

Zaštitno kodiranje II

Teorija informacije

- ▢ Uvod
 - Komunikacijski sustav; Cilj zašt. kodiranja; Podjela zaštitnih kodova.
- ▢ Blok kodovi
 - Uvod
 - Paritetno kodiranje
 - Linearno binarni blok kodovi
 - Generirajuća matrica \mathbf{G} i njen standardni oblik
 - Kodiranje
 - Dekodiranje (dekodiranje preko sindroma)
 - Proračun vjerojatnosti ispravnog dekodiranja
 - Hammingovi kodovi
 - Ciklični kodovi

Hammingovi i ciklični kodovi

(klasa linearnih blok kodova)

Hammingovi kodovi

Definicija: Hammingov kôd



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

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

$$\mathbf{H}_1^T = \begin{matrix} \text{?} & 0 & 1 & \text{?} \\ \text{?} & 1 & 0 & \text{?} \\ \text{?} & 1 & 1 & \text{?} \\ \text{?} & 0 & 0 & \text{?} \\ \text{?} & 0 & 1 & \text{?} \\ \text{?} & 1 & 0 & \text{?} \\ \text{?} & 1 & 1 & \text{?} \end{matrix} \quad \text{ili} \quad \mathbf{H}_2^T = \begin{matrix} \text{?} & 1 & 1 & \text{?} \\ \text{?} & 1 & 0 & \text{?} \\ \text{?} & 1 & 1 & \text{?} \\ \text{?} & 0 & 1 & \text{?} \\ \text{?} & 0 & 0 & \text{?} \\ \text{?} & 1 & 0 & \text{?} \\ \text{?} & 0 & 1 & \text{?} \end{matrix}$$

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

Svojstva Hammingovih kodova: Neka je $\text{Ham}(r)$ binarni Hammingov kôd. Za $r \geq 2$ vrijedi da je $\text{Ham}(r)$:

- *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



- ▮ Primjer: Hammingov kôd [7, 4, 3]

$$\mathbf{H} = \begin{array}{c} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \begin{array}{|c|} \hline ? \\ \hline \end{array} \end{array} \begin{array}{ccccccc} 0 & 1 & 0 & 1 & 0 & 1 & ? \\ 1 & 1 & 0 & 0 & 1 & 1 & ? \\ 0 & 0 & 1 & 1 & 1 & 1 & ? \end{array}$$

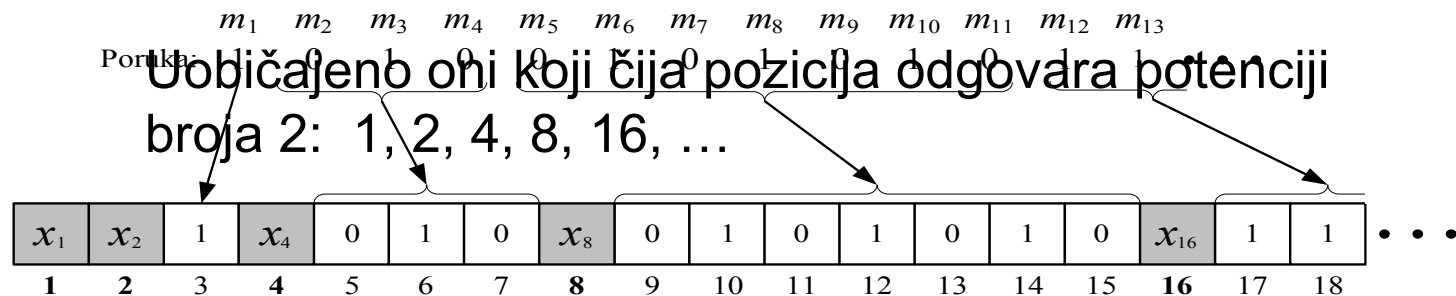
- ▮ Generirajuću matricu **G** nije jednostavno izračunati iz **H** jer ista nije u standardnom obliku, tj. jednačba $\mathbf{GH}^T = \mathbf{0}$ daje velik broj mogućnosti.
- ▮ Potrebno je dobiti sistematičan kôd iz kojeg jednostavno dobivamo poslanu kodiranu poruku.
- ▮ **Važno svojstvo matrice H:** 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

