Hibadetektáló és javító kódolások

Számítógépes adatbiztonság

Hibadetektálás és javítás

- Zajos csatornák
  - adatblokk meghibásodási valószínűségének csökkentése
  - blokk bővítése redundáns információval
  - Hálózati megoldások
    - ARQ
      - kis csatorna kapacitás, nem konstans átviteli ráta
    - FEC
      - broadcast, rossz csatorna, adattárolás

Hibák

- Véletlen bithibák
- Burst hibák

- Bit error rate (BER)
- Block error rate (BLER)
- Burst error length (BERL)

Becslés kis valószínűségekkel

- p, q egymástól független kis meghibásodási valószínűségek
- Meghibásodás valószínűsége:
  - becslés: p+q
  - pontos érték: 1-(1-p)(1-q)=p+q-pq

- Példa: BER: $1:10^7$, Mennyi a valószínűsége a meghibásodásnak (min. 1 bit) egy 10000 bites csomagban?
  - becslés: $10^4*10^{-7}=10^{-3}$
  - pontos: $1-(1-10^7)^{10000}=0.0009995$

Csatornakapacitás

- Zajos csatornák adatátviteli kapacitása
  - Shannon–Hartley tétel
    - B sávszélesség
    - S/N átlagos jel/zaj arány

$$C = B\log_2(1 + S/N)$$

Csatornakódolás kapacitástétele

- C csatornakapacitású csatornán a forrás szöveg K hosszúságú blokkjának bővítése N hosszúságúra tetszőlegesen kicsivé teszi K meghibásodásának valószínűségét, ha (K/N)<C, és K→∞.

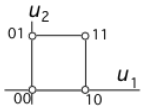
Kódolás

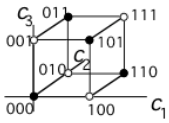
- Jelölések

$$u := (u_1, u_2, \ldots u_K)$$

$$c := (c_1, c_2, \ldots c_N)$$

$$c := f(u)$$





- Hamming távolság
  - kód tér elemei között

$$d(\mathbf{c}, \mathbf{v}) := \sum_{i=1}^{q} \chi_{\{c_i \neq v_i\}}.$$

Kódolás (folyt.)

- Dekódolás

$$c' = D(v)$$

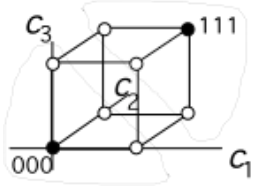
$$u' = f^{-1}(c')$$

- Kódtávolság

$$d_{\min} := \min d(c, c')$$

- Kezelhető hibák

$$t_{jel} = d_{\min} - 1 \qquad t_{jav} = Int\frac{d_{\min} - 1}{2}$$



Kódolás (folyt.)

- Singleton korlát (elhelyezhető kódszavak)
  - N hosszúságú vektorok, q elemű ABC

