Lucrarea 6

Coduri Hamming ciclice

6.1 Obiectivul lucrării

În această lucrare vor fi studiate codurile Hamming ciclice şi proprietăţile acestora, făcându-se o paralelă cu codurile Hamming grup prin analiza proprietăților suplimentare pe care codurile ciclice le prezintă.

6.2 Introducere teoretică

Cuvintele codurilor ciclice sunt polinoame reprezentative ale unor clase de resturi polinomiale, dar pot fi scrise şi ca vectori; de exemplu, polinomul de cod:

$$v(X) = a_0 + a_1X + a_2X^2 \ldots + a_{n-1}X^{n-1}$$

corespunde vectorului:

$$\mathbf{v} = \left[\begin{array}{cccc} a_0 & a_1 & a_2 & \ldots & a_{n-1} \end{array} \right].$$

Fie mulţimea polinoamelor de variabilă X cu coeficienţi în câmpul binar şi un polinom $p(X) = X^n + 1$. Se formează tabelul claselor de resturi modulo $p(X)$, scriind pe prima linie a tabelului multiplii lui $p(X)$ şi, pe celelalte linii, sumele dintre aceşti multipli şi polinoame de grad mai mic decât n.

Numărul polinoamelor de variabilă X cu coeficienţi în câmpul binar este infinit şi în fiecare dintre şirurile tabelului (denumite clase de resturi) se află un număr infinit de termeni, dar numărul şirurilor este finit şi egal cu 2^n.

Polinoamele reprezentative ale claselor de resturi modulo $p(X)$ au gradul maxim egal cu $n-1$ şi formează o algebră cu 2^n elemente.

Dintre cele 2^n polinoame reprezentative, care pot fi scrise ca polinoame de gradul $n-1$ (prin completarea cu zerouri a poziţiilor superioare), o parte pot alcătui un cod. Specificarea cuvintelor cu sens (adică a polinoamelor care aparţin codului) se poate face în mai multe feluri. Modul cel mai des folosit pentru specificarea polinoamelor de cod $v(X)$ constă în respectarea condiţiei ca $v(X)$ să fie un multiplu al unui polinom de grad m:

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_mX^m \tag{6.1}$$

adică:

$$v(X) = q(X) \cdot g(X). \tag{6.2}$$

Polinomul $g(X)$ este, în mod obligatoriu, un divizor al polinomului $p(X) = X^n + 1$ şi se numeşte polinom generator. Întrucât gradul polinomului de cod $v(X)$ este maxim $n-1$, iar $g(X)$ are gradul m, gradul polinomului $q(X)$ este egal cu $n-m-1$.

Codurile ciclice sunt denumite astfel, pentru că orice permutare a unui cuvânt de cod al codului V este tot un cuvânt al acestui cod. Într-adevăr, dacă

$$v(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_{n-1} X^{n-1} \tag{6.3}$$

aparţine codului generat de polinomul $g(X)$,

$$v(X) = q(X) \cdot g(X).$$

Prin înmulţirea cu X a relaţiei anterioare, se obţine:

$$X \cdot v(X) = X \cdot q(X) \cdot g(X). \tag{6.4}$$

Într-adevăr, polinomul $v_1(X) = X \cdot v(X)$ este multiplu al polinomului $g(X)$ şi, prin urmare, polinom de cod. Totodată,

$$\begin{aligned} v_1(X) = X \cdot v(X) &= a_0 X + a_1 X^2 + \ldots + a_{n-1} X^n \\ &= a_{n-1} + a_0 X + \ldots + a_{n-2} X^{n-1} \bmod (X^n + 1) \end{aligned} \tag{6.5}$$

deoarece $X^n = 1$ în algebra polinoamelor modulo $X^n + 1$.

Vectorii corespunzători polinoamelor $v(X)$ şi $v_1(X)$ sunt:

$$\mathbf{v} = \begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} \end{bmatrix} \tag{6.6}$$

$$\mathbf{v_1} = \begin{bmatrix} a_{n-1} & a_0 & \ldots & a_{n-2} \end{bmatrix} \tag{6.7}$$

Cu alte cuvinte, $\mathbf{v_1}$ este obţinut prin permutarea ciclică a vectorului $\mathbf{v}$ cu o poziţie.

Exemplu: Pentru cazul claselor de resturi modulo polinomul $1 + X^7$, polinoamele reprezentative ale claselor de resturi formate şi vectorii corespunzători sunt date în Tabelul 6.1.

Polinoamele reprezentative ale claselor de resturi modulo $1 + X^7$	Reprezentarea vectorială a claselor de resturi modulo $1 + X^7$
0	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
1	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
X	$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$1 + X$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
X^2	$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$
$\vdots$	$\vdots$
$1 + X + X^2 + \ldots + X^6$	$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

Tabelul 6.1: Polinoamele reprezentative ale claselor de resturi modulo $1 + X^7$ şi vectorii corespunzători

În această algebră există 2^7 elemente.

