Teoria informatiei si a codurilor

Prof. dr. ing. Racuciu Ciprian

I. TEORIA INFORMATIEI

I.1 Notiuni fundamentale de teorie a informatiei

I.1.1 Informatia si proprietatile ei principale

Informatia reprezinta partea centrala a oricarui proces de conducere si comanda. *Informatia este o stire care poarta urma unui fapt care nu era cunoscut.*

Informatia se poate gasii sub forma de:

- Carti;
- Limbaj;
- Grafice;
- Imagini;
- Suporti magnetici;

- Suporti optici;
- Afisajul instrumentelor de masura, etc.

Proprietatii:

- Informatia este foarte diversificata
  - Privitor la forma de prezentare
  - Privitor la domeniu la cere se refera
- Informatia poate fi prelucrata
- Orice informatie este un izvor de informatie noua
- Orice informatie poate fi masurata
- Informatia poate fi stocata
- Niciodata informatia nu se uzeaza prin utilizare, ci genereaza cantitati tot mai mari de informatie noua.

I.1.2 Modelul sistemului de transmisiuni

Principala problema a teoriei informatiei este studierea transformarii, pastrarii si transmiterii informatiei.

Purtatorul material al informatiei, semnalul, isi pastreza capacitatea sa de a transmite informatia numai in cadrul unui **sistem de transmisiuni**, a carui schema bloc generala este data in *figura 1*:

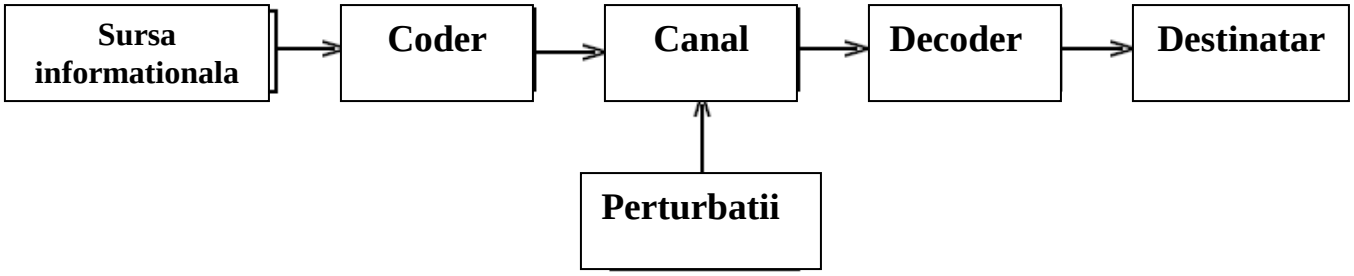


Figura 1 – Modelul general al sistemului de transmisiuni

,unde:

• **1. Sursa informationala** –poate fi omul sau un dispozitiv oarecare, care genereaza informatia sau comunicare ce urmeaza a fi transmisa

• **2. Coderul** – este acea parte a sistemului de comunicatie care efectueaza o prelucrare a informatiei date de sursa pentru a putea fi apta pentru transmiterea pe canalul de transmisie.

• **3. Canalul** – reprezinta mediul fizic prin care se face transmiterea informatiei: de exemplu linia telefonica, linia radio sau radioreleu, etc.

• **4.** Asupra canalului pot actiona anumite **perturbatii** care in liniile de
telefonie apar din cauza modificarilor caracteristicii de frecventa, a zgomotului termic, a impulsurilor parazite (a caror sursa poate fi o schema de comutare), a bruiajului intentionat al adversarului, etc.

• **5. Decoderul** – executa prelucrarea semnalului de la iesirea canalului in scopul de a reproduce la partea de receptie o copie acceptabila a iesirii sursei.

• **6. Destinatarul** – care poate fi omul sau un dispozitiv tehnic oarecare.

Coderul si decoderul se impart in cate doua blocuri (coderul de sursa si de canal, respectiv decoderul de canal si de sursa), ca in *figura 2*.

