CAPITOLUL 6

CODURI BLOC

6.1. PRINCIPIUL CODĂRII BLOC

Pentru a transmite informaţie la distanţă, se utilizează canale de comunicaţie, construite prin exploatarea mediilor de propagare a undelor de diverse naturi (acustice, electrice, electromagnetice, optice). Undele pot fi ghidate (în cabluri electrice, fibră optică, radiorelee) sau se propagă liber (în aer, vidul cosmic, apele oceanelor).

Parametrii cheie de care dispune proiectantul unui sistem digital de comunicaţie sunt *puterea de emisie a semnalului* şi *lărgimea de bandă a canalului*. Orice canal, însă, este afectat de zgomot, care poate face ca, din când în când, receptorul să ia decizii greşite cu privire la adevăratul simbol transmis. Un canal de comunicaţie se caracterizează printr-o rată a erorilor, definită ca raport dintre numărul de biţi detectaţi greşit de receptor şi numărul total de biţi recepţionaţi. Pentru un canal de comunicaţie utilizabil, rata erorilor de bit trebuie să fie mică.

Teorema codării unui canal demonstrată de Shannon ne spune că, dacă un canal discret fără memorie are o capacitate C iar o sursă generează informaţie la o viteză mai mică decât C, există o tehnică de codare astfel încât semnalul de la ieşirea sursei poate fi transmis pe canal cu o probabilitate arbitrar de mică a erorii de simbol. Teorema codării canal pune deci o limită fundamentală a vitezei cu care se poate transmite fiabil pe un canal dat, şi anume, C. Ea însă nu ne spune şi cum putem face aceasta. Cu timpul, s-a dezvoltat o teorie vastă a codurilor detectoare şi corectoare de erori, teorie care, deşi a atins deja un înalt nivel de maturitate, continuă să fie îmbogăţită cu noi şi noi contribuţii ale specialiştilor din întreaga lume.

O subclasă importantă a codurilor detectoare şi corectoare de erori grupează *codurile bloc*. Pentru simplitate, dacă nu se precizează altfel, simbolurile sunt binare şi le numim *biţi*. Sursa emite un bit la fiecare T_b secunde. Canalul este binar simetric, adică, sursa emite un şir aleator de 0 şi 1, iar receptorul dă la ieşire un şir corespunzător de 0 şi 1, aceasta însă, cu o probabilitate de eroare p. Numim *probabilitate de tranziţie* probabilitatea ca, datorită zgomotului, receptorul să transforme un 1 în 0 sau un 0 în 1. Diagrama probabilităţii de tranziţie a unui canal binar simetric este arătată în figura 6.1.

Este clar că, dacă nu luăm anumite măsuri de prevedere, orice eroare de bit rămâne nedetectată. Pentru a mări şansele ca receptorul să decidă corect, împărţim şirul biţilor de emisie în blocuri de câte k biţi, numiţi biţi de mesaj, iar la aceştia adăugăm $n–k$ biţi redundanţi, legaţi algebric de cei k biţi de mesaj, rezultând blocuri de n biţi numite *cuvinte de cod*. Codul bloc este setul celor 2^k cuvinte de cod. Lungimea cuvântului de cod fiind n, există 2^n blocuri de n biţi, dintre care numai $2^k < 2^n$ sunt cuvinte de cod. Dacă receptorul constată că blocul de n biţi nu este cuvânt de cod, interpretează aceasta ca indiciu că s-a produs o eroare: spunem că *detectează* eroarea. Un cod bloc bine proiectat este înzestrat şi cu o oarecare capacitate de *a corecta* erorile. Rata codului: $R = k/n$ determină volumul redundanţei.

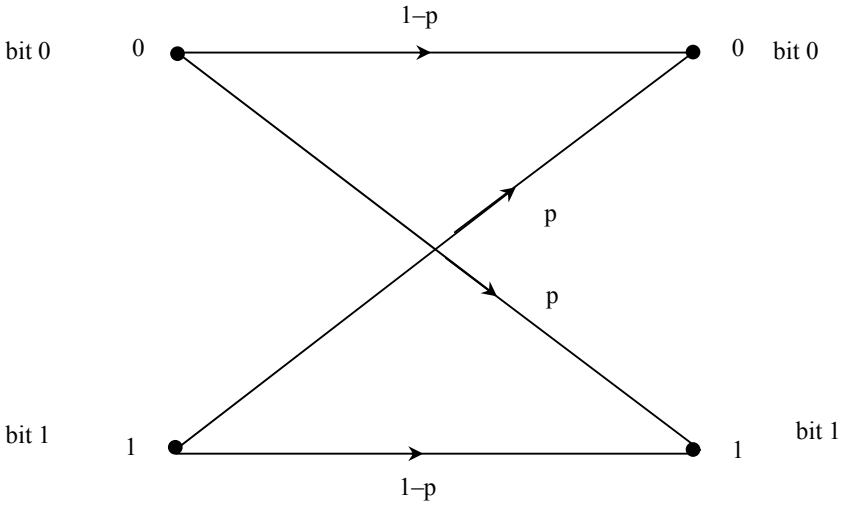

Fig. 6.1. Diagrama probabilităţii de tranziţie a unui canal binar simetric.

Codurile bloc pot fi *liniare* şi *neliniare*, după cum biţii redundanţi sunt sau nu combinaţii liniare de biţii de mesaj. Toate codurile bloc pe care le studiem în continuare sunt liniare.

6.2. CODURI BLOC LINIARE

Prin definiţie, un cod bloc de lungime n compus din 2^k cuvinte se numeşte cod liniar (n,k) dacă şi numai dacă cele 2^k cuvinte de cod formează un subspaţiu k-dimensional al spaţiului vectorial al tuturor n–tuplurilor cu elemente din corpul Galois $CG(2)$.

Este bine să ne reamintim definiţia *spaţiului vectorial*. Un spaţiu vectorial V este o mulţime de elemente numite *vectori* împreună cu două operaţii, una *internă*, numită *adunare vectorială*, şi o alta *externă*, numită *înmulţire* cu scalari dintr-un corp S. Spaţiul vectorial are structură algebrică de *grup* pentru adunarea vectorială, elementul neutru fiind notat cu **0**. Scalarii din S au un element neutru pentru adunare notat cu 0 şi un element neutru pentru înmulţire notat cu 1. Trebuie ca $1 \cdot \mathbf{v} = \mathbf{v}$ pentru orice $\mathbf{v} \in V$. Un spaţiu vectorial este n-dimensional dacă el conţine un set de n vectori liniar independenţi şi dacă orice set de $(n + 1)$ vectori este liniar dependent.

Orice astfel de set de n vectori liniar independenţi constituie o *bază* a spaţiului vectorial pe care se spune că îl *generează*, în sensul că orice vector din V se poate scrie ca o combinaţie liniară de vectorii bazei. Baza nu este unică.

Un set de $k < n$ vectori liniari independenţi generează un subspaţiu vectorial k-dimensional al spaţiului vectorial n-dimensional. Să aplicăm această proprietate în cazul unui cod bloc liniar. Este deci posibil să găsim k cuvinte de cod liniar independente $\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}$ astfel încât fiecare cuvânt de cod **v** să fie o combinaţie liniară a acestora:

$$\mathbf{v} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots + u_{k-1}\mathbf{g}_{k-1} \tag{6.1}$$

unde $u_i = 0$ sau 1 pentru $0 \le i \le k-1$.

Aranjăm cele k cuvinte de cod liniar indepentente ca linii ale unei matrice $k \times n$ după cum urmează:

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ . \\ . \\ . \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots g_{1,n-1} \\ . & & & \\ . & & & \\ . & & & \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots g_{k-1,n-1} \end{bmatrix} \tag{6.2}$$

unde $\mathbf{g}_i = (g_{i0}, g_{i1}, \cdots, g_{i,n-1})$ pentru $0 \le i \le k-1$.

Să scriem blocul celor k biți de mesaj ca vector linie $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$. Este clar că putem scrie cuvântul de cod corespunzător **v** după cum urmează:

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G} = (u_0, u_1, \cdots, u_{k-1}) \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ . \\ . \\ . \\ \mathbf{g}_{k-1} \end{bmatrix} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots + u_{k-1}\mathbf{g}_{k-1}. \tag{6.3}$$

Să observăm că, impunând codului bloc proprietatea de liniaritate, am obținut o simplificare considerabilă a procesului de codare. Într-adevăr, pentru un cod bloc neliniar, aplicația bijectivă a mulțimii mesajelor în mulțimea cuvintelor de cod trebuie dată cu ajutorul a ceea ce numim o *carte de cod*, care nu este nimic altceva decât lista completă a celor 2^k perechi mesaj-cuvânt de cod. Condiția de liniaritate reduce memoria necesară la numai k cuvinte de cod care sunt liniile matricei generatoare **G**. Precizăm că matricea generatoare **G** a unui cod dat nu este unică, întrucât orice alt set de k cuvinte de cod liniar independente poate servi aceluiaşi scop. O simplificare şi mai mare a procesului de codare se realizează înzestrând codul bloc liniar cu *structura sistematică* a cuvintelor de cod, în care un cuvânt de cod se compune din două părți, partea de mesaj şi partea redundantă de control.

Să notăm cu $c_0, c_1, \cdots, c_{n-k-1}$ cei $(n-k)$ biți de control. Adoptăm convenția că primul bit emis în timp dintr-un bloc este cel mai din dreapta. Cu aceasta, structura unui cuvânt de cod sistematic este cea arătată în figura 6.2. Este normal ca biții de mesaj să fie transmişi înaintea celor de control al parității, dar unii autori utilizează opțiunea inversă.

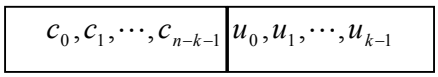

Fig. 6.2. Structura unui cuvânt de cod sistematic.

Acest format permite extragerea directă a mesajului din cuvântul de cod. Matricea generatoare pentru un cod bloc sistematic are forma următoare:

$$\mathbf{G} = \left[\mathbf{P} \quad \mathbf{I}_k\right] \tag{6.4}$$

unde $\mathbf{I}_k$ este matricea identitate $k \times k$ iar $\mathbf{P}$ este o matrice $k \times (n-k)$ de forma

$$\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} & \cdots p_{0,n-k-1} \\ p_{10} & p_{11} & \cdots p_{1,n-k-1} \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ p_{k-1,0} & p_{k-1,1} & \cdots p_{k-1,n-k-1} \end{bmatrix} \tag{6.5}$$

unde $p_{ij} = 0$ sau 1.

Relaţia dintre mesajul $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ şi cuvântul de cod corespunzător este:

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G} \tag{6.6}$$

În conformitate cu (6.4) şi (6.5), componentele lui **v** sunt:

$$v_{n-k+i} = u_i \quad \text{pentru} \quad 0 \le i \le k-1 \tag{6.7a}$$

şi

$$v_j = u_0 p_{0j} + u_1 p_{1j} + \cdots + u_{k-1} p_{k-1,j} \quad \text{pentru} \quad 0 \le j \le n-k-1 . \tag{6.7b}$$

Se constată că, impunându-se unui cod bloc liniar condiţia de a fi sistematic, dimensiunea matricei pe care trebuie să o memoreze generatorul de cod se reduce de la $k \times n$ la $k \times (n-k)$, un avantaj deloc neglijabil.

