Aurelian Claudiu VOLF

Introducere în teoria codurilor

Fiicei mele, Diana

Cuprins

Prefaţă

> "Error correction is one of the most advanced areas in the entire field of digital audio. *It is purely because of error-correction techniques that reliable digital recordings can be made, despite the frequent occurrence of tape dropouts*." [*Digital Audio Technology*, Edited by Jan Maes and Marc Vercammen, Focal Press 2001]

Codurile corectoare de erori (pe scurt, codurile) corectează sau detectează erori care apar inevitabil la transmiterea unui mesaj pe un canal care nu asigură o transmisie perfectă (canal „cu zgomot"). Această detectare/corectare se realizează prin introducerea de redundanţă în mesaj (adică, în loc de a transmite mesajul original, un mesaj mai lung este transmis, în speranţa că simbolurile adăugate vor ajuta la detectarea/corectarea erorilor). Orice comunicare digitală, orice stocare de date foloseşte o formă de coduri corectoare de erori. Compact discurile, discurile dure, memoriile interne ale calculatoarelor, memoriile flash, DVD-urile etc. sînt protejate împotriva alterării accidentale a datelor folosind astfel de coduri. Aceste dispozitive, şi multe altele, nu ar putea funcţiona fără coduri corectoare de erori.

Deci, codurile ajută la corectarea de erori, dar nu oferă confidenţialitate. Confidenţialitatea se realizează de către criptografie.

După prezentarea scopurilor teoriei codurilor şi a principiilor sale de bază în capitolul I (noţiunea de canal de comunicare, cod bloc, distanţă Hamming, algoritmul de decodare de distanţă minimă, capacitate de corectare a unui cod), se introduc obiectele principale de studiu, *codurile liniare*, în capitolul II. Aici sînt definite noţiunile de matrice generatoare, matrice de paritate, dualul unui cod, şi sînt date primele rezultate semnificative privind: evaluarea distanţei minime a unui cod liniar, inegalităţi satisfăcute de parametrii unui cod, exemple remarcabile de coduri liniare (coduri Hamming). Întrucît corpurile finite sînt esenţiale în teoria codurilor liniare, le este dedicat un capitol special, care include teorema de clasificare a corpurilor finite, construcţia unui corp finit, proprietăţi de bază ale corpurilor finite. Capitolul IV continuă studiul codurilor liniare şi descrie unele principii generale de codare şi decodare. În capitolul V sînt date diverse construcţii clasice de coduri noi din coduri existente, cu aplicaţii practice şi teoretice (coduri Reed-Muller, metode de investigare a existenţei unui cod cu anumiţi parametri).

În capitolul VI este introdusă şi studiată clasa codurilor ciclice, importantă atît prin faptul că are aplicaţii practice, cît şi prin frumuseţea matematică a descrierii lor. Subclasa codurilor BCH este introdusă în capitolul VII, fiind descris şi algoritmul de decodare Petersen-Gorenstein-Ziegler. Ultimul capitol este dedicat codurilor corectoare de pachete de erori şi a descrierii a două aplicaţii semnificative şi foarte răspîndite ale teoriei codurilor: schema de codare pentru corectarea de erori la compact-discurile

audio şi schema de detectare de erori CRC (cyclic redundancy check).

Multe monografii de teoria codurilor au mai mult de 700 de pagini. Acest curs introductiv, din motive de spaţiu şi din dorinţa de a păstra aparatul matematic necesar la un nivel cît mai accesibil (în esenţă, algebră liniară şi elemente de corpuri finite), nu include multe teme clasice de teoria codurilor care sînt foarte importante. Astfel, am omis tematici precum: grupul de automorfisme ale unui cod, coduri QR (construite cu resturi pătratice – quadratic residue codes), coduri Goppa, coduri AG (coduri provenite din geometrie algebrică – algebraic geometry codes), coduri peste inele, coduri autoduale, coduri convoluţionale, coduri LDPC (low density parity check codes), legături cu teoria design-urilor etc. Aceste tematici se pot găsi în multe din cărţile citate în bibliografie, din care menţionăm [2], [9], [13], [14]. Totuşi, avem convingerea că după parcurgerea acestui curs, cititorul va fi familiarizat cu ideile principale şi cu unele din metodele, aplicaţiile, limitările şi problemele teoriei codurilor. Acest domeniu este în plină evoluţie şi multe rezultate sau metode apar an de an. De aceea, această carte trebuie văzută mai mult ca o invitaţie la lecturi ulterioare şi cercetare în arii mai restrînse care sînt de interes pentru cititor.

Sperăm că cititorul va descoperi măcar o parte din uimitoarea cantitate de inventivitate şi de frumuseţe matematică din spatele multor lucruri pe care le considerăm astăzi normale: utilizarea unui computer, ascultarea unui CD, o convorbire pe telefonul mobil. Toate aceste tehnologii nu ar fi posibile fără teoria codurilor şi matematica pe care se bazează.

Cititorul trebuie avertizat că practic toată literatura din domeniul teoriei codurilor este în limba engleză. Multe din noţiunile folosite sînt de dată foarte recentă şi unele nu au avut timp să fie incluse în literatura românească, oricum foarte restrînsă. De aceea, este necesară familiarizarea cu terminologia engleză, echivalentele româneşti ale multor denumiri nefiind încă standardizate.

Unele notaţii

- $|A|$ desemnează cardinalul mulţimii A (numărul elemen-telor lui A, dacă A este finită).
- $x := y$ înseamnă „x este egal prin definiţie cu y” (unde y este deja definit) sau „notăm pe y cu x”.
- $\square$ marchează sfîrşitul sau absenţa unei demonstraţii.
- $\lfloor x \rfloor$ este cel mai mare întreg care este mai mic sau egal cu numărul real x (partea întreagă a lui x)
- $\lceil x \rceil = \min \{n \in \mathbb{Z} \mid x \le n\}$ este cel mai mic întreg mai mare sau egal decît numărul real x.
- $\mathrm{M}(k, n, F)$ este mulţimea matricelor de tip $k \times n$ peste inelul F.
- A^{T} este transpusa matricei A.
- $\mathbb{N}$ este mulţimea numerelor naturale: 0, 1, 2, …
- $\mathrm{Irr}(x, K)$ este polinomul minimal al elementului algebric x peste corpul K.
- $\mathbb{Z}$ este mulţimea numerelor întregi : 0, 1, 2, -1, -2, …
- $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$ este inelul claselor de resturi modulo n, cu adunarea şi înmulţirea mod n.
- $S(X) = \{\sigma : X \to X \mid \sigma \text{ este bijectivă}\}$ este mulţimea permutărilor mulţimii X. $S(X)$ este grup cu compunerea funcţiilor.

- S_n este grupul permutărilor mulţimii $\{1, 2, \ldots, n\}$. S_n are $n! = 1 \cdot 2 \cdot \ldots \cdot n$ elemente.
- $\binom{n}{k} = C_n^k$ = combinări de n luate cîte $k = \dfrac{n!}{k!(n-k)!}$

I. Coduri corectoare de erori

Fie A o mulţime finită, numită *alfabet*, ale cărei elemente le numim *simboluri*. Prin „informaţie digitală" (sau *mesaj peste A*) înţelegem un şir de simboluri (elemente) din alfabetul A. Astfel, orice frază dintr-o limbă dată este un mesaj (informaţie digitală). Orice şir de litere, chiar fără sens, este mesaj. De exemplu, 011110101100 este un şir de simboluri din alfabetul {0,1} (în acest caz, simbolurile se numesc *biţi*). Acest mesaj este un mesaj *binar*, căci alfabetul are două simboluri. Un alfabet cu q simboluri se numeşte *alfabet q-ar.*

Transmiterea unei *informaţii digitale*[1] între două puncte diferite *în spaţiu* (de exemplu o transmisie de date pe o linie telefonică) sau *în timp* (stocarea pe un suport material cum ar fi un compact disc, pentru o citire ulterioară), este supusă *erorilor* cauzate de o

[1] Transmiterea de sunete, imagini, texte etc. ca un şir de 0 şi 1 pare azi evidentă, dar în anii 1940 a fost o idee revoluţionară şi îi aparţine lui *Claude Shannon* (1916-2001), matematician american, unul din fondatorii teoriei informaţiei (articolul *A mathematical theory of communication,* 1948).

varietate de factori: zgomot pe linia telefonică, deteriorarea suportului fizic al informaţiei etc. Se impune găsirea unui procedeu prin care mesajul să poată ajunge în formă corectă la receptor (sau receptorul să poată detecta eventualele erori şi să ceară retransmisia mesajului).

Fixăm un alfabet A cu q simboluri (alfabet q-ar).

Ideea care stă la baza teoriei *codurilor bloc corectoare de erori* este următoarea: se fixează $k, n \in \mathbb{N}^*$, cu $k < n$. Se împarte mesajul original în „blocuri" (numite „*cuvinte*") de k simboluri. Fiecărui cuvînt[2] de lungime k i se asociază un cuvînt mai lung, de lungime n, după o lege prestabilită; cele $n - k$ simboluri „în plus" sînt puse pentru detectarea şi eventual corectarea erorilor ce pot apărea în transmisie. Pe canal se transmite cuvîntul de n simboluri, la recepţie urmînd ca, prin analizarea cuvîntului recepţionat, să se decidă dacă au apărut erori (sau să se reconstituie cuvîntul transmis).

1 Exemplu. Fie $A = \{0, 1\}$ (alfabet *binar*). O idee simplă şi nu prea eficientă de codare pentru corectarea erorilor este de a transmite fiecare bit de 3 ori, urmînd ca decodarea să se facă după „regula majorităţii". Mai precis, luăm $k = 1$, $n = 3$ şi stabilim următorul procedeu de codare: 0 este codat ca 000, iar 1 ca 111. Astfel, dacă mesajul original este 0101, el va fi codat ca 000111000111. Să presupunem că acest mesaj este afectat de erori

[2] Prin *cuvînt de lungime k* se înţelege un k-uplu de simboluri din A (un element din A^k).

pe canal, încît la recepţie se primeşte 001111000011. La decodare, fiecare grup de 3 biţi este tratat individual: de exemplu grupul 001 este decodat în 0 (se presupune că 001 provine din 000 în care unul din 0 a devenit 1), 011 este decodat în 1 etc. Acest procedeu de corectare a erorilor funcţionează atît timp cît nu apare mai mult de o eroare la fiecare grup de trei simboluri transmise. Acest cod se numeşte *codul* (binar) *de repetiţie* de lungime 3.

Modelăm o situaţie de tipul descris, astfel: *transmiţătorul* trimite un *mesaj* către *receptor* pe un *canal de transmisie*. *Mesajul* este un şir finit de *simboluri* din alfabetul A. Orice şir de simboluri poate fi mesaj[3]. Presupunem că o *eroare* cauzează receptarea altui simbol decît cel transmis (dar nu „pierderea" simbolului în timpul transmisiei). Posibilitatea de apariţie de erori pe canal este modelată de o *funcţie de tranziţie* $P : A \times A \to [0, 1]$, cu semnificaţia că $\forall x,\ y \in A$, $P(y, x)$ reprezintă probabilitatea ca la transmiterea simbolului x, la recepţie să fie primit simbolul y.

Unul din cele mai răspîndite modele pentru un canal de transmisie este *canalul q-ar simetric de probabilitate p*:

- A are q elemente (este un „*alfabet q-ar*");

- funcţia de tranziţie P are proprietatea că $P(y, x) = p$, $\forall y,\ x \in A$ cu $y \neq x$. Altfel spus, probabilitatea de apariţie a unei *erori*

[3] Desigur, acest lucru e fals dacă se transmit numai mesaje din limba română, de exemplu. Însă această presupunere e valabilă dacă se efecuează în prealabil o *compresie fără pierderi* a mesajului, lucru curent în practica transmisiei de date (de exemplu compresiile zip, rar, lha etc). Acest procedeu, formalizat de Huffman, se bazează pe o analiză statistică a mesajului şi codarea simbolurilor cele mai probabile în şiruri scurte şi a celor mai puţin probabile în şiruri mai lungi.

(simbolul primit diferă de cel trimis) este $(q-1)p$, *indiferent de simbolul transmis* (de unde şi denumirea de canal *simetric*) şi *indiferent de locul simbolului în mesaj* (canal *„fără memorie”*). Deci, probabilitatea ca un simbol transmis x să fie recepţionat corect este $P(x, x) = 1 - (q-1)p$. Se presupune că $p < 1/2(q-1)$ (altfel este mai probabil să se recepţioneze un simbol eronat decît cel corect!). Dacă $q = 2$, se vorbeşte de un canal *binar*.

Spunem că un canal este *canal qSC(p)* dacă este un canal *q-a*r simetric, fără memorie, de probabilitate p.

Formalizăm ideea de codare bloc de mai sus: se fixează k, $n \in \mathbb{N}$, cu $k \le n$; se dă o funcţie injectivă $E : A^k \to A^n$ care *codează* fiecare $a = a_1 \ldots a_k \in A^k$ într-un *cuvînt cod* $c = c_1 \ldots c_n \in A^n$. (Un element oarecare din A^n, $(x_1, \ldots, x_n)$, (unde $x_i \in A, \forall i$) îl scriem mai simplu $x_1 \ldots x_n$.)

Mulţimea $C := E(A^k) = \{E(a_1 \ldots a_k) \mid a_1 \ldots a_k \in A^k\}$ a tuturor cuvintelor cod se numeşte *cod* (în cazul nostru, *cod de tip* $[n, k]$ *peste* A). Observăm că $|C| = q^k$.

Dacă mesajul $a_1 \ldots a_k$ este o parte a cuvîntului cod $c_1 \ldots c_n = E(a_1 \ldots a_k)$ (de obicei $c_1 \ldots c_n = a_1 \ldots a_k p_1 \ldots p_{n-k}$, unde $p_1 \ldots p_{n-k}$ se numesc *simboluri de paritate* sau *simboluri redundante* sau *simboluri de control*), codarea (şi codul C) se numeşte *sistematic(ă)*.

Pentru funcţionarea codului trebuie dată şi o *funcţie de decodare* $D : A^n \to C$, care asociază oricărui cuvînt x din A^n cuvîntul cel mai probabil transmis $D(x) \in C$. Evident, $D(c) = c$, $\forall c \in C$. O codare sistematică are avantajul că mesajul original este recuperat prin simpla eliminare a simbolurilor de control (dacă nu au avut loc erori!).

Este utilă şi o accepţie *mai largă* a noţiunii de cod:

2 Definiţie. Fie $n \in \mathbb{N}$. Un *cod (bloc) de lungime n* peste alfabetul A este o submulţime C a lui A^n. Elementele lui C se numesc *cuvinte cod*. Dacă $|A| = q$, C se numeşte *cod q-ar*.

Un cod bloc de tip $[n, k]$ transformă orice bloc de k simboluri într-un cuvînt cod de lungime mai mare n, ceea ce va permite (se speră) detectarea sau corectarea erorilor. Însă acest procedeu *măreşte lungimea mesajelor transmise* (ceea ce nu este de dorit). Pentru a măsura eficienţa unui cod din acest punct de vedere, se defineşte *rata* de transmisie a unui cod C de tip $[n, k]$ ca fiind $R(C) := k/n$. Rata măsoară proporţia de simboluri care poartă informaţie (restul sînt simboluri *redundante*, care folosesc la detectare sau corectare de erori). Dacă C este doar o submulţime a lui A^n, ca în **Def. 2**, *rata* e definită ca $R(C) := \log_q|C|/n$ (de ce?). Observaţi că pentru un cod de tip $[n, k]_q$, cele două definiţii coincid. Rata codului de repetiţie de lungime 3 este 1/3.

3 Exemplu. Codul binar de paritate P de lungime 9 este construit astfel: fiecărui mesaj de 8 biţi i se adaugă un *bit de paritate* astfel încît cuvîntul de 9 biţi care rezultă să conţină un număr par de biţi egali cu 1. Aceasta revine la a spune că suma (în $\mathbb{Z}_2$) a celor 9 biţi este 0. Deci,

$$P = \{x_1 \ldots x_8 x_9 \in (\mathbb{Z}_2)^9 \mid x_1 + \ldots + x_9 = 0\}.$$

Cîte cuvinte are P? Care e rata sa?

Posibilitatea unui cod C de a corecta erori se bazează în întregime pe ideea că, dacă un cuvînt cod $c \in C$ este afectat pe canalul de transmisie de (un număr mic de) erori, cuvîntul receptat

$c_r \neq c$ nu este cuvînt cod (nu aparţine lui C), dar este „suficient de apropiat" de c încît să putem reconstitui c din c_r. Acest lucru este posibil doar dacă c_r nu este el însuşi un alt cuvînt cod sau nu e „mai apropiat" de alt cuvînt cod c' !

Aceste idei se pot formula riguros.

4 Definiţie. Fie A o mulţime nevidă. *Distanţa Hamming*[4] pe A^n se defineşte astfel: $\forall x, y \in A^n$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$,

$$d(x, y) := |\{i \mid 1 \leq i \leq n, x_i \neq y_i\}|.$$

Deci, distanţa între două cuvinte este *numărul de locuri în care cuvintele diferă*.

5 Propoziţie. *Distanţa Hamming* $d : A^n \times A^n \to \mathbb{R}$ *este o distanţă* (*o metrică*) *pe* A^n, *adică:*

a) $\forall x, y \in A^n$, *avem* $d(x, y) = d(y, x) \geq 0$;

b) $\forall x, y \in A^n$, *avem:* $d(x, y) = 0 \Leftrightarrow x = y$;

c) $\forall x, y, z \in A^n$, *avem:* $d(x, y) \leq d(x, z) + d(z, y)$.

Demonstraţie. *c)* Fie $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in A^n$ şi notăm $C(x, y) := \{i \mid x_i = y_i\}$. Arătăm că $d(x, y) \leq d(x, z) + d(z, y)$, $\forall x, y, z \in A^n$. Cum $d(x, y) = n - |C(x, y)|$, inegalitatea devine: $n \geq |C(x, z)| + |C(z, y)| - |C(x, y)|$.

Dar $C(x, z) \cup C(z, y) \subseteq \{1, \ldots, n\}$, deci $|C(x, z) \cup C(z, y)| \leq n$. Deci $|C(x, z)| + |C(z, y)| - |C(x, z) \cap C(z, y)| \leq n$.

Însă $C(x, z) \cap C(z, y) \subseteq C(x, y)$, deci

[4] În onoarea lui Richard Hamming (1915-1998), matematician american, fondator, alături de Shannon, al teoriei informaţiei (articolul *Error detecting and error correcting codes*, 1950).

$n \geq |C(x, z)| + |C(z, y)| - |C(x, z) \bigcap C(z, y)| \geq$
$\geq |C(x, z)| + |C(z, y)| - |C(x,y)|.$ □

Pentru $x \in A^n$ şi $r > 0$, *sfera* (*bila*) *de rază r centrată în x* este mulţimea cuvintelor care sînt la distanţă cel mult r faţă de x:

$$B_r(x) := \{y \in A^n \mid d(x, y) \leq r\}.$$

Pentru $x \in A^n$, unde $|A| = q$, şi $1 \leq i \leq n$, există exact $C_n^i (q-1)^i$ cuvinte aflate la distanţă exact i de x. Deci orice două sfere de rază r au acelaşi „volum" (număr de elemente), anume:

6 Propoziţie. *Fie* $|A| = q$. *Numărul de elemente al unei sfere de rază r din* A^n *este*

$$|B_r| = |B_r(x)| = \sum_{i=0}^{r} C_n^i (q-1)^i \ .$$ □

7 Definiţie. *Distanţa minimă a* unui cod $C \subseteq A^n$ este:

$$d(C) := \min \{d(x, y) \mid x, y \in C, x \neq y\}.$$

Distanţa minimă $d(C)$ este un parametru foarte important al codului. Orice două cuvinte cod distincte ale lui C diferă în cel puţin $d(C)$ poziţii, şi există măcar o pereche de cuvinte cod la distanţă exact $d(C)$.

Să presupunem că la transmiterea unui cuvînt cod $c \in C$ apar erori, iar y este cuvîntul recepţionat. Trebuie să găsim c cunoscînd doar pe y. Pentru orice $y \in A^n$ şi $c \in C$, fie prob($y|c$) probabilitatea ca y să fie recepţionat cînd c este trimis. La recepţionarea lui $y \in A^n$, trebuie să găsim un cuvînt cod $m(y) \in C$ astfel încît prob($y|m(y)$) să fie maximă:

$$\text{prob}(y|m(y)) = \max \{ \text{prob}(y|c) \mid c \in C\}.$$

Un algoritm care realizează acest lucru se numeşte *algoritm de maximă verosimilitate* (*maximum likelihood algorithm*). In cazul canalului qSC(p):

$$\text{prob}(y|c) = p^{d(y,c)}(1-(q-1)p)^{n-d(y,c)} = p^n\left(\frac{1-(q-1)p}{p}\right)^{n-d(y,c)} =$$

$$= p^n\left(\frac{1}{p}-(q-1)\right)^{n-d(y,c)},$$

cu $0 < p < \dfrac{1}{2(q-1)}$, deci $\dfrac{1}{p}-(q-1) > q-1 \geq 1$.

Astfel, prob($y|c$) e maximă $\Leftrightarrow$ $d(y, c)$ este minim. Aceasta arată că algoritmul de maximă verosimilitate e echivalent cu:

Algoritmul de distanţă minimă (Minimum Distance Decoding). Pentru orice $y \in A^n$, algoritmul produce un cuvînt cod $w(y) \in C$ care este cel mai apropiat de y:

$$d(y, w(y)) = \min\{d(y, c) \mid c \in C\}.$$

Este important de ştiut cînd un astfel de algoritm funcţionează.

8 Definiţie. *Capacitatea de corectare a* unui cod $C \subseteq A^n$ cu distanţa minimă $d(C)$ este

$$e(C) = \lfloor (d(C)-1)/2 \rfloor.$$

Rezultatul următor justifică denumirea de mai sus.

