Bölüm 4

Sonlu Cisimler Üzerinde Golay ve Hamming Kodları

Mustafa Özkan[1]

Elif Bıyıklı[2]

Özet

Bu çalışma kapsamında genel olarak şu konulara değinilmiştir. Öncelikle kodlama teorisi hakkında bazı genel bilgilere yer verilmiştir. Kodlama türlerinden bahsedilerek haberleşme sisteminde kodlama teorisinin önemine değinilmiştir. Kodlama teorisi dalında özellikle matematiğin farklı alanları ile bağlantı oluşturarak, iletilecek verilerin transfer sürecinde ve saklanması sürecinde dış etkenler sonucu oluşabilecek tüm bozulmaları engellemek adına çeşitli çalışmalar yapılmıştır.

Golay Kodların tarihçesi ile Voyager Programı kapsamında Satürn ve Jüpitere fırlatılan uzay araçları ile Dünya arasında veri iletiminin sağlanması konusunda bu kodların önemine yer verilmiştir. Sonra Golay Kodların tanımı yapılarak İkili ve üçlü Golay Kodların özellikleri üzerinde durulmuştur. İkili Golay Koddijital iletişim sistemlerinde kullanılan bir tür doğrusal hata düzeltme kodu olarak geliştirilmiştir. Daha sonra Hamming Kodların tanımına ve özelliklerine yer verilmiş olup örneklerle açıklamalar yapılmıştır. Bilgisayarda verilerin iletimi esnasında oluşabilecek bozulmalara karşı gönderilen verilere ilave bitler eklenerek hataların tespit edilmesi hatta düzeltilmesi amaçlanmaktadır. Bu çalışmada Golay ve Hamming Kodların temel tanım ve önemli teoremlerine ispatlarıyla birlikte yer verilmiştir. Ayrıca Mükemmel Kod tanımına değinilerek Golay Kodlar ve Hamming Kodların birer Mükemmel Kod olduğu kanıtlanmıştır. Bu kodlar iletişim sistemlerinde oluşabilecek hataların düzeltilmesinde oldukça başarılı sonuçlar vermektedir.

[1] Dr. Öğr. Üyesi, Trakya Üniversitesi, Matematik ve Fen Bilimleri Eğitimi Bölümü, mustafaozkan@trakya.edu.tr, https://orcid.org/0000-0001-7398-8564

[2] Yük. Lis. Öğr. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, elifbiyikli23@gmail.com, https://orcid.org/0009-0007-9844-0344

https://doi.org/10.58830/ozgur.pub165.c891

SONLU CİSİMLER ÜZERİNDE GOLAY VE HAMMINGKODLARI

1. KODLAMA TEORİSİNE GİRİŞ

Kodlama teorisinin miladı olarak Claude Shannon'un 1948 yılında yayınlamış olduğu 'A Mathematical Theory of Communication' isimli makalesi kabul edilir. Başlangıç sayılan bu teoriden sonra kodlama teorisi gürültü kanalları boyunca güvenilir, hızlı veri iletimi ve veri iletimi sırasında bozulmaya uğrayan mesajı düzeltme gibi konular üzerinde durmuştur. Kodlama teorisi, kodların özelliklerini ve bunların belirli uygulamalar için uygunluğunu inceleyen bir teoridir.

Kodlama türleri dörde ayrılır;

1. Veri Sıkıştırma
2. Kanal kodlama
3. Gizlilik Kodlama
4. Hat Kodlama

1. Veri Sıkıştırma (Kaynak Kodlama)

Verimlilik esasına dayalı olarak kaynak simgelerinin en düşük yapıda nasıl temsil edileceği problemidir. ASCII kodlaması kaynak kodlamaya en temel örnek olarak verilebilir. Her bir karakteri 8 bitlik byte'a çevirir.

