ANADOLU ÜNİVERSİTESİ BİLİM VE TEKNOLOJİ DERGİSİ
ANADOLU UNIVERSITY JOURNAL OF SCIENCE AND TECHNOLOGY
Cilt/Vol.:5-Sayı/No: 2 : 253-258 (2004)

ARAŞTIRMA MAKALESİ/**RESEARCH ARTICLE**

NON-HAMMING (ROSENBLOOM-TSFASMAN) METRİĞİNE GÖRE LİNEER KODLARIN YAPISI

Mehmet ÖZEN[1], İrfan ŞİAP[2], Fethi ÇALLIALP[3]

ÖZ

Bu çalışmada ρ metriğine göre lineer kodların yapıları incelendi. Kodların yapılarından faydalanılarak, bu metriğe göre lineer ve devirli kodların minimum uzaklığının kolaylıkla tespit edilebildiği gösterildi. Bu metriğe bağlı olarak lineer kodların dualleri incelendi ve MDS kodların ağarlık sayaçları bulundu.

Anahtar Kelimeler: Lineer Kodlar, Non-Hamming Metriği, MDS Kodlar

THE STRUCTURE OF LINEAR CODES WITH RESPECT TO A NON-HAMMING (ROSENBLOOM-TSFASMAN) METRIC

ABSTRACT

We explore the structure of linear codes with respect to the ρ metric. Taking advantage of this structure, we show that the minimum distance of linear and cyclic codes can be determined easily. We investigate the dual of linear codes and the weight enumerator of MDS codes with respect to this metric.

Key Words: Linear Codes, Non-Hamming Metric, MDS Codes

1. GİRİŞ

ρ non-Hamming (Rosenbloom-Tsfasman) metriği [4]'te yakın zamanda sunulmuş ve minimum uzaklık için üst sınırlar ispatlanmıştır. [1]'de bu metriğe göre Hamming ağırlık sayaçları incelenmiştir. Ayrıca, [5]'te yine bu non-Hamming metriğine göre tam ağırlık sayaçları tanımlanmış ve MacWilliams eşitlikleri ispatlanmıştır. Birinci bölümde Hamming metriğine bağlı olarak bilinen bazı temel teorem ve sonuçları verilecektir. İkinci bölümde, Hamming metriğinde bilinen ve tanımlanan bazı kavramlar, Hamming olmayan Rosenbloom-Tsfasman metriğinde incelenecektir. Üçüncü bölümde ise MDS kodlar ile ağırlık sayaçları incelenecektir. q bir asal sayının kuvveti olmak üzere, $F_q=\{\alpha_0,\alpha_1,\ldots,\alpha_{q-1}\}$, q elemanlı sonlu bir cisim olsun. $V(n,q)$, F_q üzerinde n uzunluğundaki bütün vektörlerin kümesi olsun. Bu küme, bir vektör uzayıdır. $C \subset V(n,q)$ ve C, $V(n,q)$ nun k boyutlu bir alt vektör uzayı ise C ye n uzunluğunda, k boyutlu bir lineer *kod* denir ve kısaca $[n,k]$ ile gösterilir. C nin elemanlarına ise kodsöz denir. Bir *kodsöz*deki sıfırdan farklı bileşenlerin sayısına ise o kodsözün *Hamming ağırlığı* ya da kısaca kodsözün ağırlığı denir. İki kodsöz arasındaki *Hamming uzaklığı* ise; bu kodsözlerin farklarının Hamming ağırlığına eşittir. C deki kodsözlerin sıfırdan farklı en küçük ağırlığına C nin Hamming ağırlığı denir ve kısaca $w(C)$ ile gösterilir. Diğer yandan, C deki sıfırdan farklı en küçük Hamming uzaklığına ise C nin *minimum uzaklığı* denir. Lineer kodlarda

[1] Sakarya Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Serdivan, 54100,SAKARYA
E-Posta:ozen@sakarya.edu.tr.
[2] Gaziantep Üniversitesi, Adıyaman Eğitim Fakültesi.
[3] Doğuş Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü.

