CAPITOLUL 8

CODURI BLOC PARTICULARE

Anumite subclase de coduri bloc prezintă un interes deosebit. În acest capitol, se introduc câteva astfel de coduri bloc, cu mențiunea că studiul lor aprofundat depăşeşte cu mult obiectivele unui curs universitar de inițiere. Mai înainte însă, vom introduce corpul Galois $CG(2^m)$.

8.1. CORPUL GALOIS $CG(2^m)$

Până acum, trebuie să recunoaştem, ne-am descurcat cu o matematică destul de simplă. Unitățile de informație sunt biții, adică, simboluri binare, în sensul că un bit poate lua una din două valori, să spunem 0 şi 1. Cum, cu această convenție, nu avem numărul 2, 1+1=1–1= 0. Dar numai cu atât, nu prea avem cum să punem în evidență coduri performante care, pe lângă caracteristicile generale, trebuie să posede şi anumite calități particulare. Teoria codării se foloseşte intens de un capitol al matematicii numit „structuri algebrice“. Din fericire pentru noi, structurile algebrice se studiază în liceu în clasa a XII-a destul de bine, chiar dacă nu epuizează subiectul. Astfel încât, vom începe prin a ne reaminti ce este un *corp*.

Fie o mulțime F de elemente între care definim două operații, numite convențional adunare „+“ şi înmulțire „·“. Am spus „convențional“ întrucât aceste operații nu coincid neapărat cu cele cunoscute din matematica elementară. Această mulțime F împreună cu cele două operații + şi · are structură algebrică de *corp* dacă sunt îndeplinite următoarele condiții :

C1) F este grup comutativ sub adunarea +. Elementul neutru cu privire la adunare se numeşte elementul *zero* şi se notează cu 0.

C2) Mulţimea elementelor diferite de 0 din *F* este un grup comutativ sub înmulţire ·. Elementul neutru cu privire la înmulţire se numeşte elementul *unitate* şi se notează cu 1.

C3) Înmulţirea este distributivă în raport cu adunarea, adică, pentru oricare trei elemente *a*, *b* şi *c* din *F*,

$$a\cdot(b+c) = a\cdot b+a\cdot c$$

Exemple de corpuri cu care suntem familiarizaţi sunt mulţimea numerelor reale **R** şi mulţimea numerelor complexe **C**. Mulţimea numerelor naturale **N** şi mulţimea numerelor întregi **Z** nu sunt corpuri, căci nu este îndeplinită condiţia C2.

Mulţimile **R** şi **C** sunt infinite. În teoria codării, ne interesează însă mai mult mulţimile finite. Un *corp finit* este un corp cu un număr finit de elemente. Numărul de elemente dintr-un corp se numeşte *ordinul* corpului. Din definiţia corpului, rezultă că el trebuie să aibă cel puţin două elemente, elementul neutru pentru adunare şi elementul neutru pentru înmulţire. Un corp finit se mai numeşte şi corp Galois. Corpul Galois CG (2) este de ordin 2, căci are două elemente, 0 şi 1. Cele două operaţii se numesc în acest caz adunare modulo 2 şi înmulţire modulo 2, iar regulile sunt date în Tabelul 8.1, respectiv în Tabelul 8.2.

Tabelul 8.1

Adunare modulo 2

+	0	1
0	0	1
1	1	0

Tabelul 8.2

Înmulţire modulo 2

·	0	1
0	0	0
1	0	1

În logica binară, „adevărat“ şi „fals“ corespund lui 1, respectiv lui 0, iar operaţiile de adunare şi de înmulţire modulo 2 sunt realizate cu funcţiile logice SAU EXCLUSIV, respectiv ŞI.

Ordinul unui corp finit este un număr prim *p*. Numărul 2 este prim deşi este par. Pentru orice număr prim *p*, există un corp finit cu *p* elemente. Pentru orice număr natural *m*, este posibil să extindem corpul *CG*(*p*) cu *p* prim la un corp cu p^m elemente, numit *corp de extensie* al lui *CG*(*p*) şi notat cu $CG(p^m)$. Reciproc, ordinul oricărui corp finit este o putere a unui număr prim.

Fie un corp finit cu q elemente, $CG(q)$. Să formăm următorul şir de sume de 1, elementul unitate din $CG(2)$:

$$\sum_{i=1}^{1}1=1,\ \sum_{i=1}^{2}1=1+1,\ \sum_{i=1}^{3}1=1+1+1,\cdots,\sum_{i=1}^{k}1=1+1+\cdots+1 \quad (de\ k\ ori),\cdots$$

Întrucât corpul este o mulțime închisă sub adunare, aceste sume trebuie să fie elemente din corp. Dar corpul având un număr finit de elemente, aceste sume nu pot fi toate distincte: rezultatul unei asemenea sume va fi acelaşi ca al unei sume precedente. Trebuie, deci, să existe două numere naturale m şi n astfel încât

$$\sum_{i=1}^{m}1=\sum_{i=1}^{n}1.$$

Aceasta înseamnă că $\sum_{i=0}^{n-m}1=0$. Iată de ce, trebuie să existe un cel mai mic număr natural λ astfel încât $\sum_{i=1}^{\lambda}1=0$. Acest număr natural λ se numeşte *caracteristica* lui $CG(q)$. Caracteristica lui $CG(2)$ este 2, căci 1+1 = 0. În general, caracteristica λ a unui corp finit este un număr prim.

Fie acum a un element din $CG(q)$ diferit de zero. Dar mulțimea elementelor lui CG(q) care sunt diferite de zero este închisă sub înmulțire, astfel încât puterile lui a, $a^1=a,\ a^2=a\cdot a,\ a^3=a\cdot a\cdot a,\cdots$ trebuie să fie elemente diferite de zero din $CG(q)$. Întrucât $CG(q)$ are numai un număr finit de elemente, puterile lui a nu pot fi toate distincte. Pentru două numere naturale k şi m, cu $m > k$, trebuie să avem deci $a^k = a^m$. Fie a^{-1} inversul lui a pentru înmulțire. Inversul lui a^k este $(a^{-1})^k = a^{-k}$. Înmulțind în ambii membri cu a^{-k}, obținem că:

$$1=a^{m-k}.$$

Prin urmare, există un cel mai mic număr natural n astfel încât $a^n=1$. Acest număr natural n se numeşte *ordinul* elementului a din corp. Puterile $a^1,a^2,\cdots,a^{n-1},a^n=1$ sunt toate distincte şi formează un grup sub operația de înmulțire definită în $CG(q)$.

TEOREMA 8.1: Fie a un element diferit de zero al corpului Galois $CG(q)$. Atunci $a^{q-1}=1$.

DEMONSTRAȚIE

Fie $b_1, b_2, \cdots, b_{q-1}$ cele (q–1) elemente diferite de zero ale lui C. Este evident că cele (q–1) elemente $a \cdot b_1, a \cdot b_2, \cdots, a \cdot b_{q-1}$ sunt diferite de zero şi distincte. Prin urmare,

$$\begin{aligned} (a \cdot b_1) \cdot (a \cdot b_2) \cdot \cdots \cdot (a \cdot b_{q-1}) &= b_1 \cdot b_2 \cdot \cdots \cdot b_{q-1} \\ a^{q-1} \cdot (b_1 \cdot b_2 \cdot \cdots \cdot b_{q-1}) &= b_1 \cdot b_2 \cdot \cdots \cdot b_{q-1} \end{aligned} \tag{8.1}$$

Fiindcă $a \neq 0$ şi $(b_1 \cdot b_2 \cdot \cdots \cdot b_{q-1}) \neq 0$, trebuie să avem $a^{q-1} = 1$.

TEOREMA 8.2: Fie a un element diferit de zero dintr-un corp Galois $CG(q)$. Fie n ordinul lui a. Atunci n divide (q–1).

DEMONSTRAȚIE

Să presupunem că n nu divide (q–1). Împărțind (q–1) la n, obținem:

$$q - 1 = kn + r \tag{8.2}$$

unde $0 < r < n$. Atunci:

$$a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r = (a^n)^k \cdot a^r \tag{8.3}$$

Fiindcă $a^{q-1} = 1$ şi $a^n = 1$, trebuie să avem $a^r = 1$. Dar acest lucru este imposibil, căci $0 < r < n$ iar n este cel mai mic număr natural astfel încât $a^n = 1$. Prin urmare, n trebuie să dividă (q–1).

Într-un corp Galois $CG(q)$, un element diferit de zero a se spune că este *primitiv* dacă ordinul lui a este (q–1). Iată de ce, puterile unui element primitiv generează toate elementele diferite de zero ale lui $CG(q)$. Fiecare corp finit are un element primitiv.

Fie un polinom $g(X)$ definit pe $CG(2)$:

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_m X^m. \tag{8.4}$$

Dacă $g(X)$ are un număr par de termeni, el este divizibil cu $X + 1$, căci înlocuind în (8.4) X cu 1, suma efectuându-se modulo 2, rezultatul este 0. Un polinom $p(X)$ de grad m definit pe $CG(2)$ se spune că este *ireductibil* pe $CG(2)$ dacă $p(X)$ nu este divizibil cu nici un polinom definit pe $CG(2)$ de grad mai mic decât m dar mai mare decât zero. Un polinom ireductibil $p(X)$ de grad m se spune că este *primitiv* dacă cel mai mic număr natural n pentru care $p(X)$ divide $(X^n + 1)$ este $n = 2^m - 1$.