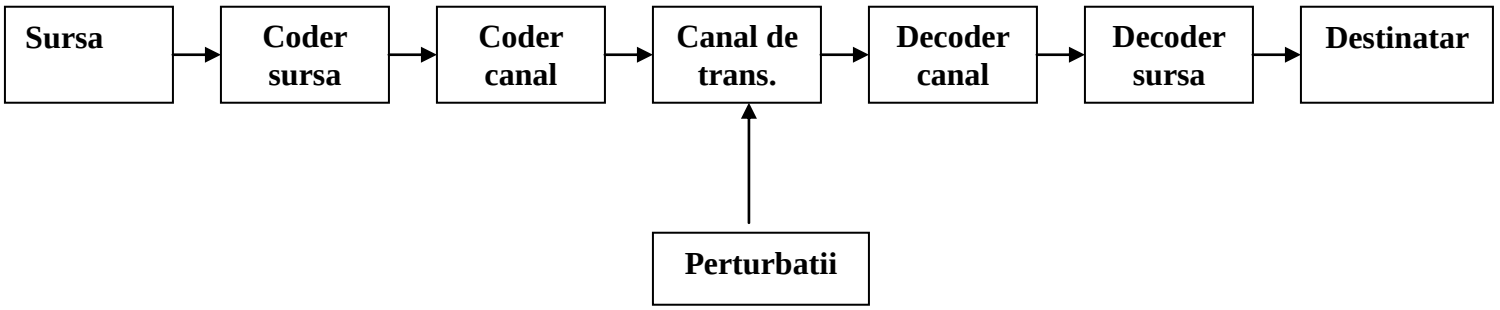


Figura 2 – modelul extins al sistemului de transmisiuni

I.1.2.1 Modelul probabilistic al semnalelor

Considera notiunea de semnal purtator de informatie. Semnalul poate sa fie ***continuu sau discret***. In studiul semnalelor discrete modelele probabilistice au un rol important.

In cazul semnalelor discrete intotdeauna se poate realiza o corespondenta biunivoca intre numarul de semnale posibile si o multime de numere naturale pe care o notam cu X , facind ca fiecarui semnal sa i se atribuie un numar x care sa apartina lui X . Altfel spus, modelul probabilistic al semnalelor este dat printr-o repartitie a variabilei aleatoare X .

$$X=\begin{pmatrix} x1 & x2 & x3 \ldots\ldots\ldots\ldots xn \\ p(x1) & p(x2) & p(x3)\ldots\ldots\ldots p(xn) \end{pmatrix}$$

,unde :

$p(x_k)$-probabilitatea de aparitie a evenimentului $x=x_k$

Observatie :

Intotdeauna :

$\Sigma p(x_k)=1 \rightarrow$ aceasta relatie este valabila pentru toate spatiile de semnale

Frecventa de aparitie a literelor in text este urmatoarea $f_k = i_k / N$ unde

- $i_k \rightarrow$ numarul de aparitii a unui simbol
- $N \rightarrow$ numarul total de simboluri din text

I.1.3 Codificarea surselor

Sursa discreta fara memorie reprezinta un generator de semnale purtatoare de informatie care genereaza semnale dicrete de tipul a_i din alfabetul sau de semnale notat cu $A= \{a_1, a_2, \dots , a_i\}$.

Daca semnalele sursei sunt statistic independente (adica sursa este fara memorie), probabilitatea unei succesiuni date $\alpha^n= (\alpha_1, \alpha_2, \dots , \alpha_n)$ de n litere de sursa este egala cu produsul probabilitatilor literelor de sursa:

$$P(\alpha_1, \alpha_2, \dots ,\alpha_n) = \prod_{i=1}^{n} P(\alpha_i)$$

Trecera de la un sistem de semnale numite primare, la un sistem de semnale, numite secundare, se numeste codificare. Cerinta de baza care se pune operatiei de codificare este aceea de a se realiza in asa fel incat decodificarea sa fie univoca.

