Capitolul 6

Coduri ciclice

6.1 Breviar teoretic

Codurile ciclice constituie un caz particular al codurilor grup.

Permutare ciclică Denumirea de "ciclic" provine de la faptul că orice permutare ciclică a unui cuvânt de cod valid produce tot un cuvânt de cod valid. Permutarea cilică, într-un pas, a unui cuvânt se obţine luând primul element şi punându-l la sfărşitul cuvăntului. Formalizând, fie cuvăntul de cod $v_{n-1}v_{n-2}v_{n-3}\dots v_3v_2v_1v_0$; un cuvânt obţinut printr-o permutare ciclică din acesta este $v_{n-2}v_{n-3}\dots v_3v_2v_1v_0v_{n-1}$; după mai mulţi paşi, prin pemutări consecutive se poate obţine cuvântul : $v_0v_{n-1}v_{n-2}v_{n-3}\dots v_3v_2v_1$.

De exemplu dacă 10111 este un cuvânt de cod (conform unui cod cilcic), atunci şi 01111 este un cuvânt de cod, de altfel ca şi 11110, 11101, 11011.

Structura şi reprezentarea codului Lungimea cuvăntului de cod se notează cu n. Dintre cele n simboluri k sunt de informaţie, iar $m = n - k$ de control. Dacă în cazul codurilor grup reprezentarea era sub formă de vectori, în cazul codurilor ciclice reprezentarea este sub formă de polinom.

Polinomul de informaţie $i(x)$ are gradul $k - 1$:

$$i(x) = i_{k-1}x^{k-1} + i_{k-2}x^{k-2} + \cdots + i_1x + i_0$$

unde $[i_{k-1}i_{k-2}\dots i_1i_0]$ sunt simbolurile de informaţie.

Cuvăntul de cod este reprezentat printr-un polinom de grad $n - 1$:

$$v(x) = v_{n-1}x^{n-1} + v_{n-2}x^{n-2} + \cdots + v_1x + v_0$$

Similar cu matricea generatoare, G, de la coduri grup, aici se utilizează polinomul generator, notat $g(x)$. Gradul acestuia este m:

$$g(x) = g_mx^m + g_{m-1}x^{m-1} + \cdots + g_1x + g_0$$

Pentru a fi un polinom generator al unui cod funcţional, $g(x)$ trebuie să fie polinom primitiv. Într-o simplificare a definiţiei în care se ţine cont şi de faptul că coeficienţii polinomului pot fi doar 0 sau 1, un polinom este primitiv dacă este:

- *ireductibil.* Acest lucru presupune că nu exista nici un polinom de grad nenul şi mai mic de m care să fie divizor al lui $g(x)$
- dacă α este o rădăcină a lui $g(x)$ ($g(\alpha) = 0$) atunci cel mai mic întreg T pentru care $\alpha^i = \alpha^{i+T}$ este $T = 2^m - 1 = 2^{grad(g)} - 1$.

De reţinut este că polinoamele primitive sunt listate (cunoscute), iar de importanţă practică este faptul că coeficienţii de grad maxim (g_m) şi minim (g_0) sunt nenuli: $g_m = 1$, $g_0 = 1$.

Echivalent matricei de control de la coduri grup, în cazul codurilor ciclice,se defineşte un polinom de control, $h(x)$. Acesta are gradul $k-1$ şi se află în relatia următoare cu polinomul generator:

$$g(x)h(x) = x^n + 1$$

Adică:

$$(g_m x^m + \cdots + g_1 x + g_0)\left(h_k x^k + \cdots + h_1 x + h_0\right) = x^n + 1$$

Matricea G echivalentă polinomului generator are k linii şi n coloane şi este de forma:

$$\begin{bmatrix} g_0 & g_1 & \dots & g_{m-1} & g_m & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{m-1} & g_m & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & g_0 & g_1 & \dots & g_m \end{bmatrix}$$

