Zavod za telekomunikacije

Zaštitno kodiranje II

Teorija informacije

Sadržaj predavanja

Hammingovi i ciklični kodovi

(klasa linearnih blok kodova)

Hammingovi kodovi

Definicija: Hammingov kôd

Hammingov kôd: *Neka je r pozitivan cijeli broj i neka je* **H** *matrica dimenzija* $r\times(2^r-1)$ *čije stupce sačinjavaju svi vektori dimenzije r različiti od* **0** *iz vektorskog prostora V*(*r*). *Matrica* **H** *je matrica provjere pariteta Hammingovog koda s oznakom* Ham(*r*).

- Primjer: Matrice provjere pariteta: $r = 3$, $n = 2^3 - 1 = 7$

$$\mathbf{H}_1^T = \left[\begin{array}{ccc|c} 0&0&1&1\\ 0&1&0&2\\ 0&1&1&3\\ 1&0&0&4\\ 1&0&1&5\\ 1&1&0&6\\ 1&1&1&7 \end{array}\right] \quad ili \quad \mathbf{H}_2^T = \left[\begin{array}{ccc|c} 1&1&1&7\\ 1&1&0&6\\ 0&1&1&3\\ 1&0&1&5\\ 1&0&0&4\\ 0&1&0&2\\ 0&0&1&1 \end{array}\right]$$

- Stupci matrica provjere pariteta su binarni ekvivalenti cijelih brojeva od 1 do 2^r-1! Redoslijed je nevažan!

Svojstva Hammingovih kodova

Svojstva Hammingovih kodova: *Neka je* Ham(*r*) *binarni Hammingov kôd. Za r* ≥ 2 *vrijedi da je* Ham(*r*):

- *linearan blok-kôd* $[2^r-1, 2^r-1-r]$;
- *ima najmanju distancu* 3 (*otkriva dvostruku i ispravlja jednostruku pogrešku*);
- *perfektan kôd*.

Neki mogući Hammingovi kodovi i njihove distance!

$[n,k,3]$	$[n,k,5]$	$[n,k,7]$	$[n,k,9]$	$[n,k,11]$	$[n,k,13]$
[3,1,3]	[5,1,5]	[7,1,7]	[9,1,9]	[11,1,11]	[13,1,13]
[5,2,3]	[8,2,5]	[11,2,7]	[14,2,9]	[17,2,11]	[20,2,13]
[6,3,3]	[10,3,5]	[13,3,7]	[17,3,9]	[20,3,11]	[24,3,13]
[7,4,3]	[11,4,5]	[14,4,7]	[19,4,9]	[22,4,11]	[26,4,13]
[9,5,3]	[13,5,5]	[15,5,7]	[20,5,9]	[23,5,11]	[27,5,13]
[10,6,3]	[14,6,5]	[17,6,7]	[22,6,9]	[25,6,11]	[29,6,13]
[11,7,3]	[15,7,5]	[18,7,7]	[24,7,9]	[26,7,11]	[32,7,13]
[12,8,3]	[16,8,5]	[19,8,7]	[25,8,9]	[28,8,11]	[34,8,13]
[13,9,3]	[17,9,5]	[20,9,7]	[26,9,9]	[30,9,11]	[35,9,13]
[14,10,3]	[19,10,5]	[21,10,7]	[28,10,9]	[31,10,11]	[36,10,13]

Kodiranje pomoću Hammingovog koda

Zavod za telekomunikacije

- Primjer: Hammingov kôd [7, 4, 3]

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Generirajuću matricu **G** nije jednostavno izračunati iz **H** jer ista nije u standardnom obliku, tj. jednadžba $\mathbf{GH}^T=\mathbf{0}$ daje velik broj mogućnosti.
- Potrebno je dobiti sistematičan kôd iz kojeg jednostavno dobivamo poslanu kodiranu poruku.
- Važno svojstvo matrice H: Svaki redak matrice provjere pariteta određuje pozicije simbola kodne riječi čiji zbroj mora bit paran broj (ili jednak 0 u aritm. mod. 2).