Vom introduce acum o altă matrice importantă, şi anume, matricea de control al parităţii **H**. Se ştie de la teoria spaţiilor vectoriale că, pentru

orice matrice generatoare $k \times n$, notată cu **G**, cu cele k linii liniar independente, există o matrice $(n-k)\times n$, notată cu **H**, cu cele $(n-k)$ linii liniar independente, astfel încât orice vector din spațiul generat de liniile lui **G** este ortogonal cu liniile lui **H**, iar orice vector care este ortogonal cu liniile lui **H** se găseşte în spațiul generat de liniile lui **G**. Putem, deci, descrie codul liniar (n,k) generat de **G** şi în modul următor: un n-tuplu **v** este un cuvânt de cod din codul bloc generat de **G** dacă şi numai dacă

$$\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}. \tag{6.8}$$

Cele 2^{n-k} combinații liniare ale liniilor matricei **H** formează un cod bloc liniar $(n, n-k)$, notat cu V_d şi numit codul dual al lui V. Codul dual V_d este spațiul nul al codului bloc liniar V generat de matricea **G**, adică, pentru orice $\mathbf{v} \in V$ şi orice $\mathbf{w} \in V_d$, $\mathbf{v} \cdot \mathbf{w} = 0$. Prin urmare, o matrice de control pentru codul bloc liniar V este o matrice generatoare pentru codul dual V_d.

Pentru un cod sistematic, a cărui matrice generatoare are forma (6.4), matricea de control se poate scrie:

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \quad \mathbf{P}^T\right] \tag{6.9}$$

unde $\mathbf{P}^T$ este transpusa matricei **P**, iar $\mathbf{I}_{n-k}$ este matricea identitate $(n-k)\times(n-k)$.

Matricea transpusă a lui **H** se scrie:

$$\mathbf{H}^T = \begin{bmatrix} \mathbf{I}_{n-k} \\ \mathbf{P} \end{bmatrix}. \tag{6.10}$$

Fie $\mathbf{h}_j$ linia j a lui **H**, $0 \le j \le n-k-1$:

$$\mathbf{h}_j = (0,0,\cdots,\underset{i}{1},\cdots,0, p_{0j}, p_{1j}, \cdots, p_{k-1,j}).$$

Fie $\mathbf{g}_i$ linia i a lui **G**, $0 \le i \le k-1$:

$$\mathbf{g}_i = \left(p_{i0}, p_{i1}, \cdots, p_{i,n-k-1}, 0,0,\cdots,\underset{j}{1},\cdots,0 \right).$$

Efectuând produsul scalar, obținem că $\mathbf{g}_i \cdot \mathbf{h}_j = p_{ij} + p_{ij} = 0$. Aceasta implică faptul că

$$\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}. \tag{6.11}$$

Ecuațiile de control date de (6.7b) se pot obține şi cu ajutorul matricei **H**. Fie $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ mesajul de codat. În fomă sistematică,

cuvântul de cod corespunzător **v** va fi $\mathbf{v} = (v_0, v_1, \cdots, v_{n-k-1}, u_0, u_1, \cdots, u_{k-1})$. Utilizând ecuația (6.8), obținem pentru $0 \le j \le n-k-1$:

$$v_j + u_0 p_{0j} + u_1 p_{1j} + \cdots + u_{k-1} p_{k-1,j} = 0 \qquad (6.12)$$

Având în vedere că operațiile se efectuează modulo 2, obținem aceleaşi ecuații de control ca şi în (6.7b). Prin urmare, un cod liniar (*n*,*k*) este specificat complet de matricea sa de control.

EXEMPLUL 6.1: Cod bloc liniar sistematic (7,4)

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Codorul unui cod bloc liniar sistematic (*n*,*k*) se poate realiza cu două registre de deplasare şi cu un număr de porți logice SAU EXCLUSIV. Schema bloc a codorului care generează codul bloc liniar sistematic din exemplul 6.1 este arătată în figura 6.3.

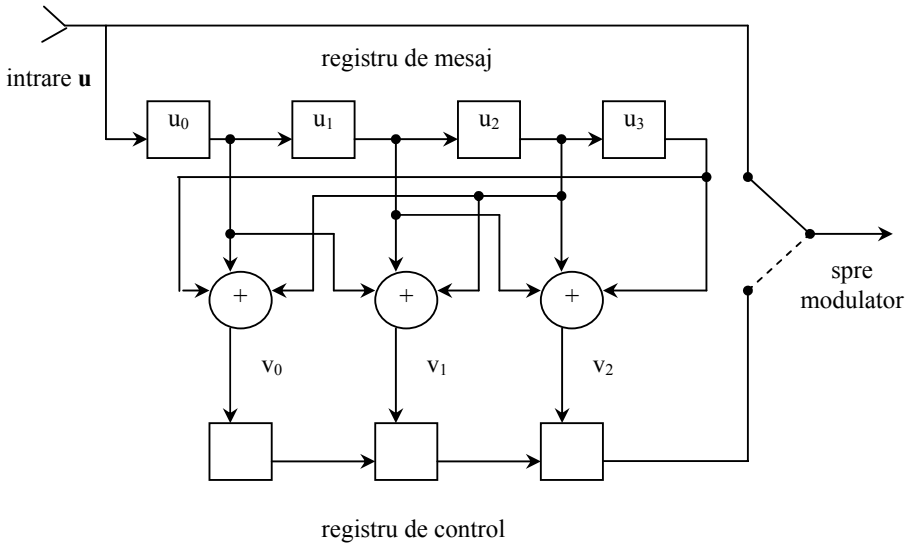

Fig. 6.3. Circuit de codare pentru codul bloc liniar sistematic (7,4) din exemplul 6.1.

Mesajul $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ de codat se deplasează în registrul de mesaj şi, simultan, în modulator, care formează semnalul de emisie în canal. Îndată ce întregul mesaj va fi intrat în registrul de mesaj, la ieşirea celor $(n-k)$ porți logice SAU EXCLUSIV se formează simbolurile de control al parității care sunt înscrise în paralel în registrul de control. Ele sunt apoi serializate şi deplasate în modulator.

Pentru un cod bloc liniar dat, complexitatea circuitului de codare este proporțională cu lungimea blocului *n*.

6.3. STRUCTURA TRELLIS A CODURILOR BLOC LINIARE

Un cod bloc liniar (*n*,*k*) definit pe corpul Galois *CG*(2) este caracterizat de matricea de control al parității **H**

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_i, \cdots, \mathbf{h}_{n-1}] \tag{6.13}$$

unde $\mathbf{h}_i$ este un vector coloană $(n-k)\times 1$. Codul constă din toți vectorii binari

$$\mathbf{v} = (v_0, v_1, \cdots, v_i, \cdots, v_{n-1}), \quad v_i \in CG(2) \tag{6.14}$$

astfel încât

$$\mathbf{v}\mathbf{H}^T = v_0\mathbf{h}_0 + v_1\mathbf{h}_1 + \cdots + v_{n-1}\mathbf{h}_{n-1} = \mathbf{0} \tag{6.15}$$

Este util să caracterizăm codul şi cu ajutorul unui graf orientat numit *trellis*. Nodurile acestui graf se numesc *stări*, iar ramurile se numesc *tranziții de stare*. Un cod (*n*,*k*) poate avea cel mult 2^{n-k} stări, starea fiind un (*n*–*k*)–tuplu notat cu $S_i(l)$, unde numărul natural *l* este *adâncimea* trellisului, iar *i* este un alt număr natural. Stările se ordonează de la 0 la $2^{n-k} - 1$, 0 fiind (*n*–*k*)–tuplul cu toate componentele egale cu 0; pentru o adâncime *l* dată, stările se figurează prin puncte dispuse pe verticală, cel mai sus fiind punctul corespunzător stării 0.

Există un singur nod la adâncimea 0, notat cu $S_0(0)$, şi un singur nod la adâncimea *n*, notat cu $S_0(n)$. Un drum prin trellisul de lungime *L* este un şir de *L* ramuri. Notăm cu I_l mulțimea indicilor nodurilor de la adâncimea *l*; ea este o submulțime a numerelor naturale $\{0, 1, 2, \cdots, 2^{n-k} - 1\}$.

La adâncimea $l = 0$, trellisul nu conține decât un nod, $S_0(0)$, care este $(n–k)$– tuplul având toate componentele egale cu 0.

Pentru fiecare $l = 0, 1, \cdots, (n-1)$, mulțimea stărilor de la adâncimea $(l+1)$ se obține din mulțimea nodurilor de la adâncimea l prin formula:

$$S_m(l+1) = S_i(l) + \alpha_i^j \mathbf{h}_l \tag{6.16}$$

pentru toți $i \in I_l$, $m \in I_{l+1}$ şi $j \in \{0, 1\}$, unde α_i^j sunt intrări binare.

$$\alpha_i^j = \begin{cases} 1 & \text{daca } j = 1 \\ 0 & \text{daca } j = 0 \end{cases} \tag{6.17}$$

Prin urmare, pentru fiecare i din I_l, se formează ramuri, sau tranziții de stare, între nodul $S_i(l)$ şi două noduri de adâncime $(l + 1)$, pentru două valori binare diferite $\alpha_i^j \in \{0,1\}$, conform cu formula (6.16). Fiecare ramură se etichetează cu valoarea corespunzătoare α_i^j.

La adâncimea $l = n$, nodul final, $S_0(n)$, este dat de

$$S_0(n) = S_0(0) + \sum_{i=0}^{n-1} \alpha_i^j \mathbf{h}_i = 0 \tag{6.18}$$

Întrucât atât $S_0(n)$ cât şi $S_0(0)$ sunt stări cu toate componentele egale cu 0, din (6.18) rezultă că

$$\sum_{i=0}^{n-1} \alpha_i^j \mathbf{h}_i = 0 \tag{6.19}$$

Având însă în vedere că orice cuvânt de cod satisface ecuația (6.15), identică, evident, cu ecuația (6.19), rezultă că numai acele α_i^j ce constituie un cuvânt de cod vor forma drumuri prin trellis terminate în starea 0. Aşadar, orice drum valabil prin trellis corespunde unui cuvânt de cod.

Să remarcăm că, prin metoda de construcție din ecuația (6.16), se formează în trellis toate n–tuplurile binare posibile, care sunt în număr de 2^n. Dar numai 2^k dintre acestea sunt cuvinte de cod. Vom elimina, deci, acele noduri de la care nici un drum nu duce la starea 0 de adâncime n, precum şi toate ramurile ce duc la aceste noduri eliminate.

EXEMPLUL 6.2: Pentru codul bloc liniar sistematic (7,4) din exemplul 6.1, se trasează mai întâi diagrama trellis din figura 6.4, utilizând procedura descrisă mai sus. Din aceasta, se elimină toate nodurile care nu au un drum ducând la starea 0 la adâncime $l = n = 7$, precum şi toate ramurile ce duc la nodurile eliminate, rezultând trellisul din figura 6.5.