Vom deduce acum o proprietate interesantă şi utilă a polinoamelor cu coeficienți în $CG(2)$. Să ridicăm la pătrat polinomul $p(X)$ definit în (8.4).

$$\begin{aligned} g^2(X) &= \left(g_0 + g_1X + \cdots + g_mX^m\right)^2 \\ &= \left[g_0 + \left(g_1X + g_2X^2 + \cdots + g_mX^m\right)\right]^2 \\ &= g_0^2 + g_0 \cdot \left(g_1X + g_2X^2 + \cdots + g_mX^m\right) + \\ &+ g_0 \cdot \left(g_1X + g_2X^2 + \cdots + g_mX^m\right) + \\ &+ \left(g_1X + g_2X^2 + \cdots + g_mX^m\right)^2 = \\ &= g_0^2 + \left(g_1X + g_2X^2 + \cdots + g_mX^m\right)^2. \end{aligned} \tag{8.5}$$

Dezvoltând ecuația (8.5) repetat, în cele din urmă obținem:

$$g^2(X) = g_0^2 + (g_1X)^2 + \left(g_2X^2\right)^2 + \cdots + \left(g_mX^m\right)^2. \tag{8.6}$$

Dar $g_i = 0$ sau 1, astfel încât $g_i^2 = g_i$. Prin urmare, avem:

$$g^2(X) = g_0 + g_1X^2 + g_2\left(X^2\right)^2 + \cdots + g_m\left(X^2\right)^2 = g\left(X^2\right) \tag{8.7}$$

Din (8.7) urmează că, pentru orice număr natural *l*,

$$\left[g(X)\right]^{2^l} = g\left(X^{2^l}\right). \tag{8.8}$$

Înainte de a arăta cum se construieşte corpul de extensie cu 2^m elemente al corpului binar *CG*(2), să ne reamintim cum se ajunge la construcția corpului numerelor complexe **C** plecând de la corpul numerelor reale **R**. Fie trinomul de gradul doi:

$$T(x) = ax^2 + bx + c \tag{8.9}$$

unde *a, b* şi *c* sunt numere reale. Se ştie că, pentru $b^2 - 4ac < 0$, $T(x)$ nu are rădăcini în corpul numerelor reale. Introducând un nou element $i = \sqrt{-1}$, $T(x)$ va avea întotdeauna rădăcini, dar nu în **R**, ci în **C**.

Vom proceda asemănător pentru a construi corpul Galois de extensie cu 2^m elemente. La cele două elemente 0 şi 1 ale lui *CG*(2), adăugăm un nou simbol α şi definim înmulțirea „·“ astfel:

$$\begin{aligned} &0 \cdot 0 = 0 \\ &0 \cdot 1 = 1 \cdot 0 = 0 \\ &1 \cdot 1 = 1 \\ &0 \cdot \alpha = \alpha \cdot 0 = 0 \\ &1 \cdot \alpha = \alpha \cdot 1 = \alpha \end{aligned} \tag{8.10}$$

În continuare, definim un şir de puteri:

$$\begin{aligned}
&\alpha^2 = \alpha \cdot \alpha \\
&\alpha^3 = \alpha \cdot \alpha \cdot \alpha \\
&\vdots \\
&\alpha^j = \alpha \cdot \alpha \cdot \cdots \cdot \alpha \quad (\textbf{de } j \textbf{ ori}) \\
&\vdots
\end{aligned} \tag{8.11}$$

Din definiția de mai sus a înmulțirii, urmează că:

$$\begin{aligned}
&0 \cdot \alpha^j = \alpha^j \cdot 0 = 0 \\
&1 \cdot \alpha^j = \alpha^j \cdot 1 = \alpha^j \\
&\alpha^i \cdot \alpha^j = \alpha^j \cdot \alpha^i = \alpha^{i+j}
\end{aligned} \tag{8.12}$$

Avem acum următoarea mulțime de elemente pe care am definit operația „$\cdot$“:

$$F = \{0,1,\alpha,\alpha^2,\cdots,\alpha^j,\cdots\}. \tag{8.13}$$

Punem condiția ca mulțimea F să conțină numai 2^m elemente şi să fie închisă sub operația de înmulțire „$\cdot$“. Fie $p(X)$ un polinom primitiv de grad m cu coeficienți în $CG(2)$. Conform definiției polinomului primitiv, avem

$$X^{2^m-1} + 1 = q(X)p(X). \tag{8.14}$$

Punem condiția ca

$$p(\alpha) = 0. \tag{8.15}$$

Înlocuind în (8.14) X cu α şi ținând seama de (8.15), obținem

$$\alpha^{2^m-1} + 1 = q(\alpha) \cdot 0 \tag{8.16}$$

Dacă vom considera $q(\alpha)$ drept un polinom de α cu coeficienți în $CG(2)$, $q(\alpha) \cdot 0 = 0$. În definitiv, obținem următoarea egalitate:

$$\alpha^{2^m-1} + 1 = 0. \tag{8.17}$$

Adunând 1 la ambii membri ai lui (8.17) şi utilizând adunarea modulo 2, obținem:

$$\alpha^{2^m-1} = 1. \tag{8.18}$$

Prin urmare, cu condiția ca $p(\alpha) = 0$, mulțimea F devine finită şi conține următoarele elemente:

$$F = \{0,1,\alpha,\alpha^2,\cdots,\alpha^{2^m-2}\}. \tag{8.19}$$

Se verifică uşor că elementele diferite de zero din F formează un grup de ordin (2^m-1) pentru operaţia de înmulţire „·“, elementul neutru fiind $\alpha^0=\alpha^{2^m-1}=1$.

Vom defini şi o operaţie de adunare „+“ astfel încât F să formeze un grup comutativ sub această operaţie. Pentru $0\le i<2^m-1$, împărţim polinomul X^i la $p(X)$ şi obţinem:

$$X^i=q_i(X)p(X)+a_i(X). \tag{8.20}$$

Polinomul rest $a_i(X)$ cu coeficienţi în $CG(2)$ are grad $(m-1)$ sau mai mic şi este de forma următoare:

$$a_i(X)=a_{i0}+a_{i1}X+a_{i2}X^2+\cdots+a_{i,m-1}X^{m-1}. \tag{8.21}$$

Polinoamele X şi $p(X)$ sunt relativ prime, astfel încât, pentru orice $i\ge 0$,

$$a_i(X)\ne 0. \tag{8.22}$$

Pentru $0\le i,\ j<2^m-1$ şi $i\ne j$, vom arăta că:

$$a_i(X)\ne a_j(X). \tag{8.23}$$

Într-adevăr, în ipoteza că $a_i(X)=a_j(X)$, din (8.20) urmează că:

$$\begin{aligned} X^i+X^j&=\left[q_i(X)+q_j(X)\right]p(X)+a_i(X)+a_j(X)\\ &=\left[q_i(X)+q_j(X)\right]p(X)\end{aligned} \tag{8.24}$$

Presupunând că $j>i$, ar rezulta că $p(X)$ divide $X^i+X^j=X^i\left(1+X^{j-i}\right)$. Acest lucru este însă imposibil căci $j-i<2^m-1$ iar $p(X)$ este un polinom primitiv de grad m care nu divide X^n+1 pentru $n<2^m-1$. Aşadar, ipoteza noastră că $a_i(X)=a_j(X)$ este nefondată. Deci, pentru $i=0,1,2,\cdots,2^m-1$, obţinem 2^m-1 polinoame diferite de zero şi distincte $a_i(X)$ de grad $(m-1)$ sau mai mic. Înlocuind aici X cu α în (8.20) şi ţinând seama că $p(\alpha)=0$, obţinem următoarea expresie polinomială pentru α^i :

$$\alpha^i=a_i(\alpha)=a_{i_0}+a_{i_1}\alpha+a_{i_2}\alpha^2+\cdots+a_{i,m-1}\alpha^{m-1} \tag{8.25}$$

Prin urmare, cele 2^m-1 elemente diferite de zero, $\alpha^0,\alpha^1,\cdots,\alpha^{2^m-2}$, din F sunt reprezentate de 2^m-1 polinoame de α diferite de zero şi distincte

cu coeficienţi în CG (2) şi având grad (m–1) sau mai mic. Elementul 0 din F poate fi reprezentat de polinomul zero. Definim acum o adunare „+“ după cum urmează :

$$0+0 = 0 \tag{8.26.a}$$

Pentru $0 \le i, j < 2^m - 1$,

$$0 + \alpha^i = \alpha^i + 0 = \alpha^i \tag{8.26.b}$$

$$\begin{aligned} \alpha^i + \alpha^j &= \left(a_{i_0} + a_{i_1}\alpha + \cdots + a_{i,m-1}\alpha^{m-1}\right) + \left(a_{j_0} + a_{j_1}\alpha + \cdots + a_{j,m-1}\alpha^{m-1}\right) \\ &= \left(a_{i_0} + a_{j_1}\right) + \left(a_{i_1} + a_{j_1}\right)\alpha + \cdots + \left(a_{i,m-1} + a_{j,m-1}\right)\alpha^{m-1} \end{aligned} \tag{8.26.c}$$

Operaţia $a_{i,l} + a_{j,l}$ se efectuează modulo 2. Din (8.26.c), se vede că, pentru $i=j$,

$$\alpha^i + \alpha^i = 0 \tag{8.27}$$

şi că, pentru $i \ne j$,

$$\left(a_{i_0} + a_{j_1}\right) + \left(a_{i_1} + a_{j_1}\right)\alpha + \cdots + \left(a_{i,m-1} + a_{j,m-1}\right)\alpha^{m-1}$$

este diferit de zero şi trebuie deci să fie expresia polinomială pentru un α^k din F. Este uşor de verificat că F este grup comutativ sub „+“, cu 0 drept element neutru. Utilizând reprezentarea polinomială pentru elementele din F, se vede că înmulţirea este distributivă faţă de adunare. Iată de ce, mulţimea $F = \left\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\right\}$ este un corp Galois cu 2^m elemente, notat cu $CG(2^m)$. Este evident că $CG(2)$ este un subcorp al lui $CG(2^m)$. În mod obişnuit, corpul binar CG(2) se numneşte corpul de *bază* al lui $CG(2^m)$. Caracteristica lui $CG(2^m)$ este 2.

