TEMA 6.3 CODURI CICLICE

Codurile ciclice sunt sistematice liniare- bloc.

Fiecare cuvânt de cod este codat și decodat aparte (coduri bloc), cuvintele de cod constau din n_0 biți informaționali și k biți de control (coduri sistematice).

Codurile ciclice se notează (n, n_0).

Cuvintele de cod se pot scrie sub forma unei matrice de formare cu n coloane, în care n_0 rânduri sunt liniar independente. Fiecare rând din matrice poate fi obținut prin deplasarea ciclică la stânga a unui cuvânt de cod inițial.

0001011
0010110
0101100
1011000
0110001
1100010
1000101

Elementele cuvântului de cod $d = (d_{n-1}, d_{n-2}, \ldots, d_0)$ pot fi considerate drept coeficienţi a unui polinom cu variabila fictivă x.

$$d(x) = d_{n-1} \cdot x^{n-1} + d_{n-2} \cdot x^{n-2} + \ldots + d_0 \cdot x^0$$

Exemplu: $01011 = x^3 + x + 1$ (Polinom de ordinul 3). Ordinul polinomului se determină după puterea cea mai mare a lui x cu coeficientul 1.

Exemple:

10111

100010

1101110

ARITMETICA POLINOMIALĂ

Adunarea şi scăderea.

Reg. de adunare:	Reg. de scădere:	Exemple:		
$0+0=0$ $0+1=1$ $1+0=1$ $1+1=0^*$	$0-0=0$ $0-1=1^*$ $1-0=1$ $1-1=0$	$+\begin{array}{r}1010\\ \underline{1111}\\ 0101\end{array}\ \oplus$	$-\begin{array}{r}1010\\ \underline{1111}\\ 0101\end{array}\ \oplus$	$\begin{array}{r}10101101\\ 00101000\\ 11101011\\ \overline{01101110}\end{array}\ +,-$

În aritmetica polinomială $x+x=0$, deoarece $x+x=(1+1)\cdot x=0\cdot x=0$.

ÎNMULȚIREA

Înmulţirea polinomului la x^i coincide cu deplasarea la stânga cu i biţi.

$$x^3 \cdot (x^3 + x + 1) = x^6 + x^4 + x^3$$

$$1000 \cdot (1011) = 1011000$$

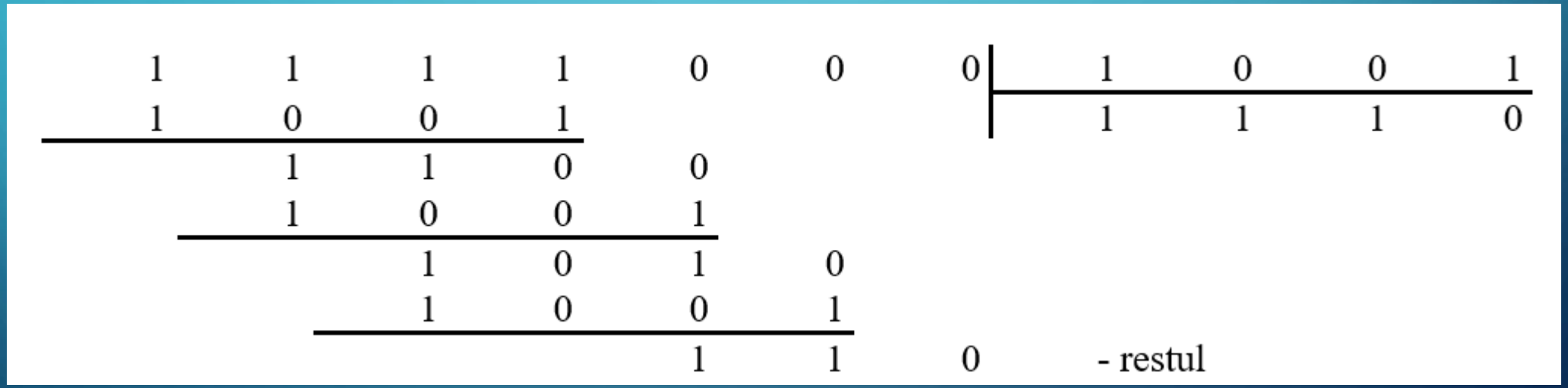
Înmulţirea unui polinom la altul constă din 2 etape: 1. Determinarea produselor intermediare conform regulilor aritmeticii clasice. 2. Adunarea produselor intermediare conform regulilor aritmeticii polinomiale.

