

Tema 6.3 Coduri ciclice (CRC- Cyclic Redundancy Code)

Codurile ciclice se utilizează pe larg la transmiterea datelor datorită eficienței înalte de detectare și corectare a erorilor. Ele au o redundanță relativ mică iar dispozitivele de codare și decodare se pot realiza simplu, în baza registrelor de delasare cu reacție.

La fel ca și codurile Hamming, 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 $d = (d_{n-1}, d_{n-2}, \dots, d_0)$ pot fi considerate drept coeficienți a unui polinom cu variabila fictivă x .

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

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.

Aritmetica polinomială

Aritmetica polinomială, utilizată pentru efectuarea operațiilor matematice asupra codurilor ciclice este o aritmetică unde nu se ia în considerație transportul.

Adunarea și scăderea.

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

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

Înmulțirea

Înmulțirea polinomului la x^i coincide cu deplasarea la stânga cu i biți.

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

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

Înmulțirea 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 |
| | | | | 1 | 0 | 1 | 1 | 1 | 1 |
| | | 1 | 0 | 1 | 1 | 1 | 1 | 1 | \oplus |
| 1 | 0 | 1 | 1 | 1 | | | | \oplus | |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Împărțirea

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

$$\begin{array}{cccccc|cccc}
 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
 \hline
 1 & 0 & 0 & 1 & & & & 1 & 1 & 1 & 0 \\
 & 1 & 1 & 0 & 0 & & & & & & \\
 & \hline
 & 1 & 0 & 0 & 1 & & & & & & \\
 & & 1 & 0 & 1 & 0 & & & & & \\
 & & \hline
 & & 1 & 0 & 0 & 1 & & & & & \\
 & & & 1 & 1 & 0 & & & & & - \text{restul}
 \end{array}$$

Deplasarea ciclică la stânga e echivalentă cu înmulțirea la x și împărțirea la $x^n + 1$.

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

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

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

$$x^4 + x^3 + x \quad | \quad x^4 + 1$$

$$\underline{x^4 \qquad \qquad + 1}$$

$$x^3 + x + 1 \Rightarrow 1011$$

Polinoame generatoare

În codurile ciclice fiecare cuvânt de cod este multiplu al unui și aceluși 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 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.

| | | |
|-------------|-------|----|
| $x+1$ | 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 efectuează înmulțirea $x^k d(x)$, unde $k=n-n_0$ este numărul biților de control, care coincide cu ordinul lui $g(x)$. Operația este echivalentă cu completarea a k zerouri din dreapta.

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

Explicație:

$$\frac{x^k d(x)}{g(x)} = Q(x) + \frac{r(x)}{g(x)} \quad | \text{inmultim la } g(x)$$

$$x^k d(x) = Q(x)g(x) + r(x)$$

Aici $F(x) = Q(x)g(x)$ este un cuvânt de cod valid fiind multiplu al lui $g(x)$.

$F(x) = Q(x)g(x) = x^k d(x) + r(x)$, operațiile de adunare și scădere fiind identice.

Numărul biților de control k se determină în felul următor:

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

$$n=7 \quad k=3 \quad n_0=4$$

$$n=15 \quad k=4 \quad n_0=11$$

$$n=31 \quad k=5 \quad n_0=26$$

Pentru $d > 3$

$$d\text{- impar: } k = \lceil \frac{d-1}{2} \log_2(n+1) \rceil, \quad d\text{- par: } k = \lceil \frac{d-2}{2} \log_2(n+1) \rceil$$

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

Exemplu.

Să se obțină un cuvânt de cod pentru transmiterea a 7 biți, 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 obținem un cod ciclic (7,4).

