Kode linear

Misalkan F adalah lapangan dengan q elemen dan himpunan semua pesan adalah himpunan k-tupel yang komponen-komponennya adalah anggota dari lapangan F. Selanjutnya himpunan semua k-tupel atas F ditulis $V_k(F)$ sehingga ada q^k pesan. Lebih jauh lagi $V_k(F)$ adalah ruang vektor terhadap operasi penjumlahan vektor dan perkalian skalar dan disebut message space. Untuk dapat mendeteksi dan mengoreksi kesalahan yang mungkin maka harus ditambahkan suatu redundansi sehingga pesan k-tupel disisipkan ke dalam n-tupel, n >k. Selanjutnya akan dikonstruksikan suatu fungsi bijektif dari himpunan pesan ke subruang dari $V_n(F)$. Banyaknya subruang dari $V_n(F)$ yang berdimensi k adalah $\frac{(q^n-1)(q^{n-1}-1)...(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)...(q-1)}$.

Kemudian jika S adalah salah satu dari subruang tersebut, maka kita dapat mendefinisikan fungsi bijektif dari S ke ruang pesan M. Misalkan B = { v_1, v_2, …, v_k} basis untuk S , didefinisikan f : M $\rightarrow$ S dengan f(m) = $\sum_{i=1}^{k} m_i v_i$ untuk setiap m di M dengan m = (m_1 m_2… m_k) adalah pesan k-tupel.

Contoh :

M adalah ruang pesan yang terdiri dari empat pesan 2-tupel, yaitu M = { (00), (10), (01), (11)}, ambil S adalah subruang dari $V_4(Z_2)$ dan dimensi S adalah 2 dengan basis B = { v_1 = (1100), v_2 = (0110)}. Jika f : M $\rightarrow$ S dengan f(m) = $\sum_{i=1}^{2} m_i v_i$,

maka (00) $\rightarrow$(0000), (10) $\rightarrow$(1100), (01) $\rightarrow$(0110), (11) $\rightarrow$(1010).
Jadi S = { (0000), (1100), (0110), (1010)}.

Definisi 1 : Suatu (n,k)-*code* linear atas F adalah subruang berdimensi k dari $V_n(F)$.
Kadang-kadang suatu (n,k)-*code* linear hanya ditulis (n,k)-*code* saja.

Algoritma untuk mencari basis suatu code linear:
Input: S $\subset V_n(F(q))$
Output: Basis dari code linear C = $< S >$

Caranya:

Bentuk matriks A dengan baris-barisnya adalah elemen-elemen S.

Lakukan OBE pada A sampai diperoleh bentuk eselon baris.

Baris tak nol dari bentuk eselon baris adalah basis untuk code linear C.

Contoh:

Cari basis untuk code linear C atas Z_3 yang dibangun oleh

$S = \{(12101), (20110), (01122), (11010)\}$

Jawab:

Bentuk matriks A =

Definisi 2 : *Hamming weight* suatu vektor v di $V_n(F)$, ditulis w(v), adalah banyaknya koordinat tak nol dari v.

Definisi 3 : *Hamming weight* dari (n,k)-*code* C adalah $w(C) = \min\{w(x) : x \in C, x \neq 0\}$.

Berdasarkan definisi di atas maka jarak d dari (n,k)-*code* C adalah d = w(C).

Misalkan C adalah (5,3)-*code* dan $C \subseteq V_5(Z_2)$ dengan basis B = { v_1 = (10000), v_2 = (11010), v_3 = (11101)} sehingga C = { (00000), (10000), (11010), (11101), 01010), (01101), (00111), (10111)}. Jika $G = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$ dan m = (m_1 m_2 m_3)$\in$M , maka *codeword* di C yang berasosiasi dengan m adalah

$$mG = \begin{pmatrix} m_1 & m_2 & m_3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} = \sum_{i=1}^{3} m_i v_i \, .$$

Kemudian jika diambil m = (011), maka mG = (00111). Jika diambil basis yang lain , yaitu B_1 = { u_1 = (10000), u_2 = (01010), u_3 = (00111)} , maka G_1= (u_1 u_2 u_3)^T sehingga mG_1 = (01101). Dari contoh ini ternyata pengambilan basis yang berbeda akan menyebabkan suatu pesan dikodekan dengan kode yang berbeda.

Berdasarkan contoh di atas berikut ini didefinisikan suatu matriks generator.

Definisi 4 : Misalkan C adalah (n,k)-*code*. Suatu matriks generator G untuk C adalah matriks ukuran k x n yang barisnya adalah anggota-anggota basis dari C.

Jika G suatu matriks generator untuk C dengan G = [I_k A], I matriks identitas kxk, A matriks kx(n-k), maka G dikatakan **bentuk standar**.

Definisi 5 : Misalkan C dan C_1 adalah (n,k)-*code* atas F. C dan C_1 dikatakan ekuivalen jika ada matriks generator G untuk C dan G_1 untuk C_1 dan matriks permutasi P sehingga G_1 = GP.

Selanjutnya dapat ditunjukkan bahwa Jika C dan C_1 adalah (n,k)-*code* atas F yang ekuivalen , maka ada matriks generator G untuk C atau untuk C_1 sehingga G =[I_k A].

Misalkan C adalah (n,k) –*code* , didefinisikan komplemen ortogonal $C^{\perp}$ sebagai berikut : $C^{\perp} = \{x \in V_n(F) : \quad x \bullet y = 0, \forall y \in C\}$. Selanjutnya $C^{\perp}$ disebut *code dual* dari C.

Teorema 3 : Jika C adalah (n,k)-*code* atas F, maka $C^{\perp}$ adalah (n,n-k)-*code* atas F.

Berdasarkan teorema ini diturunkan sifat bahwa : Jika G =[I_k A] adalah matriks generator untuk C , maka H = [$-A^T$ I_{n-k}] adalah matriks generator untuk $C^{\perp}$.

Contoh :

Misalkan C adalah (6,3)-*code* atas Z_2 yang dibangun oleh $G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$, kemudian dengan operasi baris elementer diperoleh matriks generator $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = [I_3 A]$

dengan $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Selanjutnya matriks generator untuk $C^{\perp}$ adalah H = $[-A^T \ I_3]$ = $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$.

Matriks G dan H tersebut memenuhi $G H^T = 0$.

Jadi untuk setiap vektor x di $V_n(F)$ adalah codeword dari (n,k)-*code* C jika dan hanya jika $Hx^T = 0$, dengan H adalah matriks generator untuk $C^{\perp}$.