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

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?



$$x_1 = m_1 + m_2 + m_4 + m_8 + m_{16} + \dots + K$$

$$x_2 = m_1 + m_3 + m_6 + m_7 + m_{10} + m_{11} + \dots + K$$


$$x_4 = m_2 + m_3 + m_5 + m_6 + m_9 + m_{10} + m_{12} + m_{13} + m_{14} + m_{15} + \dots + K$$

M

M

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



Poruka  1 0 1 0

x_1	x_2		x_4			
-------	-------	--	-------	--	--	--

Okvir kodne riječi

H =

x		x		Ø		Ø	?
	Ø	x			x	Ø	?
			x	Ø	x	Ø	?

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



- (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

1 2 4
↓ ↓ ↓

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

Generirajuća matrica Hammingovog kôda

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

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

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

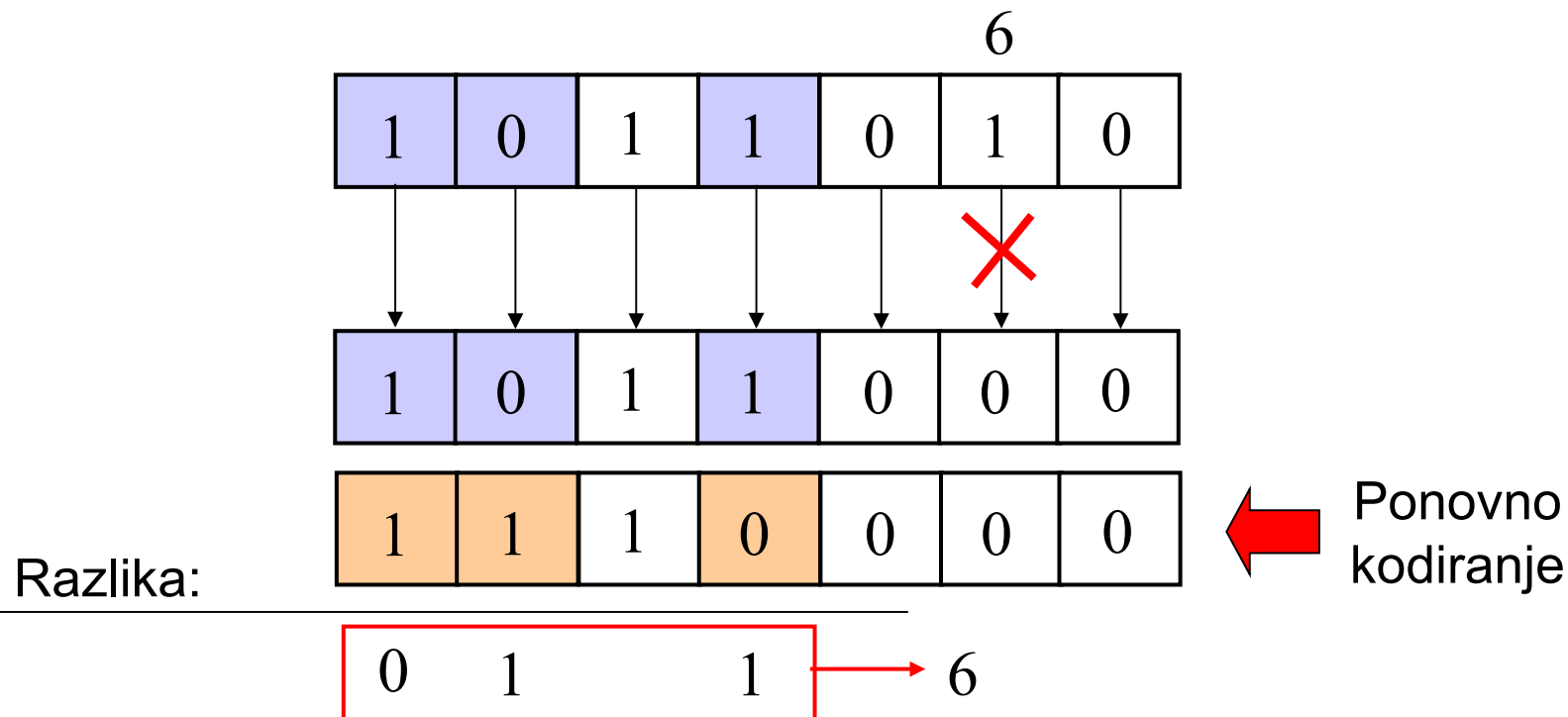


Napomena: Vrijedi samo za standardni način formiranja Hammingovih riječi!

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

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

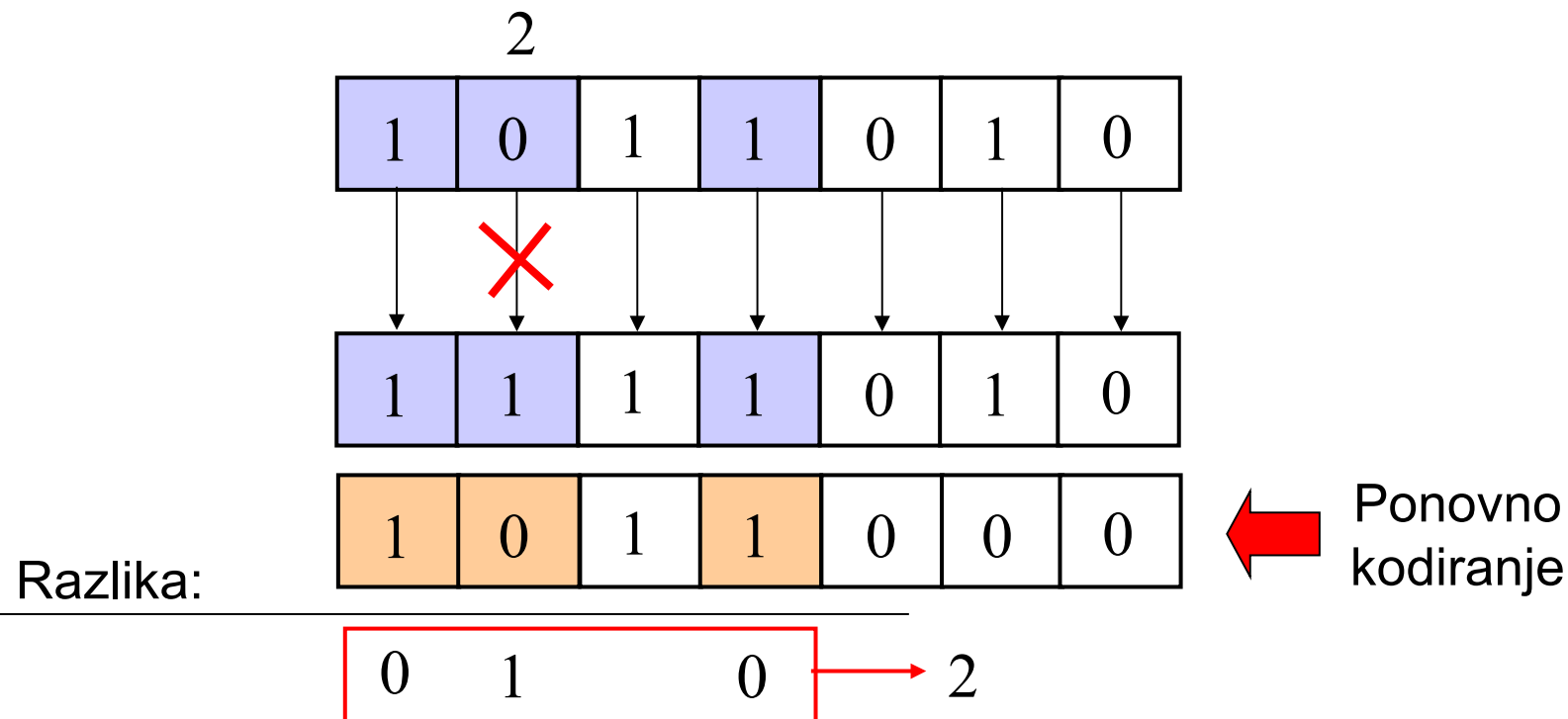
Primjer: određivanje sindroma bez matrice provjere pariteta (1/2)