2. Kanal Kodlama (Hata Düzeltme)

Kaynak simgelerinin birbirlerinden uzak olacak şekilde nasıl gösterileceği problemidir. Meydana gelebilecek küçük değişikliklere(gürültü) rağmen sonuçta değişen simgelerin fark edilmesi ve hataları düzeltebilmesi mümkün olmaktadır. Hamming Kodlar, Reed Solomon Kodlar, BCH kodlar, Reed Müller kodlar vs.

3. Gizlilik Kodlama(Şifreleme-Kriptografi)

Şifreleme bunlardan farklı olarak gönderilen veriyi çeşitli algoritmalara göre bir anahtar ile karmaşık hale getirmektir. Böylece kanal boyunca iletilen kod sözcüklerinin bozulmaya uğrama oranları azalır. Örneğin RSA, DES, AES gibi şifreleme algoritmaları bunlara örnek verilebilir.

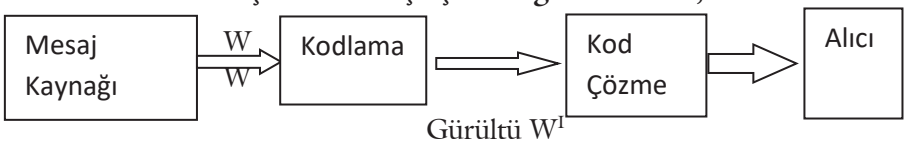
4. Hat Kodlama

İletim ortamının özelliklerine göre iletilecek olan işareti uygun hale getirip, bozucu dış etkenlerden minimum düzeyde etkilenebilecek şekilde ve en az bant genişliği kullanabilecek biçimde oluşturma işlemidir.

Kodlar, verimli ve güvenilir bir şekilde veri aktarım yöntemlerinin oluşturulması amacıyla çeşitli bilimsel disiplinler tarafından incelenir. Birçok bilim dalında kodlama teorisi önemli bir yere sahiptir. Bunlardan bazılarını şöyle sıralayabiliriz:

- Matematik
- Bilgisayar Bilimleri,
- Bilgi Teorisi,
- Elektrik-Elektronik Mühendisliği
- Haberleşme alanında

Basit bir haberleşme sistemi şu şekilde gösterilebilir;



Şekil 1. Hata Doğrulama

Günlük hayatın vazgeçilmez bir bütünü haline gelen iletişim sistemlerinde, hatasız ve hızlı bilgilerin iletiminin gerekliliği önemli bir konu olarak karşımıza çıkar. Haberleşme sistemlerinde bilgilerin iletilebilmesi için vericiden gönderilen mesaj işareti, işaretin gönderildiği kanaldan ve ayrıca verici ile alıcı devrelerinden kaynaklı olacak şekilde işareti bozucu dış etkilerden dolayı, bozulmaya uğrar ve dolayısıyla alıcıdan gönderilenden farklı bir bilgi alınabilir. Bu durum haberleşme sisteminin hatalı mesaj göndermesi olarak ifade edilir. Kodlama teorisinin amacı, dijital bilginin iletilmesi veya saklanması esnasında oluşabilecek hataları tespit etmek, eğer hatalar oluşmuş ise bu hataları düzeltmektir.

2. GOLAY KODLAR

Golay Kodlar 1940'ların sonlarında Marcel J.E. Golay tarafından keşfedilmiştir. Marcel Golay matematiğin gerçek dünyadaki uygulamalarına yaptığı katkılarla tanınan başarılı bir matematikçi ve bilgi teorisyenidir. Golay mükemmel kodları aradı. Matematikçilerin çok ilgisini çeken mükemmel kodlar en iyi kodlar olarak adlandırılır. Golay kodları da mükemmel kod örnekleridir. Görünüşe göre Golay Kodları ikili ve üçlü kodların olması anlamında esasen benzersizdir. Onlarla aynı parametrelerle onlara eşdeğer gösterilebilirler.