Fig.6.4. (A4L)

Fig.6.5. (A4L)

6.4. SINDROMUL ŞI DETECȚIA ERORILOR

Fie $\mathrm{v} = (v_0, v_1, \cdots, v_{n-1})$ un cuvânt de cod care a fost transmis serial, bit cu bit, pe un canal zgomotos, utilizându-se o modulație binară (de amplitudine, de frecvență sau de fază). La recepția bitului v_i, pentru $0 \le i \le n-1$, demodulatorul, din cauza zgomotului, produce o mărime r_i care poate lua valori într-un interval continuu, cu alte cuvinte, dacă v_i este un număr întreg, r_i este un număr real. Un alt bloc din receptor decide, conform unei reguli de probabilitate maximă, dacă r_i corespunde unui bit de 0 sau de 1. Decizia poate fi *fermă* sau *suplă*.

Decizia fermă face o alegere tranşantă între 0 şi 1. Decizia suplă ține seama şi de fiabilitatea cu care este ea luată. În acest capitol, considerăm că decizia este fermă, astfel încât, vectorul recepționat $\mathbf{r} = (r_0, r_1, \cdots, r_{n-1})$ are componente binare. Din cauza zgomotului, **r** poate fi diferit de **v**. Definim *vectorul de eroare* **e** drept diferența dintre vectorul recepționat **r** şi cuvântul de cod emis **v** , diferență care, în cazul simbolurilor binare, este totuna cu suma:

$$\mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \cdots, e_{n-1}) \tag{6.20}$$

În cazul unei *erori de transmisie*, $r_i \neq v_i$, astfel încât e_i = 1; dacă decizia este corectă, $r_i = v_i$ şi e_i = 0. Reamintind că simbolurile sunt binare, din (6.20) rezultă că vectorul recepționat **r** este suma vectorială dintre cuvântul de cod emis şi vectorul de eroare:

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \tag{6.21}$$

Dar componentele vectorului **r** nu sunt independente, căci prin codare s-a introdus controlat o redundanță informațională care dă receptorului o şansă de a constata că s-au produs erori. Pentru un cuvânt de cod, este verificată ecuația (6.8). De aceea, la recepționarea unui vector **r**, decodorul calculează următorul (*n*–*k*)–tuplu, numit *sindromul* lui **r**:

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (s_0, s_1, \cdots, s_{n-k-1}) \tag{6.22}$$

Este clar că $\mathbf{s} = \mathbf{0}$ dacă şi numai dacă **r** este un cuvânt de cod; faptul că $\mathbf{s} \neq \mathbf{0}$ este un indiciu clar că **r** nu este un cuvânt de cod şi că, deci, sunt erori. Dacă vectorul de eroare **e** este identic cu un cuvânt de cod diferit de zero, **r** conține erori dar $\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = \mathbf{0}$ astfel că erorile sunt indetectabile. Întrucât există $2^k - 1$ cuvinte de cod diferite de zero, avem toți atâția vectori incluzând erori nedetectabile. Un astfel de vector determină decodorul să facă o *eroare de decodare*.

Să scriem (6.22) desfăşurat:

$$\mathbf{s}=\left(s_0,s_1,\cdots,s_{n-k-1}\right)=$$

$$=\left(r_0,r_1,\cdots,r_{n-1}\right)\begin{bmatrix}1 & 0 & 0 & \cdot & \cdot & \cdot & 0\\ 0 & 1 & 0 & \cdot & \cdot & \cdot & 0\\ 0 & 0 & 1 & \cdot & \cdot & \cdot & 0\\ \cdot & & & & & & \cdot\\ \cdot & & & & & & \cdot\\ \cdot & & & & & & \cdot\\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 1\\ p_{00} & p_{01} & p_{02} & \cdot & \cdot & \cdot & p_{0,n-k-1}\\ p_{10} & p_{11} & p_{12} & \cdot & \cdot & \cdot & p_{1,n-k-1}\\ p_{20} & p_{21} & p_{22} & \cdot & \cdot & \cdot & p_{2,n-k-1}\\ \cdot & & & & & & \cdot\\ \cdot & & & & & & \cdot\\ \cdot & & & & & & \cdot\\ p_{k-1,0} & p_{k-1,1} & p_{k-1,2} & \cdot & \cdot & \cdot & p_{k-1,n-k-1}\end{bmatrix} \tag{6.23}$$

Din (6.23), rezultă componentele sindromului

$$\begin{aligned}
s_0 &= r_0 + r_{n-k}\cdot p_{00} + r_{n-k+1}\cdot p_{10} + \cdots + r_{n-1}\cdot p_{k-1,0}\\
s_1 &= r_1 + r_{n-k}\cdot p_{01} + r_{n-k+1}\cdot p_{11} + \cdots + r_{n-1}\cdot p_{k-1,1}\\
&\vdots\\
s_{n-k-1} &= r_{n-k-1} + r_{n-k}\cdot p_{0,n-k-1} + r_{n-k+1}\cdot p_{1,n-k-1} + \cdots + r_{n-1,n-k-1}
\end{aligned} \tag{6.24}$$

EXEMPLUL 6.3: Considerăm acelaşi cod bloc liniar sistematic (7,4). Fie $\mathbf{r}=\left(r_0,r_1,r_2,r_3,r_4,r_5,r_6\right)$ vectorul recepționat. Sindromul este dat de

$$\mathbf{s}=\left(s_0,s_1,s_2\right)=$$

$$=\left(r_0,r_1,r_2,r_3,r_4,r_5,r_6\right)\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}$$

$$s_0 = r_0 + r_3 + r_5 + r_6$$
$$s_1 = r_1 + r_3 + r_4 + r_5$$
$$s_2 = r_2 + r_4 + r_5 + r_6$$

Sindromul poate fi calculat cu circuitul arătat în fig. 6.6.

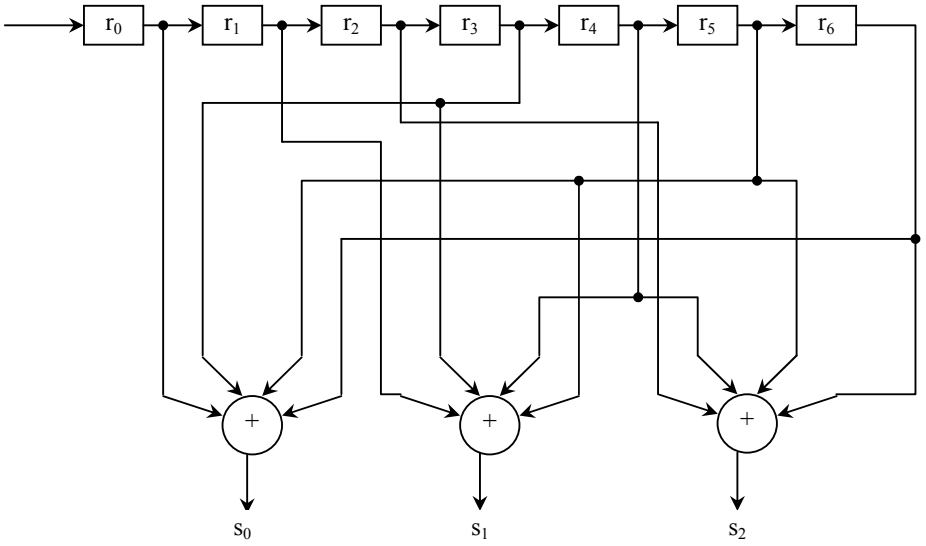

Fig. 6.6. Circuitul de calcul al sindromului pentru codul bloc liniar sistematic (7,4).

O proprietate interesantă a sindromului **s**, calculat din vectorul recepționat **r**, este că nu depinde de cuvântul de cod emis **v**, ci de vectorul de eroare **e**. Într-adevăr:

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{v} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T .$$

Dar $\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$, astfel că, în definitiv,

$$\mathbf{s} = \mathbf{e} \cdot \mathbf{H}^T \tag{6.25}$$

Între componentele sindromului şi componentele vectorului de eroare rezultă, deci, următoarea relație:

$$\begin{aligned} s_0 &= e_0 + e_{n-k} \cdot p_{00} + e_{n-k+1} \cdot p_{10} + \cdots + e_{n-1} \cdot p_{k-1,0} \\ s_1 &= e_1 + e_{n-k} \cdot p_{01} + e_{n-k+1} \cdot p_{11} + \cdots + e_{n-1} \cdot p_{k-1,1} \\ &\vdots \\ s_{n-k-1} &= e_{n-k-1} + e_{n-k} \cdot p_{0,n-k+1} + e_{n-k+1} \cdot p_{1,n-k-1} + \cdots + e_{n-1} \cdot p_{k-1,n-k-1} \end{aligned} \tag{6.26}$$

Se vede că simbolurile sindromului sunt combinații liniare ale simbolurilor de eroare. Ele furnizează informație cu privire la biții eronați şi pot fi deci utilizate pentru corecția erorilor.

6.5. DISTANȚA MINIMĂ A UNUI COD BLOC

Am construit un cod bloc segmentând şirul biților de informație în blocuri de câte k biți şi adăugând la fiecare bloc, numit mesaj, (n–k) biți redundanți, rezultând cuvinte de cod. Mulțimea mesajelor cuprinde toate blocurile de k biți, de la 00...0 la 11...1, astfel încât există $k \cdot 2^{k-1}$ perechi de mesaje ce diferă între ele printr-un singur bit. Iată de ce, dacă nu am introduce biții redundanți, un singur bit eronat la recepție schimbă un mesaj în altul. Biții redundanți trebuie să facă mai diferite între ele cuvintele de cod, dând o mai mare şansă receptorului să le deosebească. Vom introduce deci o măsură a deosebirii dintre cuvintele unui cod.

Ponderea Hamming (sau *ponderea*, pe scurt) a unui n–tuplu binar $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ este prin definiție numărul de componente diferite de zero ale lui **v** şi se notează cu $p(\mathbf{v})$. Spre exemplu, ponderea Hamming a lui **v** = (1 0 0 1 0 1 1) este 4. Fie **v** şi **w** două n–tupluri. *Distanța Hamming* (sau *distanța*, pe scurt) dintre **v** şi **w**, notată cu d (**v**, **w**), este prin definiție numărul de locuri în care ele diferă. Spre exemplu, pentru acelaşi **v** şi **w** = (1 0 1 0 1 1 0), d (**v**, **w**) = 4. Distanța Hamming este o funcție metrică ce satisface *inegalitatea triunghiului*. Fie **v**, **w** şi **z** trei n–tupluri. Avem:

$$d(\mathbf{v}, \mathbf{w}) + d(\mathbf{w}, \mathbf{z}) \geq d(\mathbf{v}, \mathbf{z}) \tag{6.27}$$

Din definiția distanței Hamming şi definiția adunării modulo 2, urmează că distanța Hamming dintre două n–tupluri **v** şi **w** este egală cu ponderea Hamming a sumei dintre **v** şi **w**:

$$d(\mathbf{v}, \mathbf{w}) = p(\mathbf{v} + \mathbf{w}) \tag{6.28}$$

Pentru exemplul de mai sus, **v** + **w** = (0 0 1 1 1 0 1), care are pondere 4.

