MODULUL 3
CODURI DETECTOARE ŞI CORECTOARE DE ERORI

În cazul transmisiilor la distanţe relativ mari, prin apariţia inerentă a perturbaţiilor, o parte din simbolurile din alfabetul codului, ce formează cuvintele de cod ataşate mesajelor, pot fi modificate, astfel încât ceea ce se recepţionează nu mai corespunde cu ceea ce s-a transmis. Deoarece în marea majoritate a situaţiilor practice se foloseşte ca alfabet al codului numai 0 şi 1 (uşor de realizat) vom considera în continuare doar acest caz. În situaţia în care alfabetul codului este numai 0 şi 1, datorită perturbaţiilor codului, un 0 transmis poate deveni 1 şi invers. Din această cauză se spune că perturbaţiile care apar au un caracter aditiv.

$\oplus$	0	1
0	0	1
1	1	0

Dacă se transmite 0 şi se recepţionează 1 α perturbaţia $0 \oplus 1 = 1$.

Din codarea mesajelor (surselor) pentru canale cu perturbaţii se pun două probleme:

1. detecţia erorilor
2. corecţia automată a erorilor

1 α codarea trebuie astfel efectuată încât la recepţie să putem decide dacă ceea ce s-a recepţionat este corect sau eronat, fără pretenţia de a stabili şi locurile în cuvântul de cod în care s-au introdus erori.

2 α codarea trebuie astfel efectuată, încât la recepţie să avem posibilitatea nu numai a decide dacă ceea ce s-a obţinut este corect, ci şi de a corecta automat erorile care au apărut pe canal.

Problema detecţiei erorilor este mai simplă, în schimb necesită un canal de transmisiuni cu dublu sens, deoarece, ori de câte ori la recepţie se detectează prezenţa erorilor, să existe posibilitatea cererii de retransmisie a cuvântului recepţionat eronat. Se cere transmiterea cuvântului recepţionat eronat până ce acesta este recepţionat corect ; rezultă o întârziere la recepţionarea informaţiei.

În scopul întocmirii codurilor detectoare de erori sau corectoare de erori, se folosesc o serie întreagă de coduri, bazate pe diferite teorii matematice, o primă clasificare constând în :

- coduri bloc α la care fiecare cuvânt de cod are aceeaşi lungime
- coduri nonbloc (sau recurente) α la care transmisia se face cursiv, fără o delimitare precisă a cuvântului de cod.

MODULUL 3
CAPITOLUL 1

CODURI DETECTOARE ŞI CORECTOARE DE ERORI

3.1. Codarea si decodarea pe canale perturbate

S-a aratat anterior ca performanta globala a unui sistem de transmitere de date este probablitatea de eroare.

Transmiterea în banda de baza sau modulatia sunt afectate de o serie de constrângeri care fac uneori imposibila obtinerea unei probabilitati de eroare prescrise.

Calea prin care se poate obtine probabilitatea de eroare prescrisa este folosirea redundantei controlate. Blocurile functionale care efectueaza aceasta sarcina sunt codorul si decodorul canalului.

Codorul canalului adauga în mod sistematic biti la mesajul transmis. Acesti biti aditionali, desi nu transporta informatie, fac posibili detectia si corectia erorilor.

Detectia erorilor si/sau corectia lor coboara probabilitatea de eroare.

Problema codarii pe canale perturbate poate fi formulata astfel. Referindu-ne la figura 5.1 sistemul digital de comunicatie urmareste transmiterea iesirii codorului sursei $\{b_k\}$ cu un debit r_b pe un canal zgomotos.

Datorita zgomotului fluxului de date receptionate $\{\hat{b}_k\}$ difera uneori de secventa transmisa $\{b_k\}$.

Se impune ca probabilitatea de eroare $P\left(\hat{b}_k \neq b_k\right)$ sa fie mai mica decât o anumita valoare.

Codorul canalului si decodorul canalului au ca scop reducerea probabilitatii globale de eroare.

Codorul împarte biti mesajului în blocuri de câte k biti si înlocuieste fiecare bloc cu un cuvânt de cod de n biti, adaugând $n-k$ biti. Decodorul primeste cuvântul de cod, care este uneori alterat si încearca sa decodeze cei k biti ai mesajului.

Desi biti de control nu aduc nici o informatie receptorului, ei permit decodorului sa detecteze si sa corecteze erorile de tramsmitere reducând prin aceasta probabilitatea de eroare.

Proiectarea unui codor/decodor consta în selectarea regulilor de generare a cuvintelor de cod pornind de la blocurile mesaj si apoi de extragere a blocurilor mesaj din versiunea receptionata de cuvânt de cod.

În figura 3.1 este prezentata schema bloc pentru un sistem de codare/decodare.

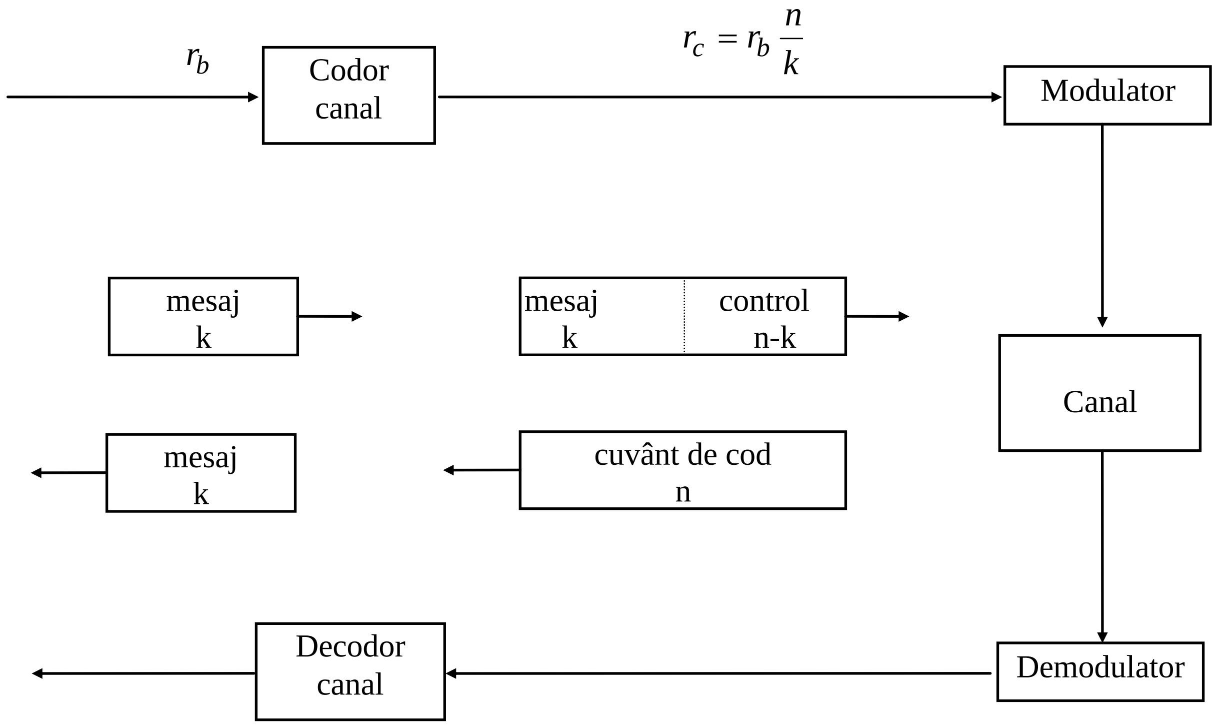


Fig. 3.1

Codurile care efectueaza controlul erorii sunt clasificate în: coduri bloc si coduri convolutionare. Din codurile bloc, unui mesaj de k biti i se asocieaza un cuvânt de cod de n biti care actioneaza r biti pe baza celor k biti cu continut informational. La receptie biti de control sunt utilizati pentru a verifica biti de informatie din blocul precedent. Pentru codurile convolutionare, biti de control sunt în mod continuu inserati între biti de informatie; biti de control verificând nu numai biti de informatie din blocul precedent ci si din alte blocuri anterioare.