Formiranje kodne riječi Hammingovog koda

Zavod za telekomunikacije

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

prvi redak	Pozicije (1), (3), (5) i (7).
drugi redak	Pozicije (2, 3), (6 i 7),
treći redak	Pozicije (4, 5, 6 i 7),

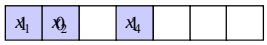
Ključno pitanje - koji bitovi su zaštitni?

$$x_1 = m_1 + m_2 + m_4 + m_5 + m_7 + \ldots = x_3 + x_5 + x_7 + x_9 + \ldots$$
$$x_2 = m_1 + m_3 + m_4 + m_6 + m_7 + \ldots = x_3 + x_6 + x_7 + x_{10} + x_{11} + \ldots$$
$$x_4 = m_2 + m_3 + m_4 + m_8 + m_9 + m_{10} + m_{11} + \ldots = x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{13} + x_{15} \ldots$$
$$\vdots$$

Primjer: formiranje kodne riječi za Hammingov kôd [7, 4, 3]

Zavod za telekomunikacije

Poruka ⇒ 1 0 1 0



Okvir kodne riječi

$$\mathbf{H} = \begin{bmatrix} x & & x & & x & & x \\ & x & x & & & x & x \\ & & & x & x & x & x \end{bmatrix}$$

Primjer: generirajuća matrica za Hammingov kôd [7, 4, 3]

Zavod za telekomunikacije

(1) Izbriši one stupce koji su na pozicijama paritetnih bitova
(2) Dobivenu matricu transponiraj
(3) Stupce transponirane matrice postavi na pozicije 1, 2, 4, 8, 16, …
(4) Ostatak stupaca popuni jediničnom matricom

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

1 2 4

Generirajuća matrica Hammingovog koda

1 2 3 4 5 6 7

$$\mathbf{I}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Primjer: sindrom za Hammingov kôd [7, 4, 3]

Zavod za telekomunikacije

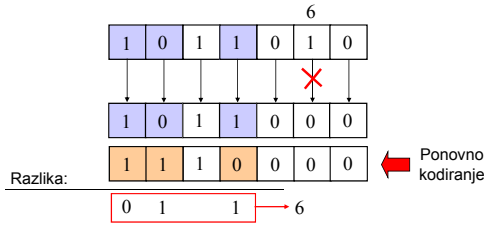
Napomena: Vrijedi samo za standardni način formiranja Hammingovih riječi!

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

e	S(y)	CJELOBROJNI EKVIVALENT
1 0 0 0 0 0 0	1 0 0	1
0 1 0 0 0 0 0	0 1 0	2
0 0 1 0 0 0 0	1 1 0	3
0 0 0 1 0 0 0	0 0 1	4
0 0 0 0 1 0 0	1 0 1	5
0 0 0 0 0 1 0	0 1 1	6
0 0 0 0 0 0 1	1 1 1	7

Primjer: određivanje sindroma bez matrice provjere pariteta (1/2)

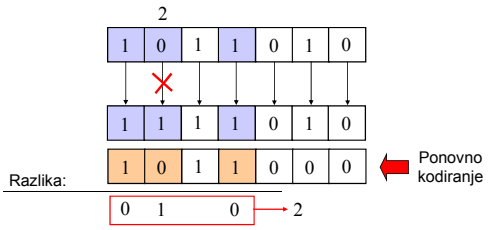
Zavod za telekomunikacije



Pogreška je na poziciji br. 6, a ispravna kodna riječ
1 0 1 1 0 1 0

Primjer: određivanje sindroma bez matrice provjere pariteta (2/2)

Zavod za telekomunikacije



Pogreška je na poziciji br. 2, a ispravna kodna riječ
1 0 1 1 0 1 0

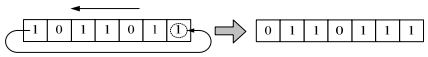
Zavod za telekomunikacije

Ciklični kodovi

Definicija: ciklični kôd

Zavod za telekomunikacije

***Ciklični kôd**: Blok kôd K je ciklični kôd ako je:*
- *linearan blok-kôd i*
- *ako bilo koji ciklični posmak kodne riječi iz K opet daje kodnu riječ iz K.*



