Volume x No x xxxxx (20xx)

e-ISSN: **2615-3270**

p-ISSN: **2615-3599**

Eigen Mathematics Journal

Homepage jurnal: http://eigen.unram.ac.id

SIMULASI KEMAMPUAN KOREKSI KESALAHAN KODE KUASI SIKLIK DIPERUMUM-LDPC PADA CHANNEL BINER SIMETRIS

Muhammad Sukriadi[1], Dr. Irwansyah, M.Si.[2],Dr. I Gede Adhitya Wisnu Wardhana, S.Si., M.Si.[3]

[1] Program Studi Matematika, FMIPA, Universitas Mataram, Jl. Majapahit No. 62 MAtaram, 83125, Indonesia, Email: sukri.maret97@gmail.com

[2] Program Studi Matematika, FMIPA, Universitas Mataram, Jl. Majapahit No. 62 MAtaram, 83125, Indonesia, Email: irw@unram.ac.id

[3] Program Studi Matematika, FMIPA, Universitas Mataram, Jl. Majapahit No. 62 MAtaram, 83125, Indonesia, Email: adhitya.wardhana@unram.ac.id

A B S T R A C T

Low Density Parity Check code or abbreviated as LDPC is a linear error correcting that is used to maintain the integrity of the data. This code is known to have error-correcting capabilities that are close to the maximum theoretical error-correction limit. LDPC code can be made efficient by hybridizing with generalized quasi-cyclic code. Quasi-cyclic codes are generalizations of cyclic codes. The error correction capability of this generalized quasi-cyclic code-LDPC is closely related to the decoding algorithm chosen for the LDPC code. The algorithm used in this research is the Log-Likelihood Ratio Sum-Product Algorithm or abbreviated as LLR-SPA. In this research, simulation of quasi-cyclic code error correction capability in general-LDPC is given on a symmetric binary channel. The main objective of this research is the maximum number of errors that can be corrected by a generalized quasi-cyclic code-LDPC on a symmetric binary channel. Based on the simulation, the main result is that the greater the number of errors added, the smaller the possibility of the message being received in its entirety.

Keywords: *Code, Coding Theory, Error Correction, Generalized Quasi-cyclic, Low Density Parity Check*

A B S T R A K

Kode *Low Density Parity Check* atau disingkat menjadi LDPC merupakan pengoreksi kesalahan linear yang digunakan untuk menjaga integritas data. Kode ini dikenal memiliki kemampuan mengoreksi kesalahan yang mendekati batas maksimum pengoreksi kesalahan secara teoritis. Kode LDPC dapat dibuat efisien dengan melakukan *hybrid* dengan kode kuasi siklik diperumum. Kode kuasi siklik merupakan perumuman dari kode siklik. Kemampuan koreksi kesalahan kode kuasi siklik diperumum-LDPC ini berkaitan erat dengan algoritma *decoding*

* Corresponding author.
Alamat e-mail: author@institute.xxx

yang dipilih untuk kode LDPC. Algoritma yang digunakan dalam penelitian ini adalah *Log-Likelihood Ratio Sum-Product Algorithm* atau disingkat menjadi LLR-SPA. Pada penelitian ini diberikan simulasi kemampuan koreksi kesalahan kode kuasi siklik diperumum-LDPC pada *channel* biner simetris. Tujuan utama dari penelitian ini adalah maksimum jumlah kesalahan dapat dikoreksi oleh kode kuasi siklik diperumum-LDPC pada *channel* biner simetris. Berdasarkan simulasi diperoleh hasil utamanya adalah semakin besar jumlah kesalahan yang ditambahkan mengakibatkan kemungkinan pesan yang diterima secara utuh menjadi kecil.

Kata kunci : Kode, Koreksi Kesalahan, Kuasi Siklik Diperumum, *Low Density Parity Check*, Teori Koding

Diserahkan: xx-xx-xxxx; Diterima: xx-xx-xxxx; Doi: https://doi.org/10.29303/emj.xxx.x

1. Pendahuluan

Teknologi merupakan alat atau mesin yang diciptakan untuk mempermudah manusia dalam menyelesaikan berbagai macam masalah yang terdapat di dunia. Perkembangan teknologi saat ini telah memperkecil frekuensi interaksi atau komunikasi langsung antar manusia dan memungkinkan untuk saling berinteraksi secara bebas dalam skala global. Salah satu aspek penting dalam teknologi komunikasi adalah integritas data. Hal ini disebabkan karena aspek ini menjamin data yang disimpan/dikirim dapat diterima atau dibaca kembali secara utuh. Salah satu cara untuk menjamin integritas data dalam komunikasi adalah dengan menggunakan pengkodean data transmisi. Pengkodean menjadi sangat penting karena saluran komunikasi sering mengalami gangguan, seperti cuaca, kekuatan sinyal, kerusakan perangkat komunikasi, dan sebagainya.

