u_i$. Setiap sifat untuk $\Psi_{k,p}$ juga dapat dibuktikan juga dengan mudah berlaku untuk $\bar{\Psi}_{k,p}$.

Misalkan T adalah matriks yang membentuk pergeseran siklis pada sebuah vektor, yakni $T(v_1, v_2, \dots, v_n) = (v_n, v_1, \dots, v_{n-1})$. Misalkan $\sigma_{i,k}$ adalah permutasi pada $[1, 2^k]_{\mathbb{Z}}$ yang didefinisikan sebagai

$$(\sigma_{i,k})_{[p2^i+1, (p+1)2^i]_{\mathbb{Z}}} = T^{2^{i-1}}(p2^i + 1, p2^i + 2, \dots, (p+1)2^i),$$

untuk setiap $p \in [0, 2^{k-i} - 1]_{\mathbb{Z}}$. Misalkan $\Sigma_{i,k}$ adalah permutasi pada elemen-elemen dari $\mathbb{F}_2^{2^k}$ yang diinduksi oleh $\sigma_{i,k}$, yakni untuk setiap $x = (x_1, x_2, \dots, x_{2^k}) \in \mathbb{F}_2^{2^k}$,

$$\sum_{i,k} (x_1, x_2, \dots, x_{2^k}) = (x_{\sigma_{i,k}(1)}, x_{\sigma_{i,k}(2)}, \dots, x_{\sigma_{i,k}(2^k)}).$$

Maka kita peroleh sifat berikut.

Lema 4.8 (Irwansyah, dkk., 2016) Misalkan $k \geq 1$ dan $i \in [1, k]_{\mathbb{Z}}$. Untuk setiap $x \in B_{k,2}$ berlaku

$$\sum_{i,k} (\Phi_k(x)) = \Phi_k(\theta_i(x)).$$

Kita dapat memperluas definisi permutasi $\Sigma_{i,k}$ pada sumbhimpunan dari $[1, k]_{\mathbb{Z}}$. Untuk subhimpunan $A \subseteq [1, k]_{\mathbb{Z}}$, kita definisikan permutasi $\Sigma_{A,k}$ sebagai

$$\sum_{A,k} = \prod_{i \in A} \sum_{i,k}.$$

Jelas bahwa untuk setiap $x \in B_{k,2}$ berlaku hubungan

$$\sum_{A,k} (\Phi_k(x)) = \Phi_k(\Theta_A(x)).$$

Karakterisasi kode siklis miring atas $B_{k,2}$

Misalkan $S \subseteq [1, k]_{\mathbb{Z}}$ dan misalkan pula $\sum_S = \tau_S \circ T^{2^k}$ adalah permutasi pada elemen-elemen dari $\mathbb{F}_2^{n2^k}$, dengan T adalah pergeseran siklis modulo $n2^k$ dan τ_S adalah permutasi pada elemen-elemen dari $\mathbb{F}_2^{n2^k}$ yang didefinisikan untuk setiap elemen

$$x = (x_1^1, x_2^1, \dots, x_{2^k}^1, x_1^2, x_2^2, \dots, x_{2^k}^2, \dots, x_1^n, x_2^n, \dots, x_{2^k}^n) \in \mathbb{F}_2^{n2^k}$$

sebagai

$$\begin{aligned} \tau_S(x) &= \tau_S((x_1^1, x_2^1, \dots, x_{2^k}^1, x_1^2, x_2^2, \dots, x_{2^k}^2, \dots, x_1^n, x_2^n, \dots, x_{2^k}^n)) \\ &= \left(\sum_{S,k} (x^1), \sum_{S,k} (x^2), \dots, \sum_{S,k} (x^n) \right), \end{aligned}$$

dengan $x^j = (x_1^j, x_2^j, \dots, x_{2^k}^j)$, dan $j \in [1, n]_{\mathbb{Z}}$. Karena T^{2^k} dan τ_S komutatif, maka berlaku $\sum_S = T^{2^k} \circ \tau_S$. Misalkan σ_S menyatakan permutasi pada himpunan $[1, n2^k]_{\mathbb{Z}}$, himpunan indeks dari elemen-elemen dalam $\mathbb{F}_2^{n2^k}$, yang menginduksi permutasi Σ_S di atas. Maka kita miliki syarat perlu dan cukup bagi kode linear C agar merupakan kode siklis miring atas $B_{k,2}$.

Lema 4.9 (Irwansyah, dkk., 2016) Misalkan C adalah kode linear atas $B_{k,2}$ dengan panjang n . Kode $\Phi_k(C)$ ditetapkan oleh permutasi Σ_S jika dan hanya jika C adalah kode siklis- Θ_S .

Kita memiliki karakterisasi pertama dari kode linear C agar merupakan kode siklis- Θ_S atas $B_{k,2}$, yang diberikan dalam pemetaan Gray Φ_k sebagai berikut.

Teorema 4.10 (Irwansyah, dkk., 2016) Misalkan C kode linear atas $B_{k,2}$ dengan panjang n .

1. Jika n ganjil, maka C merupakan kode siklis miring jika dan hanya jika kode $\Phi_k(C)$ ekuivalen dengan kode kuasi-siklis dalam $\mathbb{F}_2^{n2^k}$ dengan indeks 2^{k-1} .
2. Jika n genap, maka C merupakan kode siklis miring jika dan hanya jika kode $\Phi_k(C)$ ekuivalen dengan kode kuasi-siklis dalam $\mathbb{F}_2^{n2^k}$ dengan indeks 2^k .

Kita juga memiliki karakterisasi kedua dari kode linear C agar merupakan kode siklis- Θ_S atas $B_{k,2}$, yang diberikan dalam pemetaan Gray $\Psi_{k,p}$ sebagai berikut.

Teorema 4.11 (Irwansyah, dkk., 2016) *Kode linear C atas $B_{k,2}$ dengan panjang n merupakan kode siklis- Θ_S jika dan hanya jika $C = \Psi_{k,p}^{-1}(C_1, C_2, \dots, C_s)$, dengan $C_1, C_2, \dots, C_s$ semuanya adalah kode kuasi siklis dengan indeks 2 yang memenuhi hubungan*

$$T_{\Theta_{S'}}(C_i) \subseteq C_{\mu(i)},$$

untuk suatu $S' \subseteq S$ dan permutasi μ .

Selanjutnya, marilah kita tinjau beberapa konstruksi kode siklis miring atas $B_{k,2}$. Pertama, ring $B_{k,2}$ isomorf dengan $\mathbb{F}_2^{2^k}$ melalui Teorema Sisa Cina (Teorema 2.5 dalam Cengellenmis, Dertli, dan Dougherty, 2014). Misalkan $CRT: \mathbb{F}_2^{2^k} \rightarrow B_{k,2}$ adalah pemetaan kanonik. Misalkan $CRT(C_1, C_2, \dots, C_{2^k})$ adalah kode atas $B_{k,2}$ yang dibentuk dengan mengambil peta dari $C_1 \times C_2 \times \dots \times C_{2^k}$ oleh CRT , dengan $C_1, C_2, \dots, C_{2^k}$ seluruhnya adalah kode biner.

Selanjutnya, kita definisikan pemetaan $\Gamma: \mathbb{F}_2^{n2^k} \rightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n \times \dots \times \mathbb{F}_2^n$ dengan

$$\Gamma(x_1^1, \dots, x_1^{2^k}, x_2^1, \dots, x_2^{2^k}, \dots, x_n^1, \dots, x_n^{2^k}) = \left((x_1^1, \dots, x_n^1), (x_1^2, \dots, x_n^2), \dots, (x_1^{2^k}, \dots, x_n^{2^k}) \right).$$

Untuk semua kode linear C atas $B_{k,2}$ dengan $C = CRT(C_1, C_2, \dots, C_{2^k})$, kita peroleh hubungan

$$\Gamma \circ \Phi_k(C) = (C_1, C_2, \dots, C_{2^k}).$$

Dua lema di bawah ini memberikan syarat cukup untuk eksistensi kode siklis miring atas ring $B_{k,2}$. Untuk kode dengan panjang genap kita telah membuktikan sifat berikut.

Lema 4.12 (Irwansyah, dkk., 2016) *Misalkan n bilangan genap dan misalkan $C_1, C_2, \dots, C_{2^k}$ kode linear biner dengan panjang n . Maka untuk setiap $A \subseteq [1, k]_{\mathbb{Z}}$, terdapat kode siklis- Θ_A C atas $B_{k,2}$ dengan panjang n .*

Sementara itu, untuk kode dengan panjang ganjil, kita memiliki sifat di bawah ini.

Lema 4.13 (Irwansyah, dkk., 2016) Misalkan n bilangan ganjil dan misalkan $C_1, C_2, \dots, C_{2^{k-1}}$ kode linear biner dengan panjang $2n$. Maka untuk setiap $S \subseteq [1, k]_{\mathbb{Z}}$, terdapat kode siklis- Θ_S C atas $B_{k,2}$ dengan panjang n .

Sekarang, kita akan memberikan sebuah algoritma untuk mengonstruksi kode siklis- Θ_S . Untuk keperluan itu, kita definisikan lebih dahulu pemetaan berikut: $\Gamma_1: \mathbb{F}_2^{n2^{k-1}} \rightarrow \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \times \dots \times \mathbb{F}_2^{2n}$, dengan

$$\begin{aligned} \Gamma_1 \left(x_1^1, \dots, x_1^{2^{k-1}}, x_2^1, \dots, x_2^{2^{k-1}}, \dots, x_n^1, \dots, x_n^{2^{k-1}} \right) \\ = \left((x_1^1, \dots, x_{2n}^1), (x_1^2, \dots, x_{2n}^2), \dots, (x_1^{2^{k-1}}, \dots, x_{2n}^{2^{k-1}}) \right). \end{aligned}$$

Berikut adalah algoritma untuk mengonstruksi kode siklis- Θ_S .