$$(x^4 + x^2 + x + 1) \cdot (x^3 + x + 1) = x^7 + 1$$

			1	0	1	1	1
				1	0	1	1
			1	0	1	1	1
		1	0	1	1	1	⊕
1	0	1	1	1		⊕	
1	0	0	0	0	0	0	1

ÎMPĂRȚIREA

Împărțirea se efectuiază conform regulilor aritmeticii clasice cu excepția operațiilor de scădere, care se înlocuesc cu adunarea mod 2. Împărțirea se efectuiază până când ordinul restului nu va fi mai mic decât ordinul împărțitorului.



EXEMPLU

X=1011000, Y=1101

Deplasarea ciclică la stânga e echivalentă cu înmulţirea la x şi împărţirea la x^n+1.

$$1101 \Rightarrow x^3 + x^2 + 1$$

$$x^n + 1 = x^4 + 1$$

$$x \cdot (x^3 + x^2 + 1) = x^4 + x^3 + x$$

$$\begin{array}{l|l} x^4 + x^3 + x & x^4 + 1 \\ \underline{x^4 \qquad\quad + 1} & \\ x^3 + x + 1 \Rightarrow 1011 & \end{array}$$

POLINOAME GENERATOARE

În codurile ciclice fiecare cuvânt de cod este multiplu al unui și acelui polinom de ordin $n-n_0=k$, numit polinom generator **g(x)**.

g(x) este un polinom primitiv (nu poate fi reprezentat în formă de produs a altor polinoame de ordin mai mic).

În orice **g(x)** coeficientul lui $\mathbf{x_0}$ este egal cu **1**. Este o condiție de formare a polinomului primitiv.

Fiecare cuvânt de cod valid se împarte fără rest doar la **g(x)**.

Orice alt cuvânt interzis se va împărți cu rest. Valoarea restului permite detectarea și corectarea erorilor.

EXEMPLE DE POLINOAME GENERATOARE

$x+1$	11	3
x^2+x+1	111	7
x^3+x+1	1011	11
x^3+x^2+1	1101	13
x^4+x+1	10011	19

FORMAREA CUVÂNTULUI DE COD (CODAREA

Etapele:

1. Se efectuiază înmulţirea $x^k d(x)$, unde k=n-n_0 este numărul biţilor de control, care coincide cu ordinul lui g(x). Operaţia este echivalentă cu completarea a k zerouri din dreapta.

2. La produsul $x^k d(x)$ se adună restul r(x), obţinut în urma împărţirii $x^k d(x)$ la g(x). $F(x) = x^k d(x) + r(x)$.

DETERMINAREA NUMĂRULUI BIȚILOR DE CONTROL K

Pentru corectarea unei erori($d_{min} = 3$): $k = [\log_2(n+1)]$, $n = 2^k - 1$, $n + 1 \leq 2^k$

n=7 k=3 n_0=4
n=15 k=4 n_0=11
n=31 k=5 n_0=26

Pentru $d > 3$

d- impar: $k = [\frac{d-1}{2} \log(n+1)]$, d- par: $k = [\frac{d-2}{2} \log_2(n+1)]$

Pentru alegerea g(x), ordinul polinomului trebuie să fie mai mare sau egal cu k., numărul unităţilor din g(x) – mai mare sau egal cu d_{min}.

EXEMPLU

Să se obţină un cuvânt de cod pentru transmiterea a 7 biţi, cu corectarea unei erori singulare.

1. Se determină k. $k = \log_2(7+1) = 3$
2. se determină n_0. $n_0 = n - k = 4$

Deci obţinem un cod ciclic (7,4).