Pentru un cod bloc *C*, se poate calcula distanța Hamming dintre oricare două cuvinte de cod distincte. Prin definiție, *distanța minimă* a lui *C*, notată cu d_{min}, este

$$d_{\min} = \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \tag{6.29}$$

Dar dacă *C* este un cod bloc liniar, suma dintre două cuvinte este şi ea un cuvânt de cod. Din (6.28), rezultă că distanța Hamming dintre două cuvinte de cod este egală cu ponderea Hamming a unui al treilea cuvânt de cod din *C*. Din (6.29), urmează că

$$\begin{aligned} d_{\min} &= \min\{p(\mathbf{v}+\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} = \\ &= \min\{p(\mathbf{z}) : \mathbf{z} \in C, \mathbf{z} \neq \mathbf{0}\} \triangleq p_{\min}. \end{aligned} \tag{6.30}$$

Parametrul $p_{\min} \triangleq \{p(\mathbf{z}) : \mathbf{z} \in C, \mathbf{z} \neq \mathbf{0}\}$ se numeşte ponderea minimă a codului liniar *C*. Acest rezultat se exprimă în forma următoarei teoreme.

TEOREMA 6.1: Distanța minimă a unui cod bloc liniar este egală cu ponderea minimă a cuvintelor de cod diferite de zero.

Utilizând această teoremă, pentru a determina distanța minimă a unui cod bloc liniar, nu avem altceva de făcut decât să vedem care este ponderea minimă. Codul (7,4) din Exemplul 6.1 are ponderea minimă 3, aşa încât distanța sa minimă este egală cu 3.

TEOREMA 6.2: Fie *C* un cod bloc liniar (*n,k*) cu matrice de control **H**. Pentru fiecare cuvânt de cod de pondere Hamming *l*, există *l* coloane ale lui **H** astfel încât suma vectorială a acestor *l* coloane este egală cu vectorul zero. Reciproc, dacă există *l* coloane ale lui **H** a căror sumă vectorială este vectorul zero, există în *C* un cuvânt de cod de pondere Hamming *l*.

DEMONSTRAȚIE

Să exprimăm matricea de cod **H** în următoarea formă:

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}] \tag{6.31}$$

unde $\mathbf{h}_i$ reprezintă coloana *i* a lui **H**. Fie $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ un cuvânt de cod de pondere *l*. Aceasta înseamnă că **v** are *l* componente diferite de zero, fie ele $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$, unde $0 \le i_1 < i_2 < \cdots < i_l \le n-1$. Codul fiind binar, $v_{i_1} = v_{i_2} = \cdots = v_{i_l} = 1$. Întrucât **v** este cuvânt de cod, conform cu ecuația (6.15), trebuie să avem:

$$\begin{aligned}\mathbf{0} = \mathbf{v}\cdot\mathbf{H}^T &= v_0\mathbf{h}_0 + v_1\cdot\mathbf{h}_1 + \cdots + v_{n-1}\cdot\mathbf{h}_{n-1} \\ &= v_{i_1}\cdot\mathbf{h}_{i_1} + v_{i_2}\cdot\mathbf{h}_{i_2} + \cdots + v_{i_l}\cdot\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}\end{aligned} \tag{6.32}$$

Am demonstrat astfel prima parte a teoremei. Să presupunem acum că $\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}$ sunt *l* coloane ale lui **H** astfel încât

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}. \tag{6.33}$$

Să formăm vectorul binar $\mathbf{w} = (w_0, w_1, \cdots, w_{n-1})$ ale cărui componente nenule sunt $w_{i_1}, w_{i_2}, \cdots, w_{i_l}$. Ponderea Hamming a lui **w** este *l*. Considerăm produsul:

$$\begin{aligned}\mathbf{w}\cdot\mathbf{H}^T &= w_0\mathbf{h}_0 + \mathbf{w}_1\mathbf{h}_1 + \cdots + w_{n-1}\mathbf{h}_{n-1} \\ &= w_{i_1}\mathbf{h}_{i_1} + w_{i_2}\mathbf{h}_{i_2} + \cdots + w_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}.\end{aligned}$$

Din (6.33), urmează că $\mathbf{w}\cdot\mathbf{H}^T = \mathbf{0}$. Deci, **w** este un cuvânt de cod de pondere *l* din *C*. Am demonstrat astfel şi partea a doua a teoremei.

COROLAR 6.1: Fie *C* un cod bloc liniar (*n*,*k*) cu matrice de control **H**. Dacă nu există *d*–1 sau mai puține coloane ale lui **H** a căror sumă să fie **O**, codul are pondere minimă cel puțin egală cu *d*.

COROLAR 6.2: Fie *C* un cod bloc liniar (*n*,*k*) cu matrice de control **H**. Ponderea minimă (sau distanța minimă) a lui *C* este egală cu cel mai mic număr de coloane ale lui **H** a căror sumă este **O**.

EXEMPLUL 6.4: Pentru codul (7,4) considerat în exemplul 6.1, fiindcă toate coloanele lui **H** sunt nenule şi diferite între ele, suma a două coloane nu poate fi zero. Rezultă că ponderea minimă a acestui cod este de cel puțin 3. Observăm că suma dintre coloanele 0, 1 şi 3 este **O**, astfel că ponderea minimă a codului este chiar 3.

6.6. CAPACITATEA UNUI COD BLOC LINIAR DE DETECȚIE ŞI DE CORECȚIE A ERORILOR

Dacă se transmite un cuvânt de cod **v** pe un canal afectat de zgomot şi se produc *l* erori de bit, vectorul recepționat **r** va diferi de cel emis în *l* componente: $d(\mathbf{v},\mathbf{r}) = l$. Fie d_{min} distanța minimă a unui cod bloc *C*, ceea ce

înseamnă că oricare două cuvinte de cod diferă în cel puţin d_{min} componente. Un număr de d_{min}–1 erori de bit sau mai puţine nu transformă un cuvânt de cod în altul. Cu alte cuvinte, d_{min}–1 erori de bit sau mai puţine produc un vector recepţionat **r** care nu este cuvânt de cod din C. Atunci când receptorul constată că vectorul de cod recepţionat nu este cuvânt de cod din C, spunem că au fost detectate erori. Prin urmare, un cod bloc cu distanţă minimă d_{min} poate detecta d_{min}–1 erori de bit sau mai puţine dintr-un cuvânt de n biţi.

Un cod bloc cu distanţa minimă d_{min} garantează detecţia tuturor combinaţiilor de d_{min}–1 erori de bit sau mai puţine, dar detectează şi o mare parte din combinaţiile cu mai multe erori. Între cei 2^n–1 posibili vectori de eroare diferiţi de zero, există 2^k–1 care sunt identici cu cele 2^k–1 cuvinte de cod diferite de cuvântul de cod **O**. Dacă zgomotul produce oricare dintre aceşti 2^k–1 vectori de eroare, vectorul emis va fi transformat într-un alt cuvânt de cod **w**. Sindromul lui **w** este zero, astfel încât decodorul acceptă **w** ca pe cuvântul de cod transmis şi face, deci, o decodare incorectă. Prin urmare, există 2^k–1 vectori de eroare nedetectabili şi 2^n–2^k vectori de eroare detectabili.

Notăm cu A_i numărul cuvintelor de cod de pondere i din C. Numerele $A_0, A_1, \cdots, A_n$ constituie *distribuţia de pondere* a lui C. Pentru un cod bloc liniar, A_0=1, iar numerele de la A_1 la $A_{d_{\min}-1}$ sunt zero.

Vom calcula probabilitatea ca decodorul să nu detecteze prezenţa erorilor la transmisia pe un canal binar simetric cu probabilitate de tranziţie p. Notăm cu P_n probabilitatea unei erori nedetectabile. O eroare nedetectabilă apare numai atunci când vectorul de eroare este identic cu un cuvânt de cod diferit de zero din C:

$$P_n = \sum_{i=d_{\min}}^{n} A_i p^i (1-p)^{n-i}. \qquad (6.34)$$

EXEMPLUL 6.5: Pentru codul (7.4) considerat în exemplul 6.1, distribuţia de pondere este: $A_0 = 1,\ A_1 = A_2 = 0,\ A_3 = 7,\ A_4 = 7,\ A_5 = A_6 = 0,$ şi $A_7 = 1$. Probabilitatea unei erori nedetectate este

$$P_7 = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7.$$

Dacă $p = 10^{-2}$, $P_7 \cong 7 \cdot 10^{-6}$. Aşadar, dacă transmitem pe un canal binar simetric cu $p = 10^{-2}$ un milion de cuvinte de cod, în medie, numai 7 cuvinte de cod eronate vor trece prin decodor fără a fi detectate.

Distanța minimă d_{min} este un număr natural par sau impar. Fie t un număr natural astfel încât

$$2t+1 \le d_{\min} \le 2t+2 \tag{6.35}$$

După cum vom demonstra, codul C poate corecta toți vectorii de eroare ce conțin t erori de bit sau mai puține. Fie $\mathbf{v}$ cuvântul de cod emis, $\mathbf{r}$ vectorul recepționat şi $\mathbf{w}$ oricare alt cuvânt de cod din C. Distanțele Hamming dintre $\mathbf{v}$, $\mathbf{r}$ şi $\mathbf{w}$ satisfac inegalitatea triunghiului:

$$d(\mathbf{v},\mathbf{r}) + d(\mathbf{w},\mathbf{r}) \ge d(\mathbf{v},\mathbf{w}) \tag{6.36}$$

Să presupunem că, în cursul transmisiei lui $\mathbf{v}$, apar t' erori. Vectorul recepționat $\mathbf{r}$ diferă de $\mathbf{v}$ în t' componente şi, deci, $d(\mathbf{v},\mathbf{r}) = t'$. Întrucât $\mathbf{v}$ şi $\mathbf{w}$ sunt cuvinte de cod din C, avem

$$d(\mathbf{v},\mathbf{w}) \ge d_{\min} \ge 2t+1 \tag{6.37}$$

Din relațiile de mai sus, rezultă că

$$d(\mathbf{w},\mathbf{r}) \ge 2t+1-t'. \tag{6.38}$$

Din (6.38) urmează că, dacă $t' \le t$,

$$d(\mathbf{w},\mathbf{r}) > t. \tag{6.39}$$

Inegalitatea (6.39) spune că, dacă a apărut un vector de eroare de t erori sau mai puține, vectorul recepționat $\mathbf{r}$ este mai apropiat ca distanță Hamming de cuvântul de cod emis $\mathbf{v}$ dacât de oricare alt cuvânt de cod din C. Pentru un canal binar simetric, aceasta înseamnă că probabilitatea condiționată $P(\mathbf{r} \mid \mathbf{v})$ este mai mare decât probabilitatea condiționată $P(\mathbf{r} \mid \mathbf{w})$ pentru $\mathbf{w} \ne \mathbf{v}$. Dacă receptorul aplică o schemă de decodare de probabilitate maximă, $\mathbf{r}$ este decodat drept $\mathbf{v}$, care este cuvântul de cod transmis în realitate. Prin urmare, erorile sunt corectate.