1. Konstruksi kode siklis- Θ_S atas $B_{k,2}$ dengan panjang genap.
 - a) Tinjau kode biner $C_1, C_2, \dots, C_{2^k}$ dengan panjang n .
 - b) Terapkan pemetaan Γ^{-1} untuk memperoleh kode kuasi siklis C' dengan indeks 2^k dan panjang $n2^k$.
 - c) Terapkan pemetaan $\Phi_k^{-1} \circ \sigma_{S_2}^{-1}$ pada C' ; diperoleh kode siklis- Θ_S C atas ring $B_{k,2}$.
2. Konstruksi kode siklis- Θ_S atas $B_{k,2}$ dengan panjang ganjil.
 - a) Tinjau kode biner $C_1, C_2, \dots, C_{2^{k-1}}$ dengan panjang $2n$.
 - b) Terapkan pemetaan Γ_1^{-1} untuk memperoleh kode kuasi siklis C' dengan indeks 2^{k-1} dan panjang $n2^k$.
 - c) Terapkan pemetaan $\Phi_k^{-1} \circ \sigma_{S_1}^{-1}$ pada C' ; diperoleh kode siklis- Θ_S C atas ring $B_{k,2}$.
3. Konstruksi kode siklis- Θ_S atas $B_{k,2}$ dari kode atas $B_{k,2}$, dengan $p < k$.
 - a) Tinjau kode kuasi siklis atas $B_{p,2}$ dengan indeks 2, $C_1, C_2, \dots, C_s$, yang memenuhi hubungan inklusi pada Teorema 4.11.
 - b) Terapkan pemetaan $\Psi_{k,p}$ pada $(C_1, C_2, \dots, C_s)$; diperoleh kode siklis- Θ_S atas $B_{k,2}$.

Sekarang, marilah kita beralih kepada kode siklis miring atas ring $B_{k,p}$.

Kode siklis miring atas ring $B_{k,q}$

Sebagaimana jelas dari definisinya, ring $B_{k,q}$ merupakan perumuman dari ring $B_{k,2}$, yang sudah kita diskusikan sebelumnya. Kita juga memiliki fakta lain terkait pemetaan Gray dan automorfisma pada $B_{k,q}$.

Misalkan $S_1, S_2 \in 2^{[1,k]_{\mathbb{Z}}}$ dua unsur dengan kardinalitas yang sama. Misalkan λ_{S_1, S_2} adalah korespondensi satu-satu antara S_1 dan S_2 dan $\lambda_{S_1, S_2}(i) = i$, untuk semua $i \notin S_1$. Untuk setiap $\alpha \in \mathbb{F}_{p^r}$, kita definisikan pemetaan $\Lambda_{S_1, S_2, t}$ sebagai

$$\Lambda_{S_1, S_2, t}(\alpha v_i) = \alpha^{p^t} v_{\lambda_{S_1, S_2}(i)},$$

untuk setiap $i \in S_1$, dan $t \in [0, r]_{\mathbb{Z}}$. Dapat ditunjukkan bahwa $\Lambda_{S_1, S_2, t}$ mendefinisikan automorfisma pada $B_{k,q}$.

Dengan menggunakan dua kelas automorfisma, yaitu Θ_S dan $\Lambda_{S_1, S_2, t}$, kita dapat mendeskripsikan semua automorfisma pada ring $B_{k,q}$ seperti diberikan oleh lema di bawah.

Lema 4.14 (Irwansyah dkk, 2016) *Jika θ adalah automorfisma pada ring $B_{k,q}$, maka terdapat tiga subhimpunan $S, S_1, S_2 \in [1, k]_{\mathbb{Z}}$ dan bilangan bulat t , dengan $|S_1| = |S_2|$ dan $t \in [0, r]_{\mathbb{Z}}$, sehingga*

$$\theta = \Theta_S \circ \Lambda_{S_1, S_2, t}.$$

Seperti yang terjadi pada ring $B_{k,2}$, untuk memudahkan pembaca, kita ulang kembali di sini. Misalkan T adalah matriks yang merupakan operator pergeseran siklis pada suatu vektor. Misalkan pula $\sigma_{i,k}$ adalah permutasi pada $[1, 2^k]_{\mathbb{Z}}$ yang didefinisikan sebagai

$$(\sigma_{i,k})_{[j2^{i-1}+1, (j+1)2^i]_{\mathbb{Z}}} = T^{2^{i-1}}(j2^i + 1, j2^i + 2, \dots, (j+1)2^i),$$

untuk setiap $j \in [0, 2^{k-i} - 1]_{\mathbb{Z}}$. Misalkan $\Sigma_{i,k}$ adalah permutasi pada elemen-elemen dari $\mathbb{F}_{p^r}^{2^k}$ yang diinduksi oleh permutasi $\sigma_{i,k}$, yakni untuk setiap $x = (x_1, x_2, \dots, x_{2^k}) \in \mathbb{F}_{p^r}^{2^k}$,

$$\sum_{i,k} (x_1, x_2, \dots, x_{2^k}) = (x_{\sigma_{i,k}(1)}, x_{\sigma_{i,k}(2)}, \dots, x_{\sigma_{i,k}(2^k)}).$$

Terkait dengan pemetaan Gray, lema yang berlaku untuk ring $B_{k,2}$ juga berlaku untuk ring $B_{k,q}$.

Lema 4.15 (Irwansyah, dkk., 2018a) Misalkan $k \geq 1$ dan $i \in [1, k]_{\mathbb{Z}}$. Untuk setiap $x \in B_{k,q}$ berlaku

$$\sum_{i,k} (\Phi_k(x)) = \Phi_k(\theta_i(x)).$$

Karakterisasi kode siklis miring atas $B_{k,q}$

Misalkan $S, S_1, S_2 \subseteq [1, k]_{\mathbb{Z}}$, dengan $|S_1| = |S_2|$. Misalkan $\Xi_{S, S_1, S_2, t} = \xi_{S, S_1, S_2, t} \circ T^{2^k}$ adalah pemetaan bijektif pada elemen-elemen dari $\mathbb{F}_{p^r}^{n2^k}$, dengan T adalah operator pergeseran siklis modulo $n2^k$ dan $\xi_{S, S_1, S_2, t}$ didefinisikan pada semua elemen

$$x = (x_1^1, x_2^1, \dots, x_{2^k}^1, x_1^2, x_2^2, \dots, x_{2^k}^2, \dots, x_1^n, x_2^n, \dots, x_{2^k}^n) \in \mathbb{F}_{p^r}^{n2^k}$$

sebagai

$$\begin{aligned} \xi_{S, S_1, S_2, t}(x) &= \xi_{S, S_1, S_2, t}(x_1^1, x_2^1, \dots, x_{2^k}^1, x_1^2, x_2^2, \dots, x_{2^k}^2, \dots, x_1^n, x_2^n, \dots, x_{2^k}^n) \\ &= \left(\left(\sum_{S,k} \circ \Gamma_{S, S_1, S_2, t} \right) (x^1), \left(\sum_{S,k} \circ \Gamma_{S, S_1, S_2, t} \right) (x^2), \dots, \left(\sum_{S,k} \circ \Gamma_{S, S_1, S_2, t} \right) (x^n) \right), \end{aligned}$$

dengan $x_j = (x_1^j, x_2^j, \dots, x_{2^k}^j)$, dan $j \in [1, n]_{\mathbb{Z}}$. Karena T^{2^k} dan $\xi_{S, S_1, S_2, t}$ komutatif, maka berlaku $\Xi_{S, S_1, S_2, t} = \xi_{S, S_1, S_2, t} \circ T^{2^k} = T^{2^k} \circ \xi_{S, S_1, S_2, t}$. Dua sifat di bawah ini memberikan karakterisasi dari kode siklis- θ atas ring $B_{k,q}$. Karakterisasi pertama diberikan oleh teorema berikut.

Teorema 4.16 (Irwansyah, dkk., 2018b) Misalkan C adalah kode linear atas $B_{k,q}$ dengan panjang n . Misalkan $\theta = \theta_S \circ \Lambda_{S_1, S_2, t}$ adalah automorfisma pada $B_{k,q}$, untuk suatu subhimpunan $S, S_1, S_2 \subseteq [1, k]_{\mathbb{Z}}$ dan $t \in [0, r]_{\mathbb{Z}}$. Maka kode $\Phi_k(C)$ invarian terhadap pemetaan $\Xi_{S, S_1, S_2, t}$ jika dan hanya jika C merupakan kode siklis- θ .

Misalkan $\tilde{\lambda}_{S_1, S_2}$ adalah permutasi pada himpunan $[1, 2^k]_{\mathbb{Z}}$ yang diinduksi oleh pemetaan $\theta_S \circ \Lambda_{S_1, S_2, t}$. Tuliskan orde dari $\tilde{\lambda}_{S_1, S_2}$ sebagai $\text{Ord}(\tilde{\lambda}_{S_1, S_2})$. Teorema berikut memberikan karakterisasi kedua bagi kode siklis- θ atas $B_{k,q}$.