Distanta Hamming. Distanta între doua cuvinte binare de lungime n $u = x_1, x_2, \ldots\ldots, x_n$; $v = y_1, y_2, \ldots\ldots, y_n$ $\$\left(x_i, y_i \in \{0{,}1\}\right)$ este numarul pozitiilor de acelas rang în care doua cuvinte difera

$$d(u,v) = \sum_{i=1}^{n} x_i \oplus y_i \tag{3.1}$$

Observatie

Numarul natural $d(u,v)$ verifica axiomele distantei

$$\begin{aligned} &(a)\ d(u,v) = d(v,u) \geq 0 \\ &(b)\ d(u,v) = 0 \Leftrightarrow u = v \\ &(c)\ d(u,v) \leq d(u,w) + d(w,v) \end{aligned} \tag{3.2}$$

O reprezentare geometrica a lui u poate fi un punct de coordonate $x_1, \ldots\ldots x_n$ In R^n. Cele 2^n combinatii de n biti sunt vârfurile unui hipercub de latura 1. In figura următoare este reprezentat un astfel de cub pentru R^3.

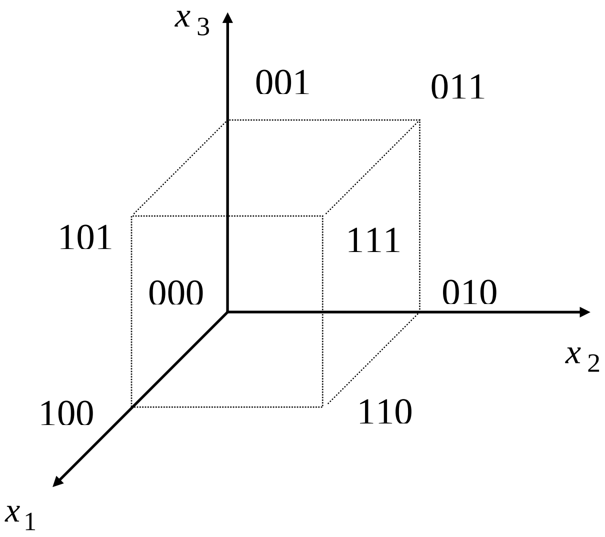


Fig 3.2

Distanta Hamming între doua vârfuri este cel mai mic numar de laturi care le unesc

Daca toate cuvintele de cod au sens, atunci orice eroare conduce la un alt cuvânt de cod si nu poate fi depistata. Daca însa separam din cele 2^n cuvinte de cod, numai 2^k atunci este posibil sa se depisteze unele erori singulare deoarece 2^{n-k} combinate nu au sens. În general, fie un cod în care toate cuvintele sunt la distante mutuale de cel putin egale cu d_0.

Cazul 1

Conditia necesara si suficienta ca un cod binar sa poata corecta cel mult r erori este ca $d_0 \geq 2r + 1$

Cazul 2

Daca $d_0 \geq 2r$ se pot corecta cel mult $r - 1$ erori.

3.2. Coduri Bloc Liniare

Se considera coduri bloc, în care fiecare, în fiecare bloc de k biti mesaj este codat într-un bloc de $n > k$ biti prin adaugarea de $n - k$ biti de control. Bitii de control sunt obtinuti pe baza celor k biti mesaj, asa cum este ilustrat în figura 3.3.

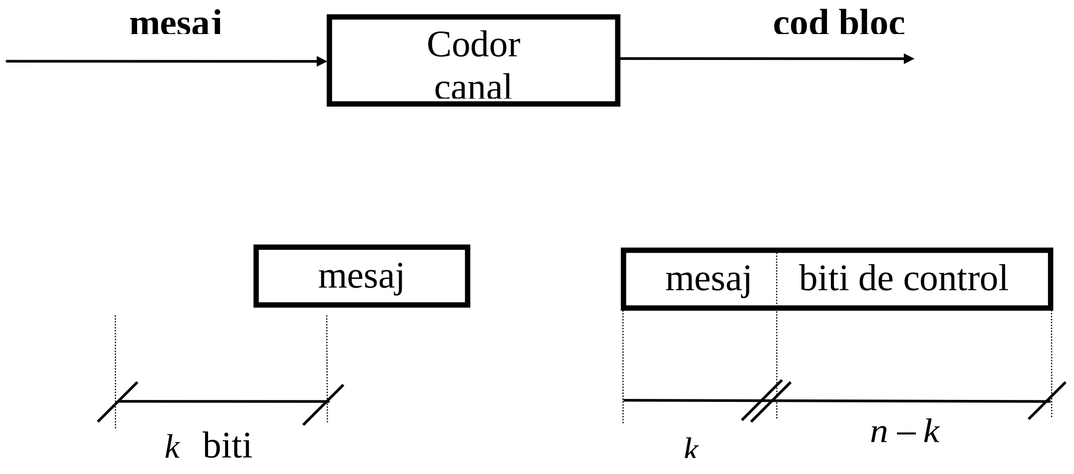


Fig. 3.3

Blocurile de n biti de la iesirea codorului canalului sunt numite cuvinte de cod si codurile pentru care biii mesaj apar la începutul cuvântului de cod sunt numite coduri sistematice. În plus daca fiecare di cele 2^k cuvinte de cod poate fi exprimat ca o combinatie lineara de k vectori independenti, atunci codul este si linear.

Codarea consta în doua etape:

(1) secventa de biti informationali este segmentate în blocuri mesaj de câte k biti.

(2) codorul transforma fiecare bloc mesaj într-un bloc mai mare de n biti în conformitate cu anumite reguli. Acesti $n-k$ biti aditionali sunt generati printr-o combinatie lineara de biti mesaj si operatiile pot fi descrise folosind matrice.

Blocul mesaj este reprezentat printr-un vector linie având k componente

$$D = [d_1 \quad d_2 \quad \ldots\ldots \quad d_k] \quad cu \quad d_i \in \{0,1\};\ i \in \left(\overline{1,k}\right) \tag{3.3}$$

Fiecare bloc mesaj este transformat într-un cuvânt de cod c de lungime n

$$C = [c_1 \quad c_2 \quad \ldots\ldots \quad c_n]$$

Se observa ca eficienta acestui cod este k/n.