Tanım2.1 ([4]) : G, 12x24 matris olsun.

$$G = (I_{12}\,/A)$$

I_{12} 12×12 birim matris ve A 12×24 matris olsun. Üreteç matrisi G olan ikili doğrusal koda genişletilmiş ikili Golay Kodu denir ve G_{24} ile gösterilir. Aynı zamanda üreteç G matrisli doğrusal koda denk olan diğer tüm kodlara da genişletilmiş ikili Golay Kodu denir. Burada A matrisi şu şekildedir.

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Genişletilmiş ikili Golay Kodu Nasa tarafından yürütülen Voyager programı kapsamında kullanıldı. Voyager1 ve Voyager2 uzay araçları 1977 de Jüpiter ve Satürn'e doğru fırlatılmış olup gezegenlere ait uyduların ayrıntılı fotoğraflarını elde eden ilk çalışma olmuştur. Voyager günümüzde Dünya'ya veri iletmek amacıyla düzenli ve etkin biçimde komutları almak için derin uzay ağı ile iletişim kurmaya devam etmektedir.

Önerme 2.1 ([4]): Genelleştirilmiş ikili Golay Kodun özellikleri;

i. G_{24}'ün uzunluğu 24 ve boyutu 12'dir.

ii. G_{24} için bir parite kontrol matrisi 12×24 matrisidir.
$H = (A\,/I_{12})$

iii. G_{24} kodu bir kendi-dual koddur. Yani;
$$G_{24}^{\perp} = G_{24}$$

iv. G_{24} için başka bir eşlik kontrol matrisi 12×24 matrisidir.
$$H' = (I_{12}/A) \quad (= G)$$

v. G_{24}için başka bir üreteç matrisi 12×24 matrisidir.
$$G' = (A/I_{12}) \quad (= H)$$

vi. G_{24}' teki her kod sözcüğünün ağırlığı 4'ün katıdır.

vii. Ağırlığı 4 olan kod sözcüğü G_{24}' de yoktur. Bu nedenle G_{24}'ün mesafesi d=8 dir.

viii. G_{24} kodu tam olarak üç hata düzeltme kodudur.

Kanıt ([4]):

i. Tanımdan anlaşılmaktadır.

ii. Teorem: Eğer $G = (I_k/X)$ standart form oluşturucu matris ise [n,k]-kodu C ise o zaman C için bir parite kontrol matrisi $H = (X^T/I_{n-k})$ olur.

İspat: $H.G^T = 0$ denklemi sağlanır.

Son $n-k$ koordinat dikkate alınarak H satırlarının doğrusal olarak bağımsız olduğu açıktır.

iii. G matrisinin satırlarının ortogonal (dik olduğuna) dikkat edelim yani; r_i ve r_j satırları için $r_i \cdot r_j = 0$ dır. Bu G_{24}alt kümesi veya eşittir $G_{24}^{\perp}$ anlamındadır. G_{24} ve $G_{24}^{\perp}$ boyutları 12'dir. $G_{24} = G_{24}^{\perp}$ dir.

iv. G'_{24}ün bir parite kontrol matrisi $G_{24} = G_{24}^{\perp}$ 'ün bir üretici matrisidir. G böyle bir matristir.

v. G'_{24}ün bir üretici matrisi $G_{24} = G_{24}^{\perp}$ ' ün bir parite kontrol matrisidir. H böyle bir matristir.

vi. vG'de bir kod sözcüğü olsun. $wt(v)'$nin 4'ün katı olduğunu göstermek istiyoruz. v' nin G'nin satırlarının lineer bir kombinasyonu olduğuna dikkat edelim. r_i G'nin i. satırını göstersin.

İlk olarak v'nin G'nin satırlarından biri olduğunu varsayalım. G' nin ağırlığı 8 veya 12 olduğundan v' nin ağırlığı 4'ün katıdır. Sonra v G' nin iki farklı satırının toplamı olsun. $(r_i + r_j)r_i$ ve r_j ağırlıkları 4'e bölünebilir olduğundan $(r_i + r_j)$ de 4'ün katıdır.

