KODLAMA TEORİSİ

• Hata düzelen kodlar

• Şifreleme (Kriptografiya)
ÖRNEKLERLE KODLAR:

• Örnek 1: International Standard Book Number (ISBN)
4

Dil Basımevi Kitap numarası kontrol hanesi (bit)

\[ \begin{align*}
1 \times 9 + 2 \times 7 + 3 \times 5 + 4 \times 8 + 5 \times 6 + 6 \times 4 + 7 \times 4 + 8 \times 0 + 9 \times 3 & \equiv 3 \pmod{11}
\end{align*} \]

**Genel olarak: ISBN No:**

\[ d_1 - d_2d_3d_4 - d_5d_6d_7d_8d_9 - d_{10} \]

\[ d_{10} = 1 \times d_1 + 2 \times d_2 + 3 \times d_3 + 4 \times d_4 + 5 \times d_5 \]
\[ + 6 \times d_6 + 7 \times d_7 + 8 \times d_8 + 9 \times d_9 \pmod{11} \]

\[ d_{10} = 10 = X \]

ISBN kodlaması bir hata tespit edebilir!
Örnek 2: Tekrar Kodu:

OKEY → OOOKKKEEEYYY

\((1,0,1,0) \rightarrow (1,0,1,0,1,0,1,0,1,0,1,0)\)

BİLGİ TRANSFER ŞEMASI

1011 1011010 zararlı etki 1010010 1011010 1011
Örnek 3:

Ali, Oya’ın güvenli bir şekilde geçebileceği güzergah yönünü aşağıdaki gibi verir:

KKBKKBGGBBBKKKKBBK

C1 = \{00, 01, 10, 11\} \quad \{K, B, G, D\}

00000100000101111101010000000000010100

C2 = \{000, 011, 101, 110\}

1 hata tespit edilebilir.

C3 = \{00000, 01101, 10110, 11011\}

1 hata düzeltebilir.
Örnek 4:

"KODLAMA"

Haberleşme-Depolama Kanalın Özellikleri:

hatalı sembol ulaşıma olasılığı: \[ y = 0.1 \]
hatasız sembol ulaşıma olasılığı: \[ d = 0.9 \]

Kodlamadan önce:
doğru bilginin ulaşıma olasılığı: \[ d^7 = 0.48 \]
Kodlamadan sonra: (5 kez tekrar kodu ile)

“KKKKKOOOOODDDDDDLLLLLA
AAAAAMMMMMAAAAA”

doğru harfi dekodlama olasılığı

$$d^5 + 5d^4 y + 10d^3 y^2 = 0.99$$

doğru bilginin ulaşma olasılığı!

$$(0.99)^7 = 0.94$$

(Tekrarlı) Kodlama yapımadan önce doğru bilgi ulaşma olasılığı:

$${d}^7 = 0.48$$

Kodlamadan sonra ise;

$$(0.99)^7 = 0.94$$
Örnek 5: (CD-KİTAP, Jack H. Van Lint,98)

\[ \phi_{31} = \{ 0,1,3,...,29,30 \} \]

Eşleme: Alfabe \rightarrow Modüler (Kalan Sınıflar) Sayılar

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>ç</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>ğ</th>
<th>h</th>
<th>i</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
</tbody>
</table>

| m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z | . |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Ali okula gitti. \rightarrow 01151200181425150100081224241230
Mesaj kodlanması:

$$\left( a_2, a_3, a_4, a_5 \right) \rightarrow \left( a_0, a_1, a_2, a_3, a_4, a_5 \right)$$

Kodlama metodu:

$$a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \left( \text{mod } 31 \right)$$

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \equiv 0 \left( \text{mod } 31 \right)$$
\[
(\alpha_2, \alpha_3, \alpha_4, \alpha_5) \leftrightarrow (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)
\]

\[
\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5 \equiv 0 \mod(31)
\]

\[
\alpha_1 \equiv -(2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5) \mod(31)
\]

\[
\alpha_1 \equiv -(2 \cdot 6 + 3 \cdot 15 + 4 \cdot 16 + 5 \cdot 1) \equiv 29 \mod(31)
\]

\[
\alpha_1 \leftrightarrow \mathbb{Z}
\]

\[
\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 \equiv 0 \mod(31)
\]

\[
\alpha_0 \equiv -(\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5) \equiv 26 \mod(31)
\]

\[
\alpha_0 \leftrightarrow \mathbb{U}
\]
Örnek:

ELMA

(6,15,16,1)

ÜZELMA

(26,29,6,15,16,1)
Bu kodlanmanın kullanıldığı bir kitabı inceleyelim:
(En fazla bir hata meydana gelebilme varsayımı altında)

BRANMA 022101171601

KONTROL:

$$a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \equiv 27 \pmod{31}$$

HATA VAR!!!

Sembollerden birinin değeri 27 artmıştır,
\[ a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \equiv 19 \ (\text{mod} \ 31) \]

\[ 27i = 19 \quad -4i = 19 \quad 4i = -19 = 12 \]

\[ 8 \cdot 4i = 8 \cdot 12 \quad i = 3 \]

Hata i=3 te meydana gelmiştir.

\[ a_3 = 17 - 27 = -10 = 21 = R \]

DÜZELTİLİMİŞ HALİ:

BRANMA \hspace{1cm} ARMA
Bu Kodlanmanın Bir Kitap Üzerindeki Etkileri:

KİTAP : 200 SAYFA
SAYFA: 3000 KARAKTER

YAZICININ KÜÇÜK HARF YANLIŞ YAZMA OLASILIĞI: % 0,02

YAZICININ DİĞER SEMBOLLERDE HATA YAPMA OLASILIĞI: % 0,01.

KODLAMA ÖNÇESİ: SAYFA BAŞINA YAKLAŞIK 3 HATA,

TOPLAM HATA: 600!
YUKARIDAKİ KODLAMA METODU İLE:

HIZ: 4/6

HER SAYFADA 4500 (1,5 kat) ADET SEMBOL

YAZICININ KÜÇÜK HARF YANLIŞ YAZMA OLASILIĞI: % 0,02

6 UZUNLUĞUNDAKİ BİR SÖZCÜKTEN 1 DEN FAZLA HATA İÇERME OLASILIĞI:

\[ \sum_{i=2}^{6} \binom{6}{i} (0.002)^i (0.998)^{6-i} \approx 0.00006 \]
BİR SAYFADA 6 UZUNLUĞUNDA 4500/6=750 SÖZ VAR.

KİTAPTA 6 UZUNLUĞUNDA 200*750=150 000 SÖZ VAR.

150000*0.00006=9 (HATA BÜTÜN KİTAPTA!)

CD lerde benzer teknik kullanılmaktadır.
Ancak daha karmaşık!

1sn lik müzik yaklaşık: 4 321 800 bit
1 CD dijital formda yaklaşık: 5 km bit!
TEŞEKKÜR

• TÜBİTAK-BİDEB
• Prof. Dr. Mehmet AY-Çalıştay Başkanı
• Katılımcı-Değerli Öğretmenler
• TÜSSİDE