Construind corpul de extensie $CG(2^m)$ din $CG(2)$, am elaborat două reprezentări pentru elementele diferite de zero din F : reprezentarea ca serie de puteri, convenabilă pentru înmulţire şi reprezentarea polinomială, convenabilă pentru adunare.

EXEMPLUL 8.1: Fie m = 4. Polinomul $p(X) = 1 + X + X^4$ este primitiv pe $CG(2)$. Facem $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, de unde $\alpha^4 = 1 + \alpha$. Utilizând această identitate repetat, putem construi $CG(2^4)$. Elementele lui $CG(2^4)$ sunt date în Tabelul 8.1.

Tabelul 8.1

Trei reprezentări pentru elementele corpului Galois CG(2^4) generat de $p(X) = 1 + X + X^4$

Reprezentare prin puteri	Reprezentare polinomială	Reprezentare drept 4-tuplu
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

Spre exemplu,

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha(1+\alpha) = \alpha + \alpha^2$$
$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$$
$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3.$$

Pentru a înmulți două elemente α^i şi α^j, adunăm exponenții şi utilizăm faptul că $\alpha^{15} = 1$. Spre exemplu, $\alpha^6 \cdot \alpha^7 = \alpha^{13}$ şi $\alpha^{11} \cdot \alpha^7 = \alpha^{18} = \alpha^3$. Pentru a împărți α^j la α^i, înmulțim α^j cu inversul multiplicativ α^{15-i} al lui α^i. Spre exemplu, $\alpha^4 / \alpha^{12} = \alpha^4 \cdot \alpha^3 = \alpha^7$.

În tabelul 8.1, se arată şi o altă reprezentare pentru elementele corpului Galois $CG(2^m)$. Astfel, dacă $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ este reprezentarea polinomială a unui element, îl putem reprezenta pe acesta şi drept un şir ordonat de m componente, numit m-tuplu, astfel :

$$(a_0, a_1, a_2, \cdots, a_{m-1}).$$

Vom vedea în continuare câteva proprietăți de bază ale corpului Galois $CG(2^m)$.

TEOREMA 8.3: Fie *g(X)* un polinom cu coeficienți din *CG*(2). Fie β un element dintr-un corp de extensie al lui *CG* (2). Dacă β este o rădăcină a lui *g(X)*, atunci şi β^{2^l} este o rădăcină a aceluiaşi polinom, pentru orice număr natural *l*.

DEMONSTRAȚIE
Înlocuind β în ecuația (8.8) obținem

$$[g(\beta)]^{2^l} = g\left(\beta^{2^l}\right) \tag{8.28}$$

Dar întrucât $g(\beta) = 0$, avem şi că $g\left(\beta^{2^l}\right) = 0$, ceea ce arată că β^{2^l} este rădăcină a lui $g(X)$.

Elementul β^{2^l} se numeşte conjugat al lui β. Teorema 8.3 ne spune că, dacă β, un element din $CG(2^m)$, este o rădăcină a unui polinom *g(X)* cu coeficienți din *CG*(2), toate conjugatele distincte ale lui β, şi ele elemente din $CG(2^m)$, sunt de asemenea rădăcini ale lui $g(X)$.

TEOREMA 8.4: Cele 2^m–1 elemente diferite de zero ale lui $CG(2^m)$ formează toate rădăcinile lui $X^{2^m-1}+1$.

DEMONSTRAȚIE
Fie β un element diferit de zero din corpul Galois $CG(2^m)$. Conform Teoremei 8.1, avem atunci

$$\beta^{2^m-1} = 1 \tag{8.29}$$

Adunând 1 în ambii membri ai ecuației (8.29), obținem

$$\beta^{2^m-1} + 1 = 0 \tag{8.30}$$

Ecuația (8.30) spune că β este o rădăcină a polinomului $X^{2^m-1}+1$. Prin urmare, orice element diferit de zero al lui $CG(2^m)$ este o rădăcină a lui $X^{2^m-1}+1$. Întrucât gradul acestui polinom este (2^m–1), cele (2^m–1) elemente diferite ale lui $CG(2^m)$ formează toate rădăcinile lui $X^{2^m-1}+1$.

COROLAR 8.4.1: Elementele lui $CG(2^m)$ formează toate rădăcinile polinomului $X^{2^m} + X$.

Fie $\phi(X)$ polinomul cu coeficienți din $CG(2)$ de gradul cel mai mic astfel încât $\phi(\beta)=0$. Acest polinom se numește *polinomul minimal* al lui β.

TEOREMA 8.5: Polinomul minimal $\phi(X)$ al unui element β al corpului este ireductibil.

DEMONSTRAȚIE
Să presupunem că $\phi(X)$ nu este ireductibil, astfel că $\phi(X)=\phi_1(X)\phi_2(X)$, unde $\phi_1(X)$ şi $\phi_2(X)$ au grade mai mari decât 0 dar mai mici decât gradul lui $\phi(X)$. Întrucât $\phi(\beta)=\phi_1(\beta)\phi_2(\beta)=0$, fie $\phi_1(\beta)=0$, fie $\phi_2(\beta)=0$. Dar aceasta contrazice ipoteza că $\phi(X)$ este un polinom de cel mai mic grad astfel încât $\phi(\beta)=0$. Prin urmare, $\phi(X)$ trebuie să fie ireductibil.

TEOREMA 8.6: Fie $g(X)$ un polinom cu coeficienți din $CG(2)$. Fie $\phi(X)$ polinomul minimal al unui element β al corpului de extensie. Dacă β este o rădăcină a lui $g(X)$, atunci acest $g(X)$ este divizibil cu $\phi(X)$.

DEMONSTRAȚIE
Înpărțind $g(X)$ la $\phi(X)$, obținem:

$$g(X)=q(X)\phi(X)+r(X) \tag{8.31}$$

În (8.31), gradul restului $r(X)$ este mai mic decât gradul lui $\phi(X)$. Înlocuind β în (8.31) şi având în vedere că $g(\beta)=\phi(\beta)=0$, rezultă că $r(\beta)=0$. Dacă $r(X)\neq 0$, $r(X)$ ar fi un polinom de grad mai mic decât $\phi(X)$ care are β drept rădăcină. Dar aceasta contrazice faptul că $\phi(X)$ este polinomul minimal al lui β. Prin urmare, $r(X)$ trebuie să fie identic cu 0, aşa încât $\phi(X)$ divide $g(X)$.

TEOREMA 8.7: Polinomul minimal $\phi(X)$ al unui element β din $CG(2^m)$ divide $X^{2^m}+X$.

DEMONSTRAȚIE
Aceasta rezultă din corolarul 8.4.1 şi din teorema 8.7.

TEOREMA 8.8: Fie $f(X)$ un polinom ireductibil pe $CG(2^m)$. Fie $\phi(X)$ polinomul minimal al lui β. Dacă $f(\beta)=0$, atunci $\phi(X)=f(X)$.

DEMONSTRAȚIE
Din teorema 8.7, urmează că $\phi(X)$ divide $f(X)$. Întrucât $\phi(X)\neq 1$, iar $f(X)$ este ireductibil, trebuie să avem $\phi(X)=f(X)$.

TEOREMA 8.9: Fie β un element din $CG(2^m)$ şi fie s cel mai mic număr natural astfel încât $\beta^{2^s}=\beta$. Atunci

$$f(X)=\prod_{i=0}^{s-1}\left(X+\beta^{2^i}\right)$$

este un polinom ireductibil pe $CG(2)$.

