**ENCODING DAN DECODING KODE BCH**

**(BOSE CHAUDHURI HOCQUENGHEM) UNTUK TRANSMISI DATA MENGGUNAKAN ALGORITMA BERLEKAMP MASSEY DAN**

**CHIEN SEARCH**

**SKRIPSI**

Diajukan kepada Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Negeri Yogyakarta

untuk Memenuhi Sebagian Persyaratan guna Memperoleh Gelar

Sarjana Sains



Oleh

Luthfiana Arista

NIM. 11305141014

**PROGRAM STUDI MATEMATIKA**

**JURUSAN PENDIDIKAN MATEMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS NEGERI YOGYAKARTA**

**2016**

**ENCODING DAN DECODING KODE BCH**

**(BOSE CHAUDHURI HOCQUENGHEM) UNTUK TRANSMISI DATA MENGGUNAKAN ALGORITMA BERLEKAMP MASSEY DAN**

**CHIEN SEARCH**

**SKRIPSI**

Diajukan kepada Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Negeri Yogyakarta

untuk Memenuhi Sebagian Persyaratan guna Memperoleh Gelar

Sarjana Sains



Oleh

Luthfiana Arista

NIM. 11305141014

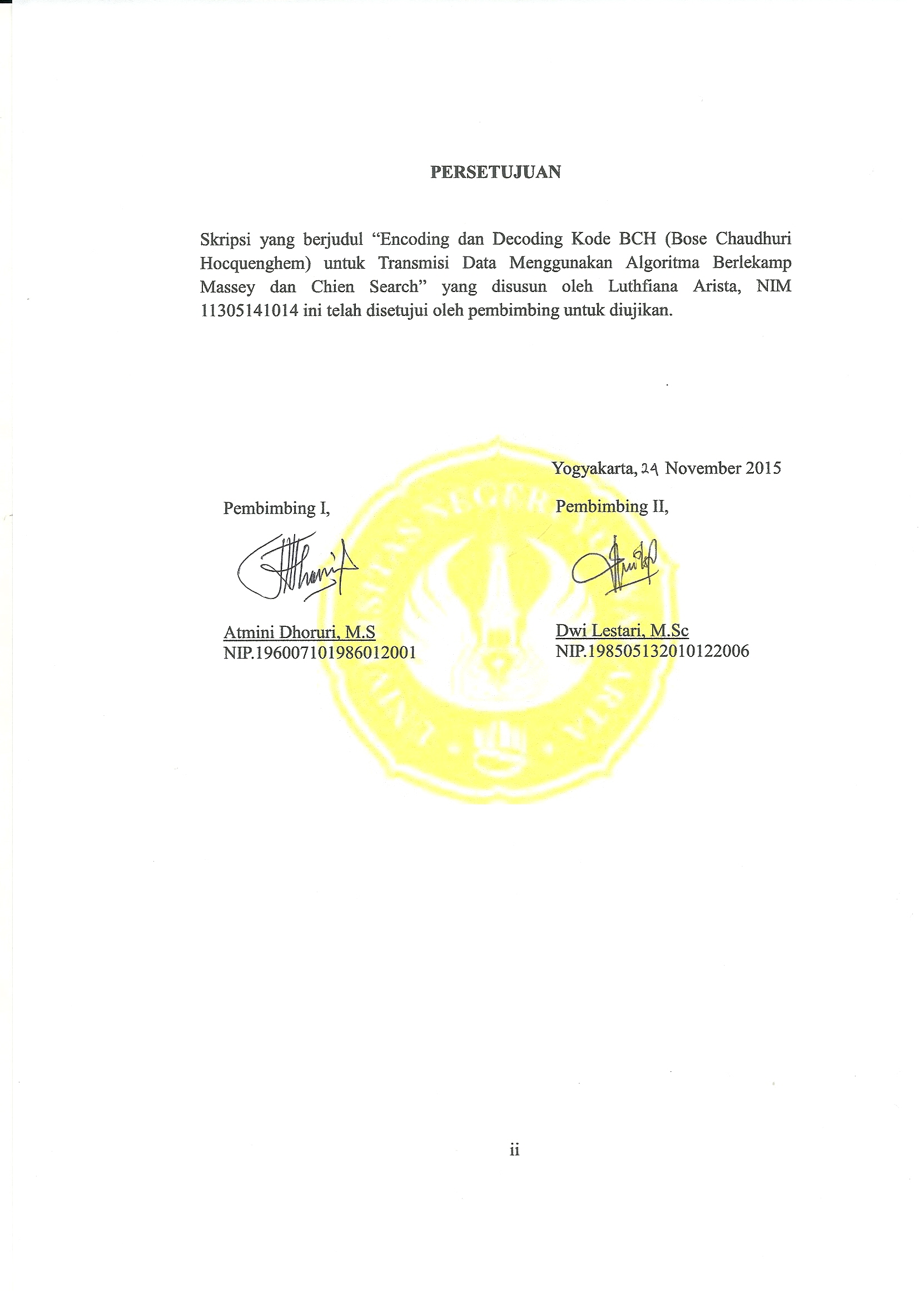
**PROGRAM STUDI MATEMATIKA**

**JURUSAN PENDIDIKAN MATEMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS NEGERI YOGYAKARTA**

**2016**



# G:\Scan_Pic0002.jpgG:\Scan_Pic0003.jpg

# MOTTO

*“Berbuat baiklah kapanpun kamu bisa,*

*berbuat baik bisa dilakukan kapanpun."*

*(Dalai Lama)*

*"Rahasia menjadi orang yang maju adalah*

*menjadi orang yang mulai melangkah."*

*(Mark Twain)*

# PERSEMBAHAN

Dengan memanjatkan puji syukur kehadirat Allah SWT, karya sederhana ini ku persembahkan kepada:

1. Bapak Aris Rubiyono dan Ibu Anifah Ilmayanti, yang selalu mendoakan dan memberikan motivasi*.*
2. Adik-adikku Dinda Sofiana Arista, Burhan Zaki Ilmawan, Arina Rifky Arista, Aisyah Nurilhusna Arista, dan Sarah Husnannajia Arista*.*
3. Guru, dosen, dan pendidik atas ilmu dan nasehat-nasehatnya.
4. Keluarga MATSUB’11, terima kasih telah menjadi kawan seperjuangan dalam menuntut ilmu selama masa kuliah, khususnya *playground’s playgroup kids* (Yuli, Nurma, A’yun, Casca, Atul, Muhsin, Humam, Noval, Sahid, Mahasin, dan Yoga) atas petualangannya.
5. Teman-teman satu hobi, mbak Ir, Nita, staf OSWI, staf SFI , staf WoofWoof, SWY, Sirius dan kru, dan teman-teman shawol yang tidak dapat disebut satu-persatu.

**ENCODING DAN DECODING KODE BCH**

**(BOSE CHAUDHURI HOCQUENGHEM) UNTUK TRANSMISI DATA MENGGUNAKAN ALGORITMA BERLEKAMP MASSEY DAN**

**CHIEN SEARCH**

Oleh

Luthfiana Arista

NIM. 11305141014

# ABSTRAK

Untuk menghasilkan suatu sistem transmisi data yang handal, diperlukan suatu kode yang dapat mengoreksi galat (*error*) yang terjadi. Salah satu kode pengoreksi galat yang populer adalah kode BCH (Bose Chaudhuri Hocquenghem). Salah satu karakter utama dari kode BCH adalah pendesain dapat mendesain kode dengan kapasitas koreksi yang diinginkan. Penulisan penelitian ini bertujuan untuk menjelaskan cara *encoding* (mengkodekan) kode BCH dan menjelaskan cara *decoding* (menguraikan/ membaca) kode BCH dengan algoritma Berlekamp Massey dan Chien Search.

Dalam penelitian ini, digunakan metode *encoding* sistematis, yaitu suatu metode *encoding* kode BCH dengan cara meletakkan bit pesan dan bit *check* bersebelahan. Selain itu, diterapkan algoritma Berlekamp Massey dan algoritma Chien Search untuk melakukan *decoding* pada kode BCH. Langkah pertama dalam melakukan *decoding* kode BCH adalah penghitungan syndrome. Langkah kedua adalah penggunaan Algoritma Berlekamp Massey. Langkah ketiga adalah penggunaan algoritma Chien Search.

Berdasarkan penggunaan algoritma Berlekamp Massey dan Chien Search, diperoleh hasil akhir yaitu posisi galat yang terjadi di dalam barisan yang diterima. Setelah posisi galat diketahui, kata (*word*)yang diterima dikoreksi menjadi pesan yang benar.

**Kata Kunci:** Algoritma Berlekamp Massey, algoritma Chien Search, *decoding*, *encoding*, kode BCH

# KATA PENGANTAR

*Assalamu’alaikum wr. wb*

*Alhamdulillahirobbil’alamin*, puji syukur penulis panjatkan kepada Allah SWT yang senantiasa memberikan nikmat dan rahmatNya sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul **“**Encoding dan Decoding Kode BCH (Bose Chaudhuri Hocquenghem) untuk Transmisi Data Menggunakan Algoritma Berlekamp Massey dan Chien Search**”**. Tugas akhir Skripsi ini dibuat sebagai salah satu syarat untuk menyelesaikan studi Sarjana Sains (S.Si).

Banyak pihak yang telah mendukung dan membantu penulis sejak awal kuliah hingga penulisan tugas akhir skripsi. Pada kesempatan ini, penulis mengucapkan terima kasih pada pihak-pihak yang telah membantu dan memberikan dukungan kepada penulis, yaitu:

1. Bapak Dr. Hartono selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Yogyakarta.
2. Bapak Dr. Sugiman selaku Ketua Jurusan Pendidikan Matematika FMIPA Universitas Negeri Yogyakarta yang telah memberikan kelancaran dalam urusan akademik.
3. Bapak Dr. Agus Maman Abadi selaku Ketua Program Studi Matematika FMIPA Universitas Negeri Yogyakarta.
4. Bapak Bambang Sumarno H.M., M.Kom selaku Dosen Pembimbing Akademik yang telah memberikan arahan, bimbingan, dan nasehat selama proses studi di UNY.
5. Ibu Atmini Dhoruri, M.S dan Ibu Dwi Lestari, M.Sc selaku Dosen Pembimbing Skripsi yang telah memberikan bimbingan, arahan, dan saran sehingga penulis dapat menyelesaikan penulisan Tugas Akhir Skripsi ini.
6. Bapak Ibu dosen Jurusan Pendidikan Matematika yang telah memberikan ilmu kepada penulis baik secara langsung maupun tidak langsung.
7. Bapak Aris Rubiyono, Ibu Anifah Ilmayanti, dan keluarga yang tidak pernah lelah memberikan dukungan, semangat, dan doa untuk penulis.
8. Sahabat-sahabat dan semua pihak yang telah memberikan motivasi dan membantu secara langsung maupun tidak langsung sehingga dapat memperlancar proses penyusunan tugas akhir ini.