$$M \le q^{(N-d_{\min}+1)}$$

- MDS (maximum distance separable) kód
  - egyenlőség esetén
- Hamming korlát

$$m^K \sum_{i=0}^{t_{jav}} \binom{N}{i} (q-1)^i \le q^N$$

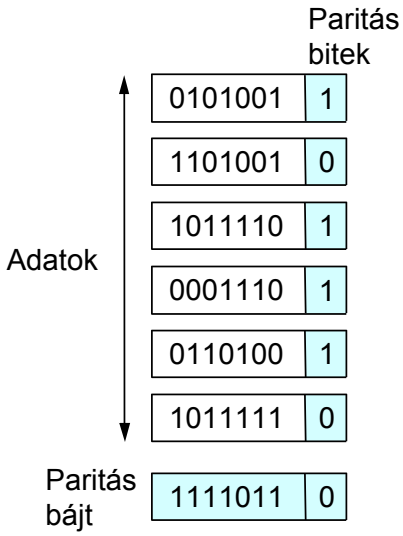
- Perfekt kód
  - egyenlőség esetén

Paritás bitek

- Paritás bit
  - páros
  - páratlan paritás

- Hibadetektálási képesség (pl.)
  - K=8, N=9 bin. kódolás (1 paritás bit),BER 1:10^4
  - 8 bites hibás üzenet (paritás nélkül)
    - $1-(1-10^{-4})^8=0.000799$
  - paritással nem detektált hibás üzenet (felső becslés)
    - detektálható 1 bites hibák
      - $9*10^{-4}(1-10^{-4})^8$
    - $1-(1-10^{-4})^9-9*10^{-4}(1-10^{-4})^8=0.000000359$

Két dimenziós paritás



CRC

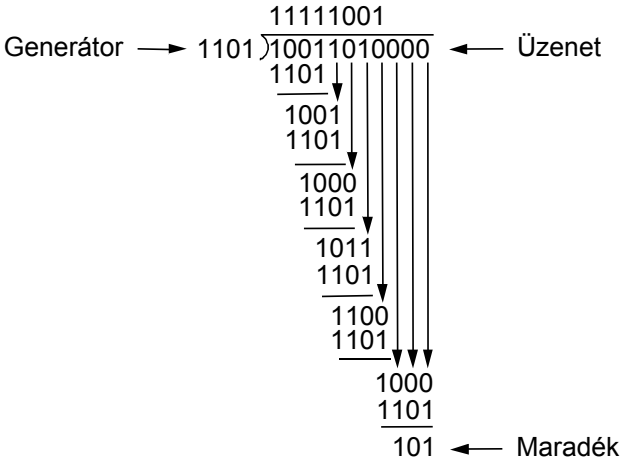
- üzenet polinom (M) és generátor polinom (G) osztásakor keletkező maradék (R) mint redundancia =>
- C=M+R maradék nélkül osztható G-vel
- vett üzenet (V), hiba (E)
  - V=C+E
- válasszunk olyan G-t, hogy E-vel ne 0 maradékot adjon

CRC (folyt.)

MSG=10011010 $M(x) = x^7 + x^4 + x^3 + x^1$

$G(x) = x^3 + x^2 + 1$ (1101)

$M*x^k = x^{10} + x^7 + x^6 + x^4$ (10011010000)



10011010000 XOR 101 = 10011010101

CRC (folyt.)

- CRC generátor polinomok

CRC	$C(x)$
CRC-8	$x^8+x^2+x^1+1$
CRC-10	$x^{10}+x^9+x^5+x^4+x^1+1$
CRC-12	$x^{12}+x^{11}+x^3+x^2+x^1+1$
CRC-16	$x^{16}+x^{15}+x^2+1$
CRC-CCITT	$x^{16}+x^{12}+x^5+1$
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Internet checksum

- Gyorsan számolható
- 1-es komplemense 16 bites üzenetdarabok 1-es komplemens összegének
- Gyenge hibadetektálási tulajdonságok

```
unsigned short
tcpcksum(struct ep *pep, unsigned len)
{
      struct     ip    *pip = (struct ip *)pep->ep_data;
      struct     tcp   *ptcp = (struct tcp *)pip->ip_data;
      unsigned   short *sptr;
      unsigned   long tcksum;
      unsigned   i;

      tcksum = 0;

      sptr = (unsigned short *) &pip->ip_src;
      /* 2*IP_ALEN octets = IP_ALEN shorts... */
      /* they are in net order.          */
      for (i=0; i<IP_ALEN; ++i)
            tcksum += *sptr++;
      sptr = (unsigned short *)ptcp;
      tcksum += hs2net(IPT_TCP + len);
      if (len % 2) {
            ((char *)ptcp)[len] = 0;     /* pad */
            len += 1;   /* for the following division */
      }
      len >>= 1;  /* convert to length in shorts */

      for (i=0; i<len; ++i)
            tcksum += *sptr++;
      tcksum = (tcksum >> 16) + (tcksum & 0xffff);
      tcksum += (tcksum >> 16);

      return (short)(~tcksum & 0xffff);
}
```