Multimea tuturor cuvintelor de cod se numeste **cod**.

Cunoasterea unei surse implica de fapt, cunoasterea probabilitatilor cu care se genereaza semnalele din alfabetul sau de-a lungul existentei sale.

Codarea surselor se face prin intermediul coderului de sursa. Presupunem ca alfabetul sursei (discrete si fara memorie) contine M semnale primare notate cu $a_1, a_2, \dots , a_M$ care apar cu probabilitatile $p(a_1), p(a_2), \dots , p(a_M)$. Fiecare litera a sursei trebuie sa fie codificata printr-o combinatie de semnale secundare luate din alfabetul codului care contine N semnale, $X=\{x_1, x_2, \dots, x_N\}$. Aceste combinatii se numesc cuvinte de cod, iar totalitatea lor formeaza un cod $C=\{c_1, c_2, \dots, c_M\}$.

Dintre toate **codurile unic decodabile** prezinta interes din punct de vedere economic , acel cod care conduce la un numar mediu de litere de cod pe litere de sursa, $\bar{l}$, cat mai mic posibil. $\bar{l}$ se numeste **lungimea medie** a combinatiilor de cod.

$$\bar{l} = \sum P(a_k) \cdot l_k$$

Codurile pot fi de doua tipuri: 1. coduri uniforme

2. coduri neuniforme,

Codurile neuniforme au lungimea medie a cuvintelor mai mica de cat a celor uniforme, sunt si utilizate in aplicatii.

Codul C se numeste unic decodabil daca succesiunile cuvintelor de cod, corespunzatoare diferitelor succesiuni de lungime finita a sursei, sunt distincte.

Fie un cuvant de cod $c_i = x_{i1}, x_{i2}, \ldots, x_{im}$. Sirul de litere $x_{i1}, x_{i2}, \ldots, x_{ik,}$ unde $k \leq m$ se numeste **prefixul** lui c_i.

Cu ajutorul notiunii de prefix putem defini subclasa codurilor unic decodabile care prezinta un interes deosebit din punct de vedere practic.

Codul in care nici un cuvant de cod nu este prefixul unui alt cuvant de cod se numeste **cod cu proprietate de prefix**.

Codurile cu proprietate de prefix se mai numesc si **coduri instantanee**, deoarece o combinatie de cod se poate recunoaste fara nici o referinta la urmatoarea combinatie de cod.

I.1.4 Teorema de existenta a codurilor cu proprietate de prefix. Inegalitatea Kraft – Fano

Conditia necesara si suficienta de existenta a unui cod $C = \{c_1, c_2, \ldots, c_M\}$ cu proprietate de prefix si cu lungimile cuvintelor de cod $n_1, n_2, \ldots, n_M$ este ca

$\sum_{k=1}^{N} M^{-l_k} \leq 1$, unde M = numarul de semnale secundare din cadrul alfabetului.

I.1.5 Teorema de codifcare a sursei. Prima teorema a lui Shannon

Multimea semnalelor primare $A=\{a_1,a_2,\ldots,a_M\}$, avand entropia:

$$H(A) = \sum_{k=1}^{M} P(a_k) \log \frac{1}{P(a_k)},$$

se poate codifica printr-un cod unic decodabil M-ar in asa fel incat lungimea medie a cuvintelor de cod n sa satisfaca relatia:

$$\frac{H(A)}{\log M} \leq \bar{l} < \frac{H(A)}{\log M} + 1$$

I.1.6 Capacitatea, eficienta si redundanta codului

Entropia unui mesaj, codificat cu ajutorul unui alfabet de cod $X=\{x_1,x_2,\ldots,x_D\}$, se noteaza cu H(X) care ia valoarea maxima, log M, in cazul cand elementele alfabetului codului apar cu aceeasi probabilitate, deci $\max H(X) = \log M$.