9 Teoremă. Fie $C \subseteq A^n$ *un cod cu* $d(C) = d$ şi $e(C) = e = \lfloor (d-1)/2 \rfloor$. *Atunci:*

a) Orice două sfere de rază e centrate în cuvinte cod distincte sînt disjuncte.

b) Dacă la transmiterea unui cuvînt cod $c \in C$, $x \in A^n$ *este recepţionat şi au avut loc cel mult e erori* ($d(c, x) \le e$), *atunci c este unicul cuvînt cod din C cel mai apropiat de x (algoritmul de distanţă minimă decodează corect pe x în c)*

c) Dacă d este impar (*adică* $d = 2e + 1$), *atunci există cuvinte cod u,* $v \in C$ *şi* $x \in A^n$ *astfel încît* $d(u, x) = e + 1$, $d(v, x) = e$. *Deci există o situaţie cînd un cuvînt u este afectat de* $e + 1$ *erori şi nu este decodat corect de algoritmul de distanţă minimă.*

Demonstraţie. *a)* Presupunem că există $u, v \in C$ şi $x \in A^n$ astfel încît $x \in B_e(u) \cap B_e(v)$. Atunci:

$d(u, v) \le d(u, x) + d(x, v) \le e + e < d$, contradicţie.

b) Avem $d(c, x) \le e$, deci $x \in B_e(c)$. Pentru orice alt $u \in C$, $x \notin B_e(u)$, deci $d(x, u) > e$.

c) Exerciţiu. □

Dacă $x \in A^n$ este recepţionat şi $\delta = \min\{d(x, c) \mid c \in C\} > e$, mai multe cuvinte cod pot fi la distanţă δ de x. Aceasta înseamnă că o decodare corectă nu e posibilă. Chiar dacă există un unic $c \in C$ la distanţă δ, decodarea lui x în c poate fi incorectă, ca în *c)* mai sus.

10 Observaţie. Utilizarea unui cod C de lungime n, distanţă minimă d şi capacitate de corectare e se poate face în două moduri distincte:

- modul „corectare de erori”: se presupune că orice bloc de n simboluri c este afectat de cel mult e erori. Dacă cuvîntul recepţionat este c_r, c_r poate fi decodat în mod univoc în c. De aici provine şi denumirea de *capacitate de corectare a lui C* ce se dă lui e.

- modul „detectare de erori”: se presupune că la transmiterea oricărui bloc de n simboluri apar cel mult $d-1$ erori. Atunci niciun cuvînt cod c nu poate fi transformat pe parcursul transmiterii în alt cuvînt cod c'. Astfel, dacă receptorul primeşte un cuvînt c_r care nu este cuvînt cod, semnalează „eroare” (şi cere eventual retransmiterea cuvîntului). De aceea, $d-1$ se numeşte *capacitatea de detectare* a codului C.

În unele cazuri o combinaţie a acestor moduri este posibilă (un exemplu remarcabil este schema de corectare/detectare de erori folosită la Compact Disc).

11 Definiţie. Un cod q-ar tip $[n, k]$ cu distanţa minimă d este numit cod tip $[n, k, d]_q$ sau $[n, k, d]_q$-cod. Adesea, indicele q este omis dacă este clar din context.

Ştersături. Am definit o *eroare* ca fiind o situaţie cînd un simbol transmis e recepţionat ca un simbol diferit. În acest caz receptorul nu ştie apriori că o eroare a avut loc, nici nu ştie unde e plasată eroarea. Un alt model pentru canalul de transmisie include *ştersături* (*erasures*): simbolul recepţionat nu poate fi citit. O ştersătură poate fi interpretată ca o *eroare a cărei poziţie e cunoscută*. Ştersăturile sînt mai uşor de corectat (căci sînt deja *detectate* şi *localizate*). Putem modela această situaţie permiţînd ca în cuvintele receptate să poată apărea şi un nou simbol * (care notează o ştersătură); desigur, * nu aparţine alfabetului A. Notăm deci $A^* = A \cup \{*\}$. Pentru orice $c = c_1 \ldots c_n \in C$ transmis, fie $x = x_1 \ldots x_n \in A^{*n}$ cuvîntul recepţionat. Fie $S = \{i \mid x_i = *\}$ mulţimea poziţiilor lui x unde sînt ştersături şi fie $x_S \in A^{n-|S|}$ cuvîntul x din

care eliminăm toate ştersăturile. Algoritmul de distanţă minimă, în acest caz, va căuta un cuvînt cod $c' \in C$ astfel încît

$$d(x_S, c'_S) = \min \{d(x_S, y_S) \mid y \in C\}.$$

Rezultatul următor generalizează **Teorema 9** pentru cazul cînd apar ştersături şi erori simultan:

12 Teoremă. *Fie $C \subseteq A^n$ un cod de distanţă minimă d. Presupunem că $c \in C$ este transmis, $x \in A^{*n}$ este recepţionat şi au apărut ε erori şi δ ştersături, unde $2\varepsilon + \delta < d$. Atunci c este unicul cuvînt cod din C cu proprietatea că*

$$d(x_S, c_S) = \min \{d(x_S, y_S) \mid y \in C\}$$

Deci, algoritmul de distanţă minimă decodează corect pe x în c.

Demonstraţie. Folosim notaţiile de mai sus. $S = \{i \mid x_i = *\}$ are δ elemente. Avem $d(x_S, c_S) = \varepsilon$. Fie $y \in C$, $y \neq c$, şi să presupunem prin reducere la absurd că $d(x_S, y_S) \leq \varepsilon$. Atunci:

$$d(y_S, c_S) \leq d(y_S, x_S) + d(x_S, c_S) \leq 2\varepsilon.$$

Aceasta implică $d(y, x) = 2\varepsilon + \delta < d$, contradicţie. □

Teorema lui Shannon asupra capacităţii unui canal. Fixăm un canal $qSC(p)$. Pentru un cod q-ar C dat şi un cuvînt cod $x \in C$, $P_x(C)$ este definit ca probabilitatea ca, la transmiterea lui x pe canal, cuvîntul receptat să nu fie decodat corect de algoritmul de distanţă minimă.

Definim *probabilitatea de eroare* (sau *aşteptarea de eroare*, error expectation) $P(C)$ ca fiind media acestor probabilităţi individuale:

$$P(C) = |C|^{-1} \sum_{x \in C} P_x(C).$$

Aceasta este o măsură importantă a calităţii codului: sînt interesante codurile C pentru care $P(C)$ este foarte mică. Desigur, $P(C)$ depinde şi de *canal* (adică de q şi probabilitatea de tranziţie p), nu numai de codul C.

Pentru a enunţa teorema fundamentală a lui Shannon asupra capacităţii unui canal qSC(p), definim $H_q : [0,\ (q-1)/q] \to \mathbb{R}$, *funcţia de entropie q-ară*: $\forall\ p \in (0, (q-1)/q]$,

$$H_q(p) = -p\log_q(p/(q-1)) - (1-p)\log_q(1-p),$$

şi punem $H_q(0) = 0$ prin continuitate. Funcţia de *capacitate q-ară* C_q este definită pe $[0, 1/q]$ astfel:

$$C_q(p) = 1 - H_q((q-1)p),\ \forall\ p \in [0, 1/q].$$

În cazul $q = 2$, o interpretare a $H_2(p)$ este următoarea: pentru un simbol transmis s, $H_2(p)$ este incertitudinea ca simbolul recepţionat s' să fie chiar s (echivalent, $C_2(p) = 1 - H_2(p)$ este cantitatea de informaţie pe care s' o poartă despre s). Deşi extrem de interesante şi instructive, nu insistăm asupra acestor aspecte, deorece ţin mai mult de teoria informaţiei decît de codare şi necesită incursiuni în teoria probabilităţii. $C_q(p)$ se numeşte *capacitatea* canalului qSC(p).

13 Teoremă (Shannon) *Fie un canal qSC(p). Atunci, pentru orice R cu $R < C_q(p)$, există un şir de coduri $(C_m)_{m \geq 1}$, de tip $[n_m, k_m]$, cu rată $R_m = k_m/n_m > R$, astfel încît $P(C_m) \to 0$ cînd $m \to \infty$.*

Pentru orice $R > C_q(p)$, nu există şiruri de coduri cu rate $\geq R$ şi probabilităţi de eroare care tind la zero. □

Teorema lui Shannon spune în esenţă că *dacă rata R de transmisie e mai mică decît capacitatea* $C_q(p)$ *a canalului, atunci există coduri de rată (cel puţin) R cu probabilitate de eroare arbitrar de mică.*

Demonstraţia nu este constructivă, adică nu furnizează explicit un şir de coduri cu proprietăţile din enunţ. De aceea, unul din scopurile teoriei codurilor este de a găsi coduri sau familii de coduri care au rata cît mai apropiată de capacitatea canalului şi probabilitatea de eroare cît mai mică.

Vom prezenta numai aspecte din teoria codurilor *bloc* corectoare de erori şi unele aplicaţii, ignorînd o clasă de coduri corectoare de erori numite coduri *convoluţionale*. Un codor convoluţional tip [*n, k*] divide mesajul de intrare în blocuri de lungime *k* şi le codează ca blocuri de lungime *n*. Dar codarea unui bloc depinde nu numai de ultimul bloc mesaj (ca la codurile bloc corectoare de erori), ci şi de *m* blocuri de informaţie precedente (unde *m* este un număr fixat).

Exerciţii

1. Daţi exemplu de cod binar de lungime 3 cu 4 cuvinte cod. De ce nu există niciun cod binar de lungime 4 cu 18 cuvinte cod?

2. De ce este funcţia de codare presupusă injectivă?

3. De ce rata unui cod este definită ca $\log_q|C|/n$?

4. Fie codul binar $C = \{01101, 00011, 10110, 11000\}$. Determinaţi distanţa sa minimă şi rata. Folosind algoritmul de distanţă minimă, decodaţi următoarele cuvinte recepţionate: a) 00000; b) 01111; c) 10110; d) 10011; e) 11011.

5. Presupunem că un cod C are distanţa minimă număr par: $d = 2m$, cu $m \in \mathbb{N}^*$. Atunci $e = m - 1$. Demonstraţi că există două cuvinte $b, c \in C$ şi o situaţie cînd b este transmis şi este afectat de $e + 1 = m$ erori, situaţie în care algoritmul de distanţă minimă nu decodează unic cuvîntul recepţionat y în b (mai precis $d(y, b) = d(y, c) = m$).

6. Fie codul de repetiţie C_n de lungime n peste un alfabet q-ar A, $C_n := \{c...c \in A^n \mid c \in A\}$. Estimaţi rata R_n şi aşteptarea de eroare $P(C_n)$ pentru un canal $qSC(p)$. Satisface şirul $(C_n)_{n \geq 1}$ teorema lui Shannon?

7. Fie $n \geq 2$. Fie C un cod binar de lungime n şi distanţă minimă n. Cîte cuvinte are C? Cîte astfel de coduri există? Trataţi cazul q-ar.

8. Un *număr ISBN* este un şir de simboluri de forma $x_1 \ldots x_{10}$, cu $x_1, \ldots, x_9 \in \{0, 1, \ldots, 9\}$, $x_{10} \in \{0, 1, \ldots, 9, X\}$ şi $\sum_{i=1}^{10} i x_i = 0 \pmod{11}$, unde X notează numărul 10. a) Cum puteţi defini această schemă de codare în contextul teoriei codurilor (care este alfabetul, codul, rata etc.)? b) Cîte numere ISBN există?; c) Demonstraţi că această schemă de codare poate detecta permutarea a două simboluri şi schimbarea unui simbol cu altul. d) Care este distanţa minimă a acestui cod?

II. Coduri liniare

Dezvoltarea teoriei codurilor bloc corectoare de erori, precum şi găsirea unor algoritmi eficienţi de codare şi decodare, sînt mult uşurate pentru acele coduri C care au o anumită *structură*. O astfel de situaţie este cea în care *alfabetul este un corp finit* F (cu q elemente, unde q este o putere a unui număr prim), iar codul C, submulţime a lui F^n, este *subspaţiu liniar* în F^n. Deşi aceste condiţii limitează drastic clasa codurilor pe care le studiem, această clasă este suficient de vastă pentru a furniza coduri importante şi eficiente, folosite pe scară largă în practică. În continuare presupunem că cititorul este familiarizat cu noţiuni şi rezultate elementare de algebră liniară: spaţiu liniar, dependenţă liniară, sistem de generatori, baze, dimensiune, produsul scalar standard în F-spaţiul liniar F^n.

Reamintim în continuare cîteva lucruri de bază privind spaţiile liniare. Unele rezultate sînt date fără demonstraţie. Acest paragraf are rolul de a fixa notaţiile şi de a enunţa unele rezultatele pe care le vom utiliza, dar nu se poate substitui unei curs de algebră liniară.

În acest capitol notăm cu F un corp comutativ fixat. Corpul cu q elemente este notat $\mathbb{F}_q$. Cititorul care nu este încă familiarizat cu corpurile finite poate presupune că F este corpul cu două elemente $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ (inelul de clase de resturi modulo 2).

Cînd vorbim de spaţii liniare peste F, elementele lui F mai sînt numite *scalari*. O mulţime nevidă V (ale cărei elemente le numim *vectori*) se numeşte *spaţiu liniar* (sau *vectorial*) *peste* F dacă:

- este definită o *adunare* a vectorilor din V, adică o funcţie

$$+ : V \times V \to V, (u, v) \mapsto u + v, \ \forall u, v \in V;$$

- este definită o *înmulţire a vectorilor din V cu scalari din F:*

$$\cdot : F \times V \to V, (\lambda, v) \mapsto \lambda v \in V, \forall \lambda \in F, \forall v \in V;$$

- aceste operaţii satisfac condiţiile următoare:

(V, +) este un *grup abelian*, adică:

a) Adunarea e asociativă: $(x + y) + z = x + (y + z)$, $\forall x, y, z \in V$.

b) Adunarea e comutativă: $x + y = y + x$, $\forall x, y \in V$.

c) Există un vector $0 \in V$ astfel încît $x + 0 = 0 + x = x$, $\forall x \in V$.

d) Pentru orice $x \in V$ există $-x \in V$ astfel încît

$$x + (-x) = (-x) + x = 0.$$

Adunarea vectorilor şi înmulţirea cu scalari satisfac în plus proprietăţile următoare, pentru orice $\lambda \in F$ şi $x, y \in V$:

e) $\lambda(x + y) = \lambda x + \lambda y$

f) $(\lambda\mu)x = \lambda(\mu x)$

g) $1x = x$, unde 1 notează elementul unitate al lui F.

Am notat cu 0 atît vectorul 0 ($\in V$), cît şi scalarul 0 ($\in F$). Cititorul nu trebuie să le confunde. În loc de „spaţiu liniar peste F”, se spune adesea „F-spaţiu liniar”.

1 Exemplu. a) Mulţimea $F^n = \{(x_1, \ldots, x_n) \mid x_i \in F,\ 1 \le i \le n\}$ este un F-spaţiu liniar. Adunarea şi înmulţirea cu scalari se definesc „pe componente”:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n),$$
$$\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n),$$

pentru orice $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in F^n$, $\forall \lambda \in F$.

Verificarea faptului că V este într-adevăr un spaţiu linar este imediată. Vectorul 0 este $0 := (0, \ldots, 0)$. Pentru orice $(x_1, \ldots, x_n) \in F^n$, avem $-(x_1, \ldots, x_n) := (-x_1, \ldots, -x_n)$.

Exemplul acesta este fundamental (în sensul că orice F-spaţiu liniar finit dimensional este izomorf cu un unic F^n). *În esenţă, acestea sînt spaţiile liniare cu care vom lucra*.

b) Mulţimea polinoamelor cu coeficienţi în F, $F[X]$, este un F-spaţiu liniar. Care sînt operaţiile?

2 Definiţie. O submulţime nevidă C a unui F-spaţiu liniar V este un *subspaţiu liniar* al lui V dacă C este el însuşi un F-spaţiu liniar cu adunarea vectorilor şi înmulţirea cu scalari definite pe V. Mai precis, C este subspaţiu liniar în V dacă C este o mulţime de vectori din V care este parte stabilă la adunare şi la înmulţirea externă cu scalari din F:

$$\forall u, v \in C, \forall \alpha \in F, \text{ au loc: } u + v \in C \text{ şi } \alpha v \in C.$$

Scriem $C \le {}_F V$ dacă C este un subspaţiu al F- spaţiului liniar V (sau mai simplu $C \le V$ dacă nu există pericol de confuzie).

3 Exemple. a) Codul din exemplul **I. 1** este $C = \{000, 111\}$ şi este subspaţiu al $\mathbb{Z}_2$-spaţiului liniar $\mathbb{Z}_2{}^3$ (verificaţi!).

b) Pentru orice $k \in \mathbb{N}^*$, mulţimea polinoamelor de grad $< k$ din $F[X]$ este un subspaţiu liniar în $F[X]$ (verificaţi!).

4 Observaţie. Condiţia (din definiţia noţiunii de subspaţiu liniar) ca submulţimea C să fie parte stabilă la înmulţirea cu scalari este superfluă în cazul în care F este corpul cu două elemente $\mathbb{Z}_2$. De ce? Mai puteţi da exemple de corpuri pentru care se întîmplă acelaşi fenomen? Ce se întîmplă dacă $F = \mathbb{Q}$?

5 Definiţie. Fie ${}_F V$, $n \geq 1$ şi $v_1, \ldots, v_n \in V$. Orice vector de forma

$$\lambda_1 v_1 + \ldots + \lambda_n v_n,$$

unde $\lambda_1, \ldots, \lambda_n \in F$, se numeşte *combinaţie liniară* a vectorilor $v_1, \ldots, v_n$. Scalarii $\lambda_1, \ldots, \lambda_n$ se numesc *coeficienţii* acestei combinaţii liniare, iar numărul natural n se numeşte *lungimea* combinaţiei liniare. Convenim că *vectorul* 0 *este singura combinaţie liniară de o mulţime vidă de vectori*.

Dacă C este un subspaţiu în V, atunci orice combinaţie liniară de vectori din C este în C.

Pentru orice submulţime S a lui V, cel mai mic (în sensul incluziunii) subspaţiu al lui V care include S se numeşte *subspaţiul generat de* S şi este notat $< S >$. Se poate arăta uşor că $< S >$ există (este intersecţia tuturor subspaţiilor care includ S) şi este mulţimea tuturor combinaţiilor liniare de vectori din S:

$$< S > = \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid n \in \mathbb{N}^*,\ \lambda_1, \ldots, \lambda_n \in F,$$
$$v_1, \ldots, v_n \in S\}.$$

Dacă $< S > = V$, S se numeşte un sistem de generatori pentru V.

O mulţime $B = \{v_1, \ldots, v_n\}$ de vectori se numeşte *liniar independentă* dacă orice combinaţie liniară de $v_1, \ldots, v_n$ care este egală cu 0 are toţi coeficienţii egali cu 0:

$$\forall\ \lambda_1, \ldots, \lambda_n \in F, \text{ dacă } \lambda_1 v_1 + \ldots + \lambda_n v_n = 0, \text{ atunci}$$
$$\lambda_1 = \ldots = \lambda_n = 0.$$

O submulţime B a lui V se numeşte *bază* a lui V dacă B este liniar independentă şi $< B > = V$. Dacă $B = \{v_1, \ldots, v_n\}$ e finită, B este bază $\Leftrightarrow$ orice vector din V poate fi scris în mod unic ca o combinaţie liniară de $\{v_1, \ldots, v_n\}$:

$$\forall v \in V, \exists!\ (\lambda_1, \ldots, \lambda_n) \in F^n \text{ astfel încît } v = \lambda_1 v_1 + \ldots + \lambda_n v_n .$$

6 Exemplu. O bază pentru F^n este *baza canonică* $\{e_1, \ldots, e_n\}$, unde $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0)$, $\ldots$, $e_n = (0, 0, \ldots, 1)$. Există multe alte baze în F^n (dacă $n > 1$ sau $|F| > 2$).

7 Teoremă. *a) Orice F-spaţiu liniar V are o bază. Mai mult, orice mulţime liniar independentă de vectori poate fi completată pînă la o bază; din orice sistem de generatori ai lui V se poate extrage o bază.*

b) Orice două baze ale lui V au acelaşi cardinal (acelaşi număr de elemente). Acest număr este numit dimensiunea *lui* $_F V$ *şi se notează* $\dim_F V$ (sau $\dim V$). □

8 Definiţie. Fie U, V spaţii liniare peste corpul F. O funcţie $\varphi : U \to V$ se numeşte *aplicaţie F-liniară (*sau *F-morfism de spaţii liniare,* sau *operator liniar)* dacă :

$$\varphi(x + y) = \varphi(x) + \varphi(y),\ \forall x, y \in U;$$
$$\varphi(\lambda x) = \lambda\varphi(x),\ \forall x \in U,\ \forall \lambda \in F.$$

Este uşor de văzut că φ este liniară dacă şi numai dacă păstrează combinaţiile liniare:

$$\varphi(\lambda_1 v_1 + \ldots + \lambda_n v_n) = \lambda_1 \varphi(v_1) + \ldots + \lambda_n \varphi(v_n),$$
$$\forall n \in \mathbb{N}, \forall \lambda_1, \ldots, \lambda_n \in F, \forall v_1, \ldots, v_n \in U$$

Un morfism *bijectiv* de spaţii linare se numeşte *izomorfism*. Dacă există un izomorfism între spaţiile liniare U şi V, spunem că U şi V sînt *izomorfe* şi scriem $U \cong V$.

9 Observaţie. Dacă V este un spaţiu liniar de dimensiune n peste F şi $B = \{v_1, \ldots, v_n\}$ este o bază pentru V, atunci funcţia

$$\varphi : F^n \to V, \varphi(\lambda_1, \ldots, \lambda_n) = \lambda_1 v_1 + \ldots + \lambda_n v_n, \ \forall (\lambda_1, \ldots, \lambda_n) \in F^n,$$

este un izomorfism (demonstraţi!). Deci, toate F-spaţiile liniare cu aceeaşi dimensiune n sînt izomorfe.