Geliş: 02 Ocak 2002; **Düzeltme:** 18 Kasım2002; **Kabul;** 04 Mayıs 2004

$d(C) = w(C)$ dir. Bir vektör uzayı olarak tanımlanan bir C kodu için uzunluk, boyut parametreleri yanında minimum uzaklık parametresinin rolü çok önemlidir. Minimum uzaklığa göre bir kodun hata düzeltme özelliği ölçülebilir [2]. C, $[n,k]$ bir lineer kod olsun. Satırları C nin bazından oluşan bir G', $k \times n$ matrisine C nin üreteç matrisi denir. Eğer bir C kodunun bileşenlerine bir permütasyon uygulanarak C' kodu elde ediliyorsa C kodu ile C' kodu birbirine denktir denir. Dikkat edilirse C ile C' nün üç temel parametreleri n, k, ve d aynıdır ve kodlama anlamında farklı yapılar değildirler.

Teorem 1. *[2] F_q üzerinde, C [n,k,d] lineer kodu verildiğinde; ilk k sütunu k boyutlu I_k birim matrisi olan $G = [I_k, A]$ stand art formdaki üreteç matrisine sahip bir C' koduna denktir.*

Hamming metriğinde iç çarpım, C nin herhangi $\boldsymbol{x} = (x_1, x_2, ..., x_n)$ ve $\boldsymbol{y} = (y_1, y_2, ..., y_n)$ kodsözleri için, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_i$ şeklinde tanımlanır. $C^{\perp} = \{ \boldsymbol{x} \in V(n,q) \mid \langle \boldsymbol{x}, c \rangle = 0, \forall c \in C \}$ kümesine C nin dual kodu denir.

Teorem 2. *[3] $G = [I_k, A]$ standart formdaki üreteç matrise sahip C bir $[n,k]$ lineer kod olsun. O zaman $C^{\perp}$, $H = [-A^T, I_{n-k}]$ üreteçli, $[n, n-k]$ lineer kod olur.*

Yukarıdaki teoremde adı geçen H matrisine C kodunun **kontrol matrisi** denir.

$R_n = F_q[x]/\langle x^n - 1 \rangle$, bir temel ideal halkasıdır. Φ: $V(n,q) \to R_n$ ve $\Phi((c_0, c_1, ..., c_{n-1})) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$ ise Φ, $V(n,q)$ ile R_n arasında bir vektör uzayı izomorfizmasıdır. Eğer herhangi bir $(c_0, c_1, ..., c_{n-1}) \in C$ için $(c_{n-1}, c_0, ..., c_{n-2}) \in C$ ise $C \subset V(n,q)$ ye bir devirli kod denir. C devirli kodu $\Phi(C)$ ile özdeşliğinde R_n in bir ideali olduğu görülür.

Önerme 3. *[3] C, R_n in bir ideali olsun. Bu durumda $C = \langle f(x) \rangle$ ve $f(x) \mid x^n - 1$ olacak şekilde bir $f(x) = a_0 + a_1 x + ... + a_r x^r$, $a_r = 1$ vardır. C, $f(x)$ tarafından üretilen $n - r = k$ boyutlu ve*

$$G = \begin{bmatrix} 0 & \cdots & 0 & a_0 & \cdots & a_r \\ 0 & \cdots & a_0 & \cdots & a_r & 0 \\ \vdots & & & & & \vdots \\ a_0 & \cdots & a_r & 0 & \cdots & 0 \end{bmatrix}_{k \times n}$$

üreteç matrisli bir devirli koddur.

$f(x) \mid x^n - 1$ olmak üzere $C = \langle f(x) \rangle$ devirli bir kod (ideal) olsun. $x^n - 1 = f(x)h(x)$ ise $h(x)$ e, C nin kontrol polinomu denir

Teorem 4. [3] $h(x)$, devirli C, $[n,n-r]$ lineer kodunun, R_n deki kontrol polinomu olsun. O zaman kontrol matrisi,

$$H = \begin{bmatrix} 0 & \cdots & 0 & 0 & h_{n-r} & \cdots & h_0 \\ \vdots & & & & & & \vdots \\ 0 & h_{n-r} & \cdots & h_0 & 0 & \cdots & 0 \\ h_{n-r} & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

olur ve r boyutlu devirli dual kodunun üreteç polinomu $h^{\perp}(x) = h_0^{-1} x^{n-r} h(x^{-1})$ dir.