Ako je 11110000 kodna riječ, onda su su kodne riječi i

11100001
11000011
10000111
00001111
00011110
00111100
01111000

Polinomski zapis kodne riječi

Zavod za telekomunikacije

- Kodna riječ $[a_{n-1}\ a_{n-2}\ldots\ a_2\ a_1\ a_0]$ cikličnog koda može se poistovjetiti s polinomom stupnja $n-1$:

$$\mathbf{a} = [a_{n-1}\ldots a_2\ a_1\ a_0] \leftrightarrow \quad a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x^1 + a_0x^0$$

$a(x)$ ne promatramo kao funkciju, nego čisto kao način zapisa. Na primjer,

$$a_{n-1}\left(x^n - 1\right) + a_{n-2}x^{n-1} + \ldots + a_1x^2 + a_0x^1 + a_{n-1}x^0 \quad : \quad x^n - 1 = a_{n-1}$$

Koeficijenti aritmeti

$$-a_{n-1}\left(x^n - 1\right)$$

$$a_{n-2}x^{n-1} + \ldots + a_1x^2 + a_0x^1 + a_{n-1}x^0 \qquad \leftarrow ostatak\ nakon\ dijeljenja.$$

$$= \quad a_{n-1}\left(x^n - 1\right) + a_{n-2}x^{n-1} + \ldots + a_1x^2 + a_0x^1 + a_{n-1}x^0.$$

Nad polinomima kodnih riječi vršimo operacije u aritmetici modulo x^n-1! Zbrajanje polinoma odgovora zbrajanju vektora, a množenje s x odgovara cikličnom posmaku ulijevo.

Primjer: ciklični posmak kodne riječi

Zavod za telekomunikacije

- **a= [1 0 1] – polinom je $a(x) = x^2 + 1$, duljina riječi $n = 3$**

$$b'(x) = a(x)\cdot x = x^3 + x,$$

$$x^3 + x \quad : x^3 - 1 = 1$$

$$-x^3 \quad +1$$

$$x + 1 \qquad \leftarrow ostatak\ nakon\ dijeljenja.$$

- **b** = [0 1 1] kodna riječ nastala cikličnim posmakom kodne riječi **a** ulijevo za jedno mjesto**!**
- Svaka kodna riječ duljine n je polinom stupnja $n-1$ i nad njim sve operacije provodimo u aritmetici mod x^n-1;
- Skup svih riječi u mod $x^n - 1$ aritmetici označavamo s R_n;
- Ciklični kôd je neki podskup od R_n:

$$K \subset Rn$$

Uvjeti za cikličan kôd

Zavod za telekomunikacije

***Uvjeti za cikličan kôd**: Kôd $K \subset R_n$ je cikličan kôd ako i samo ako K zadovoljava sljedeća dva uvjeta*:
- $\forall\ a(x), b(x) \in K$, *vrijedi* $a(x) + b(x) \in K$ (svojstvo linearnosti);
- $\forall\ a(x) \in K\ i\ \forall\ r(x) \in R_n$, *vrijedi* $r(x)\cdot a(x) \bmod (x^n\text{-}1) \in K$.

Kako dobiti sve kodne riječi nekog cikličkog koda?

- izaberi bilo koji polinom $f(x)$ najvećeg stupnja $n-1$;
- sve kodne riječi cikličnog koda K dobit će se množenjem svih $r(x) \in R$ s $f(x)$;

Kaže se da je kôd K generiran polinomom $f(x)$:

$$K \equiv \langle f(x) \rangle = \{r(x)\, f(x) \mid r(x) \in R_n\}.$$

$f(x)$ je kodna riječ koda K!

Primjer: generiranje cikličnog koda

Zavod za telekomunikacije

- Polinom kojim se generira kôd *K*: $f(x) = x^2 + 1$
- n=3, broj polinoma u R^n je $2^3 = 8$.

$$
\begin{array}{lcll}
(0x^2+0x+0) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 0x^2+0x+0 \quad [000] \\
(0x^2+0x+1) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 1x^2+0x+1 \quad [101] \\
(0x^2+1x+0) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 0x^2+1x+1 \quad [011] \\
(0x^2+1x+1) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 1x^2+1x+0 \quad [110] \\
(1x^2+0x+0) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 1x^2+1x+0 \quad [110] \\
(1x^2+0x+1) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 0x^2+1x+1 \quad [011] \\
(1x^2+1x+0) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 1x^2+0x+1 \quad [101] \\
(1x^2+1x+1) & \cdot & (x^2+1)(\mathrm{mod}\,(x^3-1)) & = 0x^2+0x+0 \quad [000]
\end{array}
$$

$$
K = \begin{Bmatrix} 0\,0\,0 \\ 1\,0\,1 \\ 0\,1\,1 \\ 1\,1\,0 \end{Bmatrix} \Rightarrow \mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}
$$