Fie $\varphi : U \to V$ o aplicaţie liniară şi U, V spaţii liniare de dimensiuni n, respectiv m. Se definesc:

- *imaginea* lui φ, $\operatorname{Im} \varphi = \{v \in V \mid \exists u \in U$ astfel încît $\varphi(u) = v\}$
- *nucleul* lui φ, $\operatorname{Ker} \varphi = \{u \in U \mid \varphi(u) = 0\}$

Este binecunoscut (şi uşor de demonstrat) că $\operatorname{Im} \varphi$ este subspaţiu în V şi $\operatorname{Ker} \varphi$ este subspaţiu în U. În plus, are loc rezultatul important:

10 Propoziţie. *Fie $\varphi : U \to V$ o aplicaţie liniară. Atunci:*

$$\dim \operatorname{Im} \varphi + \dim \operatorname{Ker} \varphi = \dim U. \qquad \square$$

O aplicaţie liniară $\varphi : U \to V$ este perfect determinată dacă se cunosc valorile lui φ pe o bază $\{u_1, \ldots, u_n\}$ a lui U. Fixînd o bază $\{v_1, \ldots, v_m\}$ în V, $\varphi(u_j)$ se scrie în mod unic ca o combinaţie liniară de $\{v_1, \ldots, v_m\}$:

$$\varphi(u_j) = a_{1j} v_1 + \ldots + a_{mj} v_m, \text{ pentru } j = 1, \ldots, n.$$

Se obţine o matrice $A = (a_{ij})$ de tip $m \times n$ cu elemente din F, numită *matricea aplicaţiei liniare* φ (în bazele alese).

Invers, fiind dată o matrice $A = (a_{ij}) \in \mathrm{M}(m, n, F)$, există o unică aplicaţie liniară $\varphi_A : U \to V$ astfel încît

$$\varphi_A(u_j) = a_{1j}v_1 + \ldots + a_{mj}v_m, \text{ pentru } j = 1, \ldots, n.$$

Mai simplu, putem vedea A ca aplicaţie liniară definită pe spaţiul vectorilor coloană F^n cu valori în F^m,

$$(x_1, \ldots, x_n)^T \mapsto A(x_1, \ldots, x_n)^T.$$

Matricea compunerii a două aplicaţii liniare este produsul matricelor corespunzătoare (acesta este şi motivul pentru care se defineşte înmulţirea matricelor în modul cunoscut).

11 Propoziţie. *Fie* $A \in \mathrm{M}(m, n, F)$. *Atunci următoarele numere sînt egale:*

- numărul maxim de linii liniar independente ale lui A;

- numărul maxim de coloane liniar independente ale lui A;

- ordinul maxim al minorilor nenuli ai lui A;

- dimensiunea subspaţiului $\mathrm{Im}\varphi_A$.

Acest număr se numeşte rangul lui A şi se notează rang A. □

Revenim la coduri.

12 Definiţie. Fie F un corp finit cu q elemente. Se numeşte *cod liniar* de lungime n peste F orice subspaţiu liniar C al lui F^n.

Cu alte cuvinte, C este o mulţime de cuvinte de lungime n în care simbolurile sînt elemente din F, închisă la adunarea (pe componente) din F^n şi la înmulţirea cu scalari din F.

Dimensiunea codului liniar C este dimensiunea lui C ca spaţiu liniar peste F. Dacă C este cod de lungime n, dim $C = k$ şi distanţa

minimă a lui C este d, spunem că C este cod liniar *de tip* $[n, k, d]_q$ (sau *cod liniar q-ar de tip* $[n, k, d]$); n, k, d se numesc *parametrii* codului C. Observaţi că această notaţie este în acord cu cea de la **I.11**: C este F-spaţiu liniar de dimensiune k, deci $C \cong F^k$ şi C are q^k cuvinte cod.

La un cod liniar C de tip $[n, k, d]$, cuvintele cod au lungime n; numărul de simboluri care poartă informaţie este k. Restul de $n - k$ simboluri sînt folosite pentru corectare/detectare de erori. *Rata* codului este $R = k/n$.

13 Exemplu. Codul de repetiţie de lungime 3 peste $\mathbb{F}_2$ în exemplul **I.1** este $C = \{000, 111\}$, care este un subspaţiu în $\mathbb{F}_2^3$ de dimensiune 1 (de ce?). Distanţa minimă a lui C este 3, deci C este un cod binar tip [3, 1, 3]. Astfel, capacitatea de corectare a lui C este $e(C) = 1$.

Pentru un cod C dat, determinarea distanţei minime este foarte importantă. A priori, pentru aceasta ar trebui să considerăm toate distanţele $d(x, y)$ cu $x, y \in C$ distincte, adică $|C|\cdot(|C| - 1)/2$ distanţe, ceea ce este practic inabordabil (de exemplu, un cod Reed-Solomon folosit în CD-uri are $256^{28} \approx 2.69\cdot 10^{67}$ cuvinte cod). La coduri *liniare*, avem deja o sarcină uşurată:

14 Propoziţie. *Fie F un corp finit. Atunci distanţa Hamming pe F^n este invariantă la translaţii: $d(x, y) = d(x + z, y + z)$, $\forall x, y, z \in F^n$. În particular, $d(x, y) = d(x - y, 0)$ şi deci distanţa minimă a unui cod <u>liniar</u> $C \leq F^n$ este:*

$$d(C) = \min\{d(x, 0) \mid x \in C, x \neq 0\}. \qquad \square$$

Ponderea (*Hamming*) wt(x) a unui cuvînt (vector) $x = x_1 \ldots x_n \in F^n$ se defineşte ca numărul coordonatelor sale nenule (echivalent, wt(x) = $d(x, 0)$). Notaţia *wt* vine de la *weight* (greutate, pondere). Deci:

15 Corolar. *Distanţa minimă a unui cod liniar este ponderea minimă nenulă a cuvintelor cod.* □

Aşadar, în locul calculului tuturor celor $|C|\cdot(|C| - 1)/2$ distanţe, codurile liniare cer „doar" $|C| - 1$ calcule de ponderi în scopul aflării distanţei minime. În multe cazuri acest calcul este tot prea lung, dar există alternative mai rapide (Teorema **21** de mai jos).

Cum putem descrie în mod concret un cod liniar? Există două moduri naturale de a da un subspaţiu liniar C (un cod liniar) de dimensiune k în F^n:

- se dă o *bază* a lui C (adică se dau k *vectori liniar independenţi în* C);

- se descrie C ca *mulţimea soluţiilor unui sistem omogen de* $n - k$ *ecuaţii liniar independente.* Reamintim că, *dacă matricea* H *a unui sistem liniar omogen cu* n *necunoscute are rang* r*, atunci mulţimea soluţiilor sistemului este subspaţiu liniar în* F^n*, de dimensiune* $n - r$*, numit şi spaţiul soluţiilor sistemului.* Interpretînd H ca aplicaţie liniară, aceasta nu este decît o reformulare a propoziţiei **10.**

Corespunzător, se obţin următoarele noţiuni:

16 Definiţie. Fie $C \leq F^n$ un cod liniar de dimensiune $k \leq n$ peste corpul F. O *matrice generatoare* a lui C este o matrice

$G \in \mathrm{M}(k, n, F)$ ale cărei *linii* (văzute ca vectori în F^n) formează o bază în C. Deci, o matrice G este matrice generatoare pentru C dacă şi numai dacă G este o matrice $k \times n$ cu liniile liniar independente (condiţie echivalentă cu rang $G = k$), iar subspaţiul generat de liniile lui G este C.

O *matrice de paritate* (se mai foloseşte terminologia *„matrice de control”*) a lui C este o matrice $H = (h_{ij}) \in \mathrm{M}(n - k, n, F)$ astfel încît, $\forall x = (x_1, \ldots, x_n) \in F^n$:

$$x \in C \Leftrightarrow h_{i1}x_1 + \ldots + h_{in}x_n = 0,\ 1 \le i \le n - k.$$

Deci, pentru ca H să fie o matrice de paritate pentru codul C de dimensiune k, trebuie ca rang $H = n - k$ şi să aibă loc:

$$\forall x \in F^n\colon x \in C \Leftrightarrow Hx^T = 0 \in \mathrm{M}(n - k, 1, F).$$

O matrice de paritate a codului C nu este altceva decît matricea unui sistem liniar omogen (cu ecuaţiile liniar independente) ale cărui soluţii sînt exact vectorii din C.

17 Observaţie. Denumirea de *matrice de paritate* (*parity-check matrix*) provine din cazul particular al codului binar următor: se fixează $k \in \mathbb{N}^*$ şi orice vector $x_1 \ldots x_k \in \mathbb{F}_2^k$ este codat ca $x_1 \ldots x_k x_{k+1}$, unde x_{k+1} este astfel încît $x_1 + \ldots + x_k + x_{k+1} = 0$ (în $\mathbb{F}_2$). Codul este deci

$$C = \{x_1 \ldots x_k x_{k+1} \in \mathbb{F}_2^{k+1} \mid x_1 + \ldots + x_k + x_{k+1} = 0\}.$$

Orice cuvînt cod are un număr par de biţi egali cu 1 şi de aceea bitul x_{k+1} este numit *bit de paritate*. Verificarea faptului că un cuvînt x este cuvînt cod revine la a verifica „paritatea” cuvîntului, adică un tip particular de sistem liniar omogen pe care îl satisfac coordonatele lui x. Acesta se numeşte codul (binar) de paritate şi

este liniar, de tip $[k+1, k, 2]$ (demonstraţi!). Ce rată de transmisie are?

18 Definiţie. Definim *produsul scalar standard pe* F^n*:*

$$\forall x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in F^n,$$
$$\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n \in F.$$

Doi vectori $x, y \in F^n$ se numesc *ortogonali* sau *perpendiculari* dacă $\langle x, y\rangle = 0$. Dacă $S \subseteq F^n$, fie $S^\perp := \{y \in F^n \mid \langle x, y\rangle = 0, \forall x \in S\}$ *ortogonalul lui S.*

Aşadar: $H \in \mathrm{M}(n-k, n, F)$ *este matrice de paritate pentru* $C \leq F^n \Leftrightarrow$ *liniile lui H sînt liniar independente şi C este mulţimea vectorilor din* F^n *ortogonali pe toate liniile lui H.*

Produsul scalar standard e o *formă biliniară simetrică* pe F^n, adică este o funcţie $\langle\cdot, \cdot\rangle$: $F^n \times F^n \to F$ care satisface proprietăţile:

$$\langle x, y\rangle = \langle y, x\rangle$$
$$\langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle$$
$$\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$$
$$\langle \alpha x, y\rangle = \alpha\langle x, y\rangle$$

pentru orice $x, y, z \in F^n$, $\alpha \in F$. Demonstraţi!

19 Propoziţie. *Fie* $S \subseteq F^n$*. Atunci:*

a) $S^\perp$ *este un subspaţiu în* F^n*, numit* subspaţiul ortogonal pe *S*;

b) $S \subseteq S^{\perp\perp}$;

c) Dacă $T \subseteq F^n$ *şi* $S \subseteq T$*, atunci* $T^\perp \subseteq S^\perp$;

d) Dacă $U \leq E$*, atunci* $U^\perp = S^\perp$*, pentru orice sistem de generatori S al lui U.*

Demonstraţie. a), c) Verificare directă, cu definiţia.

b) Fie $x \in S$. Atunci $\langle x, y\rangle = 0, \ \forall y \in S^{\perp}$, deci x este în ortogonalul lui $S^{\perp}$.

d) Fie $S = \{v_1, \ldots, v_k\}$. Deoarece $S \subseteq U$, avem $U^{\perp} \subseteq S^{\perp}$. Orice $x \in U$ este o combinaţie liniară de v_i : $x = \lambda_1 v_1 + \ldots + \lambda_k v_k$, pentru nişte $\lambda_1, \ldots, \lambda_k \in F$. Pentru orice $y \in S^{\perp}$,

$$\langle x, y\rangle = \langle \lambda_1 v_1 + \ldots + \lambda_k v_k, y\rangle = \lambda_1 \langle v_1, y\rangle + \ldots + \lambda_k \langle v_k, y\rangle = 0,$$

ceea ce arată că $y \in U^{\perp}$. □

20 Teoremă. *Fie C un cod liniar de tip* $[n, k, d]$ *peste corpul F. Atunci:*

a) $C^{\perp}$ *este un cod liniar de dimensiune* $n - k$ *(numit codul dual lui C).*

b) $(C^{\perp})^{\perp} = C$.

c) Dacă G este o matrice generatoare a lui C, atunci G este o matrice de paritate pentru $C^{\perp}$. *Dacă H este matrice de paritate pentru C, atunci H este matrice generatoare pentru* $C^{\perp}$.

Demonstraţie. a) Fie $G \in \mathrm{M}(k, n, F)$ o matrice generatoare pentru C. Atunci $x \in C^{\perp} \Leftrightarrow x$ este ortogonal pe liniile lui G (căci aceste linii generează C). Deci $C^{\perp}$ este spaţiul soluţiilor sistemului liniar omogen de matrice G, care este de dimensiune $n - \mathrm{rang} G = n - k$.

b), c) Exerciţiu. □

Deoarece un spaţiu liniar poate avea multe baze, un cod liniar poate avea multe matrice generatoare şi multe matrice de paritate. Observaţi că, spre deosebire de spaţiile liniare reale (cum este $\mathbb{R}^n$), un vector nenul în F^n poate fi ortogonal pe el însuşi (de ex. (1, 1) în $\mathbb{F}_2{}^2$), deci este posibil ca C şi $C^{\perp}$ să aibă intersecţie nenulă. Dacă $C = C^{\perp}$, C se numeşte *cod autodual* (*self-orthogonal code*).

Distanţa minimă a unui cod liniar poate fi citită de pe matricea sa de paritate:

21 Teoremă. *Fie C un cod liniar peste F şi $H \in \mathrm{M}(n-k, n, F)$ o matrice de paritate pentru C. Atunci distanţa minimă d a lui C este:*

$$d = \min\{\delta \in \mathbb{N} \mid \text{există } \delta \text{ coloane în } H \text{ liniar dependente}\} =$$
$$= 1 + \max\{\varepsilon \in \mathbb{N} \mid \text{orice } \varepsilon \text{ coloane din } H \text{ sînt liniar independente}\}.$$

Demonstraţie. Fie $H_i \in F^{n-k}$ coloana i a lui H, $1 \le i \le n$. Avem $(x_1, \ldots, x_n) \in C$ dacă şi numai dacă $x_1H_1 + \ldots + x_nH_n = 0$. Fie $d' = \min\{\delta \mid \text{există } \delta \text{ coloane în } H, \text{ liniar dependente}\}$.

Fie $(x_1, \ldots, x_n) \in C$, de pondere minimă d. Atunci coloanele H_i pentru care $x_i \neq 0$ (în număr de d) sînt liniar dependente, deci $d' \le d$. Reciproc, fie o mulţime de d' coloane $\{H_i\}_{i \in J}$, liniar dependentă. Atunci există $(x_1, \ldots, x_n) \in F^n$ cu $x_1H_1 + \ldots + x_nH_n = 0$ şi $x_i \neq 0 \Rightarrow i \in J$. Deci $x = (x_1, \ldots, x_n) \in C$ şi $d \le \mathrm{wt}(x) \le d'$. □

22 Observaţie. Dacă o coloană a matricei de paritate este 0, atunci distanţa minimă a codului este 1 (deci codul este neinteresant din punct de vedere al capacităţii de corectare). Justificaţi!

Construim o clasă importantă de coduri de distanţă minimă 3, pe baza acestui rezultat. Familia de coduri descrisă în continuare a fost descoperită independent în 1949 de Marcel Golay şi în 1950 de Richard Hamming.

23 Definiţie. (Coduri Hamming) Fie F corp cu q elemente şi $r \in \mathbb{N}^*$ fixat. Definim *codul Hamming q-ar de redundanţă r*, notat $H_{q, r}$, astfel:

Construim o matrice de paritate H formată din cît mai multe coloane de lungime r care să aibă orice 2 coloane liniar independente (deci distanţa minimă a codului va fi cel puţin 3). Aceasta înseamnă ca, dacă o coloană apare în matrice, nici un multiplu al coloanei nu mai poate apărea. Aşadar, alegem cîte un vector nenul din fiecare subspaţiu de dimensiune 1 din F^r şi construim matricea H ce are drept coloane aceşti vectori (într-o ordine arbitrară). Matricea H este prin definiţie matricea de paritate H a codului $H_{q, r}$.

Un alt mod de a exprima ideea de mai sus este: pe $F^r \setminus \{0\}$ definim relaţia de echivalenţă:

$$\forall x, y \in F^r,\ x \sim y \Leftrightarrow \exists \alpha \in F^* \text{ astfel încît } y = \alpha \cdot x$$

Din fiecare clasă de echivalenţă alegem cîte un vector. Aceşti vectori sînt coloanele matricei de paritate H.

Cîte coloane are H? Se observă că clasele de echivalenţă de mai sus au fiecare cîte $q - 1$ elemente (clasa de echivalenţă a lui $x \in F^r \setminus \{0\}$ este $\{\alpha \cdot x \mid \alpha \in F^*\}$). Cum reuniunea lor (disjunctă) este $F^r \setminus \{0\}$, avem $q^r - 1 = n(q - 1)$, unde n este numărul claselor de echivalenţă.

Deci H are $n = (q^r - 1)/(q - 1)$ coloane şi r linii.

Pentru ca $H \in \mathrm{M}(r, n, K)$ să fie matrice de paritate, trebuie ca rang $H = r$. Există într-adevăr r coloane liniar independente în H, de exemplu (multipli scalari de) $(1, 0, \ldots, 0)^T$, $(0, 1, \ldots, 0)^T$, …, $(0, 0, \ldots, 1)^T$.

Există 3 coloane liniar dependente (justificaţi!), deci distanţa minimă a lui $H_{q,r}$ este 3, din Teorema **II.21.** În concluzie:

24 Propoziţie. *$H_{q,r}$ este un cod liniar q-ar de tip* $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$. □

25 Observaţie. Construcţia de mai sus nu determină în mod unic matricea de paritate H. De exemplu, pentru două ordonări diferite ale coloanelor se obţin două matrice de paritate H, H' distincte şi deci coduri Hamming corespunzătoare *distincte* C, C'. Însă aceste coduri sînt *echivalente pînă la o permutare*, în sensul că există o permutare $\sigma \in S_n$ (grupul permutărilor mulţimii $\{1, 2, \ldots, n\}$) astfel încît:

$$\forall x_1 \ldots x_n \in F^n : x_1 \ldots x_n \in C \Leftrightarrow x_{\sigma(1)} \ldots x_{\sigma(n)} \in C'.$$

Altfel spus, funcţia $\varphi_\sigma : C \to C'$, $\varphi_\sigma(x_1 \ldots x_n) = x_{\sigma(1)} \ldots x_{\sigma(n)}$ este o bijecţie.

Pe de altă parte, dacă în matricea de paritate H a codului Hamming C se înlocuieşte coloana i (fie aceasta P_i) cu coloana αP_i, unde $\alpha \in F^*$, atunci matricea H' obţinută este matrice de paritate pentru un cod C'. Are loc:

$$\forall x_1 \ldots x_i \ldots x_n \in F^n, \quad x_1 \ldots x_i \ldots x_n \in C \quad \Leftrightarrow \quad x_1 \ldots (\alpha^{-1} x_i) \ldots x_n \in C.$$

Această situaţie sugerează definirea unui alt tip de echivalenţă: două coduri C, C' de lungime n peste corpul F se numesc *diagonal echivalente* dacă $\exists \ \alpha = (\alpha_1, \ldots, \alpha_n) \in (F^*)^n$ astfel încît $\forall (x_1, \ldots, x_n) \in F^n$, avem $(x_1, \ldots, x_n) \in C \Leftrightarrow (\alpha_1 x_1, \ldots, \alpha_n x_n) \in C'$, adică $\varphi_\alpha : C \to C'$, $\varphi_\alpha(x_1, \ldots, x_n) = (\alpha_1 x_1, \ldots, \alpha_n x_n)$, este o bijecţie.

Se demonstrează uşor că funcţiile φ_α şi φ_σ de mai sus sînt *izometrii*, adică *păstrează distanţele Hamming* (o funcţie

$\varphi : F^n \to F^n$ cu proprietatea că $d(\varphi(x), \varphi(y)) = d(x, y)$, pentru orice $x, y \in F^n$, se numeşte *izometrie*).

26 Exerciţiu. Folosim notaţiile de mai sus. Demonstraţi că:

a) Compunerea a două izometrii (liniare) este o izometrie (liniară).

b) Orice izometrie este bijectivă. Mulţimea izometriilor liniare ale lui F^n formează un grup în raport cu compunerea.

c) $\varphi_\alpha \circ \varphi_\sigma\ ((x_1, \ldots, x_n)) = (\alpha_1 x_{\sigma(1)}, \ldots, \alpha_n x_{\sigma(n)})$. Notăm această izometrie cu $M_{\alpha, \sigma}$.

d) $M_{\alpha, \sigma} \circ M_{\beta, \tau}((x_1, \ldots, x_n)) = (\alpha_1 \beta_{\sigma(1)} x_{\tau(\sigma(1))}, \ldots, \alpha_n \beta_{\sigma(n)} x_{\tau(\sigma(n))})$.

e) Orice izometrie liniară duce vectori de pondere 1 în vectori de pondere 1.

f) Orice izometrie liniară este de forma $M_{\alpha, \sigma}$, cu $\alpha = (\alpha_1, \ldots, \alpha_n) \in (F^*)^n$ şi $\sigma \in S_n$.

g) Scrieţi matricea izometriei liniare $M_{\alpha, \sigma}$. O astfel de matrice se numeşte matrice *monomială*.

27 Definiţie. Codurile C şi C' de lungime n peste F se numesc *izometric echivalente* dacă există o izometrie $\varphi : F^n \to F^n$ astfel încît $\varphi(C) = C'$. Două coduri *liniare* C şi C' se numesc *izometric echivalente* (sau *monomial echivalente*) dacă există o izometrie *liniară* $\varphi : F^n \to F^n$ astfel încît $\varphi(C) = C'$.

