
**Düzce Üniversitesi Bilim ve Teknoloji Dergisi**

*Araştırma Makalesi*

# Denk Kodlar Arasındaki Permütasyonu Bulmak

Ekrem EMRE*

*Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı Doktora Öğrencisi, Düzce Üniversitesi, Düzce, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: ekrememre@duzce.edu.tr*

## ÖZET

McEliece sistemi [1] gibi bazı şifreleme sistemlerinde denk kodlar kullanılmaktadır ve bu sistemlerin güvenliği verilen iki kodun denk olup olmadığının tespitine ve eğer denk iseler aralarındaki permütasyonun bulunmasının zorluğuna dayanmaktadır [2]. Bu amaç için kullanılabilecek yöntemlerden bir tanesi Support Splitting Algoritma [3] olarak adlandırılan yöntemdir. Bu makalede [4] de yer alan "About the Code Equivalence" adlı makaleden hareketle, Support Splitting Algoritmaya alternatif bir metot anlatılmış ve bir örneğe yer verilmiştir.

***Anahtar Kelimeler:*** *Denk Kodlar*

# Finding Permutation between Equivalent Codes

## ABSTRACT

In the some cryptosystems like the McEliece [1], equivalence codes are used and security of these systems are based on difficulty of detecting whether or not given two codes are equivalent and if so finding permutation between the two codes [2]. One of the methods which can be used for this purpose is the method called Support Splitting Algorithm [3]. In this article an alternative method based on the article "About the Code Equivalence" in [4] has been described and one example has been given.

***Keywords:*** *Equivalent Codes*

Geliş: 01/04/2014, Düzeltme: 16/04/2014, Kabul: 22/04/2014 

# I. GİRİŞ

**Tanım 1.1.** $F_2^n = \{(x_1, x_2, \dots, x_n) | x_i \in F_2, 1 \leq i \leq n\}$ olmak üzere $F_2^n$ nin bir alt kümesi n uzunluğunda $F_2$ üzerinde tanımlı bir kod olarak adlandırılır.

Bu makalede geçen kodları $F_2$ üzerinde tanımlı n uzunluğundaki kodlar olarak alalım.

**Tanım 1.2.** Bir $C$ kodu verildiğinde $\forall c \in C$ kod sözleri için, $w(c) =$ "$c$ kod sözündeki birlerin sayısı" şeklinde tanımlı fonksiyona $c$ kod sözünün Hamming ağırlığı [5] denir.

**Tanım 1.3.** $N = \{1,2, \dots, n\}$ olmak üzere $N$ üzerinde tanımlı tüm permütasyonların kümesi bileşke işlemi ile birlikte bir grup oluşturur ve bu grup $S_n$ ile gösterilir.

**Tanım 1.4.** $F_2$ üzerinde tanımlı $n$ uzunluğunda $C$ ve $C'$ kodları verildiğinde eğer $\forall c' \in C'$ kod sözü için $c' = \pi(c)$ , $c \in C$ olacak şekilde sabit bir $\pi \in S_n$ permütasyonu bulunabiliyorsa $C$ ve $C'$ kodlarına denktirler denir ve kısaca $C \sim C'$ yazılır.

**Tanım 1.5.** $\{P_i\}_{i \in I}$, $P_i \subseteq N$, $\bigcup_{i \in I} P_i = N$, $P_i \cap P_j = \emptyset$ , $i, j \in I$ $i \neq j$ koşullarını sağlayan bir $\{P_i\}_{i \in I}$ ailesine $N$ kümesinin bir parçalanışı denir.

# II. DENK KODLAR ARASINDAKİ PERMÜTASYONU BULMAK

$F_2$ cismi üzerinde $n$ uzunluğunda ve $m$ tane kod sözden oluşan bir $C$ kodu verildiğinde kod sözleri alt alta yazarsak $mxn$ boyutlu bir $M$ matrisi elde ederiz. $M$ matrisinin satır vektörlerini $\alpha_i', (1 \leq i \leq m)$ şeklinde ve sütun vektörlerini de $\alpha_j (1 \leq j \leq n)$ şeklinde gösterelim. Şimdi $V$ ve $V'$ kümeleri sırası ile $I_m$ ve $I_n$ indis kümelerinin herhangi alt kümeleri olmak üzere, satır ve sütun vektörleri ile $V$ ve $V'$ kümeleri üzerinde bir $d$ fonksiyonu tanımlayıp buna göre $I_m$ ve $I_n$ kümelerinin bir parçalanışını elde edelim.