Generirajući polinom cikličnog koda

Zavod za telekomunikacije

Generiranje cikličnog koda: *Neka je K ciklični kôd dimenzije veće od* 1, *podskup od* R_n.
- *Postoji jedinstven polinom g(x) najmanjeg stupnja u K.*
- *Kôd K je generiran upravo polinomom g(x).*
- *g(x) je faktor polinoma* $x^n - 1$, *tj.* $x^n - 1 = g(x) \cdot q(x)$.

Polinom $g(x)$ koji zadovoljava ovo svojstvo nazivamo:

Generirajući polinom cikličkog koda

Primjer: $g(x)$ je jedan od faktora polinoma $x^{15} - 1$:

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

Svaki faktor generira jedan mogući ciklički kôd, pa faktoriziranjem polinoma $x^{15} - 1$ praktički dobivamo 5 različitih cikličkih kodova s generirajućim polinomima:

$$g_1(x) = x+1, \quad g_2(x) = x^2+x+1, \quad g_3(x) = x^4+x+1,$$
$$g_4(x) = x^4+x^3+1, \quad g_5(x) = x^4+x^3+x^2+x+1$$

Generirajuća matrica cikličnog koda

Zavod za telekomunikacije

Generirajuća matrica cikličnog koda: *Neka je generirajući polinom cikličnog koda* $K \subset R_n$:

$$g(x) = g_r x^r + \ldots + g_2 x^2 + g_1 x + g_0.$$

Onda je dimenzija koda $k = n - r$, *a generirajuća matrica koda je*:

$$
\mathbf{G} = \begin{bmatrix}
g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\
0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\
0 & 0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & \vdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & 0 & \cdots & 0 & g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0
\end{bmatrix}.
$$

- Broj redaka matrice **G** odgovara dimenziji koda - $k = n - r$;
- Broj stupaca matrice **G** odgovara duljini kodne riječi – n;
- Što je stupanj generirajućeg polinoma $g(x)$ veći, dimenzija koda je manja!

Primjer: generirajuća matrica cikličnog koda (n = 5)

Zavod za telekomunikacije

$$n = 5 \Rightarrow x^5 - 1 = (x+1)(x^4+x^3+x^2+x+1)$$

Potencijalni generirajući polinomi:

$$g_1(x) = x+1 \Leftarrow r = 1, k = 5-1 = 4$$
$$g_2(x) = x^4+x^3+x^2+x+1 \Leftarrow r = 4, k = 5-4 = 1$$

$$
g_1(x) = x+1 \Rightarrow \mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad k = 4, \quad n = 5
$$

$$
g_2(x) = x^4+x^3+x^2+x^1+1 \Rightarrow \mathbf{G} = [\,1\;1\;1\;1\;1\,]
$$

Faktorizacije nekih polinoma oblika $x^n - 1$

Zavod za telekomunikacije

n	aritmetika	*faktorizacija u aritmetici modulo 2*
1	x^1-1	$x+1$
2	x^2-1	$(x+1)^2$
3	x^3-1	$(x+1)(x^2+x+1)$
5	x^5-1	$(x+1)(x^4+x^3+x^2+x+1)$
7	x^7-1	$(x+1)(x^3+x+1)(x^3+x^2+1)$
9	x^9-1	$(x+1)(x^2+x+1)(x^6+x^3+1)$
11	$x^{11}-1$	$(x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
13	$x^{13}-1$	$(x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
15	$x^{15}-1$	$(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$
17	$x^{17}-1$	$(x+1)(x^8+x^5+x^4+x^3+1)(x^8+x^7+x^6+x^4+x^2+x+1)$
19	$x^{19}-1$	$(x+1)(x^{18}+x^{17}+x^{16}+\ldots+x^4+x^3+x^2+x+1)$