Pe mulţimea codurilor liniare de lungime n peste F, relaţia „C este izometric echivalent cu C'" este o *relaţie de echivalenţă*.

Se demonstrează uşor că orice izometrie este injectivă. Întrucît F^n este o mulţime finită, rezultă ca izometriile sînt *bijecţii*. Deci *două coduri izometric echivalente au acelaşi număr de cuvinte*

(aceeaşi dimensiune, pentru coduri liniare). În plus, două coduri izometric echivalente C şi C' se comportă identic din punct de vedere al teoriei codurilor: au aceeaşi distanţă minimă, aceeaşi distribuţie a ponderilor (dacă C are n_k cuvinte de pondere k, C' are tot n_k cuvinte de pondere k). De aceea, este utilă o clasificare a codurilor liniare *pînă la o izometrie* (liniară, în cazul codurilor liniare).

Un studiu aprofundat privind izometriile şi clasele de echivalenţă (pînă la o izometrie) de coduri liniare este realizat în monografia [2].

28 Exemplu. (codul binar Hamming [7, 4, 3]) Pentru $q = 2$ şi $r = 3$, avem $n = 7$. Cum $F = \mathbb{F}_2$, corpul cu două elemente, coloanele lui H sînt unic determinate pînă la o ordonare (orice subspaţiu de dimensiune 1 are un unic vector nenul). Alegem să ordonăm coloanele lexicografic (adică scriem „vertical” toate numerele nenule de 3 cifre în baza 2, în ordine crescătoare). Deci H este:

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

Acest cod are o importanţă istorică deosebită: A fost primul cod *corector* de erori folosit în computere (coduri *detectoare* de erori mai fuseseră folosite înainte).

Studiile superioare ale lui Hamming erau de matematică pură, iar teza sa de doctorat era despre ecuaţii diferenţiale. A făcut parte din "Manhattan Project", proiectul ultrasecret de fabricare a bombei atomice de la Los Alamos din timpul celui de al doilea război mondial. În 1946 a plecat de la Los Alamos la Bell Laboratories:

> *I was a pure mathematician – I felt somewhat lost at the place. Every once in a while I got terribly discouraged at the department being mostly electrical engineering.*

La Bell Labs aveau un computer Model V, care ocupa 90 metri pătraţi, cîntărea 10 tone şi putea rezolva sisteme liniare de 13 ecuaţii în mai puţin de 4 ore. Hamming avea acces doar în weekend la computer; cum nu exista personal de supraveghere în weekenduri, dacă computerul descoperea o eroare, abandona pur şi simplu sarcina şi trecea la următoarea.

> *Two weekends in a row I came in and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed because I wanted those answers and two weekends had been lost. And so I said "Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?"*

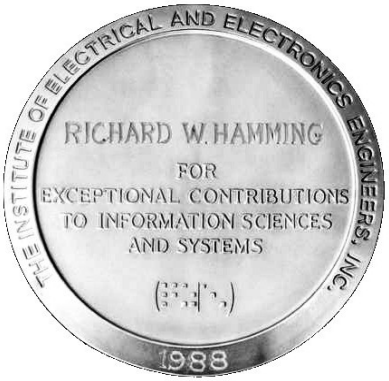
Codul pe care l-a descoperit Hamming este chiar codul binar tip [7, 4, 3] de mai sus, care poate corecta o eroare la 7 simboluri. Nu este totdeauna de dorit să obţinem coduri care să corecteze cît mai multe erori, deoarece rata de transmisie ar putea fi prea mică sau decodarea ar putea consuma prea mult timp. Este necesară obţinerea de coduri suficient de bune pentru o anumită sarcină. Hamming spunea în legătură cu aceasta:

> *The Relay Computer, operating with a self-checking code, stops whenever an error is detected. Under normal operating conditions this amounts to two or three stops per day. However, if we imagine a comparable electronic computing machine operating* 10^5 *times the speed and with elements* 10^3 *times more reliable than relays, we find two to three hundred stops per day.*

Putem spune că Hamming a prevăzut apariţia atît a computerelor rapide de astăzi, cît şi a sistemelor de operare Windows.

O matrice de paritate a codului binar Hamming [7, 4, 3] este imprimată pe medalia "Richard W. Hamming" a IEEE (Institute of Electrical and Electronics Engineers)[5]:

[5] Matricea de pe medalie nu este cea aleasă de noi. Ce legătură este între codurile respective?



Să descriem o modalitate practică de codare şi de decodare pentru acest cod $H_{2,3}$. Întrucît este un cod tip [7, 4], fiecare mesaj de 4 biţi este codat pe un cuvînt cod de 7 biţi. Coordonatele unui cuvînt cod $d = d_1 \ldots d_7 \in H_{2,3}$ satisfac ecuaţia $Pd^{\mathrm{T}} = 0$, adică

$$\begin{aligned} d_1 + d_3 + d_5 + d_7 &= 0 \\ d_2 + d_3 + d_6 + d_7 &= 0 \qquad (*) \\ d_4 + d_5 + d_6 + d_7 &= 0 \end{aligned}$$

Alegem biţii d_1, d_2, d_4 să fie „de control", iar biţii mesajului original sînt plasaţi în poziţiile 3, 5, 6, 7. Biţii d_1, d_2, d_4 se obţin din ecuaţiile de mai sus, adică $d_1 = d_3 + d_5 + d_7$ etc.[6]

La recepţia unui cuvînt de 7 biţi $r = r_1 \ldots r_7$, se verifică dacă r este cuvînt cod (adică dacă $r_1, \ldots, r_7$ satisfac ecuaţiile (*)). Altfel spus, se calculează $(c_1, c_2, c_3) = H(r_1, \ldots, r_7)^T$.

Dacă $(c_1, c_2, c_3) = (0, 0, 0)$, atunci nu au avut loc erori. Dacă $(c_1, c_2, c_3) \neq (0, 0, 0)$, atunci eroarea (presupusă a fi singura) e plasată în bitul a cărui poziţie este dată de numărul binar $\overline{c_3 c_2 c_1}$ (şi

[6] De ce s-a ales astfel poziţia biţilor de control?

deci poate fi corectată!). Demonstraţia acestei „scamatorii” e propusă ca exerciţiu.

Acest cod este mai eficient decît codul binar de repetiţie de lungime 3. Rata sa este 4/7, o îmbunătăţire substanţială faţă de 1/3. Dar poate corecta maximum o eroare la 7 biţi, în timp ce codul de repetiţie corectează o eroare la 3 biţi.

29 Exerciţiu. Presupunem că folosim codul $H_{2,3}$ şi că s-a recepţionat cuvîntul 110100. Decideţi dacă au avut erori şi corectaţi.

În continuare prezentăm cîteva inegalităţi (*bounds*) pe care le satisfac parametrii unui cod oarecare. Pentru *n, q, d* fixate, un cod *q*-ar *C* de lungime *n* şi distanţă minimă *d* nu poate avea prea multe cuvinte (cuvintele cod trebuie sa fie suficient de „împrăştiate”, la distanţă cel puţin *d* unul de altul).

30 Teoremă (inegalitatea Hamming). *Fie C un cod q-ar (nu neapărat liniar) de lungime n cu capacitate de corectare e. Atunci*

$$|C|\sum_{i=0}^{e} C_n^i (q-1)^i \le q^n.$$

Demonstraţie. Sînt q^n elemente în A^n şi $|C|$ cuvinte cod în C. Sferele de rază e centrate în cuvintele cod sînt disjuncte două cîte două, deci $|C|\cdot|B(x, e)| \le q^n$. Înlocuind $|B(x, e)|$ cu volumul sferei (**I.6**) se obţine rezultatul. □

Pentru orice cod C (nu neapărat liniar) de capacitate de corectare e, sferele centrate în cuvintele cod de rază e sînt disjuncte; dacă reuniunea lor este întreg F^n, atunci codul se

numeşte (*e*-)*perfect*. Echivalent, *un cod este perfect dacă are loc egalitate în inegalitatea Hamming.*

31 Exerciţiu. Orice cod *e*-perfect are distanţă minimă $2e + 1$.

Codurile Hamming sînt 1-*perfecte* (verificaţi!). Altfel spus, orice cuvînt din F^n se găseşte la distanţă ≤ 1 de exact un cuvînt cod. Acest fenomen are aplicaţii oarecum surprinzătoare.

32 Aplicaţie. *Jocul Pronosport* constă în ghicirea rezultatelor a 13 partide de fotbal. Rezultatul unei partide este un element al mulţimii {x, 1, 2} (x = egalitate; 1 = cîştigă gazdele; 2 = cîştigă oaspeţii). Jucătorii completează *variante*; numim variantă orice 13-uplu $(s_1,\ldots, s_{13})$, cu $s_i \in \{x, 1, 2\}$. Pentru a cîştiga cu siguranţă premiul I (13 rezultate exacte), este necesară a priori completarea a 3^{13} variante. Se pune întrebarea: *care este numărul minim de variante ce trebuie completate pentru a cîştiga cu siguranţă premiul* II (12 *rezultate exacte*)?

Reformulăm problema în termenii teoriei codurilor: *Fie* $F = \mathbb{Z}_3$. *Să se găsească o submulţime* (*un cod*) $S \subseteq F^{13}$ (*cît mai „mică”*), *astfel încît orice cuvînt din* F^{13} *să se găsească la distanţă cel mult* 1 *de un cuvînt din S. Altfel spus, să se găsească un cod* 1-*perfect de lungime* 13 *peste* $\mathbb{Z}_3$.

Răspunsul este dat de codul Hamming cu $q = 3$ şi $r = 3$: avem $n = (3^3 - 1)/2 = 13$, deci este un cod tip $[13, 10, 3]_3$. Numărul de cuvinte cod (de „variante”) este $3^{10} = 59049$.

33 Teoremă. (inegalitatea Singleton, Singleton Bound) *Fie C un cod de lungime n şi distanţă minimă d peste un alfabet A cu q*

simboluri. Atunci $|C| \le q^{n-d+1}$. *Dacă C este liniar, atunci* $d \le n - k + 1$.

Demonstraţie. Pentru $(x_1, \ldots, x_{n-d+1}) \in A^{n-d+1}$ fixat, există cel mult un cuvînt cod în C ale cărui coordonate de pe primele $n - d + 1$ locuri sînt $(x_1, \ldots, x_{n-d+1})$ (dacă ar exista două astfel de cuvinte în C, distanţa dintre ele ar fi $< d$). Deci $|C| \le |A|^{n-d+1} = q^{n-d+1}$. Dacă C este liniar, atunci $|C| = q^k$. □

Codurile liniare pentru care $d = n - k + 1$ se numesc *coduri MDS* (*Maximum Distance Separable*) şi sînt „cele mai bune" dintr-un anumit punct de vedere (distanţa minimă a codului este maxim posibilă dacă dimensiunea şi lungimea codului sînt fixate).

Rezultatele de mai sus limitează numărul cuvintelor cod, pentru o lungime şi o distanţă minimă date („upper bounds"). Iată şi rezultate care afirmă că, pentru o distanţă minimă dată, există coduri care conţin măcar un număr garantat de cuvinte („lower bounds").

34 Teoremă (Inegalitatea Gilbert, Gilbert Bound) *Fie* $q, n \in \mathbb{N}$ *şi* $d \le n$. *Atunci există coduri q-are (nu neapărat liniare) C de lungime n şi distanţă minimă d astfel încît:*

$$|C| \ge \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}.$$

Demonstraţie. Dintre codurile q-are de lungime n şi distanţă minimă d alegem un cod C cu un număr maxim de cuvinte. Presupunem că pentru C inegalitatea de mai sus este falsă. Atunci

reuniunea sferelor de rază $d-1$ centrate în cuvintele din C este strict inclusă în F^n, deoarece:

$$\left|\bigcup_{x\in C} B_{d-1}(x)\right| \le |C|\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i < q^n,$$

Deci, există $v \in F^n$ cu $d(v, C) = \min\{d(v, x) \mid x \in C\} \ge d$. Atunci $C \cup \{v\}$ are mai multe cuvinte decît C şi are distanţa minimă d, contradicţie. □

Versiunea liniară a rezultatului de mai sus este următoarea:

35 Teoremă *Fie F un corp finit cu q elemente, $n \in \mathbb{N}$ şi $d \le n$. Atunci există coduri liniare C de lungime n peste F şi distanţă minimă d astfel încît:*

$$|C| \ge \frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i}.$$

Demonstraţie. Dintre codurile liniare peste F de lungime n şi distanţă minimă d alegem un cod C cu un număr maxim de cuvinte. Ca la demonstraţia precedentă, dacă concluzia este falsă, atunci există un $v \in F^n$ cu $d(v, C) = \min\{d(v, x) \mid x \in C\} \ge d$. Fie C' subspaţiul liniar generat de C şi v. Demonstrăm că $d(C') = d$. E suficient să arătăm că pentru orice $\lambda, \mu \in F$, $\forall x, y \in C$, $x + \lambda v \ne y + \mu v$ implică $d(x + \lambda v, y + \mu v) \ge d$. Avem:

$$d(x + \lambda v, y + \mu v) = \mathrm{wt}(x - y + (\lambda - \mu)v) = d(x - y, (\mu - \lambda)v).$$

Dacă $\mu - \lambda = 0$, atunci $d(x - y, 0) = d(x, y) \ge d$ dacă $x \ne y$.

Dacă $\mu - \lambda \ne 0$, atunci:

$$\mathrm{wt}(x - y + (\lambda - \mu)v) = \mathrm{wt}((\lambda - \mu)^{-1}(x - y) + v) = d((\lambda - \mu)^{-1}(x - y), v) \ge d,$$

pentru că $(\lambda - \mu)^{-1}(x - y) \in C$.

Cum $v \notin C' \setminus C$, C' include strict pe C, contradicţie cu maximalitatea lui C. □

36 Teoremă (Inegalitatea Varshamov, Varshamov Bound) *Fie F un corp finit cu q elemente. Dacă*

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i .$$

atunci există un cod F-liniar C, de tip $[n, k]$, cu distanţa minimă cel puţin d.

Demonstraţie. Arătăm că există o matrice H tip $(n-k) \times n$ peste F astfel încît orice $d-1$ coloane ale lui H sînt liniar independente. Construim coloanele $c_1, \ldots, c_n$ ale lui H astfel:

Fie c_1 orice vector nenul din F^{n-k}. Fie $c_2 \in F^{n-k} \setminus < c_1 >$.

Pentru orice $2 \le j \le n$, fie c_j orice vector care nu se poate scrie ca o combinaţie liniară de $d-2$ (sau mai puţini) vectori dintre $c_1, \ldots, c_{j-1}$. Există un astfel de vector?

O combinaţie liniară de i vectori $(i \le d-2)$ aleşi dintre $c_1, \ldots, c_{j-1}$ este determinată dacă alegem i indici din $j-1$ şi ataşăm fiecărui indice un coeficient nenul din F. Aceasta se poate face în $\binom{j-1}{i}(q-1)^i$ moduri. Deci există cel mult $\sum_{i=0}^{d-2} \binom{j-1}{i}(q-1)^i$ astfel de vectori. Deoarece

$$\sum_{i=0}^{d-2} \binom{j-1}{i}(q-1)^i \le \sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i < q^{n-k},$$

vectorul c_j poate fi găsit, pentru orice $j \le n$.

Fie C subspaţiul ortogonal pe liniile lui H. Atunci C are dimensiune cel puţin k (liniile lui H pot să nu fie liniar independente, adică rang $H < n - k$). Deoarece un cuvînt din C de pondere $< d$ corespunde unei combinaţii liniare nule de mai puţin decît d coloane ale lui H, ponderea minimă a cuvintelor nenule din C este cel puţin d. Dacă vrem un cod de dimensiune exact k, alegem orice subspaţiu al lui C de dimensiune k. □

Versiunile „asimptotice" (nu aprofundăm acest aspect) ale acestor inegalităţi coincid, şi de aceea se vorbeşte de „inegalitatea Gilbert-Varshamov".

37 Observaţie. O problemă importantă în teoria codurilor (departe de a fi rezolvată în cazul general) este aceea de a determina, pentru q fixat, cardinalul celui mai mare cod (respectiv celui mai mare cod liniar) de lungime n şi distanţă minimă d, notat $A_q(n, d)$ (respectiv $B_q(n, d)$). Echivalent, se pune problema găsirii codului q-ar de o mărime (dimensiune, în cazul codurilor liniare) dată, care să aibă cea mai mare distanţă minimă. Există mai multe baze de date cu diverse estimări în această direcţie. De exemplu, la *http://www.codetables.de* [7] există astfel de tabele. Pentru $q = 2$, $n = 55$, $k = 17$, această bază de date furnizează $16 \le d \le 19$. Aceasta înseamnă că se poate construi un cod binar ($q = 2$) liniar de tip [55, 17, 16], şi că orice cod binar liniar tip [55, 17, d] are $d \le 19$. Dar nu se ştie în acest moment dacă nu există cumva coduri binare liniare [55, 17, 17], [55, 17, 18] sau [55, 17, 19].

Exerciţii

1. Fie F un corp cu q elemente, $n \in \mathbb{N}$ şi $m < q^n$. Cîte coduri de lungime n peste F cu m cuvinte există? Cîte din acestea sînt liniare? (*Ind.* Dacă m nu este de forma q^k, nu există subspaţii liniare cu m elemente în F^n. Dacă $m = q^k$, trebuie găsit numărul subspaţiilor liniare de dimensiune k din F^n.)

2. Fie $C \leq F^n$, $\dim C = k$ şi fie $y \notin C^\perp$. Demonstraţi că funcţia $p_y : C \to F$, $p_y(x) = \langle x, y \rangle$ este un morfism surjectiv de spaţii liniare, iar nucleul său are dimensiunea $k - 1$. Arătaţi că, $\forall \alpha \in F$, există exact q^{k-1} elemente x în C astfel încît $\langle x, y \rangle = \alpha$. (*Ind.* Aplicaţi teorema fundamentală de izomorfism.)

3. Scrieţi o matrice de paritate pentru codul din Aplicaţia **32**.

4. Demonstraţi că a scrie o matrice de paritate a unui cod $[n, k, d]$ peste F este echivalent cu a scrie n vectori coloană din F^{n-k} cu proprietatea că oricare $d - 1$ sînt liniar independenţi (şi există d liniar dependenţi).

5. (Coduri de repetiţie) Considerăm următorul procedeu de codare: pentru a coda cuvinte oarecare de lungime k (peste alfabetul binar $\{0, 1\} = F$) se repetă fiecare bit de r ori; astfel, orice cuvînt $x_1 \ldots x_k$ este codat ca $x_1 \ldots x_1 x_2 \ldots x_2 \ldots x_k \ldots x_k$ (fiecare x_i apare de r ori). Se obţine un cod de lungime kr.

a) Arătaţi că acest cod este liniar, de dimensiune k.

b) Arătaţi că distanţa sa minimă este r.

c) Folosim codul de repetiţie de tip [3,1]. Dacă se primeşte mesajul 000101111100, unde au apărut erori? Corectaţi-le.

d) Care este rata de transmisie a codului de repetiţie tip $[kr, k]$?

6. Scrieţi toate cuvintele codului Hamming $H_{2,2}$. Care este rata sa de transmisie?

7. Scrieţi parametrii şi matrice de paritate pentru codurile Hamming $H_{2,r}$, cu $r \leq 4$.

8. Scrieţi toate cuvintele codului binar Hamming tip [7, 4, 3]. Care este rata sa de transmisie?

9. (Algoritm de decodare pentru coduri binare Hamming) Folosim notaţiile din Exemplul **28.** Fie $e = e_1 \ldots e_7$ *vectorul eroare* şi fie h_1, …, h_7 coloanele lui H.

a) Demonstraţi că

$$H(r_1, \ldots, r_7)^T = H(e_1, \ldots, e_7)^T = e_1h_1 + \ldots + e_7h_7$$

b) Dacă are loc exact o eroare, atunci $\mathrm{wt}(e) = 1$. Fie $e_i \neq 0$. Atunci $(c_1, c_2, c_3)^T = h_i$.

c) Folosind faptul că h_i este numărul i scris în baza 2, corectaţi eroarea.

d) Generalizaţi algoritmul pentru orice cod binar Hamming $H_{2,r}$.

10. Calculaţi numărul de cuvinte şi rata de transmisie ale codului Hamming $H_{q,r}$ (în general) şi pentru $q = 2$, $r \leq 5$.

11. Fie C un cod liniar de tip $[n, k, d]$ peste F, corp cu q elemente.

a) Arătaţi că: ori toate cuvintele din C încep cu 0, ori exact $1/q$ din cuvinte încep cu 0. (*Ind.* Fie $D := \{x_1 \ldots x_n \in F^n \mid x_1 = 0\}$, subspaţiu liniar în F^n. Aplicaţi formula pentru $\dim(C + D)$).

b) Demonstraţi că suma ponderilor tuturor cuvintelor lui C este cel mult $n(q-1)q^{k-1}$.

c) Demonstraţi că $d \leq \dfrac{n(q-1)q^{k-1}}{q^k - 1}$. (*Ind.* Distanţa minimă este mai mică decit media ponderilor cuvintelor nenule.)

d) (Inegalitatea Plotkin) Demonstraţi că, dacă $\frac{d}{n} > \frac{q-1}{q}$, atunci $|C| \le \frac{d}{d - \frac{q-1}{q} n}$.

12. Arătaţi că un cod liniar C peste $\mathbb{F}_q$ care are aceiaşi parametri ca un cod Hamming trebuie să fie un cod Hamming. (*Ind.* Deoarece $d(C) = 3$, o matrice de paritate a lui C trebuie să aibă orice două coloane liniar independente.)