Matricea H echivalentă polinomului de control are m linii şi n coloane şi este de forma:

$$\begin{bmatrix} 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 \\ 0 & \dots & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 \end{bmatrix}$$

Codarea

1. Codarea $v(x) = i(x)g(x)$. Această variantă corespunde codării $v = iG$ de la coduri grup. Practic se realizează înmulţirea polinoamelor iar formulele fiecărui simbol ale cuvântului de cod se obţin prin identificare de coeficinţi. Codul rezultat nu este sistematic.
2. Codarea $v(x) = x^m i(x) +$ rest$\left[\frac{x^m i(x)}{g(x)}\right]$. Această variantă corespunde cazului $Hv^T = 0$ de la coduri grup. Pe primele k poziţii ale cuvântului de cod se vor plasa simbolurile de informaţie, iar pe ultimele $n-k=m$ simbolurile de control. Polinomul corector asociat simbolurilor de control $c(x)$ este restul împărţirii lui $x^m i(x)$ la $g(x)$. Codul rezultat este sistematic.

Circuite de codare Există două circuite de codare uzuale. Ambele corespund variantei de cod sistematic. Acestea sunt:

1. Circuit de codare prin divizare.
2. Circuit de codare cu registru de deplasare şi reacţie negativă.

6.2 Probleme rezolvate

1. [1] *Un cod Hamming ciclic este generat cu ajutorul polinomului primitiv* $g(x) = x^3 + x + 1$*:*

   (a) *Să se determine numărul de simboluri de informaţie şi numărul de simboluri de control. Să se determine proprietăţile de corecţie / detecţie ale acestui cod.*

   (b) *Să se calculeze polinomul corector.*

   (c) *Să se calculeze matricea generatoare şi matricea de control a codului.*

   (d) *Să se genereze toate cuvintele de cod folosind atât codarea cu polinomul generator cât şi cu cel corector.*

   (e) *Să determine schema codorului cu divizor şi să se analizeze funcţionarea lui.*

   (f) *Să determine schema codorului cu registru de deplasare şi reacţie şi să se analizeze funcţionarea lui.*

   (g) *Să se analizeze tranziţiile stărilor codorului cu reacţie.*

   Rezolvare:

   (a) Parametri codului : se ştie că polinomul generator este de grad m (numarul de simboluri de control). Codurile ciclice sunt coduri perfecte. Atunci marginea Hamming (pentru o eroare) funcţioneaza cu egalitate:

   $$\text{lungimea cuvântului de cod este} n = 2^m - 1 = 7$$

   $$\text{simbolurile de informaţie sunt } k = n - m = 4$$

   (b) Polinomul de control se obţine ca fiind câtul împărtirii (modulo 2) $\frac{x^n+1}{g(x)}$:

   $$h(x) = \frac{x^7+1}{x^3+x+1} = x^4 + x^2 + x + 1$$

   Ar fi de observat faptul că gradul lui $h(x)$ (indiferent de problemă) este

   $$\text{grad}(h) = \text{grad}(x^n + 1) - \text{grad}(g) = n - m = k$$

   În plus este obligatoriu ca $g(x)$ sa aibă coeficienţii corespunzători lui x^m si x^0 nenuli (coeficientul lui x^0 este nenul pentru că altfel $g(x)$ ar admite ca divizor pe x şi nu ar mai fi ireductibil). Aceste fapte obligă şi pe $h(x)$ la acelaşi comportament: coeficenţii lui x^k şi x^0 sunt nenuli.