Bu şekilde tümevarımla devam edilerek ispatı bitirebiliriz.

vii. G'nin son satırının ağırlığı 8 olan bir kod sözcüğü olduğuna dikkat edelim. Bu gerçekle birlikte önermenin (vi). ifadesi ile d=4 veya 8 olduğunu ima eder.

G_{24} 'ün $wt(v) = 4$ olan sıfır olmayan bir v kod sözcüğü içerdiğini varsayalım. v'yi $(v_1 + v_2)$olarak yazalım. Burada v_1 ilk 12 koordinattan oluşan (12 uzunluğunda) vektördür ve v_2 , son 12 koordinattan oluşan (12 uzunluğunda) vektördür. O zaman aşağıdaki durumlardan biri gerçekleşmelidir.

Durum 1: $wt(v_1) = 0$ ve $wt(v_2) = 4$ olsun. (Ağırlık 0 ve 4)

Bu muhtemelen olamaz çünkü, üreteç matrisi *G*'ye bakıldığında bu türden tek kelime 0'dır ağırlık 0'dır.

Durum2: $wt(v_1) = 1$ ve $wt(v_2) = 3$

Bu durumda yine *G*' ye bakılarak v, *G*'nin satırlarından biri olmalıdır ki; Bu da yine bir çelişkidir.

Durum 3: $wt(v_1) = 2$ ve $wt(v_2) = 2$

O halde v, *G* 'nin iki satırının toplamıdır. Bu tür toplamlarda hiçbirinin $wt(v_2) = 2$ vermediğini kontrol etmek kolaydır.

Durum 4: $wt(v_1) = 3$ ve $wt(v_2) = 1$

G' bir üreteç matrisi olduğundan v G' nün satırlarından biri olmalı, bu açıkça çelişki veriyor.

Durum 5 : $wt(v_1) = 4$ ve $wt(v_2) = 0$

Bu durumda *G* yerine G' kullanılınca durum 1'e benzer.

Tüm bu durumlarda çelişkiler elde ettiğimiz için d=4 imkânsızdır. Böylece d=8 olur.

viii. Teorem: Bir *C*-Kodu, ancak ve ancak $\mathrm{d}(C) \geq 2v + 1$ ise v-hatası düzelticidir. Yani; d mesafesine sahip bir kod tam olarak $(d - 1)/2$ hata düzeltme kodudur. Dolayısıyla tam olarak 3 hata düzeltme kodudur.

Tanım 2.2 : $\hat{G}$; 12×23 matris olsun.

$\hat{G} = (I_{12}/\hat{A})$

Burada I_{12}; 12×12 birim matristir.

$\hat{A}$, *A*'nın son sütunu silinerek elde edilen 12×11 ' lik matristir. Üreteç matrisi $\hat{G}$ olan ikili doğrusal koda bir ikili Golay Kodu adı verilir. G_{23} ile gösterilir.

G_{24}' te ki her kod kelimesinin son koordinatı silinerek elde edilen ikili Golay Kodu alternatif kod olarak tanımlanabilir.

İkili Golay Kodun Özellikleri

i. G_{23}'ün uzunluğu 23 ve Boyutu 12'dir.

ii. G_{23} için bir parite kontrol matrisi 11×23 matris $\hat{H} = (\hat{A}^T/I_{11})$

iii. G_{23}'ün genişletilmiş kodu G_{24}'tür.

iv. G_{23}'ün mesafesi d=7 dir.

v. G_{23} kodu tam olarak üç hata düzeltme kodudur.

Üçlü Golay Kod

Tanım 2.3 : B'nin 6×6 'lık matris olduğu, üreteç matrisi $G = (I_6/B)$ olan üçlü doğrusal kod olarak G_{12}'den genişletilmiş koda üçlü Golay Kod denir.