Standardni oblik generirajuće matrice

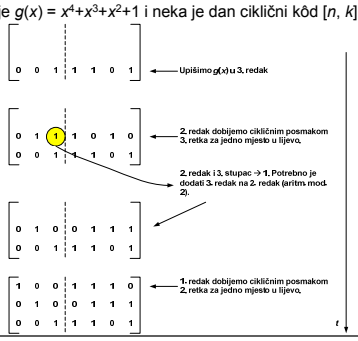
Zavod za telekomunikacije

- Traženi oblik matrice **G**: $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{A}]$.

ALGORITAM:
- I. Upiši $g(x)$ u binarnom obliku u k-ti redak.
- II. (k - 1)-vi redak dobije se cikličnim posmakom k-tog retka za jedno mjesto u lijevo. Ovo odgovara operaciji $xg(x)$.
- k-ti stupac mora u (k - 1)-om retku imati nulu kako bi imali standardni oblik matrice **G**.
  - Ako je 1 → na (k - 1)-i redak treba dodati k-ti redak (aritm. mod. 2);
- III. Za (k - 2) redak treba primijeniti postupak iz točke II.
  - Napraviti ciklični posmak (k - 1)-og retka za jedno mjesto u lijevo.
  - Ako k–ti stupac u (k - 2)-om retku ima 1 → dodaj na (k - 2)-i redak k-ti redak (aritm. mod. 2);
- Ponavljaj algoritam za svaki sljedeći redak sve dok se ne popuni matrica **G**.

Primjer: standardni oblik generirajuće matrice **G**

- Neka je $g(x) = x^4+x^3+x^2+1$ i neka je dan ciklični kôd $[n, k] = [7, 3]$.



Matrica provjere pariteta cikličnog koda

Polinom za provjeru pariteta: *Neka je K ciklični kôd duljine n i dimenzije k [n,k] s generirajućim polinomom g(x). Neka je h(x) polinom koji zadovoljava jednadžbu:*

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

h(x) se zove ***polinom za provjeru pariteta*** *cikličnog koda K.*

Matrica provjere pariteta cikličnog koda: *Neka je $K \subset R_n$ ciklični kôd duljine n i dimenzije k s generirajućim polinomom g(x) i polinomom za provjeru pariteta*

$$h(x) = h_k x^k + \ldots + h_2 x^2 + h_1 x + h_0.$$

- *Bilo koji polinom c(x) koda K zadovoljava jednakost $c(x)\cdot h(x) = 0$.*
- *Paritetna matrica koda K je*:

$$\mathbf{H} = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & 0 & \cdots & 0 \\ 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & 0 & \cdots & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k & \vdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k \end{bmatrix}.$$

Primjer: matrica provjere pariteta cikličnog koda ($n = 7$)

Promatramo ciklički kod $n = 7$: $g(x) = x^3 + x^2 + 1$

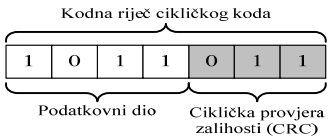
$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \quad \Rightarrow \quad h(x) = \underbrace{1 + x^2 + x^3 + x^4}_{1\ 0\ 1\ 1\ 1}$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & & & & & \end{bmatrix} \quad r = 3, \quad n = 7$$

Implementacija kodera cikličnog koda (1/2)

- Duljina kodne riječi može biti iznimno velika!
- Generirajuća i paritetna matrica imaju prevelike dimenzije za praktičnu implementaciju.
- Želimo kodnu riječ koja je sistematična tako da odmah možemo razlučiti zaštitne bitove od bitova kodirane poruke:



Rješenje:

- Ciklička provjera zalihosti izračunati na osnovu podatkovnog dijela!