   (c) Matricea generatoare, de k linii şi n coloane, are forma:

   $$G = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

   Matricea de control, H, având m linii şi n coloane este:

   $$H = \begin{bmatrix} 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

(d) Codarea cu polinomul generator este echivalentă cu codarea (de la codurile grup) cu matrice generatoare:

$$v = iG \Longleftrightarrow v(x) = i(x)g(x)$$

Polinomul asociat cuvântului de cod este:

$$v = \begin{bmatrix} v_6 & v_5 & v_4 & v_3 & v_2 & v_1 & v_0 \end{bmatrix} \quad v(x) = v_6x^6+v_5x^5+v_4x^4+v_3x^3+v_2x^2+v_1x+v_0$$

Polinomul de informaţie este:

$$i = \begin{bmatrix} i_3 & i_2 & i_1 & i_0 \end{bmatrix} \quad i(x) = i_3x^3 + i_2x^2 + i_1x + i_0$$

Simbolurile cuvântului de cod se obţin efectuând înmulţirea polinoamelor $g(x)$ şi $i(x)$ identificând coeficienţii după gradul monomului:

$$\begin{aligned} v(x) =&g(x)i(x) = (x^3 + x + 1)(i_3x^3 + i_2x^2 + i_1x + i_0) = \\ =&i_3x^6 + i_2x^5 + (i_1 + i_3)x^4 + (i_0 + i_2 + i_3)x^3 + (i_1 + i_2)x^2 + (i_0 + i_1)x + i_0 \end{aligned}$$

$$\Longrightarrow v_6 = i_3 \;\; v_5 = i_2 \;\; v_4 = i_1 + i_3 \;\; v_3 = i_0 + i_2 + i_3 \;\; v_2 = i_1 + i_2 v_1 = i_0 + i_1 \;\; v_0 = i_0$$

Dacă se realizează înmultirea $v = iG$ rezultatele obţinute sunt aceleaşi:

$$v = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{bmatrix} = iG = \begin{bmatrix} i_0 & i_1 & i_2 & i_3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} i_0 \\ i_0 + i_1 \\ i_1 + i_2 \\ i_0 + i_2 + i_3 \\ i_1 + i_3 \\ i_2 \\ i_3 \end{bmatrix}$$

Codul obţinut nu este sistematic. Mai mult decât aât, nici măcar toate simbolurile de informaţie nu apar nealterate ca simboluri in cuvântul de cod.
Un cod sistematic se obţine dacă se realizează codarea cu matricea de control $Hv^T = 0$. Echivalent, este fomarea cuvantului de cod din polinom de informaţie si polinom de control:

$$c(x) = c_2x^2 + c_1x + c_0 \;\; c(x) = \text{rest}\frac{x^m i(x)}{g(x)}$$

$$v(x) = c(x) + x^m i(x)$$

$$\begin{aligned} c(x) =&\text{rest}\frac{i_3x^6 + i_2x^5 + i_1x^4 + i_0x^3}{x^3 + x + 1} = \\ =&(i_1 + i_2 + i_3)x^2 + (i_0 + i_1 + i_2)x + (i_0 + i_2 + i_3) \end{aligned}$$

$$\Longleftrightarrow v = \begin{bmatrix} i_0 + i_2 + i_3 \\ i_0 + i_1 + i_2 \\ i_1 + i_2 + i_3 \\ i_0 \\ i_1 \\ i_2 \\ i_3 \end{bmatrix}$$

Pe de altă parte, codarea cu matricea de control presupune:

$$Hv^T = 0 \Longleftrightarrow \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ i_0 \\ i_1 \\ i_2 \\ i_3 \end{bmatrix} \begin{bmatrix} c_2 + i_1 + i_2 + i_3 \\ c_1 + i_0 + i_1 + i_2 \\ c_2 + c_0 + i_0 + i_1 \end{bmatrix} = 0_3$$

$$\Longleftrightarrow \begin{bmatrix} c_2 = i_1 + i_2 + i_3 \\ c_1 = i_0 + i_1 + i_2 \\ c_0 = c_2 + i_0 + i_1 = i_0 + i_2 + i_3 \end{bmatrix}$$