**Tanım 2.1.** $d(\alpha_i', V) =$ "$\alpha_i'$ vektörünün $V$ kümesi tarafından indislenen koordinatlarındaki 1'lerin sayısıdır" .

**Tanım 2.1*.** $d(\alpha_j, V') =$ "$\alpha_j$ vektöründe $V'$ kümesi tarafından indislenen koordinatlarındaki 1'lerin sayısıdır".

**Tanım 2.2.** $I_n$ kümesinin bir parçalanışı $\{V_1, V_2, \dots, V_{N'}\}$ olsun. Buna göre $\forall i_{p_1}, i_{p_2} \in I_m$ aynı sınıftadır ancak ve ancak $d\left(\alpha'_{i_{p_1}}, V_{r'}\right) = d\left(\alpha'_{i_{p_2}}, V_{r'}\right), \forall r, 1 \leq r' \leq N'$ dır .

**Tanım 2.2*.** $I_m$ kümesinin bir parçalanışı $\{V_1', V_2', \dots, V_N'\}$ olsun. Buna göre $\forall j_{p_1}, j_{p_2} \in I_n$ aynı sınıftadır ancak ve ancak $d\left(\alpha_{j_{p_1}}, V_r'\right) = d\left(\alpha_{j_{p_2}}, V_r'\right), \forall r, 1 \leq r \leq N$ dır .

Tanım 2.2 ye göre $I_m$ kümesinin bir parçalanışını elde ederiz. Çünkü bu tanıma göre her eleman bir sınıfa aittir ve farklı iki sınıf ortak eleman içermez. Benzer şekilde Tanım 2.2* ye göre de $I_n$ kümesinin bir parçalanışını elde ederiz. Dolayısıyla aşağıdaki önermeyi yazabiliriz.

**Önerme 2.1.** $I_m$ kümesinin bir parçalanışı $\{V_1', V_2', \dots, V_N'\}$ olsun. Buna göre $\forall \alpha_j, 1 \leq j \leq n$ vektörleri için

$$\sum_{r=1}^{N} d(\alpha_j, V_r') = w(\alpha_j)$$

yazılabilir. Benzer şekilde $I_n$ kümesinin bir parçalanışı $\{V_1, V_2, \dots, V_{N\prime}\}$ olsun. Buna göre $\forall \alpha'_i, 1 \leq i \leq m$ vektörleri için

$$\sum_{r\prime=1}^{N\prime} d(\alpha_i', V_{r\prime}) = w(\alpha_i')$$

yazılabilir.

**Sonuç 2.1.** $I_n$ nin bir parçalanışı $\pi_k^{Col} = \left\{V_1, V_2, \dots, V_{t_k'}\right\}$ olmak üzere $I_m$ nin bir $\pi_{k+1}^{Row} = \{V_1', V_2', \dots, V_{t_{k+1}}'\}$ parçalanışını aşağıdaki gibi tanımlayalım:

$j_1, j_2$ elemanları aynı $V_r'$ , $1 \leq \mathrm{r} \leq t_{k+1}$ sınıfındadır ancak ve ancak $\forall r', 1 \leq r' \leq t_k'$ için $d(\alpha_{j_1}', V_{r\prime}) = d(\alpha_{j_2}', V_{r\prime})$ yazılabilir.

Benzer şekilde $I_n$ nin bir $\pi_{k+1}^{Col} = \{V_1, V_2, \dots, V_{t_{k+1}'}\}$ parçalanışını; $i_1$ , $i_2$ elemanları aynı $V_{r'}$ , $1 \leq \mathrm{r}' \leq t_{k+1}'$ sınıfındadır ancak ve ancak $\forall r, 1 \leq r \leq t_{k+1}$ için $d(\alpha_{i_1}, V_r') = d(\alpha_{i_2}, V_r')$ yazılabilir şeklinde tanımlayalım.