Pe de altă parte, codul nu poate corecta toți vectorii de eroare conținând l erori cu $l > t$, căci există cel puțin un caz în care vectorul de eroare conținând l erori face ca vectorul recepționat să fie mai apropiat de un cuvânt de cod diferit de cel transmis în realitate. Pentru a arăta aceasta, fie două cuvinte de cod din C astfel încât

$$d(\mathbf{v},\mathbf{w}) = d_{\min}.$$

Fie $\mathbf{e}_1$ şi $\mathbf{e}_2$ doi vectori de eroare ce satisfac următoarele condiții:

1. $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
2. $\mathbf{e}_1$ şi $\mathbf{e}_2$ nu au biți de 1 în locuri comune.

Evident, avem

$$p(\mathbf{e}_1) + p(\mathbf{e}_2) = p(\mathbf{v}+\mathbf{w}) = d(\mathbf{v},\mathbf{w}) = d_{\min}. \tag{6.40}$$

Presupunem că se transmite **v** care este afectat de vectorul de eroare $\mathbf{e}_1$. Vectorul recepționat este

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1. \tag{6.41}$$

Distanța Hamming dintre **v** şi **r** este

$$d(\mathbf{v},\mathbf{r}) = p(\mathbf{v}+\mathbf{r}) = p(\mathbf{e}_1) \tag{6.42}$$

Distanța Hamming dintre **w** şi **r** este

$$d(\mathbf{w},\mathbf{r}) = p(\mathbf{w}+\mathbf{r}) = p(\mathbf{w}+\mathbf{v}+\mathbf{e}_1) = p(\mathbf{e}_2). \tag{6.43}$$

Să presupunem acum că vectorul de eroare $\mathbf{e}_1$ conține mai mult decât *t* erori, adică, $p(\mathbf{e}_1) > t$. Ținând seama de (6.35) şi de (6.40), obținem că

$$p(\mathbf{e}_2) \le t+1. \tag{6.44}$$

Din (6.42) şi (6.43), rezultă că

$$d(\mathbf{v},\mathbf{r}) \ge d(\mathbf{w},\mathbf{r}). \tag{6.45}$$

Inegalitatea (6.45) ne spune că există un vector de eroare conținând *l* erori $(l > t)$ care face ca vectorul recepționat să fie mai aproape de un cuvânt de cod diferit de cel transmis în realitate. Prin aplicarea schemei de decodare de plauzibilitate maximă, se face astfel o decodare incorectă.

În concluzie, notând cu $\lfloor (d_{\min}-1)/2 \rfloor$ cel mai mare număr natural mai mic decât $(d_{\min}-1)/2$, un cod bloc liniar cu distanța minimă $d_{\min}$ garantează corectarea tuturor vectorilor de eroare conținând $t = \lfloor (d_{\min}-1)/2 \rfloor$ erori sau mai puține. Parametrul $t = \lfloor (d_{\min}-1)/2 \rfloor$ se numeşte capacitatea de corecție a erorilor aleatoare pe care o are codul.

6.7. TABLOUL STANDARD ŞI DECODAREA CU AJUTORUL SINDROMULUI

Fie $\mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_{2^k-1}$ cele 2^k cuvinte de cod din codul *C*. Indiferent ce cuvânt de cod este transmis pe canal, din cauza zgomotului, vectorul recepționat **r** poate fi oricare din cei 2^n vectori definiți pe corpul Galois *CG*(2). În vederea decodării, partiționăm mulțimea celor 2^n vectori în

submulțimi $D_0, D_1, \cdots, D_{2^k-1}$ astfel încât cuvântul de cod $\mathbf{v}_i$ să fie conținut în submulțimea D_i pentru $0 \le i \le 2^k - 1$. Vom fi realizat astfel o bijecție între mulțimea cuvintelor de cod şi mulțimea $\{D_i\}$. Regula de decodare pe care o stabilim este aceea că, dacă vectorul recepționat **r** se găseşte în submulțimea D_i, rezultatul decodării este $\mathbf{v}_i$. Decodarea este corectă dacă şi numai dacă vectorul recepționat **r** aparține submulțimii D_i corespunzătoare cuvântului de cod transmis. Apartența vectorilor la submulțimi se stabileşte după cum urmează:

1. Cele 2^k cuvinte de cod din *C* se dispun pe un rând de la stânga la dreapta începând cu $\mathbf{v}_0 = (0,0,\cdots,0)$.
2. Din restul de $2^n - 2^k$ vectori *n*-dimensionali, se alege unul, notat cu $\mathbf{e}_1$, şi se aşează sub $\mathbf{v}_0$. Se completează al doilea rând adunând vectorul $\mathbf{e}_1$ la fiecare cuvânt de cod $\mathbf{v}_i$ din primul rând şi se aşează suma $\mathbf{e}_1 + \mathbf{v}_i$ sub $\mathbf{v}_i$.
3. La completarea rândului al doilea, se alege un vector neutilizat $\mathbf{e}_2$ şi se aşează sub $\mathbf{e}_1$. Se adună $\mathbf{e}_2$ la fiecare vector de cod $\mathbf{v}_i$ din primul rând şi se aşează $\mathbf{e}_2 + \mathbf{v}_i$ sub $\mathbf{e}_1 + \mathbf{v}_i$.
4. Se procedează la fel până ce se vor fi fost utilizați toți vectorii *n*-dimensionali.

Rezultă tabloul standard al codului bloc liniar *C*:

$$
\begin{array}{ccccccc}
\mathbf{v}_0 = \mathbf{0} & \mathbf{v}_1 & \cdots & \mathbf{v}_i & \cdots & \mathbf{v}_{2^k-1} \\
\mathbf{e}_1 & \mathbf{e}_1 + \mathbf{v}_1 & \cdots & \mathbf{e}_1 + \mathbf{v}_i & \cdots & \mathbf{e}_1 + \mathbf{v}_{2^k-1} \\
\mathbf{e}_2 & \mathbf{e}_2 + \mathbf{v}_1 & \cdots & \mathbf{e}_2 + \mathbf{v}_i & \cdots & \mathbf{e}_2 + \mathbf{v}_{2^k-1} \\
\vdots & & & & & \\
\mathbf{e}_l & \mathbf{e}_l + \mathbf{v}_1 & \cdots & \mathbf{e}_l + \mathbf{v}_i & \cdots & \mathbf{e}_l + \mathbf{v}_{2^k-1} \\
\vdots & & & & & \\
\mathbf{e}_{2^{n-k}-1} & \mathbf{e}_{2^{n-k}-1} + \mathbf{v}_1 & \cdots & \mathbf{e}_{2^{n-k}-1} + \mathbf{v}_i & \cdots & \mathbf{e}_{2^{n-k}-1} + \mathbf{v}_{2^k-1}
\end{array}
$$

Observăm că suma dintre oricare doi vectori de pe acelaşi rând este un cuvânt de cod din *C*.

TEOREMA 6.3: În acelaşi rând al unui tablou standard nu există doi vectori identici. Fiecare vector apare într-un rând şi numai în unul.

DEMONSTRAȚIE
Cuvintele de cod sunt distincte, de unde rezultă adevărul din prima parte a teoremei. Din regula de construcție a tabloului standard, rezultă că fiecare vector apare cel puțin o dată. Să presupunem acum că un vector apare atât pe rândul l cât şi pe rândul m, cu $l < m$. Acest vector trebuie să fie egal cu $\mathbf{e}_l + \mathbf{v}_i$ pentru un i şi să fie egal cu $\mathbf{e}_m + \mathbf{v}_j$ pentru un j. Rezultă că $\mathbf{e}_l + \mathbf{v}_i = \mathbf{e}_m + \mathbf{v}_j$ şi prin urmare $\mathbf{e}_m = \mathbf{e}_l + (\mathbf{v}_i + \mathbf{v}_j)$. Dar $\mathbf{v}_i$ şi $\mathbf{v}_j$ sunt cuvinte de cod din C, astfel încât şi suma lor este un cuvânt de cod, să spunem $\mathbf{v}_s$. Deci $\mathbf{e}_m = \mathbf{e}_l + \mathbf{v}_s$, ceea ce implică faptul că $\mathbf{e}_m$ este pe rândul l, iar aceasta contrazice regula de construcție a tabloului conform căreia $\mathbf{e}_m$, primul element de pe rândul m, nu trebuie să fi fost utilizat în vreun rând precedent. În concluzie, nici un vector nu poate să apară în mai mult decât un singur rând al tabloului.

În tabloul standard, există $2^n / 2^k = 2^{n-k}$ rânduri disjuncte, iar fiecare rând constă din 2^k elemente distincte. Cele 2^{n-k} rânduri se numesc *coseturile* codului C, iar primul vector $\mathbf{e}_l$ din fiecare coset se numeşte *lider de coset*. Orice element dintr-un coset poate fi luat drept lider de coset. Aceasta nu schimbă elementele din coset, ci doar le permută.

EXEMPLUL 6.6: Tabloul standard pentru codul bloc liniar sistematic (7,4) din exemplul 6.1 este dat pe pagina următoare.

Aşa cum se vede şi din exemplul de mai sus, un tablou standard al unui cod bloc liniar (n,k) constă din 2^k coloane disjuncte. Fiecare coloană constă din 2^{n-k} n–tupluri, cel mai de sus fiind un cuvânt de cod. Notăm cu D_j coloana j a tabloului standard:

$$D_j = \{\mathbf{v}_j, \mathbf{e}_1 + \mathbf{v}_j, \mathbf{e}_2 + \mathbf{v}_j, \cdots, \mathbf{e}_{2^{n-k}-1} + \mathbf{v}_j\} \tag{6.46}$$

În (6.46), $\mathbf{v}_j$ este un cuvânt de cod iar $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_{2^{n-k}-1}$ sunt lideri de coset. Cele 2^k coloane disjuncte se pot utiliza pentru decodare. Să presupunem că pe un canal zgomotos se transmite un cuvânt de cod $\mathbf{v}_j$. Din (6.46), vedem că vectorul recepționat $\mathbf{r}$ se găseşte în D_j dacă vectorul de eroare produs de canal este un lider de coset. În acest caz, vectorul recepționat $\mathbf{r}$ va fi decodat corect, rezultatul decodării fiind cuvântul emis $\mathbf{v}_j$. Dacă însă vectorul de eroare nu este un lider de coset, decodarea va fi eronată. Într-a-devăr, să notăm cu $\mathbf{e}$ vectorul de eroare produs de canal. El trebuie să fie în unul din coseturi şi sub un cuvânt de cod diferit de zero, să spunem în cosetul l şi sub cuvântul de cod $\mathbf{v}_i \neq \mathbf{0}$. Atunci $\mathbf{e} = \mathbf{e}_l + \mathbf{v}_i$ iar vectorul recepționat este

$$\mathbf{r} = \mathbf{v}_j + \mathbf{e} = \mathbf{e}_l + (\mathbf{v}_i + \mathbf{v}_j) = \mathbf{e}_l + \mathbf{v}_s .$$

Tabloul standard

Vectorul recepționat **r** se găseşte, deci, în coloana D_s şi este decodat drept $\mathbf{v}_s$, care nu este cuvântul de cod transmis. Rezultatul este o decodare eronată. Iată de ce, decodarea este corectă dacă şi numai dacă vectorul de eroare produs de canal este un lider de coset. Din acest motiv, cei 2^{n-k} lideri de coset (inclusiv vectorul **0**) se numesc *vectori de eroare corectabili*. Aceasta se exprimă în teorema următoare:

TEOREMA 6.4: Orice cod bloc liniar (*n,k*) poate corecta 2^{n-k} vectori de eroare.