Alegând $g(X) = 1 + X + X^3$ divizor al polinomului $1 + X^7$, multiplii acestuia formează un cod ale cărui cuvinte au lungimea $n = 7$. Gradul polinomului $g(X)$ este $m = 3$, deci $k = n - m = 7 - 3 = 4$. În acest cod, există 2^4 cuvinte cu sens sau cuvinte de cod.

6.2.1 Codarea codurilor ciclice

Dacă considerăm $q(X) = i(X) = i_0 + i_1X + i_2X^2 + \ldots + i_{k-1}X^{k-1}$, obținem relația de codare în formă nesistematică:

$$v(X) = i(X) \cdot g(X). \tag{6.8}$$

Numărul coeficienţilor polinomului $i(X)$ este $n - m = k$, în care cei k coeficienţi ai polinomului $i(X)$ sunt simbolurile de informație. Cu acești coeficienți, se pot scrie 2^k polinoame $i(X)$ şi, în consecinţă, numărul cuvintelor de cod posibile este 2^k. Dezavantajul codării în formă nesistematică, denumită codare prin multiplicare, constă în faptul că simbolurile de informație și cele de control sunt amestecate.

Pentru a realiza codarea în formă sistematică se va folosi o altă metodă, denumită codare prin divizare, ce foloseşte, pentru calculul polinoamelor de cod, relaţia:

$$v(X) = c(X) + X^m \cdot i(X). \tag{6.9}$$

Coeficienţii polinomului,

$$c(X) = c_0 + c_1X + c_2X^2 + \ldots + c_{m-1}X^{m-1} \tag{6.10}$$

în număr de m sunt simbolurile de control, iar coeficienţii polinomului

$$i(X) = i_0 + i_1X + i_2X^2 + \ldots + i_{k-1}X^{k-1} \tag{6.11}$$

sunt simbolurile de informaţie.

Determinarea polinomului de control $c(X)$ reprezintă tocmai operaţia de codare şi se efectuează cu relaţia:

$$c(X) = rest\frac{X^m \cdot i(X)}{g(X)}. \tag{6.12}$$

Exemplu: În cazul codului $C(7,4)$ generat de polinomul $g(X) = 1 + X + X^3$, pentru polinomul de informaţie particular

$$i(X) = 1 + X^3$$

polinomul de control are valoarea

$$c(X) = rest\frac{X^3 \cdot (1 + X^3)}{1 + X + X^3} = X + X^2.$$

Polinomul de cod corespunzător, conform relaţiei (6.9), este:

$$v(X) = X + X^2 + X^3 + X^6$$

căruia îi corespunde vectorul $\mathbf{v} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$.

6.2.2 Matricea generatoare şi matricea de control

Codurile ciclice sunt coduri grup particulare, pentru care pot fi definite matrici **G** şi **H** specifice. Matricea generatoare se scrie pornind de la expresia (6.1) a polinomului $g(X)$ şi are forma:

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 & 0 \\ 0 & g_1 & \dots & g_{m-1} & g_m & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & g_0 & g_1 & \dots & g_m & 0 \\ 0 & 0 & \dots & 0 & g_0 & \dots & g_{m-1} & g_m \end{bmatrix}. \tag{6.13}$$

Matricea de control se poate scrie cu ajutorul coeficienţilor unui polinomul $h(X)$, definit ca:

$$h(X) = \frac{X^n + 1}{g(X)} = h_0 + h_1 X + h_2 X^2 + \ldots + h_k X^k. \tag{6.14}$$

Matricea de control are forma:

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & \dots & 0 & h_k & \dots & h_1 & h_0 \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & h_k & \dots & h_1 & h_0 & \dots & 0 & 0 \\ h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 & 0 \end{bmatrix}. \tag{6.15}$$

Exemplu: Pentru codul studiat mai sus

$$h(X) = \frac{X^7 + 1}{X^3 + X + 1} = 1 + X + X^2 + X^4$$

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

6.2.3 Decodarea codurilor ciclice

În cazul codurilor ciclice, modificarea simbolurilor transmise de către perturbaţii este exprimată matematic prin adunarea polinomului transmis $v(X)$ cu un polinom eroare $e(X)$ de gradul $n-1$ ai cărui coeficienţi sunt diferiţi de zero numai pe poziţiile pe care intervin erori; astfel, polinomul recepţionat este:

$$v_{rec}(X) = v(X) + e(X). \tag{6.16}$$

Decodarea, în cazul detecţiei erorilor, înseamnă calculul unui polinom $z(X)$ de gradul m, denumit polinom corector sau sindrom. Acesta este dat de relaţia:

$$z(X) = rest\frac{v_{rec}(X)}{g(X)} \tag{6.17}$$

sau de relaţia echivalentă:

$$z(X) = rest\frac{v(X)}{g(X)} + rest\frac{e(X)}{g(X)} = rest\frac{e(X)}{g(X)}. \tag{6.18}$$

Dacă $z(X)$ este egal cu zero, $v_{rec}(X)$ aparţine codului sau, altfel spus, transmisia a fost efectuată corect. Dacă $z(X)$ este diferit de zero, se trage concluzia că au fost introduse erori în cuvântul de cod transmis.