Buna göre başlangıç değeri, $\pi_0^{Col} = \{V_1\}, V_1 = [1,2, \dots, n]$ olarak seçilirse Önerme 2.1. den dolayı, eğer $i$ ve $j$ elemanları başlangıçta farklı sınıflarda iseler daha sonra ki adımlarda da farklı sınıflarda olacaklarından $\pi_{N+1}^{Row} = \pi_N^{Row}$ veya $\pi_{N+1}^{Col} = \pi_N^{Col}$ şartını sağlayan bir $N$ sayısı bulunacaktır. Sonuç olarak verilen $C$ koduna karşılık sırasıyla $I_m$ ve $I_n$ kümelerinin parçalanışlarından oluşan bir

$$\pi_C = \left(\pi_C^{Row}, \pi_C^{Col}\right);\ \pi_C^{Row} = \pi_N^{Row}, \pi_C^{Col} = \pi_N^{Col}$$

parçalanışı elde edilmiş olur.

**Önerme 2.2.** $C$ koduna bir $\sigma \in S_n$ permütasyonu uygulanarak $C'$ kodunun elde edildiğini kabul edelim. Bu durumda $\pi_C = (\pi_C^{Row}, \pi_C^{Col})$ ve $\pi_{C\prime} = (\pi_{C'}^{Row}, \pi_{C'}^{Col})$ olmak üzere

$$\pi_C^{Row} = \pi_{C'}^{Row} \quad \text{ve} \quad \pi_C^{Col} = \sigma(\pi_{C'}^{Col})$$

yazılabilir.

**İspat.** $(\pi_0^{Col})_{C'} = (W_1)$ , $W_1 = [1,2,\dots,n]$ , $(\pi_0^{Col})_C = (V_1)$ , $V_1 = \sigma(W_1)$ olmak üzere $\forall i \in I_m, \forall j \in I_n$ elemanları için $\beta'_{ij} = \alpha'_{i\sigma(j)}$ yazılabilir. Buna göre $d(\beta'_i, W_1) = d\big(\alpha'_i, \sigma(W_1)\big) = d(\alpha'_i, V_1)$ yazılabileceğinden $(\pi_1^{Row})_C = (\pi_1^{Row})_{C'}$ elde edilir. Dolayısıyla $\forall V'_r \in (\pi_1^{Row})_C$ ve $\forall W'_r \in (\pi_1^{Row})_{C'}$ parçalanışları için $V'_r = W'_r$ yazılabilir. $\forall j \in I_n$ elemanı için $\beta_j = \alpha_{\sigma(j)}$ yazılabileceğinden bu sonuca göre $d\big(\beta_j, W'_r\big) = d\big(\alpha_{\sigma(j)}, V'_r\big)$ elde edilir. Dolayısıyla $(\pi_1^{Col})_C = \sigma\big[(\pi_1^{Col})_{C'}\big]$ yazılabileceğinden $\forall V_{r'} \in (\pi_1^{Col})_C$ ve $\forall W_{r'} \in \big(\pi_1^{Col}\big)_{C'}$ parçalanışları için $V_{r'} = \sigma(W_{r'})$ elde edilir. O halde $n = 1$ için hipotezimiz doğrudur.

$n = k$ için hipotezimizin doğru olduğunu varsayalım. Buna göre $\big(\pi_k^{Col}\big)_C = \sigma\left[\big(\pi_k^{Col}\big)_{C'}\right]$ olmak üzere $\forall V_{r'} \in (\pi_k^{Col})_C$ , $\forall W_{r'} \in (\pi_k^{Col})_{C'}$ parçalanışları için $V_{r'} = \sigma(W_{r'})$ yazılabilir. Dolayısıyla $\forall i \in I_m$ için $d(\beta'_i, W_{r'}) = d(\alpha'_i, \sigma(W_{r'})) = d(\alpha'_i, V_{r'})$ yazılabileceğinden $(\pi_{k+1}^{Row})_C = (\pi_{k+1}^{Row})_{C'}$ elde edilir. Sonuç olarak $\forall V'_r \in (\pi_{k+1}^{Row})_C$ , $\forall W'_r \in (\pi_{k+1}^{Row})_{C'}$ parçalanışları için $V'_r = W'_r$ yazılabilir. Buna göre $d\big(\beta_j, W'_r\big) = d\big(\alpha_{\sigma(j)}, V'_r\big)\big)$ yazılabileceğinden $(\pi_{k+1}^{Col})_C = \sigma[\big(\pi_{k+1}^{Col}\big)_{C'}]$ elde edilir. Dolayısıyla $\forall V_{r'} \in \big(\pi_{k+1}^{Col}\big)_C$ , $\forall W_{r'} \in \big(\pi_{k+1}^{Col}\big)_{C'}$ parçalanışları için $V_{r'} = \sigma(W_{r'})$ yazılabileceğinden istenen elde edilir.