Prin definitie, valoarea maxima a entropiei alfabetului codului se numeste **capacitatea codului**.

Din teorema lui Shannon rezulta ca lungimea minima a unui cuvant de cod este

$$\bar{l}_{\min} = \frac{H(A)}{\log M}$$

Raportul $\frac{\bar{l}_{\min}}{\bar{l}} = \frac{H(A)}{\bar{l}\cdot \log M} = \eta$ se numeste **eficienta codului** C.

Redundanta codului se defineste ca, complementarul eficientei:

$$1-\eta = 1-\frac{H(X)}{\log M}$$

I.1.7 Metode de codificare

Exista doua metode de codificare neredundanta; **metoda Shannon – Fano**, si **metoda lui Huffman**.

Metoda lui Huffman:

Furnizeaza intotdeauna un cod optim unic decodabil cu proprietate de prefix si lungime medie minima.

Etapele metodei:

1. Se ordoneaza evenimentele astfel incat $p(a_1)\geq p(a_2)\geq\ldots\geq p(a_N)$
2. Se construieste sursa redusa de ordinul I.

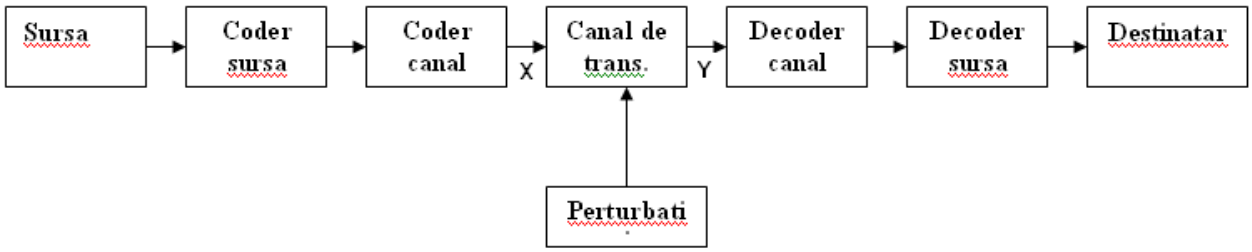
   Sursa redusa se obtine din sursa initiala prin gruparea ultimelor 2 litere pentru care impunem ca probabilitatea de aparitie sa fie suma probabilitatilor initiale iar gruparea se face prin reuniunea evenimentelor din sursa principala.
3. Se contruieste sursa redusa de ordinul II in mod analog cu obtinerea sursei reduse de ordinul I combinand ultimele 2 elemente ale sursei reduse de ordinul I.

4. Se procedeaza in mod similar la o succesiune de etape de reducere pana cand se ajunge la o sursa redusa alcatuita din 2 elemente.(in cazul codificarii binare)
   Observatie:
   Dupa fiecare etapa de reducere inainte de a face operatiunea de reducere, urmatoarea sursa redusa va fi reordonata conform pasului I.
5. Sursa redusa de 2 elemente la care s-a ajuns va trebui codificata cu un cod optim (binar) astfel incat primul eveniment va fi codificat cu simbolul 0 iar al doilea va fi codificat cu simbolul 1.
   Se aplica procedura de parcurgere in sens invers reducerilor urmarind similar cu parcurgerea unui graf arborescent identificarea fiecarui element din sursa redusa de ordinul inferior. Se transfera codificarea pentru elementele din $A^{(N-2)}$ la sursa $A^{(N-3)}$ cu adaugarea unui simbol suplimentar la fel ca ala bifurcarea radacinii in graful arborescent pentru elementele care contribuie la reuniunea de doua elemente.
6. Se procedeaza uin mod similar pana cand vom ajunge la reprezentarea eveniomentelor din sursa initiala transferand succesiv codurile de reprezentare a evenimentelor la sursele reduse de ordin inferior dupa procedura descrisa.

I.1.8 Canale de transmisiuni

Orice dispozitiv sau mediu prin care se transmit semnale de la emitator la receptor se numeste canal de transmisiune.

