JURNAL FOURIER | Oktober 2020, Vol. 9, No. 2, 49-58 ISSN 2252-763X
DOI: 10.14421/fourier.2020.92.49-58 E-ISSN 2541-5239

Kode Linear untuk Deteksi dan Koreksi Kesalahan Penulisan dalam Huruf Hijaiyah

Muhamad Zaki Riyanto

Program Studi Matematika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga, Jl. Marsda Adisucipto No. 1 Yogyakarta, Indonesia.

Korespondensi; Muhamad Zaki Riyanto, Email: zaki.riyanto@uin-suka.ac.id

Abstrak

Huruf hijaiyah memainkan peran yang sangat penting dalam dunia Islam, salah satu alasannya karena Al-Qur'an ditulis dalam huruf Arab yang menggunakan huruf hijaiyah. Perkembangan teknologi memudahkan setiap orang untuk menulis dan menyebarkan ayat-ayat Al-Qur'an dalam berbagai media elektronik. Pada beberapa kasus, dijumpai kesalahan penulisan yang dapat merubah arti dan makna dari suatu ayat. Di dalam ilmu aljabar, dikenal teori pengkodean yang mempelajari bagaimana suatu pesan itu dikodekan, sehingga memiliki kemampuan deteksi dan koreksi kesalahan yang terjadi. Salah satu jenis kode yang sering digunakan adalah kode linear yang dikonstruksi melalui sebuah subruang dari suatu ruang vektor atas lapangan hingga. Kode linear dapat diterapkan untuk deteksi dan koreksi kesalahan penulisan pesan dalam huruf hijaiyah. Oleh karena itu, perlu dikaji cara mengkonstruksi korespondensi huruf hijaiyah agar dapat dikodekan menggunakan kode linear, juga perlu diketahui jenis kesalahan seperti apa yang dapat dideteksi dan dikoreksi menggunakan kode linear, dan terakhir adalah bagaimana cara mendeteksi dan mengkoreksi kesalahan penulisan dalam huruf hijaiyah menggunakan kode linear. Dalam penelitian ini, lapangan hingga yang digunakan adalah lapangan biner. Oleh karena itu, setiap huruf hijaiyah harus dikorespondensikan dengan ekspansi biner sesuai dengan urutan hurufnya dengan panjang 5 bit. Kode linear yang digunakan adalah kode Hamming berorder 3 atas lapangan biner, dengan matriks generator berupa matriks biner berukuran 4x7, dan matriks cek paritas berupa sebuah matriks biner berukuran 3x7. Matriks generator digunakan untuk mengkodekan, sedangkan matriks cek paritas digunakan untuk mendeteksi dan mengkoreksi kesalahan. Jenis kesalahan penulisan yang dapat dideteksi dan dikoreksi adalah dalam setiap blok pesan yang terdiri dari 4 huruf hijaiyah hanya boleh ada 1 huruf yang berubah menjadi huruf hijaiyah yang lainnya. Konsekuensi dari adanya pengkodean ini adalah bertambahnya panjang setiap blok pesan, dari yang semula memiliki panjang 20 bit, setelah dikodekan menjadi 35 bit, atau terjadi penambahan cek bit sebesar 15 bit.

Kata Kunci: kode linear; huruf hijaiyah; lapangan hingga; ruang vektor; teori pengkodean.

Abstract

Hijaiyah letters play a very important role in the Islamic world, one of the reasons is because the Qur'an is written in Arabic letters using hijaiyah letters. The development of technology makes it easy for everyone to write and spread the verses of the Qur'an in various electronic media. In some cases, writing errors are found that can change the meaning of a verse. In algebra, we have the coding theory that studies how a message is coded, so it has the ability to detect and correct errors that occur. One type of code that is often used is linear code which is constructed using a subspace of a vector space over a finite field. Linear code can be applied for the detection and correction of writing errors in hijaiyah letters. It is necessary to study how to construct hijaiyah correspondence so that it can be encoded using linear code, we also need to know what types of errors can be detected and corrected using linear code, and finally how to detect and correct writing errors in hijaiyah letters using linear code. In this research, the binary field is used. Therefore, each hijaiyah letter must be corresponded with a binary expansion according to the order of the letters with a length of 5 bits. The linear code used is the order 3 Hamming code on the binary field, with the generator matrix is a 4x7 binary matrix, and the parity check matrix is a 3x7 binary matrix. The generator matrix is used to encode, while the parity check matrix is used to detect and correct errors. The type of writing error that can be detected and corrected is that in each block of messages consisting of 4 hijaiyah letters there can only be 1 letter that changes to another hijaiyah letter. The consequence of this encoding is that the length of each message block increases, from what was originally 20 bits long, after it has been coded to 35 bits, or an additional check bit by 15 bits occurs.

Keywords: linear code; hijaiyah letters; finite field; vector space; coding theory.