Teorema 4.17 (Irwansyah, dkk., 2018b) Kode linear C atas $B_{k,q}$ dengan panjang n adalah kode siklis- θ jika dan hanya jika terdapat kode kuasi siklis- $\tilde{\theta}$ $C_1, C_2, \dots, C_{2^k}$ atas $\mathbb{F}_{p^r}$ dengan panjang n dan indeks $\text{Ord}(\tilde{\lambda}_{S_1, S_2})$ sehingga berlaku

$$C = \Psi_k^{-1}(C_1, C_2, \dots, C_{2^k}),$$

dengan $\tilde{\theta} = \phi^{t \text{Ord}(\tilde{\lambda}_{S_1, S_2})}$, untuk suatu $t \in [0, r]_{\mathbb{Z}}$, dengan ϕ adalah automorfisma Frobenius pada $\mathbb{F}_{p^r}$, dan $T_{\tilde{\theta}}(C_i) \subseteq C_j$, dengan $j \in S \cup S_2$, untuk setiap $i \in [1, 2^k]_{\mathbb{Z}}$.

Teorema terakhir di atas memberi kita sebuah algoritma untuk mengonstruksi kode siklis miring atas ring $B_{k,q}$.

Algoritma konstruksi kode siklis miring atas $B_{k,q}$.

Diberikan bilangan bulat positif n , ring $B_{k,q}$, dan automorfisma θ .

1. Dekomposisi θ menjadi $\theta = \Theta_S \circ \Lambda_{S_1, S_2, t}$.
2. Tentukan $\text{Ord}(\tilde{\lambda}_{S_1, S_2})$ dan $\tilde{\theta} = \theta|_{\mathbb{F}_{p^r}} = \phi^t$, dengan ϕ adalah automorfisma Frobenius pada $\mathbb{F}_{p^r}$.
3. Pilih kode kuasi siklis- $\tilde{\theta}$ atas $\mathbb{F}_{p^r}$, katakanlah $C_1, C_2, \dots, C_{2^k}$, sehingga
 - a. $T_{\tilde{\theta}}^t(C_i) \subseteq C_j$,
 - b. dengan $j \in S \cup S_2$, untuk setiap $i \in [1, 2^k]_{\mathbb{Z}}$.
4. Hitunglah $C = \Psi_k^{-1}(C_1, C_2, \dots, C_{2^k})$; C adalah kode siklis- θ atas $B_{k,q}$.

4.2.1.2 Kode Siklis Miring dengan Derivasi Atas Ring Non-rantai Hingga

Tujuh tahun setelah memperkenalkan gagasan kode siklis miring atas lapangan hingga, (Boucher dan Ulmer, 2014) memperumum gagasan tersebut dengan memperkenalkan apa yang disebutnya sebagai kode siklis miring atas lapangan hingga dengan derivasi. Kode ini dapat dipandang sebagai perumuman dua-langkah dari kode siklis, yakni dengan meninjau automorfisma non-identitas dan derivasi tak-nol.

Misalkan R adalah ring hingga dan $\Theta: R \rightarrow R$ adalah automorfisma pada R . Maka pemetaan $\Delta_{\Theta}: R \rightarrow R$ disebut derivasi pada R jika dua syarat berikut dipenuhi:

1. $\Delta_{\Theta}(x + y) = \Delta_{\Theta}(x) + \Delta_{\Theta}(y)$; dan
2. $\Delta_{\Theta}(xy) = \Delta_{\Theta}(x)y + \Theta(x)\Delta_{\Theta}(y)$.

Misalkan R adalah ring dengan automorfisma Θ dan derivasi Δ_Θ . Ring polinom-miring $R[x; \Theta, \Delta_\Theta]$ adalah himpunan polinom atas R dengan operasi penjumlahan polinom biasa dan operasi perkalian yang didefinisikan sebagai

$$xa := \Theta(a)x + \Delta_\Theta(a),$$

untuk setiap $a \in R$. Operasi perkalian ini diperluas secara natural pada polinom dalam $R[x; \Theta, \Delta_\Theta]$. Ring ini diperkenalkan untuk pertama kalinya oleh (Ore, 1933), dengan R adalah lapangan hingga $\mathbb{F}_q$.

Kode $C \subseteq R^n$ dikatakan kode linear- Δ_Θ dengan panjang n atas R jika C adalah submodul kiri dari $\frac{R[x; \Theta, \Delta_\Theta]}{\langle f(x) \rangle}$ atas $R[x; \Theta, \Delta_\Theta]$, dengan $f(x) \in R[x; \Theta, \Delta_\Theta]$ polinom berderajat n . Jika $f(x)$ merupakan elemen sentral maka C disebut kode linear- Δ_Θ sentral.

Kode linear $C \subseteq R^n$ dikatakan kode siklis- Δ_Θ dengan panjang n atas R jika untuk setiap $c = (c_0, c_1, \dots, c_{n-1}) \in C$ berlaku

$$T_{\Delta_\Theta}(c) := (\Theta(c_{n-1}) + \Delta_\Theta(c_0), \Theta(c_0) + \Delta_\Theta(c_1), \dots, \Theta(c_{n-2}) + \Delta_\Theta(c_{n-1})) \in C.$$

T_{Δ_Θ} kita sebut operator pergeseran siklis- Δ_Θ .

Gagasan tentang kode siklis- Δ_Θ dengan derivasi atas lapangan hingga yang pada semula diperkenalkan oleh (Boucher dan Ulmer, 2014) diperluas oleh (Sharma dan Baintwal, 2018) ke dalam ring hingga $\mathbb{Z}_4 + u\mathbb{Z}_4$, dengan $u^2 = 1$. (Ma, Gao, Li, dan Fu, 2021) lebih memperluas lagi konsep ini dengan meninjau kode kuasi siklis- Δ_Θ atas ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, dengan $u^2 = 1$. Baru-baru ini, (Patel dan Prakash, 2022) menyelidiki kode siklis- Δ_Θ atas ring $B_{2,q}$. Pada perkembangan terbaru, bersama dengan Tang, penulis (Suprijanto dan Tang, 2024+) telah menyelidiki kode siklis- Δ_Θ atas ring $\mathbb{Z}_4 + v\mathbb{Z}_4$, dengan $v^2 = 1$. Untuk penyederhanaan notasi, mulai saat ini dan selanjutnya, misalkan $R := \mathbb{Z}_4 + v\mathbb{Z}_4$, dengan $v^2 = 1$.

Tinjau dua pemetaan dari R ke R berikut:

- $\theta(a + bv) = a + b - bv$; dan
- $\Delta_\theta(a + bv) = (1 + 2v)(\theta(a + bv) - (a + bv))$.

Dapat dibuktikan dengan mudah bahwa kedua pemetaan di atas merupakan automorfisma dan derivasi pada R . Terkait automorfisma dan derivasi terkait di atas, kita memiliki sifat-sifat berikut.

Lema 4.18 (Suprijanto dan Tang, 2024+) *Ketiga pernyataan berikut dipenuhi:*

1. $\Delta_\theta \theta + \theta \Delta_\theta \equiv 0$.
2. $\Delta_\theta \Delta_\theta \equiv 0$.
3. Untuk setiap $x \in R$, berlaku $\Delta_\theta(x) = 0$ jika dan hanya jika $\theta(x) = x$.

Dengan menggunakan lema di atas kita dapat buktikan dengan mudah sifat berikut.

Lema 4.19 (Suprijanto dan Tang, 2024+) *Untuk setiap $a \in R$, berlaku hubungan $x^2 a = a x^2$.*

Sebagai akibat dari lema di atas kita peroleh sifat di bawah ini.

Akibat 4.20 (Suprijanto dan Tang, 2024+) *Untuk setiap $a \in R$ dan $n \in \mathbb{Z}^+$ berlaku hubungan*

$$x^n a = \begin{cases} (\theta(a)x + \Delta_\theta(a))x^{n-1}, & \text{jika } n \text{ ganjil,} \\ ax^n, & \text{jika } n \text{ genap.} \end{cases}$$

Karena ring R tidak komutatif, maka algoritma pembagian tidak berlaku di sini. Tetapi, sejenis algoritma pembagian, yang kita sebut algoritma pembagian-kanan, bisa kita buktikan berlaku dan banyak membantu kita dalam penyelidikan selanjutnya.

Lema 4.21 (Suprijanto dan Tang, 2024+) *Misalkan $f(x), g(x) \in R[x; \theta, \Delta_\theta]$ dengan koefisien utama dari $g(x)$ adalah unit. Maka terdapat polinom $q(x), r(x) \in R[x; \theta, \Delta_\theta]$ sehingga berlaku*

$$f(x) = q(x)g(x) + r(x),$$

dengan $r(x) = 0$ atau $\text{der}(r(x)) < \text{der}(g(x))$.

Sifat-sifat struktural dari kode siklis miring dengan derivasi atas R

Pada bagian ini akan kita sampaikan beberapa sifat struktural dari kode siklis miring dengan derivasi atas ring R . Untuk keperluan itu, kita sampaikan kembali korespondensi satu-satu berikut, yang serupa dengan yang terjadi pada kode siklis atas lapangan:

$$\frac{R[x; \theta, \Delta_\theta]}{\langle f(x) \rangle} \ni c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \mapsto (c_0, c_1, \dots, c_{n-1}) \in R^n.$$

Misalkan R_{n, Δ_θ} menyatakan ring $\frac{R[x; \theta, \Delta_\theta]}{\langle x^{n-1} \rangle}$. Maka kita peroleh beberapa sifat berikut.

Lema 4.22 (Suprijanto dan Tang, 2024+) Jika polinom $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in R_{n,\Delta_\theta}$ diidentifikasi sebagai katakode $(c_0, c_1, \dots, c_{n-1}) \in R^n$, maka $xc(x) \in R_{n,\Delta_\theta}$ diidentifikasi sebagai $T_{\Delta_\theta}(c) \in R^n$.