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

Not: Yukarıdaki koda denk olan herhangi bir doğrusal kod genişletilmiş üçlü Golay Kodu olarak da anılır.

Tanım 2.4 : Üçlü Golay Kodu G_{11}, G_{12}'yi son koordinatta delerek elde edilen koddur. G_{11} 'in Hamming sınırını karşıladığını ve bu nedenle mükemmel bir üçlü $[11, 6, 5]$ kodlu olduğunu doğrulayabiliriz.

Mükemmel Kodlar

Tanım 2.5 ([9]): Eğer q'lu bir kod Hamming sınırına ulaşabilirse yani;

$$M = \frac{q^n}{V_q^n(\left\lfloor \frac{d-1}{2} \right\rfloor)}$$

Eşitliğini sağlayan kodlara mükemmel kod denir.

Mükemmel olan üç tane ikili kod vardır. Bunlar; Tekrarlı Kod, Hamming Kodları ve Golay Kodlardır.

Lemma 2.1 ([9]) : $G_{23} = [23,12,7]$ parametreli kod, mükemmel koddur.

Kanıt ([9]) : $M = \frac{2^n}{V_2^n(3)}$ eşitliği sağlanırsa bu kod mükemmeldir.

$$V_2^n(3) = \binom{23}{0} + \binom{23}{1} + \binom{23}{2} = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

$$M = 2^{12} = \frac{2^{23}}{2^{11}} = \frac{2^n}{V_2^n(3)}$$

Böylece G_{23} kodu mükemmeldir.

3. HAMMING KODLAR

Richard Hamming tarafından 1940'lı yılların sonunda icat edilen Hamming Kod lineer hata düzelten bir koddur. Hamming Kodları tek bitlik hataları saptayıp düzeltebilirken iki bitlik hataları da tespit edebilir. Her veri kelimeleri üzerinde bir çok sayıda eşitlik denetimi gerçekleştirilerek Hamming Kodlama yapılır. Eşitlik denetimine ilişkin ek bitler veri kelimesi ile birlikte gönderilir. Herhangi bir $GF(q)$ sonlu cismi üzerinde tanımlanabilmektedir. Hamming kodu en uygun biçimde, eşlik-denetim (parity-check) matrisi ile belirtilir.

Tanım 3.1 ([6]): *r*, sıfırdan büyük bir tam sayı ve *H*; sütunları, $(F_q)^n$ in vektörleri sıfırdan farklı olan bir $r \times (2^r - 1)$ şeklinde matris olsun. *H* eşlik denetim matrisi olan bir koda, ikili (binary) Hamming kodu denir. Ham $(r, 2)$ ile gösterilir.

1. Ham $(r, 2)$ kodunun uzunluğu $n = 2^r - 1$, boyutu $k = n - r$ şeklindedir. Burada $r = n - k$, her bir kod sözcüğündeki kontrol sembollerinin sayıdır.
2. *H* nin sütunları karışık bir sırada alınabileceğinden, verilen *r* tane tamsayı için Ham $(r, 2)$ kodu, denk kodlardan biridir.
3. İkili Hamming Ham $(r, 2)$ kodu, bir $[\, 2^r - 1, 2^r - 1 - r, 3\,]$ koddur.

Teorem 3.1 ([6]) : İkili Hamming Kod Ham $(r, 2)$, $r \geq 2$ için;

1. Bir $[\, 2^r - 1, 2^r - 1 - r\,]$ - koddur.
2. Minimum uzaklığı 3'tür. (Bu yüzden tek hata düzeltir.)
3. Bir yetkin koddur.

Örnek 3.1 : $r = 3$ için Ham(3,2) yi oluşturalım.

$(GF(2))^3$ sıfırdan ve birbirlerinden farklı vektörlerini sütunlara yazarak bir H matrisi oluşturalım.

$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{3\times 7}$ olsun bu matriste elementer satır işlemleri yaparak *H* matrisini standart formda yazalım.