Giriş bölümündeki temel bilgi ve teoremlerle ilgili olarak daha geniş bilgi için [2] ve [3] kaynaklarına bakılabilir.

2. NON-HAMMING METRİĞİNE GÖRE LİNEER KODLARIN YAPISI

$\boldsymbol{x} = (\xi_1, \xi_2, ..., \xi_n) \in C$ kodsözünün non-Hamming ağırlığı,

$$w_N(\boldsymbol{x}) = \begin{cases} \max\{ i \mid \xi_i \neq 0 \}, & \boldsymbol{x} \neq 0 \\ 0, & \boldsymbol{x} = 0 \end{cases}.$$

Herhangi $\boldsymbol{x}, \boldsymbol{y} \in C$ için $\rho(\boldsymbol{x}, \boldsymbol{y}) = w_N(\boldsymbol{x} - \boldsymbol{y})$ şeklinde tanımlanan ρ fonksiyonuna $\boldsymbol{x}$ ve $\boldsymbol{y}$ kodsözlerinin non-Hamming Rosenbloom-Tsfasman uzaklığı denir. ρ bir metriktir [4]. Non-Hamming metriğinde minimum uzaklık, $d_N(C) = \min_{\boldsymbol{x}, \boldsymbol{y} \in C} \{ \rho(\boldsymbol{x}, \boldsymbol{y}) \mid \rho(\boldsymbol{x}, \boldsymbol{y}) \neq 0 \}$ şeklinde tanımlanır ve kısaca d_N ile gösterilir. Non-Hamming metriğinde bir C kodunun minimum ağırlığı ise, $w_N(C) = \min_{\boldsymbol{x} \in C} \{ w_N(\boldsymbol{x}) \mid \boldsymbol{x} \neq 0 \}$ şeklinde tanımlanır ve kısaca $w_N(C)$ ile gösterilir. Hamming metriğinde olduğu gibi, C lineer bir kod ise $d_N(C) = w_N(C)$ olur.

2.1. Lineer Kodun Üreteç Matrisi

Satırları k boyutlu C nin bazından oluşan bir G', $k \times n$ matrisi C nin üreteç matrisi olsun. Genelliği bozmadan G' matrisinin son sütununun sıfırdan farklı olduğu kabul edilir.

Önerme 5. *C, $[n,k]$ parametreli bir lineer kod olsun.C kodu,*

$$G=\begin{bmatrix} g_{11} & \cdots & g_{1s_k-1} & 0 & g_{1s_k+1} & \cdots & g_{1s_2-1} & 0 & g_{1s_2+1} & \cdots & g_{1s_1} \\ g_{21} & \cdots & g_{2s_k-1} & 0 & g_{2s_k+1} & \cdots & g_{2s_2-1} & g_{2s_2} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k1} & \cdots & g_{ks_k-1} & g_{ks_k} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \quad \textbf{(1)}$$

$n \geq s_1 > s_2 > s_3 > ... > s_k \geq 1$ *ve* $g_{1s_1} = g_{2s_2} = ... = g_{ks_k} = 1$ şeklindeki bir üreteç matrisine sahiptir.

Kanıt: G' matrisi lineer cebirden bilinen elemanter satır işlemleri ile (sütun işlemleri yapmadan) yukarıdaki gibi üçgensel formda olan G matrisine indirgenir.

Tanım 6. *Yukarıdaki önermede verilen ve non-Hamming metriğine göre yapılan incelemede temel teşkil edecek (1) matrisine bir kodun standart formdaki üreteç matrisi denir.*

Önerme 7. *Non-Hamming metriğine göre, (1) standart formundaki G üreteç matrisine sahip C kodunun minimum uzaklığı $d_N = s_k$ olur.*

Kanıt: Standart forma getirilen matriste $g_{1s_1}, g_{2s_2}, ..., g_{ks_k}$ bileşenleri sıfırdan farklıdır. Bütün kodsözler bu üreteç matrisin satırlarının lineer kombinasyonlarından oluşur. Dolayısıyla k nıncı satırdakinden daha küçük ağırlığa sahip kodsöz oluşamaz. Non-Hamming metriğine göre $d_N = s_k$ olur.