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

Primer: određivanje sindroma bez matrice provjere pariteta

(2/2)



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

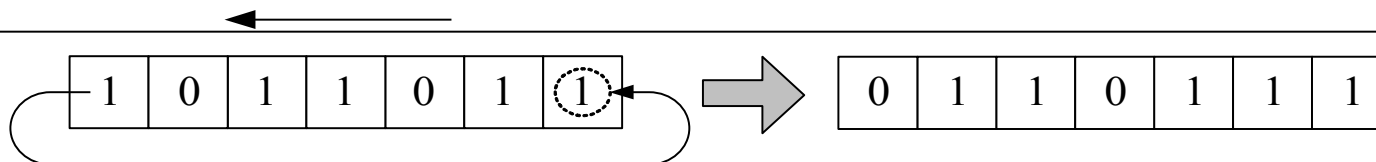
Ciklični kodovi

Definicija: ciklični kôd



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 kodne riječi i

11100001
11000011
10000111
00001111
00011110
00111100
01111000

Polinomski zapis kodne riječi



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

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

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

$$x^4(1+x^2) = 1 + x^2 + x^4 + x^6 + \dots \quad \mathbf{a} = [1 \ 0 \ 1 \ 0 \ 1] \Rightarrow a(x) = x^4 + x^2 + 1 = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x^1 + a_0x^0$$

Koeficijenti a_i su iz skupa $\{0, 1\}$, a sve operacije nad njima provodimo u aritmetici modulo 2. Ciklički posmak ulijevo možemo realizirati ovako:

$$= x^n(a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x^1 + a_0x^0) = a_{n-1}x^{2n-1} + a_{n-2}x^{2n-2} + \dots + a_1x^{2n-1} + a_0x^{2n-1}$$

$$= a_{n-1}(x^n - 1) + a_{n-2}x^{n-1} + \dots + a_1x^2 + a_0x^1 + a_{n-1}x^0.$$

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

Primjer: ciklični posmak kodne riječi



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

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

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

$$\begin{array}{r} -x^3 \quad +1 \\ \hline x+1 \end{array}$$

▮ *ostatak nakon dijeljenja.*

- ▮ $\mathbf{b} = [0\ 1\ 1]$ kodna riječ nastala cikličnim posmakom kodne riječi \mathbf{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 :

$$K \subseteq R_n$$

Uvjeti za cikličan kôd: Kôd $K \subseteq R_n$ 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);
- $\forall a(x) \in K \text{ i } \forall r(x) \in R_n$, vrijedi $r(x) \cdot a(x) \bmod (x^n - 1) \in K$.

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 $f(x)$:

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

$f(x)$ je kodna riječ koda K !

Primjer: generiranje cikličnog koda



Polinom kojim se generira kôd $f(x) = x^2 + 1$

$n=3$, broj polinoma u R^n je $2^3 = 8$.

$(0x^2 + 0x + 0)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 0x^2 + 0x + 0$	[000]
$(0x^2 + 0x + 1)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 1x^2 + 0x + 1$	[101]
$(0x^2 + 1x + 0)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 0x^2 + 1x + 1$	[011]
$(0x^2 + 1x + 1)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 1x^2 + 1x + 0$	[110]
$(1x^2 + 0x + 0)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 1x^2 + 1x + 0$	[110]
$(1x^2 + 0x + 1)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 0x^2 + 1x + 1$	[011]
$(1x^2 + 1x + 0)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 1x^2 + 0x + 1$	[101]
$(1x^2 + 1x + 1)$	$\diamond (x^2 + 1)(\text{mod } (x^3 - 1))$	$= 0x^2 + 0x + 0$	[000]

$$K = \begin{cases} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{cases}$$



$$G = \begin{matrix} \diamond & 0 & 1 & \diamond \\ \diamond & & & \diamond \\ \diamond & 1 & 1 & \diamond \end{matrix}$$