13. Fie $q = p^t$, cu p un număr prim. Demonstraţi că un cod q-ar perfect are cardinalul o putere a lui p.

14. Demonstraţi că un cod binar perfect cu distanţa minimă 7 are lungimea $n = 7$ sau $n = 23$. (*Ind.* Se scrie inegalitatea lui Hamming cu egalitate. După calcule, rezultă $(n + 1)(n^2 - n + 6) = 2^t \cdot 6$, cu $t \ge 6$ din inegalitatea Singleton. Rezultă că $n + 1 = 2^a \cdot 3^b$, cu $b = 0$ sau 1. O analiză a celor două cazuri arată că $a > 3$ duce la contradicţii.)[7]

[7] Puteţi da exemplu de cod binar perfect de lungime 7? Există şi un cod binar liniar perfect de lungime 23 şi distanţă minimă 7 (codul *Golay* binar). Demonstraţi că dimensiunea acestui cod este 12.

III. Corpuri finite

Corpurile finite au depăşit de mult stadiul de curiozitate matematică. Corpurile finite sînt esenţiale în tehnologiile legate de *transmisia, stocarea, secretizarea şi prelucrarea informaţiei digitale. Codurile liniare corectoare de erori* se bazează pe corpuri finite. Unele din cele mai puternice *scheme criptografice* şi de *autentificare* moderne au la bază logaritmul discret într-un corp finit.

Clasificarea corpurilor finite este simplă: *pentru orice număr q, putere a unui prim, există un unic (pînă la izomorfism) corp finit cu q elemente, notat* $\mathbb{F}_q$. *Acestea sînt toate corpurile finite (pînă la izomorfism)*. În plus, grupul $(\mathbb{F}_q^*, \cdot)$ este ciclic. Vom demonstra în continuare aceste fapte. Reamintim cîteva noţiuni fundamenale de algebră.

Se numeşte *inel* un triplet $(R, +, \cdot)$ format dintr-o mulţime nevidă R şi două operaţii interne pe R,

$$+ : R \times R \to R,\ (x, y) \mapsto x + y,\ \forall x, y \in R \text{ (numită } \textit{adunare}\text{)},$$

$$\cdot : R \times R \to R,\ (x, y) \mapsto x \cdot y,\ \forall x, y \in R \text{ (numită } \textit{înmulţire}\text{)},$$

care satisfac următoarele condiţii:

1) $(R, +)$ este *grup comutativ* (*abelian*), adică

a) $\forall x, y, z \in R, (x + y) + z = x + (y + z)$ (*asociativitatea adunării*);

b) $\exists 0 \in R$ astfel încît, $\forall x \in R, x + 0 = 0 + x = x$ (*există element neutru* 0 *pentru adunare*);

c) $\forall x \in R, \exists -x \in R$ astfel încît $x + (-x) = (-x) + x = 0$ (*orice element x are un opus $-x$*); d) $\forall x, y \in R, x + y = y + x$ (*comutativitatea adunării*);

2) *Înmulţirea este asociativă şi distributivă faţă de adunare*, adică

$\forall x, y, z \in R, (xy)z = x(yz)$ (*asociativitatea înmulţirii*);

$\forall x, y, z \in R, x(y + z) = xy + xz$ (*distributivitatea la stînga a înmulţirii faţă de adunare*);

$\forall x, y, z \in R, (y + z)x = yx + zx$ (*distributivitatea la dreapta a înmulţirii faţă de adunare*).

Toate inelele R pe care le considerăm sînt *inele unitare*: există $1 \in R$ astfel încît $x1 = 1x = x, \forall x \in R$. Dacă înmulţirea este comutativă, ($\forall x, y \in R, xy = yx$) R se numeşte *inel comutativ*.

Un *corp* F este un inel unitar (cu $1 \neq 0$) în care orice element nenul are un invers faţă de înmulţire: $\forall x \in F\backslash\{0\} := F^*, \exists x^{-1} \in F^*$ astfel încît $xx^{-1} = x^{-1}x = 1$. Orice corp are măcar două elemente: 0 şi 1. Un corp în care înmulţirea este comutativă se numeşte *corp comutativ* (numit uneori *cîmp*).

În acest curs, „corp” înseamnă „corp comutativ”.

O submulţime E a unui corp F este numită *subcorp al lui* F dacă este parte stabilă la înmulţire, adunare şi la inversarea elementelor nenule. Astfel, E este corp cu operaţiile induse. Se demonstrează uşor că *E este subcorp în F dacă şi numai dacă* $\forall x, y \in E$, *cu* $y \neq 0$, *avem* $x - y \in E$ *şi* $xy^{-1} \in E$.

Mulţimea numerelor întregi $\mathbb{Z}$ este un inel comutativ, dar nu este corp (2 nu e inversabil în $\mathbb{Z}$). Mulţimea numerelor raţionale $\mathbb{Q}$ este corp şi este subcorp al lui $\mathbb{R}$. Aceste corpuri sînt infinite. Sîntem interesaţi de corpuri *finite*.

O funcţie $\varphi : E \to F$, unde E şi F sînt inele, se numeşte *morfism de inele* dacă păstrează operaţiile: $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$, $\forall x, y \in E$ şi $\varphi(1) = 1$. Dacă E şi F sînt corpuri, spunem că φ este *morfism de corpuri. Orice morfism de corpuri e injectiv* (demonstraţi!).

Construcţia corpurilor finite se bazează pe construcţia importantă a *inelului factor*, care reia în context mai general construcţia inelului $\mathbb{Z}_n$ al întregilor modulo n. Schiţăm ideile acestor construcţii.

Fie n un număr întreg fixat (numit *modul*). Spunem că numerele întregi a şi b sînt *congruente modulo n* dacă n divide $a - b$. Scriem aceasta sub forma $a \equiv b \pmod{n}$. Se demonstrează imediat că relaţia „$\equiv \pmod{n}$" de congruenţă modulo n este o relaţie de echivalenţă pe $\mathbb{Z}$. Pentru orice $a \in \mathbb{Z}$, se notează cu $\widehat{a}$ clasa lui a în raport cu relaţia de congruenţă modulo n. Avem deci $\widehat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$. Mulţimea factor $\mathbb{Z}/\equiv \pmod{n}$ (adică $\{\widehat{a} \mid a \in \mathbb{Z}\}$) se notează cu $\mathbb{Z}_n$ şi se numeşte *mulţimea claselor de resturi modulo n*.

Denumirea de clase de resturi este motivată de faptul că că două numere întregi a şi b sînt congruente modulo n dacă şi numai dacă dau acelaşi rest la împărţirea cu n.

Pe $\mathbb{Z}_n$ se pot defini două operaţii (numite *adunarea*, respectiv *înmulţirea modulo n*), în raport cu care $\mathbb{Z}_n$ devine *inel comutativ şi unitar*. Pentru orice $\hat{a}$, $\hat{b} \in \mathbb{Z}_n$ (cu $a, b \in \mathbb{Z}$), definim:

$$\hat{a} + \hat{b} := \widehat{a + b};\ \hat{a} \cdot \hat{b} := \widehat{a \cdot b}$$

Demonstrarea corectitudinii definiţiilor de mai sus (adică independenţa de alegerea reprezentanţilor) şi verificarea axiomelor de inel este propusă cititorului.

Vom aplica ideea construcţiei de mai sus într-o situaţie mai generală. În acest scop, observăm că putem defini relaţia de congruenţă modulo n pe $\mathbb{Z}$ şi în felul următor: Notăm $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$. Avem atunci, $\forall a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z}.$$

Se vede imediat că $\hat{a} = \{a + nk \mid k \in \mathbb{Z}\}$, motiv pentru care $\hat{a}$ se mai notează cu $a + n\mathbb{Z}$. Deci, $\hat{0} = n\mathbb{Z}$, $\hat{1} = 1 + n\mathbb{Z}$ etc.

Mulţimea $n\mathbb{Z}$ este *ideal în* $\mathbb{Z}$, în sensul că este parte stabilă la adunare şi, $\forall x \in \mathbb{Z}$, $\forall a \in n\mathbb{Z}$, rezultă că $xa \in n\mathbb{Z}$ ($n\mathbb{Z}$ este parte stabilă la înmulţirea cu *orice* element din $\mathbb{Z}$).

Mai general, dacă R este *inel* (presupus pentru simplitate *comutativ şi unitar*), o submulţime nevidă I a sa se numeşte *ideal* în R (fapt notat $I \leq R$) dacă satisface condiţiile:

- $\forall a, b \in I$, rezultă $a + b \in I$;
- $\forall a \in I$, $\forall r \in R$, rezultă $ra \in I$.

Se observă imediat că orice ideal I al lui R este subgrup al grupului aditiv $(R, +)$ (demonstraţi!) şi deci $0 \in I$. Idealul I se numeşte *propriu* dacă $I \neq R$.

Propoziţia următoare arată că ideea de construcţie a lui $\mathbb{Z}_n$ pornind de la $\mathbb{Z}$ şi un ideal al său (de forma $n\mathbb{Z}$) se generalizează

cuvînt cu cuvînt la cazul unui inel R şi al unui ideal I al său. Demonstraţia constă în verificarea directă a proprietăţilor enunţate şi o lăsăm cititorului (şi poate fi găsită în orice carte introductivă de algebră „modernă").

1 Propoziţie. *Fie R un inel comutativ unitar şi I un ideal al său.*

a) Relaţia (de congruenţă modulo I), definită prin:

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I$$

este o relaţie de echivalenţă pe I. Notînd cu $\widehat{a} = \{b \in R \mid a \equiv b \pmod{I}\}$ (numită clasa lui a modulo I), are loc $\widehat{a} = \{a + x \mid x \in I\}$ ($\widehat{a}$ se mai notează $a + I$ din acest motiv).

b) Operaţiile pe mulţimea factor $R/I := \{\widehat{a} \mid a \in R\}$, date de:

$$\widehat{a} + \widehat{b} := \widehat{a + b} \text{ şi } \widehat{a} \cdot \widehat{b} \equiv \widehat{a \cdot b},\ \forall a, b \in R,$$

sînt corect definite şi înzestrează pe R/I cu o structură de inel comutativ unitar (numit inelul factor al lui R în raport cu I).

c) Aplicaţia $\pi : R \to R/I$, $\pi(r) = \widehat{r} = r + I$, $\forall r \in R$, este un morfism surjectiv de inele (numit surjecţia canonică a inelului factor R/I). □

În termeni mai puţin riguroşi, trecerea de la inelul R la inelul factor R/I „duce toate elementele din I în zero" sau „anulează elementele lui I". Cu notaţiile de mai sus, inelul factor $\mathbb{Z}/n\mathbb{Z}$ este exact $\mathbb{Z}_n$. Multe afirmaţii referitoare la idealul I în R se traduc prin afirmaţii referitoare la idealul 0 în R/I, idee aplicată adesea în raţionamente.

2 Teoremă. *(teorema fundamentală de izomorfism pentru inele) Fie R, S inele comutative şi $\varphi : R \to S$ un morfism de inele. Atunci*

nucleul lui φ, $\mathrm{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$ *este un ideal al lui* R *şi există un izomorfism canonic*

$$\frac{R}{\mathrm{Ker}\varphi} \cong \mathrm{Im}\,\varphi$$

$$r + \mathrm{Ker}\varphi \mapsto \varphi(r),\ \forall r \in R. \qquad \square$$

Propoziţia următoare dă cele mai simple exemple de corpuri finite, care sînt blocurile de bază pentru orice corp finit.

3 Teoremă. *Fie* $n \in \mathbb{N}^*$. *Atunci inelul* $\mathbb{Z}_n$ *este corp dacă şi numai dacă* n *este prim.*

Demonstraţie. Presupunem că n e prim. E suficient să arătăm că orice element nenul din $\mathbb{Z}_n$ este inversabil. Fie $a \in \mathbb{Z}$ astfel încît $\widehat{a} \neq \widehat{0}$ în $\mathbb{Z}_n$. Aceasta înseamnă că $(a, n) = 1$. Un rezultat cunoscut afirmă că în acest caz există $u,\ v \in \mathbb{Z}$ astfel încît $ua + vn = (a, n) = 1$. Trecînd la clase modulo n, obţinem $\widehat{u}\,\widehat{a} = \widehat{1}$, căci $\widehat{n} = \widehat{0}$. Reciproc, presupunem că $\mathbb{Z}_n$ este corp şi totuşi n nu este prim. Atunci $n = ab$, cu $1 < a,\ b < n$, deci avem $\widehat{a}\widehat{b} = \widehat{n} = \widehat{0}$ în corpul $\mathbb{Z}_n$, imposibil, căci $\widehat{a}$ şi $\widehat{b}$ sînt nenule. Contradicţia arată că n trebuie să fie prim. $\square$

4 Definiţie. Fie $K,\ L$ corpuri. Dacă $\sigma : K \to L$ este un morfism de corpuri (cu necesitate injectiv), atunci tripletul $(K,\ L,\ \sigma)$ se numeşte o *extindere a lui* K. În acest caz, pentru orice element $a \in K$, obişnuim să identificăm $\sigma(a) \in L$ cu $a \in K$. Astfel, dacă $a \in K$ şi $x \in L$, vom scrie $a \cdot x$ în loc de $\sigma(a) \cdot x$ etc. Prin această identificare, K este *subcorp* al lui L şi scriem, prin abuz, „extinderea $K \subseteq L$" în loc de „extinderea $(K,\ L,\ \sigma)$". În general, la o extindere $K \subseteq L$ putem privi K drept subcorp în L.

Rezultatul următor conţine o construcţie de corpuri extrem de importantă. *Toate corpurile finite sînt construite în acest mod.*

5 Propoziţie. *Fie K un corp şi $f \in K[X]$ un polinom ireductibil de grad cel puţin 2 (deci f nu are rădăcini în K). Fie $(f) = \{gf \mid g \in K[X]\}$ idealul generat de f.*

a) Inelul factor $L := K[X]/(f)$ este un corp[8] (extindere a lui K) şi f are o rădăcină în L, anume $X + (f)$, clasa lui X mod f.

b) Există o extindere E a lui K astfel încît f are toate rădăcinile în E (f se descompune în factori liniari în $E[X]$).

Demonstraţie. a) Fie $\widehat{g} \neq \widehat{0}$ un element nenul în L, unde $g \in K[X]$. Aceasta înseamnă că f nu divide g; cum f este ireductibil, avem $(f, g) = 1$. Atunci există $u, v \in K[X]$ astfel încît $1 = uf + vg$. Trecînd la clase modulo f, $\widehat{1} = \widehat{uf + vg} = \widehat{vg}$. Deci $\widehat{g}$ are un invers, anume $\widehat{v} \in L$.

Rădăcina lui f în L este $\widehat{X}$. Într-adevăr, fie $f = a_0 + a_1X + \ldots + a_nX^n$; atunci:

$$f(\widehat{X}) = a_0\widehat{1} + a_1\widehat{X} + \ldots + a_n\widehat{X}^n = \widehat{f(X)} = \widehat{0}.$$

b) Se foloseşte o inducţie după grad f.

Observaţi că se consideră K drept subcorp în $K[X]/(f)$ via aplicaţia canonică $\varphi : K \to K[X]/(f)$, $\varphi(a) = \widehat{a}$ (clasa lui a modulo (f)), $\forall a \in K$, care este un morfism de corpuri.

Avem nevoie de unele definiţii şi rezultate fundamentale din teoria extinderilor de corpuri.

---

[8] Rezultatul şi demonstraţia sînt asemănătoare cu faptul că $\mathbb{Z}_n$ este corp dacă şi numai dacă n este prim. Aceasta nu e întîmplător: $\mathbb{Z}$ şi $K[X]$ sînt „inele principale” .

6 Definiţie. Fie $K \subseteq L$ o extindere şi $x \in L$. Spunem că x este *algebric peste* K dacă există un polinom nenul $f \in K[X]$ astfel încît $f(x) = 0$. Altfel spus, x este algebric peste K dacă şi numai dacă *morfismul de evaluare* $ev_x : K[X] \to L$, $ev_x(f) = f(x)$ $\forall f \in K[X]$, *nu este injectiv.* De exemplu, în extinderea $\mathbb{Q} \subseteq \mathbb{R}$, elementul $\sqrt{2}$ este algebric peste $\mathbb{Q}$, căci este rădăcină a lui $X^2 - 2 \in \mathbb{Q}[X]$.

7 Teoremă. *Fie $K \subseteq L$ o extindere de corpuri şi $x \in L$, algebric peste K. Fie f un polinom cu coeficienţi în K. Următoarele afirmaţii sînt echivalente:*

a) $f(x) = 0$ *şi* $\operatorname{grad} f = \min\{\operatorname{grad} g \mid g \in K[X], g(x) = 0, g \neq 0\}$.

b) $f(x) = 0$ *şi f este ireductibil*.

c) $f(x) = 0$ *şi, oricare ar fi* $g \in K[X]$ *cu* $g(x) = 0$, *rezultă că* $f \mid g$.

Demonstraţie. *a)*$\Rightarrow$*b)* Dacă f ar fi reductibil, atunci $f = gh$, cu g, $h \in K[X]$, $1 \leq \operatorname{grad} h$, $\operatorname{grad} g < \operatorname{grad} f$. Cum $g(x)h(x) = f(x) = 0$, x este o rădăcină a lui g sau h, ale căror grade sînt mai mici decît $\operatorname{grad} f$, contradicţie cu definiţia lui f.

b)$\Rightarrow$*c)* Fie $0 \neq g \in K[X]$ astfel încît $g(x) = 0$. Cum $f(x) = 0$, rezultă că $d(x) = 0$, unde $d = \operatorname{GCD}(f, g)$, deci $\operatorname{grad} d > 0$. Însă $d \mid f$ şi f este ireductibil, deci $d = f$, i.e. $f \mid g$.

c)$\Rightarrow$*a)* Fie $g \in K[X]$ cu $g(x) = 0$, $g \neq 0$. Din ipoteză, $f \mid g$, deci $\operatorname{grad} f \leq \operatorname{grad} g$.

8 Definiţie. Fie $K \subseteq L$ o extindere de corpuri şi fie $x \in L$ algebric peste K. *Polinomul minimal al lui x peste K* (notat $\operatorname{Irr}(x, K)$)

este polinomul *monic*[9] din $K[X]$ care satisface una din condiţiile echivalente de mai sus. De exemplu, $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ deoarece $X^2 - 2 \in \mathbb{Q}[X]$ este monic, ireductibil în $\mathbb{Q}[X]$ şi are rădăcină pe $\sqrt{2}$.

9 Definiţie. Fie $K \subseteq L$ o extindere de corpuri. Atunci L are o structură canonică de K-spaţiu vectorial: înmulţirea unui „scalar" din K cu un „vector" din L este înmulţirea din L. Dimensiunea lui L văzut ca spaţiu vectorial peste K se numeşte *gradul extinderii* $K \subseteq L$ şi se notează $[L : K]$. O extindere se numeşte *extindere finită* dacă gradul său este finit.

De exemplu, în extinderea $\mathbb{R} \subseteq \mathbb{C}$, elementul $i \in \mathbb{C}$ este algebric peste $\mathbb{R}$, deoarece este rădăcina polinomului $X^2 + 1 \in \mathbb{R}[X]$. Gradul extinderii este $[\mathbb{C} : \mathbb{R}] = 2$, deoarece $\{1, i\}$ este o bază a $\mathbb{R}$-spaţiului liniar $\mathbb{C}$.

Fie extinderea $K \subseteq L$ şi $x \in L$. Sînt de primă importanţă următoarele noţiuni:

- *subinelul* lui L generat[10] de K şi $\{x\}$, notat $K[x]$. Are loc (demonstraţi):

$$K[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N}, a_i \in K, 0 \le i \le n\} = \mathrm{Im}\, ev_x,$$

unde $ev_x : K \to L$ este morfismul de evaluare în x.

- *subcorpul* lui L generat de K şi $\{x\}$, notat $K(x)$. Are loc:

---

[9] Un polinom se numeşte monic (sau unitar) dacă are coeficientul termenului de grad maxim egal cu 1.

[10] Subinelul lui L generat de o submulţime S a lui L este definit ca intersecţia tuturor subinelelor lui L care includ S. Este „cel mai mic" subinel al lui L care include pe S. La fel se defineşte subcorpul generat de S.

$$K(x) = \{\alpha\beta^{-1} \mid \alpha, \beta \in K[x], \beta \neq 0\}.$$

De exemplu, subcorpul lui $\mathbb{C}$ generat de $\mathbb{Q}$ şi $\sqrt{2}$ este $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (demonstraţi!). Se observă că nu este nevoie să luăm *toate* expresiile polinomiale (de orice grad) în $\sqrt{2}$, cu coeficienţi în $\mathbb{Q}$, ca în caracterizarea precedentă, ci doar cele de grad mai mic decît 2 (adică gradul lui Irr($\sqrt{2}$, $\mathbb{Q}$)). De asemenea, are loc şi $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. Lucrul acesta nu este întîmplător şi este caracteristic elementelor *algebrice*:

10 Teoremă (caracterizarea elementelor algebrice). *Fie $K \subseteq L$ o extindere de corpuri şi $x \in L$. Următoarele afirmaţii sînt echivalente:*

a) x este algebric peste K.

b) $K[x]$ este corp.

c) $K[x] = K(x)$.

d) Extinderea $K \subseteq K(x)$ este finită.

Dacă x este algebric peste K şi $f = Irr(x, K)$, grad $f = n$, atunci

$$K[X]/(f) \cong K(x).$$

În particular, $[K(x) : K] = n$ şi o bază a K-spaţiului liniar $K(x)$ este $\{1, x, \ldots, x^{n-1}\}$.