Pendahuluan

Al-Quran merupakan pegangan hidup dari setiap muslim untuk mengarungi kehidupan sampai di hari kiamat. Al-Quran diturunkan oleh Allah S.W.T. melalui malaikat Jibril kepada Nabi Muhammad s.a.w. untuk umat manusia. Di dalamnya terdapat berbagai perintah, larangan, kisah dan hal-hal lainnya yang menakjubkan. Al-Quran senantiasa dijaga keasliannya oleh Allah sebagai salah satu bukti kebenaran dan kemukjizatannya. Salah satu cara Allah s.w.t menjaga keaslian Al-Quran adalah dengan membuatnya mudah dihafalkan bahkan oleh orang yang bahasa ibunya bukan bahasa arab. Hingga kini telah ada banyak orang yang mampu menghafalkan Al-Quran. Allah berfirman dalam Surat Al-Qomar ayat 17:

وَلَقَدْ يَسَّرْنَا الْقُرْاٰنَ لِلذِّكْرِ فَهَلْ مِنْ مُّدَّكِرٍ ۝٢٢

yang artinya: "Dan sesungguhnya Kami mudahkan al-Quran untuk pelajaran, maka adalah orang yang mau mengambil pelajaran." (Qs. Al-Qomar: 17).

Perkembangan teknologi dapat memudahkan penulisan Al-Quran dalam berbagai media cetak dan elektronik. Akan tetapi, tidak ada hal yang sempurna di dunia ini, manusia dapat melakukan kesalahan, baik itu disengaja maupun tidak disengaja. Tak terkecuali dalam penulisan ayat Al-Quran. Tak jarang dijumpai kasus kesalahan penulisan ayat Al-Quran, seperti pada kasus kesalahan penulisan oleh seseorang yang ditayangkan di sebuah televisi swasta nasional. Kasus lain tentang kesalahan penulisan ayat Al-Quran juga ditemui pada beberapa buku Pendidikan Agama Islam (Republika, 29 Oktober 2017). Salah satu cara untuk menyelesaikan tersebut adalah melakukan pengkodean huruf hijaiyah yang digunakan dalam penulisan ayat menggunakan teori pengkodean. Teori pengkodean bermula dari penelitian Shannon (1948). Oleh Shannon dijelaskan konsep awal tentang teori pengkodean untuk pendeteksian adanya kesalahan dan kemungkinan dalam melakukan koreksinya. Hingga saat ini, teori pengkodean telah berkembang pesat, sehingga memunculkan berbagai jenis kode, salah satunya adalah kode linear (Jurgen Bierbrauer, 2016).

Teknik pengkodean huruf hijaiyah telah dilakukan oleh Yahya Alqahtani dkk (2013), dilanjutkan oleh Prakash Kuppuswamy dan Yahya Alqahtani (2014) untuk enkripsi pesan rahasia dalam huruh hijaiyah. Perkembangan pengkodean huruf hijaiyah terus dilakukan oleh Ameer Kadhim Hadi (2017) untuk pengamanan pesan rahasia. Akan tetapi, dari penelitian-penelitian tersebut belum menyinggung tentang pengkodean untuk kepentingan deteksi dan koreksi kesalahan penulisan teks menggunakan huruf hijaiyah. Dalam penelitian ini, adanya kesalahan dalam penulisan dalam huruf hijaiyah akan dideteksi dan dikoreksi menggunakan kode linear, proses perhitungannya dilakukan pada suatu subruang dari ruang vektor yang dikonstruksi melalui sebuah matriks tertentu. Oleh karena itu, perlu dikonstruksi suatu korespondensi antara huruf hijaiyah dengan vektor. Dalam penelitian ini akan dikaji korespondensi huruf hijaiyah kode linear untuk pengkodean huruf hijaiyah, jenis kesalahan penulisan dalam huruf hijaiyah yang dapat dikoreksi menggunakan kode linear, serta cara mendeteksi dan mengkoreksi adanya kesalahan penulisan dalam huruf hijaiyah yang telah dikodekan menggunakan kode linear.

Kode Linear

Definisi 2.1. (Jurgen Bierbrauer, 2016) *Diberikan F adalah suatu lapangan dan $n \in N$, dibentuk $V_n(F)$ ruang vektor atas F. Suatu* ***(n,k)-kode linear*** *C atas F adalah subruang dari $V_n(F)$ yang berdimensi k.*