Orice sistem de transmisiune are un canal de transmisiuni.



,unde :

- multimea semnalelor de intrare : $X = \{x_{1,\dots\dots}x_n\}$
- multimea semnalelor de iesire : $Y = \{y_{1,\dots\dots}y_m\}$
- multimea probabilitatilor conditionate : $P = \{p(y_k / x_j) \mid x_j \in X, y_k \in Y\}$

Clasificarea canalelor :

• canale stationare (probabilitatile de tranzitie nu se schimba in timp)
• canale cu memorie (valorile probabilitatilor de trecere depind de evenimentele anterioare)
• canale variabile in timp (valorile probabilitatilor de trecere depind de timpul de observatie)

Procesul de tranzitie poate fi caracterizat prin 2 marimi :

• numarul mediu de simboluri binare pe secunda pe care canalul le transmite de la intrare la iesire
• probabilitatea erorii pe simbol

Teorema lui Shannon : Pentru orice canal cu memorie finita se poate determina o marime notata cu C, numita capacitatea de transmisie a canalului astfel incat, pentru orice viteza R<C, probabilitatea erorii pe simbol poate sa fie facuta oricat de mica printr-o constructie corespunzatoare a coderului, decoderului si a canalului.

I.2 Proiectarea sursei informationale

Pentru proiectarea sursei informationale am ales un text format din N= 15182 de caractere. Astfel, numarul de caractere distincte din alfabetul sursei va fi L=28 de caractere.

Dupa efectuarea calculului probabilitatilor de aparitie a fiecarui caracter, putem realiza modelul probabilistic al sursei:

Caracter a_i	**Probabilitate de aparitie** $P(a_i)$
.	0.00738
Spatiu	0.14484
A	0.10414
B	0.00850

C	0.03965
D	0.02661
E	0.10954
F	0.01317
G	0.00863
H	0.00178
I	0.09077
J	0.00099
K	0.00020
L	0.04018
M	0.02286
N	0.04986
O	0.04321
P	0.02602
Q	0.00007
R	0.06066
S	0.03886
T	0.06126
U	0.04512
V	0.00922
W	0.00007
X	0.00329
Y	0.00013
Z	0.04301

Astfel, putem afla entropia alfabetului sursei informationale cu urmatoarea formula:

$$H(A) = \sum_{i=1}^{28} p(a_i) \cdot \log \frac{1}{p(a_i)} \quad \rightarrow$$

H(A)= 4.03536 [biti/caracter]

Aplicand metoda de codificare Huffman obtinem urmatoarele cuvinte de cod:

Caracter	**Cuvant de cod**
.	0011110
Spatiu	010

A	101
B	0011101
C	00101
D	11000
E	100
F	0000010
G	0011100
H	001111110
I	111
J	0011111110
K	00111111111
L	00100
M	000000
N	1101
O	00010
P	11001
Q	0011111111010
R	0111
S	00110
T	0110
U	00001
V	0000011
W	0011111111011
X	00111110
Y	001111111100
Z	00011

Verificarea primei teoreme a lui Shannon consta in verificarea relatiei:

$$\frac{H(A)}{\log M} \le \bar{l} < \frac{H(A)}{\log M} + 1$$

,unde:

- H(A) = 4.0354 [biti/caracter]
- M = 2 (folosim un cod binar)
- $\bar{l}$ = 4.0714
- eficienta = 0.9911
- redundanta = 0.0088

Din cele de mai sus rezulta ca $4.0354 \leq 4.0714 \leq 5.0354$ =>

Teorema I a lui Shannon este verificata !!!

II. TEORIA CODURILOR

II.1 NOTIUNI TEORETICE

Pentru proiectarea coderului de canal am folosit codul Reed-Muller deoarece satisface conditiile impuse de proiect.