Penulis menyadari bahwa dengan keterbatasan yang dimiliki, penulisan skripsi ini masih jauh dari sempurna. Oleh sebab itu, penulis sangat mengharap kritik dan masukan yang membangun sehingga dapat membuat skripsi ini menjadi lebih baik.

Semoga tugas akhir ini dapat bermanfaat bagi pembaca dan pihak lain yang terkait. Aamiin.

*Wassalamu’alaikum wr. wb.*

Yogyakarta, November 2015

Luthfiana Arista

NIM. 11305141014

# DAFTAR ISI

HALAMAN JUDUL ………………………………………………………. i

[PERSETUJUAN **Error! Bookmark not defined.**](#_Toc440787017)

[PENGESAHAN ii](#_Toc440787018)

[HALAMAN PERNYATAAN **Error! Bookmark not defined.**](#_Toc440787019)

[MOTTO v](#_Toc440787020)

[PERSEMBAHAN vi](#_Toc440787021)

[ABSTRAK vii](#_Toc440787022)

[KATA PENGANTAR viii](#_Toc440787023)

[DAFTAR ISI x](#_Toc440787024)

[DAFTAR TABEL xii](#_Toc440787025)

[DAFTAR GAMBAR xiii](#_Toc440787026)

[DAFTAR SIMBOL xiv](#_Toc440787027)

[BAB I PENDAHULUAN 1](#_Toc440787028)

[A. Latar Belakang 1](#_Toc440787029)

[B. Rumusan Masalah 5](#_Toc440787030)

[C. Tujuan Penelitian 5](#_Toc440787031)

[D. Manfaat Penelitian 5](#_Toc440787032)

[BAB II KAJIAN TEORI 7](#_Toc440787033)

[A. Grup 7](#_Toc440787034)

[B. Ring 8](#_Toc440787035)

[C. Lapangan 9](#_Toc440787036)

[D. Lapangan Hingga 10](#_Toc440787037)

[E. Lapangan Galois 11](#_Toc440787038)

[F. Kata Kode (*Codeword*) 12](#_Toc440787039)

[G. Jarak Hamming 12](#_Toc440787040)

[H. Bobot Hamming 14](#_Toc440787041)

[I. Kode Linear 14](#_Toc440787042)

[J. Matriks Generator 15](#_Toc440787043)

[K. Matriks *Parity Check* 18](#_Toc440787044)

[L. Syndrome 19](#_Toc440787045)

[M. Ring Polinomial 21](#_Toc440787046)

[N. Polinomial Minimal 22](#_Toc440787047)

[O. Matriks Vandermonde 24](#_Toc440787048)

[BAB III PEMBAHASAN 26](#_Toc440787049)

[A. Kode Pengoreksi Galat 26](#_Toc440787050)

[B. Kode BCH 27](#_Toc440787051)

[C. Parameter Kode BCH 33](#_Toc440787052)

[D. Batas Kode BCH 36](#_Toc440787053)

[E. *Encoding* Kode BCH 39](#_Toc440787054)

[F. *Decoding* Kode BCH 44](#_Toc440787055)

[a. Prosedur Pendeteksian Galat 44](#_Toc440787056)

[b. *Syndrome* dari Kata yang Diterima 45](#_Toc440787057)

[c. Algoritma Berlekamp Massey 48](#_Toc440787058)

[d. Algoritma Chien Search 58](#_Toc440787059)

[G. Implementasi *Encoder* dan *Decoder* Kode BCH 60](#_Toc440787060)

[a. Implementasi *Encoder* untuk kode BCH (31, 11) pada FPGA 60](#_Toc440787061)

[b. Implementasi *Decoder* BCH (63, 51) untuk WBAN 63](#_Toc440787062)

[BAB IV PENUTUP 66](#_Toc440787063)

[A. Kesimpulan 66](#_Toc440787064)

[B. Saran 67](#_Toc440787065)

[DAFTAR PUSTAKA 68](#_Toc440787066)

LAMPIRAN………………………………………………………………. 70

# DAFTAR TABEL

Tabel 2.1 *Standard Array* kode- …………………………………..….. 20

Tabel 2.2 *Coset leader* dan *Syndrome* kode- ……………………….… 21

Tabel 2.3 Elemen-Elemen ………………………………………….. 25

Tabel 3.1 Representasi dari ………....…………………………….… 40

Tabel 3.2 Lapangan dengan Elemen yang dibangun oleh polinomial

………………………………………………………. 41

Tabel 3.3 Tabel iterasi pencarian ……………………………………… 54

Tabel 3.4 Iterasi pencarian dengan algoritma yang disederhanakan ….. 55

Tabel 3.5 Hasil pencarian ……………………………………………… 58

# DAFTAR GAMBAR

Gambar 3.1 *Encoding* dengan suatu (n-k) *stage shift register* ………..………. 62

Gambar 3.2 Sirkuit logika *encoding* kode BCH (31, 11) yang diimplementasikan pada FPGA ……………………………………………..……….. 62

Gambar 3.3 Diagram Blok *Decoder* BCH (63, 51, 2) …………………..…….. 64

Gambar 3.4 Implementasi Penghitungan *Syndrome* dan Pencarian Koefisien .. 64

Gambar 3.5 Implementasi Blok Chien Search ………………………………... 65

# DAFTAR SIMBOL

|  |  |
| --- | --- |
|  | Panjang blok. |
|  | Banyaknya digit *parity check.* |
|  | Jarak minimum |
|  | *Galois Field* dengan banyak elemen . |
|  | Polinomial minimal dari . |
|  | Koset siklotomik darimodulo yang memuat. |
|  | Bobot hamming dari . |
|  | Akhir pembuktian. |

# BAB I

**PENDAHULUAN**

## Latar Belakang

Meningkatnya penggunaan komunikasi digital dan munculnya komputer digital sebagai alat yang penting dalam teknologi saat ini menuntut adanya sistem komunikasi yang dapat diandalkan. Tuntutan tersebut semakin meningkat seiring munculnya jaringan data berskala besar dan berkecepatan tinggi yang digunakan untuk bertukar, memproses, dan menyimpan informasi digital di lingkungan militer, kepemerintahan, dan juga swasta. Diperlukan adanya teknologi komputer dan komunikasi dalam merancang sistem yang handal tersebut. Salah satu masalah terbesar yang dihadapi rancangan-rancangan tersebut adalah kendali terhadap galat (*error*) yang terjadi sehingga pengolahan data yang tangguh dapat tercapai.

Dalam makalah ‘*A Mathematical Theory of Communication*’ yang diterbitkan pada tahun 1948, Claude Shanon menunjukkan bahwa sistem komunikasi yang dapat diandalkan dapat dicapai jika dilakukan proses *encoding* (mengkodekan pesan) dan *decoding* (menguraikan/membaca pesan) yang tepat. Makalah tersebut menandai munculnya teori pengkodean, suatu bidang studi yang membahas hal-hal terkait pengiriman data melalui *channel* komunikasi dan perbaikan galat yang terjadi selama pengiriman. Perkembangan di bidang pengkodean baru-baru ini terpusat pada pencapaian sistem digital berkecepatan tinggi, dan penggunaan pengkodean untuk komputer digital dan sistem komunikasi.

Saat data dikirimkan, terkadang gangguan yang terjadi di dalam *channel* menyebabkan terjadinya galat di dalam pesan yang dikirimkan. Walaupun tidak ada yang dapat dilakukan untuk mencegah *channel* menyebabkan galat tersebut, dapat dilakukan perbaikan terhadap galat yang terjadi menggunakan pengkodean. Banyak komputer kini menanamkan kemampuan pengoreksian galat ke dalam RAM (*Random Access Memory*) karena memperbaiki galat yang terjadi selama pengiriman pesan lebih murah daripada membangun sirkuit terintegrasi yang 100% dapat diandalkan. Ide dasarnya adalah mengambil himpunan bit yang akan dikirimkan, tambahkan bit *check*, dan kirimkan seluruh bit. Diasumsikan bahwa jika gangguan di dalam *channel* mengubah beberapa bit dari bit yang dikirimkan, bit *check* akan mampu memberikan cukup informasi untuk memungkinkan dilakukannya pendeteksian dan pengoreksian kesalahan yang terjadi.

Salah satu kode pengoreksi galat yang popular adalah kode BCH (Bose Chaudhuri Hocquenghem). Kode BCH ditemukan oleh R. C. Bose dan D. V. Ray-Chaudhuri pada tahun 1960 dan secara terpisah pada tahun 1959 oleh A. Hocquenghem. Kode BCH adalah generalisasi kode Hamming (salah satu bentuk kode linear yang ditemukan oleh R. W. Hamming dan M. J. E. Golay) untuk *multiple error correction*. Fitur pembeda yang paling utama dari kode BCH adalah kemungkinan untuk memilih banyaknya galat yang akan dikoreksi.

Di dalam proses transmisi data terdapat dua proses utama, yaitu *encoding* (mengkodekan pesan) dan *decoding* (menguraikan/membaca pesan). Salah satu cara *encoding* kode BCH adalah dengan melakukan *encoding* sistematis dengan meletakkan bit pesan dan bit *check* bersebelahan. Salah satu cara *decoding* kode BCH adalah dengan menggunakan algoritma Berlekamp Massey dan Chien Search. Elwyn Berlekamp menemukan cara *decoding* kode BCH pada tahun 1968 dan James Massey mengembangkan algoritma tersebut pada tahun 1969.

Dalam suatu *channel* komunikasi dengan pengkodean, hanya kata kode (*codeword*) yang ditransimisikan. Misalkan ada suatu kata kode *w* yang diterima. Jika *w* suatu kata kode yang valid, dapat disimpulkan bahwa tidak ada galat yang terjadi selama transmisi. Jika bukan, diketahui bahwa ada beberapa galat yang terjadi. Dalam hal ini, dibutuhkan suatu aturan untuk menemukan kata kode yang paling mungkin dikirimkan berdasarkan galat yang diterima.