DEMONSTRAȚIE
Ridicăm la pătrat polinomul $f(X)$:

$$[f(X)]^2=\left[\prod_{i=0}^{s-1}\left(X+\beta^{2^i}\right)\right]^2=\prod_{i=0}^{s-1}\left(X+\beta^{2^i}\right)^2. \tag{8.32}$$

Avem:

$$\begin{aligned}\left(X+\beta^{2^i}\right)^2&=X^2+\left(\beta^{2^i}+\beta^{2^i}\right)X+\beta^{2^{i+1}}\\&=X^2+\beta^{2^{i+1}}\end{aligned}. \tag{8.33}$$

Din (8.32) şi (8.33), urmează că:

$$\begin{aligned}\left[f(X)\right]^2&=\prod_{i=0}^{s-1}\left(X^2+\beta^{2^{i+1}}\right)=\prod_{i=0}^{s}\left(X^2+\beta^{2^i}\right)\\&=\left[\prod_{i=1}^{s-1}\left(X^2+\beta^{2^i}\right)\left(X^2+\beta^{2^s}\right)\right]\end{aligned}. \tag{8.34}$$

Dar $\beta^{2^s}=\beta$, astfel încât:

$$[f(X)]^2=\prod_{i=0}^{s-1}\left(X^2+\beta^{2^i}\right)=f\left(X^2\right). \tag{8.35}$$

Fie:

$$f(X) = f_0 + f_1 X + \cdots + f_s X^s \tag{8.36}$$

unde $f_s = 1$. Să dezvoltăm

$$\begin{aligned} \left[f(X) \right]^2 &= \left(f_0 + f_1 X + \cdots + f_s X^s \right)^2 \\ &= \sum_{i=0}^{s} f_i^2 X^{2i} \end{aligned} \quad . \tag{8.37}$$

Din (8.35) şi (8.37), obținem:

$$\sum_{i=0}^{s} f_i X^{2i} = \sum_{i=0}^{s} f_i^2 X^{2i} \; . \tag{8.38}$$

Prin urmare, trebuie să avem:

$$f_i = f_i^2, \quad 0 \le i \le s \tag{8.39}$$

Egalitatea (8.39) este adevărată numai dacă $f_i = 0$ sau 1. Deci, $f(X)$ are coeficienții din *CG*(2).

Să presupunem însă că $f(X)$ n-ar fi ireductibil pe *CG*(2), astfel încât

$$f(X) = a(X) b(X). \tag{8.40}$$

Întrucât $f(\beta) = 0$, fie $a(\beta) = 0$, fie $b(\beta) = 0$. Dacă $a(\beta) = 0$, $a(X)$ are rădăcinile $\beta, \beta^2, \cdots, \beta^{2^{s-1}}$, astfel încât gradul său este s şi deci, $a(X) = f(X)$. Similar, dacă $b(\beta) = 0$, $b(X) = f(X)$. În concluzie, $f(X)$ trebuie să fie ireductibil.

TEOREMA 8.10: Fie $\phi(X)$ polinomul minimal al unui element β din *CG*(2). Fie s cel mai mic număr natural astfel încât $\beta^{2^s} = \beta$. Atunci

$$\phi(X) = \prod_{i=0}^{s-1} \left(X + \beta^{2^i} \right) \tag{8.41}$$

DEMONSTRAȚIE
Ecuația (8.41) este o consecință directă a teoremelor 8.8 şi 8.9.

EXEMPLUL 8.2: Să considerăm corpul Galois $CG(2^4)$ dat în tabelul 8.1. Fie $\beta = \alpha^3$. Conjugatele lui β sunt:

$$\beta^2 = \alpha^6, \quad \beta^{2^2} = \alpha^{12}, \quad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

Polinomul minimal al lui $\beta = \alpha^3$ este deci:

$$\phi(X) = \left(X + \alpha^3\right)\left(X + \alpha^6\right)\left(X + \alpha^{12}\right)\left(X + \alpha^9\right).$$

Efectuând înmulțirile din membrul drept al ecuației de mai sus cu ajutorul tabelului 8.1, obținem:

$$\begin{aligned}\phi(X) &= \left[X^2 + \left(\alpha^3 + \alpha^6\right)X + \alpha^9\right]\left[X^2 + \left(\alpha^{12} + \alpha^9\right)X + \alpha^{21}\right] \\ &= \left(X^2 + \alpha^2 X + \alpha^9\right)\left(X^2 + \alpha^8 X + \alpha^6\right) \\ &= X^4 + \left(\alpha^2 + \alpha^8\right)X^3 + \left(\alpha^6 + \alpha^{10} + \alpha^9\right)X^2 + \left(\alpha^{17} + \alpha^8\right)X + \alpha^{15} \\ &= X^4 + X^3 + X^2 + X + 1\end{aligned}$$

Există şi un alt mod de a găsi polinomul minimal al unui element al corpului, ilustrat în exemplul următor.

EXEMPLUL 8.3: Să presupunem că vrem să determinăm polinomul minimal $\phi(X)$ al lui $\gamma = \alpha^7$ din $CG(2^4)$. Conjugatele distincte ale lui γ sunt:

$$\gamma^4 = \alpha^{14}, \quad \gamma^{2^2} = \alpha^{28} = \alpha^{13}, \quad \gamma^{2^3} = \alpha^{56} = \alpha^{11}.$$

Prin urmare, $\phi(X)$ are grad 4 şi trebuie să fie de forma următoare:

$$\phi(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + X^4.$$

Înlocuind γ în $\phi(X)$, avem:

$$\phi(\gamma) = a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + \gamma^4 = 0.$$

Utilizând reprezentările polinomiale pentru $\gamma, \gamma^2, \gamma^3$ şi γ^4 în ecuația de mai sus obținem:

$$\begin{aligned}&a_0 + a_1\left(1 + \alpha + \alpha^3\right) + a_2\left(1 + \alpha^3\right) + a_3\left(\alpha^2 + \alpha^3\right) + \left(1 + \alpha^2 + \alpha^3\right) = 0 \\ &\left(a_0 + a_1 + a_2 + 1\right) + a_1\alpha + \left(a_3 + 1\right)\alpha^2 + \left(a_1 + a_2 + a_3 + 1\right)\alpha^3 = 0\end{aligned}$$

Pentru ca egalitatea de mai sus să fie adevărată, coeficienții trebuie să fie egali cu zero:

$$\begin{aligned}a_0 + a_1 + a_2 \qquad + 1 &= 0 \\ a_1 \qquad\qquad\quad &= 0 \\ a_3 + 1 &= 0 \\ a_1 + a_2 + a_3 + 1 &= 0\end{aligned}$$

Rezolvând sistemul de ecuații liniare de mai sus, obținem: $a_0 = 1, a_1 = a_2 = 0$ şi $a_3 = 1$. Prin urmare, polinomul minimal al lui $\gamma = \alpha^7$

este $\phi(X) = 1 + X^3 + X^4$. Toate polinoamele minimale ale elementelor din $CG(2^4)$ sunt date în tabelul 8.2.

Tabelul 8.2

Polinoamele minimale ale elementelor din $CG(2^4)$ generat de $p(X) = X^4 + X + 1$.

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

TEOREMA 8.11: Fie $\phi(X)$ polinomul minimal al unui element β din $CG(2^m)$. Fie s gradul lui $\phi(X)$.

Acest s este atunci cel mai mic număr natural astfel încât $\beta^{2^s} = \beta$. În afară de aceasta, $s \le m$.

DEMONSTRAȚIE
Rezultă direct din teorema 8.10.

Gradul polinomului minimal al oricărui element din $CG(2^m)$ divide m.

În construcția corpului Galois $CG(2^m)$, utilizăm un polinom primitiv $p(X)$ de grad m şi punem condiția ca elementul α să fie o rădăcină a lui $p(X)$. Întrucât puterile lui α generează toate elementele diferite de zero ale lui $CG(2^m)$, α este un element primitiv. Mai mult decât atât, toate conjugatele lui α sunt şi ele elemente primitive ale lui $CG(2^m)$.

8.2. CODURI HAMMING

Pentru orice număr natural $m \ge 3$, există un cod Hamming cu următorii parametri:

Lungimea codului: $n = 2^m - 1$

Numărul biților de informație: $k = 2^m - m - 1$

Numărul biților de control: $n - k = m$

Capacitatea de corecție a erorilor: $t = 1$

Distanța minimă: $d_{\min} = 3$.

Matricea de control **H** a acestui cod constă din toate *m*–tuplurile diferite de zero drept coloane. În formă sistematică, matricea **H** se scrie:

$$\mathbf{H} = [\mathbf{I}_m \ \mathbf{Q}], \tag{8.42}$$

unde $\mathbf{I}_m$ este matricea identitate $m \times m$ iar submatricea **Q** constă din $(2^m - m - 1)$ coloane care sunt *m*–tupluri de pondere 2 sau mai mare.

EXEMPLUL 8.4: Pentru $m = 3$, avem codul Hamming (7,4) cu matrice de control:

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

Recunoaştem că acesta este codul (7,4) dat în exemplul 6.1.

Un cod corector de *t* erori se numeşte *perfect* dacă liderii de coset din tabloul său standard sunt toți vectorii de eroare de *t* erori sau mai puține. Codurile perfecte sunt rare. Codurile Hamming formează o clasă de coduri perfecte ce corectează o singură eroare.

Codurile Hamming se pot pune şi în formă ciclică. Un cod Hamming ciclic de lungime $2^m - 1$ cu $m \geq 3$ este generat de un polinom primitiv $p(X)$ de grad *m*.