Lema 4.23 (Suprijanto dan Tang, 2024+) Kode $C \subseteq R^n$ adalah kode siklis- Δ_θ jika dan hanya jika C merupakan submodul kiri dari R_{n,Δ_θ} atas ring $R[x; \theta, \Delta_\theta]$.

Sebagai akibat dari sifat di atas, kita peroleh sifat yang natural bagi kode siklis di bawah ini.

Akibat 4.24 (Suprijanto dan Tang, 2024+) Jika kode $C \subseteq R^n$ adalah kode siklis- Δ_θ , maka C merupakan ideal dari R_{n,Δ_θ} .

Lebih dari itu, kita juga dapat menunjukkan bahwa sifat kode siklis- Δ_θ atas ring R dapat direduksi menjadi kode siklis atau kode kuasi siklis atas ring R , bergantung apakah panjang kode tersebut ganjil atau genap.

Lema 4.25 (Suprijanto dan Tang, 2024+) Misalkan $C \subseteq R^n$ adalah kode siklis- Δ_θ . Maka berlaku:

1. C adalah kode siklis dengan panjang n atas R , untuk n ganjil.
2. C adalah kode kuasi siklis dengan indeks 2 dan panjang n atas R , untuk n genap.

Akhirnya, kita sampaikan juga sebuah lema yang memberikan beberapa sifat dari polinom pembangkit dari kode siklis- Δ_θ .

Lema 4.26 (Suprijanto dan Tang, 2024+) Misalkan $C \subseteq R^n$ adalah kode siklis- Δ_θ dan misalkan pula $g(x)$ adalah polinom tak nol dalam C berderajat positif terkecil yang koefisien utamanya adalah unit di R . Maka berlaku

1. $C = \langle g(x) \rangle$.
2. $g(x)$ adalah pembagi kanan dari $x^n - 1$.
3. $\{g(x), xg(x), xg^2(x), \dots, x^{n-k-1}g(x)\}$ adalah basis dari C , dengan $k = \text{der}(g(x))$.

Masih banyak aspek yang bisa kita paparkan di sini terkait dengan sifat-sifat struktural dari kode siklis- Δ_θ , termasuk di dalamnya sifat-sifat yang terkait dengan dual dari kode siklis- Δ_θ . Selain itu, hal penting lain yang disampaikan adalah terkait aspek aplikasi dari menyelidiki kode siklis- Δ_θ atas ring R untuk

mengonstruksi cukup banyak kode linear baru ¹⁷ atas $\mathbb{Z}_4$ yang optimal atau mendekati optimal. Meski demikian, ruang ini, di samping waktu yang terbatas, tidak memungkinkan untuk mendeskripsikan semua itu.

4.3 Beberapa Hasil Lain Terkait Kode Linear Atas Lapangan dan Ring Hingga

Masih ada beberapa hasil penelitian penting lain yang menjadi favorit kami, dan akan kami uraikan secara ringkas di sini: (1) (Muchlis, Pradananta, Astuti, dan Suprijanto, 2021), (2) (Tang dan Suprijanto, 2023a), dan (3) (Tang dan Suprijanto, 2023b).

Pada artikel yang disebutkan pertama, kami berhasil memberikan nilai eksak bagi dimensi dari *twisted centralizer codes* dengan pendekatan yang elementer, ketika para peneliti di bidang ini -termasuk dua “orang besar” di dalamnya, yakni Cheryl Praeger dan Patrick Solé- meyakini bahwa penentuan dimensi itu “bukanlah merupakan masalah yang trivial.”¹⁸ Lebih dari itu, kami juga berhasil memberikan algoritma untuk mengonstruksi basis dari kode yang dimaksud. Pada artikel kedua, kami berhasil memberikan bukti alternatif dan elementer bagi batas Plotkin untuk kode linear atas ring $\mathbb{Z}_4$, dan memberikan sebuah pendekatan baru untuk mengonstruksi kode linear atas ring $\mathbb{Z}_4$ ini. Melalui metode baru ini, kami berhasil mengonstruksi banyak kode linear optimal atas $\mathbb{Z}_4$ yang belum diketahui sebelumnya¹⁹. Pada artikel ketiga, kami berhasil memberikan semua parameter yang mungkin bagi kode linear yang memiliki tepat dua bobot saja (*two-weight codes*) optimal atas ring $\mathbb{Z}_4$. Kami juga memberikan sebuah metode untuk mengonstruksi kode optimal tersebut, di mana metode konstruksi yang telah diketahui sebelumnya²⁰ hanyalah merupakan kasus khusus saja dari metode konstruksi yang kami perkenalkan.

¹⁷ Klaim kebaruan ini didasarkan pada fakta bahwa kode optimal atau hampir optimal yang kami hasilkan tersebut belum ada di dalam database berikut: <http://quantumcodes.info/Z4>.

¹⁸ “In general determining the dimension of such a code given A is a non-trivial problem, and we were only able to give a spectral characterization of the dimension over an extension of the base field” (lihat hal.76 dalam A. Alahmadi, S. Alamoudi, S. Karadeniz, B. Yildiz, C.E. Praeger, P. Solé, “Centraliser codes,” *Linear Algebra Appl.* **463** (2014) 68-77.)

¹⁹ Lihat catatan 16.

²⁰ Lihat, misalnya, metode yang diperkenalkan oleh Shi M., Xuan W., Solé P., Two families of two-weight codes over $\mathbb{Z}_4$, *Des. Codes Cryptogr.* **88**(12), 2493–2505 (2020).

5. PENUTUP

Teori desain, khususnya *spherical designs* dan *Euclidean designs*, dan teori koding -dua objek penting dalam kombinatorika aljabar- masih menyisakan sangat banyak masalah terbuka untuk dikaji lebih lanjut. Satu hal yang sangat menarik dari kedua objek kombinatorika ini adalah bahwa kajian atas keduanya hampir selalu menggunakan cabang matematika lain, termasuk di dalamnya bentuk-bentuk modular (*modular forms*), teori bilangan geometris (*geometric number theory*) -khususnya teori latis (*lattices theory*)-, teori lapangan hingga dan ring hingga, untuk sekedar menyebut beberapa di antaranya. Di sinilah salah satu aspek keindahan dari objek kajian ini. Keindahan lainnya dari kedua objek kajian ini adalah bahwa aspek aplikasi dari teori desain dan teori koding dapat dideskripsikan kepada masyarakat umum dalam bahasa yang mudah mereka pahami.

Sebagai penutup, kami ingin kutipkan kembali sebuah pernyataan dari Israel M. Gelfand (1913-2009), seorang matematikawan Rusia, yang memotivasi kami untuk bekerja lebih dalam dan lebih serius di dalam bidang kombinatorika aljabar:

“The older I get, the more I believe that at the bottom of most deep mathematical problems there is a combinatorial problem”— Lecture to Courant Institute (1990).

6. UCAPAN TERIMA KASIH

Pupung Pursita Dewi (istri), Muhammad Dafnis Fazlur Rahman, Felicitia Ifianasa Lathifah, dan Malvin Faikar Rahman (anak) —*atas doa, kebaikan dan keberkahan yang tidak pernah putus serta kesabaran dan kasih sayang selama ini.*

Bapak Ibu: H. Soedigdo dan Hj. Kasimah. Ayah Ibu mertua: H. Im Bunyamin Hidayat (alm), Hj. E. Suharah —atas asuhan sayang dan didikan sejak kecil hingga dewasa.

Adik-adik: Rita Andrijani, Tri Susianti, Harry Septanto, serta kakak adik ipar: Dudi Djanuardi, Oki Fitriadi, Dian Pramitasari, Uu Tjatja Kurnia, Teti Sustiwati, Erwan Muhammad Yamin, Gunawan Martawiguna, Karina Kamarullah, Tika Ratna Juwita, Fadli Purnomo —atas perhatian dan dukungan semangat dalam menempuh studi dan karier.

Dosen pembimbing studi di perguruan tinggi: Ahmad Muchlis, Ph.D. (Sarjana, Institut Teknologi Bandung), Prof. Edy Tri Baskoro, Ph.D. (magister, Institut Teknologi Bandung), Prof. DSc. Eiichi Bannai (MMath, Ph.D., Kyushu University, Jepang) —atas limpahan ilmu yang diberikan.

Guru-guru saat belajar di SMAN 3-Bandung, SMPN 7-Bandung, SDN Tilil IV Bandung —atas bimbingan ilmu dan dasar pendidikan yang diberikan. Secara khusus saya ingin menyebut Ibu Rusmaeni (almh.) guru matematika SD, Bapak Herawan (alm.), guru matematika SMP, dan Bapak Obos (alm.), guru matematika SMA. Ketiganya telah berperan penting atas tumbuhnya minat saya pada matematika.

Prof. Etsuko Bannai, Ph.D. (Kyushu University, Jepang), Prof. Akihiro Munemasa, Ph.D. (Tohoku University, Jepang), Prof. Hajime Tanaka, PhD (Tohoku University, Jepang) —atas dukungan dalam membangun ilmu dan jejaring riset dunia.

Pemberi rekomendasi: Prof. Edy Tri Baskoro, Ph.D., Prof. Dr. M. Salman A. N., Prof. Dr. Umar Fauzi, Prof. Dr. Trio Adiono, Prof. Satria Bijaksana, Ph.D., Prof. Slamini, Ph.D., Prof. DSc. Eiichi Bannai (Kyushu University), Prof. Akihiro Munemasa, Ph.D. (Tohoku University) —atas dukungan untuk mencapai jabatan tinggi.

Pembimbing tugas akhir S1: Ahmad Muchlis, Ph.D. – atas diberikannya kesempatan menjadi dosen ITB.