Beberapa penelitian mengenai karakter dan *decoding* kode BCH telah dilakukan:

1. *An Enhanced (31,11,5) Binary BCH Encoder and Decoder for Data Transmission* oleh P.Mozhiarasi, C.Gayathri, dan V.Deepan. Tulisan ini mendeskripsikan desain *encoder* dan *decoder* BCH (31,11,5) dengan 31, 11 dan 5 yang secara berturut-turut merepresentasikan panjang blok (*n*), panjang data (*k*) dan banyaknya galat maksimal yang dapat diperbaiki.
2. Analisis Kinerja Kode BCH oleh Edy Susanto. Dalam tulisan ini penulis menggunakan algoritma Berlekamp sebagai algoritma pendekodean BCH. Tulisan ini membahas bagaimana pengaruh implementasi kode pengoreksi galat terhadap kinerja sistem komunikasi secara keseluruhan.
3. *Step-by-step Decoding of the Bose-Chaudhuri-Hocquenghem Codes* oleh James L. Massey. Tulisan ini memberikan konsep serta *step by step* *decoding* kode BCH dengan menggunakan batas BCH yang telah diketahui.
4. *Some codes related to BCH-codes of low dimension* oleh Yves Edela, Jurgen Bierbrauer. Tulisan ini mengkonstruksikan banyak kode biner, terner dan kuaterner dengan metode yang melibatkan penelitian tentang kode BCH atas lapangan, rangkaian dan konstruksi X yang lebih besar dan ragam konstruksi Griesmer (kode residual).
5. *Hardware Implementation of (63, 51) BCH Encoder and Decoder for WBAN using LFSR and BMA* oleh Priya Mathew dkk. Di dalam tulisan ini diberikan contoh implementasi kode BCH (63, 51) pada WBAN (Wireless Body Area Network). Kode tersebut diimplementasikan pada *device* FPGA (*Field Programmable Gate Array*) Virtex 4.
6. *Implementation of Encoder for (31, k) Binary BCH Code based on FPGA for Multiple Error Correction Control* oleh Samir Jasim Mohammed. Tulisan ini menjelaskan desain dan implementasi *encoder* kode BCH (31, k) menggunakan chip FPGA yang dapat dikonfigurasi.

Berdasarkan penelitian-penelitian sebelumnya, terutama *An Enhanced (31,11,5) Binary BCH Encoder and Decoder for Data Transmission* oleh P.Mozhiarasi, C.Gayathri, dan V.Deepan (2015), tugas akhir ini merupakan studi dari jurnal tersebut dengan judul “Encoding dan Decoding kode BCH (Bose Chaudhuri Hocquenghem) untuk Transmisi Data menggunakan Algoritma Berlekamp Massey dan Chien Search”. Selanjutnya diberikan contoh implementasi *encoder* dan *decoder* kode BCH pada WBAN (*Wireless Body Are Network*)dan FPGA (*Field Programmable Gate Arrays*). Dengan penelitian ini, diharapkan dapat menambah pemahaman mengenai cara melakukan *encoding* dan *decoding* kode BCH.

## Rumusan Masalah

Berdasarkan latar belakang di atas, dapat ditemukan beberapa permasalahan yang dirumuskan sebagai berikut:

1. Bagaimana cara melakukan *encoding* (mengkodekan) kode BCH?
2. Bagaimana cara melakukan *decoding* (menguraikan/membaca) kode BCH dengan algoritma Berlekamp Massey dan Chien Search?
3. Bagaimana contoh implementasi *encoding* dan *decoding* kode BCH?

## Tujuan Penelitian

Tujuan penulisan penelitian ini adalah:

1. Menjelaskan cara *encoding* (mengkodekan) kode BCH, dan
2. Menjelaskan cara *decoding* (menguraikan/membaca) kode BCH dengan algoritma Berlekamp Massey dan Chien Search.
3. Menjelaskan contoh implementasi *encoding* dan *decoding* kode BCH.

## Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah:

1. Bagi penulis

Bagi penulis, penulisan skripsi ini dapat menambah pengetahuan dan wawasan tentang kode pengoreksi galat (*error correcting code*) pada umumnya, dan kode BCH pada khususnya.

1. Bagi para pembaca

Sebagai salah satu bahan dalam mempelajari kode BCH dan diharapkan penelitian ini dapat dijadikan sebagai referensi untuk penelitian selanjutnya.

1. Bagi perpustakaan Universitas Negeri Yogyakarta

Penulisan skripsi ini juga menambah koleksi bahan pustaka bagi Universitas Negeri Yogyakarta pada umumnya, dan mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam pada khususnya.

# BAB II

**KAJIAN TEORI**

Pada Bab II ini berisi kajian teori. Di bab ini akan dijelaskan beberapa definisi mengenai grup, ring, dan lapangan serta teori-teori pengkodean yang mendasari teori kode BCH.

## Grup

**Definisi** **2.1** **(Fraleigh, 2003 : 20).** *Operasi biner pada himpunan S adalah suatu pemetaan fungsi ke . Untuk setiap , elemen dari S dilambangkan dengan .*

**Definisi** **2.2** **(Fraleigh, 2003 : 37).** *Grup adalah suatu himpunan G yang tertutup dengan operasi biner , sedemikian sehingga aksioma-aksioma berikut dipenuhi:*

1. *Untuk setiap , berlaku atau sifat asosiatif dari .*
2. *Ada suatu elemen di sedemikian sehingga untuk setiap , , adalah elemen identitas untuk .*
3. *Untuk setiap , ada suatu elemen di sedemikian sehingga , adalah invers dari .*

**Definisi** **2.3** **(Fraleigh, 2003 : 39).** *Grup disebut grup abelian jika operasi binernya bersifat komutatif.*

Berikut akan diberikan contoh grup abelian.

**Contoh 2.1.** Himpunan adalah suatu grup abelian. Himpunan adalah himpunan semua kelas bilangan bulat modulo dengan penjumlahan modulo .

Bukti:

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Memperhatikan tabel Cayley untuk penjumlahan modulo terlihat bahwa sifat tertutupnya terpenuhi, elemen identitasnya adalah , invers terhadap penjumlahan modulo 2 yaitu .

Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo bersifat komutatif.

## Ring

Ring adalah suatu struktur aljabar dengan dua operasi biner.

**Definisi** **2.4** **(Fraleigh, 2003 : 167).** *Ring adalah suatu himpunan dengan dua operasi biner dan , yang kemudian disebut operasi penjumlahan dan perkalian. Kedua operasi tersebut didefinisikan pada sedemikian sehingga aksioma-aksioma berikut dipenuhi:*

1. *adalah grup abelian.*
2. *Operasi perkaliannya bersifat asosiatif.*
3. *Untuk setiap , berlaku sifat distributif kiri, dan sifat distributif kanan .*

Berikut diberikan contoh dari ring.

**Contoh 2.2.** Himpunan adalah suatu ring. Himpunan adalah himpunan semua kelas bilangan bulat modulo dengan penjumlahan modulo dan perkalian modulo adalah suatu ring.

Bukti:

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Memperhatikan tabel Cayley untuk penjumlahan modulo terlihat bahwa sifat tertutupnya terpenuhi, elemen nolnya adalah , invers terhadap penjumlahan modulo 2 yaitu . Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo bersifat komutatif. Himpunan terhadap perkalian modulo bersifat tertutup.

## Lapangan

**Definisi 2.5 (Gallian, 2006 : 250).** *Lapangan adalah suatu ring komutatif dengan elemen kesatuan yang setiap elemen yang bukan nol adalah suatu unit (mempunyai invers terhadap perkalian).*

Berikut adalah contoh dari lapangan.

**Contoh 2.3.** Himpunan adalah himpunan semua kelas bilangan bulat modulo dengan penjumlahan modulo dan perkalian modulo adalah suatu lapangan.

Bukti:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | [2] | [3] | [4] |
| [0] |  | [1] | [2] | [3] | [4] |
| [1] | [1] | [2] | [3] | [4] | [0] |
| [2] | [2] | [3] | [4] | [0] | [1] |
| [3] | [3] | [4] | [0] | [1] | [2] |
| [4] | [4] | [0] | [1] | [2] | [3] |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | [2] | [3] | [4] |
| [0] |  |  |  |  |  |
| [1] |  |  |  |  |  |
| [2] |  |  | [4] |  |  |
| [3] |  |  |  |  |  |
| [4] |  |  |  |  |  |

Memperhatikan tabel Cayley untuk penjumlahan modulo terlihat bahwa sifat tertutupnya terpenuhi, elemen nolnya adalah , invers terhadap penjumlahan modulo 5, yaitu . Tabel simetris terhadap diagonal utama, sehingga penjumlahan modulo maupun perkalian modulo bersifat komutatif. Himpunan terhadap perkalian modulo bersifat tertutup, elemen kesatuannya adalah dan invers dari setiap elemenennya terhadap perkalian modulo , yaitu .

## Lapangan Hingga

Definisi 2.6 (Lange, 2011). *Suatu lapangan yang memuat elemen sebanyak berhingga disebut lapangan berhingga. Lapangan hingga yang memuat sebanyak elemen dilambangkan dengan .*

Berikut akan diberikan contoh lapangan hingga.

**Contoh 2.4.** Himpunan adalah suatu lapangan hingga karenaadalah suatu lapangan dengan banyak elemen yang berhingga.

## Lapangan Galois

Definisi 2.7 (Vanstone dan Oorschot, 1989 : 28). *Jika suatu lapangan hingga dengan elemen, dan dengan bilangan prima dan bilangan asli, maka dilambangkan dengan .*

Untuk mengkonstruksi suatu lapangan hingga yang memuatelemen digunakan suatu polinomial tak tereduksi dengan derajatdalam. Untuk kasus, akan dibuktikan bahwa selalu ada suatu polinomial kuadrat tidak tereduksi dalam. Adapolinomial monik (polinomial dengan derajatdengan koefisien dariadalah) berderajat dua dalam. Jika satu daripolinomial tersebut yang dapat direduksi, maka polinomial tersebut adalah suatu hasil perkalian dari polinomial monik berderajat. Ada tepatpolinomial monik berderajat. Menggunakan polinomial-polinomial monik berderajat tersebut didapatkan polinomial kuadrat monik yang dapat direduksi, dengan adalah kombinasi dari . Sehingga banyaknya polinomial kuadrat monik yang tidak tereduksi adalah

yang membuktikan keberadaan polinomial kuadrat tidak tereduksi.

**Contoh 2.5.** Untukdan, ada dua polinomial monik pangkat tiga yang tidak tereduksi atas yaitudan. Misal ambil sehingga elemen-elemen adalah , , , , , , , . Jika dilambangkan dengan maka elemen-elemen dari adalah

## Kata Kode (*Codeword*)

Definisi 2.**8 (Ling S. & Xing C., 2004 : 5).** *Misal adalah himpunan berukuran q, yang kemudian disebut alfabet kode dan elemen-elemennya disebut simbol kode.*

1. *Kata (word) q-er dengan panjang atas adalah suatu barisan dengan untuk setiap .*
2. *Kode blok q-er dengan panjang atas adalah suatu himpunan tidak kosong yang berisi kata dengan panjang n.*
3. *Suatu elemen disebut kata kode dalam .*

Biasanya alfabet kode yang digunakan diambil dari lapangan hingga dengan order . Kode atas alfabet kode disebut kode biner.

## Jarak Hamming

Definisi 2.9 **(Ling S. & Xing C., 2004 : 9).** *Misaldanadalah kata kode dengan panjangatas. Jarak Hamming darike, dinotasikan denganadalah banyaknya posisi yang berbeda antara dan. Jikadan , maka*

*dengandandianggap sebagai kata dengan panjang , dan*

Berikut adalah contoh penghitungan jarak Hamming dari dua kata kode.