3. Alegem g(x). Ordinul polinomului ≥ 3 (k)
   Numărul unităţilor ≥ 3 (d_{min})

$$g(x) = x^3 + x + 1 \rightarrow 1011$$

4. $d(x) = 1101$ blocul de date cu polinomul corespunzător $x^3 + x + 1$
5. Înmulţim la x^k 1000 (1101) = 1101000
6. Efectuăm împărţirea la g(x)

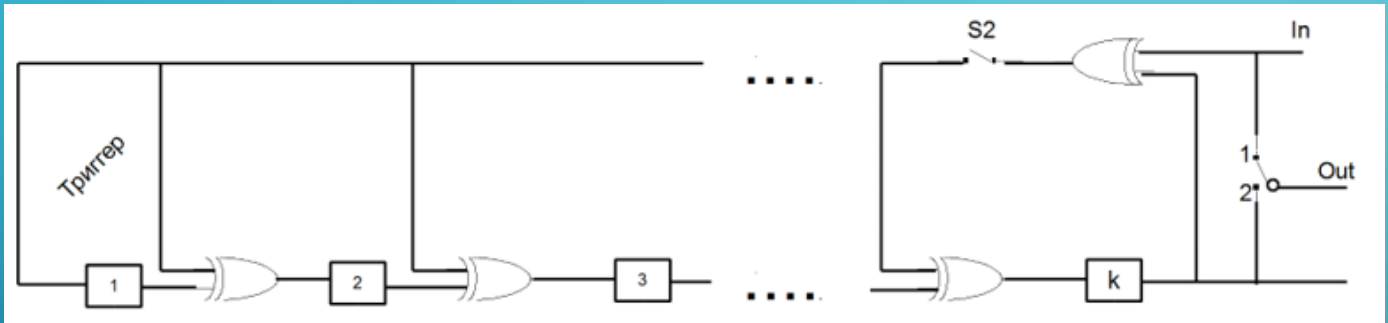
```
1101000 | 1011
1011    | 1111
-------
 1100
 1011
-------
  1110
  1011
-------
  1010
  1011
-------
     1   –  r(x)
```

7. Formăm cuvântul de cod: F(x) = 1101001

CIRCUITUL DE CODARE

Obținerea restului se efectuiază pe un registru de k-biți cu deplasare stânga și linii de reacție cu elemente XOR.

Circuitul de codare pentru un polinom generator de ordin k cu coeficienți nenuli:

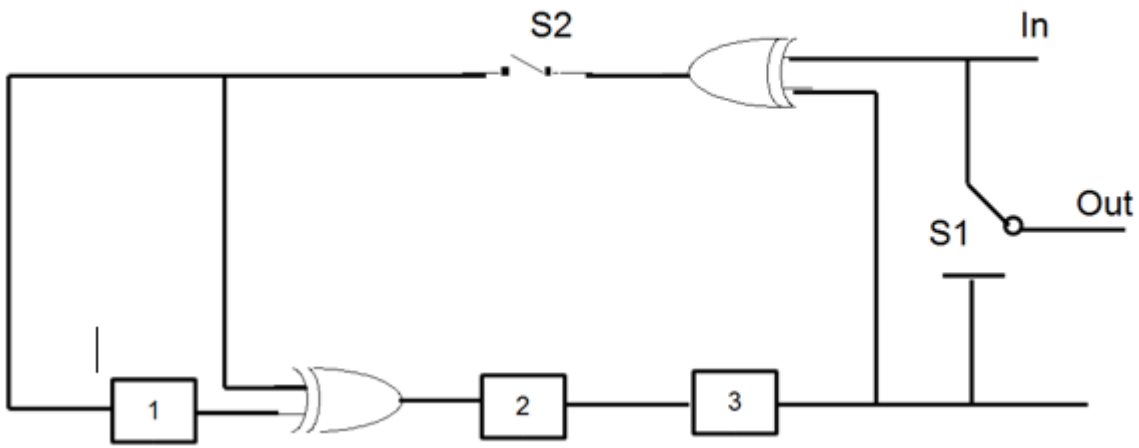


Numărul elementelor XOR este egal cu numărul unităţilor din g(x) fără cea mai semnificativă, deoarece cei mai semnificativi biţi din d(x) şi g(x) sunt întotdeauna egali cu 1 iar $1 \oplus 1 = 0$.

La început întrerupătorul S1 se află în poziţia 1, S2 e închis. Cuvântul format din n_0 biţi informaţionali este transferat spre ieşire şi, în acelaşi timp, în registru. Timp de n_0 impulsuri de ceas se formează restul r(x), care şi reprezintă biţii de control. După aceasta S2 sw deschide, S1 trece în poziţia 2 şi biţii de control sunt transferaţi spre ieşire timp de k impulsuri de ceas.