Matricea de control **H** se poate scrie mai compact lucrând într-un corp de extensie. Cu referire la exemplul 8.4, să identificăm coloanele matricei **H** cu elemente din $CG(2^3)$. Fie $a(\alpha) = a_0 + a_1\alpha + a_2\alpha^2$ reprezentarea polinomială a unui element al corpului Galois. Astfel, într-o coloană a matricei **H**, a_0 este prima componentă de sus, a_1 cea din mijloc iar a_2 cea de jos. Utilizând polinomul primitiv $p(X) = 1 + X + X^3$ pentru a construi $CG(2^3)$ şi punând condiția ca $p(\alpha) = 0$, matricea **H** devine:

$$\mathbf{H} = [\alpha^0 \ \ \alpha^1 \ \ \alpha^2 \ \ \alpha^3 \ \ \alpha^4 \ \ \alpha^5 \ \ \alpha^6].$$

Matricea de control este acum o matrice 1×7 definită pe corpul de extensie $CG(2^3)$. Pentru orice cuvânt de cod **v** definit pe $CG(2)$, trebuie să avem:

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

Acest mod de a gândi în corpul de extensie ne va uşura întelegerea codurilor BCH şi Reed – Solomon.

8.3. CODURI REED – MULLER

Pentru orice număr natural m şi pentru orice număr natural r mai mic decât m, există un cod Reed – Muller de lungime 2^m numit codul Reed – Muller de ordin r şi lungime 2^m.

Vom defini un cod Reed – Muller printr-o procedură de construcţie a unei matrice generatoare. În acest scop, să definim mai întâi *produsul* dintre doi vectori **a** şi **b** ca o înmulţire pe componente. Fie:

$$\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$$
$$\mathbf{b} = (b_0, b_1, \cdots, b_{n-1}).$$

Produsul este vectorul:

$$\mathbf{ab} = (a_0 b_0, a_1 b_1, \cdots, a_{n-1} b_{n-1}). \tag{8.43}$$

Matricea generatoare pentru codul Reed – Muller de ordin r şi lungime 2^m se defineşte drept un tablou de blocuri:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ . \\ . \\ . \\ \mathbf{G}_r \end{bmatrix}. \tag{8.44}$$

În (8.44), $\mathbf{G}_0$ este un vector de lungime $n = 2^m$ cu toate componentele egale cu unu, $\mathbf{G}_1$ este o matrice $m \times 2^m$ ale cărei coloane sunt toate m–tuplurile binare, iar $\mathbf{G}_l$ se construieşte din $\mathbf{G}_1$ astfel încât liniile sale sunt toate produsele posibile de linii ale lui $\mathbf{G}_1$ luate câte l într-un produs. Pentru o scriere ordonată, coloana cea mai din stânga a lui $\mathbf{G}_1$ are toate componentele egale cu zero, coloana cea mai din dreapta le are egale cu unu, iar celelalte sunt m–tupluri binare în ordine crescătoare, cu bitul de ordin inferior în linia cea mai de jos.

Există $\binom{m}{l}$ moduri de a alege cele *l* linii dintr-un produs, astfel încât $\mathbf{G}_l$ este o matrice $\binom{m}{l} \times 2^m$. Cu condiția ca liniile lui **G** să fie liniar independente, este clar că numărul liniilor *k* este egal cu

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} \tag{8.45}$$

Având în vedere că (vezi binomul lui Newton)

$$n = 2^m = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} + \cdots + \binom{m}{m},$$

iar $\binom{m}{r} = \binom{m}{m-r}$, numărul biților de paritate este

$$n - k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-r-1}. \tag{8.46}$$

EXEMPLUL 8.5: Codul Reed – Muller de ordin 0 este un cod (n,1). Acesta este un simplu cod de repetiție, numit astfel întrucât $v_0 = v_1 = v_2 = \cdots = v_{n-1}$. El are numai două cuvinte de cod, primul având toți biții egali cu 0, iar al doilea, cu 1. Decodarea se face banal, printr-o logică de majoritate : dacă cel puțin jumătate din cei *n* biți de recepție sunt 0, decodorul declară că bitul de informație transmis este 0; în caz contrar, rezultatul decodării este 1.

EXEMPLUL 8.6: Fie *m* = 4, *n* = 16 şi *r* = 3. Avem atunci

$$\mathbf{G}_0 = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1] = [\mathbf{a}_0],$$

$$\mathbf{G}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \mathbf{a}_3 \\ \mathbf{a}_4 \end{bmatrix}$$

Deoarece $\mathbf{G}_1$ are patru linii, $\mathbf{G}_2$ are $\binom{4}{2} = 6$ linii, iar $\mathbf{G}_3$ are $\binom{4}{3} = 4$ linii:

$$\mathbf{G}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1\ \mathbf{a}_2 \\ \mathbf{a}_1\ \mathbf{a}_3 \\ \mathbf{a}_1\ \mathbf{a}_4 \\ \mathbf{a}_2\ \mathbf{a}_3 \\ \mathbf{a}_2\ \mathbf{a}_4 \\ \mathbf{a}_3\ \mathbf{a}_4 \end{bmatrix}.$$

$$\mathbf{G}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1\ \mathbf{a}_2\ \mathbf{a}_3 \\ \mathbf{a}_1\ \mathbf{a}_2\ \mathbf{a}_4 \\ \mathbf{a}_1\ \mathbf{a}_3\ \mathbf{a}_4 \\ \mathbf{a}_2\ \mathbf{a}_3\ \mathbf{a}_4 \end{bmatrix}.$$

Matricea generatoare pentru codul Reed – Muller de ordinul al treilea de lungime 16 este matricea 15×16:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{bmatrix}.$$

Această matrice generatoare ne dă un cod (16,15) definit pe *CG*(2). El nu este altceva decât un simplu cod de control al parității, adică, un cod cu un singur bit de control care face ca suma modulo 2 a tuturor biților dintr-un cuvânt de cod să fie egală cu zero.

Din aceleaşi matrice, obținem un alt cod Reed – Muller alegând *r* egal cu 2. Matricea generatoare este

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \mathbf{G}_2 \end{bmatrix}.$$

Obținem astfel un cod (16,11) definit pe *CG*(2), care este de fapt codul Hamming (15,11) extins cu un bit de control suplimentar.

Distanța Hamming a unui cod Reed – Muller de ordin *r* este $d_H = 2^{m-r}$. Pentru a demonstra această proprietate, să observăm mai întâi că

un cod Reed – Muller de ordin r se poate obține augmentând un cod Reed – Muller de ordin $(r-1)$ şi că un cod Reed – Muller de ordin $(r-1)$ se poate obține expurgând un cod Reed – Muller de ordin r[1]. Fiecare linie a matricei $\mathbf{G}_l$ are pondere 2^{m-l}. Deci, fiecare linie a matricei generatoare **G** are pondere pară, iar suma a doi vectori binari de pondere pară trebuie să aibă pondere pară. Prin urmare, toate combinațiile liniare de linii ale lui **G** au pondere pară, adică, toate cuvintele de cod au pondere pară. Matricea $\mathbf{G}_r$ are linii de pondere 2^{m-r}, astfel încât ponderea minimă nu este mai mare de 2^{m-r}.

Vom arăta că un cod Reed – Muller de ordin r trebuie să aibă pondere minimă de 2^{m-r} şi că liniile matricei **G** trebuie să fie liniar independente dezvoltând un algoritm de decodare ce corectează $\left(\frac{1}{2}\cdot 2^{m-r}-1\right)$ şi recuperează cei k biți de informație, de unde va rezulta că distanța minimă este de cel puțin 2^{m-r}-1 şi fiincă este pară, că este de cel puțin 2^{m-r}. Algoritmul de decodare poartă numele celui care l-a imaginat, Reed.

Algoritmul Reed a fost elaborat special pentru codurile Reed – Muller. Desigur, pentru decodare se poate utiliza metoda generală, bazată pe calculul sindromului, dar este preferabilă o metodă mai simplă, ce exploatează structura particulară a codurilor Reed – Muller. Am văzut deja că putem decoda codul Reed – Muller de ordin 0 printr-o simplă regulă de logică majoritară. Presupunem că avem un decodor pentru un cod Reed – Muller de ordin $(r-1)$ în prezența a $\left(\frac{1}{2}\cdot 2^{m-(r-1)}-1\right)$ erori. Vom construi un decodor pentru un cod Reed – Muller de ordin r în prezența a $\left(\frac{1}{2}\cdot 2^{m-r}-1\right)$ erori reducându-l la cazul precedent, obținând astfel un algoritm de decodare prin inducție.

Examinând expresia numărului de biți de informație k din (8.45), constatăm că mesajul se compune din $(r+1)$ segmente, pe care le scriem

$$\mathbf{u}=\left[\mathbf{U}_0,\mathbf{U}_1,\cdots,\mathbf{U}_r\right]. \tag{8.47}$$

În (8.47), segmentul $\mathbf{U}_l$ conține $\binom{m}{l}$ biți de informație. Fiecare segment înmulțeşte un bloc din matricea generatoare **G**:

[1] Pentru definiția augmentării şi a expurgării, a se vedea Cap. 6, ultima parte.

$$\mathbf{v} = \left[\mathbf{U}_0, \mathbf{U}_1, \cdots, \mathbf{U}_r\right] \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ . \\ . \\ . \\ \mathbf{G}_r \end{bmatrix} = \mathbf{uG} . \tag{8.48}$$

Vectorul de recepție **w** este:

$$\mathbf{w} = \left[\mathbf{U}_0, \mathbf{U}_1, \cdots, \mathbf{U}_r\right] \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ . \\ . \\ . \\ \mathbf{G}_r \end{bmatrix} + \mathbf{e} . \tag{8.49}$$

Algoritmul de decodare va recupera mai întâi U_r din **w**. Apoi, el calculează:

$$\mathbf{w}' = \mathbf{w} - \mathbf{U}_r\mathbf{G}_r = \left[\mathbf{U}_0, \mathbf{U}_1, \cdots, \mathbf{U}_{r-1}\right] \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ . \\ . \\ . \\ \mathbf{G}_{r-1} \end{bmatrix} + \mathbf{e} . \tag{8.50}$$

În (8.50), am folosit semnul „ – “ pentru a pune în evidență faptul că operația este de scădere, dar, desigur, în cazul unui cod binar, „ – “ este acelaşi lucru cu „ + “ . Vectorul de recepție **w'** este un cuvânt de cod dintr-un cod Reed – Muller de ordin (r – 1) afectat de zgomot.