**Contoh 2.6.** Jika dan,,maka

Definisi 2.10 **(Vanstone dan Oorschot, 1989 : 7).** *Jikasuatu kode- (kode dengan panjangmemuat kata kode) maka jarak Hammingdari kodeadalah*

Dengan kata lain, jarak Hamming dari suatu kode adalah jarak minimum antara dua kata kode yang berbeda, atas semua pasang kata kode.

Contoh 2.7. Misalkan dengan

diperoleh

Jadi mempunyai jarak.

## Bobot Hamming

**Definisi 2.11** **(Ling S. & Xing C., 2004 : 46).** *Misalsuatu kata kode dalam. Bobot Hamming dari, disimbolkan, didefinisikan sebagai banyaknya koordinat tak nol di. Untuk setiap elemendaribobot Hamming didefinisikan sebagai berikut:*

Jika dengan maka bobot Hamming darijuga secara ekuivalen didefinisikan sebagai

**Definisi 2.12** **(Ling S. & Xing C., 2004 : 48).** *Jikasuatu kode maka bobot (Hamming) minimum dari, dilambangkan denganadalah bobot terkecil dari kata kode tak nol dari*.

Berikut diberikan contoh penghitungan bobot Hamming dari suatu kode.

**Contoh 2.8.** Misal ada suatu kode biner linear.

Sehingga.

## Kode Linear

Definisi 2.13 (Ling S. & Xing C., 2004 : 45). *Suatu kode linear dengan panjang atas adalah suatu subruang vektor dari ruang vektor dengan adalah himpunan semua vektor dengan panjang yang entri-entrinya adalah elemen*

Definisi 2.14 (Ling S. & Xing C., 2004 : 46). *Kode adalah kode linear dengan panjang berdimensi atas .*

**Contoh 2.9.** Berikut ini adalah kode linear:

. Kode ini disebut *repetition code*.

dengan

dengan .

dengan .

## Matriks Generator

Matriks yang digunakan untuk membentuk suatu kode linear adalah matriks generator.

**Definisi 2.15** **(Vanstone dan Oorschot, 1989 : 51).** *Suatu Matriks Generatoruntuk kodeadalah matriksyang barisnya merupakan basis ruang vektor dari*.

Kata kode dari suatu kode linear(atas lapangan) dengan matriks generatoradalah semua kombinasi linear (atas) dari baris-baris. Kemudiandisebut kode yang dibangun oleh matriks.

Operasi baris elementer yang dilakukan padaakan memberikan matriks-matriks yang juga membangun. Misalnya, jika dapat ditemukan suatu matriks generator yang berbentuk dengan adalah matriks identitasdanadalah suatu matriks, maka simbol informasi berada di posisipertama dari suatu kata kode. Matriksdengan bentuk tersebut disebut matriks generator dengan bentuk standar. Tidak dapat dijamin bahwa akan selalu adauntuk. Meski demikian, menukar posisi koordinat dari suatu kodemenghasilkan ruang bagianyang memiliki bobot dan jarak Hamming yang sama dengan. Sehinggadanadalah kode yang sama, yang kemudian mendorong adanya definisi berikut, dengan *matriks permutasi* adalah suatu matriks identitas dengan baris atau kolom yang ditukar.

**Definisi 2.16 (Vanstone dan Oorschot, 1989:52).** *Dua kode-danatas lapangandikatakan kode ekuivalen jika ada matriks generatordanuntukdandan suatu matriks permutasidengan ukuransedemikian sehingga*

Matriksmenukar kolom, sehingga menukar posisi koordinat diyang menghasilkan kode.

**Contoh 2.10.** Misaladalah suatu kode- yang dibangun oleh matriks generator

adalah kode-dengan matriks generator

Dapat ditunjukkan bahwadanadalah kode ekuivalen sebagai berikut. Dengan operasi baris pada

didapatkan matriks generator lain untukyaitu

Dipilih matriks permutasi yang akan menghasilkan

didapatkan

Perkalian antara matriks G dan matriks menukar kolomdandari, sehingga menukar koordinatdandari setiap kata kode dari. Kedua kode tersebut ekuivalen, tetapi tidak identik.

**Definisi 2.17 (Vanstone dan Oorschot, 1989 : 54).** *Jikaadalah suatu kode-atas lapanganmaka komplemen ortogonaluntuk semua*.

Himpunan adalah himpunan -tupel atas yang ortogonal terhadap setiap vektor di. Kode selanjutnya disebut sebagai kode dual dari.

**Definisi 2.18 (Vanstone dan Oorschot, 1989 : 55).** *Jikaadalah matriks generator untuk, maka adalah matriks generator untuk.*

**Contoh 2.11.** Kode adalah kode-atas yang dibangun oleh

Dengan melakukan operasi baris elementer yang sesuai terhadap , didapatkan matriksyang membangun kode yang sama, dengan

Matriks generator yang membangun komplemen ortogonal dariadalah

## Matriks *Parity Check*

**Definisi 2.19 (Ling S. & Xing C., 2004 : 52**). *Matriks Parity Checkuntuk suatu kode linearadalah matriks generator untuk kode*

Jikaadalah matriks generator untukdanadalah matriks generator untuk, makaadalah matriks *parity check* untukdanadalah matriks *parity check* untuk.

**Contoh 2.12.** Jikaadalah matriks *parity check* untuk kode-atasmaka matriks generator untukadalah

## Syndrome

**Definisi 2.20** **(Ling S. & Xing C., 2004 : 59).** *Jikaadalah suatu kode linear dengan panjangatasdan adalah sebarang vektor dengan panjang, maka koset dariyang ditentukan olehadalah himpunan*

Grup dengan operasi penjumlahan vektor adalah suatu grup abelian berhingga dan kode linear atas dengan panjang adalah suatu subgrup dari sehingga .

**Definisi 2.21 (Ling S. & Xing C., 2004 : 60).** *Suatu kata atau kata kode dengan bobot (Hamming) terkecil dalam suatu koset disebut coset leader*.

**Definisi 2.22 (Ling S. & Xing C., 2004 : 62).** *Misaladalah suatu kode linear-atas danadalah matriks parity check untuk, untuk setiap . Syndrome dari kodeadalah .*

**Contoh 2.13.** Suatu kode-dengan matriks generator dan matriks *parity check*

**Tabel 2.1** *Standard Array* kode-

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Coset Leader* |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Semua vektor yang berbobot 1 merupakan coset leader, sehingga leader yang terletak di baris terakhir tidak langsung terlihat dengan jelas. Leader ini dapat diperoleh setelah menghitung semua vektor berbobot 2 dari ketujuh leader yang telah didapatkan.

Untuk menghitung syndrome, digunakan sehingga:

**Tabel 2.2** *Coset leader* dan *Syndrome* kode-

|  |  |
| --- | --- |
| *Coset Leader* | *Syndrome* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Ring Polinomial

**Definisi 2.23** **(Ling S. & Xing C., 2004 : 22).** *Misaladalah suatu lapangan. Himpunan*

*disebut ring polinomial atas. Suatu elemen daridisebut suatu polinomial atas. Dalam polinomial , bilangan bulatdisebut derajat dari, dilambangkan dengan, jika*.

Polinomial tak nol berderajatdisebut polinomial monik jika. Polinomialyang berderajat positif disebut *reducible* (atas) jika ada dua polinomialdanatassedemikian sehingga,dan. Jika syarat-syarat tersebut tidak dipenuhi, polinomialberderajat positif tersebut disebut *irreducible* atas.

**Contoh 2.14**

1. Polinomial adalah suatu polinomial berderajatyang dapat direduksi karena .
2. Polinomial adalah polinomial berderajatyang tidak tereduksi karena jikatereduksi makaakan memiliki faktor linearatau, yaituatauakan menjadi akar dari, akan tetapi .
3. Dengan argumen yang sama dengan poin ii, dan keduanya tidak tereduksi ataskarena keduanya tidak memiliki faktor linear.

## Polinomial Minimal

**Definisi 2.24 (Togneri dan deSilva, 2006 : 339)**

1. *Misaldanadalah dua lapangan. Lapanganadalah suatu extension field darijika ada suatu isomorfisme ring darike himpunan bagian.*
2. *Polinomial dengan derajatdan koefisien dariadalahdisebut polinomial monik.*
3. *Jikasuatu lapangan danadalah elemen dariatau extension field dari,adalah suatu polinomial monik tidak tereduksi dengan dan tidak ada polinomial lain dengan derajat yang lebih kecil dariyang memenuhi , makaadalah polinomial minimum dariatas.*
4. *Jikaadalah polinomial minimum dariatas, makaadalah faktor dari polinomial lainyang memenuhi .*
5. *Misal saling prima dengan , yaitu . Koset siklotomik dari (atau -koset siklotomik) modulo memuat didefinisikan oleh*

Himpunan bagian dari disebut himpunan lengkap dari representatif koset siklotomik dari modulo jika berbeda dan

**Teorema 2.1.** *Jikaadalah elemen primitif (generator grup perkalian) dari maka polinomial minimal dari terhadap adalah*

*dengan adalah koset siklotomik unik darimoduloyang memuat*

**Bukti**

Langkah 1: adalah akar darikarena .

Langkah 2: Misal dengan dan . Dengan memangkatkan setiap koefisien dengandidapatkan

Di dalam rumus di atas sehingga untuk semua . Artinya,adalah suatu polinomial atas.

Langkah 3: Elemenadalah suatu elemen primitif, sehingga untuk dua elemen yang berbedadandari. Sehinggatidak memiliki akar berganda. Kemudian jika dan . Berlaku untuk maka untuk sebarang ada suatu bilangan bulat sedemikian sehingga Sehingga

Langkah yang ketiga mengimplikasikan bahwaadalah pembagi dari.

Ketiga langkah tadi menunjukkan bahwaadalah polinomial minimal dari.

## Matriks Vandermonde

**Definisi 2.25 (Pretzel, 1992 : 203).** *Suatu matriks Vandermonde berukuran didefinisikan sebagai berikut:*

*Baris pertama dari dapat dipilih secara sebarang:*

*Kemudian keseluruhan matriks adalah*

**Contoh 2.15.** Kode BCHdengan polynomial generator yang dibentuk dari polynomial primitif atas memiliki matriks *parity check*. Kolom-kolom matriks tersebut merepresentasikan elemen-elemen tak nol dari .

**Tabel 2.3** Elemen-Elemen

|  |  |
| --- | --- |
| Bentuk Pangkat | Bentuk Polinomial |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Dengan memilih elemen primitif diperoleh kolom-kolomnya adalah

jikaberjalan darisampaimaka matriks lengkapnya adalah

.

# 

# BAB III

**PEMBAHASAN**

Pada Bab III ini berisi pembahasan tentang konsep kode pengoreksi galat (*error correcting code*), proses *encoding* menggunakan sistem *encoding* sistematis, serta proses *decoding* menggunakan algoritma Berlekamp Massey dan Chien Search.

