Capitolul 4
"Codarea surselor pentru canale cu perturbații"

M. Ivanovici

octombrie 2008

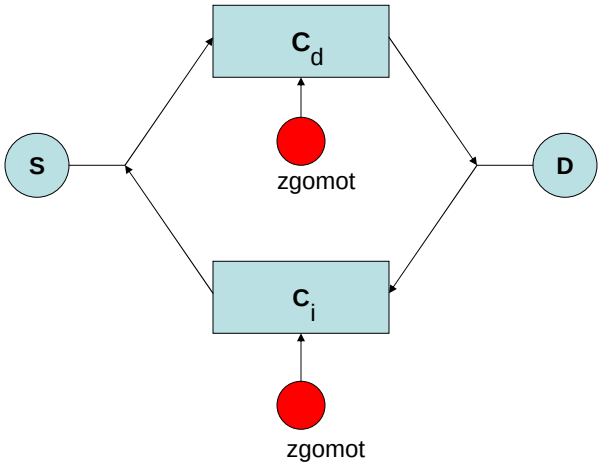
1

4.1 Introducere

- Fie o sursă de entropie maximă, care generează **simboluri de informație**, având aceeaşi probabilitate
- Înainte de a fi transmise pe canal, se introduce o anumită redundanță prin adăugarea unor **simboluri de control** ce au menirea de a indica utilizatorului prezența erorilor (cauzate de zgomotul de pe canal) sau chiar de a le corecta

2

- În cazul detecţiei erorilor este necesar un canal de întoarcere



3

- Cantitatea necesară solicitării retransmisiei este foarte mică (Ex. TCP: 1518 B pachetul de date, 64 B pachetul de acknowledgement)
- Capacitatea canalului invers este de regulă foarte mică
- ARQ (Automatic Repetition Request) este larg utilizat pentru sursele cu debit controlabil

4

4.2 Clasificare

- **Coduri bloc** – prelucrările necesare pentru a realiza detecția și corecția se realizează pe blocuri de *n* simboluri (pe cuvinte)
- **Coduri convoluționale** – prelucrarea cuvintelor generate de sursă se face în mod continuu, nu pe blocuri

5

Coduri bloc

- **Coduri grup**: cuvintele de cod reprezintă elemente ale unui spațiu vectorial
- **Coduri ciclice**: cuvintele de cod sunt elemente dintr-o algebră

6

4.3 Teorema lui Shannon pentru canale cu perturbații

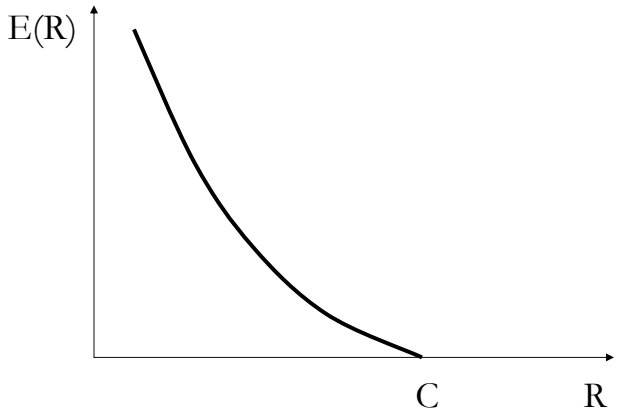
- Dacă avem o sursă cu un debit de informație R biți/s și un canal de capacitate C biți/s și dacă $R < C$ atunci există un cod cu cuvinte de lungime n astfel încât probabilitatea unei erori de decodare P_E să fie:

$$P_E \leq 2^{-nE(R)}$$

Unde n este lungimea cuvântului de cod, iar $E(R)$ este o funcție nenegativă numită "exponentul erorii"

7

Exponentul erorii



8

- Teorema afirmă existența unor coduri a căror probabilitate de decodare eronată este arbitrar de mică, dar nu arată cum pot fi construite astfel de coduri
- Indiferent de nivelul zgomotului dintr-un canal, se pot face transmisiuni cu o probabilitate a erorii oricât de mică

9

4.4 Coduri grup

- Sunt coduri bloc în care cele *n* simboluri care formează un cuvânt sunt considerate ca fiind componentele unui vector *n* dimensional
- Spațiul vectorial are o structură de grup
- Componentele unui cuvânt vor fi:

$$w = [a_1\ a_2\ ...\ a_n]$$

- În cazul unui cod binar, elementele a_i sunt elementele unui câmp GF(2) cu 2 elemente (0,1)

10

Regulile de operare ale GF(2)

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

GF = Galois Field (câmp Galois)

11

Specificarea cuvintelor cu sens

- W = mulțimea tuturor cuvintelor;

  $card\ W = N = 2^n$

- V = mulțimea cuvintelor cu sens;

  $card\ V = S = 2^k$

- Dacă atribuim sens tuturor cuvintelor, respectiv: $I = log\ N = n$, iar informația medie pe simbol:

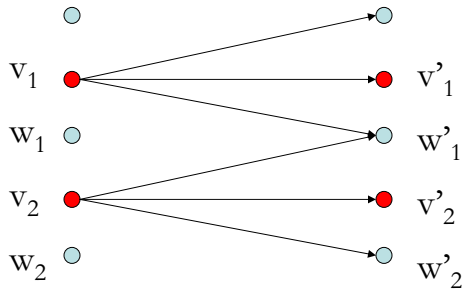
  $i_n = I/n = 1$ bit (valoare maximă)

12

- Dacă toate cuvintele sunt cuvinte de cod, nu există posibilitatea de a detecta sau corecta erorile ce apar în procesul de transmisiune prin canal: *prin modificarea de către zgomot a unui simbol dintr-un cuvânt de cod se obţine tot un cuvânt de cod*
- Pentru a putea detecta erorile se procedează după cum urmează:
  - Mulţimea W a cuvintelor se împarte în două submulţimi V şi F
  - Tuturor cuvintelor v_i din V li se atribuie sens

13

  - Numărul cuvintelor cu sens este $S = 2^k$, unde $k < n$ este un număr întreg
  - Cuvintelor w_i din mulţimea F, nu li se atribuie sens (nu conţin informaţie)



14

- Informaţia medie transmisă cu un cuvânt de cod este în acest caz:

$$I = \log S = k$$

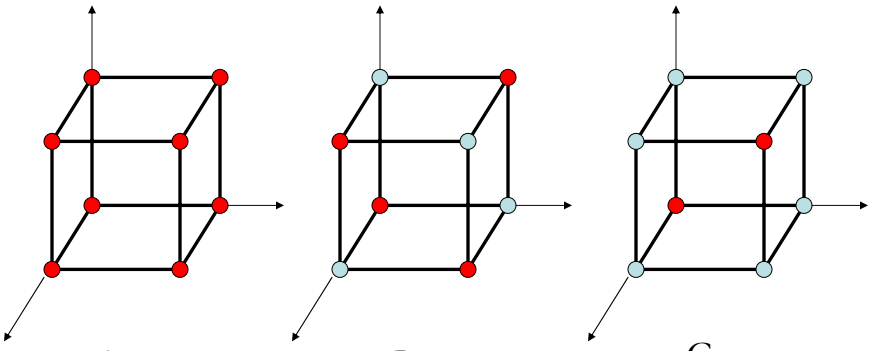
- Iar informaţia medie pe simbol este:

$$i_k = k / n$$

mai mică decât 1 bit.

15

- Ilustrarea geometrică a alegerii cuvintelor de cod pentru cazul $n = 3$ simboluri.



16

- **A**: toate cuvintele ce se pot forma sunt cuvinte de cod ($N = 2^3 = 8$); apariția unei erori nu poate fi detectată
- **B**: se aleg $S = 2^2 = 4$ cuvinte de cod; apariția unei erori conduce la un cuvânt fără sens, deoarece se modifică doar o coordonată. Se poate astfel detecta o eroare, fără posibilitatea de a o corecta
- **C**: se aleg $S = 2^1 = 2$ cuvinte de cod; apariția unei erori poate fi detectată si eroarea corectată

17

- Cuvintele de cod:

  $v_i = [\, a_{i1}\ a_{i2} \ldots a_{in} \,]$
- Cuvintele recepționate:

  $v'_i = [\, a'_{i1}\ a'_{i2} \ldots a'_{in} \,]$
- Dacă $v'_i = v_i$, respectiv $a'_{i1} = a_{i1}$, $a'_{i2} = a_{i2}$, ..., $a'_{in} = a_{in}$ se spune că transmisiunea s-a efectuat fără eroare

18

Cuvântul eroare

- Acțiunea zgomotului poate fi modelată printr-un operator aleator *P* care face transformarea de la spațiul cuvintelor v_i la spațiul cuvintelor recepționate v'_i:

$$P\{v_i\} = v'_i$$

- Relația se poate scrie mai simplu dacă se definește un cuvânt eroare, cu simboluri din același alfabet cu cuvintele de cod v_i

$$\varepsilon = [\, \varepsilon_1 \, \varepsilon_2 \ldots \varepsilon_n]$$

19

- În cazul binar, simbolurile ε_i pot lua valori 0 și 1
- Cuvântul eroare mai poate fi scris și sub forma:

$$\varepsilon = [\ldots \alpha_{i1} \ldots \alpha_{ie} \ldots]$$

unde simbolurile $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ie}$ sunt simboluri 1, celelalte simboluri fiind zero; iar indicii i_1, i_2 arată poziția în care apare o eroare

- Relația ce definește operatorul *P* devine:

$$P\{v_i\} = v_i + \varepsilon = v'_i$$

Unde semnul + indică adunare modulo 2

- Transformarea inversă: $v_i = P^{-1}\{v_i\} = v'_i + \varepsilon$

20

$v_i = [\, a_{i1}\ a_{i2} \ldots a_{in} \,]$

$v'_i = [\, a'_{i1}\ a'_{i2} \ldots a'_{in} \,]$

$a'_{i1} = a_{i1} + \varepsilon_1$ $\qquad$ $a_{i1} = a'_{i1} + \varepsilon_1$

$a'_{i2} = a_{i2} + \varepsilon_2$ $\qquad$ $a_{i2} = a'_{i2} + \varepsilon_2$

..... $\qquad$ .....