Pentru $g(x) = x^3 + x + 1$

$\overleftarrow{1101}$



	CLK	In	Rg 1 2 3	Out	
	0	-	0 0 0	-	x_{n-1}
n_0	1	1	1 1 0	1	
	2	1	1 0 1	1	
	3	0	1 0 0	0	
	4	1	1 0 0	1	
K	5	-	- 1 0	0	x_0
	6	-	- - 1	0	
	7	-	- - -	1	

EXEMPLU

$$g(x) = x^4 + x^2 + x + 1$$

EXEMPLU

$$g(x) = x^5 + x^3 + x^2 + 1$$

DETECTAREA ȘI CORECTAREA ERORILOR

1. Împărţirea cuvântului de cod recepţionat $F'(x)$ la $g(x)$, formând sindromul erorii $s(x)$. Dacă $s(x)=0$ – cuvântul a fost transmis fără erori. Dacă $s(x)\neq 0$ – a avut loc o eroare.

2. Pentru a corecta eroarea, numărul unităţilor în $s(x)$ trebuie să fie egal cu numărul erorilor. Dacă numărul unităţilor este mai mare, se efectuiază deplasarea ciclică cu o poziţie la stănga a $F'(x)$ şi se repetă p.1 până când condiţia devine adevărată.

3. Se efectuiază adunarea modulo2 dintre ultimul deâmpărţit şi ultimului rest.

4. Se efectuiază deplasarea inversă.

EXEMPLU

Cuvântul transmis F'(x) = 0101001

1)

$$\begin{array}{r|l} 0101001 & 1011 \\ \hline 1011 & \\ \hline 101 - r(x) & \end{array} \qquad w = 2 \quad 2>1$$

2) $F''(x) = \overleftarrow{F'}^{1}(x)$

$$\begin{array}{r|l} 1010010 & 1011 \\ \hline 1011 & \\ \hline 1010 & \\ 1011 & \\ \hline \underline{1} - r(x) & \end{array} \qquad w = 1 \quad 1 = 1$$

3)

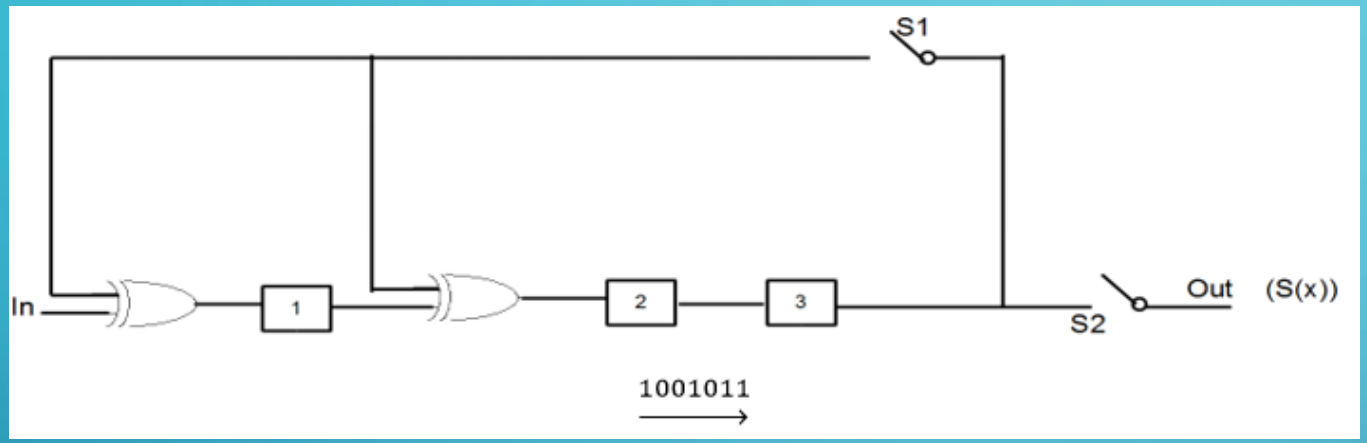
$F''(x) = 1010010 \quad \oplus$

$F_{cor}(x) \quad \underset{1010011}{1}$

4) $F(x) = \overrightarrow{F_{cor}}^{1}(x)$

$F(x) = 1101001$

CIRCUITUL DE CALCUL AL SINDROMULUI:



S2 iniţial e închis, s2 - deschis. După 7 impulsuri de ceas, registrul va conţine sindromul erorii. S2 se deschide iar s1 se închide.