Demonstraţie. *a)⇒b)* Fie $f = \text{Irr}(x,K) \in K[X]$ şi $ev_x : K[X] \to L$ morfismul de evaluare în x. Avem Ker $ev_x = f$. Din teorema de izomorfism pentru inele, $K[X]/(f) \cong \text{Im } ev_x = K[x]$. Cum f este ireductibil în $K[X]$, $K[X]/(f)$ este corp. Atunci $K[x]$, izomorf cu $K[X]/(f)$, este şi el corp.

b)⇔c) Evident.

c)⇒a) Presupunem că $x \neq 0$ şi fie $x^{-1} = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ inversul lui x. Înmulţind cu x, obţinem $a_0x + a_1x^2 + \ldots + a_nx^{n+1} - 1 = 0$, adică x este rădăcina unui polinom nenul cu coeficienţi în K.

d)⇒a) Familia infinită $\{x^i \mid i \in \mathbb{N}\}$ de elemente ale K-spaţiului vectorial finit dimensional $K(x)$ este liniar dependentă. Deci, există o relaţie de dependenţă liniară de forma $a_0 \cdot 1 + a_1x + \ldots + a_nx^n = 0$, cu $n \in \mathbb{N}$ şi $a_0, a_1, \ldots, a_n \in K$, nu toţi nuli, adică x este algebric peste K.

a)⇒d) Avem K-izomorfismul de corpuri $K[X]/(f) \cong K(x)$. Acesta este şi un izomorfism de K-spaţii vectoriale. Fie $n = \operatorname{grad} f$. Demonstrăm că în K-spaţiul vectorial $K[X]/(f)$, clasele elementelor $1, X, \ldots, X^{n-1}$ sînt elementele unei baze. Dacă $= a_0\widehat{1} + a_1\widehat{X} + \ldots + a_n\widehat{X}^n = \widehat{0}$, cu $a_0, a_1, \ldots, a_{n-1} \in K$, atunci $g = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in (f)$, adică $f \mid g$. Cum $\operatorname{grad} f = n$, rezultă că $g = 0$, adică $a_0, a_1, \ldots, a_{n-1}$ sînt nule. Pe de altă parte, folosind teorema împărţirii cu rest, orice clasă modulo f a unui polinom $h \in K[X]$ are un reprezentant de grad mai mic decît n. Aceasta înseamnă că $\widehat{h}$ este combinaţie liniară cu coeficienţi în K de $\widehat{1}, \widehat{X}, \ldots, \widehat{X}^{n-1}$.

Izomorfismul $K[X]/(f) \cong K(x)$ duce $X + (f)$ în x, deci baza $\{\widehat{1}, \widehat{X}, \ldots, \widehat{X}^{n-1}\}$ este dusă în baza $\{1, x, \ldots, x^{n-1}\}$ în $K[x]$. □

11 Definiţie. Fie K un corp şi x un element algebric peste K. Gradul extinderii $K \subseteq K[x]$ (egal cu $\operatorname{grad} \operatorname{Irr}(x, K)$) se numeşte *gradul elementului x peste K*.

Caracteristica $\operatorname{char} R$ a unui inel $(R, +, \cdot)$ cu unitate e este definită ca fiind 0 (dacă $ne \neq 0$, $\forall n \in \mathbb{N}^*$) sau cel mai mic număr natural $n \neq 0$ astfel încît $ne = 0$ în R. Deci, $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = 0$;

char $\mathbb{Z}_n = n$. *Caracteristica unui corp F este* 0 *sau un număr* <u>*prim*</u> *p. (demonstraţi!).*

12 Lemă. *(endomorfismul Frobenius) Fie R un inel comutativ de caracteristică* $p > 0$, cu *p prim. Atunci aplicaţia* $\varphi : R \to R$, $\varphi(x) = x^p$, $\forall x \in R$, *este un morfism de corpuri* (numit endomorfismul lui Frobenius[11] *al lui R*). *Dacă R este finit, atunci* φ *este bijectiv* (*este un* automorfism *al lui R*). *Notînd* $q = p^n$, *atunci* $\varphi^n = \varphi \circ \ldots \circ \varphi$ (*de n ori*) *este morfism, iar* $\varphi^n(x) = x^q$, $\forall x \in R$.

Demonstraţie. Fie $x, y \in R$. Este clar că $\varphi(xy) = \varphi(x)\varphi(y)$. Corpul *R* fiind comutativ, are loc formula binomului lui Newton:

$$\varphi(x+y) = (x+y)^p = \sum_{0 \le i \le p} C_p^i x^{p-i} y^i = x^p + y^p,$$

ultima egalitate avînd loc pentru că *p* divide coeficienţii binomiali C_p^i dacă $1 \le i < p$ (de ce?).

Morfismul de corpuri $\varphi : R \to R$ este injectiv, deci bijectiv dacă *R* este finit.

Avem $(\varphi \circ \varphi)(x) = \varphi(x^p) = (\varphi(x))^p = x^{p^2}$ şi, prin inducţie, $\varphi^n(x) = x^{p^n}$, $\forall x \in R$, $\forall n \in \mathbb{N}$. □

Endomorfismul Frobenius este aplicaţia identitate în cazul corpului $\mathbb{Z}_p$ (mica teoremă a lui Fermat afirmă că $x^p = x$, $\forall x \in \mathbb{Z}_p$).

Avem nevoie de un criteriu pentru a decide dacă un polinom are rădăcini multiple, folosind noţiunea de *derivată formală* a unui polinom.

---

[11] Ferdinand Georg Frobenius (1849-1917), matematician german.

13 Definiţie. Fie R un inel comutativ unitar şi $f = a_0 + a_1X + \ldots + a_nX^n \in R[X]$. Spunem că $\alpha \in R$ este *rădăcină multiplă de ordin* m a lui $f \in F[X]$ dacă $(X-\alpha)^m \mid f$ şi $(X-\alpha)^{m+1} \nmid f$.

Numim *derivată (formală)* a polinomului f polinomul

$$\mathrm{d}f := a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

Se mai foloseşte notaţia $\mathrm{d}f = f'$ sau $\mathrm{d}f = f^{(1)}$.

Un calcul direct arată că derivata formală are proprietăţile uzuale ale derivatei cunoscute din Analiză:

$$(f+g)' = f' + g', \quad (af)' = af', \quad (fg)' = f'g + fg', \quad \forall a \in R, \forall f, g \in R[X].$$

Compunerea morfismului d cu el însuşi de n ori ($n \in \mathbb{N}^*$) se notează d^n; $\mathrm{d}^n : R[X] \to R[X]$. Avem deci $\mathrm{d}^n = \mathrm{d} \circ \mathrm{d}^{n-1}$, $\forall n \in \mathbb{N}^*$, cu convenţia că $\mathrm{d}^0 = \mathrm{id}$. Mai notăm $\mathrm{d}^n f = f^{(n)}$, $\forall f \in R[X]$.

14 Propoziţie. *Fie F un corp, $f \in F[X]$ un polinom de grad $n > 0$ şi $\alpha \in F$.*

a) Există şi sînt unice elementele $b_0, \ldots, b_n \in F$ astfel încît $f = \sum_{0 \le i \le n} b_i (X-\alpha)^i$.

b) Dacă α este rădăcină multiplă de ordin m ($m \in \mathbb{N}^*$) a polinomului f, atunci $f^{(i)}(\alpha) = 0$, pentru orice $i \in \{0, \ldots, m-1\}$.

c) Dacă $f(\alpha) = f$ şi $f'(\alpha) = 0$, atunci α este rădăcină multiplă a lui f (de multiplicitate cel puţin 2).

Demonstraţie. a) Prin inducţie după grad f. Dacă $f = a_0 + a_1X$, atunci $f = a_0 + a_1\alpha + a_1(X-\alpha)$. Dacă $\operatorname{grad} f = n > 1$, aplicînd teorema împărţirii cu rest, obţinem $f = (X-\alpha)g + b_0$, cu $b_0 \in F$ şi $g \in F[X]$, $\operatorname{grad} g = n-1$. Scriind pe g sub forma dată de ipoteza de inducţie şi înlocuind în relaţia precedentă, se obţine rezultatul.

Unicitatea scrierii este echivalentă cu F-liniara independenţă a mulţimii de polinoame $\{(X-\alpha)^i \mid i \in \mathbb{N}\}$ în $F[X]$, uşor de demonstrat.

b) Din relaţia dedusă la punctul a), rezultă că $(X-\alpha)^m \mid f$ dacă şi numai dacă $b_0,\ b_1,\ldots,\ b_{m-1}$ sînt nuli. Pe de altă parte, se demonstrează uşor că $f^{(i)}(\alpha) = i!b_i,\ \forall i \in \{0,\ \ldots,\ n\}$. De aici rezultă că $f^{(i)}(\alpha) = 0,\ \forall i \in \{0,\ \ldots,\ m-1\}$.

c) Din cele demonstrate pînă acum, obţinem că $f(\alpha) = b_0 = 0$ şi $f,(\alpha) = b_1 = 0$. Deci $(X-\alpha)^2 \mid f$. □

În cazul polinoamelor cu coeficienţi într-un corp K, un element α dintr-o extindere E a lui K este rădăcină multiplă a polinomului f dacă şi numai dacă este simultan rădăcină a polinomului şi a derivatei sale, adică $(X-\alpha) \mid f$ şi $(X-\alpha) \mid f'$. Aceasta implică faptul că cmmdc al lui f şi f' în $E[X]$ este de grad ≥ 1. *Însă cmmdc a două polinoame se obţine cu algoritmul lui Euclid şi nu depinde de corpul considerat*: *dacă $K \subseteq L$ este o extindere de corpuri, iar $f,\ g \in K[X]$, atunci $(f,\ g)_{K[X]} = (f,\ g)_{L[X]}$*. În concluzie:

15 Propoziţie. *Fie K un corp şi $f \in K[X]$. Atunci f are rădăcini multiple dacă şi numai dacă f şi f' nu sînt prime între ele.* □

Astfel, se poate decide dacă un polinom are rădăcini multiple *fără a cunoaşte rădăcinile*.

Putem acum enunţa şi demonstra teorema de existenţă şi unicitate pentru corpurile finite.

16 Teoremă. *a) Fie F un corp finit cu q elemente. Atunci există un număr prim p şi $n \in \mathbb{N}^*$ astfel încît $|F| = p^n$.*

b) Pentru orice număr prim p şi $n \in \mathbb{N}^*$*, există un corp finit cu* p^n *elemente.*

Demonstraţie. a) Fie e elementul unitate al lui F. Atunci mulţimea multiplilor lui e, $P := \{n \cdot e \mid n \in \mathbb{N}^*\}$, este o submulţime a lui F şi este finită. Deci există $p \in \mathbb{N}^*$ astfel încît $p \cdot e = 0$. Alegem p să fie minim cu această proprietate ($p = \operatorname{char} F$). Dacă p nu ar fi prim, atunci $p = ab$, cu $1 < a, b < p$. Cum

$$p \cdot e = (ab) \cdot e = (a \cdot e) \cdot (b \cdot e) = 0,$$

rezultă că $a \cdot e = 0$ sau $b \cdot e = 0$, contradicţie cu minimalitatea lui p.

Rămîne că există un unic p prim astfel încît $p \cdot e = 0$. Deci $P = \{0, e, 2e, \ldots, (p-1)e\}$. Observăm că există o bijecţie între P şi $\mathbb{Z}_p = \{\hat{0}, \hat{1}, \ldots, \widehat{p-1}\}$ (inelul claselor de resturi modulo p), dată de $i \cdot e \mapsto \hat{i}$. Este chiar un izomorfism, după cum se verifică imediat. Deci P este corp (fiind izomorf cu corpul $\mathbb{Z}_p$), iar F este o extindere a sa.

Interpretăm F ca un spaţiu liniar peste P. Atunci dimensiunea lui F peste P este finită, fie $\dim_P F = n$. Deci $F \cong P^n$ (izomorfism de spaţii liniare), adică $|F| = p^n$.

b) Presupunem problema rezolvată: dacă F este corp finit cu $q := p^n$ elemente, grupul $(F^*, \cdot)$ are $q - 1$ elemente. Aplicînd teorema lui Lagrange privind ordinul unui element într-un grup finit, obţinem că $x^{q-1} = 1$, deci $x^q = x$, $\forall x \in F$. Pe de altă parte, din punctul *a)*, F conţine un subcorp izomorf cu $\mathbb{Z}_p$. Deci F este o extindere a lui $\mathbb{Z}_p$, iar $X^q - X \in \mathbb{Z}_p[X]$ se descompune în factori liniari în $F[X]$ (toate elementele din F sînt rădăcini ale lui $X^q - X$).

Argumentăm acum astfel existenţa unui corp cu $q = p^n$ elemente: fie corpul $\mathbb{Z}_p$ şi $f = X^q - X \in \mathbb{Z}_p[X]$. Există o extindere E a lui $\mathbb{Z}_p$ încît f se descompune în factori liniari în $E[X]$. Considerăm

mulţimea $F := \{x \in E \mid x^q = x\}$. Să demonstrăm că F este subcorp al lui E (va fi corpul cu q elemente căutat). Fie $x, y \in F$. Atunci $(xy)^q = x^q y^q = xy$, deci $xy \in F$. Avem şi $(x+y)^q = x^q + y^q$ ($q = p^n$, deci $x \mapsto x^q$ este o putere a endomorfismului Frobenius), deci $x + y \in F$. Dacă $x \neq 0$, atunci $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, deci $x^{-1} \in F$. Elementele lui F sînt exact rădăcinile polinomului f, iar acestea sînt în număr de exact q. Într-adevăr, un polinom de grad q are cel mult q rădăcini; pe de altă parte, f nu are rădăcini multiple, după cum se vede folosind criteriul cu derivata formală: $f' = qX^{q-1} - 1 = -1$, deci $(f, f') = 1$. □

Grupul multiplicativ al unui corp finit este *ciclic*, proprietate pe care nu o demonstrăm, dar care are multe aplicaţii:

17 Teoremă. *Fie F un corp finit cu q elemente. Atunci grupul $(F^*, \cdot)$ este ciclic: există $\alpha \in F^*$ astfel încît $F^* = \{\alpha^i \mid 1 \leq i \leq q-1\}$. Un astfel de element α se numeşte* element primitiv *al lui F.* □

18 Teoremă. *Orice două corpuri finite care au acelaşi cardinal sînt izomorfe.*

Demonstraţie. Fie F, E corpuri finite cu $q = p^n$ elemente (cu p prim) şi $\alpha \in F$ un element primitiv. Atunci $f = X^q - X \in \mathbb{Z}_p[X]$ are rădăcina α în F. Pe de altă parte, f este produs de polinoame ireductibile în $\mathbb{Z}_p[X]$; deci există un (unic) factor ireductibil g al lui f astfel încît $g(\alpha) = 0$. Atunci $\operatorname{grad} g = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = n$. Fie β o rădăcină a lui g în E (g are toate rădăcinile în E), atunci $[\mathbb{Z}_p[\beta] : \mathbb{Z}_p] = \operatorname{grad} g = n = [E : \mathbb{Z}_p]$, deci $\mathbb{Z}_p[\beta] = E$. Avem acum izomorfismele: $F = \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[X]/(g) \cong \mathbb{Z}_p[\beta] = E$. □

Corpul finit cu p^n elemente (unic pînă la izomorfism) se notează cu GF(p^n) (Galois Field = corp Galois)[12] sau $\mathbb{F}_{p^n}$.

Din existenţa unui corp finit F cu p^n elemente rezultă că *există polinoame ireductibile de grad n cu coeficienţi în* $\mathbb{Z}_p$: de exemplu, polinomul minimal peste $\mathbb{Z}_p$ al unui element primitiv al lui F. Construcţia concretă a corpului cu p^n elemente este dată de:

19 Propoziţie. *Pentru orice* $n \in \mathbb{N}^*$*, există măcar un polinom ireductibil de grad n în* $\mathbb{F}_p[X]$*; pentru orice astfel de polinom f,* $\mathbb{F}_p[X]/(f)$ *este un corp cu* p^n *elemente.* □

Problema construcţiei efective a unui corp cu p^n *elemente se reduce la căutarea unui polinom ireductibil g de grad n în* $\mathbb{Z}_p[X]$*. Corpul căutat va fi inelul factor* $\mathbb{Z}_p[X]/(g)$.

20 Exemplu: Corpul cu 4 elemente. Fie $\mathbb{Z}_2 = \mathbb{F}_2 = \{0, 1\}$ corpul cu două elemente (omitem căciula pentru a nota clasele modulo 2. Deci, $1 + 1 = 0$). Căutăm un polinom ireductibil de grad 2 in $\mathbb{Z}_2[X]$. Polinomul

$$g = X^2 + X + 1$$

nu are rădăcini în $\mathbb{Z}_2$ ($g(0) = 1$, $g(1) = 1$) şi are grad 2, deci este ireductibil. Aşadar corpul cu 4 elemente este:

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(g)} = \{h + (g) \mid h \in \mathbb{F}_2[X]\},$$

[12] Structura corpurilor finite a fost determinată de Galois în 1830.

unde $h + (g)$ notează clasa lui h modulo g. Din teorema împărţirii cu rest, $\forall h \in \mathbb{F}_2[X]$ se scrie ca $h = gq + r$, unde $q,\ r \in \mathbb{F}_2[X]$ şi grad $r <$ 2 = grad g. Trecînd la clase modulo g:

$$h + (g) = gq + r + (g) = r + (g),$$

deoarece clasa lui g este 0. Un polinom oarecare de grad < 2 e de forma $r = a + bX,\ a,\ b \in \mathbb{F}_2$. Identificăm $a \in \mathbb{F}_2$ with $a + (g) \in \mathbb{F}_4$ şi notăm $X + (g)$ cu α. Obţinem că elementele lui $\mathbb{F}_4$ sînt de forma

$$a + bX + (g) = a + b\alpha, \text{ cu } a,\ b \in \mathbb{F}_2$$

Cum $X^2 + X + 1 + (g) = 0 + (g)$, rezultă că α satisface $\alpha^2 + \alpha + 1 = 0$, adică $\alpha^2 = \alpha + 1$. Rezumînd:

$\mathbb{F}_4 = \{\ a + b\alpha \mid a,\ b \in \mathbb{F}_2\} = \{0,\ 1,\ \alpha,\ 1 + \alpha\}$, unde $\alpha^2 = \alpha + 1$.

De exemplu, $\alpha(1 + \alpha) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$

$$\alpha + (1 + \alpha) = 1$$

Am folosit că $\alpha^2 = \alpha + 1$ şi $\alpha + \alpha = 0$. Un element primitiv din $\mathbb{F}_4$ este α (de ce?).

Încheiem acest capitol cu un rezultat important, care leagă distribuţia ponderilor unui cod liniar de distribuţia ponderilor dualului său.

21 Definiţie. Fie C un cod liniar de lungime n peste F. Polinomul omogen de grad n

$$A_C(X,Y) = \sum_{c \in C} X^{wt(c)} Y^{n - wt(c)}$$

se numeşte *polinomul enumerator al ponderilor* lui C (*weight enumerator polynomial*). Dacă A_i este numărul cuvintelor de pondere i din C, atunci

$$A_C(X,Y) = \sum_{i=0}^{n} A_i X^i Y^{n-i}\ .$$

Observăm că, pentru orice două polinoame omogene g, h în X, Y, avem $g(X, Y) = h(X, Y) \Leftrightarrow g(X, 1) = h(X, 1)$.

22 Teoremă (Identităţile MacWilliams). Fie C un cod liniar de tip $[n, k]$ peste corpul cu q elemente F. Atunci:

$$A_{C^\perp}(X,Y) = \frac{1}{q^k} A_C\left(Y - X, Y + (q-1)X\right)$$

Demonstraţie. Fixăm χ un caracter aditiv netrivial al lui F (vezi exerciţiul **10**). Definim, $\forall x \in F^n$, polinomul (din $\mathbb{C}[Z]$):

$$B(x) := \sum_{y \in F^n} \chi\left(\langle x, y\rangle\right) Z^{\mathrm{wt}(y)}$$

Avem: $\sum_{x \in C} B(x) = \sum_{y \in F^n} Z^{\mathrm{wt}(y)} \sum_{x \in C} \chi\left(\langle x, y\rangle\right)$.

Dacă $y \in C^\perp$, atunci $\langle x, y\rangle = 0$, deci $\sum_{x \in C} \chi\left(\langle x, y\rangle\right) = |C|$. Dacă $y \notin C^\perp$, atunci $\langle x, y\rangle$ ia fiecare valoare din F de q^{k-1} ori cînd x parcurge C (vezi exerciţiul **II.2**), deci:

$$\sum_{x \in C} \chi\left(\langle x, y\rangle\right) = q^{k-1} \sum_{\alpha \in F} \chi(\alpha) = 0$$

În concluzie,

$$\sum_{x \in C} B(x) = |C| \sum_{y \in C^\perp} Z^{\mathrm{wt}(y)} = |C| A_{C^\perp}(Z, 1). \qquad (1)$$

Pe de altă parte, putem scrie $B(x)$ sub altă formă. Fie $x = (x_1, \ldots, x_n) \in C$, $y = (y_1, \ldots, y_n) \in F^n$ şi $\alpha \in F$; definim $\mathrm{wt}(\alpha) = 0$ dacă $\alpha = 0$, respectiv $\mathrm{wt}(\alpha) = 1$ dacă $\alpha \neq 0$.