	i_0	i_1	i_2	i_3	$v = iG$	$Hv^T = 0$
0	0	0	0	0	0 0 0 0 0 0 0	0 0 0 0 0 0 0
1	0	0	0	1	0 0 0 1 1 0 1	1 0 1 0 0 0 1
2	0	0	1	0	0 0 1 1 0 1 0	1 1 1 0 0 1 0
3	0	0	1	1	0 0 1 0 1 1 1	0 1 0 0 0 1 1
4	0	1	0	0	0 1 1 0 1 0 0	0 1 1 0 1 0 0
5	0	1	0	1	0 1 1 1 0 0 1	1 1 0 0 1 0 1
6	0	1	1	0	0 1 0 1 1 1 0	1 0 0 0 1 1 0
7	0	1	1	1	0 1 0 0 0 1 1	0 0 1 0 1 1 1
8	1	0	0	0	0 1 0 1 0 0 0	1 1 0 1 0 0 0
9	1	0	0	1	1 1 0 0 1 0 1	0 1 1 1 0 0 1
10	1	0	1	0	1 1 1 0 0 1 0	0 0 1 1 0 1 0
11	1	0	1	1	1 1 1 1 1 1 1	1 0 0 1 0 1 1
12	1	1	0	0	1 0 1 1 1 0 0	1 0 1 1 1 0 0
13	1	1	0	1	1 0 1 0 0 0 1	0 0 0 1 1 0 1
14	1	1	1	0	1 0 0 0 1 1 0	0 1 0 1 1 1 0
15	1	1	1	1	1 0 0 1 0 1 1	1 1 1 1 1 1 1

Tabela 6.1: Cuvintele de cod

Cuvintele de cod obţinute, în cele două variante, sunt trecute în tabela 6.1.
După cum se poate observa atât din relaţiile de codare cât şi din tabel, cele două variante de codare duc, pentru acelaşi vector de informaţie, la cuvinte de cod diferite. Totuşi, mulţimea cuvintelor de cod este aceeaşi. De pildă, cuvântul de pe poziţia a 4-a (codat cu iG) se regăseşte pe poziţia 13-a în cazul codării cu matricea de control; ş.a.m.d.
De asemenea, se poate verifica, în tabela 6.1, proprietatea fundamentală a codurilor ciclice: orice permutare ciclică a unui cuvânt de cod duce la alt cuvânt de cod; de exemplu: cuvântul 0001101 (poziţia 2 iG), permutat o dată, duce la 1000110 care se află pe pozţia 14; de două ori duce la 0100011 care este pe poziţia 7; ş.a.m.d.

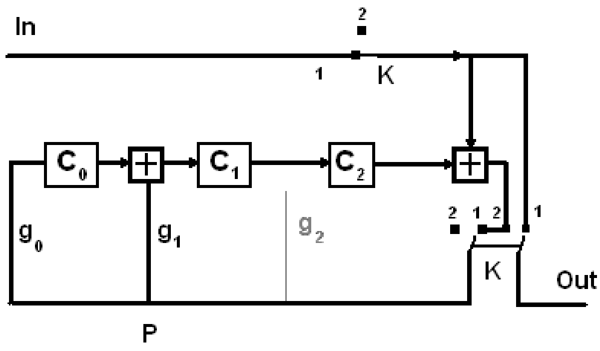

Figura 6.1: Codorul unui cod ciclic realizat cu registru cu deplasare. În primele $k = 4$ cicluri de ceas comutatoarele K sunt în poziţia 1; în următoarele $n - k = m = 3$ cicli de ceas este în poziţia 2.

(e) Schema codorului cu divizare este prezentată în figura 6.1.

În construcţia circuitului, legăturile verticale din partea inferioară exista în funcţie de valorile coeficienţilor polinomului $g(x)$. Astfel legăturile asociate lui g_0 şi g_1 există, în timp ce cea corespunzătoare lui $g_2 = 0$ nu.