In	CLK	Rg			
		1	2	3	
1001011	0	0	0	0	
100101	1	1	0	0	
10010	2	1	1	0	
1001	3	0	1	1	
100	4	0	1	1	
10	5	1	1	1	
1	6	1	0	1	
-	7	0	0	0	S(x)

PROPRIETĂȚILE POLINOMULUI GENERATOR

g(x) = CRC

CRC – 1	11 x+1	Bit de paritate k=1
CRC – 8	(9 biţi)	
CRC – 16	(17 biți)	16, 12, 5, 0 - XMODEM, Bluetooth
CRC – 32	(33 biţi)	32, 26, 23, 22, 16, 12, 11, 10, 8, 7, 5, 4, 2, 1, 0 - Ethernet, MPEG
CRC – 128	MD5	Message Digest Algorithm 5 (în criptografie)
CRC – 160	SHA	Secure Hash Algorithm (în criptografie)

Proprietăţile

1. g(x)va detecta toate erorile singulare dacă cel puţin 2 coeficienţi sunt nenuli.

$E(x) = x^i$ g(x) = x+1 $\frac{x^i}{x+1}$ va da întotdeauna rest

2. Erorile duble vor fi detectate în cazul când g(x) are cel puţin 2 termeni şi nu-l divide pe

$x^{i-j} + 1$ (11, 101, 1001,…)

$E(x) = x^i + x^j = x^j(x^{i-j} + 1)$, $i > j$ и $i - j < k$

3. Dacă g(x)are un număr par de termeni , codul va detecta toate modelele de erori cu număr impar. Această propriettae asigură capacitatea de a detecta jumătate din toate modelele posibile de erori.

4. g(x)detectează pachete de erori de lungime $l = n - n_0$ $(l \le k)$

Polinomul corespunzător unui pachet de erori de lungime l se poate scrie ca $x^i p(x)$, unde $p(x)$ are ordinul maxim $l-1<n-n_0$ şi nu este divizibil prin g(x) de ordin n- n_0.

EXEMPLU

Să se obțină un cuvânt de cod pentru transmiterea a 15 biți cu capacitatea de detectare și corectare a unei erori singulare. Dmin=3

1) $k = \log_2(n+1) = 4$
2) $n_0 = n - k = 15 - 4 = 11$
3) $g(x) = 10011$
4) $d(x) = 00000000101$
5) $x^4 d(x) = 000000001010000$
6)

```
000000001010000 | 10011
   10011
   -----
   11100
   10011
   -----
    1111
```

7) $F(x) = 000000001011111$

$F_e(x) = 0100000001011111$

8) $F_e(x)/g(x) = S(x)$

```
0100000001011111 | 10011
 10011           |------
 -----           |
  11001          |
  10011          |
  -----          |
  10100          |
  10011          |
  -----          |
  11111          |
  10011          |
  -----          |
  11001          |
  10011          |
  -----          |
  10101          |
  10011          |
  -----          |
   1101          |
```

$S(x) = 1101 \quad W = 3 \quad S = 1$

9) $\xleftarrow{1}$

$F_e(x)$

```
1000000010111110 | 10011
10011
-----
 11001
 10011
-----
  10100
  10011
-----
   11111
   10011
-----
    11001
    10011
-----
     10101
     10011
-----
      11010
      10011
-----
       1001
```

$S(x) = 1001 \quad W = 2 \quad S = 1$

10) $\xleftarrow{2}{F_e(x)}$

$$
\begin{array}{r|l}
000000101111110 & 10011 \\
1 & \\
\cline{1-1}
10011 & \\
\cline{1-1}
11001 & \\
10011 & \\
\cline{1-1}
001 &
\end{array}
$$

$S(x) = 0001 \quad W = 1 \quad S = 1$

11)

$$
\begin{array}{r}
000000101111101 \\
1 \\
\hline
000000101111100
\end{array}
\quad \oplus
$$

12) $F(x) = \xrightarrow{2}{F_e(x)}$ 000000001011111