Pentru a minimiza probabilitatea unei erori de decodare, drept lideri de coset se aleg cei mai probabili vectori de eroare. Pe un canal binar simetric, un vector de eroare de pondere mică este mai probabil decât unul cu pondere mai mare. Iată de ce, la formarea unui tablou standard, drept lider de coset se alege un vector cu cea mai mică pondere dintre cei rămaşi disponibili.

Să notăm cu α_i numărul liderilor de coset de pondere *i*. Numerele $\alpha_0, \alpha_1, \cdots, \alpha_n$ constituie *distribuția de pondere* a liderilor de coset. Cunoscând aceste numere, putem calcula probabilitatea unei erori de decodare. Ținând seama că o eroare de decodare apare dacă şi numai dacă vectorul de eroare nu este un lider de coset, probabilitatea de eroare pentru un canal binar simetric cu probabilitate de tranziție *p* este

$$P_E = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i} \tag{6.47}$$

EXEMPLUL 6.7: Pentru codul bloc liniar (7.4) considerat în exemplul 6.6, $\alpha_0 = 1, \alpha_1 = 7$, iar $\alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 = \alpha_7 = 0$.

Deci, $P_E = 1 - (1-p)^7 - 7p(1-p)^6$.

Pentru $p = 10^{-2}$, avem $P_E \cong 2{,}34 \cdot 10^{-3}$.

TEOREMA 6.5: Toate cele 2^k *n*–tupluri ale unui coset au acelaşi sindrom. Sindroamele pentru coseturi diferite sunt diferite.

DEMONSTRAȚIE

Considerăm cosetul al cărui lider este $\mathbf{e}_l$. Un vector din acest coset este suma dintre $\mathbf{e}_l$ şi un cuvânt de cod $\mathbf{v}_i$. Sindromul acestui vector este

$$(\mathbf{e}_l + \mathbf{v}_i)\mathbf{H}^T = \mathbf{e}_l \mathbf{H}^T + \mathbf{v}_i \mathbf{H}^T = \mathbf{e}_l \mathbf{H}^T. \tag{6.48}$$

Egalitatea (6.48) ne spune că sindromul oricărui vector dintr-un coset este egal cu sindromul liderului de coset. Prin urmare, toți vectorii dintr-un coset au același sindrom.

Fie $\mathbf{e}_j$ şi $\mathbf{e}_l$ liderii coseturilor j şi l respectiv, unde $j < l$. Să presupunem că sindroamele acestor două coseturi sunt egale. Atunci

$$\mathbf{e}_j\mathbf{H}^T = \mathbf{e}_l\mathbf{H}^T$$

de unde

$$\left(\mathbf{e}_j + \mathbf{e}_l\right)\mathbf{H}^T = \mathbf{0}.$$

Aceasta implică faptul că $\mathbf{e}_j + \mathbf{e}_l = \mathbf{v}_i$ şi $\mathbf{e}_l = \mathbf{e}_j + \mathbf{v}_i$. De aici ar rezulta că $\mathbf{e}_l$ se găseşte în cosetul j, ceea ce contrazice regula de construcție a unui tablou standard care spune că un lider de coset trebuie să nu fi fost utilizat anterior. Prin urmare, două coseturi nu pot avea același sindrom.

Sindromul unui n–tuplu este un (n–k)–tuplu şi există 2^{n-k} astfel de (n–k)–tupluri distincte. Din teorema 6.5, rezultă că este o bijecție de la mulțimea coseturilor la mulțimea sindroamelor. Cum însă liderul de coset este reprezentantul cosetului, există şi o aplicație bijectivă de la mulțimea liderilor de coset la mulțimea sindroamelor. Utilizând această bijecție, putem forma un tablou de decodare mult mai simplu decât un tablou standard. Tabloul constă în 2^{n-k} lideri de coset şi în sindromele lor corespunzătoare. Acest tablou este fie memorat, fie cablat în receptor.

Decodarea unui vector recepționat constă în trei paşi:

Pasul 1. Se calculează sindromul lui $\mathbf{r}$, $\mathbf{r} \cdot \mathbf{H}^T$.

Pasul 2. Se identifică liderul de coset $\mathbf{e}_l$ al cărui sindrom este egal cu $\mathbf{r} \cdot \mathbf{H}^T$. Se admite ipoteza că $\mathbf{e}_l$ este vectorul de eroare produs de canal.

Pasul 3. Rezultatul decodării vectorului recepționat $\mathbf{r}$ este cuvântul de cod $\mathbf{v} = \mathbf{r} + \mathbf{e}_l$.

EXEMPLUL 6.8: Pentru codul bloc liniar sistematic (7,4) considerat în exemplele din acest capitol, există $2^3 = 8$ coseturi şi, deci, avem opt vectori de eroare corectabili (inclusiv vectorul zero). Întrucât distanța minimă a codului este 3, el poate corecta toți vectorii de eroare de pondere 1 sau 0. Prin urmare, toate cele şapte n–tupluri de pondere 1 plus vectorul de pondere 0 se pot utiliza drept lideri de coset.

Tabloul de decodare pentru codul (7,4)

Sindrom	Lider de coset
1 0 0	1 0 0 0 0 0 0
0 1 0	0 1 0 0 0 0 0
0 0 1	0 0 1 0 0 0 0
1 1 0	0 0 0 1 0 0 0
0 1 1	0 0 0 0 1 0 0
1 1 1	0 0 0 0 0 1 0
1 0 1	0 0 0 0 0 0 1

Să presupunem că se transmite cuvântul de cod $\mathbf{v} = (1\ 0\ 0\ 1\ 0\ 1\ 1)$ şi se recepționează $\mathbf{r} = (1\ 0\ 0\ 1\ 1\ 1\ 1)$. Calculăm sindromul lui **r**:

$$\mathbf{s} = (1\ 0\ 0\ 1\ 1\ 1\ 1)\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = (0\ 1\ 1).$$

Din tabloul de decodare, vedem că (0 1 1) este sindromul liderului de coset $\mathbf{e} = (0\ 0\ 0\ 0\ 1\ 0\ 0)$. În ipoteza că acesta este vectorul de eroare produs de canal, decodăm **r** drept

$$\mathbf{v}^* = \mathbf{r} + \mathbf{e} = (1\ 0\ 0\ 1\ 1\ 1\ 1) + (0\ 0\ 0\ 0\ 1\ 0\ 0) = (1\ 0\ 0\ 1\ 0\ 1\ 1).$$

Acesta este chiar cuvântul de cod transmis.

Presupunem acum că se transmite cuvântul de cod $\mathbf{v} = (0\ 0\ 0\ 0\ 0\ 0\ 0)$, dar se recepționează (1 0 0 0 01 0 0). Calculăm sindromul:

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (1\ 1\ 1).$$

Din tabloul de decodare, vedem că acestui sindrom îi corespunde liderul de coset $\mathbf{e} = (0\ 0\ 0\ 0\ 0\ 1\ 0)$. Drept rezultat, **r** este decodat drept

$$\mathbf{v}^* = \mathbf{r} + \mathbf{e} = (1\ 0\ 0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 0\ 1\ 0) = (1\ 0\ 0\ 0\ 1\ 1\ 0).$$

Întrucât $\mathbf{v}^*$ nu este cuvântul de cod transmis, receptorul a facut o eroare de decodare.

6.8. DECODAREA SUPLĂ A CODURILOR BLOC

Decodarea codurilor bloc cu ajutorul sindromului şi al tabloului standard operează asupra unui vector de recepţie **r** cu componente binare, ceea ce presupune că asupra simbolului demodulat se ia o decizie fermă, care alege între 0 şi 1. În etapa de dezvoltare a electronicii digitale când au fost elaborate primele coduri bloc, o prelucrare mai avansată a semnalului recepţionat nu mai era posibilă. Între timp, situaţia s-a îmbunătăţit considerabil, atât în ce priveşte teoria, cât şi posibilităţile de a o aplica în practică. În această secţiune, vom vedea avantajele unei decodări suple în comparaţie cu decodarea fermă.

Considerăm sistemul de comunicaţie reprezentat în fig. 6.6.

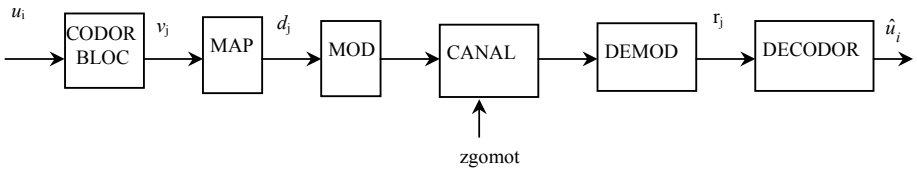

Fig. 6.6. Schema bloc a unui sistem de comunicaţie ce decodare suplă.

Şirul biţilor generaţi de sursa de informaţie este mai întâi segmentat în blocuri de lungime k, numite mesaje, iar fiecare mesaj este transformat de codul bloc într-un cuvânt de cod. Biţii $\{v_j\}$ ai cuvintelor de cod iau valorile 0 şi 1 cu egală probabilitate. Ei intră unul câte unul într-un modulator de amplitudine a pulsurilor (MAP) care face ca valorilor 0 şi 1 ale bitului v_j să le corespundă valorile –1 şi +1 respectiv ale variabilei d_j. Modulatorul MOD efectuează o modulaţie binară (de amplitudine, frecvenţă sau fază), ceea ce înseamnă că aplică la intrarea în canal una din două forme de undă, una pentru $d_j = -1$, cealaltă pentru $d_j = +1$. Vom presupune că zgomotul introdus de canal este aditiv, alb şi gaussian. Prelucrând forma de undă recepţionată, coruptă de zgomot, demodulatorul DEMOD produce variabila r_j, care poate lua orice valoare dintr-un interval continuu simetric faţă de 0. Dacă receptorul ia o decizie fermă, r_j se compară cu pragul de 0 şi se decide că bitul emis va fi fost 0 sau 1, decodarea făcându-se apoi algebric, utilizând sindromul. O stategie mai bună este, însă, de a face o decodare suplă. Pentru aceasta, teoria probabilităţii ne va fi din nou deosebit de utilă. Să ne

reamintim teorema lui Bayes, învățată la Cap.1 cu prilejul introducerii probabilității condiționate. Fie *A* şi *B* două evenimente discrete. Prin definiție, probabilitatea evenimentului *A* condiționată de producerea evenimentului *B*, notată cu *P(A/B)*, este egală cu raportul dintre probabilitatea comună *P(A,B)* şi probabilitatea evenimentului *B*, *P*(*B*) :

$$P(A/B)=\frac{P(A,B)}{P(B)}.$$

Schimbând între ele evenimentele *A* şi *B*, avem de asemenea :

$$P(B/A)=\frac{P(A,B)}{P(B)}.$$

Teorema (sau regula) lui Bayes rezultă din cele două egalități de mai sus eliminând *P(A,B)* :

$$P(A/B)P(B)=P(B/A)P(A).$$

Acum, dacă demodulatorul, la timpul discret *j*, furnizează un număr real r_j, diferit atât de –1 cât şi de +1, ce putem afirma despre valoarea d_j emisă? Spunem că r_j este o variabilă aleatoare „observabilă“, căci ea apare la ieşirea demodulatorului ca o tensiune electrică pe care o putem măsura. Spre deosebire de variabila aleatoare de la emisie d_j, care ia valori discrete –1 şi +1, variabila aleatoare de la recepție r_j este de tip continuu, astfel încât trebuie să o descriem cu ajutorul unei funcții de densitate de probabilitate (fdp). Dacă se emite d_j = –1, datorită zgomotului gaussian, funcția densitate de probabilitate a lui r_j, condiționată de emisia lui –1, are forma cunoscută, de clopot, cu valoarea medie egală cu –1, pentru care curba îşi are maximul; similar pentru cazul în care se emite d_j = +1. Cele două funcții de densitate de probabilitate condiționată sunt reprezentate grafic în fig 6.7.