Berdasarkan hasil penelitian San Ling dan Caophing Xing (2004), proses pembentukan suatu (n,k) −kode linear C atas lapangan F dapat ditentukan melalui pemilihan basis untuk C yang disusun dalam sebuah matriks G, matriks tersebut dinamakan dengan matriks generator. Diberikan $B = \{v_1, v_2, \dots v_k,\} \subseteq V_n(F)$ basis untuk C berdimensi k, misalkan $v_1 = (a_{11}a_{12} \dots a_{1n}), v_2 = (a_{21}a_{22} \dots a_{2n}), \dots, v_k = (a_{k1}a_{k2} \dots a_{kn})$. Dibentuk matriks generator dari C yaitu

$$G=\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}.$$

Untuk melakukan pengkodean pada teks pesan yang telah dirubah sebagai elemen dari ruang vektor $V_k \in F$ yaitu $M=(m_1,m_2,\ldots,m_k)\in V_k(F)$, proses pengkodeannya adalah

$$MG=\left(m_1,m_2,\ldots,m_k\right)\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}=\left(x_1,x_2,\ldots,x_n\right),$$

dan vektor $c=(x_1,x_2,\ldots,x_n)$ disebut dengan katakode *(codeword)* dari M setelah dikodekan menggunakan kode linear dengan matriks G sebagai matriks generatornya (Vanstone dan Oorschot, 1989). Matriks generator disebut dalam bentuk standar apabila $G=[I_k A]$ dengan I_k adalah matriks identitas berorde k dan A adalah suatu matriks berukuran $k\times(n-k)$.

Definisi 2.2. (Vanstone dan Oorschot, 1989) *Diberikan F adalah suatu lapangan dan $x,y\in V_n(F)$. **Jarak Hamming** dari x dan y, dinotasikan dengan $d(x,y)$ didefinisikan sebagai banyaknya posisi koordinat yang berbeda dari x dan y. Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. **Jarak Hamming dari C** dinotasikan dengan $d(C)$, didefinisikan sebagai $d(C)=min\{d(x,y):x,y\in C,x\neq y\}$.*

Berkaitan dengan konsep deteksi dan koreksi adanya kesalahan, yang dimaksud dengan error atau kesalahan adalah apabila vektor yang dikirimkan yaitu $x=(x_1,x_2,\ldots,x_n)$ mengalami perubahan menjadi vektor lain. Dengan demikian, kesalahan yang terjadi adalah adanya beberapa x_i yang nilainya berubah.

Teorema 2.3. (Vanstone dan Oorschot, 1989*) Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Jika C memiliki jarak Hamming $d(C)=d$, maka C memiliki kemampuan untuk mendeteksi $d-1$ kesalahan, serta mampu mengkoreksi $\left[\frac{d-1}{2}\right]$ kesalahan.*

Definisi 2.4. (Vanstone dan Oorschot, 1989) *Diberikan F adalah lapangan.*

(1) *Bobot Hamming dari $x\in V_n(F)$ dinotasikan dengan $w(x)$, didefinisikan sebagai banyaknya koordinat tak nol dari x.*

(2) *Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Bobot Hamming dari C dinotasikan dengan $w(C)$, didefinisikan sebagai $w(C)=min\{w(x):x\in V_n(F),x\neq 0\}$.*

Teorema 2.5. (Vanstone dan Oorschot, 1989) *Diberikan C adalah suatu (n,k)-kode linear atas lapangan F, maka $w(C)=d(C)$.*

Definisi 2.6. (Vanstone dan Oorschot, 1989) *Diberikan F adalah lapangan dan vektor-vektor $x=(x_1,x_2,\ldots,x_n),y=(y_1,y_2,\ldots,y_n)\in V_n(F)$. **Hasil kali dalam** (Euclid) dari x dan y didefinisikan sebagai $\langle x,y\rangle=\sum_{i=1}^{n}x_iy_i$. Vektor x dan y dikatakan tegak lurus (ortogonal) apabila $\langle x,y\rangle=0$. Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Komplemen tegak lurus dari C dinotasikan dengan $C^{\perp}$ dan didefinisikan sebagai $C^{\perp}=\{x\in V_n(F):\langle x,y\rangle=0,\forall y\in C\}$.*

Teorema 2.7. (Vanstone dan Oorschot, 1989) *Diberikan C suatu (n,k)-kode linear atas lapangan F, maka $C^{\perp}$ suatu $(n,n-k)$-kode linear atas F. Lebih lanjut, jika $G=[I_k A]$ adalah matriks generator untuk C, maka $H=[-A^T I_{n-k}]$ adalah matriks generator untuk $C^{\perp}$. Selanjutnya, matriks H tersebut dinamakan dengan* ***matriks cek paritas*** *untuk C.*

Diberikan C adalah (n,k)-kode linear atas F dengan matriks generator $G=[I_k A]$. Diberikan pesan yang akan dikodekan yaitu $m=(m_1,m_2,\dots,m_k)\in V_k(F)$. Menggunakan matriks generator G diperoleh pesan yang telah dikodekan berupa katakode $c=mG=m=(m_1 m_2 \dots m_k x_1 x_2 \dots x_{n-k})\in V_n(F)$. Penambahan vector $(x_1 x_2 \dots x_{n-k})$ pada m disebut dengan cek simbol. Pada kasus lapangan biner, maka penambahan vektor tersebut dinamakan dengan cek bit. Dikarenakan G adalah matriks generator untuk C, dan H adalah matriks generator untuk $C^{\perp}$, maka untuk setiap $x\in C$ pasti memenuhi $Hx^T=0$, dengan 0 yang dimaksud adalah vektor nol dalam bentuk kolom. Dengan demikian, dapat disimpulkan bahwa kata kode c tidak terdeteksi error jika dan hanya jika $Hc^T=0$, dan terdeteksi error jika dan hanya jika $Hc^T\neq 0$.

$$Hx^T=\begin{pmatrix}1&0&1&0&0&0\\0&1&0&1&0&0\\1&0&0&0&1&0\\0&1&0&0&0&1\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}\neq\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

Dapat dilihat bahwa $Hx^T\neq 0$, sehingga $x\notin C$, yaitu terdeteksi adanya kesalahan.

