Kablosuz Kanallarda Kodlama

İrfan Köprücü

Ana Başlıklar

- Giriş
- Linear Block Codes
- Cyclic Codes
- BHC Codes

Giriş

- Hata düzeltme kodları:
  - Gürültülü kanallarda mesajlar iletilirken
  - Belli bir yerde tutulan veri aktarılırken

- Gürültü, ısıl(Thermal noise) olabilir, bir ışıma sebebiyle oluşmuş, insan hatalarından kaynaklanıyor, ekipmanın yanlış işlerliğinden, ya da voltaj dalgalanmalarından meydana gelebilir.
- Hataları bulup düzeltmek için Hata Kontrol Kodlaması başka bir isimle Kanal kodlaması(Channel Coding) yapılır.

Kanal Kodlama Ana Fikri

- Mesaja, gürültülü kanal üzerinde iletimi öncesi belli bir oranda fazlalık kod eklenir.
- Temelde fazladan sembollerden oluşan bu fazlalık bilinen şekle eklenir.

Kanal Kodlayıcılı Dijital bir iletim sistemi

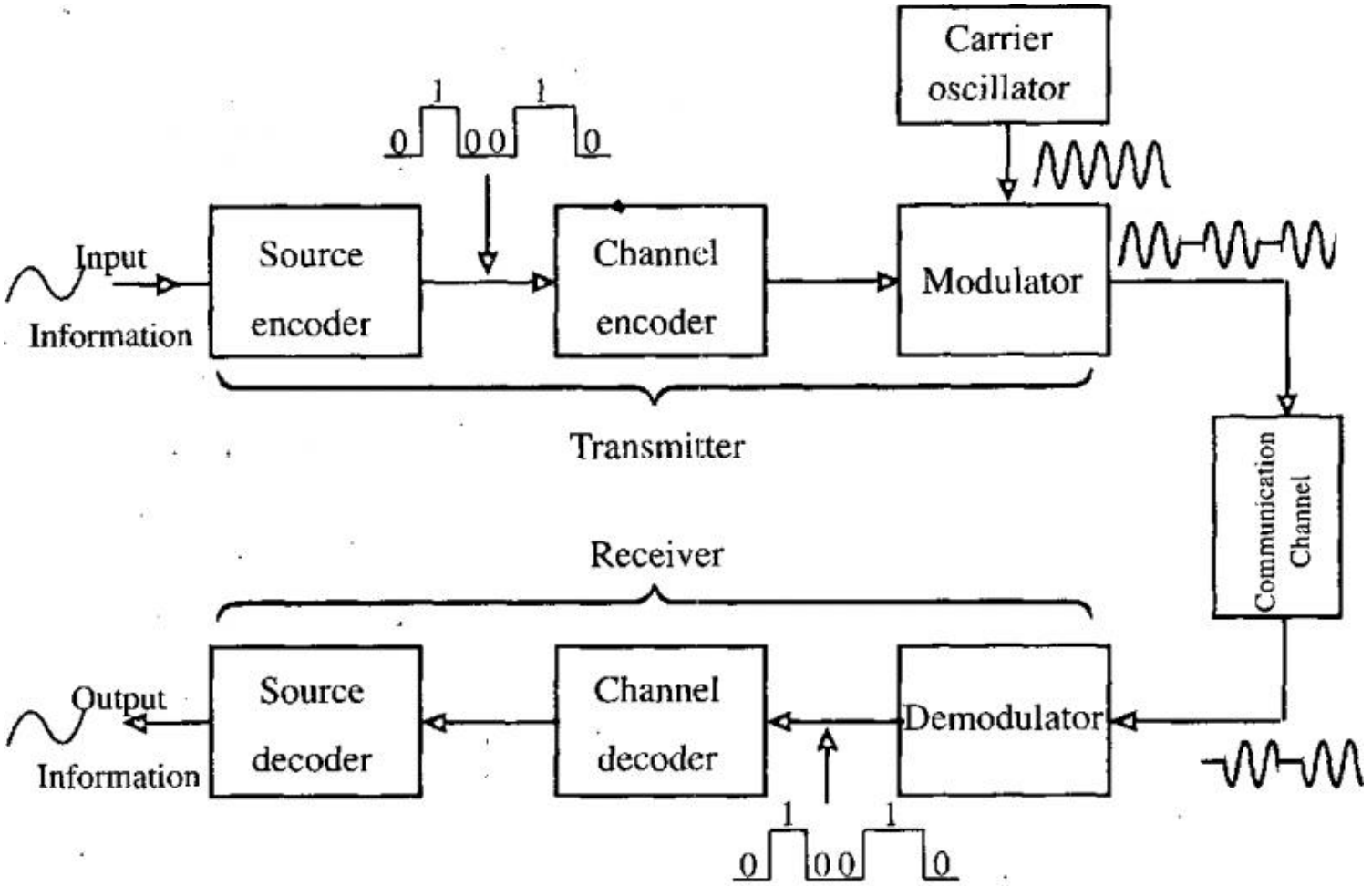


Fig. 16.6

Tanımlar

- Kelime(*Word*) sembollerin dizisidir.
- Kod*(Code)* şifre*(codewords)* denen bir vektörler kümesidir.
- Bir şifrenin Hamming Ağırlığı şifrenin içinde bulunan sıfır olmayan elemanların sayısına eşittir ve *w(c)* ile gösterilir.
- İki şifre arasında ki Hamming Uzaklığı şifrelerin farklı olduğu yerlerin sayısıdır. c_1 ve c_2 iki şifre olmak üzere aralarında ki Hamming Uzaklığı $d(c_1, c_2)$ ile gösterilir ve *d(c1, c2)=w(c1-c2)* olduğu kolayca görülebilir.
- Örneğin: w(10110)=4 ve d(10110, 11011) =3.