Consideram V_n un spatiu vectorial peste GF(2), n-dimensional. Totodata consideram $u=(a_1,a_2,a_3,\ldots,a_n)$ si $v=(b_1,b_2,b_3,\ldots,b_n)$, pe spatiul vectorial V_n ; prin urmare se pot defini:

- produsul vectorial $uxV=(a_1*b_1, a_2*b_2,\ldots a_n*b_n)$
- produsul scalar $\vec{u}*\vec{V}=\sum a_i \bullet b_i$ si $\vec{u}*\vec{V} \in GF(2)$.

Produsul scalar este nul daca ponderea produsului vectorial este un numar par iar multimea vectorilor de n elemente formeaza o algebra liniara, asociativa si comutativa.

In cadrul codului Reed-Muller se definesc :

- $n=2^m$, unde *n* este dimensiunea vectorilor cuvintelor de cod
- $k=\sum_{k=0}^{r} C_n^{\,k}$, unde *k* este numarul de simboluri din cod
- $d=2^{m-r}$, unde *d* este distanta minima

- $n-k=1+C_m^1+C_m^2+...+C_m^{n-r-1}$, pentru codul RM(m,r)
- $t=\left[\frac{d-1}{2}\right]$ unde *t* este numarul de erori pe care le poate corecta codul RM(m,r)

Prototipul codului Reed-Muller :

Vectorii care alcatuiesc matricea generatoare sunt urmatorii:

V_0=1111 1111 1111 1111

V_m=0000 0000 0000 1111

V_{m-1}=0000 1111 0000 1111

V_m x V_{m-1}= .....

.....

V_r x V_{r-1} x V_1= .....

In cadrul programului pe care l-am elaborat am folosit codul Reed-Muller (5,2).

RM(5,2):

m=5;

r=2;

$n=2^m=32$

$k=\sum_{k=0}^{2} C_5^k=16$

$d=2^{m-r}=8$

$t=\left[\frac{d-1}{2}\right]=3$ =>capacitatea de corectie a codului este de 3 erori.

Matricea generatoare a acestuia este urmatoarea :

G=	1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	v_0
	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	v_5
	0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1	v_4
	0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1	v_3
	0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1	v_2
	0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1	v_1
	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1	v_{54}
	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0	v_{53}

0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1 v_{52}

0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1 v_{51}

0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1 v_{43}

0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1 v_{42}

0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1 v_{41}

0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,1 v_{32}

0,0,0,0,0,1,0,1,0,0,0,0,0,1,0,1,0,0,0,0,0,1,1,1,0,0,0,0,0,1,0,1 v_{31}

0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,1 v_{21}

Liniile matricii au cate 32 de simboluri binare, dar partea a doua a matricii pare a avea mai multe.

Procesul codificarii in cazul codului R-M poate fi descries prin acelasi produs matricial de tipul $\overrightarrow{X} = \overrightarrow{m} x G$.

Vectorul mesaj are forma :

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

Algoritmul de decodificare presupune scrierea relatiilor de control, fiecare componenta a mesajului informational va fi definita cu ajutorul unui set de relatii de control.

Acest set de relatii de control se scrie pentru fiecare componenta in parte a mesajului informational intr-un mod particular tinandu-se cont de vectorul liniar independent din interiorul matricii generatoare care ii corespunde acestei componenete.

In functie de numarul de componenete diferite de 0 din vectorul respectiv se vor scrie in acelasi numar relatii de control in setul amintit.

Intotdeauna se va scrie setul de relatii de control incepand cu ultima componenta informationala a mesajului.