În cazul corecţiei erorilor, decodarea înseamnă determinarea polinomului $e(X)$ şi adunarea lui cu polinomul transmis:

$$v(X) = v_{rec}(X) + e(X). \tag{6.19}$$

Exemplu: Dacă, în urma acţiunii perturbaţiilor, poziţia a cincea a cuvântului de cod determinat anterior este modificată, vectorul eroare, respectiv polinomul eroare au structurile:

$$e(X) = X^4$$
$$\mathbf{e} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

iar $v_{rec}(X) = X + X^2 + X^3 + X^4 + X^6$.

Polinomul corector este:

$$z(X) = rest\frac{X + X^2 + X^3 + X^4 + X^6}{1 + X + X^3} = rest\frac{X^4}{1 + X + X^3} = X + X^2.$$

Pentru a efectua corecția cuvintelor recepționate, determinarea $e(X)$ pornind de la $z(X)$ nu se poate face în mod direct. Din acest motiv, se recurge la relația de decodare:

$$\mathbf{z} = \mathbf{H} \cdot \mathbf{v}_{rec}^T \tag{6.20}$$

ce permite corecția cuvântului recepționat în mod similar decodării în regim de corecție întâlnite la codurile grup.

6.2.4 Coduri Hamming ciclice

Dintre polinoamele reprezentative ale claselor de resturi, o parte sunt polinoame primitive. Un polinom primitiv este un polinom ireductibil care poate genera toate elementele dintr-un câmp extins $GF(2^m)$. Fie α o rădăcină a unui polinom $g(X)$ de grad m. Dacă primele $2^m - 1$ puteri ale elementului α sunt diferite și toate cele $2^m - 1$ elementele nenule din $GF(2^m)$ pot fi reprezentate ca puteri succesive ale lui α ($1 = \alpha^{2^m-1}$, α, α^2, ..., α^{2^m-2}), atunci α se numește element primitiv.

Exemplu: Fie polinomul $g(X) = 1 + X + X^3$ şi α o rădăcină a lui. Pentru a verifica dacă acest polinom este primitiv, respectiv dacă rădăcina sa α este un element primitiv, se calculează puterile elementului α până când se determină o putere a lui α este egală cu 1. Această putere se numește ordinul lui α. Dacă ordinul lui α este $2^3 - 1 = 7$, atunci spunem că s-a parcurs un ciclu complet și polinomul este primitiv. Puterile rădăcinii α sunt date în Tabelul 6.2, unde pentru calculul puterilor α^i, s-a ţinut seama de faptul că $1 + \alpha + \alpha^3 = 0$, α fiind rădăcină a polinomului $g(X)$.

Un cod Hamming ciclic este generat de un polinom primitiv. Exemple de polinoame primitive sunt următoarele:

α^i	Forma polinomială a puterilor lui α^i	Forma vectorială a puterilor lui α^i
α^0	1	$[1 \quad 0 \quad 0]$
α^1	α	$[0 \quad 1 \quad 0]$
α^2	α^2	$[0 \quad 0 \quad 1]$
α^3	$1 + \alpha$	$[1 \quad 1 \quad 0]$
α^4	$\alpha + \alpha^2$	$[0 \quad 1 \quad 1]$
α^5	$1 + \alpha + \alpha^2$	$[1 \quad 1 \quad 1]$
α^6	$1 + \alpha^2$	$[1 \quad 0 \quad 1]$

Tabelul 6.2: Puterile rădăcinii α a polinomului $g(X) = 1 + X + X^3$

- Pentru $m = 3$

$$\begin{aligned} g_1(X) &= 1 + X + X^3 \\ g_2(X) &= 1 + X^2 + X^3 \end{aligned} \tag{6.21}$$

- Pentru $m = 4$

$$\begin{aligned} g_1(X) &= 1 + X + X^4 \\ g_2(X) &= 1 + X^3 + X^4 \end{aligned} \tag{6.22}$$

Codarea Hamming ciclică se poate face urmărind o formă nesistematică (relația (6.8)) sau o formă sistematică (relația (6.9)). În cazul codării în formă nesistematică, se poate folosi și matricea generatoare $\mathbf{G}$ dedusă cu ajutorul relației (6.13) și relația $\mathbf{v} = \mathbf{i} \cdot \mathbf{G}$, ce a fost deja utilizată în cazul codurilor grup. Similar, în cazul codării în formă sistematică, se poate folosi și matricea de control $\mathbf{H}$ dedusă cu ajutorul relației (6.15) și relația $\mathbf{H} \cdot \mathbf{v}^T = 0$, ce a fost deja utilizată în cazul codurilor grup. Spre deosebire de codurile Hamming grup, folosirea relației din urmă este posibilă numai în cazul codării sistematice, simbolurile de control fiind grupate la începutul cuvântului de cod.