$a'_{in} = a_{in} + \varepsilon_n$ $\qquad$ $a_{in} = a'_{in} + \varepsilon_n$

21

Mecanismul de detecție și de corecție a erorilor

- Se consideră un spațiu *m*-dimensional ($m = n - k$) numit *spaţiul de corecţie* *Z*, cu 2^m elemente z din *Z*, numite *corectori*
- Corectorul se mai numește și *vector de control de paritate* sau *sindrom*
- Corectorii au menirea de a indica pozițiile din cuvântul de cod în care care s-au introdus erori

22

- Astfel, se stabileşte o corespondenţă univocă între mulţimea tuturor cuvintelor recepţionate (spaţiul *W*) şi mulţimea corectorilor (spaţiul *Z*), definind operatorul *H*:

$$H\{v'_i\} = z$$

Unde $v'_i \in W$ şi $z \in Z$

- Dacă $v'_i = v_i$, transmisiunea s-a efectuat fără erori, z trebuie să fie acelaşi pentru orice *i*, indicând astfel că nu sunt erori: se alege pt. z valoarea *0*:

$$H\{v_i\} = 0 \text{ , v } i \text{ de la 1 la } S=2^k$$

23

- Se impune astfel, operatorului *H* condiţia ca $H\{v'_i\} = 0$, respectiv $z = 0$, dacă şi numai dacă v'_i este un cuvânt de cod, respectiv $v'_i = v_i$
- *Pentru a putea corecta erorile este necesar ca pentru fiecare cuvânt de eroare care poate apărea din cauza zgomotului să existe un singur corector distinct diferit de zero*
- Dacă $H\{v'_i\} \neq 0$ dar nu se cunoaşte z – detecţie
- Dacă $H\{v'_i\} = z$ se poate determina cuvântul de eroare ε – detecţie + corecţie

24

Matricea de corecție (control)

- Cea mai simplă structură pentru operatorul H se obține dacă se consideră o transformare liniară de la spațiul cuvintelor recepționate, la spațiul corectorilor, definită de ecuațiile:

$$h_{11}\, a'_1 + h_{12}\, a'_2 + \ldots + h_{1n}\, a'_n = c_1$$
$$h_{21}\, a'_1 + h_{22}\, a'_2 + \ldots + h_{2n}\, a'_n = c_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$h_{m1}\, a'_1 + h_{m2}\, a'_2 + \ldots + h_{mn}\, a'_n = c_m$$

unde h_{ij} sunt parametrii care determină transformarea H, a_i simbolurile unui cuvânt recepționat, c_i coordonatele care determină punctul z (componentele corectorului z)

25

- Matricea **H** se numește **matrice de control**:

$$H = \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} & \ldots & h_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ h_{m1} & h_{m2} & \ldots & h_{mn} \end{bmatrix}$$

26

Matricea **H** poate fi scrisă sub forma următoare

$$H = \begin{bmatrix} 1 & 0 & \dots & 0 & q_{11} & q_{12} & \dots & q_{1k} \\ 0 & 1 & \dots & 0 & q_{21} & q_{22} & \dots & q_{2k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & q_{m1} & q_{m2} & \dots & q_{mk} \end{bmatrix} = \begin{bmatrix} I_m Q \end{bmatrix}$$

unde I_m este matricea unitate de ordinul m
Iar Q este:

27

$$Q = \begin{bmatrix} q_{11} & q_{12} & \dots & q_{1k} \\ q_{21} & q_{22} & \dots & q_{2k} \\ \dots & \dots & \dots & \dots \\ q_{m1} & q_{m2} & \dots & q_{mk} \end{bmatrix}$$

Cu notațiile de până acum:

$$v'_i = [\, a'_{i1}\ a'_{i2} \dots a'_{in} \,] \qquad z = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix}$$

28

$$H \cdot v'^T = z$$

Dacă cuvântul recepţionat este un cuvânt de cod

$$v' = v$$

Corectorul este nul:

$$H \cdot v'^T = 0$$

29

Codarea codurilor grup cu ajutorul matricei de control **H**

- În cele ce urmează vom conveni că în cuvântul de cod:

  $v = [\, a_1 \ldots a_m \, a_{m+1} \ldots a_n \,]$

  primele m simboluri:

  $c = [\, a_1 \, a_2 \ldots a_m \,]$

  să fie simboluri redundante care servesc detecţiei sau corecţiei de erori (**simboluri de control**),

  iar ultimele k simboluri:

30

$i = [\, a_{m+1}\, a_{m+2} \ldots a_{m+k}\,]$, *unde* $m + k = n$

să fie simboluri generate de sursă (**simboluri de informație**)

Forma cuvintelor de cod: $v = [\boldsymbol{c}\, \boldsymbol{i}]$

Pentru a determina cele m simboluri de control în funcție de cele k simboluri de informație:

$$\boldsymbol{H}\, v^T = 0$$

31