Primul bit care se decodează este u_{k-1}, care înmulțește ultima linie a lui $\mathbf{G}_r$. Există 2^{m-r} ecuații de control pentru cei 2^m biți de recepție; fiecare ecuație implică 2^r biți ai cuvântului recepționat, iar fiecare bit de recepție este utilizat numai într-o ecuație de control. Să considerăm codul Reed – Muller (16,11), pentru care $m = 4$ şi $r = 2$.

EXEMPLUL 8.7: Decodarea codului Reed – Muller de lungime $2^m = 16$ şi de ordin $r = 2$.

Vectorul de mesaj este $\mathbf{u} = (u_0, u_1, \cdots, u_{10})$. Pentru bitul u_{10}, cele patru ecuații de control sunt:

$$u_{10} = v_0 + v_1 + v_2 + v_3 \tag{8.51a}$$

$$u_{10} = v_4 + v_5 + v_6 + v_7 \tag{8.51b}$$

$$u_{10} = v_8 + v_9 + v_{10} + v_{11} \tag{8.51c}$$

$$u_{10} = v_{12} + v_{13} + v_{14} + v_{15} \tag{8.51d}$$

Dacă nu se produce decât o singură eroare, numai una din cele patru sume va fi greşită, astfel încât o decizie bazată pe logică majoritară ne dă u_{10}. Dacă apar două erori, nu există majoritate, astfel încât se detectează o eroare dublă.

La fel se procedează cu restul biților de informație care înmulțesc o linie a lui $\mathbf{G}_r = \mathbf{G}_2$. După ce toți aceşti biți de informație vor fi fost cunoscuți, contribuția lor la cuvântul de cod se scade din vectorul recepționat. Rezultă un cuvânt de cod dintr-un cod Reed – Muller de ordin $(r - 1) = 1$. Se decodează acum biții de informație care înmulțesc $\mathbf{G}_{r-1} = \mathbf{G}_1$.

Procesul se repetă până când vor fi recuperați toți biții de informație.

8.4. CODURI BCH

Codurile BCH au fost inventate de Bhose şi Chaudhuri şi, independent, de Hocquenghem; BCH sunt inițialele acestor nume. Codurile BCH sunt o generalizare a codurilor Hamming pentru corecția erorilor multiple.

Pentru orice numere naturale m $(m \geq 3)$ şi $t\left(t < 2^{m-1}\right)$, există un cod BCH cu următorii parametri:

Lungimea codului: $n = 2^m - 1$
Numărul biților de control: $n - k \leq mt$
Capacitatea de corecție a erorilor: t
Distanța minimă: $d_{\min} \geq 2t + 1$.

Fie α un element primitiv din $CG(2^m)$. Polinomul generator $g(X)$ al codului BCH de lungime $\left(2^m - 1\right)$ corector de t erori este polinomul de

gradul cel mai mic definit pe $CG(2^m)$ care are $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ drept rădăcini:

$$g(\alpha^i) = 0 \text{ pentru } 1 \le i \le 2t \tag{8.52}$$

Conform teoremei 8.3, toate rădăcinile lui $g(X)$ sunt $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ şi conjugatele lor. Fie $\phi_i(X)$ polinomul minimal al lui α^i. Polinomul generator $g(X)$ trebuie să fie *cel mai mic multiplu comun* al polinoamelor minimale $\phi_1(X), \phi_2(X), \cdots, \phi_{2t}(X)$:

$$g(X) = c.m.m.m.c.\{\phi_1(X), \phi_2(X), \cdots, \phi_{2t}(X)\}. \tag{8.53}$$

Această expresie implică 2*t* polinoame minimale. Vom reduce acest număr făcând observaţia următoare. Dacă *i* este un număr natural par, el poate fi exprimat drept un produs dintre un număr impar *i'* şi o putere a lui 2, să spunem 2^l, cu $l \ge 1$. În acest caz, $\alpha^i = (\alpha^{i'})^{2^l}$ este o conjugată a lui $\alpha^{i'}$, astfel încât α^i şi $\alpha^{i'}$ au acelaşi polinom minimal:

$$\phi_i(X) = \phi_{i'}(X). \tag{8.54}$$

Prin urmare, fiecare putere pară a lui α din şirul $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ are acelaşi polinom minimal ca şi o putere impară precedentă a lui α din şir. Rezultă că polinomul generator $g(X)$ al codului BCH de lungime $(2^m - 1)$ corector de *t* erori dat de (8.53) se poate reduce la

$$g(X) = c.m.m.m.c.\{\phi_1(X), \phi_3(X), \cdots, \phi_{2t-1}(X)\} \tag{8.55}$$

Întrucât gradul fiecărui polinom minimal este *m* sau mai mic, gradul lui $g(X)$ este de cel mult *mt*. Prin urmare, numărul (*n*–*k*) al biţilor de control este cel mult egal cu *mt*. Nu există o formulă simplă pentru (*n*–*k*), dar dacă *t* este mic, (*n*–*k*) este exact egal cu *mt*.

După cum se vede din (8.55), codul BCH de lungime $(2^m - 1)$ corector de o singură eroare ($t = 1$) este generat de

$$g(X) = \phi_1(X) \tag{8.56}$$

Dar fiindcă α este un element primitiv al lui $CG(2^m)$, $\phi_1(X)$ este un polinom primitiv de grad *m*. Prin urmare, codul BCH de lungime $(2^m - 1)$ corector de o singură eroare este un cod Hamming.

EXEMPLUL 8.8: Fie α un element primitiv al corpului Galois $CG(2^4)$ astfel încât $1+\alpha+\alpha^4=0$. Polinoamele minimale ale lui α, α^3 şi α^5 sunt, respectiv:

$$\phi_1(X) = 1 + X + X^4 \tag{8.57}$$

$$\phi_3(X) = 1 + X + X^2 + X^3 + X^4 \tag{8.58}$$

$$\phi_5(X) = 1 + X + X^2 \tag{8.59}$$

Din (8.55), urmează că acel cod BCH de lungime $n = 2^4 - 1 = 15$ corector de erori duble este generat de:

$$g(X) = c.m.m.m.c.\{\phi_1(X), \phi_3(X)\} \tag{8.60}$$

Fiindcă $\phi_1(X)$ şi $\phi_3(X)$ sunt două polinoame ireductibile distincte, avem:

$$\begin{aligned} g(X) &= \phi_1(X)\phi_3(X) \\ &= (1 + X + X^4)(1 + X + X^2 + X^3 + X^4) \\ &= 1 + X^4 + X^6 + X^7 + X^8. \end{aligned} \tag{8.61}$$

Deci, codul acesta este un cod ciclic (15,7) cu $d_{\min} \geq 5$. Întrucât polinomul generator este un polinom de cod de pondere 5, distanţa minimă nu poate fi mai mare şi este, deci, exact 5.

Codul BCH de lungime 15 corector de erori triple este generat de:

$$\begin{aligned} g(X) &= c.m.m.m.c.\{\Phi_1(X), \Phi_3(X), \Phi_5(X)\} \\ &= (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)(1 + X + X^2) \\ &= 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}. \end{aligned} \tag{8.62}$$

Acest cod BCH corector de erori triple este un cod ciclic (15,5) cu $d_{\min} \geq 7$. Întrucât ponderea polinomului generator este 7, distanţa minimă a acestui cod este chiar 7.

Din definiţia unui cod BCH de lungime $n = 2^m - 1$ corector de t erori, urmează că fiecare polinom de cod are drept rădăcini $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ şi conjugatele lor. Fie $v(X) = v_0 + v_1 X + \cdots + v_{n-1} X^{n-1}$ un polinom cu coeficienţi din $CG(2)$. Dacă $v(X)$ are $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$ drept rădăcini, este

divizibil cu polinoamele minimale $\phi_1(X),\phi_2(X),\cdots,\phi_{2t}(X)$ ale lui $\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2t}$ respectiv. Evident, $v(X)$ este divizibil cu cel mai mic multiplu comun al lor (polinomul generator)

$$g(X)=c.m.m.m.c.\{\phi_1(X),\phi_2(X),\cdots,\phi_{2t}(X)\}.$$

Prin urmare, $v(X)$ este un polinom de cod. În consecință, putem defini un cod BCH de lungime $n=2^m-1$ corector de t erori în modul următor: un n–tuplu binar $\mathbf{v}=(v_0,v_1,v_2,\cdots,v_{n-1})$ este un cuvânt de cod dacă şi numai dacă polinomul $v(X)=v_0+v_1X+\cdots+v_{n-1}X^{n-1}$ are printre rădăcinile sale $\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2t}$. Întrucât α^i este o rădăcină a lui $v(X)$ pentru $1\le i\le 2t$, avem:

$$v(\alpha^i)=v_0+v_1\alpha^i+v_2\alpha^{2i}+\cdots+v_{n-1}\alpha^{(n-1)i}=0 \qquad (8.63)$$