## Kode Pengoreksi Galat

Teori kode pendeteksi dan pengoreksi galat adalah cabang ilmu matematika dan teknik yang berhubungan dengan transmisi dan penyimpanan data. Media informasi tidak 100% dapat diandalkan, artinya gangguan-gangguan (*noise*) sering menyebabkan data menjadi berubah atau rusak. Untuk menangani masalah tersebut, ditambahkan redundansi ke data asli. Dengan redundansi tersebut, galat (*error*) yang terjadi sampai batas toleransi tertentu dapat diperbaiki, atau minimal adanya galat dapat dideteksi. Berikut diberikan contoh untuk menggambarkan konsep tersebut (Vanstone dan Oorschot, 1989 : 1).

**Contoh 3.1.** Misal informasi yang dikirimkan berbentuk himpunan {apel, anggur, nanas, nangka}. Masing-masing elemen himpunan tersebut dipasangkan dengan suatu barisan angka 0 dan 1 sebagai berikut:

A 🡪 00

B 🡪 10

C 🡪 01

D 🡪 11.

Sehingga jika dikirimkan barisan 00, maka penerima akan mengartikan barisan tersebut sebagai apel. Jika pengirim mengirimkan 00 dan penerima menerima 01, maka terjadi satu galat. Penerima tidak mengetahui adanya galat tersebut karena 01 adalah potongan informasi valid yang berarti nanas.

Peningkatan kehandalan transmisi data dilakukan dengan menambahkan redundansi ke setiap pesan. Misal dibuat pasangan baru sebagai berikut:

A 🡪 00 🡪 00000

B 🡪 10 🡪 10110

C 🡪 01 🡪 01011

D 🡪 11 🡪 11101.

Jika penerima menerima 01000, maka akan diketahui bahwa ada galat di dalam pesan yang diterima tersebut karena 01000 tidak ada dalam daftar kode yang dikirimkan.

## Kode BCH

Kode BCH adalah suatu kelas kode yang ditemukan pada tahun 1960 oleh R. C. Bose dan D. Ray Chaudhuri dan juga ditemukan secara independen oleh A. Hocquenghem secara terpisah pada tahun 1959. Nama BCH diambil dari penemu-penemu tersebut (Bose Chaudhuri Hocquenghem). Kode BCH mengoreksi galat yang lokasinya acak dalam suatu *data stream* berdasarkan batasan yang melekat pada kode tersebut.

**Definisi 3.1** **(Vanstone dan Oorschot, 1989 : 205).** *Kode BCH atas dengan panjang blokdan jarak yang ditentukan (designed distance) adalah suatu kode yang dibentuk oleh suatu polinomial dengan KPK kelipatan persekutuan terkecil. Himpunan akar dari polinomial memuat elemen yang berbeda , denganadalah suatu akar primitif ke-dari elemen kesatuan danadalah suatu bilangan bulat*.

**Definisi 3.2** **(Vanstone dan Oorschot, 1989 : 205).** *Jikauntuk bilangan bulat positif, maka kode tersebut adalah suatu kode primitif, dan jikamaka kode tersebut disebut narrow-sense.*

Elemenadalah suatu akar ke-dari elemen kesatuan, sehingga juga merupakan suatu akar ke-dari elemen kesatuan untuk semua, sehingga membagi danmembagi pula.

Misaladalah polinomial minimal dari, adalah kelipatan persekutuan terkecil (KPK) dariyaitu . Polinomial disederhanakan menjadi karena setiap pangkat genap dari elemen primitif akan menghasilkan polinomial yang sama dengan beberapa pangkat ganjil.

**Contoh 3.2.** Misalsuatu elemen primitif darisedemikian sehingga*.* Polinomial minimal dari*,*, dan adalah berturut-turut

,

,

,

Kode BCH yang mengoreksi dua galat dengan panjangdibentuk oleh . Didapatkan sehingga kode tersebut adalah suatu kode*.* Bobot dari polinomial generatornya adalah, sehingga kode tersebut adalah suatu kode.

**Definisi 3.3 (Ling dan Xing, 2004 : 159)**

1. *artinya kelipatan persekutuan terkecil dari polinomial .*
2. *Polinomialmelambangkan polinomial minimal dariyang merupakan suatu elemen dari , suatu perluasan lapangan.*
3. *Kelipatan Persekutuan Terkecil dari dua polinomial tak nol adalah polinomial monik dengan derajat terkecil yang merupakan kelipatan daridan.*
4. *Misal adapolinomial tak nol . KPK dari adalah polinomial monik dengan derajat terkecil yang merupakan kelipatan dari semua , yang dilambangkan dengan .*
5. *Jika mempunyai bentuk faktorisasi dengan dan adalah polinomial monik tidak tereduksi atas, maka*

.

Berikut diberikan contoh penghitungan kelipatan persekutuan terkecil dari beberapa polinomial biner.

**Contoh 3.3.** Misal diketahui polinomial biner

Berdasarkan Definisi 3.3

**Lemma 3.1.** *Misal adalah polinomial atas. Jikaterbagi oleh setiap polinomialuntuk , makajuga terbagi oleh* .

**Bukti:**

Misal . Berdasarkan algoritma pembagian, ada dua polinomialdanatassedemikian sehingga dan.

Sehinggadan menyebabkanjuga terbagi oleh semua.

Polinomialmemiliki derajat yang terkecil, sehingga.

**Contoh 3.4:**

1. Polinomialterbagi oleh,, dan . Sehingga juga terbagi oleh .
2. Ditetapkan suatu elemen primitifdari dan dilambangkan polinomial minimal dariterhadapdengan. Setiap akardariadalah elemen dari sedemikian sehinggamemenuhi , sehinggaadalah pembagi linear dari .Polinomial tidak memiliki akar berganda sehingga adalah pembagi dari . Untuk himpunan bagian I dari , juga merupakan suatu pembagi dari

Contoh 3.4.2 memberikan suatu metode untuk mendapatkan pembagi dari . Pembagi tersebut dapat dipilih sebagai polinomial generator dari kode dengan panjang .

Suatu kode BCH yang mengoreksigalat dengan panjangdapat didefinisikan dengan cara sebagai berikut: suatu -tupel biner adalah kata kode jika dan hanya jika polinomial mempunyai akar . Kemudian adalah akar dariuntuk, sehingga

(3.1)

Persamaan tersebut dapat ditulis sebagai hasil kali matriks sebagai berikut:

(3.2)

Untuk. Syarat yang diberikan oleh persamaan tersebut menyatakan bahwa hasil kali dalam dari dan ) sama dengan nol. Kemudian dibentuk matriks berikut:

(3.3)

Jika adalah kata kode dalam kode BCH yang mengoreksi galat, maka

(3.4)

Di sisi lain, jika suatu -tupel memenuhi syarat (3.4), -tupel tersebut mengikuti (3.2) dan (3.1) bahwa untuk , adalah suatu akar polinomial. Sehinggamerupakan suatu kata kode dalam kode BCH yang mengoreksigalat. Oleh karena itu kode tersebut adalah ruang nol dari matriks, danadalah matriks *parity check* dari kode tersebut. Jika untukdan, adalah konjugat dari , didapatkanjika dan hanya jika. Hal tersebut menunjukkan bahwa hasil kali dalam dari dan baris ke-darijuga nol. Oleh karena itu, baris ke-daridapat dihilangkan. Hasilnya matrikspada (3.3) dapat direduksi menjadi bentuk berikut:

Entri-entri dariadalah elemen-elemen. Setiap elemen di dapat direpresentasikan oleh suatu -tupel atas. Jika setiap entri daridiganti oleh-tupel atasyang bersesuaian dalam bentuk kolom, didapatkan matriks *parity check* biner untuk kode tersebut.

## Parameter Kode BCH

Panjang kode BCH adalah. Pertama-tama akan dibahas dimensi dari kode BCH.

**Teorema 3.1**

1. *Dimensi dari kode BCH-er dengan panjang yang dibangun oleh independen dari pilihan elemen primitif.*
2. *Suatu kode BCH-er dengan panjang dengan jarak yang ditentukan mempunyai dimensi minimal*.

**Bukti**:

1. Misal adalah koset siklotomik darimodulo yang memuat. Ambil

Berdasarkan definisi polinomial minimal didapatkan

Sehingga, dimensinya sama dengan . Himpunanindependen dari pilihan, sehingga hasil yang diinginkan akan mengikuti.

1. Dari bagian i, dimensimemenuhi

Hasil tersebut menunjukkan bahwa, untuk mendapatkan dimensi dari kode BCH -er dengan panjang yang dibangun oleh perlu diperiksa kardinalitas dari , dengan adalah koset siklotomik dari modulo yang memuat .

**Contoh 3.5.** Diketahuikoset siklotomik modulo. Dimensi dari kode BCH biner dengan panjangdan jarak yang ditentukan dibangun oleh adalah

**Lemma** **3.2**. *Jikaadalah kode -er dengan panjangdan polinomial generator maka semuanya adalah akar-akar daridan polinomialtidak memiliki akar berganda maka suatu elemendariadalah suatu kata kode darijika dan hanya jika untuk semua* .

**Bukti:**

Jika adalah suatu kata kode dari , maka ada suatu polinomial sedemikian sehingga . Sehingga untuk semua . Sebaliknya jika untuk semua *r*, maka terbagi oleh karena tidak memiliki akar berganda. Artinya adalah kata kode dari

**Teorema 3.2**. *Suatu kode BCH dengan jarak yang ditentukan mempunyai jarak terkecil minimal.*

**Bukti:**

Diketahui adalah elemen primitif dari dan adalah suatu kode BCH yang dibangun oleh . Elemen-elemen dari adalah akar-akar dari .

Jika jarak terkecil dari kurang dari maka ada kata kode tak nol sedemikian sehingga . Berdasarkan Lemma 3.2 diketahui untuk semua

(3.5)

Diasumsikan *support* dari adalah , jika dan hanya jika . Sehingga (3.5) menjadi

Didapatkan sistem persamaan berikut dengan memilih persamaan- persamaanyang pertama dari sistem persamaan di atas karena ,:

Determinandari matriks koefisien persamaan di atas adalah

Dengan mengombinasikan kedua persamaan terakhir akan didapatkan yang merupakan kontradiksi dari pengandaian sebelumnya.

## Batas Kode BCH

**Teorema 3.3.** *Jika adalah kode BCH atas dengan jarak yang ditentukan makamemiliki jarak minimal.*

**Bukti:**

Misalmembentukdanmempunyai panjang blok. Misaladalah akar primitif ke- dari *elemen kesatuan* dalam dan adalah elemen-elemen yang berbeda yang ada di antara akar-akar . Bentuk matriks

Misal dapat dibuktikan bahwa tidak adakolom dariyang bergantung linear atas. Kemudian dengan mengganti elemen-elemen dari dalam berdasarkan -tupel kolom masing-masing atas , diketahui bahwa tidak ada himpunan kolom dalam matriks yang didapat ini yang bergantung linear atas atau atas dalam hal ini. Selain itu, tidak ada kolom dari himpunan maksimum dari baris-baris yang bebas linear dari matriks yang didapat tersebut yang bergantung linear. Baris-baris dalam matriks tersebut adalah vektor-vektor dalam , dan suatu himpunan maksimum dari baris-baris yang bebas linear dari matriks tersebut menghasilkan suatu matriks *parity check* untuk . Kemudian karena tidak ada kolom yang bebas linear atas, *C* memiliki jarak terkecil.