Blok Kodlar(Block Codes)

- Bir blok kod sabit uzunlukta şifrelerin kümesinden oluşur.
- Bu kodların uzunluğu olan sabit uzunluğu blok uzunluğu denir ve genellikle *n* ile gösterilir.
- A blok code of size *M* defined over an alfabet with q sembols is a set of *M* q-ary sequences, each of length n
- In the special case that $q=2$, the symbols are called bits and the code is said to be a binary code. Usually, $M=q^k$ for some integer k, and we call such a code an *(n, k)* code.

Tanımlara devam edelim …

- İki şifre arasında ki en düşük Hamming Uzaklığına şifrelerin Asgari Uzaklığı denir.
- C{c_i, i =0, 1, … , M-1} şifre kümesinden oluşan bir C kümesi için kodun asgari uzaklığı $d^*=min\ d(c_i, c_j)\ i\neq j$ dir.
- The code rate of an (n, k) code is defined as the ratio (k/n), and reflects the fraction of the codeword that consist of the information symbols.

Örnek

- Blok kod C={00000, 10100, 11110, 11001} iki bitlik ikili sayıları göstermek için kullanılabilir.
  - Kodlanmamış Bitler — Şifreler
    - 00 — 00000
    - 01 — 10100
    - 10 — 11110
    - 11 — 11001
- Burada *M=4, k=2* ve *n=5* olur.
- Bit akımını çözmek için 1001010011…
  - İlk adımda bitleri ikişerli gruplarız. 10 01 01 00 11 …
  - İkinci adımda uygun şifreler yerlerine yazılır.
  - 11110 10100 10100 00000 11001 …
- Asgari uzaklık $d^* = min\ d(c_i, c_j) = 2$.