Sekretaris Jurusan Matematika, Hidayat Sardi, M.Si – atas upayanya untuk meyakinkan saya bahwa menjadi dosen ITB adalah profesi yang tepat untuk saya.

Ketua FGB ITB: Prof. Dr. Edy Tri Baskoro dan Prof. Dr. Mindriany Syafila —atas izin dan rekomendasi dalam pengajuan jabatan guru besar.

Ketua Senat Akademik ITB. Ketua Senat FMIPA ITB: Prof. Akhmaloka, Ph.D. —atas dukungan rekomendasi untuk memulai pengajuan kenaikan jabatan guru besar.

Dekanat FMIPA ITB: Prof. Ir. Wahyu Srigutomo, Ph.D., Prof. Dr. Rukman Hertadi, Dr. Hanni Garminia Y. —atas rekomendasi awal fakultas dalam memproses kenaikan jabatan guru besar.

Ketua dan anggota KK Matematika Kombinatorika FMIPA ITB: Prof. Edy Tri Baskoro, Ph.D., Prof. Dr. M. Salman A.N., Prof. Hilda Assiyatun, Ph.D., Dr. Saladin Uttunggadewa, Warsoma Djohan, M.Si, Dr. Aditya Purwa Santika, Dr. Erma Suwastika, Pritta Etriana Putri, Ph.D., Dr. Finny Oktariani, Dr. Rinovia Simanjuntak, Dr. Suhadi Wido Saputro, Yusuf Hafidh, M.Si. —atas kerja sama perkuliahan/pengajaran dan bimbingan mahasiswa.

Tim/jejaring riset: Prof. Edy Tri Baskoro, Ph.D., Prof. Dr. M. Salman A.N., Prof. Hilda Assiyatun, Ph.D., Prof. Dr. Pudji Astuti, Prof. Dr. Muchtadi Intan Detiena, Prof. Khreshna Imaduddin Ahmad Syuhada, Ph.D., Ahmad Muchlis, Ph.D., Aleams Barra, Ph.D., Dr. Irwansyah, Dr. Aditya Purwa Santika, Dr. Kristiana Wijaya, Dr. Harry Septanto, Dr. Nopendri, Dr. Arif Rahman Hakim, Hopein Christofen Tang, M.Si., Galih Pradananta, M.Si., Bustomi, M.Si., Prof. Dr. Patrick Sole (Prof Patrick Sole (the Centrale Marseille, CNRS, I2M, Aix Marseille University, Perancis), Prof. Dr. Steven Dougherty (Scranton University, USA), Olfa Yemen, Ph.D. (Université de Tunis El Manar, Institut Préparatoire aux Etudes d'Ingénieur de EL Manar, Tunisia) —atas terbangunnya jejaring riset yang baik dan terus aktif melakukan riset bereputasi.

Tim pembimbing S-3 Matematika FMIPA ITB: Aleams Barra, Ph.D. —*atas kesediaan untuk membangun riset tingkat doktoral.*

Guru Besar, Majelis, Kaprodi, Kolega Dosen Matematika FMIPA ITB: Prof. Dr. Edy Soewono, Prof. Dr. Kuntjoro Adji Sidarto, Prof. Marcus Wono Setyabudhi, Ph.D., Prof. Dr. Irawati, Prof. Dr. Pudji Astuti Waluyo, Prof. Iwan Pranoto, Ph.D., Prof. Leo Hari Wiryanto, Ph.D., Prof. Dr. Hendra Gunawan, Prof. Hilda Assiyatun, Ph.D., Prof. Dr. Agus Yodi Gunawan, Prof. Novriana Sumarti, Ph.D., Prof. Dr. Nuning Nuraini, Koko Martono, M.Si. (alm), Muhammad Syamsuddin, Ph.D. (alm), Warsoma Djohan, M.Si., Dr. Saladin Uttunggadewa, Yudi Soeharyadi, Ph.D., Dr. Rieske Hadiani, Rinovia Mery Garnierita Simanjuntak, Ph.D., Pritta Etriana Putri, Ph.D., Dr. Dewi Handayani, Dr. Elvira Kusniyanti, Dr. Rudy Kusdiantara, Denny Iwanal Hakim, Ph.D., Ifronika, M.Si. – *atas kerja sama akademik dan komunitas.*

Secara khusus, saya ingin menyebut tiga nama: Prof. Khreshna Imaduddin Ahmad Syuhada, Ph.D., Oki Neswan, Ph.D., dan Warsoma Djohan, M.Si.—*atas kerja sama dalam berbagi tawa, khususnya dalam menertawakan diri sendiri.*

Tenaga kependidikan FMIPA dan Matematika ITB: Dei Mahmud, S.T., Teh Yunita Fatmawati, Pak Tatang, Bu Noi Sukmawati, Teh Dina – *atas bantuan administrasi akademik dan kepegawaian.*

Mahasiswa S-3/S-2/S-1 –*atas kesabaran dalam proses perkuliahan dan bimbingan disertasi/tesis/tugas akhir.* Secara khusus saya harus menyebut lima nama: Ricky Aditya (mahasiswa bimbingan S-3), Irwansyah (mahasiswa S-3, kawan diskusi), Muhammad Samy Baladram (mahasiswa bimbingan S-1), Hopein Christofen Tang (mahasiswa bimbingan S-1 dan S-2), dan Galih Pradananta (mahasiswa S-2, kawan diskusi).

DAFTAR PUSTAKA

- T. Abualrub dan I. Siap, (2007), Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.* **42**(3), 273-287.
- A. Alahmadi, S. Alamoudi, S. Karadeniz, B. Yildiz, C.E. Praeger, P. Solé, (2014), Centraliser codes, *Linear Algebra Appl.* **463**, 68-77.
- A. Alahmadi, S.P. Glasby, C.E. Praeger, P. Solé, B. Yildiz, (2017), Twisted centralizer codes, *Linear Algebra Appl.* **524**, 235-249.
- A. Alahmadi, S.P. Glasby, C.E. Praeger, (2017), On the dimension of twisted centralizer codes, *Finite Fields Appl.* **48**, 43-59.
- E. F. Assmus and J. E. Key, (1994), *Designs and their Codes*, Cambridge.
- E. F. Assmus Jr. dan H. F. Mattson, (1963), Error-correcting codes: An axiomatic approach, *Inf. Control* **6**, 315-330.
- C. Bachoc, (1999), On harmonic weight enumerators of binary codes, in: Designs and Codes: A Memorial Tribute to Ed Assmus, *Des. Codes Cryptogr.* **18** (1-3) (1999) 11-28.
- C. Bachoc, (2005), Designs, groups and lattices, *J. Theor. Nombres Bordeaux* **17**(1), 25-44.
- C. Bachoc, (2006), Linear programming bounds for codes in Grassmannian spaces, *IEEE Trans. Inform. Theory* **52**(5), 2111-2125.
- C. Bachoc, E. Bannai, dan R. Coulangeon, (2004), Codes and designs in Grassmannian spaces, *Discrete Math.* **277**(1-3), 15-28.
- C. Bachoc, R. Coulangeon, dan G. Nebe, (2002), Designs in Grassmannian spaces and lattices, *J. Algebraic Combin.* **16**(1), 5-19.
- B. Bajnok, (2006), On Euclidean designs, *Adv. Geom.* **6**(3), 423-438.
- B. Bajnok, (2007), Orbits of the hyperoctahedral group as Euclidean designs, *J. Algebraic Combin.* **25**(4) 357-471.
- M.S. Baladram dan D. Suprijanto, (2014), New spherical $(2s + 1)$ -designs from Kuperberg's set: an experimental result, *Appl. Math. Comput.* **249**, 45-52.
- R.K. Bandi dan M. Bhaintwal, (2016), A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Discrete Math. Algorithms Appl.* **8**(1), 1650017.
- Et. Bannai, (2006), On antipodal Euclidean tight $(2e + 1)$ -designs, *J. Algebraic Combin.* **24**(4), 391-414.

- Et. Bannai, (2009), New examples of Euclidean tight 4-designs, *European J. Combin.* **13**(3), 665-667.
- E. Bannai dan Et. Bannai, Tight Gaussian 4-designs, (2005), *European J. Combin.* **22**(1), 39-63.
- E. Bannai dan Et. Bannai, (2006), On optimal tight 4-designs on 2 concentric spheres, *European J. Combin.* **27**(2), 179-192.
- E. Bannai, E. Bannai, (2008), Spherical designs and Euclidean designs, in: *Recent Developments in Algebra and Related Areas*, ALM, vol. 8, Higher Education Press and International Press, Beijing, Boston, 1-37.
- E. Bannai dan Et. Bannai, (2009), A survey on spherical designs and algebraic combinatorics on spheres, *European J. Combin.* **30**(6), 1392-1425.
- E. Bannai dan Et. Bannai, (2010), Euclidean designs and coherent configurations, in *Combinatorics and graphs, Contem. Math.* **531**, R. A. Brualdi et al. (Eds), 59-94.
- E. Bannai dan Et. Bannai, (2011), Tight 9-designs on two concentric spheres, *J. Math. Soc. Japan* **63**(4), 1359-1376.
- E. Bannai dan Et. Bannai, (2014), Tight t-designs on two concentric spheres, *Mosc. J. Comb. Number Theory* **4**(1), 52-77.
- E. Bannai dan Et. Bannai, Tight Euclidean 4-designs, (2006), *J. Math. Soc. Japan* **58**(3), 775-804.
- E. Bannai, Et. Bannai, T. Ito, dan R. Tanaka, (2021), *Algebraic combinatorics*, Walter de Gruyter, Berlin/ Boston.
- E. Bannai, Et. Bannai, dan D. Suprijanto, (2007), On the strong nonrigidity of certain tight Euclidean designs, *European J. Combin.* **28**(6), 1662-1680.
- E. Bannai dan S.G. Hoggar, (1985), On tight t-designs in compact symmetric spaces of rank one, *Proc. Japan Acad. Ser. A Math. Sci.* **61**(3), 78-82.
- E. Bannai dan S.G. Hoggar, (1989), Tight t-designs and squarefree integers, *European J. Combin.* **10**(2), 113-135.
- E. Bannai dan T. Ito, (1984) *Algebraic combinatorics I: Association schemes*, Benjamin/ Cummings, Menlo Park, California.
- I.F. Blake, (1972), Codes over certain rings, *Inf. Control* **20**, 396-404.
- I.F. Blake, (1975), Codes over integer residue rings, *Inf. Control* **29**, 295-300.
- L.S. Borrows dan B.M. Franaszczuk, (1973), On cyclic codes generated by graphs, *Inf. Control* **22**, 296-301.
- D. Boucher, W. Geiselmann, dan F. Ulmer, (2007), Skew cyclic codes, *Appl. Algebra Engrg. Comm. Comput.* **18**(4), 379-389.