Implementacija kodera cikličnog koda (2/2)

- $d(x)$ – polinom kodirane poruke: $[\ 1\ 0\ 1\ 1\ 1\ ] \rightarrow d(x) = x^4+x^2+x+1$
- $d(x)$ se može pomnožiti s x^r, gdje je r stupanj generirajućeg polinoma:

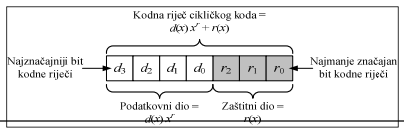
$$d(x)\cdot x^r = g(x)q(x) + r(x).$$

ostatak nakon dijeljenja s $g(x)$

generirajući polinom — kvocijent

Svaki polinom pomnožen s $g(x)$ u aritmetici $\bmod x^n - 1$ je neka kodna riječ $c(x)$ koda K, pa je i $g(x)\cdot q(x)$ neka kodna riječ. Stoga se bilo koja kodna riječ može dobiti kao zbroj:

$$c(x) = g(x)q(x) = d(x)\cdot x^r + r(x),$$
$$r(x) = d(x)\cdot x^r \bmod [g(x)].$$



Primjer: Generiranje CRC-a

- Poruka je: $\mathbf{d} = [\ 1\ 0\ 1\ 0\ ]$, tj. $d(x) = x^3 + x$,
- Generirajući polinom: $g(x) = x^3 + x + 1$ – $[\ 1\ 0\ 1\ 1\ ]$,
- Umnožak: $d(x)\cdot x^3 = x^6 + x^4$ – $[\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ ]$.

$$\overbrace{1\ 0\ 1\ 0\ 0\ 0\ 0}^{d(x)} : \overbrace{1\ 0\ 1\ 1}^{g(x)} = 1\ 0\ 0\ 1$$

$$\begin{array}{r} -\ 1\ 0\ 1\ 1 \\ \hline 0\ 0\ 1 \\ -\ 0\ 0\ 0\ 0 \\ \hline 0\ 1\ 0 \\ -\ 0\ 0\ 0\ 0 \\ \hline 1\ 0\ 0 \\ -\ 1\ 0\ 1\ 1 \\ \hline \boxed{0\ 1\ 1} \end{array}$$

ostatak nakon dijeljenja

Primjer: Dijeljenje polinoma - Generiranje CRC-a

Zavod za telekomunikacije

$q(x) = 1\ 0\ 0\ 1$

$g_3\ g_2\ g_1\ g_0$

1 0 1 1 0 0 0 0 0 : 1 0 1 1

– 1 0 1 1

(1) $R_3 = R_2 \oplus (R_3 \cdot g_2)$

(2) $R_2 = R_1 \oplus (R_3 \cdot g_1)$

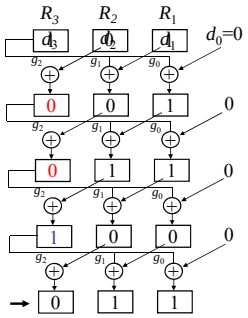
(3) $R_1 = \text{ulazni bit} \oplus (R_3 \cdot g_0)$,

1 0 0

– 1 0 1 1

0 1 1

ostatak nakon dijeljenja



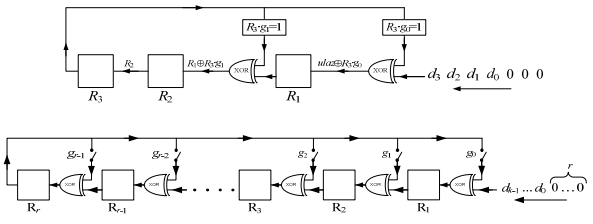
Primjer: Sklop za generiranje CRC-a

Zavod za telekomunikacije

(1) $R_3 = R_2 \oplus (R_3 \cdot g_2)$

(2) $R_2 = R_1 \oplus (R_3 \cdot g_1)$

(3) $R_1 = \text{ulazni bit} \oplus (R_3 \cdot g_0)$,



Implementacija dekodera (1/4)

Zavod za telekomunikacije

- Proračun sindroma ima preveliku složenost zbog velike duljine kodnih riječi.
- Temeljno pitanje: Možemo li sindrom izračunati principom sličnim izračunu zalihosnog dijela CRC?
- Smisao sindroma: *Svaka kodna riječ na kojoj je nastupila pogreška na istoj poziciji mora imati isti sindrom*!