Doğrusal Blok Kodlar(Linear Block Codes)

- Doğrusal kodun özellikleri
  - Bir koda ait olan iki şifrenin toplamı da aynı koda ait olan bir şifredir.
  - Tamamen sıfırlardan oluşan bir şifre her zaman bir şifredir.
  - Bir doğrusal kodun iki şifresi arasında ki asgari hamming uzaklığı, sıfırlardan oluşmayan herhangi bir şifrenin asgari ağırlığına eşittir. Örneğin: d*=w*
- Bir kodun **asgari ağırlığı**, sıfırlardan oluşmayan herhangi bir şifrenin ağırlığı en küçük olanın ağırlığıdır. Ve w* ile gösterilir.
- Tamamı sıfırdan oluşan şifrelerin varlığı bir gereksinimdir fakat doğrusallık açısından verimli bir durum değildir.

Doğrusal Blok Kodların Matris Tanımı

- Üreteç matris olan G, k uzunlukta bir vektörü n uzunlukta bir vektöre çevirir.
- Girdi vektörünü i ile gösterelim. c şifre(codeword) olmak üzere :
  - c=iG olur.
  - Burada i bilgi kelimesidir.
- Üreteç matris *kxn* matris olacaktır.

Örnek

- Aşağıdaki matrisi göz önüne alalım:

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

$c_1 = [0\ 0].G = [0\ 0\ 0]$, $c_2 = [0\ 1].G = [0\ 1\ 0]$

$c_3 = [1\ 0].G = [1\ 0\ 1]$, $c_4 = [1\ 1].G = [1\ 1\ 1]$

Böylece bu üreteç matris şu kodu üretir:

C={000, 010, 101, 111}.

Eşlik Kontrol Matrisi(Parity Check Matrix)

- Eşlik kontrol matrisi, Bir hatanın oluşup oluşmadığını anlamak için bize basit bir yol sunar.

$$cH^T=0$$

  burada c geçerli bir şifredir.

- $c= iG$ olduğundan $iGH^T=0$ olur. Buradan tüm geçerli şifreler için:

$$GH^T=0$$

- Eşlik kontrol matrisinin boyutu $(n-k)xn$ 'dir.
- P^T , P matrisinin transpozunu göstermek üzere, ve G=[I|P]

İçin Eşlik kontrol matrisi: $H=[-P^T| I]$ olur.

Örnek

- (7, 4) gibi bir doğrusal blok kod için verilen üreteç matris

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

Olsun.

G matrisinden P matrisi P= $\begin{bmatrix}1&0&1\\1&1&1\\0&1&0\\0&1&0\end{bmatrix}$ olarak elde edilir.

İkili sistemde -1=1 olduğunu göz önüne alarak.Eşlik kontrol matrisini şu şekilde yazabiliriz. $H=[-P^T|I]=$ $\begin{bmatrix}1&1&0&0&1&0&0\\0&1&1&1&0&1&0\\1&1&0&0&0&0&1\end{bmatrix}$

Syndrome Decoding (Belirti Çözme)

- H 'nin (nxk) boyutunda bir Eşlik kontrol matrisi olduğunu varsayalım. Herhangi bir v ∈ $GF(q)^n$ vektörü için

$$s=vH^T$$

Vektörüne v nin sendromu denir.

- Buna sendrom denmesinin nedeni, bize hatanın belirtilerini vermesindendir.

Cyclic Codes(Dairesel Kodlar)

- Bir kod:
  - Doğrusal bir kod ve
  - Şifrelerin dairesel döndürülmesi yine kendisine ait bir şifre oluyorsa

Daireseldir denir.

- Örnek:

İkili tabanda C1={0000, 0101, 1010, 1111} bir dairesel koddur. Ancak C2={0000, 0110, 1001, 1111} bir dairesel kod değildir.

… Devamı

- Teorem: C Rn de bir kod olmak üzere C ancak ve ancak aşağıdaki şartları sağlarsa bir dairesel koddur.