Atunci $\mathrm{wt}(y_1, \ldots, y_n) = \mathrm{wt}(y_1) + \ldots + \mathrm{wt}(y_n)$. Avem:

$$\begin{aligned} B(x) &= \sum_{(y_1,\ldots,y_n) \in F^n} \chi\left(x_1 y_1 + \ldots x_n y_n\right) Z^{\mathrm{wt}(y_1)} \ldots Z^{\mathrm{wt}(y_n)} \\ &= \sum_{(y_1,\ldots,y_n) \in F^n} \chi\left(x_1 y_1\right) Z^{\mathrm{wt}(y_1)} \ldots \chi\left(x_n y_n\right) Z^{\mathrm{wt}(y_n)} \\ &= \left(\sum_{y_1 \in F} \chi\left(x_1 y_1\right) Z^{\mathrm{wt}(y_1)}\right) \cdot \ldots \cdot \left(\sum_{y_n \in F} \chi\left(x_n y_n\right) Z^{\mathrm{wt}(y_n)}\right) \end{aligned}$$

Însă $\sum_{\alpha \in F} \chi\left(x\alpha\right) Z^{\mathrm{wt}(\alpha)} = 1 + Z \sum_{\alpha \in F^*} \chi\left(x\alpha\right)$, iar

$$\sum_{\alpha\in F^*}\chi(x\alpha)=\begin{cases}q-1, & x=0\\ -1, & x\neq 0\end{cases}$$

adică

$$\sum_{\alpha\in F}\chi(x\alpha)Z^{\mathrm{wt}(\alpha)}=\begin{cases}1+(q-1)Z, & x=0\\ 1-Z, & x\neq 0\end{cases}$$

Deci:

$$\begin{aligned}B(x)&=\left(\sum_{y_1\in F}\chi(x_1y_1)Z^{\mathrm{wt}(y_1)}\right)\cdot\ldots\cdot\left(\sum_{y_n\in F}\chi(x_ny_n)Z^{\mathrm{wt}(y_n)}\right)\\&=\left(1+(q-1)Z\right)^{n-\mathrm{wt}(x)}(1-Z)^{\mathrm{wt}(x)}\end{aligned}$$

Aşadar,

$$\begin{aligned}\sum_{x\in C}B(x)&=\sum_{x\in C}\left(1+(q-1)Z\right)^{n-\mathrm{wt}(x)}(1-Z)^{\mathrm{wt}(x)}\\&=A_C(1-Z,1+(q-1)Z)\end{aligned}$$

Comparînd cu (1), obţinem

$$A_C(1-Z,1+(q-1)Z)=|C|\,A_{C^\perp}(Z,1)$$

Făcînd substituţia $Z=X/Y$ se obţine rezultatul din enunţ. □

Exerciţii

1. (Caracteristica unui inel) Fie K un inel şi e elementul său unitate. Dacă există $k\in\mathbb{N}^*$ astfel încît $ke=0$, atunci definim $\mathrm{char}\,K=\min\{k\in\mathbb{N}^*\mid ke=0\}$. În caz contrar, punem $\mathrm{char}\,K=0$.

a) Demonstraţi că, dacă K este integru, atunci $\mathrm{char}\,K=0$ sau un număr prim.

b) Dacă K este corp de caracteristică $p > 0$, atunci K are un unic subcorp izomorf cu $\mathbb{Z}_p$.

c) Dacă K este corp de caracteristică 0, atunci K are un unic subcorp izomorf cu $\mathbb{Q}$.

2. Determinaţi toate polinoamele ireductibile de grad cel mult 5 din $\mathbb{F}_2[X]$.

3. Demonstraţi că polinomul $g = X^6 + X + 1$ este ireductibil în $\mathbb{F}_2[X]$ şi construiţi corpul $\mathbb{F}_2[X]/(g)$.

4. Dacă F este un corp cu p^n elemente, iar K este un subcorp al său, atunci există $m|n$ astfel încît $|K| = p^m$. Reciproc, pentru orice divizor m al lui n există un unic subcorp al lui F cu $p^m =: r$ elemente, anume $K = \{x \in F |\ x^r = x\}$. (Observaţie. Cu un abuz de notaţie[13], acest fapt se poate scrie: $\mathrm{GF}(q^m) = \mathrm{GF}(q^n) \Leftrightarrow m|n$.)

5. Fie f un corp finit cu q elemente şi $f \in F[X]$, ireductibil. Demonstraţi că $f \mid X^{q^n} - X$ dacă şi numai dacă grad $f \mid n$. (*Ind.* $f \mid X^{q^n} - X \Leftrightarrow$ orice rădăcină a lui f este rădăcină a lui $X^{q^n} - X$).

6. Fie F un corp finit şi $m \in \mathbb{N}^*$. Demonstraţi că există un polinom ireductibil de grad m în $F[X]$. (*Ind.* Există un corp E cu q^m elemente, care este o extindere a lui F. Consideraţi polinomul minimal al unui element primitiv al lui E.)

7. Construiţi corpuri finite cu 4, 8, 16, 25, 9 şi 27 elemente. Pentru fiecare din ele găsiţi cîte un element primitiv.

---

[13] Relaţia este corectă dacă se presupune fixată o închidere algebrică Ω a lui $\mathrm{GF}(q)$, iar toate extinderile algebrice ale lui $\mathrm{GF}(q)$ (i.e., corpurile $\mathrm{GF}(q^m)$) sînt presupuse incluse în Ω.

8. (Numărul polinoamelor ireductibile de grad m cu coeficienţi într-un corp finit) Fie $F \subseteq L$ o extindere de grad m de corpuri finite, unde F are q elemente. Pentru orice $d \in \mathbb{N}^*$, notăm $P_{q,\,d} = \{f \in F[X] \mid \operatorname{grad} f = d, f \text{ ireductibil şi unitar}\}$.

a) Demonstraţi că

$$X^{q^m} - X = \prod_{\alpha \in L} (X - \alpha) = \prod_{d|m} \prod_{f \in P_{q,d}} f\,.$$

b) Notăm cu $R_f = \{\alpha \in L \mid f(\alpha) = 0\}$, $\forall f \in F[X]$. Arătaţi că

$$\bigcup \{R_f \mid f \in P_{q,\,d},\, d|m\} = L \text{ (reuniune disjunctă).}$$

c) Demonstraţi că $q^m = \sum_{d|m} |P_{q,\,d}| \cdot d$.

d) Calculaţi $P_{2,\,m}$ şi $P_{3,\,m}$, $1 \le m \le 6$.

9. Fie F un corp cu p^n elemente, p prim. Demonstraţi că grupul aditiv $(F, +)$ este izomorf cu $(\mathbb{Z}_p)^n$.

10. Fie $(G, +)$ un grup abelian finit. Un *caracter* al lui G este o funcţie $\chi : G \to \mathbb{C}^*$ cu proprietatea că $\chi(x + y) = \chi(x)\chi(y)$, $\forall x, y \in F$ (adică un morfism de la grupul $(F, +)$ la grupul $(\mathbb{C}^*, \cdot)$). Un caracter este *trivial* dacă $\chi(x) = 1$, $\forall x \in G$.

a) Arătaţi că, dacă F este un corp finit şi $\chi : (F, +) \to (\mathbb{C}^*, \cdot)$ este caracter aditiv netrivial al lui F, atunci:

$$\sum_{x \in F} \chi(x) = 0\,.$$

(*Ind.* Fie $\alpha \in F$ cu $\chi(\alpha) \ne 1$. Avem:

$$\sum_{x \in F} \chi(x) = \sum_{x \in F} \chi(x + \alpha) = \chi(\alpha) \sum_{x \in F} \chi(x)\,,$$

deci $\big(1 - \chi(\alpha)\big) \sum_{x \in F} \chi(x) = 0$.)

b) Fie $n \in \mathbb{N}^*$. Demonstraţi că $\chi : (\mathbb{Z}_n, +) \to \mathbb{C}^*$, $\chi(\hat{k}) = e^{2ik\pi/n}$, $\forall k \in \mathbb{Z}$, este corect definit şi este un caracter netrivial. Găsiţi un caracter netrivial al unui produs de două grupuri de tip $(\mathbb{Z}_n, +)$.

c) Demonstraţi că orice corp finit F are un caracter netrivial.

11. Scrieţi polinoamele enumeratoare de ponderi pentru codul de repetiţie $[n, 1, n]$ şi pentru codul de paritate $[n, n-1, 2]$ peste corpul $\mathbb{F}_q$.

12. Fie $x = x_1 \dots x_n \in \mathbb{F}_2^{\,n}$ un cuvînt de pondere d. Cîte cuvinte de pondere i ortogonale pe x există? (*Ind.* Folosiţi identităţile MacWilliams.)

IV. Coduri liniare: codare şi decodare

Un cod este inutilizabil fără algoritmi eficienţi de codare şi decodare. Descriem cîteva principii generale de codare şi decodare pentru coduri liniare. Fixăm un corp finit F cu q elemente şi presupunem că toate spaţiile liniare sînt peste F.

Dacă un cod C tip $[n, k]$ peste F are o matrice generatoare G, liniile sale $g_1,\ldots, g_k$ formează o bază în C. Codul C poate coda cuvinte mesaj de lungime k în cuvinte cod de lungime n astfel: un mesaj de forma $m_1 \ldots m_k \in F^k$ este codat ca $m_1g_1 + \ldots + m_kg_k$. În formă matricială, $m = m_1 \ldots m_k$ este codat ca $mG \in F^n$. Desigur, forma matricei generatoare ar trebui aleasă astfel încît procedura de codare să fie cît mai economică. O astfel de formă este *forma standard*, care duce la o codare *sistematică*.

1 Definiţie. O matrice generatoare G a unui cod liniar C tip $[n, k]$ peste F este *în formă standard*[14] dacă $G = (I_k \mid A)$, unde I_k

[14] Uneori o matrice este declarată în formă standard dacă G este de forma $(A \mid I_k)$.

este matricea identitate $k \times k$ şi A este o matrice $k \times (n-k)$ peste F:

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & \dots & 0 & a_{11} & a_{12} & \dots & a_{1n-k} \\ 0 & 1 & \dots & 0 & a_{21} & a_{22} & \dots & a_{2n-k} \\ & & \ddots & & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a_{k1} & a_{k2} & \dots & a_{k,n-k} \end{array}\right]$$

Dacă G este în formă standard, ca mai sus, cuvîntul mesaj $m_1 \dots m_k$ este codat sub forma $mG = m_1 \dots m_k c_1 \dots c_{n-k}$, adică la cuvîntul mesaj $m_1 \dots m_k$ sînt ataşate *simbolurile de control* $c_1 \dots c_{n-k}$ pentru a forma cuvîntul cod. Desigur,

$$c_i = m_1 a_{1i} + \dots + m_k a_{ki},\ 1 \le i \le n-k.$$

În acest caz, $\{1, 2, \dots, k\}$ este mulţimea de coordonate care poartă simbolurile de informaţie. Orice cuvînt cod e perfect determinat de primele sale k coordonate. Aceasta înseamnă că proiecţia pe primele k coordonate

$$\pi : C \to F^k,\ \pi(x_1 \dots x_n) = (x_1 \dots x_k)$$

este o bijecţie liniară (un izomorfism). Mai general:

2 Definiţie. Fie C un cod liniar $[n, k, d]$. O mulţime $S \subseteq \{1, 2, \dots, n\}$ de coordonate se numeşte *mulţime de informaţie (information set)* dacă proiecţia pe coordonatele din S, $\pi_S : C \to F^{|S|}$, $\pi_S(x_1 \dots x_n) = (x_i)_{i \in S}$ este un izomorfism. Aşadar, *orice mulţime de informaţie are k elemente* (deoarece C şi $F^{|S|}$ sînt izomorfe, au aceeaşi dimensiune k).

Observăm că: S *este o mulţime de informaţie* $\Leftrightarrow |S| = k$ şi $\forall x \in C$, $\pi_S(x) = 0 \in F^{|S|}$ *implică* $x = 0$ (singurul cuvînt cod care e 0 pe S este cuvîntul 0).

3 Propoziţie. *Fie G o matrice generatoare a lui C, H o matrice de paritate a lui C şi $S \subseteq \{1, 2, \ldots, n\}$, $|S| = k$. Următoarele afirmaţii sînt echivalente:*

a) S este o mulţime de informaţie.

b) Coloanele lui G corespunzătoare coordonatelor din S sînt liniar independente.

c) Coloanele lui H corespunzătoare coordonatelor care nu sînt în S sînt liniar independente.

Demonstraţie. Fie $g_1, \ldots, g_k$ liniile lui G şi $H_1, \ldots, H_n$ coloanele lui H. Coloanele lui G corespunzătoare coordonatelor din S formează o matrice R tip $k \times k$.

"*a)*$\Rightarrow$*b)*" Fie $r_1, \ldots, r_k$ liniile lui R. O relaţie de dependenţă liniară $\alpha_1 r_1 + \ldots + \alpha_k r_k = 0$ corespunde unui cuvînt cod nenul $x = \alpha_1 g_1 + \ldots + \alpha_k g_k$ cu $\pi_S(x) = 0$, contradicţie. Astfel, rang $R = k$ şi coloanele lui R sînt independente.

"*b)*$\Rightarrow$*a)*" Avem rang $R = k$, deci liniile lui R sînt independente. Un cuvînt cod nenul $x = \alpha_1 g_1 + \ldots + \alpha_k g_k$ cu $\pi_S(x) = 0$ conduce la o relaţie de dependenţă liniară $\alpha_1 r_1 + \ldots + \alpha_k r_k = 0$, contradicţie.

"*a)*$\Rightarrow$*c)*" Pentru simplitate, presupunem că $S = \{1, 2, \ldots, k\}$. Dacă, prin absurd, coloanele $H_{k+1}, \ldots, H_n$ nu ar fi liniar independente, există $\alpha_{k+1}, \ldots, \alpha_n \in F$, nu toţi zero, astfel încît $\alpha_{k+1} H_{k+1} + \ldots + \alpha_n H_n = 0$. Atunci $0 \ldots 0 \alpha_{k+1} \ldots \alpha_n \in C$ (căci $x_1 \ldots x_n \in C$ dacă şi numai dacă $x_1 H_1 + \ldots + x_n H_n = 0$), contradicţie.

Restul implicaţiilor sînt propuse ca exerciţiu. □

4 Propoziţie. *Fie C un cod tip $[n, k, d]$ şi fie $S \subseteq \{1, 2, \ldots, n\}$.*

a) Dacă $|S| \geq n - d + 1$, atunci S include o mulţime de informaţie.

b) C este cod MDS $\Leftrightarrow$ *orice mulţime de k coordonate este mulţime de informaţie.*

Demonstraţie. a) Fie G o matrice generatoare a lui C şi fie G_S matricea formată din coloanele lui G care corespund coordonatelor din S. Presupunem că S nu include o mulţime de informaţie. Aceasta înseamnă că orice k coloane din G_S sînt liniar dependente, deci rang $G_S < k$. Deci liniile lui G_S sînt dependente, şi aceasta produce un cuvînt cod nenul x care este zero pe S (cf. demonstraţia precedentă). Dar atunci $\text{wt}(x) \le n - |S| \le d - 1$, contradicţie.

b) "$\Rightarrow$"Avem : C este MDS $\Leftrightarrow d = n - k + 1$. Deci, dacă S are k elemente, $k \ge n - d + 1$ şi aplicăm a).

"$\Leftarrow$" Presupunem că $d < n - k + 1$. Fie $0 \ne x \in C$ cu $\text{wt}(x) = d < n - k + 1$. Atunci $S = \{i \mid x_i = 0\}$ are $n - d > k - 1$ elemente şi S nu este mulţime de informaţie, contradicţie. □

Nu orice cod liniar are o matrice generatoare în formă standard, dar este echivalent cu un cod care are una. În ceea ce urmează schiţăm o demonstraţie a acestui fapt.

5 Definiţie. Spunem că o matrice peste F este în *formă eşalon pe linii* (REF, *row echelon form*) dacă:

- toate liniile nenule (i.e. cu cel puţin un element nenul) sînt deasupra oricărei linii formate doar din zerouri;

- primul (de la stînga) coeficient nenul (numit *pivot*) al unei linii nenule este întotdeauna strict mai la dreapta pivotului de pe linia de deasupra.

Dacă în plus fiecare pivot este 1 şi este unicul element nenul de pe coloana sa (adică elementele de deasupra lui sînt 0), spunem că

matricea este in *forma eşalon redusă pe linii* (*reduced row echelon form,* RREF).

Spre exemplu, fie matricele:

$$A = \begin{bmatrix} 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; B = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A este în REF, *B* este în RREF. Mai mult, *B* şi *A* sînt *echivalente* (*B* se obţine din *A* prin înlocuirea liniei 1 cu linia 1 + (– 2)·linia 3). Observăm că o matrice $k \times n$ *de rang k în RREF conţine coloanele matricei identitate* I_k.

Dacă $A \in \mathrm{M}(k,\ n,\ F)$ şi $1 \le i,\ j \le k\ ,\ i \ne j,\ a \in F^*$, definim *transformările elementare de tip I, II, III asupra liniilor lui A*:

Tip I: se adună la linia *i* linia *j* înmulţită cu *a*.

Tip II: se permută linia *i* cu linia *j*.

Tip III: se înmulţeşte linia *i* cu *a.*

6 Exerciţiu. Demonstraţi că *orice transformare elementară asupra liniilor lui A produce o matrice A' cu proprietatea că subspaţiul generat de liniile lui A' este egal cu subspaţiul generat de liniile lui A.*

Un rezultat cunoscut de Algebră liniară afirmă că, *pentru orice matrice* $A \in \mathrm{M}(k, n, F)$, *există un şir finit de transformări elementare asupra liniilor lui A, care transformă matricea A într-o matrice A' în RREF şi care are subspaţiul generat de linii egal cu cel generat de liniile lui A. Mai mult, matricea A' cu aceste proprietăţi este unică (şi se numeşte* forma eşalon redusă *pe linii a lui A).*

Rezultatul de mai sus ne asigură că, plecînd de la o matrice generatoare oarecare G a unui cod liniar C, obţinem (prin transformări elementare pe liniile lui A) o matrice generatoare G_1 a lui C, care este în RREF; G_1 conţine coloanele matricei identitate, dar nu neapărat pe primele k locuri, încît G_1 să fie în formă standard (vezi de exemplu matricea B de mai sus). O permutare adecvată a coloanelor furnizează o matrice G' (în formă standard). Matricea G' este matrice generatoare a unui cod C', care este echivalent pînă la o permutare cu C. Rezumînd:

7 Propoziţie. *Orice cod liniar este echivalent pînă la o permutare cu un cod care are o matrice generatoare în formă standard.* □

O matrice generatoare în formă standard furnizează imediat o matrice de paritate:

8 Propoziţie. *Fie C un cod liniar $[n, k, d]$ astfel încît $G = (I_k \mid A)$ este o matrice generatoare a lui C în formă standard. Atunci $H := (-A^{\mathrm{T}} \mid I_{n-k})$ este o matrice de paritate a lui C (adică o matrice generatoare pentru $C^{\perp}$).*

Demonstraţie. Un calcul direct arată că orice linie a lui H este ortogonală pe orice linie a lui G. Deci subspaţiul generat de liniile lui H este inclus în $C^{\perp}$. Deoarece rang $H = n - k$ (H conţine I_{n-k} ca submatrice), rezultă că subspaţiul generat de liniile lui H are dimensiune $n - k$. Cum dim $C^{\perp} = n - k$, H este matrice generatoare pentru $C^{\perp}$. □

Pentru a descrie *algoritmi de decodare* pentru coduri liniare avem nevoie de noţiunea de *coset* al unui subspaţiu liniar. Construcţia e similară cu cea de la inelul factor.

9 Definiţie. Fie U un subspaţiu al spaţiului liniar V. Relaţia pe V, definită de:

$$x \equiv y (\mathrm{mod}\ U) \Leftrightarrow x - y \in U$$

este o relaţie de echivalenţă (*relaţia de congruenţă modulo* U). Clasa de echivalenţă a elementului $v \in V$ se numeşte *cosetul* lui U determinat de v. Se vede uşor că acest coset este:

$$v + U = \{v + u \mid u \in U\}.$$

Astfel, cosetul lui U determinat de v se obţine adunînd v la fiecare vector al lui U, şi are acelaşi număr de elemente ca U. Mulţimea tuturor coseturilor lui U se numeşte *spaţiul liniar factor* V/U; acesta e spaţiu liniar dacă definim operaţiile astfel: pentru orice $v, w \in V, \lambda \in F$:

$$(v + U) + (w + U) = v + w + U$$
$$\lambda(v + U) = \lambda v + U.$$

Verificarea axiomelor este imediată. Au loc următoarele rezultate clasice de algebră liniară, uşor de demonstrat:

10 Teoremă. *Fie F un corp cu q elemente şi $U \leq_F V$. Atunci orice bază a lui U poate fi completată pînă la o bază a lui V. Dacă $\{u_1, \ldots, u_k\}$ este o bază a lui U şi $\{u_1, \ldots, u_k, u_{k+1}, \ldots, u_n\}$ este o bază a lui V, atunci $\{u_{k+1} + U, \ldots, u_n + U\}$ este o bază a lui V/U. În particular,* $\dim(V/U) = \dim(V) - \dim(U) =$ *numărul de coseturi distincte ale lui U. Aşadar, există q^{n-k} coseturi ale lui U şi fiecare coset are q^k elemente.* □

11 Teoremă. *Fie U şi V două F-spaţii liniare finit dimensionale şi fie $\varphi : U \to V$ o aplicaţie liniară. Atunci:*

a) Nucleul lui φ, $\operatorname{Ker}\ \varphi := \{u \in U \mid \varphi(u) = 0\}$ *este subspaţiu liniar al lui U.*

b) (Teorema fundamentală de izomorfism) Există un izomorfism canonic:

$$\frac{U}{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi, \quad u + \operatorname{Ker}\varphi \mapsto \varphi(u), \ \forall u \in U.$$

c) $dim(U) = dim(\operatorname{Im}\varphi) + \dim(Ker\varphi)$. □

Ne întoarcem la problema decodării. Fie w cuvîntul cod original transmis şi fie x cuvîntul recepţionat. Atunci $x = w + \varepsilon$, unde ε este *cuvîntul eroare* (ε este un cuvînt din F^n). Deci x *şi* ε *sînt în acelaşi coset al lui C, anume $x + C$.* Pentru a găsi w, e suficient să găsim ε. Algoritmul de distanţă minimă, pentru x dat, caută acel $w \in C$ care este cel mai aproape de x. Deoarece $\varepsilon = x - w$, aceasta înseamnă că ε *este cuvîntul de pondere minimă în cosetul $x + C$.*

Sîntem conduşi la definiţia următoare. Pentru orice coset D al lui V, un vector ε din D se numeşte un *lider al cosetului D* dacă ponderea sa este cea mai mică printre ponderile cuvintelor din D: $\operatorname{wt}(\varepsilon) = \min\{\operatorname{wt}(x) \mid x \in D\}$. Un coset poate avea mai mulţi lideri (de aceeaşi pondere, desigur).