Generirajući polinom cikličnog koda



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:

$$\begin{aligned} g_1(x) &= x + 1, & g_2(x) &= x^2 + x + 1, & g_3(x) &= x^4 + x + 1, \\ g_4(x) &= x^4 + x^3 + 1, & g_5(x) &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Generirajuća matrica cikličnog koda

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

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

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

$$G = \begin{pmatrix} g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & 0 & 0 & \dots & 0 \\ 0 & g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & 0 & \dots & 0 \\ 0 & 0 & g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ M & M & O & O & O & O & O & O & O & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & L & 0 & g_r & g_{r-1} & g_{r-2} & L & g_1 & g_0 & \vdots \end{pmatrix}$$

- 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 ($n = 5$)



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

Potencijalni generirajući polinomi: $\left\{ \begin{array}{ll} g_1(x) = x + 1 & \leftarrow r = 1, k = 5 - 1 = 4 \\ g_2(x) = x^4 + x^3 + x^2 + x + 1 & \leftarrow r = 4, k = 5 - 4 = 1 \end{array} \right.$

$$g_1(x) = x + 1 \quad \Rightarrow \quad \mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad \begin{array}{c} \uparrow \\ k = 4 \\ \downarrow \end{array}$$

$\leftarrow n = 5 \rightarrow$

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

Faktorizacije nekih polinoma oblika $x^n - 1$



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	$x^{19} - 1$	$(x + 1)(x^{18} + x^{17} + x^{16} + \dots + x^4 + x^3 + x^2 + x + 1)$

Standardni oblik generirajuće matrice



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

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 \mathbf{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 \mathbf{G} .

Primjer: standardni oblik generirajuće matrice G



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

$$\left[\begin{array}{ccc|cccc} & & & & & & \\ & & & & & & \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right] \quad \leftarrow \text{Upišimo } g(x) \text{ u 3. redak}$$

$$\left[\begin{array}{ccc|cccc} & & & & & & \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right] \quad \leftarrow \begin{array}{l} \text{2. redak dobijemo cikličnim posmakom} \\ \text{3. retka za jedno mjesto u lijevo.} \end{array}$$

2. redak i 3. stupac \rightarrow 1. Potrebno je dodati 3. redak na 2. redak (aritm. mod. 2).

$$\left[\begin{array}{ccc|cccc} & & & & & & \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right]$$

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right] \quad \leftarrow \begin{array}{l} \text{1. redak dobijemo cikličnim posmakom} \\ \text{2. retka za jedno mjesto u lijevo.} \end{array}$$

$t \downarrow$

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 $K \subseteq R_n$ ciklični kôd duljine n i dimenzije k s generirajućim polinomom $g(x)$ i polinomom za provjeru pariteta $h(x) = h_{k-1}x^{k-1} + \dots + h_2x^2 + h_1x + h_0$.

• Bilo koji polinom $c(x)$ koda K zadovoljava jednakost $c(x) \cdot h(x) = 0$.

• Paritetna matrica koda K je:

$$H = \begin{pmatrix} h_{k-1} & h_k & 0 & 0 & L & 0 & ? \\ 0 & h_0 & h_1 & h_2 & L & h_{k-1} & h_k & 0 & L & 0 & ? \\ ? & 0 & h_0 & h_1 & h_2 & L & h_{k-1} & h_k & M & 0 & ? \\ ? & M & M & O & O & O & O & O & O & 0 & ? \\ ? & 0 & L & 0 & h_0 & h_1 & h_2 & L & h_{k-1} & h_k & ? \end{pmatrix}$$