Fig. 6.7. Funcțiile de densitate de probabilitate condiționată de valoarea simbolului emis d_j.

Conform teoriei deciziei, definim două ipoteze, notate cu I_1 şi I_2. În ipoteza I_1, a fost emis +1, iar în ipoteza I_2, a fost emis –1. Regula de decizie, numită *maximum a posteriori* (MAP), este următoarea:

$$P\left(d_j = +1 \mid r_j\right) \underset{I_2}{\overset{I_1}{\gtrless}} P\left(d_j = -1 \mid r_j\right). \tag{6.49}$$

Relaţia (6.49) ne spune că se confirmă ipoteza $I_1\left(d_j = +1\right)$ dacă $P\left(d_j = +1 \mid r_j\right)$ este mai mare decât $P\left(d_j = -1 \mid r_j\right)$. În caz contrar, se confirmă ipoteza $I_2\left(d_j = -1\right)$. Utilizând teorema lui Bayes, găsim expresia echivalentă:

$$p\left(r_j \mid d_j = +1\right) P\left(d_j = +1\right) \underset{I_2}{\overset{I_1}{\gtrless}} p\left(r_j \mid d_j = -1\right) P\left(d_j = -1\right) \tag{6.50}$$

De aici, obţinem aşa-zisul *test al raportului de probabilitate*:

$$\frac{p(r_j \mid d_j = +1)}{p(r_j \mid d_j = -1)} \underset{I_2}{\overset{I_1}{\gtrless}} \frac{P(d_j = -1)}{P(d_j = +1)} \tag{6.51}$$

Echivalent, acesta se poate scrie:

$$\frac{p(r_j \mid d_j = +1) P(d_j = +1)}{p(r_j \mid d_j = -1) P(d_j = -1)} \underset{I_2}{\overset{I_1}{\gtrless}} 1 \tag{6.52}$$

Luând logaritmul raportului de probabilitate, obţinem o metrică utilă numită *log-raport de probabilitate*:

$$L\left(d_j \mid r_j\right) = \log\left[\frac{P\left(d_j = +1 \mid r_j\right)}{P\left(d_j = -1 \mid r_j\right)}\right] = \log\left[\frac{p\left(r_j \mid d_j = +1\right) P\left(d_j = +1\right)}{p\left(r_j \mid d_j = -1\right) P\left(d_j = -1\right)}\right] \tag{6.53}$$

Din (6.53) rezultă:

$$L\left(d_j \mid r_j\right) = \log\left[\frac{p\left(r_j \mid d_j = +1\right)}{p\left(r_j \mid d_j = -1\right)}\right] + \log\left[\frac{P\left(d_j = +1\right)}{P\left(d_j = -1\right)}\right] \tag{6.54}$$

sau

$$L\left(d_j \mid r_j\right) = L\left(r_j \mid d_j\right) + L\left(d_j\right). \tag{6.55}$$

În (6.55), $L\left(d_j \mid r_j\right)$ este log-raportul de probabilitate al statisticii de test r_j obţinute prin măsurători ale ieşirii demodulatorului r_j în condiţiile în care se

va fi transmis $d_j = +1$ sau $d_j = -1$, iar $L(d_j)$ este log-raportul de probabilitate *a priori* al bitului de date d_j la momentul discret j. Pentru a simplifica notația, vom rescrie (6.55) astfel:

$$L'\left(\hat{d}_j\right) = L_c\left(r_j\right) + L\left(d_j\right) \tag{6.56}$$

Notația $L_c\left(r_j\right)$ în loc de $L\left(r_j \mid d_j\right)$ subliniază faptul că acest termen este rezultatul unei măsurători a canalului făcute la recepție. În cazul unui decodor proiectat pentru un cod bloc sistematic, ieşirea suplă a decodorului este egală cu

$$L\left(\hat{d}_j\right) = L'\left(\hat{d}_j\right) + L_e\left(\hat{d}_j\right) \tag{6.57}$$

unde $L'\left(\hat{d}_j\right)$ este log-raportul de probabilitate al bitului de date la ieşirea din demodulator şi la intrarea în decodor, iar $L_e\left(\hat{d}_j\right)$ este log-raportul de probabilitate *extrinsec*, reprezentând o cunoaştere suplimentară obținută în procesul de decodare datorită redundanței informaționale introduse între biții cuvântului de cod. Prin urmare, log-raportul de probabilitate la ieşirea decodorului este

$$L\left(\hat{d}_j\right) = L_c\left(r_j\right) + L\left(d_j\right) + L_e\left(\hat{d}_j\right). \tag{6.58}$$

Ecuația (6.58) arată că log-raportul de probabilitate la ieşirea unui decodor sistematic are trei termeni, independenți statistic: o măsurare a canalului, o cunoaştere *a priori* a bitului şi un log-raport de probabilitate extrinsec generat de decodor pe baza redundanței introduse prin codare. Ieşirea suplă a decodorului $L\left(\hat{d}_j\right)$ este un număr real care asigură atât o decizie fermă cât şi fiabilitatea acestei decizii. Semnul lui $L\left(\hat{d}_j\right)$ ne dă decizia fermă, în sensul că o valoare pozitivă decide că $d_j = +1$, iar o valoare negativă, că $d_j = -1$.

Modulul lui $L\left(\hat{d}_j\right)$ ne arată fiabilitatea deciziei. Să renunțăm, pentru comoditatea scrierii, la indicele de timp discret j. Este convenabil să introducem o algebră a log-raporturilor de probabilitate. Pentru doi biți statistic independenți d_1 şi d_2, definim suma a două log-raporturi de probabilitate astfel:

$$L(d_1) \boxplus L(d_2) = L(d_1 \oplus d_2) \tag{6.59}$$

Vom da o formă mai utilizabilă acestei relații adoptând logaritmul natural. Din algebra lui Boole, ştim că:

$$d_1 \oplus d_2 = d_1 \cdot \overline{d}_2 + \overline{d}_1 \cdot d_2$$

$$\overline{d_1 \oplus d_2} = d_1 \cdot d_2 + \overline{d}_1 \cdot \overline{d}_2$$

Conform definiției log-raportului de probabilitate, avem:

$$L(d_1 \oplus d_2) = \ln \frac{P(d_1 \oplus d_2 = +1)}{P(d_1 \oplus d_2 = -1)} =$$

$$= \ln \frac{P(d_1 = +1)P(d_2 = -1) + P(d_1 = -1)P(d_2 = +1)}{P(d_1 = +1)P(d_2 = +1) + P(d_1 = -1)P(d_2 = -1)} = \quad (6.60)$$

$$= \frac{\frac{P(d_1 = +1)}{P(d_1 = -1)} + \frac{P(d_2 = +1)}{P(d_2 = -1)}}{1 + \frac{P(d_1 = +1)}{P(d_1 = -1)} \cdot \frac{P(d_2 = +1)}{P(d_2 = -1)}} = \ln \frac{e^{L(d_1)} + e^{L(d_2)}}{1 + e^{L(d_1)} e^{L(d_2)}}$$

Din (6.60), se obţine o formulă aproximativă utilă dacă $L(d_1)$ şi $L(d_2)$ diferă mult ca mărime:

$$L(d_1) \boxplus L(d_2) = (-1) \times \operatorname{sgn}[L(d_1)] \times \operatorname{sgn}[L(d_2)] \times \min(|L(d_1)|, |L(d_2)|) \quad (6.61)$$

Conform cu (6.61), avem:

$$L(d) \boxplus \infty = -L(d) \quad (6.62a)$$

şi

$$L(d) \boxplus 0 = 0 \quad (6.62b)$$

Pentru semnalul r_j, obţinut prin demodulare la timpul discret j, avem:

$$L_c(r_j) = \ln \left[\frac{p(r_j \mid d_j = +1)}{p(r_j \mid d_j = -1)} \right] = \ln \left(\frac{\frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2} \left(\frac{r_j - 1}{\sigma} \right)^2 \right]}{\frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2} \left(\frac{r_j + 1}{\sigma} \right)^2 \right]} \right) = \quad (6.63)$$

$$= -\frac{1}{2} \left(\frac{r_j - 1}{\sigma} \right)^2 + \frac{1}{2} \left(\frac{r_j + 1}{\sigma} \right)^2 = \frac{2}{\sigma^2} r_j .$$

EXEMPLUL 6.9: Considerăm acelaşi cod bloc liniar sistematic (7,4) ca în toate exemplele precedente. Fie (u_0, u_1, u_2, u_3) mesajul emis la timpul j şi $(c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ cuvântul de cod respectiv. Utilizând matricea generatoare **G** din exemplul 6.1, obţinem:

$$c_0 = u_0 \oplus u_2 \oplus u_3 \qquad c_3 = u_0$$
$$c_1 = u_0 \oplus u_1 \oplus u_2 \qquad c_4 = u_1$$
$$c_2 = u_1 \oplus u_2 \oplus u_3 \qquad c_5 = u_2$$
$$c_6 = u_3$$

Ceea ce ne interesează, este să decodăm corect biții de informație c_3, c_4, c_5 şi c_6. La decodare, trebuie să contribuie şi biții de paritate c_0, c_1 şi c_2. Din egalitățile de definiție ale acestora, obținem:

$$\begin{aligned} u_0 &= u_1 \oplus c_0 \oplus c_2 \\ u_0 &= u_3 \oplus c_1 \oplus c_2 \\ u_1 &= u_3 \oplus c_0 \oplus c_1 \\ u_1 &= u_0 \oplus c_0 \oplus c_2 \end{aligned} \qquad \begin{aligned} u_2 &= u_0 \oplus u_3 \oplus c_0 \\ u_2 &= u_0 \oplus u_1 \oplus c_1 \\ u_2 &= u_1 \oplus u_3 \oplus c_2 \\ u_3 &= u_1 \oplus c_0 \oplus c_1 \\ u_3 &= u_0 \oplus c_1 \oplus c_2 \end{aligned}$$

Vom utiliza aceste expresii pentru a calcula log-raporturile extrinseci. Vedem că pentru fiecare bit de informație, există cel puțin două expresii, dar ele nu sunt statistic independente, căci includ variabile comune. De exemplu, ambele expresii pentru u_0 depind de c_2.