Pentru un cod linear, sistematic primii k biti ai cuvântului de cod sunt bitii mesaj adica

$$c_i = d_i \qquad i = 1,2,\ldots\ldots,k \tag{3.4}$$

Ultimii $n-k$ biti ai cuvântului de cod sunt bitii de control generatii pe baza celor k biti ai mesajului în conformitate cu anumite reguli predeterminate:

$$
\begin{aligned}
c_{k+1} &= p_{11}d_1 + p_{21}d_2 + - - - - - - - - - + p_{k,1}d_k \\
&\vdots \\
&\vdots \\
c_n &= p_{1,n-k}d_1 + p_{2,n-k}d_2 + - - - - - - - - - + p_{k,n-k}d_k
\end{aligned}
\tag{3.5}
$$

Coeficientii $p_{i,j}$ din ecuatiile (3.5) sunt booleene iar sumarea se face modulo -2. Ecuatiile (3.4) si (3.5) pot fi combinate sub o forma matriceala

$$
\begin{bmatrix} c_1 & \ldots & c_n \end{bmatrix} = \begin{bmatrix} d_1 & \ldots & d_k \end{bmatrix}
\begin{bmatrix}
1000\ldots0 & p_{11}p_{12}\cdots p_{1,n-k} \\
0100\ldots0 & p_{21}p_{22}\cdots p_{2,n-k} \\
0010\ldots0 & p_{31}p_{32}\cdots p_{3,n-k} \\
\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\
000\ldots01 & p_{k,1}p_{k2}\cdots p_{k,n-k}
\end{bmatrix}_{k \times n}
\tag{3.6}
$$

sau

$$C = D \cdot G \tag{3.7}$$

unde G este o matrice de tip $k \times n$ numita matricea generatoare a codului si are forma

$$G = \begin{bmatrix} I_k | P \end{bmatrix}_{k \times n} \tag{3.8}$$

Matricea I_k este matricea unitate de ordinul k iar P este o matrice arbritara $k \times (n-k)$. Sa remarcam ca specificarea lui P defineste complet codul bloc (n,k).

Proiectarea unui cod bloc (n,k) prin selectarea unei matrici P trebuie sa aiba în vedere urmatoarele proprieteti

- comoditatea implementarii
- capacitatea de a corecta erorile singulare si pachetele de erori (burst errors)
- eficienta codului da fie ridicata

Prin eficienta codului se Intelege raportul $\frac{k}{n}$ pentru o anumita capacitate de detectie/corectie.

Trebuie mentionat ca nu exista o procedura de selectie a matricei P care sa satisfaca toate proprietatile de mai sus.

3.3. Exemple de coduri liniare

Codul Hamming

Cele mai cunoscute coduri liniare sint codurile binare Hamming . Ele se dau cu ajutorul matricei de control H, care este formata din m linii si 2^m - 1 coloane, lar coloanele sunt toate elementele nenule de lungime m. Spatiul nul al acestei matrice are distanta minima egala 3, adica este un cod (n k) ce corecteaza o eroare si are urmatoarele caracteristici:

- lungimea combinatiilor de cod este n = 2m -1;
- numarul simbolurilor de control este r=n - k ;
- numarul simbolurilor informationale este k

Codul Reed-Muller

Reprezinta o categorie de coduri liniare care se deosebesc in mod esential de clasa codurilor liniare prin algoritmul de codificare si decodificare (codul Hamming , coduri simetrice pe k pozitii) .

La acest cod, spre deosebire de codurile simetrice algoritmul de decodificare nu poate fi etapizat, atat detectia, corectia, cat si decodificarea propriu-zisa se produc simultan, rezultand in urma algoritmului, in mod direct simbolurile informationale continute in cuvantul de cod receptionat.

Lungimea n a codului este o putere a lui 2, adică $n=2^m$. Pentru r, număr întreg pozitiv, numărul poziţiilor informaţionale este

$$k = \sum_{i=0}^{r} C_m^i \tag{3.8}$$

Numărul simbolurilor de control este dat de relaţia

$$n - k = 1 + C_m^1 + ... + C_{m-r-1}^m \tag{3.9}$$

Distanţa minimă Hamming este $d=2^{m-r}$

La codul Reed-Muller, spre deosebire de cele sistematice, algoritmul de decodificare nu poate fi etapizat, adica atat detectia cat si corectia si decodificarea propriu-zisa, se produc simultan, rezultand in urma algoritmului in mod direct simbolurile informationale detinute din codul receptionat.

Fie Vn un spatiu vectorial peste GF(2), n–dimensionali avand componentele 0 sau 1. Fie u=(a1,a2,a3,…,an) si v=(b1,b2,b3,…,bn), pe spatiul vectorial Vn se poate defini produsul vectorial u x V=(a1*b1, a2*b2,…an*bn) si produsul scalar $\vec{u} * \vec{V} = \sum a_i \bullet b_i$ si $\vec{u} * \vec{V} \in GF(2)$.

Se pot observa urmatoarele :

- produsul scalar este nul daca ponderea produsului vectorial este un numar par ;
- fata de operatiile descrise, multimea vectorilor de n elemente formeaza o algebra liniara, asociativa si comutativa.

Codul Reed-Muller se poate defini cu urmatorii parametrii :

- n=2m, unde n este dimensiunea vectorilot cuvintelor de cod ;
- $k = \sum_{k=0}^{r} C_n{}^k$, unde k este numarul de simboluri informationale din cod ;
- d=2m-r, unde d este distanta minima a codurilor ;
- $n - k = 1 + C_m^1 + C_m^2 + ... + C_m^{n-r-1}$, pentru care se defineste codul RM(m,r) ;
- $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ unde t este numarul de erori pe care il poate corecta codul RM(m,r).

Un cod Reed-Muller de ordinul r avand lungimea cuvintelor de cod 2m este un subspatiu vectorial, generat de urmatorii vectori liniari independenti care constituie matricea generatoare :

V0=1111 1111 1111 …..1111
Vm=0000 0000 0000 …..1111

Vm-1=0000 1111 0000 …. 1111
………………………………
Vm x Vm-1= …………………. (3.10)
……………………………….
V2 x V1= ……………………..
………………………………..
Vr x Vr-1 x V1= ……………….

Algoritmul de codificare presupune produsul dintre mesajul informational X=a1xk x Gkxn.

Codul Reed-Muller (5,2)

Folosind relatiile generale ale codului Reed-Muller(m,r) ne rezulta urmatoarele valori :

m=5 ; r=2 ; n=32 ; k=16 ; n-k=16 ; d=8 ; t=3, de aici rezulta ca putem corecta maxim 3 erori pe cuvant.

Matricea V pentru RM(5,2) este :

(1111 1111 1111 1111 1111 1111 1111 1111){V0}
(0000 0000 0000 0000 1111 1111 1111 1111){V5}
(0000 0000 1111 1111 0000 0000 1111 1111){V4}
(0000 1111 0000 1111 0000 1111 0000 1111){V3}
(0011 0011 0011 0011 0011 0011 0011 0011){V2}
(0101 0101 0101 0101 0101 0101 0101 0101){V1}
(0000 0000 0000 0000 0000 0000 1111 1111){V54}
(0000 0000 0000 0000 0000 1111 0000 1111){V53} (3.11)
(0000 0000 0000 0000 0011 0011 0011 0011){V52}
(0000 0000 0000 0000 0101 0101 0101 0101){V51}
(0000 0000 0000 1111 0000 0000 0000 1111){V43}
(0000 0000 0011 0011 0000 0000 0011 0011){V42}
(0000 0000 0101 0101 0000 0000 0101 0101){V41}
(0000 0011 0000 0011 0000 0011 0000 0011){V32}
(0000 0101 0000 0101 0000 0111 0000 0101){V31}
(0001 0001 0001 0001 0001 0001 0001 0001);{V21}

Se defineste $\vec{X} = \vec{m} x \vec{G}$ unde m=(a0 a5 a4 a3 a2 a1 a54 a53 a52 a51 a43 a42 a41 a32 a31 a21).