Önerme 8. [4] *(Singleton Üst Sınırı) C, F_q üzerinde bir $[n,k,d_N]$ lineer kod ise $d_N \leq n-k+1$ olur.*

Kanıt:. Burada standart formu kullanarak bağımsız ve daha basit bir ispat verilir. G' üreteç matrisi elemanter satır işlemleri sonucu $s_1 = n$ ve $s_i = s_{i-1} - 1$, $2 \leq i \leq k$ ve $s_k \leq n-k+1$ olacak şekilde (1) deki standart forma indirgenir. Bir kodun kodsözleri bu matrisin lineer kombinasyonlarından oluştuğundan elde edilecek bütün kodsözlerin ağırlıkları *n-k*+1 den büyük olamaz. Dolayısıyla $d_N \leq n-k+1$ olur.

Tanım 9. *[4] Singleton üst sınırını sağlayan kodlara maksimum uzaklığa ayrışabilir (Maximum Distance Separable) kod denir.*

G' elemanter satır işlemleri ile $s_1 = n,\ s_i = s_{i-1} - 1,\quad 2 \leq i \leq k$, $s_k = n-k+1$ ve A, $k \times (n-k)$ tipinde bir matris olmak üzere;

$$G = \left[\begin{array}{cccc} & 0 & \cdots & 1 \\ A, & & \ddots & \\ & 1 & \cdots & 0 \end{array}\right] \quad \textbf{(2)}$$

standart formuna gelen G üreteç matrisine sahip C kodu bir MDS kod olur.

2.2. Lineer Kodların Duali ve Dualinin Üreteç Matrisi

Non-Hamming metriğinde iç çarpım, C nin herhangi iki kodsöz

$\boldsymbol{x} = (x_1, x_2, ..., x_n)$ ve $\boldsymbol{y} = (y_1, y_2, ..., y_n)$ için;

$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_{n-i+1}$ şeklinde tanımlanır.[4]

Önerme 10. *(1) deki G üreteçli C, [n,k] lineer kodunun duali $C^{\perp}$, bir $[n, n-k]$ lineer kod olur.*

Kanıt: $C^{\perp}$ in lineerliği ve boyutunun $n-k$ olduğu Hamming metriğine benzer şekilde gösterilir.

Non-Hamming metriğine göre H kontrol matrisinin bulunuşu:

Standart formdaki üreteç matrisi σ_2, n-li sütun permütasyonu ile, $\sigma_2(G) = G''$, $G'' = [A, I_k]$ Hamming anlamında standart formuna getirilir. Bundan yararlanarak Hamming metriğine göre $H'' = [I_{n-k}, -A^{\mathrm{T}}]$ kontrol matrisi elde edilir. $\sigma_2^{-1}(H'') = H'$ olsun. G de herhangi bir i inci satırı $(g_{i1}, g_{i2}, ... g_{in})$ ve H' nün herhangi j inci satırı $(h''_{j,\sigma_2^{-1}(1)}, ..., h''_{j,\sigma_2^{-1}(n)})$ olsun. G'' ile H'' Hamming anlamında birbirine diktir.

$G''(H'')^{\mathrm{T}} = 0$. G nin i inci satır σ_2 altında,

$\sigma_2(g_{i1}, g_{i2}, ..., g_{in}) = (g_{i,\sigma_{2(1)}}, ..., g_{i,\sigma_2(n)}) \in G''$ ve $(h''_{j1}, ..., h''_{jn}) \in$

olsun.

$$g_{i,\sigma_{2(1)}} h''_{j1} + \cdots + g_{i,\sigma_{2(n)}} h''_{jn} = 0,$$

$$\langle (g_{i,\sigma_{2(1)}}, ..., g_{i,\sigma_{2(n)}}), (h''_{j1}, ..., h''_{jn}) \rangle = 0.$$

Her iki çarpana ayrı ayrı σ_2^{-1} permütasyonu uygulanıp skaler çarpılırsa skaler çarpımın değerinde bir değişme olmayacağıdan, $g_{i1}h''_{j,\sigma_2^{-1}(1)} + ... + g_{in}h''_{j,\sigma_2^{-1}(n)} = 0$ olur. Dolayısıyla G ile H' Hamming anlamında diktir.