Egalitatea (8.63) se poate scrie ca un produs matriceal după cum urmează:

$$(v_0,v_1,\cdots,v_{n-1})\begin{bmatrix}1\\ \alpha^i\\ \alpha^{2i}\\ .\\ .\\ .\\ \alpha^{(n-1)i}\end{bmatrix}=0 \qquad (8.64)$$

pentru $1\le i\le 2t$. Condiția dată de (8.64) spune că produsul scalar dintre $(v_0,v_1,v_2,\cdots,v_{n-1})$ şi $(1,\alpha^i,\alpha^{2i},\cdots,\alpha^{(n-1)i})$ este egal cu zero. Formăm acum matricea următoare:

$$\mathbf{H}=\begin{bmatrix}1 & \alpha & \alpha^2 & \alpha^3 & \cdot & \cdot & \cdot & \alpha^{n-1}\\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdot & \cdot & \cdot & (\alpha^2)^{n-1}\\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdot & \cdot & \cdot & (\alpha^3)^{n-1}\\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \cdot & \cdot & \cdot & (\alpha^{2t})^{n-1}\end{bmatrix}. \qquad (8.65)$$

Din (8.64) urmează că, dacă $\mathbf{v} = (v_0, v_1, v_2, \cdots, v_{n-1})$ este un cuvânt de cod din codul BCH corector de *t* erori, avem

$$\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}. \tag{8.66}$$

Pe de altă parte, dacă un *n*–tuplu $\mathbf{v} = (v_0, v_1, v_2, \cdots, v_{n-1})$ satisface condiția (8.66), din (8.63) şi (8.64) urmează că α^i este o rădăcină a polinomului $v(X)$ pentru $1 \le i \le 2t$. Din acest motiv, **v** trebuie să fie un cuvânt de cod din codul BCH corector de *t* erori. Codul este, deci, spațiul nul al matricei **H**, iar **H** este matricea de control a codului. Dacă, pentru două numere naturale *i* şi *j*, α^j este o conjugată a lui α^i, $v(\alpha^j) = 0$ dacă şi numai dacă $v(\alpha^i) = 0$. Aceasta spune că, dacă produsul scalar dintre $\mathbf{v} = (v_0, v_1, v_2, \cdots, v_{n-1})$ şi linia *i* a lui **H** este zero, produsul scalar dintre *v* şi linia *j* a lui **H** este şi el este zero. Pentru acest motiv, linia *j* a lui **H** poate fi omisă. Rezultă că matricea **H** dată de (8.65) se poate reduce la forma de mai jos:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdot & \cdot & \cdot & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdot & \cdot & \cdot & (\alpha^3)^{n-1} \\ 1 & \alpha^5 & (\alpha^5)^2 & (\alpha^5)^3 & \cdot & \cdot & \cdot & (\alpha^5)^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha^{2t-1} & (\alpha^{2t-1})^2 & (\alpha^{2t-1})^3 & \cdot & \cdot & \cdot & (\alpha^{2t-1})^{n-1} \end{bmatrix}. \tag{8.67}$$

Se observă că elementele matricei **H** sunt elemente din $CG(2^m)$. Or, fiecare element din $CG(2^m)$ poate fi reprezentat printr-un *m*–tuplu pe $CG(2)$. Dacă fiecare element din **H** se înlocuieşte prin *m*–tuplul său corespunzător pe $CG(2)$ dispus în formă de coloană, obținem o matrice de control binară pentru codul BCH.

EXEMPLUL 8.9: Să considerăm codul BCH de lungime $n = 2^4 - 1 = 15$ corector de erori duble. Din exemplul precedent, ştim că acesta este un cod (15,7). Fie α un element primitiv al lui $CG(2^4)$. Conform cu (8.67), matricea de control a acestui cod se scrie:

$$\mathbf{H}=\begin{bmatrix}1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14}\\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & \alpha^{24} & \alpha^{27} & \alpha^{30} & \alpha^{33} & \alpha^{36} & \alpha^{39} & \alpha^{42}\end{bmatrix}.$$

Utilizând tabelul pentru $CG(2^4)$ şi reprezentând fiecare element al matricei **H** prin 4–tuplul corespunzător, obţinem următoarea matrice binară de control pentru acest cod:

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

Decodarea codurilor BCH

Să presupunem că se transmite un cuvânt de cod de polinom $v(X)=v_0+v_1X+v_2X^2+\cdots+v_{n-1}X^{n-1}$ dar, din cauza perturbaţiilor din canalul de comunicaţie, se recepţionează vectorul **r**, având polinomul $r(X)=r_0+r_1X+r_2X^2+\cdots+r_{n-1}X^{n-1}$. Polinomul de eroare $e(X)$ este dat de:

$$r(X)=v(X)+e(X). \tag{8.68}$$

După cum ştim, primul pas în decodare este calculul sindromului. Pentru decodarea unui cod BCH corector de t erori, sindromul este un $2t$ – tuplu

$$\mathbf{S}=(S_1,S_2,\cdots,S_{2t})=\mathbf{r}\cdot\mathbf{H}^T \tag{8.69}$$

În (8.69), matricea **H** este cea dată în (8.67). Componenta S_i a sindromului este:

$$\begin{aligned}S_i&=r(\alpha^i)\\&=r_0+r_1\alpha^i+r_2\alpha^{2i}+\cdots+r_{n-1}\alpha^{(n-1)i}\end{aligned} \tag{8.70}$$

pentru $1 \le i \le 2t$. Componentele sindromului sunt elemente din corpul Galois $CG(2^m)$. Având polinomul de recepție $r(X)$, aceste componente se pot calcula după cum urmează. Împărțind $r(X)$ la polinomul minimal $\phi_i(X)$ al lui α^i, obținem:

$$r(X) = a_i(X)\phi_i(X) + b_i(X) \tag{8.71}$$

unde $b_i(X)$ este restul, având deci gradul mai mic decât al lui $\phi_i(X)$. Fiindcă $\phi_i(\alpha^i) = 0$, avem că

$$S_i = r(\alpha^i) = b_i(\alpha^i). \tag{8.72}$$

Din (8.72), este clar că se obține componenta S_i a sindromului evaluând $b_i(X)$ pentru $X = \alpha^i$.

EXEMPLUL 8.10: Să considerăm codul BCH (15,7) corector de erori duble dat în exemplul 8.8. Să spunem că se recepționează vectorul $\mathbf{r} = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0)$. Polinomul corespunzător este $r(X) = 1 + X^8$. Sindromul are patru componente şi se scrie: $S = (S_1, S_2, S_3, S_4)$.

Polinoamele minimale pentru α, α^2 şi α^4 sunt identice şi $\phi_1(X) = \phi_2(X) = \phi_4(X) = 1 + X + X^4$. Polinomul minimal al lui α^3 este $\phi_3(X) = 1 + X + X^2 + X^3 + X^4$. Împărțind $r(X) = 1 + X^8$ la $\phi_3(X) = 1 + X + X^2 + X^3 + X^4$, restul este $b_3(X) = 1 + X^3$.

Utilizând $CG(2^4)$ şi înlocuind α, α^2 şi α^4 în $b_1(X)$, obținem:

$$S_1 = \alpha^2,\ S_2 = \alpha^4,\ S_4 = \alpha^8.$$

Înlocuind α^3 în $b_3(X)$, obținem:

$$S_3 = 1 + \alpha^9 = 1 + \alpha + \alpha^3 = \alpha^7.$$

În definitiv, avem:

$$S = (\alpha^2, \alpha^4, \alpha^7, \alpha^8).$$

Să considerăm decodarea unui cod BCH de lungime $n = 2^m - 1$ corector de două erori. Fie α un element primitiv din $CG(2^m)$, iar $\phi_1(X)$ şi $\phi_3(X)$ polinoamele minimale ale lui α şi α^3, respectiv. Polinomul generator al codului este deci

$$g(X) = \phi_1(X)\phi_3(X). \tag{8.73}$$

Particularizând (8.63), avem:

$$\begin{aligned} v(\alpha) &= v_0 + v_1\alpha + v_2\alpha^2 + \cdots + v_{n-1}\alpha^{n-1} \\ v(\alpha^3) &= v_0 + v_1\alpha^3 + v_2\alpha^6 + \cdots + v_{n-1}\alpha^{3(n-1)} \end{aligned} \tag{8.74}$$

Cele două egalități din (8.77) se pot combina astfel:

$$(v_0, v_1, v_2, \cdots, v_{n-1}) \cdot \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^3 \\ \alpha^2 & \alpha^6 \\ . & \\ . & \\ . & \\ \alpha^{n-1} & \alpha^{3(n-1)} \end{bmatrix} = 0. \tag{8.75}$$

Întrucât α^i este un element din $CG(2^m)$, el se poate reprezenta ca un m–tuplu binar, astfel încât matricea are dimensiunile $n \times 2m$.

Să presupunem că se recepționează vectorul **r** având polinomul $r(X)$. Sindromul lui $r(X)$ este

$$\mathbf{r} \cdot \mathbf{H}^T = (S_1, S_3) = [r(\alpha), r(\alpha^3)]. \tag{8.76}$$

În (8.76), S_1 şi S_3 sunt m–tupluri binare.