Şimdi $\pi^{Row} = \{V_1, V_2, \dots, V_{N'}\}$ ve $\pi^{Col} = \{V'_1, V'_2, \dots, V'_N\}$ parçalanışları üzerinde bir sıralama tanımlayalım.

**Tanım 2.3.** $\forall V_{r'_1}$ , $V_{r'_2} \in \pi^{Row}$, $V_{r'_1} < V_{r'_2} \Leftrightarrow \forall j_1 \in V_{r'_1}$ , $\forall j_2 \in V_{r'_2}$ , $d\big(\alpha_{j_1}, V'_r\big) \neq d\big(\alpha_{j_2}, V'_r\big)$ koşulunu sağlayan en küçük $1 \le r \le N$ sayısı için $d\big(\alpha_{j_1}, V'_r\big) < d\big(\alpha_{j_2}, V'_r\big)$ şartı sağlanır.

**Tanım 2.3*.** $\forall V'_{r_1}$ , $V'_{r_2} \in \pi^{Col}, V'_{r_1} < V'_{r_2} \Leftrightarrow \forall i_1 \in V'_{r_1}$ , $\forall i_2 \in V'_{r_2}$ , $d\big(\alpha'_{i_1}, V_{r'}\big) \neq d\big(\alpha'_{i_2}, V_{r'}\big)$ koşulunu sağlayan en küçük $1 \le r' \le N'$ sayısı için $d\big(\alpha'_{i_1}, V_{r'}\big) < d\big(\alpha'_{i_2}, V_{r'}\big)$ şartı sağlanır.

**Sonuç 2.2.** Önerme 2.2. ye göre, denk $C$ ve $C'$ kodları verildiğinde $\forall V_{r_1}, V_{r_2} \in \pi_C^{Col}$ parçalanışları için $V_{r_1} < V_{r_2}$ ise $\forall j'_1 \in W_{r_1}$ , $\forall j'_2 \in W_{r_2}$ elemanları için $j_1 = \sigma(j'_1) \in V_{r_1}$ ve $j_2 = \sigma(j'_2) \in V_{r_2}$ olmak üzere

$d\big(\beta_{j'_1}, W'_r\big) = d\left(\alpha_{\sigma(j'_1)}, V'_r\right) = d\big(\alpha_{j_1}, V'_r\big) < d\big(\alpha_{j_2}, V'_r\big) = d\left(\alpha_{\sigma(j'_2)}, W'_r\right) = d\big(\beta_{j'_2}, W'_r\big)$

$\Longrightarrow W_{r_1} < W_{r_2}$

yazılabileceğinden parçalanışlar üzerinde tanımladığımız sıralamanın permütasyon altında korunduğunu söyleyebiliriz.

**Sonuç 2.3.** $C$ ve $C'$ gibi iki kod verildiğinde $\pi_C^{Row}$ ve $\pi_{C'}^{Row}$ parçalanışlarının aynı olup olmadığına bakılarak bu iki kodun denk olup olmadıkları hakkında tahminde bulunulabilir. Eğer bu iki kod denk ise $\pi_C^{Col}$ ve $\pi_{C'}^{Col}$ parçalanışları kullanılarak $M$ ve $M'$ matrislerinin sütun vektörleri karşılaştırılırsa aradaki permütasyon bulunabilir. Şimdi bunu bir örnekle açıklayalım.

**Örnek 2.1** $C = \{100110, 010110, 011001, 101010, 011001, 001011\}$ şeklinde bir $C$ kodu verilmiş olsun. Buna göre kod sözleri alt alta yazarsak aşağıdaki $M$ matrisini elde ederiz.