- D. Boucher, Sole, dan Ulmer, (2008), Skew constacyclic codes over Galois rings, *Adv. Math. Commun.* **2**(3), 273-292.
- D. Boucher dan F. Ulmer, (2009), Coding with skew polynomial rings, *J. Symb. Comput.* **44**(3-4), 1644-1656.
- D. Boucher dan F. Ulmer, (2009), Coding as modules over skew polynomial rings, in Proceedings of the 12th IMA Conference on Cryptography and Coding, *Lecture Notes in Comput. Sci.* **5921**, 38-55.
- D. Boucher dan F. Ulmer, (2014), Linear codes using skew polynomials with automorphisms and derivations, *Des. Codes Cryptogr.* **70**(3), 405-431.
- A.R. Calderbank dan N.J.A. Sloane, (1995) Modular and p -adic cyclic codes, *Des. Codes Cryptogr.* **6**(1), 21-35.
- A. R. Calderbank dan N. J. A. Sloane, (1997), Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, *J. Algebraic Combin.* **6**(2), 119-131.
- Y. Cengellenmis, A. Dertli, dan S.T. Dougherty, (2014), Codes over an infinite family of rings with a Gray map, *Des. Codes Cryptogr.*, **72**(3), 559-580.
- H.Q. Dinh dan S. R. Lopez-Permouth, (2004), Cyclic and negacyclic codes over finite chain ring, *IEEE Trans. Inform. Theory* **45**(4), 1728-1744.
- S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, dan P. Sole, (1999), Type IV self-dual codes over rings, *IEEE Trans. Inform. Theory* **45**(7), 2345-2360.
- S.T. Dougherty, J.-L. Kim, and P. Sole, (2007), Doubly circulant codes from two class association schemes, *Adv. Math. Commun.* **1**(1), 45-64.
- P. Gaborit, Quadratic double circulant codes over fields, (2002), *J. Combin. Theory Ser. A* **97**(1), 85-107.
- T. Gowers, J.-B. Green, dan I. Leader (Editors), (2008), *Princeton Companion to Mathematics*, Princeton University Press.
- A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, dan P. Sole, (1994), The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals and Related Codes, *IEEE Trans. Inform. Theory* **40**(2), 301-319.
- W.C. Huffman dan V. Pless, (2003), *Fundamentals of Error Correcting Codes*, Cambridge University Press.
- Irwansyah, A. Barra, S.T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Sole, D. Suprijanto, dan O. Yemen, (2016), Θ_5 -cyclic codes over A_k , *Int. J. Comput. Math. Comput. Syst. Theory* **1**(1), 14-31.
- Irwansyah, A. Barra, A. Muchlis, I. Muchtadi-Alamsyah, dan D. Suprijanto, (2018), Skew cyclic codes over B_k , *J. Appl. Math. Comput.* **57**(1-2), 69-84.

- Irwansyah and D. Suprijanto, Structure of linear codes over the ring B_k , (2018), *J. Appl. Math. Comput.* **58**(1-2), 755-775.
- Irwansyah dan D. Suprijanto, (2023), Linear codes over a general infinite family of rings and MacWilliams-type relations, *Discrete Math. Lett.* **11**, 53-60.
- S. Jitman, S. Ling, and P. Udomkavanich, (2021), Skew constacyclic codes over finite chain rings, *Ad. Math. Commun.* **6**(1), 39-63.
- P. Kanwar and S. R. Lopez-Permouth, (1997), Cyclic codes over the integers modulo p^m , *Finite Fields Appl.* **3**(4), 119-131.
- J.-L. Kim and P. Sole, (2008), Skew Hadamard designs and their codes, *Des. Codes Cryptogr.* **49**(1-3), 135-145.
- O. Ore, (1933), Theory of non-commutative polynomials, *Annals. Math.* **34**, 480-508.
- F. Ma, J. Gao, J. Li, and F.-W. Li, (2021), (σ, δ) -Skew quasi-cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Cryptogr. Commun.* **13**(2), 307-320.
- F.J. MacWilliams, N.J.A. Sloane, (1977), *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam.
- A. Muchlis, G. Pradananta, P. Astuti, dan D. Suprijanto, (2021), On bases and the dimensions of twisted centralizer codes, *Finite Fields Appl.* **73**, 101862.
- G. Norton dan A. Salagean-Mandache, (2000), On the structure of linear codes over finite chain rings, *Appl. Algebra Eng. Commun. Comput.* **10**(6), 489-506.
- S. Patel and O. Prakash, (2022), (θ, δ_θ) -Cyclic codes over $\frac{\mathbb{F}_q[u,v]}{\langle u^2-u, v^2-v, uv-vu \rangle}$, *Des. Codes Cryptogr.* **90**(11), 2763-2781.
- E. Prange, (1957), Cyclic error-correcting codes in two symbols, *AFCRC-TN-57-103*, Air Force Cambridge Research Center, Cambridge, Mass, Sept. 1957.
- E. Prange, (1958), Some cyclic error-correcting codes with simple decoding algorithms, *AFCRC-TN-58-156*, Air Force Cambridge Research Center, Cambridge, Mass, April. 1958.
- P. Shankar, (1979), On BCH codes over arbitrary integer rings, *IEEE Trans. Inform. Theory* **25**(4), 480-483.
- C.E. Shannon, (1948), A mathematical theory of communication, *Bell System Tech. J.* **27**(3), 379-423, dan **27**(4) (1948), 623-656.

- A. Sharma and M. Bhaintwal, (2018), A class of skew cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, with derivation, *Adv. Math. Commun.* **12**(4), 723-739.
- E. Spiegel, (1977), Code over $\mathbb{Z}_m$, *Inf. Control* **35**, 48-51.
- E. Spiegel, (1978), Codes over $\mathbb{Z}_m$ revisited, *Inf. Control* **37**, 100-104.
- D. Suprijanto, (2011), On tight Euclidean 6-designs: an experimental result, *ITB J. Science* **43** A(1), 19-42.
- D. Suprijanto and T. Nugraha, (2016), A note on linear codes from Johnson graphs, *JP Journal of Algebra Number Theory App.* **38**(5), 473-488.
- D. Suprijanto and H.C. Tang, (2024+), Skew cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with derivation, *Commun. Comb. Optim.* (akan terbit), tersedia di https://comb-opt.azaruniv.ac.ir/article_14686.html.
- D. Suprijanto and H.C. Tang, (2022), Quantum codes constructed from cyclic codes over a finite non-chain ring, *IAENG Int. J. Comput. Sci.* **49**(3), 695-700.
- D. Suprijanto and Irwansyah, Constacyclic codes over the ring $B_{k,q}$ and quantum codes, (*tentative title, a work in preparation*).
- H. Tapia-Recillas and G. Vega, (2003), Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes, *Discrete Appl. Math.* **128**(1 SPEC), 305-316.
- H.C. Tang and D. Suprijanto, (2023), New optimal linear codes over $\mathbb{Z}_4$, *Bull. Aust. Math. Soc.* **107**(1), 158-169.
- H.C. Tang and D. Suprijanto, (2023), A general family of Plotkin-optimal two-weight codes over $\mathbb{Z}_4$, *Des, Codes Cryptogr.* **91**(5), 1737-1750.
- V.D. Tonchev, Codes and Designs, in: V.S. Pless, W.C. Huffman (Eds.), (1998), *Handbook of Coding Theory*, Chapter 15, Elsevier, Amsterdam, 1229-1267.
- V.D. Tonchev, (2002), Error-correcting codes from graphs, *Discr. Math.* **257**(2-3), 549-557.
- J. Wolfmann, (1999), Negacyclic and cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **45**(7), 2527-2532.
- J. Wood, (1999), Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* **121**(3), 555-575.

CURRICULUM VITAE



Nama : Prof. Djoko Suprijanto, Ph.D.
Tempat/tgl lahir : Bandung, 16 September 1970
Kel. Keahlian : Matematika Kombinatorika
Alamat Kantor : Jl. Ganesha 10, Bandung
Nama Istri : Pupung Pursita Dewi, SPSi
Nama Anak : 1. Muhammad Dafnis Fazlur Rahman
2. Felicitia Ifianasa Lathifah
3. Malvin Faikar Rahman

I. RIWAYAT PENDIDIKAN

- Doctor of Philosophy (Ph.D.), Graduate School of Mathematics, Kyushu University, Jepang, 2004-2007.
- Master of Mathematics (M.Math), Graduate School of Mathematics, Kyushu University, Jepang, 2002-2004.
- Magister Sains (M.Si.), Departemen Matematika, Institut Teknologi Bandung, Indonesia, 1995-1998.
- Sarjana Sains (S.Si.), Departemen Matematika, Institut Teknologi Bandung, Indonesia, 1989-1994.