Dacă în transmisiune nu apar erori, sindromul este $\mathbf{r} \cdot \mathbf{H}^T = \mathbf{0}$ şi, deci, $S_1 = S_3 = 0$. Dacă însă apare o singură eroare, polinomul de eroare corespunzător este de forma:

$$e(X) = X^i \tag{8.77}$$

şi, deci,

$$\begin{aligned} \mathbf{r} \cdot \mathbf{H}^T &= \mathbf{e} \cdot \mathbf{H}^T = [e(\alpha), e(\alpha^3)] \\ &= (\alpha^i, \alpha^{3i}) \\ &= (S_1, S_3) \end{aligned} \quad . \tag{8.78}$$

Din (8.78), este evident că în acest caz $S_3 = S_1^3$.

Dacă în transmisiune apar două erori, să spunem în pozițiile i şi j, $i \neq j$, polinomul de eroare este de forma:

$$e(X) = X^i + X^j \tag{8.79}$$

Sindromul este, deci, dat de:

$$\begin{aligned} \mathbf{r} \cdot \mathbf{H}^T &= (S_1, S_3) \\ &= \left(\alpha^i + \alpha^j, \alpha^{3i} + \alpha^{3j}\right). \end{aligned} \tag{8.80}$$

Rezultă următorul sistem de ecuații:

$$\begin{aligned} \alpha^i + \alpha^j &= S_1 \\ \alpha^{3i} + \alpha^{3j} &= S_3 \end{aligned} \tag{8.81}$$

Ridicând la pătrat ambii membri ai primei ecuații de mai sus şi descompunând primul membru al ecuației a doua, avem că

$$\begin{aligned} S_1^2 &= \left(\alpha^i + \alpha^j\right)^2 \\ &= \alpha^{2i} + \alpha^{2j} \\ S_3 &= \left(\alpha^i + \alpha^j\right)\left(\alpha^{2i} + \alpha^{i+j} + \alpha^{2j}\right) \end{aligned} .$$

Combinând cele două ecuații, avem:

$$S_3 = S_1\left(S_1^2 + \alpha^{i+j}\right) \tag{8.82}$$

Din (8.82), deducem că

$$\alpha^{i+j} = S_3 \cdot S_1^{-1} + S_1^2 . \tag{8.83}$$

Având suma $\alpha^i + \alpha^j$ şi produsul α^{i+j}, formăm ecuația de gradul doi cu rădăcini α^i şi α^j:

$$Z^2 + S_1 Z + \left(S_3 \cdot S_1^{-1} + S_1^2\right) = 0 . \tag{8.84}$$

Putem găsi pozițiile erorilor rezolvând această ecuație. Polinomul din membrul stâng al ecuației (8.84) se numeşte *polinom de localizare a erorilor*.

EXEMPLUL 8.11: Fie corpul Galois $CG(2^4)$ generat de un element α care este rădăcină a polinomului primitiv $p(X) = 1 + X + X^4$. Un cod BCH (15,7) corector de două erori are matricea de control **H**

$$\mathbf{H}^T = \begin{bmatrix} 1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&1 \\ 0&0&1&0&0&0&1&1 \\ 0&0&0&1&0&1&0&1 \\ 1&1&0&0&1&1&1&1 \\ 0&1&1&0&1&0&0&0 \\ 0&0&1&1&0&0&0&1 \\ 1&1&0&1&0&0&1&1 \\ 1&0&1&0&0&1&0&1 \\ 0&1&0&1&1&1&1&1 \\ 1&1&1&0&1&0&0&0 \\ 0&1&1&1&0&0&0&1 \\ 1&1&1&1&0&0&1&1 \\ 1&0&1&1&0&1&0&1 \\ 1&0&0&1&1&1&1&1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^3 \\ \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^9 \\ \alpha^4 & \alpha^{12} \\ \alpha^5 & 1 \\ \alpha^6 & \alpha^3 \\ \alpha^7 & \alpha^6 \\ \alpha^8 & \alpha^9 \\ \alpha^9 & \alpha^{12} \\ \alpha^{10} & 1 \\ \alpha^{11} & \alpha^3 \\ \alpha^{12} & \alpha^6 \\ \alpha^{13} & \alpha^9 \\ \alpha^{14} & \alpha^{12} \end{bmatrix}. \qquad (8.85)$$

Să presupunem că se transmite un cuvânt de cod şi se recepționează un vector al cărui sindrom este:

$$S_1 = r(\alpha) = 0\ 1\ 1\ 1$$
$$S_3 = r(\alpha^3) = 1\ 0\ 1\ 0$$

Din tabelul 8.1, vedem că $S_1 \leftrightarrow \alpha^{11}$ şi $S_3 \leftrightarrow \alpha^8$. Avem apoi:

$$\begin{aligned} S_3 \cdot S_1^{-1} + S_1^2 &= \alpha^8 \cdot \alpha^{-11} + \alpha^{22} \\ &= \alpha^{12} + \alpha^7 \\ &= \alpha^2. \end{aligned}$$

Formăm polinomul de localizare a erorilor $Z^2 + \alpha^{11}Z + \alpha^2$ şi găsim că are drept rădăcini α^4 şi α^{13}. Prin urmare, receptorul poate decide că cele mai probabile erori au apărut în pozițiile 4 şi 13, adică, $e(X) = X^4 + X^{13}$. Cel mai probabil vector de eroare este, deci, 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0.

Algoritm pentru decodarea codurilor BCH corectoare de două erori

1. Se calculează sindromul:

$$\mathbf{r} \cdot \mathbf{H}^T = \left[S_1, S_3\right] = \left[r(\alpha), r\left(\alpha^3\right)\right].$$

2. Dacă $S_1 = S_3 = 0$, se conchide că n-au fost erori. Se decodează $\mathbf{v} = \mathbf{r}$ drept cuvântul de cod emis.
3. Dacă $S_1 = 0$ dar $S_3 \neq 0$, eroarea este necorectabilă.
4. Dacă $S_3 = S_1^3$, se corectează o eroare unică în poziția *i*, unde $S_1 = \alpha^i$.
5. Dacă $S_3 \neq S_1^3$, se formează ecuația de gradul doi:

$$Z^2 + S_1 Z + \left(S_2 \cdot S_1^{-1} + S_1^2\right) = 0.$$

6. Dacă ecuația în Z are două rădăcini distincte α^i şi α^j, se corectează erorile din pozițiile *i* şi *j*.
7. Dacă ecuația în Z n-are două rădăcini distincte din $CG(2^m)$, receptorul deduce că au apărut cel puțin trei erori în transmisia cuvântului de cod, erori care sunt necorectabile.

Decodarea unui cod BCH corector de trei erori revine la a rezolva o ecuație polinomială de gradul 3 cu coeficienți din $CG(2^m)$. Procedura este desigur ceva mai complicată, dar nu se deosebeşte principial de cea pentru codurile BCH corectoare de două erori. Algoritmi mai evoluați de decodare depăşesc nivelul acestui curs introductiv.

8.5. CODURI REED – SOLOMON

Codurile detectoare şi corectoare de erori pot fi şi nebinare, în care caz simbolurile sunt din corpul $CG(q)$, unde q este o putere a unui număr prim p. Acestea se numesc coduri q–are. Codurile Reed – Solomon sunt o subclasă deosebit de importantă a codurilor BCH q–are . Un cod Reed – Solomon corector de t erori cu simboluri din $CG(q)$ are următorii parametri:

Lungimea blocului: $n = q - 1$

Numărul biților de control: $n - k = 2t$

Distanța minimă: $d_{\min} = 2t + 1$.

În continuare, vom considera $q = 2^m$. Fie α un element primitiv din $CG(2^m)$. Polinomul generator al unui cod Reed – Solomon primitiv corector de t erori de lungime $n = 2^m - 1$ este:

$$\begin{aligned} g(X) &= (X+\alpha)(X+\alpha^2)\cdots(X+\alpha^{2t}) \\ &= g_0 + g_1 X + g_2 X^2 + \cdots + g_{2t-1} X^{2t-1} + X^{2t}. \end{aligned} \tag{8.86}$$

Polinomul generator are, deci, rădăcinile $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}$, iar coeficienții săi sunt elementele din $CG(2^m)$. El generează un cod ciclic ce constă din acele polinoame de grad (n–1) sau mai mic cu coeficienți din $CG(2^m)$ care sunt multipli de $g(X)$. Codarea se face similar cu cazul binar. Fie $k = (n - 2t)$ şi $u(X)$ polinomul de mesaj:

$$u(X) = u_0 + u_1 X + u_2 X^2 + \cdots + u_{k-1} X^{k-1}. \tag{8.87}$$

Ca şi în cazul binar, cuvântul de cod poate fi pus în formă sistematică împărțind $X^{2t} u(X)$ la polinomul generator $g(X)$. Decodarea se face şi ea ca în cazul binar, cu deosebirea importantă că operațiile aritmetice se fac în corpul Galois $CG(2^m)$.

Fiind importante în numeroase aplicații, cel mai adesea, în calitate de coduri exterioare în codurile concatenate, codurile Reed – Solomon au fost studiate intens, construindu-se cu timpul o teorie a lor de mari proporții. Prezentarea acestei teorii depăşeşte cu mult nivelul unui curs introductiv, ceea ce ne obligă să ne oprim aici.