Teorema 2.8. (Vanstone dan Oorschot, 1989) *Diberikan H adalah matriks cek paritas untuk (n,k)-kode linear C atas F, maka setiap himpunan yang terdiri dari $s-1$ kolom dari H adalah himpunan bebas linear jika dan hanya jika C memiliki jarak Hamming paling sedikit adalah s.*

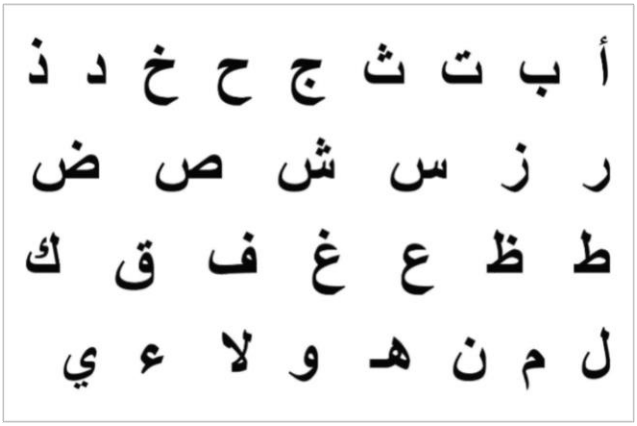
Teorema 2.8. di atas dapat digunakan untuk mengkonstruksi sebuah kode yang dapat mengkoreksi 1 kesalahan (*single error correcting code*). Caranya adalah dengan mengkonstruksi matriks cek paritas H sedemikian hingga tidak ada sebanyak 2 atau lebih kolom-kolomnya yang tidak bebas linear, yaitu ada kolom yang merupakan kombinasi dari kolom-kolom yang lainnya.

Definisi 2.9. (Vanstone dan Oorschot, 1989*) Suatu* ***kode Hamming*** *berorder r atas lapangan F dengan $|F|=q$ adalah suatu (n,k)-kode linea C atas F dengan $n=\frac{q^r-1}{q-1}$ dan $k=n-r$. Matriks cek paritasnya adalah matriks H_r berukuran $r\times n$ sedemikian hingga kolom-kolom dari H_r tidak nol dan tidak ada dua kolom yang merupakan hasil kali skalar satu sama lain.*

Berdasarkan konstruksi kode Hamming di atas, dapat dilihat dengan jelas bahwa kode Hamming memiliki jarak Hamming 3, sehingga memiliki kemampuan mendeteksi 2 kesalahan, serta mampu mengkoreksi 1 kesalahan. Oleh karena itu, kode Hamming adalah sebuah *single error correcting code*.

Pengkodean Huruf Hijaiyah

Perkembangan pengkodean huruf hijaiyah kemudian dilakukan oleh Ameer Kadhim Hadi (2017) dalam penelitiannya untuk pengamanan pesan singkat SMS. Dikarenakan dalam al-Quran tidak memuat angka dalam ayatnya, maka peneliti tidak memasukkan angka sebagai bagian dari huruf hijaiyah yang digunakan, sehingga diperoleh sebanyak 30 huruf hijaiyah, seperti diberikan dalam gambar di bawah ini.



Gambar 1. Huruf Hijaiyah (30 huruf).

Metode korespondensi yang sederhana dan melibatkan struktur aljabar yang telah dijelaskan dalam konsep grup dan ring, maka dapat digunakan himpunan semua bilangan bulat modulo $\mathbb{Z}_{30} = \{0,1,2,\dots,29\}$ dengan korespondensinya adalah huruf "alif" dikorespondensikan dengan 0, huruf "ba" dikorespondensikan dengan 1, begitu seterusnya sampai dengan huruf "ya" yang dikorespondensikan dengan 29. Himpunan $\mathbb{Z}_{30}$ memiliki struktur aljabar berupa ring komutatif dengan elemen satuan, tetapi bukan lapangan, sebab 30 bukan bilangan prima. Oleh karena itu, tidak dapat digunakan untuk mengkonstruksi kode linear yang syarat utamanya adalah penggunaan struktur aljabar berupa lapangan. Oleh karena itu, peneliti mengusulkan penggunakan himpunan $\mathbb{Z}_{31} = \{0,1,2,\dots,30\}$ dengan 31 adalah bilangan prima, hal ini dilakukan untuk mengakomodir syarat sebagai lapangan. Korespondensi yang terbentuk adalah huruf "alif" dikorespondensikan dengan 1, huruf "ba" dikorespondensikan dengan 2, begitu seterusnya sampai dengan huruf "ya" yang dikorespondensikan dengan 30.