e				**S(y)**
0 0 0 0 0	1 1 1 0 0	0 0 1 1 1	1 1 0 1 1	0 0 0
0 0 0 0 1	1 1 1 0 1	0 0 1 1 0	1 1 0 1 0	0 0 1
0 0 0 1 0	1 1 1 1 0	0 0 1 0 1	1 1 0 0 1	0 1 0
0 0 1 0 0	1 1 0 0 0	0 0 0 1 1	1 1 1 1 1	1 0 0
0 1 0 0 0	1 0 1 0 0	0 1 1 1 1	1 0 0 1 1	1 0 1
1 0 0 0 0	0 1 1 0 0	1 0 1 1 1	0 1 0 1 1	1 1 0

Implementacija dekodera (2/4)

Zavod za telekomunikacije

$e(x)$ je polinom pogreške: $\mathbf{e} = [\ 1\ 0\ 0\ 1\ 1\ ]$, $e(x) = x^4 + x + 1$

Primljena kodna riječ: $y(x) = c(x) + e(x)$.

Što dobivamo funkcijom $S[y(x)] = x^r \cdot y(x) \mod g(x)$?

$$\begin{aligned} S[y(x)] &= x^r y(x) \mod g(x) \\ &= x^r [c(x) + e(x)] \mod g(x) \\ &= x^r c(x) \mod g(x) + x^r e(x) \mod g(x) \\ &= S[c(x)] + S[e(x)]. \end{aligned}$$

$$\begin{aligned} c(x) &= g(x)q(x) \quad | \cdot x^r \quad \Rightarrow \\ c(x)x^r &= g(x)q(x)x^r. \end{aligned}$$

Ako $c(x) \cdot x^r$ podijelimo s $g(x)$ ostatak je 0!

$$S[c(x)] = x^r \cdot c(x) \mod g(x) = 0.$$

Implementacija dekodera (3/4)

Zavod za telekomunikacije

Primjenom funkcije $S[y(x)] = x^r \cdot y(x) \mod g(x)$

na primljenu kodnu riječ $y(x)$ dobivamo:

$$S[y(x)] = S[c(x)] + S[e(x)] = S[e(x)],$$

$S[y(x)]$ za kodne riječi s istom pogreškom uvijek daje isti rezultat!

$S[y(x)]$ je funkcija za računanje sindroma primljene kodne riječi!!!

$$S[y(x)] = x^r \cdot y(x) \mod [g(x)]$$
$$r(x) = d(x) \cdot x^r \mod [g(x)].$$

JOŠ VAŽNIJE:
Sindrom se određuje na IDENTIČAN način kao i zaštitni dio kodne riječi. Slijedi da je i sklop za računanje sindroma jednak onome za izračunavanje CRC-a!

Implementacija dekodera (4/4)

Zavod za telekomunikacije

Primjer dekodera za slučaj koda (7, 4, 3) s generirajućim polinomom: $g(x) = x^3 + x + 1$

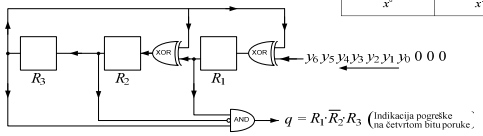
Tablica sindroma

$e(x)$	$S[e(x)]$
1	$x+1$
x	x^2+x
x^2	x^3+x+1
x^3	x^2+1
x^4	1
x^5	x
x^6	x^2

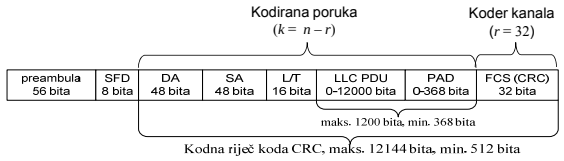
Želimo detektirati pogrešku na 4. bitu – $e(x)=x^3$

$$S[y(x)] = S[e(x)] = x^2 + 1$$

$$q = R_3 \cdot \overline{R_2} \cdot R_1$$



Primjer cikličkog koda – Ethernetski okvir – *CRC-32*



$g(x) = x^{32} + x^{26} + x^{23}$ [illegible] $x^5 + x^4 + x^2 + x + 1$.

duljina koda K - n	distanca $d(K)$
$3007 \le n \le 12144$	4
$301 \le n \le 3006$	5
$204 \le n \le 300$	6
$124 \le n \le 203$	7
$90 \le n \le 123$	8
$67 \le n \le 89$	9