H' ye $\sigma_1 = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$ permütasyonu uygulanarak satırlar ters çevrildiğinde $\sigma_1\,(H')$, elde edlir. $\sigma_1\,(H') = H^0$ olsun. H^0, G ye non-Hamming anlamında dik olur. σ_0 satır permütasyonu ile, H^0 standart forma getirilerek $\sigma_0(H^0) = H$, $(n-k)\times n$ tipindeki H kontrol matrisi bulunur.

Önerme 11. *Yukarıdaki paragrafta geçen tanım ile ve ifadeler altında, G üreteç matrisli bir kodun non-Hamming metriğine göre kontrol matrisi;* $\sigma_0(\sigma_1(\sigma_2^{-1}(H''))) = H$ *olur.*

Örnek 1. Bir C kodunun non-Hamming ağırlığa göre standart formdaki matrisi,

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

olsun. Önerme 7. ye göre $d_N = 3$ olur.

$\sigma_2 = \begin{pmatrix} 1234567 \\ 1276435 \end{pmatrix}$, G ye uygulandığında

$G'' = [A, I_3]$ olur. Bundan yararlanarak

$$H'' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

yazılır. H'' ye öncelikle σ_2^{-1} uygulanır, sonra σ_1 ile satırları ters çevirip, $\sigma_0 = \begin{pmatrix} 1234 \\ 1243 \end{pmatrix}$ satır permütasyonu kullanılarak,

$$\sigma_0(\sigma_1(\sigma_2^{-1}(H''))) = H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

bulunur.

2.3. Devirli Kodların Duali ve Minimum Uzaklık

Önerme 12. $f(x) = a_0 + a_1x + ... + a_rx^r$, $a_r = 1$ *ve* $f(x)$ fonksiyonu $x^n - 1$ i bölsün. $C = \langle f(x) \rangle$ devirli kodunun non-Hamming ağırlığına göre standart formdaki üreteç matrisi,

$$G = \begin{bmatrix} 0 & \cdots & 0 & a_0 & \cdots & a_r \\ 0 & \cdots & a_0 & \cdots & a_r & 0 \\ \vdots & & & & & \vdots \\ a_0 & \cdots & a_r & 0 & \cdots & 0 \end{bmatrix}$$

ve $\operatorname{rank}(G) = n - r = k$ olduğundan $d_N(C) = n - k + 1$ olur.

Kanıt: Elemanter satır işlemleri ile G standart formu bulunur. $a_r = 1$ ve $\operatorname{rank}(G) = k$ olduğu için non-Hamming ağırlığına göre G standart formdaki üreteç matrisinden $w_N = n - k + 1$ olduğu çıkar.

Aşağıdaki sonuç tanımlardan kolayca elde edilir.

Sonuç 1. Devirli kodlar non-Hamming metriğinde MDS kodlardır.

Sonuç 2. Devirli $C^\perp$ dual kodunun H üreteç matrisi olsun ve $rank(H) = n - k$ ise $d_N^\perp = k + 1$ olur.

Kanıt: Devirli C lineer kodunun üreteç matrisi G standart formdadır ve burada A, $k\ x\ (n-k)$ boyutlu bir matristir.

$$G = \begin{bmatrix} & 0 & \cdots & 1 \\ A, & & \ddots & \\ & 1 & \cdots & 0 \end{bmatrix}$$

G matrisinin satırları yer değiştirilerek $[A', I_k]$ full (son k sütuna birimin oturması) formuna getirilir. Bundan yararlanarak Hamming anlamında diki yazılıp satırlar ters çevrilip non-Hamming anlamında dik olan H kontrol matrisi yazılır. $H = [B, I_{n-k}]$ full formdadır. Satırlar yer değiştirilerek standart forma getirilir ve dolayısı ile $d_N^\perp = k + 1$ olduğu H matrisinden çıkar.