II. RIWAYAT KERJA DI ITB

- Staf Pengajar Matematika FMIPA ITB, 1996 – Sekarang
- Asesor Beban Kerja Dosen (BKD), Sem. I 2022/2023 – Sekarang
- Anggota Majelis Keilmuan Matematika ITB, 2024 – Sekarang
- Ketua Kelompok Keahlian Matematika Kombinatorika, Februari 2016-Desember 2020.
- Ketua Program Studi Magister Pengajaran Matematika dan Magister Aktuaria, Januari 2015 – Januari 2016.
- Ketua Tim Reakreditasi Program Studi Magister Pengajaran Matematika FMIPA ITB, Sem. I 2015/2016.

III. RIWAYAT KEPANGKATAN

- Pembina Tingkat I, IV/b 1 April 2024
- Pembina, IV/a 1 April 2016
- Penata Tingkat I, III/d 1 April 2014
- Penata, III/c 1 April 2009
- Penata Muda Tingkat I, III/b 1 April 2001
- Penata Muda, III/a 1 Januari 1996

IV. RIWAYAT JABATAN FUNGSIONAL

- Profesor/Guru Besar 1 Oktober 2023
- Lektor Kepala 1 Oktober 2013
- Lektor 1 Desember 2008
- Asisten Ahli 1 Januari 2001
- Asisten Ahli Madya 1 Desember 1998

V. KEGIATAN PENELITIAN

1. Ketua Tim Riset Unggulan ITB (2024), Kode skew siklis atas ring hingga dengan derivasi dan aplikasinya dalam konstruksi kode kuantum (II).
2. Ketua Tim Riset Unggulan ITB (2023), Kode skew siklis atas ring hingga dengan derivasi dan aplikasinya dalam konstruksi kode kuantum.
3. Ketua Tim Riset Unggulan ITB (2022), Kode siklis atas ring hingga non-rantai dan aplikasinya dalam konstruksi kode kuantum.
4. Ketua Tim Penelitian Dasar Kompetitif Nasional (tahun ke-3) (2022), Kode optimal atas grup abelian hingga dan aplikasinya dalam keamanan sistem informasi dan komunikasi.
5. Ketua Tim Riset Unggulan ITB (2021), Kode skew constasiklis atas ring hingga non-rantai dan aplikasinya dalam konstruksi kode kuantum.
6. Ketua Tim Penelitian Dasar Kompetitif Nasional (tahun ke-2) (2021), Kode optimal atas grup abelian hingga dan aplikasinya dalam keamanan sistem informasi dan komunikasi.
7. Anggota Tim Research Grant Bank Indonesia (BI Institute) (2021), Pemodelan stokastik untuk memprediksi risiko stablecoin dan Bitcoin dengan melibatkan kebergantungannya terhadap risiko energi dan nilai tukar rupiah-dolar AS selama pandemi COVID-19.

8. Ketua Tim Penelitian Dasar Unggulan Perguruan Tinggi (tahun ke-2) (2021), Kode LCD atas ring hingga dan keamanan dalam sistem komunikasi.
9. Ketua Program Riset ITB (2020), Kode swa-dual skew siklis dan skew negasiklis optimal atas ring hingga.
10. Ketua Tim Penelitian Dasar Kompetitif Nasional (tahun ke-1) (2020), Kode optimal atas grup abelian hingga dan aplikasinya dalam keamanan sistem informasi dan komunikasi.
11. Ketua Tim Penelitian Dasar Unggulan Perguruan Tinggi (tahun ke-1) (2020), Kode LCD atas ring hingga dan keamanan dalam sistem komunikasi.
12. Ketua Tim Penelitian Berbasis Kompetensi (tahun ke-3) Ristekdikti; (2019), Konstruksi kode linear atas grup abelian hingga dengan kemampuan optimal dalam koreksi kesalahan jika digunakan dalam transmisi informasi.
13. Ketua Tim Penelitian Unggulan Perguruan Tinggi (tahun ke-2) Ristekdikti; (2019), Kode siklis atas ring hingga yang memiliki kemampuan optimal dalam aplikasi di dunia telekomunikasi.
14. Ketua Program Riset ITB (2019), Kode skew siklis optimal atas ring hingga R_k
15. Ketua Tim Penelitian Berbasis Kompetensi (tahun ke-2) Ristekdikti; (2018), Konstruksi kode linear atas grup abelian hingga dengan kemampuan optimal dalam koreksi kesalahan jika digunakan dalam transmisi informasi.
16. Ketua Tim Penelitian Unggulan Perguruan Tinggi (tahun ke-2) Ristekdikti; (2018), Kode siklis atas ring hingga yang memiliki kemampuan optimal dalam aplikasi di dunia telekomunikasi.
17. Ketua Program Riset ITB (2017), Kode swa-dual optimal atas ring hingga (II).
18. Ketua Tim Penelitian Berbasis Kompetensi (tahun ke-1) Ristekdikti; (2017), Konstruksi kode linear atas grup abelian hingga dengan kemampuan optimal dalam koreksi kesalahan jika digunakan dalam transmisi informasi.
19. Ketua Tim Penelitian Unggulan Perguruan Tinggi (tahun ke-1) Ristekdikti; (2017), Kode siklis atas ring hingga yang memiliki kemampuan optimal dalam aplikasi di dunia telekomunikasi.

20. Ketua Tim Riset Unggulan Perguruan Tinggi [Desentralisasi ITB-Dikti tahun ke-2] Ristekdikti ; (2016), Konstruksi kode swa-dual MDS dan near MDS atas ring hingga (II).
21. Ketua Tim Riset ITB (2016), Kode swa-dual optimal atas ring hingga.
22. Ketua Tim Riset Unggulan Perguruan Tinggi [Desentralisasi ITB-Dikti tahun ke-1] Ristekdikti ; (2015), Konstruksi kode swa-dual MDS dan near MDS atas ring hingga (II).
23. Ketua Tim Riset KK ITB (2015), Konstruksi kode swa-dual MDS dan near MDS atas lapangan hingga (IV)
24. Ketua Tim Riset KK ITB (2014), Konstruksi kode swa-dual MDS dan near MDS atas lapangan hingga (III).
25. Ketua Tim Riset Unggulan Perguruan Tinggi [Desentralisasi ITB-Dikti tahun ke-1] Ristekdikti ; (2013), Konstruksi kode swa-dual MDS dan near MDS atas ring hingga.
26. Ketua Tim Riset KK ITB (2013), Konstruksi kode swa-dual MDS dan near MDS atas lapangan hingga (II).
27. Ketua Tim Riset KK ITB (2012), Konstruksi kode swa-dual MDS dan near MDS atas lapangan hingga (I).
28. Ketua Tim Hibah Riset IA ITB; 2011-2012, Kode swa-dual dari graf strongly regular.
29. Ketua Tim Riset KK ITB (2011), Kode swa-dual atas grup abelian hingga $\mathbb{Z}_2 \times \mathbb{Z}_2$ dan $\mathbb{Z}_4 \times \mathbb{Z}_4$.
30. Ketua Tim Riset KK ITB (2010), Kode Tipe II atas grup abelian hingga $\mathbb{Z}_p \times \mathbb{Z}_p$

VI. PUBLIKASI

1. H. C. Tang and **D. Suprijanto**, "A general family of Plotkin-optimal two-weight codes over $\mathbb{Z}_{2^r}$," *Art Discrete and Applied Mathematics* (under review).
2. **D. Suprijanto** and Irwansyah, "Skew-cyclic and skew-quasi-cyclic codes over a general infinite family of rings," *Communications in Combinatorics and Optimization* (under review).
3. H. Septanto and **D. Suprijanto**, "A novel smooth quaternion-based attitude tracking control", *Advances in Space Research* (accepted for publication) (versi online dapat diakses di:
<https://www.science-direct.com/science/article/pii/S0273117724010020>).

4. **D. Suprijanto** and H.C. Tang, "Skew cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ with derivation," *Communications in Combinatorics and Optimization* (accepted for publication) (versi online dapat diakses di: http://comb-opt.azaruniv.ac.ir/article_14686.html).
5. K. Syuhada, A. Hakim, and **D. Suprijanto**, "Assessing systemic risk and connectedness among dirty and clean energy market from quantile and expectile perspectives," *Energy Economics* **129** (2024), 107261.
6. **D. Suprijanto**, "Linear codes and cyclic codes over finite rings and their generalizations: a survey," *Electronic Journal of Graph Theory and Applications* **11**(2) (2023), 467-490.
7. H.C. Tang and **D. Suprijanto**, "A genaral family of Plotkin-optimal two-weight codes over $\mathbb{Z}_4$," *Designs, Codes, and Cryptography* **91**(5) (2023), 1737-1750.
8. H.C. Tang and **D. Suprijanto**, "New optimal linear codes over $\mathbb{Z}_4$," *Bulletin of the Australian Mathematical Society* **107**(1) (2023), 158-169.
9. H. Septanto, E. Kurniawan, and **D. Suprijanto**, "Quaternion feedback attitude control system design based on weighted-L2-gain performance," *Results in Engineering* **17** (2023), 100717.
10. Irwansyah and **D. Suprijanto**, "Linear codes over a general infinite family of rings and MacWilliams-types relations," *Discrete Mathematics Letters* **11** (2023), 53-60.
11. K. Syuhada, A. Hakim, **D. Suprijanto**, I. Muchtadi-Alamsyah, and L. Arbi, "Is Tether a safe haven of safe haven amid COVID-19? An assesment against Bitcoin and oil using improved measure of risk," *Resources Policy* **79** (2022), 103111.
12. **D. Suprijanto** and H.C. Tang, "Quantum codes constructed from cyclic codes over a finite non-chain ring," *IAENG International Journal of Computer Science* **49**(3) (2022), IJCS_49_3_08.
13. K. Syuhada, **D. Suprijanto**, and A. Hakim, "Comparing gold's and Bitcoin's safe-haven roles against energy commodities during the COVID-19 outbreak: A vine copula approach," *Finance Research Letters* **46** (2022).
14. Nopendri, I. Muchtadi-Alamsyah, **D. Suprijanto**, and A. Barra, "Cyclic codes from a sequence over finite fields," *European Journal of Pure and Applied Mathematics* **14** (3) (2021), 685-694.
15. Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, and **D. Suprijanto**, "A note on the construction and enumeration of Euclidean

