Fraktal: Jurnal Matematika dan Pendidikan Matematika
Volume 4, No. 2, November 2023, Hal. 21-26 (e-ISSN 2776-0073)
Available online at http://ejurnal.undana.ac.id/fraktal

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

Muhammad Sukriadi

Prodi Matematika, FMIPA Universitas Mataram
Email: sukri.maret97@gmail.com

Diterima (23 Agustus 2023); Revisi (17 November 2023); Diterbitkan (30 November 2023)

Abstrak

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* 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.

Abstract

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.*

PENDAHULUAN

Teknologi merupakan alat atau mesin yang diciptakan untuk mempermudah manusia dalam menyelesaikan berbagai macam masalah yang terdapat di dunia. 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 (Baldi, 2014; Nasution 2011)).

Salah satu cara untuk menjamin integritas data dalam komunikasi adalah dengan menggunakan pengkodean data transmisi. Cara ini pertama kali dikemukakan oleh Claude E. Shannon pada tahun 1948 dalam papernya yang berjudul "*A Mathematical Theory of Communication*" (Alamsyah, 2021; Ling 2004). Pengkodean menjadi sangat penting karena saluran komunikasi sering mengalami gangguan, seperti cuaca, kekuatan sinyal, kerusakan perangkat komunikasi, dan sebagainya (Bhavsar, 2014; Skjaerbaek 2010).

Salah satu jenis kode yang dapat digunakan dengan tujuan ini adalah kode *Low Density Parity Check* (LDPC). Kode LDPC dapat dibuat menjadi efisien secara kompleksitas memori dengan cara melakukan hybrid dengan kode kuasi siklik diperumum (Irwansyah, 2018; Irwansyah, 2019). Secara umum, kode LDPC menggunakan algoritma penyampaian pesan (*beliefe propagation*) untuk decoding (Hidayat, 2022; Hu, 2001). Algoritma ini didasarkan pada graf Tanner yang sesuai dari matriks *parity check* $\boldsymbol{H}$. Salah satu algoritma yang termasuk dalam algoritma penyampaian pesan adalah *Log-Likelihood Ratio Sum-Product Algorithm* (LLR-SPA) yang merupakan algoritma *soft decoding* (Ling, 2004; Mucthadi 2022).

Definisi 1 (Vanstone, 1898)) 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* $\boldsymbol{H}$ yang bobot barisnya kecil $\in \mathbb{F}_2^{(n-k)\times n}$.

Terdapat cara yang cukup mudah untuk mengkonstruksi kode kuasi siklik diperumum-LDPC, berikut diberikan algoritmanya.

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, dimana h adalah baris pertama $\boldsymbol{H}$.

b. Baris ke-i dari $\boldsymbol{H}$ sama dengan $\sigma^{i-1}(h)$, untuk setiap $i = 2,3, \dots, m_k$.

Terdapat proposisi untuk menemukan matriks parity check H dan matriks pembangun G, berikut proposisinya.

Proposisi 1 (Muchtadi, 2019) 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.

$$\boldsymbol{H} = [\boldsymbol{H_1}|\boldsymbol{H_2}| \dots |\boldsymbol{H_k}], \qquad \cdots \quad (i)$$

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

(b) Jika $\boldsymbol{H_k}$ tak singular, maka

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

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

Bukti. Diberikan vektor h merupakan baris pertama dari matriks $\boldsymbol{H}$. Berdasarkan *output* dari algoritma 1.1 dengan *input* h, maka diperoleh persamaan (i). Selanjutnya, dikarenakan setiap baris dari $\boldsymbol{G}$ merupakan suatu elemen di kernel $\boldsymbol{H}$, maka didapatkan persamaan (ii) ■

Algoritma LLR-SPA

Berikut langkah-langkah algoritmanya untuk mengoreksi kesalahan:

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*

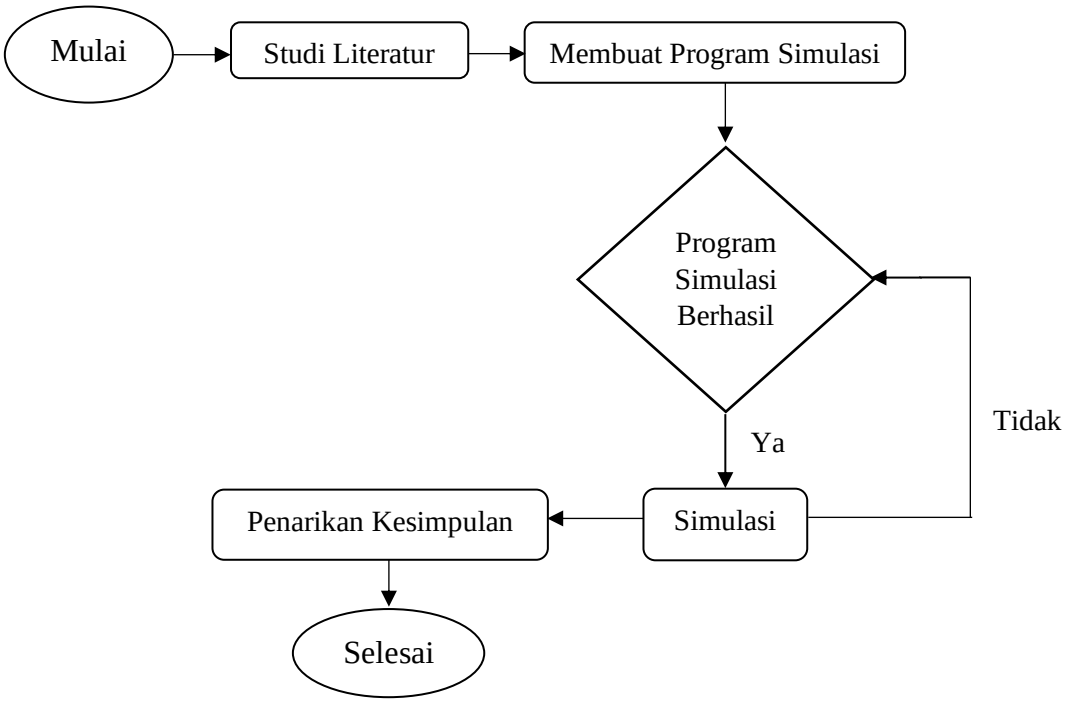
Hasil yang diperoleh dari persamaan (3.7.5) digunakan untuk estimasi nilai $\hat{x}_i = (\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n)$ dengan syarat,

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

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.

METODE

Penelitian ini termasuk dalam penelitian kuantitatif, dimana kode kuasi siklik diperumum-LDPC menjadi subjek peneliti. Data yang diperoleh dengan menggunakan metode koding *software Python*. Hasil yang diperoleh dari software akan dianalisis berdasarkan teori dan definisi yang digunakan dalam penelitian. Berikut deskripsi gambar metode penelitian.



Gambar 1. Langkah Penelitian

HASIL DAN PEMBAHASAN

Berikut tabel maksimum jumlah kesalahan yang bisa dimasukkan untuk masing-masing panjang kode, jika diambil rasio maksimum kesalahan yang dimasukkan sebesar 0,01 dan 0,05.

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	

Berdasatrkan Tabel 1 dan Tabel 2 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, hal ini menunjukkan bahwa semakin besar maksimum jumlah kesalahan yang diambil, maka hasil rasio rata-rata kesalahan juga besar.

KESIMPULAN

Bedasarkan hasil diperoleh, dapat disimpulkan bahwa semakin besar jumlah kesalahan yang dimasukkan mengakibatkan peluang pesan yang diterima secara utuh menjadi kecil.

DAFTAR PUSTAKA

Alamsyah, I. M., & Yuliawan, F. (2021). A construction of MDS involutory matrices using MDS self-dual codes: a preliminary result. In *Journal of Physics: Conference Series* (Vol. 1722, No. 1, p. 012030). IOP Publishing.

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

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

Bhavsar, N.P., & Vala, B. (2014). Design of Hard and Soft Decision Decoding Algorithms of LDPC. *International Journal of Computer Applications* (0975-8887), 90(16), 10-15. Vadodara: Parul Institute of Engineering & Technology.

Hidayat, M. I., Irwansyah, I., & Wardhana, I. (2022, December). A construction of generalized quasi-cyclic codes over finite field using gray map. In *AIP Conference Proceedings* (Vol. 2641, No. 1). AIP Publishing.

Hu, Xiao-Yu, Eleftheriou, E., Arnold, Dieter–Michael, & Dholakia, A. (2001). Efficient Implementations of the Sum-Product Algorithm for Decoding LDPC Codes. *Global Telecommunications Conference*, 2(1), 1036-1036E. Switzerland: IBM Research, Zurich Reseach Laboratory.

Irwansyah, Muchtadi-Alamsyah, I., & Yuliawan, F. (2018). Permutation LDPC Codes in McEliece Cryptosystem. *Proceedings Of the 8th SEAMS-UGM Intenational Conference On Mathematics and Its Applications*, 1-6. Mataram: Universitas Mataram.

Irwansyah, Muchtadi-Alamsyah, I., & Yuliawan, F. (2019, December). Permutation LDPC codes in McEliece cryptosystem. In *AIP Conference Proceedings* (Vol. 2192, No. 1, p. 040005). AIP Publishing LLC.

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

Muchtadi-Alamsyah, I., Irwansyah, & Barra, A. (2022). Generalized Quasi-Cyclic Codes with Arbitrary Block Lengths. *Bulletin of the Malaysian Mathematical Sciences Society*, 45(3), 1383-1407.

Muchtadi-Alamsyah, I., & Irwansyah, I. (2019, December). Asymmetric quantum codes from skew cyclic codes over B1. In *AIP Conference Proceedings* (Vol. 2192, No. 1). AIP Publishing.

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

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

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