  $a(x),\ b(x) \in C \Rightarrow a(x) + b(x) \in C$

  $a(x) \in C$ ve $r(x) \in Rn \Rightarrow a(x)r(x) \in C$

- İspat: (I)Varsayalım C Rn içinde bir dairesel kod olsun. Dairesel kodlar, doğrusal blok kodların bir alt kümesi olduğundan ilk şart sağlanır.
- (II) $r(x)= r_0+r_1X+r_2X^2 + \ldots + r_nX^n$ olsun. R(x) in x ile çarpımı sağa kaydırmadır. Tanım gereği sağa kaydırılmış şifrede geçerli bir şifredir. Yani $x.a(x) \in C$, $x.(x.a(x)) \in C$, …
- Ve $r(x)a(x)=r_0a(x)+r_1Xa(x)+r_2X^2a(x)+\ldots+r_nx^na(x) \in C$
- Çünkü her toplam C nin elemanır.

… devamı

- Sonra (I) ve (II) göz önüne alınırsa:
- r(x) 'i ölçeklenebilir bir değer alalım ve (I) den C nin doğrusal olduğunu biliyoruz, (II) de r(x) =x alırsak bu bize dairesel döndürmelerin bir şifre oluşturduğunu gösterir.
- Ve buradan (I) ve (II) bize C bir dairesel kod olduğunu gösterir.

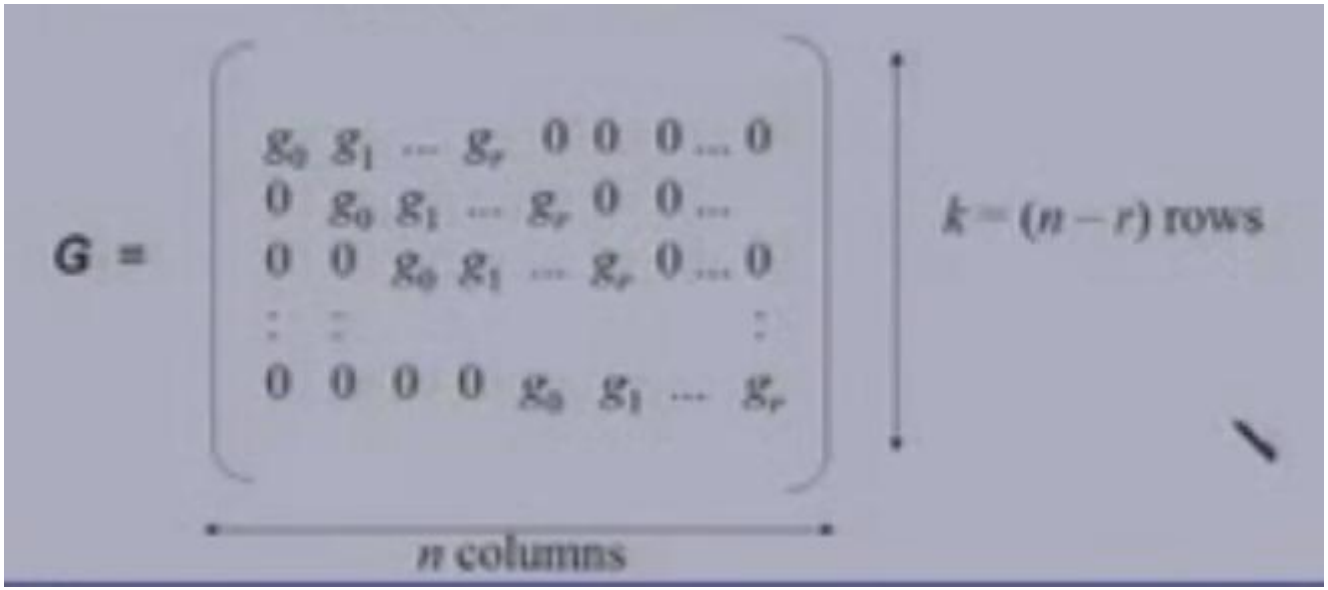
Dairesel kod üretmek için bir yöntem

- Şu adımlar kullanılabilir:
  - Rn içinde bir f(x) polinomu alalım.
  - F(x)'i Rn içindeki tüm mümkün polinomlar ile çarparak bir polinomlar kümesi oluşturalım.
  - Bu küme bir dairesel kodu oluşturan şifreleri(codeword) karşılık gelir.

Kodun blok uzunluğu n olur.