Algoritmul de decodificare se bazeaza pe relatii de control. Pentru a scrie relatiile de control pentru fiecare componenta a vectorului mesaj informational, se va analiza V, incepand de la ultima linie V21, spre prima linie V0, pentru a identifica numarul componentelor diferite de zero din fiecare linie a matricii. Pentru fiecare componenta nenula din liniile matricii vom scrie cate un set de relatii de control corespunzator componentei informationale din mesajul transmis care are acelasi indice cu vectorul analizat.

Mesajul informational este :

$a_{1xk}=(a_0\ a_5\ a_4\ a_3\ a_2\ a_1\ a_{54}\ a_{53}\ a_{52}\ a_{51}\ a_{43}\ a_{42}\ a_{41}\ a_{32}\ a_{31}\ a_{21})$.

Pentru determinarea lui aij se folosesc urmatoarele sisteme, apeland la logica majoritara. Sumele din sistem sunt modulo2. Se calculeaza valoarea pentru fiecare aij si aij este valoarea majoritara din sistem :

$$a_{21} = y_0 \oplus y_1 \oplus y_2 \oplus y_3$$

$$a_{21} = y_4 \oplus y_5 \oplus y_6 \oplus y_7$$

$$a_{21} = y_8 \oplus y_9 \oplus y_{10} \oplus y_{11}$$

$$a_{21} = y_{12} \oplus y_{13} \oplus y_{14} \oplus y_{15}$$

$$a_{21} = y_{16} \oplus y_{17} \oplus y_{18} \oplus y_{19}$$

$$a_{21} = y_{20} \oplus y_{21} \oplus y_{22} \oplus y_{23}$$

$$a_{21} = y_{24} \oplus y_{25} \oplus y_{26} \oplus y_{27}$$

$$a_{21} = y_{28} \oplus y_{29} \oplus y_{30} \oplus y_{31}$$

Iar a21 este valoarea majoritara a sistemului.

$$a_{31} = y_0 \oplus y_1 \oplus y_4 \oplus y_5$$

$$a_{31} = y_2 \oplus y_3 \oplus y_6 \oplus y_7$$

$$a_{31} = y_8 \oplus y_9 \oplus y_{12} \oplus y_{13}$$

$$a_{31} = y_{10} \oplus y_{11} \oplus y_{14} \oplus y_{15}$$

$$a_{31} = y_{16} \oplus y_{17} \oplus y_{20} \oplus y_{21}$$

$$a_{31} = y_{18} \oplus y_{19} \oplus y_{22} \oplus y_{23}$$

$$a_{31} = y_{24} \oplus y_{25} \oplus y_{28} \oplus y_{29}$$

$$a_{31} = y_{26} \oplus y_{27} \oplus y_{30} \oplus y_{31}$$

Iar a31 este valoarea majoritara a sistemului.

$$a_{32} = y_0 \oplus y_2 \oplus y_4 \oplus y_6$$

$$a_{32} = y_1 \oplus y_3 \oplus y_5 \oplus y_7$$

$$a_{32} = y_8 \oplus y_{10} \oplus y_{12} \oplus y_{14}$$

$$a_{32} = y_9 \oplus y_{11} \oplus y_{13} \oplus y_{15}$$

$$a_{32} = y_{16} \oplus y_{18} \oplus y_{20} \oplus y_{22}$$

$$a_{32} = y_{17} \oplus y_{19} \oplus y_{21} \oplus y_{23}$$

$$a_{32} = y_{24} \oplus y_{26} \oplus y_{28} \oplus y_{30}$$

$$a_{32} = y_{25} \oplus y_{27} \oplus y_{29} \oplus y_{31}$$

Iar a32 este valoarea majoritara a sistemului.

$$a_{41} = y_0 \oplus y_1 \oplus y_8 \oplus y_9$$

$$a_{41} = y_2 \oplus y_3 \oplus y_{10} \oplus y_{11}$$

$$a_{41} = y_4 \oplus y_5 \oplus y_{12} \oplus y_{13}$$

$$a_{41} = y_6 \oplus y_7 \oplus y_{14} \oplus y_{15}$$

$$a_{41} = y_{16} \oplus y_{17} \oplus y_{24} \oplus y_{25}$$

$$a_{41} = y_{18} \oplus y_{19} \oplus y_{26} \oplus y_{27}$$

$$a_{41} = y_{20} \oplus y_{21} \oplus y_{28} \oplus y_{29}$$

$$a_{41} = y_{22} \oplus y_{23} \oplus y_{30} \oplus y_{31}$$

Iar a41 este valoarea majoritara a sistemului.

$$a_{42} = y_{0} \oplus y_{2} \oplus y_{8} \oplus y_{10}$$

$$a_{42} = y_{1} \oplus y_{3} \oplus y_{9} \oplus y_{11}$$

$$a_{42} = y_{4} \oplus y_{6} \oplus y_{12} \oplus y_{14}$$

$$a_{42} = y_{5} \oplus y_{7} \oplus y_{13} \oplus y_{15}$$

$$a_{42} = y_{16} \oplus y_{18} \oplus y_{24} \oplus y_{26}$$

$$a_{42} = y_{17} \oplus y_{19} \oplus y_{25} \oplus y_{27}$$

$$a_{42} = y_{20} \oplus y_{22} \oplus y_{28} \oplus y_{30}$$

$$a_{42} = y_{21} \oplus y_{23} \oplus y_{29} \oplus y_{31}$$

Iar a42 este valoarea majoritara a sistemului.

$$a_{43} = y_{0} \oplus y_{4} \oplus y_{8} \oplus y_{12}$$

$$a_{43} = y_{1} \oplus y_{5} \oplus y_{9} \oplus y_{13}$$

$$a_{43} = y_{2} \oplus y_{6} \oplus y_{10} \oplus y_{14}$$

$$a_{43} = y_{3} \oplus y_{7} \oplus y_{11} \oplus y_{15}$$

$$a_{43} = y_{16} \oplus y_{20} \oplus y_{24} \oplus y_{28}$$

$$a_{43} = y_{17} \oplus y_{21} \oplus y_{25} \oplus y_{29}$$

$$a_{43} = y_{18} \oplus y_{22} \oplus y_{26} \oplus y_{30}$$

$a_{43} = y_{19} \oplus y_{23} \oplus y_{27} \oplus y_{31}$

Iar a43 este valoarea majoritara a sistemului.