3. Alegem $g(x)$. Ordinul polinomului ≥ 3 (k)

$$\text{Numărul unităților} \geq 3 \quad (d_{min})$$

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

4. $d(x) = 1101$ blocul de date cu polinomul corespunzător $x^3 + x + 1$

5. Înmulțim la x^k 1000 (1101) = 1101000

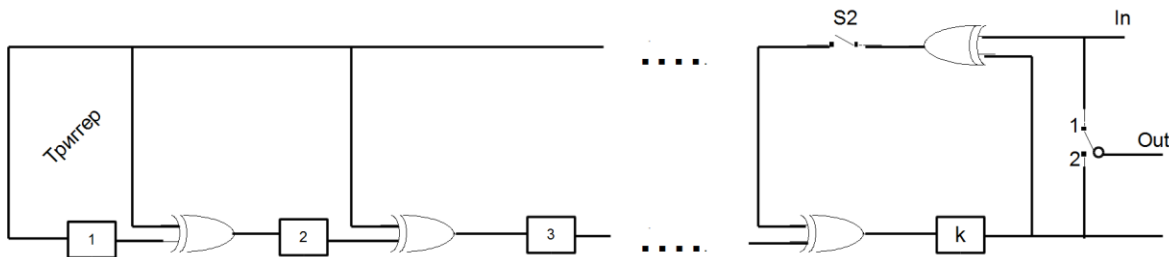
6. Efectuăm împărțirea la $g(x)$

$$\begin{array}{r}
 1101000 \overline{) 1101000} \\
 \underline{1011} \\
 1100 \\
 \underline{1011} \\
 1110 \\
 \underline{1011} \\
 1010 \\
 \underline{1011} \\
 1 - r(x)
 \end{array}$$

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

Obținerea restului se efectuează 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:

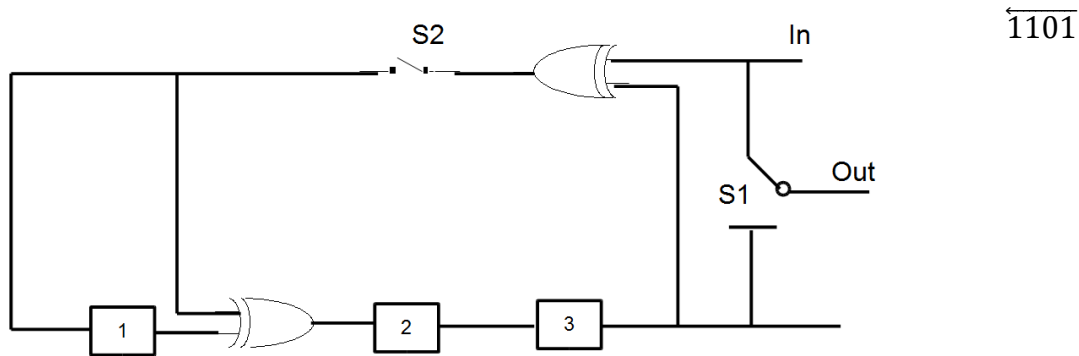


Numărul elementelor XOR este egal cu numărul unităților din $g(x)$ fără cea mai semnificativă, deoarece cei mai semnificativi biți din $d(x)$ și $g(x)$ sunt întotdeauna egali cu 1 iar $1 \oplus 1 = 0$.

La început întrerupătorul $S1$ se află în poziția 1, $S2$ e închis. Cuvântul format din n_0 biți informaționali este transferat spre ieșire și, în același timp, în registru. Timp de n_0 impulsuri de ceas se formează restul $r(x)$, care și reprezintă biții de

control. După aceasta S2 se deschide, S1 trece în poziția 2 și biții de control sunt transferați spre ieșire timp de k impulsuri de ceas.

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



| CLK | In | R _g | | | Out |
|-----|----|----------------|---|---|-----|
| | | 1 | 2 | 3 | |
| 0 | - | 0 | 0 | 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 |
| 5 | - | - | 1 | 0 | 0 |
| 6 | - | - | - | 1 | 0 |
| 7 | - | - | - | - | 1 |

Detectarea și corectarea erorilor

1. Împărțirea cuvântului de cod recepționat $F'(x)$ 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 unităților în $s(x)$ trebuie să fie egal cu numărul erorilor. Dacă numărul unităților este mai mare, se efectuează deplasarea ciclică cu o poziție la stânga a $F'(x)$ și se repetă p.1 până când condiția devine adevărată.