Semakin besar data yang dikirimkan maka semakin besar juga peluang kesalahan dalam pengiriman data dan semakin rendah laju pengiriman data. Teknik pengkodean yang dapat mendeteksi atau mengoreksi kesalahan data serta memiliki laju pengiriman yang tinggi adalah kode *Low Density Parity Check* (LDPC). Kode ini dapat dibuat menjadi efisien secara kompleksitas memori dengan cara melakukan *hybrid* dengan kode kuasi siklik diperumum. Kode *hybrid* ini memiliki kemampuan koreksi kesalahan yang kuat yang diambil dari kode LDPC dan memiliki kompleksitas memori yang rendah yang diambil dari kode kuasi siklik diperumum.

Secara umum, kode LDPC menggunakan algoritma penyampaian pesan (*beliefe propagation*) untuk *decoding*. Algoritma ini didasarkan pada graf *Tanner* yang sesuai dari matriks *parity check* H. Salah satu algoritma yang termasuk dalam algoritma penyampaian pesan adalah *Log-Likelihood Ratio Sum-Product Algorithm* (LLR-SPA) yang merupakan algoritma *soft decoding*. Algoritma LLR-SPA tidak ada rumus umum untuk menghitung kapabilitas koreksi kesalahan, tetapi kapabilitas koreksi dapat ditentukan melalui simulasi. Oleh karena itu, dalam penelitian bertujuan untuk menentukan banyaknya kesalahan yang dapat dikoreksi oleh kode kuasi siklik diperumum-LDPC pada *channel* biner simetris berdasarkan simulasi.

2. Landasan Teori

Suatu kode dengan panjang n dan ukuran k disebut suatu kode (n, k). Setiap anggota dari kode disebut kata kode (*codeword*). Suatu kode C dengan panjang n atas $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ adalah suatu subset dari $\mathbb{F}_2^n$, dan n adalah bilangan bulat tak nol.

Definisi 1 *Suatu kode linear C dengan panjang n atas $\mathbb{F}_q$ adalah subruang dari $\mathbb{F}_q^n$.*

Suatu kode linear $C[n, k]$ adalah subruang dengan dimensi k dari $\mathbb{F}_q^n$. Jika C merupakan kode linear, maka terdapat matriks pembangun G berukuran $k \times n$. Setiap kode linear C, terdapat suatu kode linear $[n-k, n]$ dimana $C^{\perp}$ adalah dual dari C terhadap *Euclidean product.* Matriks pembangun untuk $C^{\perp}$ disebut matriks parity check H berukuran $(n-k) \times n$.

Diberikan σ adalah suatu permutasi di grup simetri S_n. Permutasi σ dapat ditulis $\sigma = \sigma_1\sigma_2 \dots \sigma_k$, untuk suatu bilangan asli k, dimana $\sigma_1, \dots, \sigma_k$ adalah *disjoint cycles* dan panjang$(\sigma_i) = m_i \geq 1$, untuk semua $i = 1,2, \dots, k$. Untuk sebarang $\boldsymbol{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$, didefinisikan aksi σ terhadap vektor x, sedemikian sehingga

$$\sigma(\boldsymbol{x}) = \left(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(n)}\right).$$

Selain itu, untuk setiap $C \subseteq \mathbb{F}_q^n$, didefinisikan aksi σ ke C, sebagai berikut

$$\sigma(C) = \{\sigma(c) | \forall c \in C\}.$$

Definisi 2 *Suatu kode linear $C \subseteq \mathbb{F}_q^n$ disebut suatu kode kuasi siklik diperumum atau σ-code jika $\sigma(C) = C$.*

σ-code adalah suatu kode siklik, jika σ adalah permutasi siklik. Lebih jauh, jika $m_1 = m_2 = \cdots = m_k = l$, maka σ-code adalah suatu kode kuasi siklik berindeks l.

Definisi 3 *Diberikan σ suatu permutasi di S_n. Suatu kode linear $C[n,k] \subseteq \mathbb{F}_2^n$ disebut suatu kode kuasi siklik diperumum-LDPC $(n, n-k)$, jika C memenuhi kedua aksioma berikut.*

i. $\sigma(C) = C$, *dan*
ii. *C memiliki matriks parity check H yang bobot barisnya kecil* $\in \mathbb{F}_2^{(n-k)\times n}$.