Untuk mendapatkan hasil akhir tersebut, ambil sebarang kolom-kolom dari . Kolom-kolom tersebut membentuk satu matriks atas . Dibuktikan bahwa determinan dari matriks tersebut bukan nol, yang mengimplikasikan bahwa kolom-kolom tersebut bebas linear. Determinan dari suatu himpunan arbitrer dari kolom-kolom dari adalah

dengan . Dengan menarik faktor yang sama dari tiap-tiap kolom didapatkan

Determinan tersebut adalah determinan Vandermonde yang dapat dievaluasi dengan cara berikut: Dimulai dengan memanipulasi determinan agar mendapatkan di setiap baris dari kolom pertama kecuali baris . Kalikan baris dengan dan kurangkan hasilnya dari baris, . Kemudian perluas determinan di sepanjang kolom pertama. Kolom semuanya selain baris pertama, sehingga hasilnya adalah suatu determinan dengan suatu faktor yang sama dari dalam kolom. Hasilnya adalah

Hasil yang didapatkan juga merupakan suatu determinan Vandermonde dengan ukuran yang lebih kecil. Dengan induksi didapatkan

Elemen adalah suatu akar primitif ke dari elemen kesatuan untuk, , , sehingga .

Teorema tersebut memberikan suatu metode untuk mengkonstruksi kode dengan suatu batas bawah pada jarak kode. Akan tetapi perlu diingat bahwa jarak kode yang sesungguhnya mungkin melebihi jarak yang telah ditentukan (*designed distance*).

## *Encoding* Kode BCH

Diberikan suatu polinomial tidak tereduksi dengan derajat dan dan sebagai koefisien-koefisiennya. Dengan polinomial tersebut, dapat dibentuk suatu representasi dari Galois Field dengan elemen. Lapangan tersebut terdiri dari semua polinomial dengan derajat maksimal . Setiap elemen lapangan yang tak nol adalah akar dari persamaan . Sehingga jika adalah sebarang elemen lapangan, .

Elemen lapangan juga dapat dipikirkan sebagai vektor yang komponen−komponennya adalah koefisien dari polinomial-polinomial tersebut. Jumlah dua vektor bersesuaian dengan jumlah polinomial yang sesuai.

Kode Bose-Chaudhuri dideskripsikan dengan memberikan matriks aturan *parity check*, yaitu matriks

dengan elemen primitif lapangan (Peterson, 1960).

Matriks tersebut adalah matriks dari elemen-elemen Akan tetapi jika setiap elemen lapangan dianggap sebagai suatu vektor dari digit biner, matriks tersebut adalah matriks dari digit biner. Suatu digit biner dianggap sebagai suatu kata kode jika per kolomnya memenuhi *parity check* yang dideskripsikan. Misalnya jika hasil kali dari suatu vektor dengan matriks tersebut adalah nol. Dengan kata lain, himpunan semua kata kode adalah ruang nol (kiri) dari matriks tersebut.

**Contoh 3.6.** Misal suatu akar dari persamaan. Elemen lapangan yang tidak nol diberikan dalam Tabel 3.1.

**Tabel 3.1** Representasi dari

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Dengan mengambil , dihasilkan matriks *parity check* sebagai berikut:

Dari kedua belas kolom, kolom yang terakhir trivial dan kolom ke-11 merupakan duplikat, sehingga kedua kolom tersebut dapat dihilangkan. Sisanya independen, hasilnya adalah suatu kode dengan kata kode lima belas digit dengan sepuluh di antaranya adalah *parity check* dan lima adalah tempat informasi. Kode tersebut mengoreksi semua *triple-error*.

Untuk melakukan *encoding* sistematis, dilakukan langkah-langkah sebagai berikut:

Jika adalah suatu kode dengan polinomial generator maka blok pesan k diberikan oleh polinomial pesan m(x).

Langkah 1. Kalikan polinomial pesan dengan .

Langkah 2. Bagi hasil dari langkah 1 dengan polinomial generator dengan sebagai sisanya.

Langkah 3. Bentuk .

**Contoh 3.7.** Dikonstruksi suatu polinomial generator untuk kode BCH . Kode tersebut memiliki bit kata kode, bit redundansi, dan mengoreksi galat . Polinomial generator untuk kode tersebut dibangun menggunakan polinomial primitif atas seperti yang ditunjukkan di Tabel 3.2.

**Tabel 3.2** Lapangan dengan Elemen yang dibangun oleh polinomial

|  |  |  |  |
| --- | --- | --- | --- |
| Bentuk  Pangkat | Bentuk  Polinomial | Bentuk  4-tupel | Polinomial  Minimal |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Misal adalah elemen primitif . Polinomial generator dari kode BCH yang mengoreksi galat dengan panjang adalah polinomial dengan derajat terkecil atasdengan akar-akar , atau untuk . Empat polinomial minimal pertama dengan pangkat ganjil adalah:

Sehingga, (karena polinomial- polinomial tersebut tidak tereduksi) sehingga

Misalkan ada suatu kode biner yang melambangkan “D” dan ditempatkan di informasi bit yang kemudian ditambahkan dengan suatu barisan bit. Kemudian barisan bit tersebut dibagi oleh polinomial generator untuk mendapatkan suatu sisa. Dengan mengombinasikan barisan pesan dengan barisan sisa, didapatkan kata kode.

**Contoh 3.8:**

=

## *Decoding* Kode BCH

### Prosedur Pendeteksian Galat

Diasumsikan penggunaan kode BCH dengan panjang blok yang dirancang untuk mengoreksi maksimalgalat. Misal dikirimkan kata kodedan diterima kata . Penentuan apakah suatu kata kode atau bukan dilakukan dengan pemeriksaan oleh matriks *parity check* yaitu bukan kata kode jika. Jika galatnya adalah maka .

Jika terjadi , maka ada tepat satu kemungkinan kata galatdengan bobot maksimalyang memenuhi . Kata galat menunjukkan satu himpunan kolom dari yang jumlahnya adalah . Pendekatan yang paling sederhana untuk menentukan adalah dengan mencari himpunan kolom yang tepat. Jika maka kode tersebut adalah kode Hamming dan pencarian himpunan kolom tersebut mudah dilakukan yaitu dengan memeriksa kolom dari untuk menentukan yang mana yang memberikan *syndrome* .

Akan tetapi untuk kode BCH dengan perlu dipertimbangkan yaitu kombinasi dari kolom-kolom dan untuk dan saja angka tersebut sudah mencapai sehingga diperlukan prosedur yang lebih efisien.

Agar asumsi tersebut lebih spesifik diberikan contoh sebagai berikut:

dengan . Penomorannya dimulai dari dan dipilih berdasarkan koherensinya dengan polinomial representasi.

**Definisi 3.4 (Pretzel, 192: 234).** *Jika komponen dari kata galat tak nol, , dikatakan bahwaadalah lokasi galat dari . Himpunan lokasi-lokasi galat dilambangkan dengan* .

Saat bekerja dengan BCHdiasumsikan banyaknya galat adalah paling banyak sebanyak. Sehingga memiliki elemen dan adalah bobot dari

**Contoh 3.9.** Dalam BCH diketahui:

Katayang dikirimkan adalah ;

Katayang diterima adalah );

Jadi kata galatnya adalah ;

Sehingga dan lokasi galatnya adalah dan (dihitung dari kanan mulai dari ).

### *Syndrome* dari Kata yang Diterima

Jika dianggap sebagai suatu matriks atas maka *full syndrome* adalah suatu kata dengan panjang dengan entri dalam .

**Contoh 3.10.** Dalam BCH diketahui

sehingga

,

,

,

,

,

,

perlu diperhatikan bahwa dan .

Kemudian kode direpresentasikan oleh polinomial. Dengan

.

Polinomial yang bersesuaian adalah

sehingga

Baris-baris dari berbentuk dengan , sehingga adalah elemen primitif dari danberjalan dari ke sehingga entri ke-daridapat ditulis sebagai .

**Contoh 3.11.** Dikonstruksi suatu polinomial generator untuk kode BCH . Kode tersebut memiliki bit kata kode, bit redundansi, dan mengoreksi galat . Polinomial generator untuk kode tersebut dibangun menggunakan polinomial primitif atas . Empat polinomial minimal pertama dari dengan pangkat ganjil adalah:

Barisan yang diterima direpresentasikan oleh .

Banyaknya elemen *syndrome* adalah untuk menemukan galat. Elemen-elemen *syndrome* tersebut dilambangkan dengan dan dihitung dengan

### Algoritma Berlekamp Massey

Tujuan utama dari algoritma Berlekamp-Massey adalah untuk mengevaluasi kode BCH biner. Berlekamp menerbitkan algoritma tersebut di tahun 1986 yang beberapa waktu kemudian diikuti oleh penerbitan variasi algoritma oleh Massey.

#### *Key Equation* untuk *Decoding* Kode BCH Biner

Jika *encoder* mengirimkan kata kode BCH biner

dan noise di dalam *channel* menyebabkan terjadinya galat aditif yang diberikan oleh koefisien dari polinomial biner

dan kata yang diterima diberikan oleh

Untuk , kata kode tersebut adalah kelipatan dari polinomial minimal , sehingga

dengan lokasi galat lapangan Galois melambangkan posisi dengan . jika dibagi oleh, yaitu polinomial minimal dari maka dapat dihitung dari sisanya, yaitu . Setelah *decoder* menghitung masalah utamanya adalah menemukan lokasi galat dari persamaan

Secara umum, persamaan tersebut akan memiliki banyak solusi, masing-masing bersesuaian dengan suatu pola galat yang berbeda dalam koset grup aditif kata kode yang sama. *Decoder* harus menemukan suatu solusi dengan suatu nilai yang sekecil mungkin.

Untuk menyelesaikan persamaan tersebut, pertama-tama *decoder* berusaha menemukan koefisien dari polinomial lokator galat yang didefinisikan oleh

Setelah *decoder* menentukan polinomial lokator galat , akar *reciprocal* dari dapat ditemukan dengan Chien Search, sehingga galat dapat dikoreksi. Bagian yang tersulit dalam prosedur *decoding* tersebut adalah menemukan dari .

Untuk menghubungkan dan , diberikan fungsi pembangkit

Fraksi persamaan tersebut dapat dieliminasi dengan mengalikannya dengan .