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



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

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

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

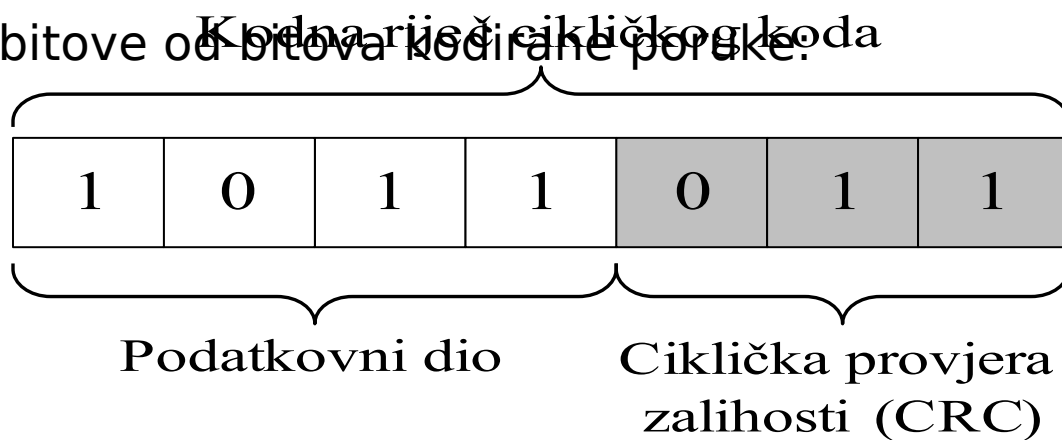
$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & & & & & \end{bmatrix} \quad \begin{matrix} \uparrow \\ r=3 \\ \downarrow \end{matrix}$$

$\leftarrow n = 7 \rightarrow$

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:

- ▮ Cikličku provjeru 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:

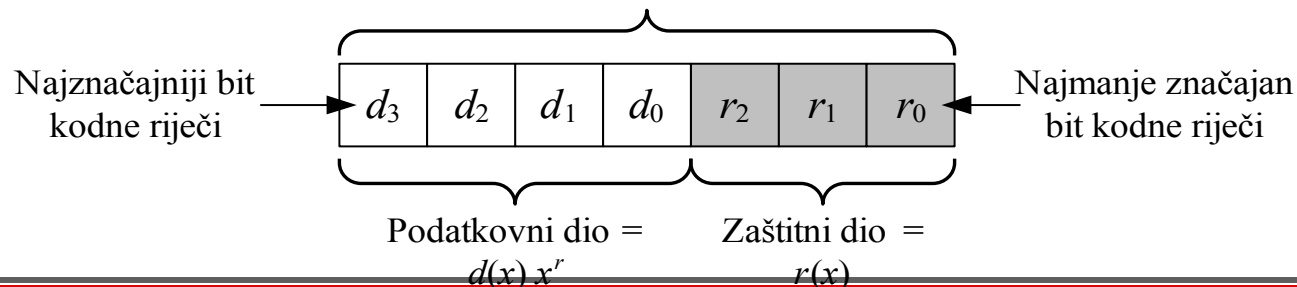
$$d(x) \square x^r = \underset{\text{generirajući polinom}}{g(x)} \underset{\text{kvocijent}}{q(x)} \square \underset{\text{ostatak nakon dijeljenja s } g(x)}{r(x)}.$$

Svaki polinom pomnožen s $g(x)$ u aritmetici mod $x^n - 1$ 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:

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

$$r(x) = d(x) \square x^r \bmod [g(x)].$$

Kodna riječ cikličkog koda =
 $d(x) x^r + r(x)$



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: $d(x) \cdot x^3 = x^6 + x^4$ – $[1\ 0\ 1\ 0\ 0\ 0\ 0]$.

$$\begin{array}{r} \overbrace{1\ 0\ 1\ 0\ 0\ 0\ 0}^{d(x)} : \overbrace{1\ 0\ 1\ 1}^{g(x)} = 1\ 0\ 0\ 1 \\ -\ 1\ 0\ 1\ 1 \\ \hline 0\ 0\ 1 \\ -\ 0\ 0\ 0\ 0 \\ \hline 0\ 1\ 0 \\ -\ 0\ 0\ 0\ 0 \\ \hline 1\ 0\ 0 \\ -\ 1\ 0\ 1\ 1 \\ \hline \boxed{0\ 1\ 1} \end{array}$$