Dairesel Kodların Matris Tanımı

- C nin g(x)=g0 + g1x +…+grxr gibi r. Dereceden bir üreteç polinoma sahip bir dairesel kod olduğunu varsayalım. Öyleyse C nin üreteç matrisi şöyle verilir.



Burst Errors

- Birçok gerçek hayat kanallarında hatalar rastgele olmaz. Patlama şeklinde olur.
- Örneğin: mobile iletişimlerde sinyal azalması patlama hatalara sebep olabilir.
- Hatalar rastgele değil sürekli ise buna patlama hatalar (Burst error) denir.
- Dairesel patlamanın uzunluğu olan t, sıfırdan farklı elemanlardan oluşan t ardışık bileşendir.

Patlama Hataları Örneği

- 10kb/s ile transfer edilen bit sırası aşağıdaki gibi olsun.

  c=0100011101010000101101
- Varsayalım ki iletim başladıktan sonra kanal 1 ms'lik bir kopukluk yaşadı.bu zaman dilimi içinde kanal iletilmiş bitleri bozabilir. Hatalı bit dizisi şöyle alınmış olabilir.

  b=0000011111111110000000
- Bu örnekte iletilmiş bitler kanal tarafından bozulmuştur.
- Burada patlamanın uzunluğu 10 bittir.

Bose-Chaudhuri Hocquenghem(BCH) Codes

- BCH kod sınıfı bilinen en güçlü doğrusal dairesel blok kod sınıflarından biridir.
- BCH kodları çoklu hata düzeltme yetenekleri ve şifreleme ve çözmenin kolaylığı ile bilinir.
- Şimdiye kadar yaklaşımımız, bir kod oluşturup hata düzeltme yeteneğini bulmak için onun asgari uzaklığını bulmaktan ibaretti.
- Bu kod sınıfında diğer uçtan başlayacağız.

BCH kodları ve RS kodları

- BCH kod sınıfı bağımsız olarak 1959 da Hocquenghem ve Bose ve Ray Chaudhuri tarafından keşfedilmişidir.
- Reed-Soloman(RS) kodları, dijital iletişimde ve veri saklama alanında bir çok uygulaması ile BHC nin önemli bir alt kümesidir.
- Reed-Soloman kodları Irving S. Reed ve Gustave Soloman tarafından 1960'da icat edilmiştir.
- Bir çok avantajına rağmen Reed-Soloman kodları icadından hemen sonra kullanıma geçilmemiştir.
- Donanım teknolojisinin gelişmesini beklemişlerdir.

BCH kodları için Üreteç Polinom

- g(x) 'in X^n-1 bir faktörü olduğunu biliyoruz.
- Böylece, f(1), f(2), f(3), …, f(4) g(x)'in minimal polinomları olmak üzere, dairesel kodun üreteç polinomu:

$$g(x)=LCM[f_1(x), f_2(x), \ldots, f_p(x)]$$

şeklinde yazılabilir.

- Each minimal polynomial corresponds to a zero of g(x) in an extension field.(?)
- We can design good codes (i.e., determine the generator polynomials) with desirable zeros using this approach.(?)

BCH kodlarının Çözümü

- BCH kodları, dairesel kodların bir alt sınıfı olduğundan, dairesel kodlarda kullanılan çözme standartları BHC için de geçerlidir.
- Ancak, BCH için özel tasarlanmış algoritmalarda mevcuttur.
- İkili çözme algoritmalarının genelleştirilmiş formu olan Gorenstein-Zierler çözme algoritması önemli bir metoddur.

Reed Solomon Codes

- Reed-Soloman(RS) kodları dijital iletişimde ve depolama alanlarında geniş uygulama alanları bulur.
- RS'nin uygulama alanları
  - Veri depolama(teyp, Cd, Dvd, barkod, etd)
  - Kablosuz ve mobil iletişim
  - Uydu bağlantıları
  - DVB (Dijital televizyon)
  - Yüksek hızlı modemler: ADSL, xDSL, gibi