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

$M$ matrisine algoritmayı uygularsak;

$\boldsymbol{k = 0}$:
$\pi_0^{Col} = ([1,2,3,4,5,6])$

$\boldsymbol{k = 1}$:
$d(*, V_1) = 3,3,3,3,3,3 \quad \Longrightarrow \quad \pi_1^{Row} = ([1,2,3,4,5,6])$
$d(*, V_1') = 2,3,4,2,4,3 \quad \Longrightarrow \quad \pi_1^{Col} = ([1,4],[2,6],[3,5])$

$\boldsymbol{k = 2}$:
$d(*, V_1) = 2,1,0,1,0,0$
$d(*, V_2) = 0,1,2,0,2,1 \quad \Longrightarrow \quad \pi_2^{Row} = ([6],[3,5],[4],[2],[1])$
$d(*, V_3) = 1,1,1,2,1,2$

$d(*, V_1') = 0,0,1,0,1,1$
$d(*, V_2') = 0,2,2,0,0,2$
$d(*, V_3') = 1,0,1,0,1,0 \quad \Longrightarrow \quad \pi_2^{Col} = ([4],[1],[2],[5],[6],[3])$
$d(*, V_4') = 0,1,0,1,1,0$
$d(*, V_5') = 1,0,0,1,1,0$

$\Longrightarrow \pi_C^{Row} = ([6],[3,5],[4],[2],[1]) \quad , \quad \pi_C^{Col} = ([4],[1],[2],[5],[6],[3])$

olarak bulunur. Burada $d(*, V_j)$ veya $d(*, V_i')$ ifadelerinde "*" ile tüm sütun veya satır vektörleri ifade edilmektedir. $C' = \{010011, 011001, 101100, 110010, 101100, 110100\}$ şeklinde $C'$ kodu verilmiş olsun. Buna göre kod sözleri alt alta yazarsak aşağıdaki $M'$ matrisini elde ederiz.

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

$M'$ matrisine algoritmayı uygularsak;

$\boldsymbol{k = 0}$:

$\pi_0^{Col} = ([1,2,3,4,5,6])$

$\boldsymbol{k = 1}$:

$d(*, V_1) = 3,3,3,3,3,3 \implies \pi_1^{Row} = ([1,2,3,4,5,6])$

$d(*, V_1') = 4,4,3,3,2,2 \implies \pi_1^{Col} = ([5,6],[3,4],[1,2])$

$\boldsymbol{k = 2}$:

$d(*, V_1) = 2,1,0,1,0,0$

$d(*, V_2) = 0,1,2,0,2,1 \implies \pi_2^{Row} = ([6],[3,5],[4],[2],[1])$

$d(*, V_3) = 1,1,1,2,1,2$

$d(*, V_1') = 1,1,0,1,0,0$

$d(*, V_2') = 2,0,2,2,0,0$

$d(*, V_3') = 1,1,0,0,1,0 \implies \pi_2^{Col} = ([6],[5],[3],[2],[4],[1])$

$d(*, V_4') = 0,1,1,0,0,1$

$d(*, V_5') = 0,1,0,0,1,1$

$\implies \pi_C^{Row} = ([6],[3,5],[4],[2],[1]) \quad , \quad \pi_C^{Col} = ([6],[5],[3],[2],[4],[1])$

yazılabilir. Dolayısıyla $k = 0,1,2$ için $(\pi_k^{Row})_{C'} = (\pi_k^{Row})_C$ yazılabileceğinden bu iki kodun denk olduğu tahmininde bulunabiliriz. Buna göre $\pi_C^{Col}$ ve $\pi_{C'}^{Col}$ parçalanışları karşılaştırılırsa

$\sigma(1) = 3$ , $\sigma(2) = 5$ , $\sigma(3) = 2$ , $\sigma(4) = 6$ , $\sigma(5) = 1$ , $\sigma(6) = 4$

yazılabileceğinden $\sigma = (1\ 3\ 2\ 5)(4\ 6)$ olarak $\sigma$ permütasyonu bulunmuş olur.

## IV. SONUÇ

$C$ ve $C'$ gibi iki kod verildiğinde bu kodların kod sözlerini alt alta yazmak suretiyle elde edilen matrisler yardımıyla kodların denk olup olmadığı tespit edilerek eğer denk iseler yine bu matrisler yardımıyla aradaki permütasyon bulunabilir.

## V. KAYNAKLAR


[1] R. J. McEliece The Deep Space Network Progress Report **(42-44)** (1978) 114-116.

[2] E. Petrank , R. M. Roth. IEEE Transactions on Information Theory **43(5)** (1997) 1602-1604.

[3] N. Sendrier IEEE Transactions on Information Theory **46(4)** ( 2000) 1193-1203.

[4] T. Shaska, W. C. Huffman, Advances in Coding Theory and Cryptography, World Scientific Publishing Co. Pte. Ltd., (2007)

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