Pentru simplitate, în acest exemplu, considerăm că variația zgomotului σ^2 este egală cu 1, astfel încât

$$L_c(r_j) = 2r_j .$$

Să presupunem că emitem cuvântul de cod (1 1 0 0 1 0 1). Dacă exprimăm biții drept valori de tensiune +1 şi –1, secvența transmisă este: +1 +1 –1 –1 +1 –1 +1.

Codul bloc liniar sistematic (7,4) poate corecta o eroare pe cuvânt de cod, utilizând decodare fermă. Pentru a vedea ce se întâmplă dacă aplicăm o decodare suplă, să considerăm că zgomotul eronează nu unul, ci doi biți, secvența recepționată (la ieşirea demodulatorului) fiind:

0,75; 1,25; –0,93; 0,1; 0,83; –0,78; –0,15.

Biții sunt emişi cu aceeaşi probabilitate, astfel încât $L(d_j) = 0$ pentru toți biții. Vom calcula mai întâi $L_c(r_j) = 2r_j$.

$$\begin{aligned} L_c(r_0) &= 1,5 \\ L_c(r_1) &= 2,5 \\ L_c(r_2) &= -1,86 \end{aligned} \qquad \begin{aligned} L_c(r_3) &= +0,2 \\ L_c(r_4) &= 1,66 \\ L_c(r_5) &= -1,56 \\ L_c(r_6) &= -0,3. \end{aligned}$$

Operația notată cu $\boxplus$ fiind asociativă, din (6.61) obținem:

$$L(d_1) \boxplus L(d_2) \boxplus L(d_3) =$$

$$= \operatorname{sgn}[L(d_1)] \times \operatorname{sgn}[L(d_2)] \times \operatorname{sgn}[L(d_3)] \times \min(|L(d_1)|, |L(d_2)|, |L(d_3)|).$$

Calculăm log-raportul de probabilitate extrinsec pentru cei patru biți de informație. Pentru u_0, avem două posibilități. Utilizând ecuația

$$u_0 = u_1 \oplus c_0 \oplus c_2$$

avem

$$L_e(u_0) = L_c(r_0) \boxplus L_c(r_2) \boxplus L_c(r_4) = -1{,}5\,.$$

Cu ecuația

$$u_0 = u_3 \oplus c_1 \oplus c_2$$

avem

$$L_e(u_0) = L_c(r_1) \boxplus L_c(r_2) \boxplus L_c(r_6) =$$

$$= (+)(-)(-1)\min(2{,}5;\ 1{,}86;\ 0{,}3) = +0{,}3$$

Cu prima valoare calculată, obținem corectarea erorii de bit din locul $c_3 = u_0$, căci

$$L(\hat{u}_0) = L_c(u_0) + L_e(u_0) = 0{,}1 - 1{,}5 = -1{,}4$$

$$\text{sgn}\,(-1{,}4) = -1 \quad \text{(corect)}$$

Cu cea de a doua ecuație, în care intervine un alt bit eronat, c_6, s-ar obține o decodare greșită. Totuşi, comparând fiabilitățile, fiindcă 1,5 > 0,3, se alege soluția dată de prima ecuație.
Pentru bitul u_1, cu ecuația:

$$u_1 = u_3 \oplus c_0 \oplus c_1$$

obținem

$$L_e(u_1) = L_c(r_0) \boxplus L_c(r_1) \boxplus L_c(r_6)$$

$$= -\min(1{,}5;\ 2{,}5;\ 0{,}3) = -0{,}3$$

Cu aceasta,

$$L(\hat{u}_1) = L_c(u_1) + L_e(u_1) = 1{,}66 - 0{,}3 = 1{,}36$$

Decodarea se face corect, deşi contribuția extrinsecă este negativă. Cu ecuația a doua,

$$u_1 = u_0 \oplus c_0 \oplus c_2$$

avem

$$L_e(u_1) = L_c(r_0) \boxplus L_c(r_2) \boxplus L_c(r_3) = -\min(1{,}5;\ 1{,}86;\ 0{,}2) = -0{,}2\,.$$

Deci

$$L(\hat{u}_1) = L_c(u_1) + L_e(u_1) = 1{,}66 - 0{,}2 = 1{,}46$$

Şi cu a doua ecuație, contribuția extrinsecă a redus fiabilitatea deciziei, care rămâne însă corectă.

Pentru u_2, cu prima ecuație,

$$u_2 = u_0 \oplus u_3 \oplus c_0$$

avem

$$L_e(u_2) = L_c(r_0) \boxplus L_c(r_3) \boxplus L_c(r_6) = -\min(1{,}5;\ 0{,}2;\ 0{,}3) = -0{,}2$$

Deci

$$L(\hat{u}_2) = L_c(u_2) + L_e(u_2) = -1{,}55 - 0{,}2 = -1{,}75\,.$$

Aceasta ne dă decodarea corectă $\hat{u}_2 = -1$.

Cu ecuația a doua,

$$u_2 = u_0 \oplus u_1 \oplus c_1$$

avem

$$L_e(u_2) = L_c(r_3) \boxplus L_c(r_4) \boxplus L_c(r_1) = +\min(2{,}5;\ 0{,}2;\ 1{,}66) = 0{,}2$$

Deci

$$L(\hat{u}_2) = -1{,}55 + 0{,}2 = -1{,}35.$$

Deşi dă decodare corectă, nu este luată în considerare căci fiabilitatea 1,35 este mai mică decât cea dinainte, de 1,75.

Avem şi o a treia ecuație:

$$u_2 = u_1 \oplus u_3 \oplus c_2\,.$$

Cu aceasta,

$$L_e(u_2) = L_c(r_2) \boxplus L_c(r_4) \boxplus L_c(r_6) = \min(1{,}86;\ 1{,}66;\ 0{,}3) = 0{,}3\,.$$

Cu ea,

$$L(\hat{u}_2) = -1{,}55 + 0{,}3 = -1{,}25\,.$$

Se obține o decizie corectă, dar fiabilitatea rămâne inferioară celei asigurate de prima ecuație. În sfârşit, pentru u_3, cu prima ecuație,

$$u_3 = u_1 \oplus c_0 \oplus c_1$$

avem:

$$L_e(u_3) = L_c(r_0) \boxplus L_c(r_1) \boxplus L_c(r_4) = \min(1{,}5;\ 2{,}5;\ 1{,}66) = 1{,}5\,.$$

Deci

$$L(\hat{u}_3) = L_c(u_3) + L_e(u_3) = -0{,}3 + 1{,}5 = 1{,}2\,.$$

Această valoare asigură decodarea corectă a unui bit care a fost recepționat eronat (–0,15).
Cu a doua ecuație,

$$u_3 = u_0 \oplus c_1 \oplus c_2$$

$$L_e(u_3) = L_c(r_1) \boxplus L_c(r_2) \boxplus L_c(r_3) = -\min(2{,}5;\ 1{,}86;\ 0{,}2) = -0{,}2\,.$$

Aceasta ne dă

$$L(\hat{u}_3) = -0{,}3 - 0{,}2 = -0{,}5$$

ceea ce ar duce la o decodare greşită a bitului u_3, dar fiabilitatea 0,5 este mai mică decât a celeilalte decizii, cea corectă, care este deci preferată.

Prin acest exemplu, am arătat că se pot corecta două erori de bit dintr-un cuvânt de cod de şapte biți, ceea ce nu este posibil cu o decodare fermă, de tip algebric.

6.9. MODIFICĂRI SIMPLE ALE UNUI COD LINIAR

Nu toate codurile bloc liniare (*n,k*) sunt la fel de performante. Pentru o lungime dată *k* a blocului de mesaj, capacitatea de detecție şi de corecție a unui cod bloc este determinată de numărul biților de control (*n–k*). De exemplu, pentru *k* = 4, am văzut că lungimea minimă a cuvântului de cod *n* trebuie să fie 7 pentru a se putea corecta o eroare de bit. Dacă inginerul ce proiectează un sistem de comunicație intenționează să-i mărească fiabilitatea prin utilizarea unui cod detector şi corector de erori, nu este neapărat să elaboreze un cod *ad hoc*, căci poate găsi coduri „bune“ în cărțile de teoria codării, cu condiția ca un astfel de cod performant să se potrivească aplicației date. Să presupunem că sursa debitează biții deja grupați în blocuri de o anumită lungime, de exemplu, 8. Atunci este, desigur, avantajos să alegem un cod pentru care *k* este egal cu această lungime. Ce facem însă dacă nu găsim aşa ceva?

Ei bine, prin modificări simple, un cod deja proiectat poate fi refolosit într-o aplicație particulară. În cazul unui cod liniar, orice modificare corespunde unei schimbări operate asupra matricei generatoare **G**: putem adăuga sau elimina o linie sau o coloană, sau şi o linie şi o coloană.

Mărirea lungimii cuvântului de cod n se numeşte *extindere*, iar acesta se poate face în două feluri: prin *lungire* dacă se măreşte k sau prin *expandare* dacă se măreşte $(n–k)$.

Există şase schimbări de bază ce se pot face:

1. *Expandarea* unui cod este mărirea lungimii prin adăugarea mai multor biți de control. Prin aceasta, creşte dimensiunea mai mare a matricei generatoare.
2. *Lungirea* unui cod este mărirea lungimii prin adăugarea mai multor biți de informație. Prin aceasta, ambele dimensiuni ale matricei generatoare cresc cu acelaşi număr.
3. *Puncturarea* unui cod este reducerea lungimii prin eliminarea unor biți de control. Prin aceasta, dimensiunea mai mare a matricei generatoare descreşte.
4. *Scurtarea* unui cod este reducerea lungimii prin eliminarea unor biți de informație. Prin aceasta, ambele dimensiuni ale matricei generatoare descresc cu acelaşi număr.
5. *Augmentarea* unui cod este mărirea numărului biților de informație fără a schimba lungimea. Prin aceasta, creşte dimensiunea mai mică a matricei generatoare.
6. *Expurgarea* unui cod este micşorarea numărului biților de informație fără a schimba lungimea. Prin acesta, scade dimensiunea mai mică a matricei generatoare.

Deseori, un cod bloc (n,k) se notează (n,k,d_H), unde d_H este distanța Hamming minimă. Orice cod binar (n,k,d_H) pentru care distanța minimă d_H este un număr natural impar poate fi expandat pentru a obține un cod $(n+1,k,d_H+1)$ prin adăugarea unui bit care să fie suma modulo 2 a tuturor celor n componente ale cuvântului de cod. Aceasta este din cauză că, dacă un cuvânt de cod din codul inițial are pondere impară, noul bit va fi un unu. Iată de ce, toate cuvintele de cod de pondere d_H devin cuvinte de cod de pondere d_H+1.