Coduri BCH

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

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

- lungimea blocului $n = 2^n - 1$, cu $m \geq 3$, întreg,
- numărul simbolurilor de control $n - k \leq mt$, $t < 2^m - 1$,
- distanța $d \geq 2t + 1$,

se numeşte cod BCH 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

$$g(\alpha^i) = 0, \quad i = \overline{1,2t}.$$

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

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

Un număr par *i* poate fi exprimat sub forma $i = k \cdot 2^j$, $k \geq 1$, inpar. Atunci

$$\alpha^i = (\alpha^k)^{2j}$$

este conjugatul elementului α^k. Dar un polinom care admite rădăcinile $\alpha^1, \alpha^2, \ldots, \alpha^{2t}$ 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

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

Gradul 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 corecției unei singure erori, t=1, rezultă n-k=mt.

Codul BCH de lungime $2^m - 1$, cu $m \leq 10$, 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)= $\Phi_1(x)$.

Polinoame minimale ale elementelor din GF(2^4) generate de $g(x)=1+x+x^4$

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

$$\Phi_1(x)=1+a_1x+a_2x^2+a_3x^3+x^4.$$

Deoarece

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

conform tabelului 3.3 înseamnă că

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

şi rezultă

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

deci

$$\Phi_1(x)=1+x+x^4.$$

Deoarece din 2t-1=3 rezultă t=2, se deduce că un cod BCH corector de două erori şi de lungime n= 2^m-1=15 este generat de

$$\text{g(x)=c.m.m.m.c.}\{\Phi_1(x),\Phi_3(x)\}=\Phi_1(x)\Phi_3(x)=1+x^4+x^6+x^7+x^8.\blacksquare$$

Fie *v(x)* un polinom de cod cu coeficienții în GF(2), asociați unui cuvânt de cod $v(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$. Polinomul de cod admite rădăcinile $\alpha,\alpha^2,\ldots,\alpha^{2t}$ din $GF(2^m)$.

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

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

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

astfel încât $vH^T = 0$.

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

Aplicație coduri BCH

Codurile BCH fac parte din categoria codurilor ciclice.
Pentru a arăta utilitatea codurilor BCH utilizăm următorul model:

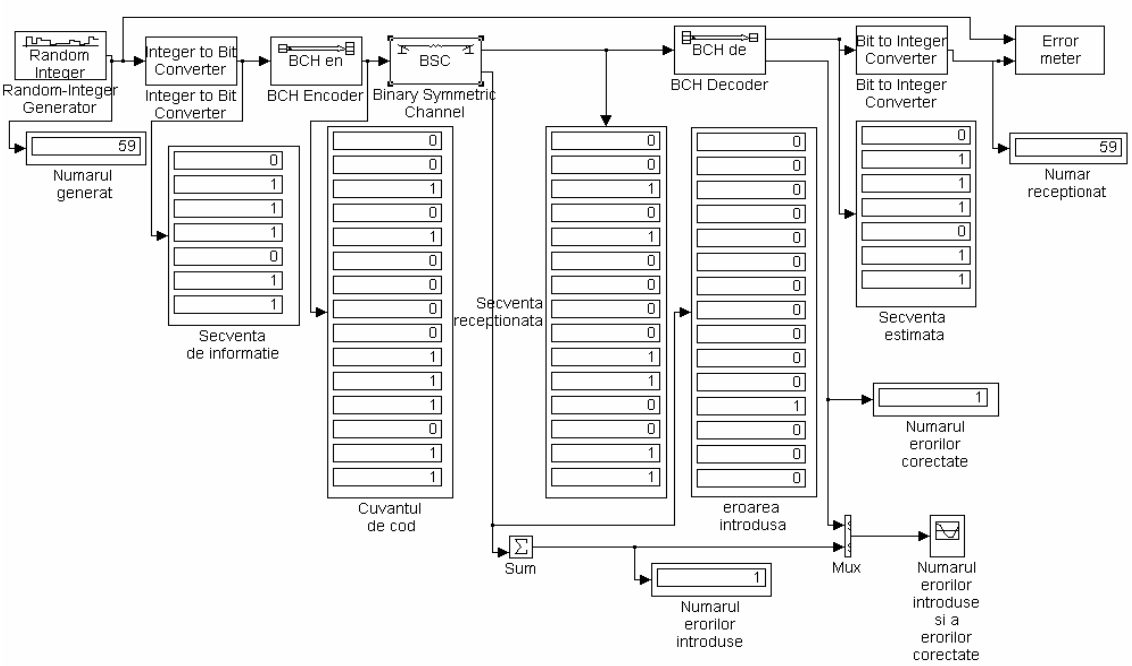

Fig. 1

Folosim 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 biți.
  - ‘Initial seed’ este [1458]. Modificând acest parametru se modifica secvența 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 biți. Parametrul blocului este:
  - ‘Number of bits per integer’ este 7. Se lucrează pe 7 biți.
- **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 biți.
  - ‘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 biți 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 biți 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.

Desfaşurarea lucrării:

1. Se va realiza schema bloc aratata şi se va rula pentru diferite valori ale probabilitatii de eroare si se vor analiza rezultatele.
2. Se vor genera diferiți întregi şi se va scoate in evidentă modalitatea de generare a acestora.
3. Se vor analiza blocurile şi se va nota rolul îndeplinit de fiecare bloc în parte şi cum modifică acestea rezultatul codării.