$$a_{51} = y_{0} \oplus y_{1} \oplus y_{16} \oplus y_{17}$$

$$a_{51} = y_{2} \oplus y_{3} \oplus y_{18} \oplus y_{19}$$

$$a_{51} = y_{4} \oplus y_{5} \oplus y_{20} \oplus y_{21}$$

$$a_{51} = y_{6} \oplus y_{7} \oplus y_{22} \oplus y_{23}$$

$$a_{51} = y_{8} \oplus y_{9} \oplus y_{24} \oplus y_{25}$$

$$a_{51} = y_{10} \oplus y_{11} \oplus y_{26} \oplus y_{27}$$

$$a_{51} = y_{10} \oplus y_{11} \oplus y_{28} \oplus y_{29}$$

$$a_{51} = y_{14} \oplus y_{15} \oplus y_{30} \oplus y_{31}$$

Iar a51 este valoarea majoritara a sistemului.

$$a_{52} = y_0 \oplus y_2 \oplus y_{16} \oplus y_{18}$$

$$a_{52} = y_1 \oplus y_3 \oplus y_{17} \oplus y_{19}$$

$$a_{52} = y_4 \oplus y_6 \oplus y_{20} \oplus y_{22}$$

$$a_{52} = y_5 \oplus y_7 \oplus y_{21} \oplus y_{23}$$

$$a_{52} = y_8 \oplus y_{10} \oplus y_{24} \oplus y_{26}$$

$$a_{52} = y_9 \oplus y_{11} \oplus y_{25} \oplus y_{27}$$

$$a_{52} = y_{12} \oplus y_{14} \oplus y_{28} \oplus y_{30}$$

$$a_{52} = y_{13} \oplus y_{15} \oplus y_{29} \oplus y_{31}$$

Iar a52 este valoarea majoritara a sistemului.

$$a_{53} = y_0 \oplus y_4 \oplus y_{16} \oplus y_{20}$$

$$a_{53} = y_1 \oplus y_5 \oplus y_{17} \oplus y_{21}$$

$$a_{53} = y_2 \oplus y_6 \oplus y_{18} \oplus y_{22}$$

$$a_{53} = y_3 \oplus y_7 \oplus y_{19} \oplus y_{23}$$

$$a_{53} = y_8 \oplus y_{12} \oplus y_{24} \oplus y_{28}$$

$$a_{53} = y_9 \oplus y_{13} \oplus y_{25} \oplus y_{29}$$

$$a_{53} = y_{10} \oplus y_{14} \oplus y_{26} \oplus y_{30}$$

$$a_{53} = y_{11} \oplus y_{15} \oplus y_{27} \oplus y_{31}$$

Iar a53 este valoarea majoritara a sistemului.

$$a_{54} = y_0 \oplus y_8 \oplus y_{16} \oplus y_{24}$$

$$a_{54} = y_1 \oplus y_9 \oplus y_{17} \oplus y_{25}$$

$$a_{54} = y_2 \oplus y_{10} \oplus y_{18} \oplus y_{26}$$

$$a_{54} = y_3 \oplus y_{11} \oplus y_{19} \oplus y_{27}$$

$$a_{54} = y_4 \oplus y_{12} \oplus y_{20} \oplus y_{28}$$

$$a_{54} = y_5 \oplus y_{13} \oplus y_{21} \oplus y_{29}$$

$$a_{54} = y_6 \oplus y_{14} \oplus y_{22} \oplus y_{30}$$

$$a_{54} = y_7 \oplus y_{15} \oplus y_{23} \oplus y_{31}$$

Iar a54 este valoarea majoritara a sistemului.

Dupa ce au fost scrise relatiile de control corespunzatoare vectorilor compusi, se procedeaza in felul urmator:

- se elimina influenta din relatiile de control a componentelor corespunzatoare vectorilor compusi ;
- se scriu numarul de relatii de control pentru vectorii simpli, in numar de cate componente diferite de zero sunt pe fiecare din liniile lui V (pentru vectorii simpli).

Urmatorul pas este determinarea lui y' :

$$y' = y-(a_{54}*V_{54}+a_{53}*V_{53}+a_{52}*V_{52}+a_{51}*V_{51}+a_{43}*V_{43}+a_{42}*V_{42}+a_{41}*V_{41}+a_{32}*V_{32}+a_{31}*V_{31}+a_{21}*V_{21});$$

Pentru a vedea valoarea componentei mesajului informational :
(a54 a53 a52 a51 a43 a42 a41 a32 a31 a21)
se procedeaza pe baza logicii majoritare.

$$a_1 = y_0 \oplus y_1$$

$$a_1 = y_2 \oplus y_3$$

$$a_1 = y_4 \oplus y_5$$

$$a_1 = y_6 \oplus y_7$$

$$a_1 = y_8 \oplus y_9$$

$$a_1 = y_{12} \oplus y_{13}$$

$$a_1 = y_{14} \oplus y_{15}$$

$$a_1 = y_{16} \oplus y_{17}$$

$$a_1 = y_{18} \oplus y_{19}$$

$$a_1 = y_{20} \oplus y_{21}$$

$$a_1 = y_{22} \oplus y_{23}$$

$$a_1 = y_{24} \oplus y_{25}$$

$$a_1 = y_{26} \oplus y_{27}$$

$$a_1 = y_{28} \oplus y_{29}$$

$$a_1 = y_{30} \oplus y_{31}$$

Iar a1 este valoarea majoritara a sistemului.

$$a_2 = y_0 \oplus y_2$$

$$a_2 = y_1 \oplus y_3$$

$$a_2 = y_4 \oplus y_6$$

$$a_2 = y_5 \oplus y_7$$

$$a_2 = y_8 \oplus y_{10}$$

$$a_2 = y_9 \oplus y_{11}$$

$$a_2 = y_{12} \oplus y_{14}$$

$$a_2 = y_{13} \oplus y_{15}$$

$$a_2 = y_{16} \oplus y_{18}$$

$$a_2 = y_{17} \oplus y_{19}$$

$$a_2 = y_{20} \oplus y_{22}$$

$$a_2 = y_{21} \oplus y_{23}$$

$$a_2 = y_{24} \oplus y_{26}$$

$$a_2 = y_{25} \oplus y_{27}$$

$$a_2 = y_{28} \oplus y_{30}$$

$$a_2 = y_{29} \oplus y_{31}$$

Iar a2 este valoarea majoritara a sistemului.

$$a_3 = y_0 + y_4$$

$$a_3 = y_1 + y_5$$

$$a_3 = y_2 + y_6$$

$$a_3 = y_3 + y_7$$

$$a_3 = y_8 + y_{12}$$

$$a_3 = y_9 + y_{13}$$

$$a_3 = y_{10} + y_{14}$$

$$a_3 = y_{11} + y_{15}$$

$$a_3 = y_{16} + y_{20}$$

$$a_3 = y_{17} + y_{21}$$

$$a_3 = y_{18} + y_{22}$$

$$a_3 = y_{19} + y_{23}$$

$$a_3 = y_{24} + y_{28}$$

$$a_3 = y_{25} + y_{29}$$

$$a_3 = y_{26} + y_{30}$$

$$a_3 = y_{27} + y_{31}$$

Iar a3 este valoarea majoritara a sistemului.