Terdapat cara mudah untuk mengkonstruksi kode kuasi siklik diperumum-LDPC.

Algoritma 1 *Diberikan $\sigma = \sigma_1\sigma_2 \dots \sigma_k$ di S_n, dimana length$(\sigma_i) = m_i$.*

a. Generate vektor $h \in \mathbb{F}_2^n$ dengan bobot kecil secara acak.
b. Baris ke-i dari H sama dengan $\sigma^{i-1}(h)$, untuk setiap $i = 2,3, \dots, m_k$.

Perlu dicatat, dengan menggunakan algoritma 1, diperoleh suatu kode LDPC (n, m_k). Terdapat proposisi untuk memperoleh matriks *parity check* dan matriks pembangun dari kode kuasi siklik diperumum-LDPC.

Proposisi 1 *Diberikan $\sigma = \sigma_1\sigma_2 \dots \sigma_k$, dimana length$(\sigma_i) = m_i$, $\forall i = 1, 2, \dots, k-1$ dan length$(m_k) = m_k = r$.*

(a) *Jika C adalah suatu LDPC $[n, r]$, maka matriks parity check H dapat ditulis seperti berikut :*

$$H = [H_1|H_2| \dots |H_k], \qquad (i)$$

dimana $H_i \in \mathbb{F}_2^{r\times m_i}$ adalah matriks sirkulan,$\forall i = 1,2, \dots, k$.

(b) *Jika H_k tak singular, maka*

$$G = \left[I_{n-r} \middle| \begin{matrix} B_1 \\ \vdots \\ B_j \end{matrix}\right], \qquad (ii)$$

dimana $B_j = \left(H_k^{-1}H_j\right)^T$, $\forall j = 1,2, \dots, k-1$.

Bukti Diberikan vektor h merupakan baris pertama dari matriks H. Berdasarkan *output* dari algoritma 1 dengan *input* h, maka diperoleh persamaan (i). Selanjutnya, dikarenakan setiap baris dari G merupakan suatu elemen di kernel H, maka didapatkan persamaan (ii) ■

Terdapat beberapa algoritma dekoding LDPC yang ada untuk mengoreksi kesalahan pada suatu data atau pesan, yaitu *Log-Likelihood Ratio Sum-Product Algorithm* (LLR-SPA).
Langkah-langkah algoritmanya sebagai berikut.

a. Inisialisasi
semua posisi yang terhubung dengan *node* ke-i dan *node* ke-k, didapatkan,

$$\Gamma_{i\to k}(x_i) = LLR(x_i),$$
$$\Lambda_{k\to i}(x_i) = 0.$$

Dimana $LLR(x_i) = ln\left[\frac{P(x_i=0|y_i=y)}{P(x_i=1|y_i=y)}\right]$, dimana $P(x_i = x|y_i = y), x \in \{0,1\}$ adalah probabilitas *codeword* bit x_i pada posisi ke-i sama dengan x, dengan pesan diterima $y_i = y$ pada *output channel*. $LLR(x_i)$ adalah *log-likelihood ratio* yang terhubung dengan *codeword* bit pada posisi i.

b. Left-Semi Iteration
untuk setiap *node* ke-k yang terhubung dengan *node* ke-i dan $j \in A(k)\backslash i$, didapatkan,

$$\Lambda_{k\to i}(x_i) = 2\cdot\tanh^{-1}\left\{\prod_{j\in A(k)\backslash i} tanh\left[\frac{1}{2}\Gamma_{i\to k}(x_j)\right]\right\}$$

c. Right-Semi Iteration
untuk setiap *node* ke-i yang terhubung dengan *node* ke-k dan $j \in B(i)\backslash k$, didapatkan,

$$\Gamma_{i\to k}(x_i) = LLR(x_i) + \sum_{j\in B(i)\backslash k}\Lambda_{j\to i}(x_i)\ , dan$$
$$\Gamma_i(x_i) = LLR(x_i) + \sum_{j\in B(i)}\Lambda_{j\to i}(x_i)$$

d. *Decision*
Hasil yang diperoleh dari *decision* digunakan untuk estimasi nilai $\hat{x}_i = (\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n)$ dengan syarat,

$$\hat{x}_i = \begin{cases} 0, jika\ \Gamma_i(x_i) \geq 0, \\ 1, jika\ \Gamma_i(x_i) < 0. \end{cases}$$

dimana $\hat{x}_i$ adalah pesan hasil koreksi menggunakan algoritma LLR-SPA. Jika $H\hat{x} = 0$, maka proses algoritmanya selesai. Jika $H\hat{x} \neq 0$, maka proses algoritma diulang dari *point b*. Proses ini akan terus berlanjut sampai kriteria terpenuhi, jika kriteria tidak terpenuhi sampai iterasi maksimum, maka hasil terakhir dari iterasi dijadikan sebagai hasilnya.