Penjumlahan denganke kedua ruas memberikan

Didefinisikan polinomial oleh persamaan

Sehingga didapatkan persamaan

Secara umum, *decoder* hanya mengetahui koefisien dari pangkat pertama daridalam , tanpa mengetahui . Dengan kata lain, *decoder* tidak mengetahui , tapi mengetahui . Persamaan yang relevan, yang disebut *key equation* dalam buku Berlekamp adalah

mod

Berlekamp memberikan suatu algoritma untuk menyelesaikan key equation tersebut atas sebarang lapangan:

Awalnya definisikan , , , , , . Kemudian dilakukan proses secara rekursif dengan syarat: Jika tidak diketahui, hentikan penghitungan, jika diketahui definisikan sebagai koefisien dari dalam hasil kali dan

Jika , atau jika , atau jika dan dan , maka

.

Akan tetapi jikadan atau dan maka

.

#### Algoritma Iteratif untuk Mendapatkan Polinomial Lokasi-Galat σ(x)

Untuk mendapatkan polinomial lokasi galat , berikut diberikan Identitas Newton yang menunjukkan hubungan antara dengan komponen *syndrome*:

.

Langkah pertama dari iterasi ini adalah mendapatkan polinomial derajat terkecil yang koefisiennya memenuhi identitas Newton yang pertama. Langkah berikutnya adalah memeriksa apakah koefisien dari juga memenuhi identitas Newton yang kedua. Jika memenuhi, maka

.

Jika tidak memenuhi, suatu syarat koreksi ditambahkan ke untuk membentuk sedemikian sehingga memiliki derajat minimum dan koefisiennya memenuhi dua identitas pertama Newton. Sehingga di akhir dari langkah kedua iterasi kita akan mendapatkan suatu polinomial dengan derajat minimum dan koefisiennya memenuhi dua identitas pertama Newton. Langkah ketiga dari iterasi tersebut adalah mencari suatu polinomial dengan derajat minimum dari sedemikian sehingga koefisien memenuhi tiga identitas pertama Newton. Jika memenuhi maka . Jika tidak memenuhi maka suatu syarat koreksi ditambahkan ke untuk membentuk. Iterasi diteruskan sampai didapatkan .

Kemudian diambil untuk menjadi polinomial lokasi galat , yaitu

,

polinomial tersebut akan menghasilkan suatu pola galat dengan bobot minimum yang memenuhi persamaan yang menunjukkan hubungan antara komponen *syndrome* dan pola galat berikut:

Jika banyaknya galat di dalam polinomial yang diterima adalah atau kurang dari , maka membentuk pola galat yang sebenarnya.

Misal

adalah polinomial derajat minimum yang didapatkan setelah langkah iterasi yang koefisiennya memenuhi identitas pertama Newton. Untuk menentukan dihitung kuantitas berikut:

Kuantitas tersebut disebut ketidakcocokan (*discrepancy*) ke-. Jika , maka koefisien dari memenuhi identitas Newton yang ke-. Sehingga

jika maka koefisien dari tidak memenuhi identitas ke- Newton dan suatu syarat koreksi perlu ditambahkan ke untuk mendapatkan . Untuk memperoleh syarat koreksi tersebut, iterasi kembali ke langkah-langkah sebelum langkah ke- dan menentukan polinomial sedemikian sehingga ketidakcocokan ke-, dan [ adalah derajat dari ] memiliki nilai terbesar. Sehingga

yang merupakan polinomial derajat minimum yang koefisiennya memenuhi pertama identitas Newton.

Untuk melakukan iterasi pencarian , dimulai dari Tabel 3.3

**Tabel 3.3** Tabel iterasi pencarian

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | 1  1 |  |  |  |

Untuk mengisi tabel, dengan adalah derajat , asumsikan semua baris telah diisi sampai baris ke-, untuk baris ke- diisi sebagai berikut:

1. Jika maka dan .
2. Jika , temukan baris lain sebelum baris ke- sedemikian sehingga dan bilangan di kolom terakhir tabel memiliki nilai terbesar, maka didapatkan dari

Untuk semua kasus,

dengan adalah koefisien dari . Polinomial di baris terakhir seharusnya merupakan yang diperlukan. Jika polinomial tersebut memiliki derajat yang lebih besar dari , artinya ada lebih dari di dalam polinomial yang diterima , dan secara umum tidak mungkin untuk menemukan lokasi galat tersebut.

#### Algoritma yang Disederhanakan untuk Mendapatkan

Untuk kode BCH biner, baris-baris di Tabel 3.3 tidak perlu diisi. Algoritma yang disederhanakan dapat dilakukan yang hanya memerlukan pengisian suatu tabel dengan t baris kosong.

**Tabel 3.4** Iterasi pencarian dengan algoritma yang disederhanakan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

Asumsikan semua baris telah diisi sampai baris ke-, untuk baris ke- diisi sebagai berikut:

1. Jika maka dan .
2. Jika , temukan baris lain sebelum baris ke-, misalkan baris ke-, sedemikian sehingga di kolom terakhir sebesar mungkin, dan , maka

Dalam kedua kasus tersebut, adalah derajat dari , dan ketidakcocokan pada langkah ke- adalah

Polinomial di baris terakhir seharusnya merupakan yang dicari. Jika polinomial tersebut memiliki derajat yang lebih besar dari pada , artinya ada lebih dari galat, dan secara umum tidak mungkin untuk menemukan lokasi galat tersebut.

**Contoh 3.12.** Dikonstruksi suatu polinomial generator untuk kode BCH . Kode tersebut memiliki bit kata kode, bit redundansi, dan mengoreksi galat . Barisan yang diterima direpresentasikan oleh r. Elemen-elemen *syndrome* dari kode tersebut adalah

“Key Equation” diberikan oleh:

(3.6)

(3.7)

(3.8)

**Langkah-langkah**:

1. Nilai awal , ,
2. Substitusikan

ke persamaan (3.6)

1. Substitusi ke (3.7)

1. Substitusi , , ke (3.8)

1. Dengan cara yang sama,

Untuk , , ,

, dan

Untuk , , ,

, dan

Untuk , , ,

, dan

Untuk , , ,

Polinomial yang terakhir yaitu adalah polinomial penunjuk letak galat. Tabel Lin dan Costello dibentuk menggunakan penghitungan yang telah dilakukan.

**Tabel 3.5** Hasil pencarian

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | - | - | - |

### Algoritma Chien Search

Chien Search adalah suatu algoritma untuk menemukan akar dari polinomial penentu lokasi galat yang didapatkan saat melakukan *decoding* suatu kode.

Misal polinomial yang akar-akarnya akan ditentukan adalah

Secara konseptual, dapat dievaluasi untuk setiap yang tak nol di , elemen-elemen yang menghasilkan adalah akar-akar dari polinomial tersebut. Chien Search berdasarkan pada dua observasi:

* Setiap tak nol dapat dinyatakan sebagai untuk beberapa , dengan adalah suatu elemen primitif dari , adalah bilangan pangkat dari elemen primitif . Sehingga pangkat untuk mencakup semua lapangan kecuali elemen nol.
* Berlaku hubungan berikut:

**Contoh 3.13.** Polinomial adalah polinomial final penunjuk letak galat.

Dan seterusnya sampai (penghitungan diberikan di Lampiran 1) sehingga akar-akarnya adalah , , , , . Posisi galat adalah invers dari akar-akarnya (, , , , ) atau , atau jika ditulis dalam bentuk polinomial . Data yang dikirimkan atau data orisinil didapat dengan melakukan penjumlahan modulo-2 antara dan .

Dalam proses *decoding*, algoritma Berlekamp Massey digunakan untuk menghitung koefisien polinomial penunjuk lokasi galat. Polinomial tersebut digunakan dalam algoritma Chien Search. Hasil akhir dari proses *decoding* adalah posisi galat yang terjadi di dalam barisan yang diterima untuk kemudian dikoreksi menjadi pesan yang benar.

## Implementasi *Encoder* dan *Decoder* Kode BCH

### Implementasi *Encoder* untuk kode BCH (31, 11) pada FPGA

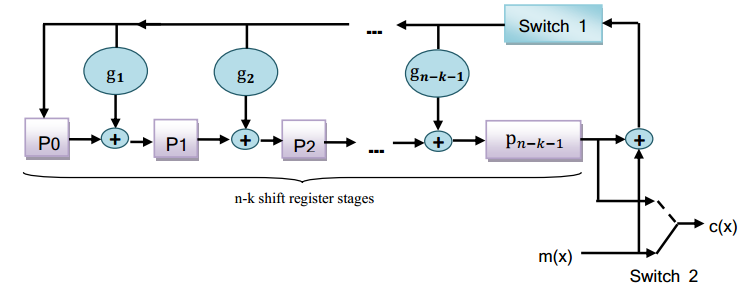
Transmisi informasi yang dapat diandalkan melalui *channel* dengan gangguan adalah salah satu persyaratan dasar dari informasi digital dan sistem komunikasi. Kode pengoreksi galat memiliki jangkauan penerapan yang luas pada bidang-bidang yang berbeda seperti komunikasi data digital, desain sistem memori, dan desain komputer yang toleran terhadap galat.

*Field-Programmable Gate Arrays* (FPGA) adalah *device* silikon yang terprogram secara elektrik untuk menjadi hampir semua sirkuit atau sistem digital (Mohammed, 2013 : 24). FPGA memberikan beberapa keuntungan dibanding teknologi *Application Specific Integrated Circuit* (ASIC), misalnya sel standar. ASIC didesain untuk aplikasi yang spesifik, dan setelah diproduksi ASIC tidak dapat dimodifikasi lagi, sedangkan FPGA dikonfigurasi dalam jangka waktu yang relatif pendek dan seringkali dapat dikonfigurasi ulang jika terjadi galat.

Suatu FPGA terdiri atas suatu susunan *Configurable Logic Blocks* (CLB) netral, *programmable interconnects* dan *Input Output Blocks* (IOB). Arsitektur FPGA didominasi oleh *programmable interconnects* dan CLB yang relatif sederhana. Fitur tersebut membuat *device* menjadi jauh lebih fleksibel dalam hal jangkauan desain yang dapat diimplementasikan dengan *device* tersebut.

Proses *encoding* kode BCH dalam bentuk yang sistematis dapat dinyatakan oleh sirkuit yang ditunjukkan dalam Gambar 3.1. Prosedur *encoding* sistematis dapat dideskripsikan dengan langkah-langkah sebagai berikut:

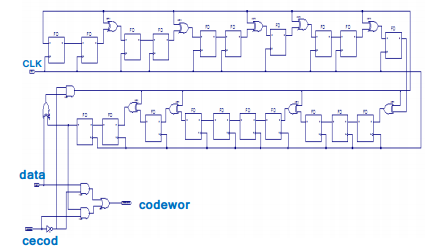
1. *Switch* 1 ditutup selama pergeseran pertama, untuk memungkinkan transmisi dari bit pesan ke *stage encoding shift register*.
2. *Switch* 2 berada dalam posisi turun untuk memungkinkan transmisi bit pesan secara langsung ke register output selama pergeseran pertama.
3. Setelah transmisi dari bit pesan ke-, *switch* 1 dibuka dan *switch* 2 dipindah ke posisi naik.
4. Sisa sebanyak pergeseran membersihkan *encoding register* dengan memindahkan bit parity ke *output register*.
5. Total banyaknya pergeseran adalah , dan konten dari *output register* adalah polinomial kata kode .