$$a_4 = y_0 + y_8$$
$$a_4 = y_1 + y_9$$
$$a_4 = y_2 + y_{10}$$
$$a_4 = y_3 + y_{11}$$
$$a_4 = y_4 + y_{12}$$
$$a_4 = y_5 + y_{13}$$
$$a_4 = y_6 + y_{14}$$
$$a_4 = y_7 + y_{15}$$
$$a_4 = y_{16} + y_{24}$$
$$a_4 = y_{17} + y_{25}$$
$$a_4 = y_{18} + y_{26}$$
$$a_4 = y_{19} + y_{27}$$
$$a_4 = y_{20} + y_{28}$$
$$a_4 = y_{21} + y_{29}$$
$$a_4 = y_{22} + y_{30}$$
$$a_4 = y_{23} + y_{31}$$

Iar a4 este valoarea majoritara a sistemului.

$$a_5 = y_0 + y_{16}$$
$$a_5 = y_1 + y_{17}$$
$$a_5 = y_2 + y_{18}$$
$$a_5 = y_3 + y_{19}$$
$$a_5 = y_4 + y_{20}$$
$$a_5 = y_5 + y_{21}$$
$$a_5 = y_6 + y_{22}$$
$$a_5 = y_7 + y_{23}$$
$$a_5 = y_8 + y_{24}$$
$$a_5 = y_9 + y_{25}$$
$$a_5 = y_{10} + y_{26}$$
$$a_5 = y_{11} + y_{27}$$
$$a_5 = y_{12} + y_{28}$$
$$a_5 = y_{11} + y_{29}$$
$$a_5 = y_{14} + y_{30}$$
$$a_5 = y_{15} + y_{31}$$

Iar a5 este valoarea majoritara a sistemului.

Dupa ce au fost evaluate componentele de la a1 la a5, se elimina influenta vectorilor simpli din vectorul y' :

y =y'-(a1*V1+ a2*V2+ a3*V3+ a4*V4+ a5*V5)

Pentru a evalua pe a0, observam numarul majoritar de componente din y » iar valoarea celor mai multe componente va fi valoarea lui a0. Mesajul corectat este :

m=(a0 a5 a4 a3 a2 a1 a54 a53 a52 a51 a43 a42 a41 a32 a31 a21)

Codul BHC

Codurile Bose-Chadhuri-Hocquenghem (BCH) constituie o clasă de coduri ciclice cu o deosebită capacitate de corecţie a erorilor, care generalizează codurile Hamming pentru corecţia erorilor multiple.

Un cod ciclic binar, corector de *t* erori, având

- Lungimea blocului n=$2^n - 1$, cu m≥ 3, întreg
- Numărul simbolurilor de control n-k $\leq$ mt, t$< 2^m - 1$,
- Distanţa d$\geq 2t + 1$,

se numeşte cod BHC dacă are drept polinom generator g(x) polinomul de cel mai mic grad peste câmpul GF(2) care are ca rădăcini elementele $\alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ ale câmpului Galois GF(2^m).

Prin urmare g(α^1)=0, i=$\overline{1,2t}$

Fie $\Phi_i(x)$ polinomul minimal al lui α^1, adică polinomul de cel mai mic grad peste GF(2) astfel încât $\Phi_i(x)$ =0. Atunci polinomul generator g(x) trebuie să fie cel mai mic multiplu comun (c.m.m.m.c) al polinoamelor $\Phi_1(x), \Phi_2(x), \ldots, \Phi_{2i}(x)$

şi anume: g(x)= (c.m.m.m.c){ $\Phi_1(x), \Phi_2(x), \ldots, \Phi_{2i}(x)$}.

Un număr par *i* poate fi exprimat sub forma i=k*2^j, k≥ 1, impar. Atunci α^i=$(\alpha^k)^{2j}$ este conjugatul elementului α^k. Dar un polinom care admite rădăcinile $\alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ admite drept rădăcini şi conjugatele acestora. Prin urmare, α^j şi α^k au acelaşi polinom minimal şi deci $\Phi_j(x) = \Phi_k(x)$. Atunci polinomul generator este de forma

g(x)= (c.m.m.m.c){ $\Phi_1(x), \Phi_3(x), \ldots, \Phi_{2t-1}(x)$}. (3.12)

Grdul fiecărui polinom minimal fiind cel mult egal cu *m* , polinomul g(x) va fi de grad cel mult egal cu *mt* , astfel încât numărul simbolurilor de control, n-k , va fi cel mult egal cu *mt* : *n-k* $\leq$*mt.* La limită, în cazul corecţiei unei singure erori, t=1, rezultă *n-k* $=$*mt.*

Codul BCH de lungime $2^m - 1$, cu m≤10 , se numesc coduri BCH în sens restrâns (sau primitive). Aceste coduri sunt generate de elemente primitive de ordin mai mic decât 2^{10} din GF(2^m).

Un cod BCH de lungime $2^m - 1$ corector de o singură eroare este generat de polinomul g(x)= $\Phi_1(x)$.

Polinoamele minimale ale elementelor din GF($\mathbf{2^4}$) generate de g(x)=1+x+$\boldsymbol{x^4}$

Rădăcini conjugate	Polinoame minimale
0	x
1	x+1
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$x^3 + x + 1$

- **Exemplu.** $\Phi_1(x)$ trebuie să fie de grad m=4 , deci de forma

$$\Phi_1(x)=1+a_1 x + a_2 x^2 + a_3 x^3 + x^4 \tag{3.13}$$

Deoarece

$$\Phi_1(x)=1+a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \alpha^4 \tag{3.14}$$

Conform tabelului 3.3 înseamnă că

$$\begin{bmatrix}0\\0\\0\\1\end{bmatrix} + a_1 \begin{bmatrix}0\\0\\1\\0\end{bmatrix} + a_2 \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + a_3 \begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} \tag{3.15}$$

şi rezultă

$$a_1 = 1, a_2 = a_3 = 0$$

Deci

$$\Phi_1(x)= 1+x+x^4 \tag{3.16}$$

Deoarece din 2t-1=3 rezultă t=2, se deduce un cod BCH corector de două erori şi de lungime n= $2^m - 1$ = 15 este generat de g(x)= (c.m.m.m.c){ $\Phi_1(x)$, $\Phi_3(x)$}=$\Phi_1(x)\Phi_3$(x)=1+$x^4 + x^6 + x^7 + x^8$.

Fie v(x) un polinom de cod cu coeficienţii în GF(2), asociaţi unuo cuvânt de cod v(x)=$a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Polinomul de cod admite rădăcinile $\alpha^1, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ din GF(2^m).

Dacă α^i este o rădăcină a lui v(x) pentru 1$\le i \le 2t$, atunci

$$v(\alpha^i) = a_0 + a_1\alpha^i + a_2\alpha^{2i} + \cdots + a_{n-1}\alpha^{(n-1)i} = 0. \tag{3.17}$$

Se introduce matricea

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix}, \tag{3.18}$$

astfel încât v H^T=0.

Rezultă că *v* este în spaţiul nul al matricei H şi deci H este matrice de control a codului.

Aplicaţii

Simularea cu ajutorul programului MATLAB a codului BCH

Codurile BCH fac parte din categoria codurilor ciclice. Se va implementa în programul MATLAB schema prezentată în figura următoare.