Funcţionarea circuitului este coordonată de un semnal periodic (denumit uneori semnal de ceas). O operaţie se desfăşoara pe parcursul unui ciclu (perioadă) a semnalului. Sumatoarele sunt instantanee. Registrele C_0, C_1, C_2 sunt registre de deplsare, adică valoare primită la intrare la momentul n este trimisă la îeşire la momentul $n + 1$. Funcţionarea circuitului este următoarea:

- La pornirea circuitului registrele de deplasare au valoarea 0 (faza de iniţializare).
- Pe primele $k = 4$ perioade ale semnalului de ceas comutatorul K este în poziţia 1. În acest timp la intrare se prezintă simbolurile de informaţie. La ieşire se transmit nealterate simbolurile de informaţie (partea corespunzătoare lui $x^m i(x)$. Relaţiile în interioriul circuitului sunt:
  - $Out(n) = In(n)$;
  - $P(n) = In(n) + C_2(n - 1)$;
  - $C_0(n) = P(n)$;
  - $C_1(n) = C_0(n - 1) + P(n)$
  - $C_2(n) = C_1(n - 1)$

  La sfârşitul acestor cicli, în registrele de deplasare se va stoca restul împărţirii lui $x^m i(x)$ la $g(x)$.
- Pe ultimele $n - k = m$ perioade ale semnalului de ceas comutatoarele K trec în poziţia 2. Intrarea va fi 0 iar la ieşire vor fi simbolurile de control (coeficienţii restului). Relaţiile în circuit sunt:
  - $In(n) = 0$;
  - $Out(n) = C_2(n - 1)$;
  - $P(n) = 0$;

– $C_0(n) = P(n)$;
– $C_1(n) = C_0(n-1) + 0$
– $C_2(n) = C_1(n-1)$

La sfârşitul acestor cicli, în registrele de deplasare se va încărca valoarea 0 (exact cum am cerut la începutul funcţionării).

Evoluţia circuitului poate fi urmaită în tabelul de mai jos:

ciclu	K	In	Out	P	C_0	C_1	C_2
0	1	NA	NA	NA	0	0	0
1	1	i_3	i_3	i_3	i_3	i_3	0
2	1	i_2	i_2	i_2	i_2	$i_2 + i_3$	i_3
3	1	i_1	i_1	$i_1 + i_3$	$i_1 + i_3$	$i_1 + i_2 + i_3$	$i_2 + i_3$
4	1	i_0	i_0	$i_0 + i_2 + i_3$	$i_0 + i_2 + i_3$	$i_0 + i_1 + i_2$	$i_1 + i_2 + i_3$
5	2	0	$i_1 + i_2 + i_3$	0	0	$i_0 + i_2 + i_3$	$i_0 + i_1 + i_2$
6	2	0	$i_0 + i_1 + i_2$	0	0	0	$i_0 + i_2 + i_3$
7	2	0	$i_0 + i_2 + i_3$	0	0	0	0

Tabela 6.2: Evoluţia codorului (NA- Not available/nedisponibil) .

(f) Schema codorului cu regiştrii de deplasare şi reacţie este prezentată în figura 6.2.

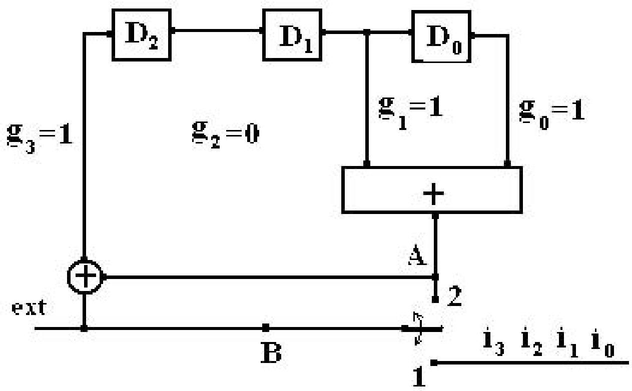

Figura 6.2: Codorul unui cod ciclic realizat cu registru cu deplasare. În primele $k = 4$ cicluri de ceas comutatorul este pe pozitia 1; în următoarele $n - k = m = 3$ cicli de ceas este în poziţia 2.