**Gambar 3.1** *Encoding* dengan suatu *stage shift register*

Bit parity dari kode BCH (31, 11) dihitung menggunakan *Linear Feedback Shift Register* (LFSR). Koneksi umpan balik dari LFSR dibentuk dalam suatu cara yang bergantung pada polinomial generator kode. Polinomial generator dari kode BCH (31, 11) adalah .

Data *input* sirkuit *encoding* adalah 11 bit dan *output*nya adalah suatu serial atas 31 bit. *Encoder* kode BCH (31, 11) yang diimplementasikan ke *device* target FPGA ditunjukkan pada Gambar 3.2.



**codeword**

**Gambar 3.2** Sirkuit logika *encoding* kode BCH (31, 11) yang diimplementasikan pada FPGA

### Implementasi *Decoder* BCH (63, 51) untuk WBAN

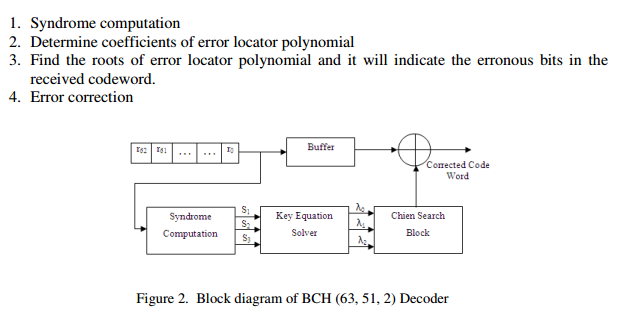
Seiring dengan berkurangnya ukuran dan meningkatnya kemampuan peralatan elektronik, *Wireless Body Area Network* (WBAN) menggantikan sistem pelayanan kesehatan konvensional dengan terus menerus memonitor kesehatan pasien. Tingkat daya baterai yang diperlukan untuk mengoperasikan peralatan membatasi banyaknya operasi komputasional dan konsumsi daya dari *front-end* radio. *Front-end* radio menentukan konsumsi daya dari *Physical Layer* (PHY) dan *Medium Access Control* (MAC)dari WBAN karena *front-end* radio merupakan bagian utama yang mengkonsumsi daya.

Dalam WBAN ini, diimplementasikan *encoder* dan *decoder* kode BCH sistematis (63, 51). WBAN menawarkan banyak penerapan baru di area *remote health monitoring*, pelayanan kesehatan, obat-obatan, multimedia, olahraga, dan lain sebagainya. Terdapat suatu standar komunikasi baru dengan lapisan MAC dan PHY, yang disebut *Narrowband* (NB), *Ultrawideband* (UWB), dan *Human Body Communications* (HBC). Di antara lapisan PHY yang ada, PHY narrowband 2.4 GHz adalah yang paling matang. BCH (63, 51, 2) adalah kode yang mengoreksi kode galat yang bagus untuk digunakan pada baseband processing dari NB PHY.

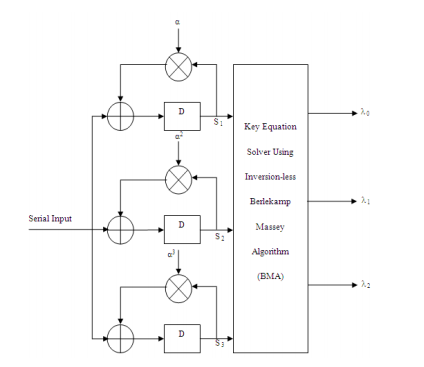
Proses *decoding* kode BCH terdiri dari empat langkah utama:

1. Penghitungan *syndrome*.
2. Penentuan koefisien dari polinomial penentu letak galat.
3. Pencarian akar dari polinomial penentu letak galat yang akan mengindikasikan bit yang salah dalam kata kode yang diterima.
4. Pengoreksian galat.

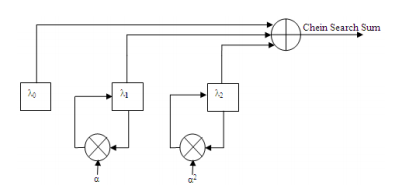
Ilustrasi implementasi langkah-langkah tersebut di dalam *decoder* ditunjukkan oleh Gambar 3.3, Gambar 3.4 dan Gambar 3.5.



**Gambar 3.3** Diagram Blok *Decoder* BCH (63, 51, 2)



**Gambar 3.4** Implementasi Penghitungan Syndrome dan Pencarian Koefisien



**Gambar 3.5** Implementasi Blok Chien Search

# BAB IV

**PENUTUP**

## Kesimpulan

Berdasarkan pembahasan yang telah diuraikan sebelumnya, kesimpulan yang dapat diambil adalah sebagai berikut.

1. Untuk melakukan *encoding* pada suatu pesan, kode biner yang melambangkan pesan yang akan dikirimkan ditempatkan di informasi bit yang kemudian ditambahkan dengan suatu barisan bit. Kemudian barisan bit tersebut dibagi oleh polinomial generator untuk mendapatkan suatu sisa. Dengan mengombinasikan barisan pesan dengan barisan sisa, didapatkan kata kode. *Encoding* yang digunakan disebut *encoding* sistematis dengan bit pesan dan bit *check* diletakkan bersebelahan.
2. Untuk melakukan *decoding* terhadap pesan yang diterima terdapat empat langkah yang perlu dilakukan. Langkah pertama adalah melakukan pendeteksian galat melalui pemeriksaan matriks *parity check*. Langkah kedua adalah menentukan *syndrome* dari kata yang diterima. Langkah ketiga adalah mengevaluasi kode BCH dengan algoritma Berlekamp Massey. Hasil dari langkah ketiga adalah suatu polinomial penunjuk letak galat. Langkah keempat adalah penentuan posisi galat yang terjadi di dalam barisan yang diterima dengan menggunakan algoritma Chien Search. Setelah posisi galat diketahui, katayang diterima kemudian dikoreksi menjadi pesan yang benar.
3. Implementasi *encoder* kode BCH pada FPGA dilakukan dengan cara

menghitung bit parity dari kode BCH (31, 11) menggunakan LFSR (*Linear Feedback Shift Register*). Koneksi umpan balik dari LFSR dibentuk dalam suatu cara yang bergantung pada polinomial generator kode. *Encoder* kode tersebut kemudian diimplementasikan ke *device* target FPGA. Implementasi *decoder* kode BCH pada WBAN (Wireless Body Area Network) menggantikan sistem pelayanan kesehatan konvensional dengan terus menerus memonitor kesehatan pasien. Dalam WBAN diimplementasikan *encoder* dan *decoder* kode BCH sistematis (63, 51).

## Saran

Pada skripsi ini cara *encoding* dan *decoding* kode BCH terbatas pada kode biner. Oleh karena itu, pada penelitian selanjutnya disarankan untuk membahas cara encoding dan *decoding* pada kode selain kode biner. Selain itu, dalam skripsi ini, saat didapati bahwa galat yang terjadi melebihi batas galat yang ditentukan, penghitungan akan berhenti dan kode tidak dapat diperbaiki. Sehingga, untuk penelitian selanjutnya disarankan untuk membahas cara agar kode tersebut tetap dapat diperbaiki.

Adanya penelitian ini dapat dijadikan informasi bahwa kode BCH yang dibentuk sebaiknya cukup besar agar dapat mengoreksi cukup banyak galat dan juga tidak terlalu besar agar tidak terlalu membebani *channel*.

# DAFTAR PUSTAKA

Berlekamp.E.R. (1968). *Algebraic Coding Theory*. New York: Mc GrawHill.

Bose, R. C. , D.K.Ray-Chaudhuri. (1960). On a class of error correcting binary group codes*. Inform. Control*. 3. Hlm. 68-79.

Edel, Yves & Bierbrauer, Jurgen. (1999). Some Codes Related to BCH-codes of Low Dimension*. Discrete Mathematics 205*.

Edy Susanto. (2009). Analisis Kerja Kode BCH. *Tugas Akhir.* Universitas Sumatera Utara.

Fraleigh, J. B. (2003). *A First Course in Algebra, 7th Edition*. USA: Pearson Education, Inc.

Gallian, Joseph A. (2006). *Contemporary Abstract Algebra, 7th Edition.* USA: Brooks/Cole, Cengage Learning.

Grillet, P. Antoine. (2007). *Abstract Algebra, 2nd Edition*. New York: Spgelangganger Science and Business Media, LLC.

Herstein, I. N. (1990). *Topics in Algebra, 2nd Edition*. New York :John Willey and Sons.

Klima, Richard E., et al. (1999). *Applications of Abstract Algebra with Maple.* New York: CRC Press.

Lange, Tanja. (2011). *Coding Theory & Cryptology I (Course Note)*. <http://www.hyperelliptic.org//> diakses pada 03 September 2015.

Ling, San, Chaoping Xing. (2004). *Coding Theory A First Course*. New York: Cambridge University Press.

Massey, James L. (1965). Step-by-step Decoding of the Bose-Chaudhuri-Hocquenghem Codes*. IEEE Transaction on Information Theory*. Volume 11.

Mathew, Priya, et al. (2014). Hardware Implementation of (63, 51) BCH Encoder dan Decoder for WBAN Using LFSR and BMA. *International Journal on Information Theory (IJIT)*. Vol.3 No.3.

Mohammed, Samir Jasim. (2013). Implementation of Encoder for (31, k) Binary BCH Code based on FPGA for Multiple Error Correction Control. *International Journal of Computer Applications.*Volume 76. No.11.

Mozhiarasi P., C. Gayathri, V. Deepan. (2015). An Enhanced (31, 11, 5) Binary BCH Encoder and Decoder for Data Transmission. *International Journal of Engineering Research and General Science*. Volume 3, Issue 2, Part 2.

Peterson, W.W. (1960). Encoding and Error-Correction procedures for the Bose-Chaudhuri Codes*. IRE Trans. Inf. Theory*. Hlm. 459-470.

Pretzel, Oliver. (1992). *Error-Correcting Codes and Finite Fields*. Oxford: Oxford University Press.

Shanon, Claude E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal.* Volume 27.

Sihar Parlinggoma Panjaitan. (2006). Analisis Algoritma Kode Konvolusi dan Kode BCH. *Jurnal Sistem Teknik Industri USU*. Volume 7. No.2.

Togneri, Roberto, Christopher J. S. deSilva. (2006). *Fundamental of Information Theory and Coding Design*. Florida: CRC Press.

Vanstone, Scott A., Paul C. van Oorschot. (1989). *An Introduction to Error Correcting Codes with Applications*. Massachusetts: Kluwer Academic Publishers.

Yunghsiang S. Han. (2006). *BCH Codes*. Graduate Institute of Communication Engineering, National Taipei UniversityTaiwan.