LINEARNO BINARNI BLOK KODOVI

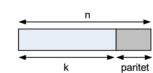
$$K: (n, M, d) \leftrightarrow [n, k, d] \leftrightarrow [n, k]$$

 $M = 2^{k}$

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

$$d(K) = \min_{x,y \in K} (d(x,y)|x \neq y)$$

$$d(x,y) = w(x-y)$$



Uvjeti lineranosti binarnog blok koda

1)
$$x + y \in K$$
, $x,y \in K$

2)
$$a \cdot x \in K, a \in \{0,1\}$$

k – broj informacijskih bitova u kodnoj riječi

n - duljina kodne riječi

M - broj kodnih riječi u kodu

d - distanca (udaljenost) koda

R - kodna brzina

w - težina kodne riječi

HAMMINGOVA MEDA ako umjesto '<=' samo' =', tada je kod PERFEKTAN

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

VJEROJATNOST NEOTKRIVENE POGRESKE U PRIJENOSU- PARNI PARITET: neparan broj '1' daje 1

$$p_{np} = \binom{n}{2} p^2 (1-p)^{n-2} + \binom{n}{4} p^4 (1-p)^{n-4} + \dots + \binom{n}{n} p^n \qquad n-\text{parno}$$

$$p_{np} = \binom{n}{2} p^2 (1-p)^{n-2} + \binom{n}{4} p^4 (1-p)^{n-4} + \dots + \binom{n}{n-1} p^{n-1} (1-p) \qquad n-\text{neparno}$$

VJEROJATNOST ISPRAVNOG DEKODIRANJA -ako treba za

$$p(K) = \sum_{i=1}^{n} \binom{n}{i} p_g^i (1 - p_g)^{n-i}$$
NEISPRAVNO KODIRANJE, tada suma ide od (t+1) do n

DEKODIRANJE LINEARNOG BINARNOG KODA:

1) Metoda najbližeg susjeda

$$d(K) \ge s + 1$$
$$s = d(K) - 1$$

$$t = \left\lfloor \frac{d(K) - 1}{2} \right\rfloor$$
$$d(K) \ge 2t + 1$$

$$2^{n-k} \ge \sum_{i=0}^{t} {n \choose i}$$

s - najveći broj pogrešaka koje kôd može otkriti

najveći broj pogrešaka koje kôd K može ispraviti

2) Sindromsko dekodiranje

$$e = y - x$$
 $e = (y) XOR (x)$

e - vektor pogreške

poslana kodna riječ

primljena kodna riječ

$$G = [I_k \mid A]$$

$$H = [A^T \mid I_{n-k}]$$

$$G = [I_k \mid A]$$

* H™ = 0 ako primljena kodna riječ dio koda

 $S(y) = y \cdot H^T$

c = d * G

d - vektor s k-bitova

c - kodna riječ u kodu

G – generirajuća matrica koda dimenzija $k \times n$

(n-k)xn H - matrica provjere pariteta

5 - sindrom

A - kvadratna matrica

HAMMINGOV KÔD

H - matrica provjere pariteta dimenzija $r \times (2^r - 1)$

$$r = n - k$$

Generirajuću matricu G je iz matrice H moguće dobiti sljedećim postupkom:

- 1. U matrici H izbrisati sve stupce koji se nalaze na pozicijama s indeksom jednakim potenciji broja 2 (pozicije 1,2,4, 8, 16, itd).
 - 2. Dobivenu matricu transponirati.
- 3. Stupce dobivene matrice smjestiti na pozicije generirajuće matrice G čiji indeksi odgovaraju potencijama broja 2.
 - 4. Ostale stupce popuniti redom stupcima jedinične matrice.

HAM [7,4]

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix}$$

CIKLIČKI KÔD

Uvieti:

- 1. $\forall a(x), b(x) \in K$, $vrijedia(x) + b(x) \in K$
- 2. $\forall a(x) \in Ki \forall r(x) \in Rn$, vrijedi

 $r(x) \cdot a(x) mod(xn-1) \in K$.

$$x^n - 1 = g(x) \cdot h(x)$$

r - stupanj generirajućeg polinoma

h(x) - polinom za provjeru pariteta cikličnog koda K.

cikličnog koda K.

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

$$r(x) = d(x) \cdot x^r \mod[g(x)] = \frac{x^{n-\kappa}d(x)}{g(x)}$$
 --> METODA CIKLI**Č**KE REDUNDANTNE ZAŠTITE

$$S(c'(x)) = \frac{x - c(x)}{g(x)}$$

 $oldsymbol{c} = [oldsymbol{d} | oldsymbol{r}]$ --> kodna rije $oldsymbol{c}$ dobivena metodom cikli $oldsymbol{c}$ ke redundantne zaštite

g(x) - generirajući polinom

q(x) - kvocijent

d(x) – polinom kodirane poruke

r(x) – ostatak nakon dijeljenja s g(x)

c(x) – kodna riječ

S(c'(x)) - sindrom primljene kodne riječi

ALGORITAM ZA DOBIVANJE GENERIRAJUĆE MATRICE G=[Ik:A] iz g(x)

- 1. upiši g(x) u binarnom obliku u k-ti redak
- 2. (k-1) redak dobije se cikličkim posmakom k-tog retka za 1 u lijevo k-ti stupac mora u (k-1) retku imati '0' kako bi G bila u standardom obliku,
 - ako ima '1' tada na (k-1) redak dodati k-ti redak ---> (k+(k-1))
- 3. ponavljaj dok G nije pun

GENERIJRAJUĆI POLINOM - onaj polinomski zapis kodne rijeci koji je jedini polinom svog stupnja i ima najmanji stupanj od svih ostalih polinoma u kodu

FAKTORIZACIJE NEKIH POLINOMA OBLIKA $x^n - 1$

N	Ari	Faktorizacija u aritmetici modulo 2
	t.	
1	x -	x + 1
2	x2 -	$(x+1)^2$
3		$(x+1)(x^2+x+1)$
5	x5 -	$(x+1)(x^4+x^3+x^2+x+1)$
7	7 –	(/ (/ (/ (
9	x9 -	$(x+1)(x^2+x+1)(x^6+x^2+1)$
11	x11	(
13	x13	$(x+1)(x^{12}+x^{11}+\cdots+x+1)$
15	x15	$(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x^4+x^4+x^4+x^4+x^4+x^4+x^4+x^4+x^4+x^4$
		1)
17	x17	$(x+1)(x^8+x^5+x^4+x^3+1)(x^8+x^7+x^6+x^4+x^2+x+$
		1)
19	x19	$(x+1)(x^{18}+x^{17}+\cdots+x+1)$