Misalkan digunakan lapangan hingga $\mathbb{Z}_{31} = \{0,1,2,\dots,30\}$. Apabila digunakan kode Hamming dengan order 2 saja, maka diperoleh $n = 32$ dan $k = 30$, diperoleh matriks generator yang cukup besar, memiliki ukuran 30x32 dengan entri dari himpunan $\mathbb{Z}_{31}$. Apabila digunakan kode Hamming dengan order 3, maka diperoleh $n = 993$ dan $k = 990$, sebuah matriks generator yang sangat besar karena memiliki ukuran 990x993. Oleh karena itu, diperlukan teknik korespondensi yang dapat menghasilkan matriks yang lebih kecil sehingga proses perhitungan pengkodean dapat berjalan lebih efisien.

Teknik korespondensi satu-satu yang digunakan untuk mengatasi masalah matriks generator yang besar adalah dengan melakukan ekspansi biner dari semua bilangan yang termuat dalam lapangan $\mathbb{Z}_{31}$, yaitu dengan cara menuliskan masing-masing bilangan sebagai vektor biner basis 2. Sebagai contohnya, bilangan 10 dapat dituliskan sebagai 10 = 8 + 2 atau 10 = 1.8 + 0.4 + 1.2 + 0.1, sehingga bilangan 10 berkorespondensi dengan vektor biner (1010). Bilangan terbesar yang mungkin adalah 30, diperoleh 30 = 1.16 + 1.8 + 1.4 + 1.2 + 0.1, sehingga 30 berkorespondensi dengan vektor biner (11110) yang memiliki panjang 5. Dengan demikian, masing-masing huruf hijaiyah dikodekan menjadi vektor biner dengan panjang 5 atau lebih dikenal dengan 5-bit, seperti diberikan dalam tabel di bawah ini.

Tabel 1. Korespondensi huruf hijaiyah dan vektor biner.

أ	1	00001	ح	6	000110	ز	11	01011	ط	16	10000	ق	21	10101	هـ	26	11010
ب	2	00010	خ	7	000111	س	12	01100	ظ	17	10001	ك	22	10110	و	27	11011
ت	3	00011	د	8	01000	ش	13	01101	ع	18	10010	ل	23	10111	لا	28	11100
ث	4	00100	ذ	9	01001	ص	14	01110	غ	19	10011	م	24	11000	ء	29	11101
ج	5	00101	ر	10	01010	ض	15	01111	ف	20	10100	ن	25	11001	ي	30	11110

Berdasarkan korespondensi yang telah diberikan pada Tabel 1. di atas, maka kode linear yang digunakan didefinisikan atas lapangan biner $\mathbb{Z}_2$. Setiap huruf hijaiyah dinyatakan sebagai vektor biner 5 bit, sehingga himpunan semua pesan awal yang belum dikodekan adalah $V_5(\mathbb{Z}_2) = \{(x_1x_2x_3x_4x_5): x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}_2\}$. Apabila diasumsikan terjadi satu kesalahan, yaitu satu huruf berubah menjadi huruf yang lain, maka artinya terdapat terjadi paling banyak 5 kesalahan. Apabila digunakan kode Hamming atas lapangan biner, maka harus dikonstruksi kode linear dengan jarak Hammingnya adalah 11. Oleh karena itu, matriks generator yang dikonstruksi masih sangat besar.

Untuk dapat menyiasati penggunaan kode Hamming yang memiliki kemampuan koreksi hanya 1 kesalahan saja, untuk dapat digunakan dalam mengkoreksi kelasahan 1 huruf hijaiyah, diasumsikan bahwa dapat terjadi perubahan satu huruf menjadi huruf lain dalam setiap blok yang terdiri dari 4 huruf. Misalkan dalam setiap blok terdiri dari 4 huruf, yaitu:

Huruf ke-1: $(a_1b_1c_1d_1e_1) \in V_5(\mathbb{Z}_2)$, Huruf ke-2: $(a_2b_2c_2d_2e_2) \in V_5(\mathbb{Z}_2)$

Huruf ke-3: $(a_3b_3c_3d_3e_3) \in V_5(\mathbb{Z}_2)$, Huruf ke-4: $(a_4b_4c_4d_4e_4) \in V_5(\mathbb{Z}_2)$

Selanjutnya, dibentuk vektor-vektor sebagai berikut:

$a = (a_1a_2a_3a_4) \in V_4(\mathbb{Z}_2)$ $b = (b_1b_2b_3b_4) \in V_4(\mathbb{Z}_2)$ $c = (c_1c_2c_3c_4) \in V_4(\mathbb{Z}_2)$

$d = (d_1d_2d_3d_4) \in V_4(\mathbb{Z}_2)$ $e = (e_1e_2e_3e_4) \in V_4(\mathbb{Z}_2)$

Dengan cara seperti ini, apabila terjadi satu kesalahan berupa berubahnya satu huruf menjadi huruf lain dalam setiap blok, maka artinya terjadi kesalahan dalam 1 bit pada setiap vektor a, b, c, d dan e. Oleh karena itu, dapat digunakan kode Hamming dengan order 3 atas lapangan biner $\mathbb{Z}_2$. Berdasarkan parameter yang disyaratkan dalam kode Hamming, dengan $q = |\mathbb{Z}_2| = 2$, maka diperoleh $n = \frac{2^3-1}{2-1} = 7$ dan $k = 7 - 3 = 4$. Selanjutnya, akan dikonstruksi sebuah (7,4)-kode linear atas $\mathbb{Z}_2$ dengan jarak Hamming 3.