Se vor utiliza următoarele blocuri:

- **Random-Integer Generator**: generează numere întregi distribuite în intervalul [0, M-1]. Parametrii blocului sunt:
  - ‘M-ary number’ este 2^7 deoarece codul BCH utilizat este BCH**(15,7)** şi numerele generate sunt reprezentate în binar pe 7 biţi.
  - ‘Initial seed’ este [1458]. Modificând acest parametru se modifica secvenţa de numere generate.
  - ‘Sample time’ este 1. Generează câte un număr la fiecare secundă.
- **Integer to Bit Converter**: transformă un vector de întregi într-un vector de biţi. Parametrul blocului este:
  - ‘Number of bits per integer’ este 7. Se lucrează pe 7 biţi.
- **BCH Encoder**: crează un cod BCH din datele vectorului binar. Parametrii blocului

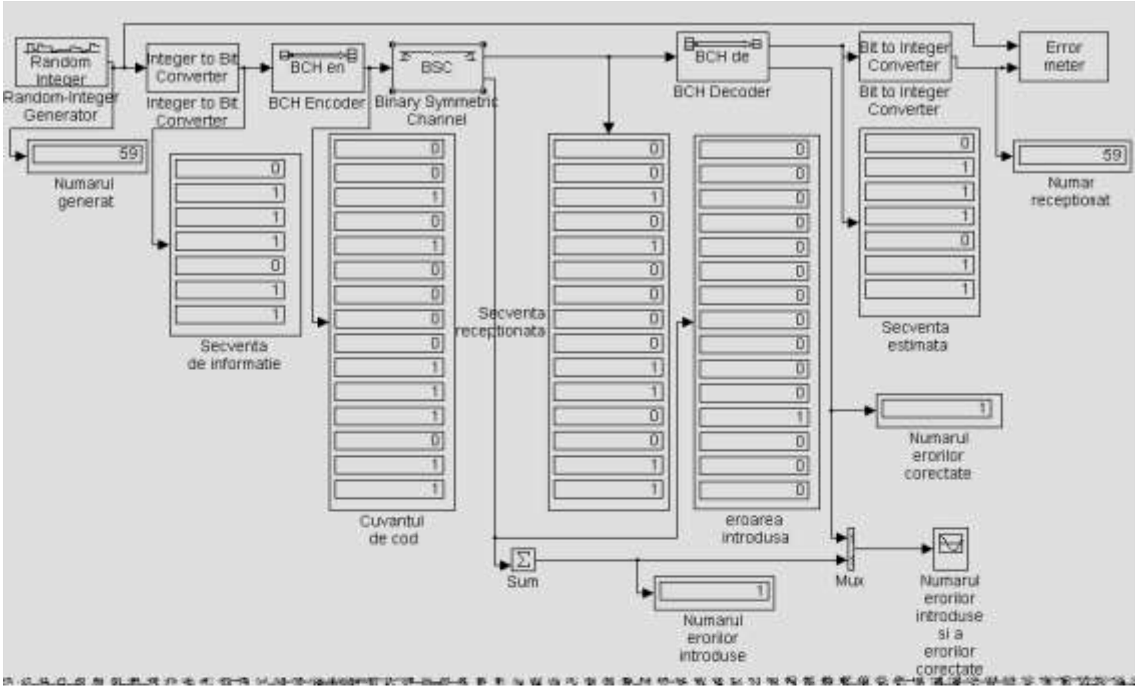
sunt:

- ‘Codeword length N’ este 15.
- ‘Message length K’ este 7 deoarece se utilizează codul BCH(15,7).

- **Binary Symmetric Channel**: introduce erori binare. Parametrii blocului sunt:
  - ‘Error probability’ este 0.1, pentru a nu introduce erori.
  - ‘Input vector length’ este 15 deoarece cuvântul de cod cu care se adună este reprezentat pe 15 biţi.
  - ‘Initial seed’ este 12345.

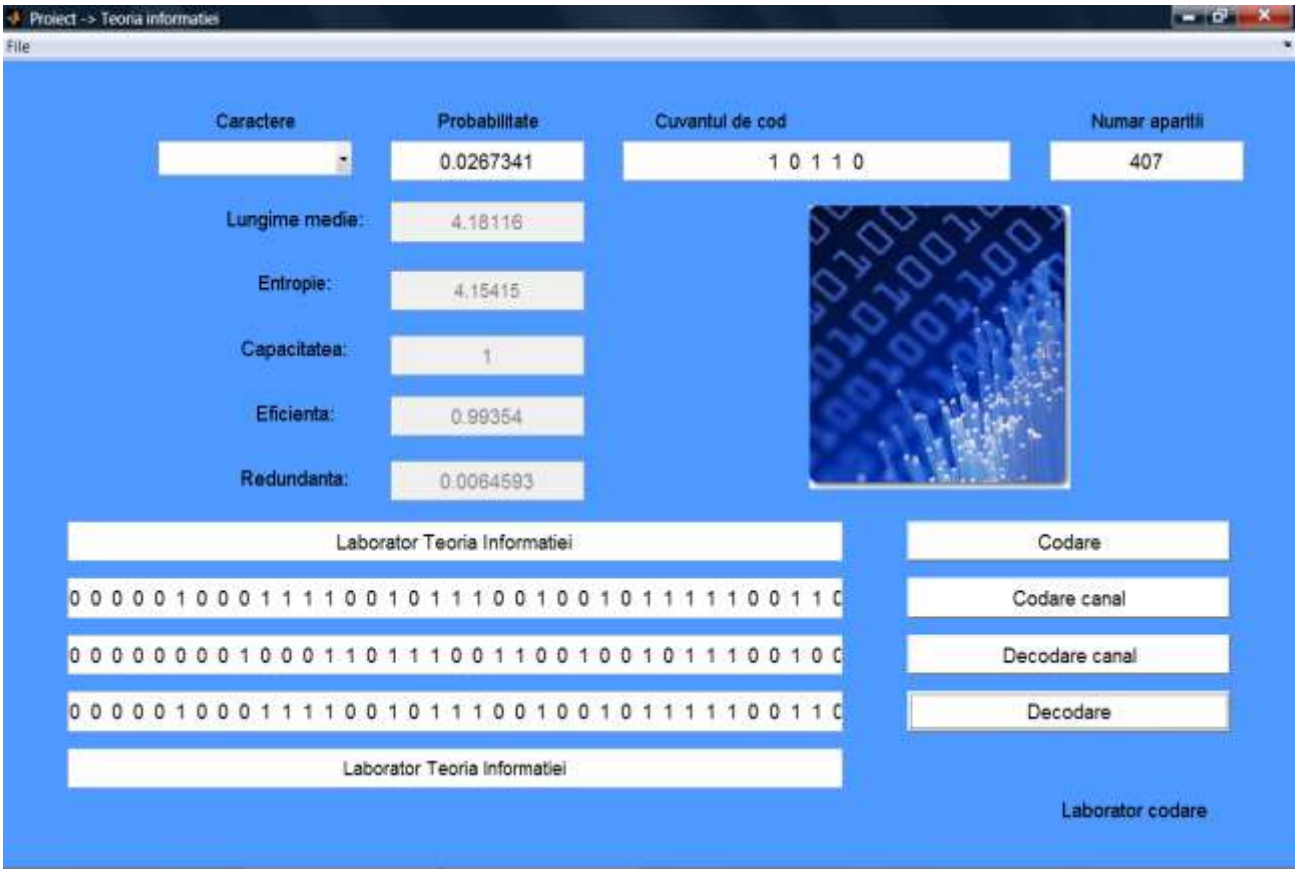
- ‘Sample time’ este 1 pentru a se genera un eşantion la fiecare secundă.- **BCH Decoder**: decodează un cod BCH pentru a reface vectorul binar transmis. Parametrii blocului sunt:
  - ‘Codeword length N’ este 15 .
  - ‘Message length K’ este 7 deoarece se utilizează codul BCH(15,7).
- **Bit to Integer Converter**: transformă un vector de biţi într-un vector de întregi. Parametrul blocului este:
  - ‘Number of bits per integer’ este 7.
- **Error Meter**: compară semnalele de la intrare, le afişează şi evaluează rata de eroare. Parametrii blocului sunt:
  - ‘Bit per symbol’ este 7 deoarece utilizează 7 biţi pentru fiecare simbol transmis.
  - ‘Number of digits on display’ este 20 deoarece afişează 20 de simboluri.
  - ‘Delay between input (1^{st} port) and output (2^{nd} port)’ este 0.
  - ‘Sample time’ este 1 deoarece se consideră un eşantion la fiecare secundă.
- **Sum**: afişează suma elementelor de la intrare. Parametrii blocului sunt:
  - ‘Icon shape’ este rectangular.
  - ‘List of signs’ este +.
- **Graph Scope**: afişează numărul de erori. Parametrii blocului sunt:
  - ‘Time range’ este 10.
  - ‘y-min’ este -1.
  - ‘y-max’ este 5.
  - ‘Line type’ este 'ro/b*'
- **Mux**: multiplexează semnalele de la intrare.
- **Display**: afişează valoarea de la intrare.