3. MDS KODLAR VE AĞIRLIK SAYAÇLARI

Teorem 13. *C, $[n, k, d_N]$ lineer kodu MDS ise duali olan $C^\perp$ de MDS dir.*

Kanıt. $C^\perp$, lineer kodunun minimum uzaklığı $d_N^\perp$ olsun. C lineer kodu MDS olduğundan üreteç matrisi (2) deki G standart formundadır ve $rank(G) = k$ olduğundan, $d_N = n - k + 1$ dir. $C^{\perp}$ lineer kod olduğundan $d_N^{\perp} \leq n - (n - k - 1)$ ve buradan da $d_N^{\perp} \leq k + 1$ olur. G matrisinin satırları yer değiştirilerek $[A', I_k]$ formuna getirilir. Bundan yararlanarak. Hamming anlamında diki yazılıp satırlar ters çevrilip non-Hamming anlamında dik olan H kontrol matrisi yazılır. $H = [B, I_{n-k}]$ full formundadır. Dolayısıyla $d_N^{\perp} = k + 1$ olur. $C^{\perp}$ in MDS olduğu gösterilmiş olur.

Tanım 14. C bir kod ve A_i, C kodundaki i non-Hamming ağırlığında olan kodsözlerin sayısı olsun.

$$W_C(z) = \sum_{i=0}^{n} A_i z^i = \sum_{c \in C} z^{w_N(c)}$$

polinomuna C kodunun non-Hamming ağırlık sayacı denir.

Teorem 15. F_q, q elemanlı sonlu bir cisim ve C, bir $[n, k, n-k+1]$ MDS kod olsun. A_i, i ağırlığındaki kodsözlerin sayısını göstermek ve i, $d_N \leq i \leq n$ olmak üzere; $A_i = (q-1)q^{i-d_N}$ olur.

Kanıt. $d_N = n - k + 1$ olduğundan C, MDS kodunun üreteç matrisi elemanter satır işlemleri ile (2) deki standart formuna getirilir. Burada A, $k \times (n-k)$ tipinde bir matrisdir. k nıncı satır için d_N ağırlığındaki kodların sayısı $q-1$ tane olur. $k-1$ inci satırda $d_N + 1$ ağırlığındaki kodlarının sayısı ise k nıncı satırla lineer kombinasyonunda, $d_N + 1$ ağırlığı değişmeyeceğinden $q(q-1)$ tane olur. $k-2$ inci satırda $d_N + 2$ ağırlığındaki kodlarının sayısı ise $(q-1)(q^2)$ olur. Tümevarım ile 1 inci satırda n ağırlığındaki kodların sayısı da $(q-1)(q^{k-1})$ olur. Dolayısıyla $d_N \leq i \leq n$ için, $A_i = (q-1)q^{i-d_N}$ olur.

Sonuç 3. F_q, q elemanlı sonlu bir cisim ve C, $[n, k, n-k+1]$ MDS kodunun duali $C^{\perp}$ olmak üzere $C^{\perp}$, $[n, k, k+1]$ MDS kodu olur. Ayrıca üreteç matrisi,

$$H = \begin{bmatrix} & 0 & \mathrm{K} & 1 \\ B, & & \mathrm{O} & \\ & 1 & \mathrm{K} & 0 \end{bmatrix}$$

olduğundan standart formdadır. Burada $n - k \times k$ tipinde bir matristir. $A_i^{\perp}$, i ağırlığındaki kodsözlerin sayısını göstersin. $d_N^{\perp} \leq i \leq n$ olmak üzere, $A_i^{\perp} = (q-1)q^{i-d_N^{\perp}}$ olur.