Relatiile de control pentru codul RM(5,2) sunt urmatoarele:

Calculul lui a_{21}:

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

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

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

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

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

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

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

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

Calculul lui a_{31}:

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

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

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

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

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

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

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

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

Calculul lui a_{32}:

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

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

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

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

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

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

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

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

Calculul lui a_{41}:

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

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

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

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

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

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

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

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

Calculul lui a_{42}:

$$a_{42} = y_0 \oplus y_2 \oplus y_8 \oplus y_{10}$$

$$a_{42} = y_1 \oplus y_3 \oplus y_9 \oplus y_{11}$$

$$a_{42} = y_4 \oplus y_6 \oplus y_{12} \oplus y_{14}$$

$$a_{42} = y_5 \oplus y_7 \oplus y_{13} \oplus y_{15}$$

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

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

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

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

Calculul lui a_{43}:

$$a_{43} = y_0 \oplus y_4 \oplus y_8 \oplus y_{12}$$

$$a_{43} = y_1 \oplus y_5 \oplus y_9 \oplus y_{13}$$

$$a_{43} = y_2 \oplus y_6 \oplus y_{10} \oplus y_{14}$$

$$a_{43} = y_3 \oplus y_7 \oplus y_{11} \oplus y_{15}$$

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

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

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

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

Calculul lui a_{51}:

$$a_{51} = y_0 \oplus y_1 \oplus y_{16} \oplus y_{17}$$

$$a_{51} = y_2 \oplus y_3 \oplus y_{18} \oplus y_{19}$$

$$a_{51} = y_4 \oplus y_5 \oplus y_{20} \oplus y_{21}$$

$$a_{51} = y_6 \oplus y_7 \oplus y_{22} \oplus y_{23}$$

$$a_{51} = y_8 \oplus y_9 \oplus y_{24} \oplus y_{25}$$

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

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

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

Calculul lui a_{52}:

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

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

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

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

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

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

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

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

Calculul lui a_{53}:

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

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

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

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

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

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

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

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

Calculul lui a_{54}:

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

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

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

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

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

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

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

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

Apoi se calculeaza y':

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

Din y' se calculeaza apoi : a_1, a_2, a_3, a_4, a_5;

Se calculeaza a_1:

$$a_1 = y_0 \oplus y_1$$

$$a_1 = y_2 \oplus y_3$$

$$a_1 = y_4 \oplus y_5$$

$$a_1 = y_6 \oplus y_7$$

$$a_1 = y_8 \oplus y_9$$

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

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

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

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

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

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

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

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

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

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

Se calculeaza a_2:

$$a_2 = y_0 \oplus y_2$$

$$a_2 = y_1 \oplus y_3$$

$$a_2 = y_4 \oplus y_6$$

$$a_2 = y_5 \oplus y_7$$

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

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

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

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

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

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

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

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

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

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

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

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

Se calculeaza apoi a_3:

$$a_3 = y_0 + y_4$$
$$a_3 = y_1 + y_5$$
$$a_3 = y_2 + y_6$$
$$a_3 = y_3 + y_7$$
$$a_3 = y_8 + y_{12}$$
$$a_3 = y_9 + y_{13}$$
$$a_3 = y_{10} + y_{14}$$
$$a_3 = y_{11} + y_{15}$$
$$a_3 = y_{16} + y_{20}$$
$$a_3 = y_{17} + y_{21}$$
$$a_3 = y_{18} + y_{22}$$
$$a_3 = y_{19} + y_{23}$$
$$a_3 = y_{24} + y_{28}$$
$$a_3 = y_{25} + y_{29}$$
$$a_3 = y_{26} + y_{30}$$
$$a_3 = y_{27} + y_{31}$$

Se calculeaza apoi a_4:

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

Se calculeaza apoi a_5:

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

Observatie:

Dupa calcularea relatiilor de control vectorul "a" se calculeaza conform **principiului logicii majoritate**: adica se compara de cate ori elementul calculat ia valoarea 1 respectiv 0 se compara si elementul primeste valoarea care are ponderea cea mai mare.

Se calculeaza apoi y'':

$$Y'' = y' - (a_4 * V_4 + a_3 * V_3 + a_2 * V_2 + a_1 * V_1);$$

Elementele calculate se trec in vectorul **a** unde vectorul a reprezinta mesajul informational trimis de coderul de sursa.