- self-dual skew-cyclic codes” *Applicable Algebra in Engineering, Communications, and Computing* **32** (2) (2021), 345-358.
16. S. Rosdiana, M.I. Detiena, **D. Suprijanto**, and A. Barra, “On linear codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$,” *IAENG International Journal of Applied Mathematics* **51** (1) (2021), 1-9.
 17. A. Muchlis, G. Pradananta, P. Astuti, and **D. Suprijanto**, “On bases and the dimensions of twisted centralizer codes,” *Finite Fields and Their Applications* **73** (2021), 101862, 17 pp.
 18. Bustomi, A.P. Santika, and **D. Suprijanto**, “Linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$,” *IAENG International Journal of Computer Science* **48** (2) (2021), 1-11.
 19. K. Wijaya, E.T. Baskoro, H. Assiyatun, and **D. Suprijanto**, “Subdivision of graph in $R(mK_2, P_4)$,” *Heliyon* **6** (6) (2020), Article number e03843.
 20. Irwansyah and **D. Suprijanto**, “Structure of linear codes over the ring B_k ” *Journal of Applied Mathematics and Computing* **58** (3-4) (2018), 755-775.
 21. Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, and **D. Suprijanto**, “Skew-cyclic codes over B_k ” *Journal of Applied Mathematics and Computing* **57** (1-2) (2018), 69-84.
 22. K. Wijaya, E.T. Baskoro, H. Assiyatun, and **D. Suprijanto**, “On Ramsey $(4K_2, P_3)$ -minimal graphs,” *AKCE International Journal of Graphs and Combinatorics* **15** (2018), 174–186.
 23. H. Septanto and **D. Suprijanto**, “Asymptotic stability of quaternion-based attitude control system with saturation function,” *International Journal of Electrical and Computer Engineering (IJECE)* **7** (1) (2017), 1994-2001.
 24. Irwansyah, I. Muchtadi-Alamsyah, A. Muchlis, A. Barra, and **D. Suprijanto**, “Codes over an infinite family of algebras” *Journal of Algebra, Combinatorics, Discrete Structures and Applications* **4** (2) (2017), 131-140.
 25. K. Wijaya, E.T. Baskoro, H. Assiyatun, and **D. Suprijanto**, “On Ramsey (mK_2, H) -minimal graphs,” *Graphs and Combinatorics* **31** (1) (2017), 233-243.
 26. I.A. Purwasih, E.T. Baskoro, H. Assiyatun, **D. Suprijanto**, and M. Baca, “The locating-chromatic number for Halin graphs,” *Communications in Combinatorics and Optimization*, **2** (1) (2017), 1-9.
 27. **D. Suprijanto** and T. Nugraha, “A note on linear code from Johnson Graphs” *JP Journal of Algebra, Number Theory and Applications* **38** (5) (2016), 473-488.
 28. Irwansyah, A. Barra, S. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Sole, **D. Suprijanto**, and O. Yemen, “ θ_S – cyclic codes over A_k ”

International Journal of Computer Mathematics: Computer System Theory **1** (1) (2016), 14-31.

29. **D. Suprijanto** and Anthony, "New examples of MDS group codes" *Applied Mathematical Sciences*, **9** (99) (2015), 4897-4906.
30. Djoko Suprijanto, "Observation on sums of powers of integers divisible by five", *Applied Mathematical Sciences*, **9** (74) (2015), 3679-3686.
31. Djoko Suprijanto, "Observation on sums of powers of integers divisible by $4k-1$ ", *Applied Mathematical Sciences*, **9** (70) (2015), 3457-3465.
32. K. Wijaya, L. Yulianti, E.T. Baskoro, H. Assiyatun, and **D. Suprijanto**, "All Ramsey $(2K_2, C_4)$ -minimal graphs," *Journal of Algorithm and Computation* **46** (2015), 9-25.
33. K. Wijaya, E.T. Baskoro, H. Assiyatun, and **D. Suprijanto**, "The complete list if Ramsey $(2K_2, K_4)$ -minimal graphs", *Electronic Journal of Graph Theory and Applications* **3** (2) (2015), 216-227.
34. Adiwijaya, M. Salman A.N., O. Serra, **D. Suprijanto**, and E.T. Baskoro, "Some graphs in $C_f 2$ based on f -coloring," *International Journal of Pure and Applied Mathematics* **102** (2) (2015), 201-207.
35. M.S. Baladram and **D. Suprijanto**, "New spherical $(2t+1)$ -designs from Kuperberg's set: an experimental result ", *Applied Mathematics and Computation* **249** (2014), 45-52.
36. **D. Suprijanto** and P. Ariestyadi, "New self-dual codes over $GF(7)$ with the highest known minimum distance", *Applied Mathematical Sciences*, **8** (75) (2014), 3737-3745.
37. **D. Suprijanto** and Rusliansyah, "Observation on sums of powers of integers divisible by four", *Applied Mathematical Sciences*, **8** (45) (2014), 2219-2226.
38. **D. Suprijanto** and I W. Suwarno, "Observation on sums of powers of integers divisible by $3k-1$ ", *Applied Mathematical Sciences*, **8** (45) (2014), 2211-2217.
39. **D. Suprijanto**, Y. Renata, and M. L. Putri, "New Hermitian self-dual MDS or near- MDS codes over finite fields", *Journal of Mathematical and Fundamental Sciences*, **46** (1) (2014), 62-75.
40. **D. Suprijanto**, "A note on new (near-) MDS Euclidean self-dual codes", *Applied Mathematical Sciences*, **7** (57-60) (2013), 2917-2924.
41. S.W. Saputro, **D. Suprijanto**, E.T. Baskoro, and M. Salman, "The metric dimension of graph composition product with star" *Journal of Indonesian Mathematical Society* **18** (2) (2012), 85-92.

42. S. W. Saputro, E.T. Baskoro, M. Salman, **D. Suprijanto**, and M. Baca, "The metric dimension of regular bipartite graphs", *Bull. Math. Soc. Sci. Math. Roumanie*, Tome **54(102)** (1) (2011), 15-28.
43. M. Arzaki and **D. Suprijanto**, "Note on elementary constructions of self-dual codes over $\mathbb{Z}_8$ ", *International Mathematical Forum*, **6** (16) (2011), 785-794.
44. **D. Suprijanto**, "On Euclidean tight 6-designs: an experimental result", *ITB Journal of Science*, **43 A** (1) (2011), 19-42.
45. **D. Suprijanto** and B. Ilman, "New binary self-dual codes of length 36", *Jurnal Matematika dan Sains*, **15** (3), Desember 2010.
46. Adiwijaya, M. Salman, **D. Suprijanto**, and E.T. Baskoro, "A classification of graphs containing wheels based on f -coloring" **Contribution in Mathematics and Applications III**, *East-West J. Math.*, special volume (2010), 200-207.
47. S. W. Saputro, E.T. Baskoro, M. Salman, and **D. Suprijanto**, "The metric dimension of a complete n -partite graph and its cartesian product with a path", *J. Combin. Math. Combin. Comp.* **71** (2009), 283-293.
48. Adiwijaya, E.T. Baskoro, M. Salman, and **D. Suprijanto**, "On the f -coloring of the corona product of cycle graph with some other graphs", *J. Combin. Math. Combin. Comp.* **71** (2009), 235-241.
49. Ei. Bannai, Et. Bannai, and **D. Suprijanto**, "On the strong-nonrigidity of certain tight Euclidean designs", *European Journal of Combinatorics*, **28(6)** (2007), 1662-1680.

VII. PENGHARGAAN

- Dosen Terbaik Bidang Penelitian Kelompok Keilmuan Matematika Kombinatorika, FMIPA ITB, 2023
- Penghargaan 25 Tahun ITB, 2021
- Tanda Kehormatan Satyalancana Karya Satya XX Tahun, 2018
- Tanda Kehormatan Satyalancana Karya Satya X Tahun, 2009



📍 Gedung STP ITB, Lantai 1,
Jl. Ganesa No. 15F Bandung 40132
☎ +62 22 20469057
🌐 www.itbpress.id
✉ office@itbpress.id
Anggota Ikapi No. 043/JBA/92
APPTI No. 005.062.1.10.2018

Forum Guru Besar Institut Teknologi Bandung

Jalan Dipati Ukur No. 4, Bandung 40132
E-mail: sekretariat-fgb@itb.ac.id
Telp. (022) 2512532

🌐 fgb.itb.ac.id [FgbItb](#) [FGB_ITB](#)
📱 [@fgbitb_1920](#) [Forum Guru Besar ITB](#)

ISBN 978-623-297-608-5