Sebagai contohnya, dikonstruksi matriks cek paritas yang memenuhi ketentuan yang disyaratkan dalam kode Hamming, yaitu tidak memuat kolom nol, dan tidak ada sebuah kolom yang merupakan hasil kali skalar dari kolom yang lain, yaitu

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Apabila dinyatakan dalam bentuk standar, diperoleh $H = [-A^T I_3]$. Selanjutnya, ditentukan matriks generator dari C yaitu

$$G = [I_4 A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Diperoleh himpunan $C = \{a' = aG, b' = bG, c' = cG, d' = dG, e' = eG\}$ dan tabel berikut:

M	MG
$a = (a_1a_2a_3a_4)$	$a' = (a_1a_2a_3a_4a_5a_6a_7)$
$b = (b_1b_2b_3b_4)$	$b' = (b_1b_2b_3b_4b_5b_6b_7)$
$c = (c_1c_2c_3c_4)$	$c' = (c_1c_2c_3c_4c_5c_6c_7)$
$d = (d_1d_2d_3d_4)$	$d' = (d_1d_2d_3d_4d_5d_6d_7)$
$e = (e_1e_2e_3e_4)$	$e' = (e_1e_2e_3e_4e_5e_6e_7)$

Setelah itu, kata kode yang diperoleh disusun kembali, sehingga diperoleh 4 huruf pertama dan 15 bit tambahannya, yaitu:

Huruf ke-1: $(a_1b_1c_1d_1e_1)$ Huruf ke-2: $(a_2b_2c_2d_2e_2)$
Huruf ke-3: $(a_3b_3c_3d_3e_3)$ Huruf ke-4: $(a_4b_4c_4d_4e_4)$,
Cek bit ke-1: $(a_5b_5c_5d_5e_5)$ Cek bit ke-2: $(a_6b_6c_6d_6e_6)$, Cek bit ke-3: $(a_7b_7c_7d_7e_7)$

Masing-masing vektor di C memiliki panjang 7-bit, yaitu terjadi penambahan sebanyak 3 bit. Oleh karena itu, total penambahan bit dalam setiap blok adalah 15 bit, hal ini berarti dari 1 blok pesan yang memiliki panjang 20 bit menjadi 35 bit. Penambahan 15 bit tersebut dinamakan dengan cek bit.

Contoh 1. Misalkan akan dikodekan pesan dalam huruf hijaiyah sebagai berikut:

ي س ت م

Berdasarkan Tabel 1. di atas, diperoleh korespondensi antara huruf hijaiyah dan vektor biner sebegai berikut:

م	11000
ت	00011
س	01100
ي	11110

Berdasarkan konstruksi kode linearnya, diperoleh $a = (1001)$, $b = (1011)$, $c = (0011)$, $d = (0101)$ dan $e = (0100)$. Selanjutnya, dilakukan pengkodean dengan mengalikannya dengan matriks generator, diperoleh hasil pengkodean sebagai berikut:

M	MG
$a=(1001)$	$a'=(1001001)$
$b=(1011)$	$b'=(1011100)$
$c=(0011)$	$c'=(0011010)$
$d=(0101)$	$d'=(0101100)$
$e=(0100)$	$e'=(0100011)$

Pesan yang telah dikodekan adalah sebagai berikut:

ي س ت م

Cek bit: 01010 00101 10001

Apabila cek bit dapat ditulis dalam huruf hijaiyah sesuai dengan tabel, diperoleh pesan yang telah dikodekan sebagai berikut:

ظ ج ر ي س ت م

Deteksi dan Koreksi Kesalahan

Diberikan C adalah (n,k)-kode linear atas lapangan F. Misalkan H adalah matriks cek paritas untuk C. Diberikan katakode $c \in C$, apabila terjadi satu kesalahan maka ada satu koordinat yang nilainya berubah, misalkan $E \in V_n(F)$ adalah vektor kesalahan sedemikian hingga pesan yang telah mengalami

1 kesalahan adalah $x = c + E$. Apabila terjadi 1 kesalahan, maka E adalah vektor yang entrinya adalah 0 kecuali untuk satu koordinat, serta diketahui $Hx^T \neq 0$, diperoleh

$$Hx^T = H\left(c+E\right)^T = H\left(c^T + E^T\right) = Hc^T + HE^T = 0 + HE^T = HE^T .$$

Oleh karena itu, HE^T muncul sebagai hasil kali skalar dari suatu kolom dalam H yang menunjukkan lokasi kesalahannya. Apabila digunakan lapangan biner, maka koordinat terjadinya kesalahan dapat dilihat dari kolom dari H dimana vektor kolom HE^T muncul.

