Zaštitni kodovi

- Blok kodovi
  - sve kodne riječi iste duljine - *n*
- Konvolucijski kodovi

- Linearni
  - ima kodnu riječ 0
- Nelinearni

Abeceda

F_q – q (broj elemenata – abeceda koda)
F_2 – binarni kôd

Distanca

d(x,y) – Hammingova udaljenost
d(K) = min(d(x,y) | x≠y)
d(K) = 2t + 1
d(K) = s + 1

Blok-kôd K(n, M, d)

n – duljina kôda
M – broj kodnih riječi u kôdu
d – distanca kôda

može otkriti najviše **d(K)-1** pogrešaka
može ispraviti najviše **floor(d(K)-1 / 2)** pogrešaka

Hammingova međa za A(n,d):

$$M \le \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots\binom{n}{t}}$$

Perfektan kôd:

$$M = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots\binom{n}{t}}$$

Linearno binarni blok kodovi

Težina kodne riječi **w(x)**
- broj pozicija u k.r. na kojim se nalazi **1**
- d(x,y) = w(x-y)

Generirajuća matrica **G**
- dim. k×n, k = $\log_2$(M)

Oznaka **[n, k]**, odnosno **[n, k, d]**

n – duljina kodne riječi
k – k-dimenzionalni potprostor V(n)
d – distanca

Ekvivalentni linearni blok kodovi K_1, K_2

G_1 i **G_2** se mogu dobiti jedna iz druge:
- zamjenom redaka
- dodavanjem jednog retka drugom retku
- zamjenom stupaca

$G = [I_k \mid A]$

Kad je G u standardnom obliku:
$m \cdot [I_k \mid A] = \{m, m \cdot A\}$

Vektor pogreške

$e = y - x = [e_1\, e_2 \ldots e_n]$

Dualni kôd

x · y = 0
K [n,k] → $K^{\perp}$ [n,n-k]

$G \cdot H^T = 0$
$x \cdot H^T$ = [0 0 ... 0]

Matrica provjere pariteta H

za **$H = [\, B \mid I_{n-k} \,]$** onda je H u standardnom obliku, B je kvadratna matrica

$G = [\, I_k \mid A \,]$
$H = [\, A^t \mid I_{n-k} \,]$

Sindrom

$S(\mathbf{y}) = \mathbf{y} \cdot \mathbf{H}^T$

jedan vektor pogreške – jedan sindrom

Kodna brzina R(K)

$$R(K) = \frac{k}{n} \le 1$$

Hammingovi kodovi

za r >= 2:
- linearan blok-kôd [2^r-1, 2^r-1-r]
- najmanja distanca je 3
- perfektan kôd

H – matrica provjere pariteta
G – generirajuća matrica

H → izbriši stupce s pozicijama parity bitova → transponiraj → postavi stupce na poz. 1,2,4,8... → ostatak stupaca popuni jediničnom matricom → G

• • • • •

Ciklični kodovi

- postoji jedinstven g(x) najmanjeg stupnja u K
- kod K definiran polinomom g(x)
- g(x) je faktor polinoma $x^n-1 = g(x)\cdot q(x)$

G = [n-r × n]

$x^n-1 = g(x)\cdot h(x)$,
tada je h(x) polinom za provjeru pariteta

$x^r \cdot d(x) = g(x)\cdot q(x) + r(x)$

d(x) – polinom kodirane poruke
g(x) – generirajući polinom
q(x) – kvocijent
r(x) – ostatak nakon dijeljenja s g(x)