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}_{3\times 7} \xrightarrow{r_1 \to r_1 + r_2} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{r_3 \to r_1 + r_3}$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{r_2 \to r_2 + r_3} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \text{ olur.}$$

Buna göre;

$$-A^T = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}_{3\times 4} , \quad A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}_{4\times 3}$$

Olur. Buradan,

$$G = [I_k/A] = [I_4/A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{4\times 7}$$

Matrisini buluruz. Böylece Ham(3,2) bir [7,4,3]-koda denktir.

Örnek 3.2 : $r = 3$ alınırsa

$(2^3 - 1, 2^3 - 1 - 3, 3) = (7,4,3)$ Kodu elde edilir.

Bu kodun Hamming sınırı hesaplanırsa

$$2^4 \sum_{i=0}^{1} \binom{7}{i} = 2^4 (1 + 7) = 2^7$$

Bu durumda (7,4,3) Hamming kodu mükemmel bir koddur.

Örnek 3.3 : 11000100 sekiz bitlik veri sözcüğümüz olsun. Hamming Kodların parity-check bitleri bulunarak nasıl hesaplandığını ve hatayı nasıl tespit ettiklerini gösterelim. İlk olarak kaç parity bitimizin olduğunu bulalım;

$m + r + 1 \leq 2^r$ (m verimizin kaç bitlik olduğunu temsil ederken r ise kaç parity bit kullanacağımızı temsil eder)

$8 + r + 1 \leq 2^r$

$9 + r \leq 2^r$

$r = 4$ (kaç parity bit olacağını ifade eder.)

Şimdi de kod kelimemizin kaç bitli olacağını bulalı;

$n = m + r$

$n = 8 + 4$

$n = 12$ (Hatayı bulmak için gönderilen kod kelimemizin bit sayısıdır.)

Part bitlerimiz 2^n şeklinde yazılabilecek yerlerde bulunmalı.

p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}
?	?	1	?	1	0	0	?	0	1	0	0

2^0 2^1 2^2 2^3

$p_1 = (3,5,7,9,11) = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$p_2 = (3,6,7,10,11) = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$p_4 = (5,6,7,12) = 1 \oplus 0 \oplus 0 \oplus 0 = 1$

$p_8 = (9,10,11,12) = 0 \oplus 1 \oplus 0 \oplus 0 = 1$

001110010100 bu 12 bitlik veri bizim yeni verimizdir.

p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}
0	0	1	1	1	0	0	1	0	1	0	0

2^0 2^1 2^2 2^3

Şimdide check bitlerimizi bulacağız;

$c_1 = (1,3,5,7,9,11) = 0 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$c_2 = (2,3,6,7,10,11) = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 = 0$

$c_4 = (3,4,5,9,10,11) = 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$

$c_8 = (4,5,6,7,12) = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$C = c_8 c_4 c_2 c_1 \Longrightarrow 0000$; $C = 0$Olduğundanhata yoktur.

Eğer $C \neq 0$ Hata vardır. *C*'nin değeri hatanın yerini gösterir.

Örneğin $C = 0101$ olsaydı $2^2 + 2^0 = 5$'tir. Bu da bize 5. bitte hata olduğunu gösterirdi.

Teorem3.2 : $GF(q)$ üzerinde eşlik- denetim matrisi *H* olan bir doğrusal kod, *C* olsun. *C*'nin en küçük mesafesinin (uzaklığının) d olması için gerek ve yeter koşul; *H* nin sütunlarından seçilen her $(d-1)$ tane sütununun determinantı sıfırdan farklı yani lineer bağımsız, fakat lineer bağımlı d tane sütunun var olmasıdır.

Ham (r, q) nun Oluşturulması

Lineer bir $[n, n-r, 3]$ şeklinde kod kurmaya çalışalım.