Untuk mendeteksi adanya kesalahan, misalkan diterima vektor-vektor berikut ini:
Huruf ke-1: $(a_1b_1c_1d_1e_1)$ Huruf ke-2: $(a_2b_2c_2d_2e_2)$ Huruf ke-3: $(a_3b_3c_3d_3e_3)$
Huruf ke-4: $(a_4b_4c_4d_4e_4)$, Cek bit ke-1: $(a_5b_5c_5d_5e_5)$, Cek bit ke-2: $(a_6b_6c_6d_6e_6)$,
Cek bit ke-3: $(a_7b_7c_7d_7e_7)$

Langkah selanjutnya, disusun vektor-vektor $a' = (a_1a_2a_3a_4a_5a_6a_7)$, $b' = (b_1b_2b_3b_4b_5b_6b_7)$, $c' = (c_1c_2c_3c_4c_5c_6c_7)$, $d' = (d_1d_2d_3d_4d_5d_6d_7)$ dan $e' = (e_1e_2e_3e_4e_5e_6e_7)$. Untuk mendeteksi adanya kesalahan, digunakan matriks cek paritas *H*, yaitu dengan menghitung $H(a')^T$, $H(b')^T$, $H(c')^T$, $H(d')^T$ dan $H(e')^T$. Apabila diperoleh hasil vektor yang tidak nol, maka terdeteksi adanya kesalahan.

Untuk proses koreksi yang diakibatkan oleh 1 kesalahan, langkah-langkahnya adalah dengan melihat hasil perhitungan $H(a')^T$, $H(b')^T$, $H(c')^T$, $H(d')^T$ dan $H(e')^T$. Apabila ditemukan hasil berupa vektor tak nol, maka hasil vektor tersebut dilihat di dalam matriks cek paritas H. Posisi koordinat terjadinya kesalahan terletak di posisi kolom dimana vektor tersebut muncul. Cara mengkoreksinya hanya dengan mengganti 0 dengan 1 atau sebaliknya.

Contoh 2. Diberikan kode Hamming dengan parameter dan kasus seperti pada Contoh 2. di atas, misalkan diterima pesan yang telah terjadi 1 kesalahan yaitu:

م ن س ي ر ج ظ

Langkah pertama adalah merubah setiap huruf menjadi vektor biner sesuai dengan tabel korespondensi, yaitu

م	11000
ن	11001
س	01100
ي	11110
ر	01010
ج	00101
ظ	10001

Selanjutnya, dibentuk vektor-vektor $a' = (1101001)$, $b' = (1111100)$, $c' = (0011010)$, $c' = (0001100)$ dan $e' = (0100010)$. Untuk melakukan deteksi kesalahan dilakukan proses perhitungan berikut:

$$H\left(a'\right)^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1101001)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H\left(b'\right)^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1111100)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H(c')^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0011010)^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H(d')^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0001100)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H(e')^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0100010)^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Berdasarkan hasil perhitungan di atas, diperoleh bahwa terjadi kesalahan pada vector a', b' dan d'. Dapat dilihat bahwa $H(a')^T = H(b')^T = H(d')^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ muncul sebagai kolom kedua dari matriks cek paritas H. Oleh karena itu, kesalahan terjadi pada bit ke-2, sehingga vektor kesalahannya adalah $E = (0100000)$. Proses koreksi dilakukan dengan menghitung:

$$a' - E = (1101001) - (0100000) = (1001001)$$

$$b' - E = (1111100) - (0100000) = (1011100)$$

$$d' - E = (0001100) - (0100000) = (0101100)$$

Diperoleh katakode-katakode yang telah dikoreksi, yaitu (1001001), (1011100), (0011010), (0101100) dan (0100011). Selanjutnya, cek bit dihilangkan, diperoleh (1001), (1011), (0011), (0101) dan (0100). Kemudian disusun dalam tabel berikut:

11000	م
00011	ت
01100	س
11110	ي

Diperoleh pesan semula yaitu

م ت س ي

Kesimpulan

Berdasarkan perhitungan-perhitungan di atas, maka dapat disimpulkan bahwa kode Hamming berorder 3 atas lapangan $\mathbb{Z}_2$ dapat digunakan untuk mendeteksi dan mengkoreksi kesalahan penulisan dalam huruf hijaiyah untuk jenis kesalahan tertentu, yaitu dalam setiap blok pesan yang terdiri dari 4 huruf, terjadi perubahan sebuah huruf menjadi huruf yang lainnya. Hal tersebut terjadi dikarenakan kode Hamming hanya memiliki kemampuan koreksi 1 kesalahan. Apabila diinginkan dapat mengkoreksi 2 kesalahan, maka harus digunakan kode linear dengan jarak Hammingnya adalah 5, yang mengakibatkan matriks generatornya menjadi lebih besar, serta penambahan cek bit yang lebih banyak.