ostatak nakon dijeljenja

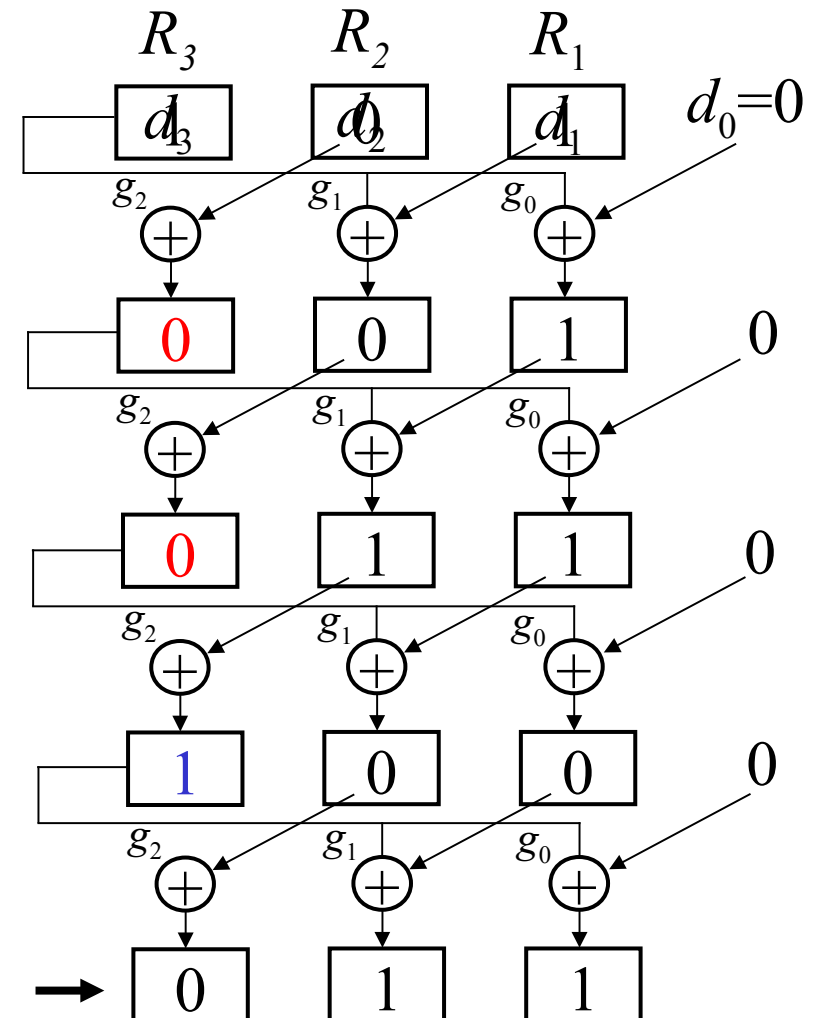
Primjer: Dijeljenje polinoma -Generiranje CRC-a



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

$$\begin{array}{r}
 \boxed{1 \ 0 \ 1} \ 0 \ 0 \ 0 \ 0 : \overset{g_3}{1} \ \overset{g_2}{0} \ \overset{g_1}{1} \ \overset{g_0}{1} \\
 - \quad \boxed{1 \ 0 \ 1 \ 1} \\
 \hline
 (1) \ \boxed{0 \ 0 \ 1} \neq R_2 \quad ? (R_3 \quad ?) \\
 (2) \ \overset{0}{R_2} \ \overset{0}{0} \ \overset{0}{0} = \overset{0}{0} \quad R_1 \quad ? (R_3 \quad ?) \\
 (3) \ \boxed{0 \ 1 \ 0} \quad \text{ulazni bit } ? (R_3 \quad ?), \\
 \quad \overset{0}{R_2} \ \overset{0}{0} \ \overset{0}{0} \ \overset{0}{0} \\
 \hline
 \quad \boxed{1 \ 0 \ 0} \\
 \quad - \quad \boxed{1 \ 0 \ 1 \ 1} \\
 \quad \hline
 \quad \boxed{0 \ 1 \ 1}
 \end{array}$$