Decodarea, în cazul corecției de erori, poate urma pașii de la codurile Hamming grup după ce se deduce matricea de control corespunzătoare folosind relația (6.15). Ca şi codurile Hamming grup, sunt coduri corectoare de o eroare şi sunt coduri perfecte.

6.3 Desfăşurarea lucrării

Pentru a efectua operații cu polinoame, vom utiliza clasa GF2m definită mai jos.

```
"""
Atentie!
(1) Polinoamele se scriu in reprezentare vectoriala incepand cu puterea cea ...
    mai mica.
(2) Coeficientii sunt 0 sau 1.
"""

import numpy as np
```

```
def grad(p):
    # np.poly1d considera putere maxima pe prima pozitie in vector
    p = np.poly1d(np.flipud(p))
    return p.order


def X(m):
    # reprezinta X^m ---> [0 0 ... 0 1]
    X = np.zeros(m+1, dtype=int)
    X[m] = 1
    return X


class GF2m:
    def __init__(self, g):
        self.g = g
        self.m = grad(g)
        self.n = np.power(2, self.m) - 1
        self.k = self.n - self.m
        self.p = self.adunare_polinoame(X(self.n), X(0)) # X^n + 1
        (self.h, _) = self.divizare_polinoame(self.p, self.g)

    def adunare_polinoame(self, a, b):
        s = np.mod(np.flipud(np.polyadd(np.flipud(a), np.flipud(b))), 2)
        return s.astype(int)

    def inmultire_polinoame(self, a, b):
        p = np.mod(np.flipud(np.polymul(np.flipud(a), np.flipud(b))), 2)
        # In algebra polinoamelor modulo (X^n + 1), X^n = X^0, X^(n+1) = X^1, ...
            s.a.m.d.
        if grad(p) > self.n - 1:
            for i in range(self.n, grad(p)+1):
                p[i-self.n] = np.mod(p[i-self.n] + p[i], 2)
                p[i] = 0
        p = p[0:grad(p)+1]
        return p

    def divizare_polinoame(self, a, b):
        (cat, rest) = np.polydiv(np.flipud(a), np.flipud(b))
        cat = np.mod(np.flipud(cat), 2)
        rest = np.mod(np.flipud(rest), 2)
        return cat.astype(int), rest.astype(int)

g = np.array([1, 1, 0, 1])  # 1+X+X^3
gf2m = GF2m(g)
print('Coeficientii polinomului p: ', gf2m.p)
print('Coeficientii polinomului h: ', gf2m.h)

s = gf2m.adunare_polinoame(np.array([1, 0, 1]), np.array([1, 1]))
print('Suma polinoamelor 1+X^2 si 1+X este: ', s)
p = gf2m.inmultire_polinoame(np.array([1, 0, 1, 0, 0, 1]), np.array([1, 0, 1, 1]))
print('Inmultirea polinoamelor 1+X^2+X^5 si 1+X^2+X^3 este:', p)
(c, r) = gf2m.divizare_polinoame(np.array([1, 0, 1, 0, 0, 1]), np.array([1, 0, ...
    1, 1]))
print('Impartirea polinoamelor 1+X^2+X^5 si 1+X^2+X^3 este: cat = ', c, ' rest ...
    = ', r)
```

6.4 Exerciţii

1. Se consideră polinomul generator $g_1(X) = 1 + X + X^3$ și codare în formă sistematică. Implementați funcțiile:

$$g1\_encode(text: str) \text{ -> } np.ndarray$$
$$g1\_decode(code\_matrix: np.ndarray) \text{ -> } str$$

   Funcția *g1_ encode* primește ca parametru un text format doar din primele 16 litere mari ale alfabetului englezesc (de la 'A' la 'P'; 'A' va fi codat ca '0000', 'B' va fi codat ca '0001', ... P va fi codat ca '1111') și returnează o matrice în care fiecare linie reprezintă codarea caracterului respectiv folosind un cod Hamming având ca polinom generator $g_1(X)$.

   Funcția *g1_ decode* primește ca parametru o matrice în care fiecare linie reprezintă codarea unui caracter (codarea este afectată de cel mult 1 eroare) și întoarce textul decodat.