Untuk mengkonstruksi korespondensi huruf hijaiyah dilakukan melalui ekspansi biner pada urutan huruf-huruf hijaiyah yang berjumlah 30 huruf, dimulai dari huruf "alif" yang dikorespondensikan dengan bilangan 1 yang memiliki ekspansi biner 5 bit yaitu 00001, sampai dengan huruf ya yang dikorespondensikan dengan bilangan 30 yang memiliki ekspansi biner 5 bit yaitu 11110. Dari 4 huruf

tersebut kemudian disusun dalam matriks, kemudian dibentuk 5 vektor dengan panjang 4-bit yang diambil pada kolom-kolomnya. Pengkodean yang digunakan berupa kode linear berupa kode Hamming order 3 atas lapangan biner $\mathbb{Z}_2$. Terjadi penambahan panjang pesan sebanyak 15 bit, dari yang semula 20 bit, setelah dikodekan menjadi 35 bit. Berdasarkan penggunaan kode Hamming atas lapangan biner $\mathbb{Z}_2$ dengan order 3, maka jenis kesalahan yang dapat dideteksi dan dikoreksi adalah apabila terjadi kesalahan penulisan dalam setiap blok yang terdiri dari 4 huruf, terjadi kejadian satu huruf menjadi huruf yang lain.

Sebagai saran, perlu dikaji jenis-jenis kode lain yang lebih cocok digunakan untuk pengkodean huruf hijaiyah, sehingga dapat meminimalisir jumlah penambahan cek bit pada pesan semula. Perlu dikaji jenis-jenis kesalahan penulisan apa saja yang sering muncul pada penulisan dalam huruf hijaiyah. Selain itu, perlu dikaji metode pengkodean untuk jenis kesalahan yang terjadi karena adanya penambahan huruf baru dalam sebuah pesan, serta jenis kesalahan yang terjadi karena adanya penghapusan huruf.

Referensi

[1] **Ameer Kadhim Hadi**. 2017. *Toward Trust and More Characters of Arabic Short Message Service using Encryption*. Journal of Engineering and Applied Sciences. Vol.12 No.21. pp.5384-5387.

[2] **Anton**, **Howard**. 2014. *Elementary Linear Algebra* 11*th Edition: Applications Version*. Canada. Wiley.

[3] **Dummit**, **David S**. dan **Foote Richard M**. 2004. *Abstract Algebra Third Edition*. New Jersey: John Wiley and Sons.

[4] **Jurgen Bierbrauer**. 2016. *Introduction to Coding Theory* 2*nd Edition*. Boca Raton Florida. Chapman and Hall/CRC.

[5] **Leon**, **Steven J**. 2002. *Linear Algebra with Applications* 6*th Edition*. New Jersey. Prentice-Hall.

[6] **Malik**, **D. S.**, **Morderson John N**. dan **Sen**, **M. K**. 1997. *Fundamentals of Abstract Algebra*. WCB/McGraw-Hill.

[7] **Prakash Kuppuswamy** dan **Yahya Alqahtani**. 2014. *New Innovation of Arabic Language Encryption Technique Using New Symmetric Key Algorithm*. International Journal of Advances in Engineering & Technology. Vol. 7 Issue 1. Mar 2014. pp. 30-37.

[8] **Republika**. 2017. *Kesalahan Penulisan Alquran, Penyeleksian Harus Diperluas*. https://www.republika.co.id/berita/dunia-islam/islam-nusantara/17/10/29/oyl5es396-kesalahan-penulisan-alquran-penyeleksian-harus-diperluas (diakses tanggal 1 September 2018)

[9] **San Ling**, **Chaoping Xing**. 2004. *Coding Theory: A First Course*. Cambridge UK. Cambridge University Press.

[10] **Shannon**, **Claude**. 1948. *A Mathematical Theory of Communication*. Bell System Technical Journal. 27 (3). Pp.379-423.

[11] **Thomas W. Judson**. 2017. *Abstract Algebra: Theory and Applications:* 2017 *Edition*. Texas. Orthogonal Publishing L3C.

[12] **Van Lint**, **J. H**. 1999. *Introduction to Coding Theory Third Edition*. Springer.

[13] **Vanstone**, **Scott A**. dan **Oorschot**, **Paul C. van**. 1989. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers.

[14] **William E. Ryan** dan **Shu Lin**. 2009. *Channel Codes: Classical and Modern*. Cambridge University Press.

[15] **Yahya Alqahtani**, **Prakash Kuppuswamy** dan **Sikandhar Shah**. 2013. *New Approach of Arabic Encryption/Decryption Technique Using Vigenere Cipher on Mod* 39. International Journal of Advanced Research in IT and Engineering. Vol.2 No.12. Dec 2013. pp.1-9.