Örnek 2. F_3 cismi üzerinde C, $[7,4,4]$ MDS kodunun standart formdaki üreteç matrisi,

$$G = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

olsun. $d_N = n - k + 1 = 4$ tür. $3^4 = 81$ tane kodsöz vardır. $d_N = 4 \leq i \leq 7$ ağırlıkları 4 olan, $A_4 = 2$ tane vardır. Ağırlıkları 5 olan , $A_5 = 6$ tane vardır. Ağırlıkları 6 olan , $A_6 = 18$ tane vardır. Ağırlıkları 7 olan $A_7 = 54$ tane vardır. Sıfır kodsözü ile toplam 81 tane kodsöz olur.

Duali için ;

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$d_N^{\perp} = k + 1 = 5 \leq i \leq 7$ için, $A_5^{\perp} = 2$ tane, $A_6^{\perp} = 6$, tane $A_7^{\perp} = 18$, tane olmak üzere sıfır, kodsözü ile toplam 27 tane kodsöz olur.

Makalenin düzeltmesinde katkıda bulunan hakeme teşekkürü bir borç biliriz.

KAYNAKÇA

[1]Dougherty, S. T. and Skriganov, M. M, (2002) MacWilliams Duality and the Rosenbloom-Tsfasman Metric, *Moscow Mathematical Journal*, Vol. 2, Number (2) 1, 83-99.

[2]MacWilliams, F.J. and Sloane N.J.A. (1977), The Theory of Error-Correcting Codes, North Holland.

[3]Roman, S. (1992),Coding and Information Theory, Springer-*Verlag*.

[4]Rosenbloom, M. Yu. and Tsfasman M. A. (1997), Codes for the m-metric, Problems of Information *Transmission* , Vol. 33, (1), 45-52.

[5]Siap, I. (2001), The Complete Weight Enumerator for Codes over $M_{n\times s}(F_q)$ 8th IMA Conference on Cryptography and Codes, Cincester, UK,

Lecture Notes on Computer Sciences Vol. 2260, pp. 20-26 .

Fethi ÇALLIALP, 1970 yılında Çapa Yüksek Öğretmen Okulunu ve İstanbul Üniversitesi Fen Fakültesi Matematik Bölümünü bitirdi. 1973 yılında, Hacettepe Üniversitesi Fen Fakültesi Matematik Bölümüne Asistan olarak,1978 yılında Doktorasını ve 1982 yılında Doçentliğini aldı. 1984-1992 yılları arasında 19 Mayıs Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünde Bölüm Başkanı olarak çalıştı. 1988 yılında Profesör olarak atandı. 1992–1998 yılları arasında İTÜ Fen- Edebiyat Fakültesi Matematik Bölümünde Prof. olarak çalışırken 1993-1996 yılları arasında Sakarya Üniversitesi Fen–Edebiyat Fakültesi Dekanı olarak atandı. 1998-2000 yılları arasında Marmara Üniversitesi Eğitim Fakültesinde Bölüm Başkanı olarak çalışırken emekli oldu ve Doğuş Üniversitesi Fen–Edebiyat Fakültesi Profesör kadrosuna atandı. Halen Matematik ve Fen Bilimleri Bölüm Başkanı olarak görev yapmaktadır.

Araştırma alanları; Cebirsel Sayılar Teorisi, Halkalar Teorisi ve Modül Teori üzerinedir

İrfan Şiap, 1992 İstanbul Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü mezunudur. 1994-1999 yıllarında Ohio State Üniversitesi (A.B.D) Matematik alanında sırasıyla Yüksek lisans ve Doktora derecelerini almıştır. 2000-2002 yılları arasında Sakarya Üniversitesinde çalışmış. 2003 yıllından itibaren Doçent olarak Gaziantep Üniversitesi Adıyaman Eğitim Fakültesi'nde çalışmaktadır. Çalışma alanı ağırlıklı olarak kodlama teorisi ve matematik eğitimi üzerinedir.

Mehmet Özen, 1994 yılı Ege Üniversitesi Fen Fakültesi Matematik mezunudur. 1998 yılında Yüksek Lisansını ve 2002 yılında da Doktorasını Sakarya Üniversitesi'nde tamamlamıştır. Halen Sakarya Üniversitesi'nde Yrd. Doç. Dr. olarak görev yapmaktadır. Çalışma alanı Cebirsel Kodlama Teorisi dir.