Registrele D_2, D_1, D_0 sunt registre de deplsare. În primele $k = 4$ cicluri de ceas comutatorul este pe pozitia 1; în această perioadă se încarcă simbolurile de informaţie. Relaţiile în interiorul circuitului sunt:

- $Out(n) = In(n)$;
- $B(n) = In(n)$;
- $D_2(n) = B(n) + A(n)$;

- $D_1(n) = D_2(n-1)$
- $D_0(n) = D_1(n-1)$
- $A(n) = D_1(n-1) + D_0(n-1)$;

În următorii $n - k = m = 3$ cicli de ceas comutatorul este în poziţia 2; acum se calculează simbolurile de control. Într-un ciclu de ceas, operaţiile efectuate sunt:

- $Out(n) = B(n)$;
- $B(n) = A(n)$;
- $D_2(n) = B(n) + A(n) = 0$;
- $D_1(n) = D_2(n-1)$
- $D_0(n) = D_1(n-1)$
- $A(n) = D_1(n-1) + D_0(n-1)$;

Pe scurt evoluţia circuitului este prezentată în tabela 6.3.
După cum se poate observa punctul, B coincide cu ieşirea circuitului. În primii n cicli de ceas se formează cuvintele de cod, pe baza relaţiilor de codare obţinute pentru un cod sistematic.

ciclu	comutator	D_2	D_1	D_0	A	B
0	1	0	0	0	0	i_3
1	1	i_3	0	0	0	i_2
2	1	i_2	i_3	0	i_3	i_1
3	1	$i_2 + i_3$	i_2	i_3	$i_2 + i_3$	i_0
4	2	$i_0 + i_2 + i_3$	$i_2 + i_3$	i_2	$i_1 + i_2 + i_3$	$i_1 + i_2 + i_3$
5	2	0	$i_0 + i_2 + i_3$	$i_2 + i_3$	$i_0 + i_1 + i_2$	$i_0 + i_1 + i_2$
6	2	0	0	$i_0 + i_2 + i_3$	$i_0 + i_2 + i_3$	$i_0 + i_2 + i_3$
7	1	0	0	0	0	i_3

Tabela 6.3: Evoluţia codorului.

(g) Analiza stărilor de funcţionare se face cand circuitul de codare lucrează autonom (adică comutatorul este în poziţia 2 - nu există intrare). Codorul conţine trei registri de deplasare. Considerăm vectorul care caracte_rizează starea codorului la momentul n, a fi vectorul:

$$S(n) = \begin{bmatrix} D_0(n) \\ D_1(n) \\ D_2(n) \end{bmatrix}$$

Convenim să notăm starea iniţială:

$$S(0) = U = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Trecerea de la o stare la alta ţine cont de relaţiile

$$D_2 \Longrightarrow D_1, \qquad D_1 \Longrightarrow D_0, \qquad D_2 = g_2 D_2 + g_1 D_1 + g_0 D_0$$

Această traziţie poate fi scrisă sub formă matriceală (similar cu traziţia unei surse Markov):

$$S(n+1) = TS(n)$$

unde T este matricea caracteristică a registrului. Ea are m linii şi m coloane şi este de forma:

$$T = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ g_0 & g_1 & \dots & g_{m-1} & \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Dezvoltând relaţia de tranziţie a stărilor se obtine:

$$S(n+1) = TS(n) \Longleftrightarrow \begin{bmatrix} D_0(n+1) \\ D_1(n+1) \\ D_2(n+1) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} D_0(n) \\ D_1(n) \\ D_2(n) \end{bmatrix}$$

$$\Longleftrightarrow \begin{bmatrix} D_2(n+1) = D_1(n) + D_0(n) \\ D_1(n+1) = D_2(n) \\ D_0(n+1) = D_0(n) \end{bmatrix}$$