Burada $d = 3$ alınmıştır. Yani *C*'nin, minimum mesafesi 3 olan bir kod olması için, *H* nin her sütun ikilisi, $(d-1 = 3-1 = 2\ olduğundan)$ lineer bağımsız olmak zorundadır. O zaman *H* nin sütunları sıfırdan farklı ve biri, diğerinin skaler katı olmamalıdır. (Skaler dediğimiz, $GF(q)$ nun elemanlarıdır.)

$(F_q)^r = (GF(q))^r$ nin $q^r - 1$ tane elemanı sıfırdan farklıdır. Bunlar içerisinde; biri diğerinin skaler katı olmayanların sayısı ise, $\frac{q^r-1}{q-1}$ 'dir.

$\frac{q^r-1}{q-1}$ tane vektör, sütunlara yazılarak H matrisi oluşturulur.

Örnek 3.4 : Ham (2, 7) için;

$r = 2\,,\ q = 7$ dir.

$$\frac{q^r-1}{q-1} = \frac{7^2-1}{7-1} = 8$$

Tane, birbirlerinin skaler katı olmayacak, sıfırdan farklı vektör vardır. Bunlar Sütunlara yazılarak H matrisini oluştururuz.

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \xrightarrow{r_1 \to r_1 + r_2}$$

$$= \begin{bmatrix} 1 & 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \xrightarrow{r_1 \to (-1) r_1}$$

$$= \begin{bmatrix} 6 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \xrightarrow{r_2 \to (-1) r_2}$$

$$= \begin{bmatrix} 6 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 6 & 0 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \xrightarrow{r_2 \to r_2 - 2r_1}$$

$$= \begin{bmatrix} 6 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 1 \end{bmatrix}$$

Buradan;

$$-A^T = \begin{bmatrix} 6 & 6 & 5 & 4 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}$$

$$-A = \begin{bmatrix} 6 & 1 \\ 6 & 2 \\ 5 & 3 \\ 4 & 4 \\ 3 & 5 \\ 2 & 6 \end{bmatrix}, \qquad A = \begin{bmatrix} 1 & 6 \\ 1 & 5 \\ 2 & 4 \\ 3 & 3 \\ 4 & 2 \\ 5 & 1 \end{bmatrix}$$

Matrisleri elde edilir.

$$G = \left[\begin{array}{cc} 1 & 1 \\ 1 & 2 \\ I_4 : 2 & 3 \\ 3 & 4 \\ 4 & 5 \\ 5 & 6 \end{array}\right]_{4\times 6} \text{ şeklindedir.}$$

KAYNAKÇA

[1] M. J. E. Golay, "Notes on digital coding," Proceedings of the IRE, vol. 37, no. 6, p. 657, 1949.

[2] E. R. Berlekamp, "Decoding the Golay code," JPL Technical Report, vol. 32-1526, pp. 81–85, 1972.

[3] Raymond Hill, "A First Course in Coding Theory", Oxford Unv Press, 1986.

[4] S. Ling and Chaoping Xing "Coding Theory A First Course", Cambridge Unv Press, 2004.

[5] S. Roman, "Coding and Information Theory", Graduate Text in Mathematics, Springer Verlag, 1992.

[6] M. ÖZKAN and F. ÖKE "On Gray Images of Constacyclic Codes" ITM Web of Conf., Volume: 22, pp: 01047-1-6, doi : 10.1051/itmconf/20182201047, 2018.

[7] J. Hamkins, "The Golay Code Outperforms the Extended Golay CodeUnder Hard-Decision Decoding" ,arXiv:1602.05620v1, arXiv. Org, 2018.

[8] M. Özkan, B. Yenice and A. T. Güroglu "Constacyclic and Negacyclic Codes over F2 + uF2 + vF2 and their Equivalents over F2" Fundamental Journal of Mathematics and Applications (FUJMA), Vol :5 (4), pp: 228-233, ISSN: 2645-8845, doi:10.33401/fujma.1124502,2023.

[9] İ.Kalkan 'Rank Metrıc and Codes 'Graduate Text in Mathematics 2012.