Se va realiza schema bloc aratată şi se va rula pentru diferite valori ale probabilitatii de eroare si se vor analiza rezultatele.



Simularea cu ajutorul programului MATLAB a codului Hamming

În cadrul lucrărilor de laborator va fi pusă la dispoziţie o aplicaţie software care implemenează algoritmul de compresie Shannon-Fano. Ecranul aplicaţiei este prezentat în figura următoare.



Exerciţii rezolvate.

Un număr de 8 simboluri se transmit cu ajutorul unui cod Hamming grup corector de o eroare şi detector de erori duble. Se cere:

a. să se determine numărul simbolurilor de informaţie k, al celor de control m, şi lungimea cuvântului de cod n;
b. să se scrie matricea de control H a codului;
c. să se stabilească expresia corectorului corespunzător eronării simbolului c_2;
d. să se determine corectorul corespunzător eronării simbolurilor c_2 şi c_1;
e. să se determine cuvintele de cod;
f. să se precizeze dacă $v = [1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0]$ este un cuvânt al acestui cod.

Soluţie

a). Numărul simbolurilor de informaţie k se determină cu relaţia $2^k \geq N = 8$ şi rezultă k=3.

Marginea Hamming dă pentru numărul simbolurilor de control: $2^m - 1 \geq n = m + k = m + 3$, din care rezultă că m=3.

La aceste simboluri de control, care permit corecţia unei erori, trebuie adăugat simbolul de verificare la paritate, aşa încât numărul total al simbolurilor de control va fi:

$$m^1\text{=m+1=3+1=4}$$

Structura cuvântului de cod va fi:

$$v = [c_0\, c_1\, c_2\, i_3\, c_4\, i_5\, i_6\,]$$

Unde c_0 este simbolul de verificare a parităţii, iar $c_1\,, c_2\,, c_4$ - simbolurile de control pebtru codul corector de o eroare.

b). Matricea H a codului corector de o eroare este de forma:

$$H=[h_1 h_2 h_3 h_4 h_5 h_6]$$

respectiv:

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

Cu relaţia (2.33) se obţine pentru matricea H^{-1} expresia:

$$H^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = [h_0^1\ h_1^1\ h_2^1\ h_3^1\ h_4^1\ h_5^1\ h_6^1]$$

c). Pentru acest caz cuvântul de eroare este de forma:

$$\varepsilon=[0\ \ 0\ 1\ \ 0\ \ 0\ \ 0\ \ 0]$$

Cu relaţia (2.34) rezultă pentru expresia corectorului

$$z^1 = [h_2^1] = \begin{bmatrix} 0 \\ 1 \\ \hline 0 \\ 1 \\ \\ \end{bmatrix} = \begin{bmatrix} h_2 \\ \hline 1 \end{bmatrix}$$

Din expresia corectorului rezultă că apare o eroare corectabilă ($z_0 = 1$) pe poziţia a 2-a (z=h_2).

d). Pentru acest caz cuvântul eroare este de forma:

$$\varepsilon = [0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

şi rezultă:

$$z^1=[h_1^1 + h_2^1] = \begin{bmatrix} 0 \\ 1 \\ \hline 0 \\ 1 \\ \\ \end{bmatrix}$$

Corectorul arată că apar două erori detecctabile ($z_0 = 0$ şi $z = 0$).

e). Cuvintele de cod se pot scrie calculând simbolurile de control din cele de informaţie cu relaţia $H^1 v^T = 0$, din care rezultă:

$$c_4 = i_5 + i_6$$

$$c_2 = i_3 + i_6$$

$$c_1 = i_3 + i_5$$

$$c_0 = c_1 + c_2 + i_3 + c_4 + i_5 + i_6 = i_3 + i_5 + i_6$$

Cuvintele de cod se găsesc în tabelul următor.

Simboluri / Cuvinte	c_0	c_1	c_2	i_3	c_4	i_5	i_6
v_0	0	0	0	0	0	0	0

v_1	1	0	1	0	1	0	1
v_2	1	1	0	0	1	1	0
v_3	0	1	1	0	0	1	1
v_4	1	1	1	1	0	0	0
v_5	0	1	0	1	1	0	1
v_6	0	0	1	1	1	1	0
v_7	1	0	0	1	0	1	1

f). Se calculează corectorul z^1 astfel:

$$z^1 = H^1 v^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \underline{0} \\ 0 \end{bmatrix} = \begin{bmatrix} z \\ \hline z_0 \end{bmatrix}$$

Deoarece $z_0 = 0$ iar z=0 cuvântul dat este un cuvânt al acestui cod, ceea ce era usor de constatat şi prin inspectarea tabelului anterior, în care îl regăsim sub forma cuvântului v_2.

TESTE DE AUTOEVALUARE ŞI TEME DE CONTROL

Testul nr. 1

Se consideră un cod grup cu matricea de control de forma:

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

a. să se determine proprietăţile de corecţie ale codului. Codul este perfect?

b. să se stabilească dacă matricea:

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

poate să fie matricea generatoare a codului.

c. să se scrie cuvintele de cod utilizând matricele H şi G.

BIBLIOGRAFIE RECOMANDATĂ LA MODULUL 3:

[1] A. Spătaru: Teoria Transmisiunii Informaţiei, Ed. Didactică şi Pedagogică, Bucureşti, 1983.

[2] A. T. Murgan, I. Spânu, I. Gavăt, I. Sztojanov, V. E. Neagoe, A. Vlad: Teoria Transmisiunii Informaţiei - probleme, Ed. Didactică şi Pedagogică, Bucureşti, 1983

[3] I. Angheloiu, Teoria codurilor, Ed. Militară, Bucureşti, 1972.

[4] J.C. Moreira, P.G. Farrell, ESSENTIALS OF ERROR-CONTROL CODING, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England,2006.