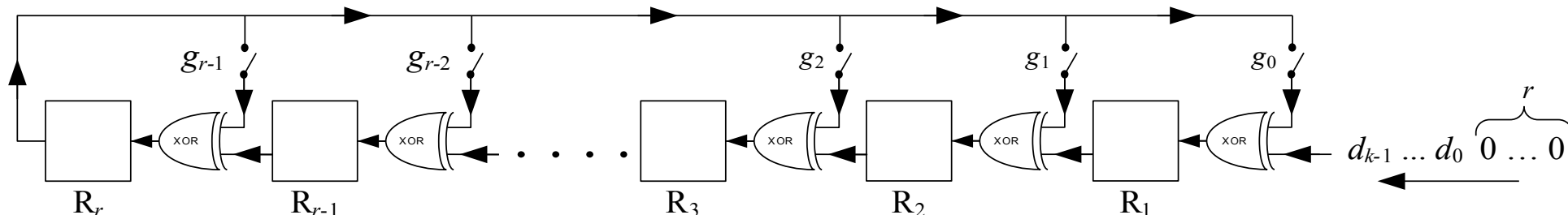
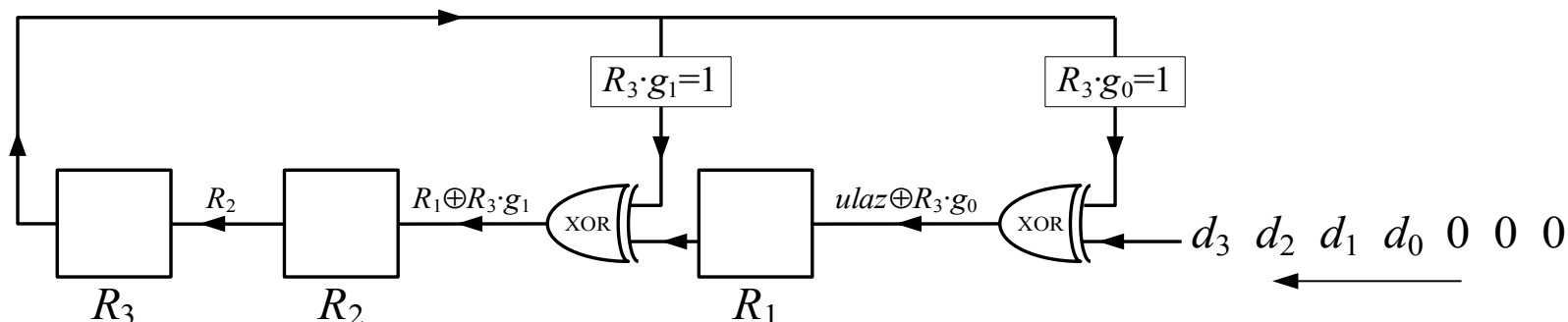
ostatak nakon dijeljenja →



Primjer: Sklop za generiranje CRC-a



$$\begin{aligned} (1) \quad R_3 &= R_2 \oplus (R_3 \oplus g_2) \\ (2) \quad R_2 &= R_1 \oplus (R_3 \oplus g_1) \\ (3) \quad R_1 &= \text{ulazni bit} \oplus (R_3 \oplus g_0), \end{aligned}$$



Implementacija dekodera (1/4)



- ▣ 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)



$e(x)$ 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 $S[y(x)] = x^r \square y(x) \bmod g(x)$?

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

$$\begin{aligned} c(x) &= g(x)q(x) \mid \text{?}^r \text{?} \\ c(x)x^r &= g(x)q(x)x^r. \end{aligned}$$

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

$$S[c(x)] = x^r \square c(x) \bmod g(x) = 0.$$

Implementacija dekodera (3/4)



Primjenom funkcije $S[y(x)] = x^r \square y(x) \bmod g(x)$

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!!!

$$S[y(x)] = x^r \square y(x) \bmod [g(x)]$$

$$r(x) = d(x) \square x^r \bmod [g(x)].$$

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)

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

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

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

$$q = R_3 \cdot R_2 \cdot R_1$$

Tablica sindroma

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