Hibajavító kódolás

- Forward Error Correction
  - nincs szükség visszacsatolásra
  - nagyobb redundancia
  - állandó átviteli sebesség
  - adattároló rendszerek, zajos csatornák (pl. rádió hálózatok)
- Blokk kódok
- Konvolúciós kódok

Bináris lineáris kódok

- lineáris tér bázisai a kódszavak
  - generátor, paritás ellenőrző mátrix, szindróma

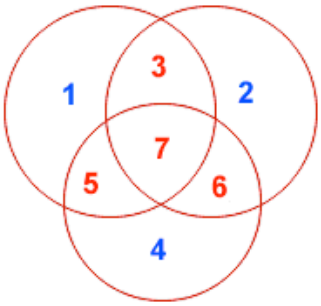
$$\mathbf{c} = \mathbf{u} \cdot \mathbf{G}$$

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$$

$$\mathbf{s}^T = \mathbf{H} \cdot \mathbf{v}^T$$

Hamming kódolás

- (7,4) Hamming kód
  - kódszó: $D_7D_6D_5P_4D_3P_2P_1$
  - Hamming távolság: 3



$$G := \left(I_k \middle| -A^T\right)$$

$$H := \left(A \middle| I_{n-k}\right)$$

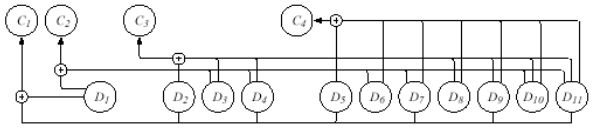
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

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

szisztematikus kód

Hamming kódolás (folyt.)

- Példa (Hamming(15,11))




```
 0111110x100x0xx
 011111011000001
Transmit it with an error:
 011101011000001
Compute parities:
 0111010110000010
 01110101          1
 0111    1000      0
 01  01  10  00    1
 0 1 0 0 1 0 0 1   1
Bit 11 (1011 in binary) is in error. Flip it:
 0111110110000010
Extract the data:
 0111110 100 0
```


Véges testek

- Véges elemszámú halmazok
- Zártak egy + és * műveletre
- Van additív {0} és multiplikatív {1} elem
- GF(q), q prím vagy prím hatvány
  - p prím esetén {0,1,...p-1} valós aritmetika moduló p-vel
- primitív elem: p-1-edik hatványnál éri el először az egységelemet

Reed-Solomon kódolás

- Nem bináris lineáris kód
  - Véges test feletti polinomok

$$\mathbf{u} = (u_1, u_2, ..., u_K) \quad \Rightarrow \quad u(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{K-1} x^{K-1}$$

$$c_1 = u(\alpha^0), c_2 = u(\alpha^1), c_3 = u(\alpha^2), ..., c_N = u(\alpha^{N-1})$$

α GF(q) primitív eleme

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & . & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & . & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & . & \alpha^{2(N-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & . & \alpha^{3(N-1)} \\ . & . & . & . & . & . \\ 1 & \alpha^{K-1} & \alpha^{2(K-1)} & \alpha^{3(K-1)} & . & \alpha^{(K-1)(N-1)} \end{pmatrix} \qquad \mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & . & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & . & \alpha^{2(N-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & . & \alpha^{3(N-1)} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & . & \alpha^{4(N-1)} \\ . & . & . & . & . & . \\ 1 & \alpha^{N-K} & \alpha^{2(N-K)} & \alpha^{3(N-K)} & . & \alpha^{(N-K)(N-1)} \end{pmatrix}$$

Reed-Solomon kódolás (folyt.)

- Törlések és hibák javítása
  - szindrómákra vonatkozó egyenlet-rendszerek megoldása
- Alkalmazások
  - 8-bites byte ABC használata RS (255,223)
  - CD lemezek, űrtávközlés, xDSL, RAID 6