3. Se efectuează adunarea modulo2 dintre ultimul deâmpărțit și ultimului rest.

4. Se efectuează deplasarea inversă.

Exemplu.

$$F(x) = 1101001$$

Cuvântul transmis $F'(x) = 0101001$

1)

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

2) $F''(x) = \overset{1}{\leftarrow} F'(x)$

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

3)

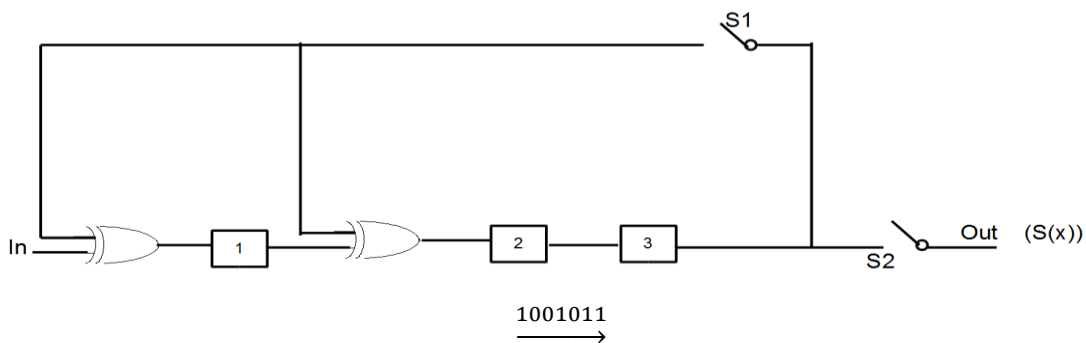
$$F''(x) = 1010010 \oplus$$

$$F_{cor}(x) = \frac{1}{1010011}$$

$$4) \quad F(x) = \overset{1}{\rightarrow} F_{cor}(x)$$

$$F(x) = 1101001$$

Circuitul de calcul al sindromului:



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

| In | CLK | Rg | | | S(x) |
|---------|-----|----|---|---|------|
| | | 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 | |

Proprietățile polinomului generator

| | | | |
|---------------------|-----------|---|-----------------------|
| $g(x) = \text{CRC}$ | | | |
| CRC – 1 | 11 | $x+1$ | Bit de paritate $k=1$ |
| CRC – 8 | (9 biți) | | |
| CRC – 16 | (17 biți) | 16, 12, 5, 0 | - XMODEM, Bluetooth |
| CRC – 32 | (33 biți) | 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) |

Proprietățile

1. $g(x)$ va detecta toate erorile singulare dacă cel puțin 2 coeficienți sunt nenuli.

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

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

$$x^{i-j} + 1 \quad (11, 101, 1001, \dots)$$

$$E(x) = x^i + x^j = x^j(x^{i-j} + 1), \quad i > j \text{ și } i - j < k$$

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

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

Polinomul corespunzător unui pachet de erori de lungime l se poate scrie ca $x^l p(x)$, unde $p(x)$ are ordinul maxim $l-1 < n-n_0$ și 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.

$$d_{min} = 3$$

- 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)

$$\begin{array}{r}
 000000001010000 \quad | \quad \underline{10011} \\
 \underline{10011} \\
 11100 \\
 \underline{10011} \\
 1111
 \end{array}$$

- 7) $F(x) = 000000001011111$
 $F_e(x) = 010000001011111$

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

$$\begin{array}{r}
 010000001011111 \quad | \quad \underline{10011} \\
 \underline{10011} \\
 11001 \\
 \underline{10011} \\
 10100 \\
 \underline{10011} \\
 11111 \\
 \underline{10011} \\
 11001 \\
 \underline{10011} \\
 10101 \\
 \underline{10011} \\
 1101
 \end{array}$$

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

9) $\overleftarrow{F_e(x)}$

$$\begin{array}{r}
 100000010111110 \quad | \quad 10011 \\
 \hline
 10011 \\
 \hline
 11001 \\
 10011 \\
 \hline
 10100 \\
 10011 \\
 \hline
 11111 \\
 10011 \\
 \hline
 11001 \\
 10011 \\
 \hline
 10101 \\
 10011 \\
 \hline
 11010 \\
 10011 \\
 \hline
 1001
 \end{array}$$

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

10) $\overleftarrow{F_e(x)}$

$$\begin{array}{r}
 00000010111110 \quad | \quad 10011 \\
 \hline
 10011 \\
 \hline
 11001 \\
 10011 \\
 \hline
 001
 \end{array}$$

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

11)

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

12) $F(x) = \overrightarrow{F_e(x)}$

000000010111111