3. Hasil dan Pembahasan

Misalkan diambil rasio maksimum kesalahan yang dimasukkan sebesar 0,01 dan 0,05, maka hasil BER

dengan masing-masing panjang kode dapat dilihat pada tabel di bawah ini.

Tabel 1. Rasio maksimum jumlah kesalahan yang dimasukkan sebesar 0,01

Panjang Kode	Maksimum Kesalahan yang dimasukkan	Rasio Kesalahan	Rasio Rata-rata Kesalahan
150	2	0,013	0,0125
250	1	0,004	
350	4	0,011	
450	10	0,022	

Tabel 2. Rasio maksimum jumlah kesalahan yang dimasukkan sebesar 0,05

Panjang Kode	Maksimum Kesalahan yang dimasukkan	Rasio Kesalahan	Rasio Rata-rata Kesalahan
150	8	0,053	0,041
250	10	0,04	
350	15	0,043	
450	13	0,029	

Tabel di atas menunjukan kemampuan koreksi kesalahan kode kuasi siklik diperumum-LDPC pada channel biner simetris. Berdasarkan beberapa percobaan yang dilakukan diperoleh rasio rata-rata kesalahan dengan maksimum jumlah kesalahan yang dimasukkan sebesar 0,01 sebanyak 0,0125, dan maksimum jumlah kesalahan yang dimasukkan sebesar 0,05 sebanyak 0,041. Selain itu, semakin besar maksimum jumlah kesalahan yang diambil, maka hasil rasio rata-rata kesalahan juga besar.

4. Kesimpulan

Berdasarkan hasil yang diperoleh dari beberapa percobaan, hal ini menunjukan bahwa semakin besar jumlah kesalahan yang dimasukkan mengakibatkan peluang pesan yang diterima secara utuh menjadi kecil.

DAFTAR PUSTAKA

[1]. Anton, H., & Rorres, C. (2005). *Elementary Linear Algebra – 9th Edition*. John Willey and Sons, Inc, New York.

[2]. Baldi, M. (2014). *QC-LDPC Code-Based Cryptography*. University Politecnica delle Marche, Ancona.

[3]. Baldi, M., & Chiaraluce, F. (2007). *Quasy-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem*. University Politecnica delle Marche, Ancona.

[4]. Bhavsar, N.P., & Vala, B. (2014). *Design of Hard and Soft Decision Decoding Algorithms of LDPC*. International Journal of Computer Applications (0975–8887) Vol. 90 – No. 16. Computer Engineering Department, Parul Institute of Engineering & Technology, Limda, Waghodiya, Vadodara

[5]. Gallager, R.G. (1963). *Low-Density Parity-Check Codes*. Cambridge, MIT Press.

[6]. Hu, Xiao-Yu, dkk. (2001). *Efficient Implementations of the Sum-Product Algorithm for Decoding LDPC Codes*. IBM Research, Zurich Reseach Laboratory, Switzerland.

[7]. Irwansyah, Muchtadi-Alamsyah, I., & Yuliawan, F. (2018). *Permutation LDPC Codes in McEliece Cryptosystem*. Universitas Mataram, Mataram.

[8]. Jacob, B. (1990). *Linear Algebra*. University of Washington, New York.

[9]. Ling, S., & Xing, C. (2004). *Coding Theory a First Course*. Cambridge University Press, New York.

[10]. Nasution A.S., dkk. (2011). *Penggunaan Teknik Pengkodean Low Density Parity Check pada Data Satelit Penginderaan Jauh*. STT Telkom Bandung, Bandung.

[11]. Skjaerbaek, T.H. (2010). *Quasi-Cyclic Codes*. Aalborg University. Department of Mathematical Sciences.

[12]. Vanstone, S.A., & Oorschot, P.C. (1989). *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, London.

[13]. Vasic, B., dkk. (2014). *Failures and Error Floors of Iterative Decoders*. Department of Electrical and Computer Engineering, University of Arizona, Tucson.