adică exact ce doream.
Starea la momentul n se poate scrie ca $S(n) = T^n U$.
Stările fiind în număr finit, se va ajunge din nou după un timp la starea iniţială. Numarul de cicli dupa care se ajunge din nou în starea iniţiala este de $2^m - 1 = 7$, dacă circuitul este generat cu ajutorul unui polinom $g(x)$ primitiv. Mai exact:

$$S_1 = TU = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$S_2 = TS_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$S_3 = TS_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$S_4 = TS_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$S_5 = TS_4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

$$S_6 = TS_5 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$S_7 = TS_6 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Ceea ce verifică că $g(x) = x^3 + x + 1$ este primitiv.
Această ciclitate a stărilor dă şi ciclitatea cuvintelor de cod.
Dacă se analizeaza multimea cuvintelor de cod, există doi cicli de perioadă 7 si doi de perioadă 1.
În cazul în care există intrare (codorul nu mai functionează autonom) starea la momentul n este dată de relaţia:

$$S(n) = TS(n-1) + \alpha U$$

unde α este simbolul aflat la intrare la momentul n. Această relaţie este uşor de verificat pe circuit.

6.3 Probleme propuse

1. Un cod Hamming ciclic este generat cu ajutorul polinomului primitiv $g_1(x) = x^3 + x^2 + 1$ sau $g_2(x) = x^4 + x + 1$
   (a) Să se determine numărul de simboluri de informaţie şi numărul de simboluri de control. Să se determine proprietăţile de corecţie / detecţie ale acestui cod.
   (b) Să se calculeze polinomul corector.
   (c) Să se calculeze matricea generatoare şi matricea de control a codului.
   (d) Să se genereze toate cuvintele de cod folosind atât codarea cu polinomul generator cât şi cu cel corector.
   (e) Să determine schema codorului si să se analizeze funcţionarea lui.
2. [2] Un numar de 16 simboluri este transmis pe un canal.
   (a) Să se determine numarul de simboluri de informatie, control si numărul total de biţi ai unui de cod.
   (b) Să se aleagă un polinom generator dintre :$x + 1$, $x^2 + 1$,$x^3 + x^2 + 1$,$x^4 + x^2 + x + 1$
   (c) Să se calculeze matricea generatoare şi matricea de control a codului.
   (d) Să se determine relaţiile de codare în cazul unui cod sistematic
3. [4] Deteminaţi ciclurile generate de registrele de deplasare cu reacţie caracterizate de polinoamele:
   (a) $g(x) = x^3 + x^2 + 1$
   (b) $g(x) = x^4 + x^3 + x^2 + x + 1$
   (c) $g(x) = x^4 + x^2 + x + 1$

   Comentaţi rezultatele.
   Indicaţie: Se construieşte matricea caracteristică a fiecărui registru de deplasare asociat unui polinom. Se generează toate stările posibile, plecând din $U = [0 \dots 01]^T$. Daca perioada este egală cu gradul polinomului, atunci $g(x)$ este primitiv.

Bibliografie

[1] Mihai Ciuc. "Note de seminar".

[2] A. T. Murgan, I. Spânu, I. Gavăt, I. Sztojanov, V. E. Neagoe, şi A. Vlad. *Teoria Transmisiunii Informatîei - probleme.* Editura Didactică şi Pedagogică, Bucureşti, România, 1983.

[3] Alexandru Spătaru. *Teoria Transmisiunii Informatţiei.* Editura Didactică şi Pedagogică, Bucureşti, România, 1983.

[4] Alexandru Spătaru. *Fondements de la theorie de la transmisssion de línformation.* Presses polytechniques romandes, Lausanne, Elveţia, 1987.

[5] Rodica Stoian. "Note de seminar".

[6] Dan Alexandru Stoichescu. "Note de seminar".

[7] Eugen Vasile. "Note de seminar".

[8] Constantin Vertan. "Note de seminar".