Astfel, receptorul caută liderul ε al cosetului ce conţine x şi decodează x în $x - \varepsilon$. Putem enunţa următorul algoritm:

Pentru un cod dat C, se calculează (înaintea oricărei transmisii) coseturile lui C cu liderii respectivi şi se aranjează într-un tablou (numit *tablou Slepian*, sau *tablou standard*). În practică, prima linie a tabloului constă în cuvintele lui C, cu cuvîntul nul 0 pe

primul loc. Dacă $j - 1$ linii au fost deja scrise, dintre cuvintele care nu sînt deja scrise se alege un cuvînt de pondere minimă e_j; acesta e declarat lider al cosetului, şi este scris ca primul element al liniei j. Pe locul i al liniei j scriem e_j adunat cu elementul de pe locul i din prima linie. Astfel am obţinut linia j, care este cosetul $e_j + C$. Continuăm procedura pîna epuizăm toate cuvintele din F^n. Se obţine un tablou cu q^{n-k} linii (fiecare linie este coset al lui C şi are q^k elemente).

La recepţia lui x, se caută cosetul care conţine x, şi fie ε liderul acestui coset. Se decodează x în $x - \varepsilon$ (adică exact cuvîntul din prima linie care e deasupra lui x).

12 Observaţie. *Fie C un cod $[n, k, d]$, cu capacitate de corectare e. Atunci:*

a) Orice lider de coset de pondere $\le e$ este unic. Deci, dacă nu au loc mai mult de e erori (i.e. vectorul de eroare are pondere $\le e$), algoritmul de mai sus decodează corect cuvîntul receptat.

b) Dacă d este par ($d = 2e + 2$), atunci există un coset care are doi lideri distincţi de pondere $e + 1$

Demonstraţie. *a)* Presupunem că u şi v au ponderi $\le e$ şi sînt în acelaşi coset. Atunci $\mathrm{wt}(u - v) \le \mathrm{wt}(u) + \mathrm{wt}(v) \le 2e < d$ şi $u - v \in C$. Aceasta implică $u - v = 0$, căci distanţa minimă a lui C este d.

b) Lăsăm demonstraţia cititorului. Deci, există un cuvînt cod c şi un vector eroare ε de pondere $e + 1$ astfel încît $c + \varepsilon$ aparţine unui coset cu cel puţin doi lideri (adică $c + \varepsilon$ nu poate fi unic decodat). Acest fapt e normal, căci $e + 1$ erori este mai mult decît capacitatea de corectare a lui C.

Decodarea cu sindroame. Algoritmul de decodare prezentat cere stocarea în memorie a tuturor cuvintelor din F^n, ceea ce poate fi costisitor sau chiar imposibil pentru n mare. O variantă a algoritmului de mai sus foloseşte următorul concept:

13 Definiţie. Fie C un cod liniar tip $[n, k, d]$ peste F, H o matrice de paritate pentru C şi $x \in F^n$. Vectorul

$$s_H(x) = Hx^{\mathrm{T}} \in F^{n-k}$$

se numeşte *sindromul* lui x (relativ la H).

Observăm că $s_H : F^n \to F^{n-k}$, $s_H(x) = Hx^{\mathrm{T}}$, $\forall x \in F^n$, este o funcţie liniară.

Avem, $\forall x \in F^n$, $x \in C \Leftrightarrow s_H(x) = 0$. Deci, $\forall u,\ v \in F^n$: $u - v \in C \Leftrightarrow s_H(u) = s_H(v)$. Adică:

Două cuvinte sînt în acelaşi coset al lui C dacă şi numai dacă au acelaşi sindrom.

Astfel, putem enunţa următorul *algoritm* (*de decodare cu sindroame*):

Înaintea oricărei transmisii se alcătuieşte o listă care conţine sindroamele tuturor coseturilor lui C pe o coloană şi liderii coseturilor respective pe următoarea coloană.

La recepţia unui cuvînt x, se calculează $s_H(x)$. Dacă $s_H(x) = 0$, atunci $x \in C$, adică nu au avut loc erori.

Dacă $s_H(x) \neq 0$, receptorul caută liderul e care are acelaşi sindrom cu x ($s_H(e) = s_H(x)$). Apoi x este decodat în $x - e \in C$.

Exerciţii

1. Demonstraţi că un cod *binar* MDS de lungime n este unul din următoarele: codul de repetiţie tip $[n, 1, n]$, codul de paritate tip $[n, n-1, 2]$, sau tot $\mathbb{F}_2^n$, de tip $[n, n, 1]$. (*Ind:* consideraţi o matrice generatoare şi folosiţi Prop. **4**)

2. Fie C un cod liniar tip $[n, k]$ şi G o matrice generatoare. Demonstraţi că distanţa minimă d a lui C este:
$d = \max\{\delta \in \mathbb{N} \mid$ orice submatrice $k\times(n-\delta+1)$ a lui G are rang $k\}$

3. Demonstraţi că dualul unui cod liniar MDS este tot MDS. (*Ind.:* folosiţi Prop. **4**)

4. Există un cod binar tip [4, 2, 3]? (*Ind:* încercaţi să construiţi o matrice de paritate.)

5. Fie C codul liniar binar cu matrice de paritate

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

a) Găsiţi o matrice generatoare a lui C şi scrieţi toate cuvintele cod din C.

b) Scrieţi coseturile lui C şi liderii acestor coseturi.

c) Folosind decodarea cu sindroame, decodaţi: 110110; 011011; 101010.

6. a) Arătaţi că orice cuvînt cod al unui cod binar autodual are pondere pară.

b) Arătaţi că orice cuvînt cod al unui cod ternar autodual are pondere multiplu de 3.

c) Construiţi un cod autodual peste $\mathbb{F}_5$ astfel încît măcar unul din cuvintele cod nu are pondere multiplu de 5.

7. a) Demonstraţi că $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ este o matrice de paritate pentru un cod binar autodual de lungime 4.

b) Scrieţi o matrice de paritate pentru un cod binar autodual de lungime 10. Generalizare.

8. Fie $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{Z}_2^n$ şi $C \leq \mathbb{Z}_2^n$. Arătaţi că:

a) $\mathrm{wt}(x) \equiv \langle x, x \rangle \pmod 2$.

b) $\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\mathrm{wt}(x \cap y)$, unde $x \cap y \in \mathbb{Z}_2^n$ are 1 exact în locurile în care x şi y au simultan 1.

c) Fie G o matrice generatoare. Demonstraţi că dacă C este autodual şi fiecare linie a lui G are pondere multiplu de 4, atunci orice cuvînt al lui G are pondere multiplu de 4.

d) Dacă orice cuvînt al lui C are pondere multiplu de 4, atunci G este autodual. (*Ind.* $\forall x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in C$, avem (mod4): $2\sum_{i=1}^{n} x_i y_i \equiv 2\mathrm{wt}(x \cap y) \equiv \mathrm{wt}(x + y) - \mathrm{wt}(x) - \mathrm{wt}(y) \equiv 0$.)

9. Fie C cod binar autodual tip $[n, k, d]$.

a) Demonstraţi că $(1, 1, \ldots, 1) \in C$.

b) Demonstraţi că $n = 2k$.

c) Demonstraţi că: fie toate cuvintele lui C au pondere multiplu de 4, fie exact jumătate din cuvintele lui C au pondere multiplu de 4.

d) Fie $n = 6$. Demonstraţi că $d = 2$.

V. Construcţii de coduri noi din coduri existente

Descriem cîteva construcţii care produc noi coduri pornind de la coduri cunoscute. Construcţiile ce urmează arată că există coduri liniare cu parametri ce se afla în anumite relaţii cu cei ai unui cod dat C. Adesea aceste coduri sînt mai „rele" decît C, dar au interes teoretic. Detaliile de demonstraţie care lipsesc sînt lăsate cititorului.

Fixăm un corp finit F şi un cod liniar C de tip $[n, k, d]$ peste F.

I. Lungire (Lengthening). Fie

$$C' = \{(x_1, \ldots, x_n, 0) \mid (x_1, \ldots, x_n) \in C\}.$$

Atunci C' este un cod liniar tip $[n + 1, k, d]$ (se spune că e obţinut prin *lungirea* lui C). Prin inducţie, se vede că:

Pentru orice $r \in \mathbb{N}$, există un cod liniar tip $[n + r, k, d]$.

II. Găurire (Puncturing). Fixăm o coordonată $i \in \{1, ..., n\}$. Ştergem coordonata i din toate cuvintele cod ale lui C, şi obţinem un cod $C' \subseteq F^{n-1}$.

Pentru simplitate, presupunem că $i = 1$. Fie $\pi : C \to C'$, $\pi(x_1 \ldots x_n) = x_2 \ldots x_n$. E clar că π este aplicaţie liniară surjectivă. Din teorema fundamentală de izomorfism (**IV.11)**, $C/\mathrm{Ker}\pi \cong C'$. Avem două cazuri:

- $\mathrm{Ker}\pi = 0$ (adică C izomorf cu C'). Atunci C' este cod tip $[n - 1, k]$. Avem $d(C') = d - 1$ dacă există un cuvînt în C de pondere minimă d care e nenul pe coordonata i. Altfel, $d(C') = d$.

- $\mathrm{Ker}\pi \neq 0$. Atunci:

$$\mathrm{Ker}\pi = \{x_1 \ldots x_n \in C \mid x_2 \ldots x_n = 0\} = \{\alpha 0 \ldots 0 \in C \mid \alpha \in F\}.$$

Deci $\mathrm{Ker}\pi \neq 0$ implică $d = 1$; dim $\mathrm{Ker}\pi = 1$, deci dim $C' = k - 1$.

Dacă $d > 1$, alegem o coordonată i astfel încît există un cuvînt în C de pondere d care e nenul pe coordonata i. Codul scurtat pe i are parametrii $[n - 1, k, d - 1]$. În concluzie:

Dacă $d > 1$, *atunci există un cod* $[n - 1, k, d - 1]$. Prin inducţie, *pentru orice* $r < d$, *există un cod* $[n - r, k, d - r]$.

Mai general, dacă $S \subseteq \{1, ..., n\}$ este o mulţime de coordonate, prin ştergerea acestor coordonate din cuvintele lui C, se obţine un cod C^S (codul C *găurit* pe S). Are parametrii $[n - |S|, k', d']$, unde $k' \geq k - |S|$, $d' \geq d - |S|$.

III. Subcod. *Există un cod tip* $[n, k - 1, d]$.

Intr-adevăr, fie $x \in C$ de pondere d; formăm o bază a lui C cu primul vector x. Codul generat de primii $k - 1$ vectori ai acestei baze are dimensiune $k - 1$ şi distanţă minimă d. Prin inducţie obţinem: *pentru orice* $r < k$, *există un cod tip* $[n, k - r, d]$.

IV. *Există un cod tip* $[n, k, d-1]$.

Pentru demonstraţie, lungim C şi formăm un cod $[n+1, k, d]$; apoi aplicăm o găurire adecvată şi obţinem un cod $[n, k, d-1]$. Prin inducţie, *pentru orice* $r < d$, *există un cod tip* $[n, k, d-r]$.

V. *Există un cod tip* $[n-1, k-1, d]$.

Dacă $k = n$, atunci $C = F^n$, deci $d = 1$. Atunci F^{n-1} este de tip $[n-1, k-1, d]$. Presupunem că $k < n$. Permutăm coordonatele lui C pentru a obţine un cod liniar care are o matrice de paritate de forma $H = (I_{n-k} \mid A)$. Ştergînd ultima coloană a lui H obţinem o matrice H'. Rangul lui H' este $n-k$, căci are primele $n-k$ coloane liniar independente. Deci H' este matrice de paritate pentru un cod C' de lungime $n-1$ şi dimensiune $n-1-(n-k) = k-1$. Cum orice $d-1$ coloane ale lui H sînt independente, acelaşi lucru se întîmplă pentru H', deci $d(C') = d' \geq d$. Dacă $d' > d$, aplicăm **IV** şi obţinem un cod tip $[n-1, k-1, d]$. Prin inducţie, *pentru orice* $r < k$, *există un cod tip* $[n-r, k-r, d]$.

VI. Extinderea unui cod.

$\overline{C} := \{(x_1, \ldots, x_n, p) \in F^{n+1} \mid (x_1, \ldots, x_n) \in C, x_1 + \ldots + x_n + p = 0\}$ se numeşte *codul extins al lui C*. Astfel, fiecărui cuvînt cod i se adaugă un „simbol de paritate p" (în cazul unui cod binar, este numit *bit de paritate*). Atunci $\overline{C}$ este un cod liniar $[n+1, k]$. Distanţa sa este d sau $d+1$ (**Exerciţiu:** discutaţi cazul binar!).

VII. Scurtare. Fie $S \subseteq \{1, ..., n\}$ o mulţime de coordonate. Fie

$$C(S) = \{x_1 \ldots x_n \in C \mid x_i = 0, \forall i \in S\}$$

Prin găurirea lui $C(S)$ pe S obţinem un cod C_S, numit codul C *scurtat pe S*. Altfel spus: luăm toate cuvintele cod din C care sînt 0

pe S, ştergem coordonatele din S şi declarăm mulţimea de cuvinte obţinută ca noul cod.

Prin scurtarea unui cod MDS se obţine tot un cod MDS (rezultat utilizat în practică):

1 Propoziţie. *Fie C un cod tip $[n, k, n-k+1]$ (cod MDS). Atunci codul C scurtat pe orice coordonată este un cod tip $[n-1, k-1, n-k+1]$ (tot un cod MDS). Prin inducţie, scurtarea lui C pe orice $r < k$ coordonate produce un cod MDS tip $[n-r, k-r, n-k+1]$.*

Demonstraţie. Presupunem că scurtăm C pe coordonata 1. Obţinem

$$C_1 = \{x_2 \ldots x_n \in F^{n-1} \mid 0x_2 \ldots x_n \in C\}.$$

C_1 este izomorf cu $\{x_1 \ldots x_n \in C \mid x_1 = 0\}$, nucleul aplicaţiei $\pi : C \to F$, $\pi(x_1 \ldots x_n) = x_1$. Afirmăm că π nu este identic 0. Într-adevăr, dacă $\pi = 0$, atunci toate cuvintele din C sînt 0 pe coordonata 1; deci C găurit pe coordonata 1 este un cod $[n-1, k, d]$, ceea ce contrazice inegalitatea Singleton.

Deci $\pi \neq 0$ şi π este surjectivă. Avem

$$\dim C = \dim \operatorname{Ker} \pi + \dim \operatorname{Im} \pi,$$

deci $k = \dim C_1 + 1$. Astfel, C_1 este un cod tip $[n-1, k-1, d(C_1)]$. Din inegalitatea Singleton $d(C_1) \leq (n-1) - (k-1) + 1 = n - k + 1$. Fie $0 \neq x_2 \ldots x_n \in C_1$, deci $0x_2 \ldots x_n \in C$. Atunci $\operatorname{wt}(x_2 \ldots x_n) = \operatorname{wt}(0x_2 \ldots x_n) \geq n - k + 1$. Aşadar $d(C_1) \geq n - k + 1$. □

VIII Suma directă. *Suma directă* a două coduri este acelaşi lucru ca suma directă (externă) a două spaţii liniare:

2. Propoziţie. *Fie* C_1 *şi* C_2 *coduri liniare tip* $[n_1, k_1, d_1]$ *(resp.* $[n_2, k_2, d_2]$*) peste F. Atunci*

$$C_1 \oplus C_2 := \{(c_1, c_2) \in F^{n_1+n_2} \mid c_1 \in C_1, c_2 \in C_2\}$$

este un cod liniar tip $[n_1 + n_2, k_1 + k_2, \min(d_1, d_2)]$ (*numit* suma directă a codurilor C_1 şi C_2). *Dacă* G_1 *şi* G_2 *sînt matrice generatoare, atunci* $\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$ *este matrice generatoare pentru* $C_1 \oplus C_2$.

Demonstraţie. Fie $\{e_1, \ldots, e_{k_1}\}$, $\{f_1, \ldots, f_{k_2}\}$ baze în C_1 (resp. C_2). Se vede uşor că $\{(e_1, 0), \ldots, (e_{k_1}, 0), (0, f_1), \ldots, (0, f_{k_2})\}$ este bază în $C_1 \oplus C_2$. Cuvintele nenule de pondere minimă sînt de forma $(c_1, 0)$ sau $(0, c_2)$, unde c_1 şi c_2 sînt nenule de pondere minimă. Deci ponderea minimă este $\min(d_1, d_2)$. □

IX Construcţia (u, u + v) ("bar product") Această construcţie poate produce coduri interesante şi practice.

3 Propoziţie. *Fie* C_1 *şi* C_2 *coduri liniare tip* $[n, k_1, d_1]$ (*resp.* $[n, k_2, d_2]$) de aceeaşi lungime *peste F. Atunci*

$$C_1 | C_2 := \{(u, u + v) \in F^{2n} \mid u \in C_1, v \in C_2\}$$

este un cod liniar tip $[2n, k_1 + k_2, \min(2d_1, d_2)]$. *Dacă* G_1 *şi* G_2 *sînt matrice generatoare, atunci* $\begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$ *este o matrice generatoare pentru* $C_1 | C_2$.

Demonstraţie. Fie $\{e_1, \ldots, e_{k_1}\}$, $\{f_1, \ldots, f_{k_2}\}$ baze în C_1 (resp. C_2). Atunci:

$$\{(e_1, e_1), \ldots, (e_{k_1}, e_{k_1}), (0, f_1), \ldots, (0, f_{k_2})\}$$

este o bază în $C_1|C_2$. Aceasta implică dim $(C_1|C_2) = k_1 + k_2$ şi afirmaţia despre matricea generatoare.

Fie $c = (u,\ u + v)$ un cuvînt nenul în $C_1|C_2$, $u \in C_1$, $v \in C_2$. Avem două cazuri:

I. $\underline{v = 0.}$ Atunci $u \neq 0$, deci $\mathrm{wt}(c) = 2\mathrm{wt}(u) \geq 2d_1 \geq \min(2d_1, d_2)$.

II. $\underline{v \neq 0.}$ Atunci

$\mathrm{wt}(u,\ u + v) = \mathrm{wt}(u) + \mathrm{wt}(u + v) \geq \mathrm{wt}(u) + \mathrm{wt}(v) - \mathrm{wt}(u) = \mathrm{wt}(v)$

$\geq d_2 \geq \min(2d_1, d_2)$

(Am folosit faptul că $\mathrm{wt}(v + u) \geq \mathrm{wt}(v) - \mathrm{wt}(u)$, $\forall v,\ u \in F^n$. Demonstraţi!)

Deci, $d(C_1|C_2) \geq \min(2d_1, d_2)$. Pentru inegalitatea opusă, observăm că, dacă $u \in C_1$ are pondere d_1, atunci $(u,\ u) \in C_1|C_2$ şi $\mathrm{wt}(u,\ u) = 2d_1$; dacă $v \in C_2$ are pondere d_2, atunci $(0,\ v) \in C_1|C_2$ şi $\mathrm{wt}(0,\ v) = d_2$. □

Fie **1** vectorul din $(\mathbb{F}_2)^n$ cu toate componentele egale cu 1. Acest vector generează codul de repetiţie de lungime n, cod binar de tip $[n,\ 1,\ n]$, pe care îl notăm tot cu **1**; acest cod are doi vectori:

$$(0, ..., 0) = \mathbf{0} \text{ şi } (1, ..., 1) = \mathbf{1}.$$

4 Corolar. *Fie C un cod binar tip $[n, k, d]$. Atunci*

$$C|\mathbf{1} := \{(u, u) \in \mathbb{F}_2^{2n} \mid u \in C\} \cup \{(u, u + \mathbf{1}) \in \mathbb{F}_2^{2n} \mid u \in C\}$$

este un cod liniar tip $[2n, k + 1, \min(2d, n)]$.

Dacă $G \in \mathrm{M}(k,\ n,\ \mathbb{F}_2)$ este o matrice generatoare a lui C, atunci $\begin{bmatrix} G & G \\ 0 & \mathbf{1} \end{bmatrix} \in \mathrm{M}(k + 1,\ 2n,\ \mathbb{F}_2)$ *este o matrice generatoare a lui $C|\mathbf{1}$.* □

Ca o aplicaţie, descriem o familie importantă de coduri care poate fi construită recursiv folosind metodele de mai sus:

5 Definiţie. Codurile *Reed-Muller binare de ordinul* 1, $R(1, m)$ ($m \geq 1$) sînt definite astfel: $R(1, 1) := \mathbb{F}_2^2$; pentru orice $m \geq 1$, $R(1, m + 1) := R(1, m)|\mathbf{1}$.

6 Propoziţie. *Pentru orice* $m \in \mathbb{N}^*$, $R(1, m)$ *este un cod binar tip* $[2^m, m + 1, 2^{m-1}]$. *Mai mult, orice cuvînt cod nenul are pondere* 2^{m-1}, *cu excepţia cuvîntului* **1** (*de pondere* 2^m).

Demonstraţie. $R(1, 1)$ este cod binar tip [2, 2, 1]. Demonstrăm afirmaţiile prin inducţie după m. Presupunem că $R(1, m)$ este cod tip $[2^m, m + 1, 2^{m-1}]$. Din Corolarul **4**, $R(1, m + 1)$ este cod tip $[2 \cdot 2^m, m + 2, \min(2^m, 2^m)]$, ca în enunţ. Fie $0 \neq c \in R(1, m + 1)$. Dacă $c = (u, u)$, cu $u \in R(1, m)$, atunci $\mathrm{wt}(u, u) = 2\mathrm{wt}(u) = 2 \cdot 2^{m-1}$ dacă $u \neq \mathbf{1}$ (sau $2 \cdot 2^m$ dacă $u = \mathbf{1}$). Dacă $c = (u, u + \mathbf{1})$, $u \in R(1, m)$, $u \neq \mathbf{1}$, atunci $\mathrm{wt}(u + \mathbf{1}) = 2^m - \mathrm{wt}(u) = 2^{m-1}$ (observaţi că adunînd **1** la u biţii care erau 1 devin 0 şi invers), deci $\mathrm{wt}(u, u + \mathbf{1}) = 2^m$. Dacă $c = (\mathbf{1}, \mathbf{1} + \mathbf{1}) = (0, \mathbf{1})$, atunci $\mathrm{wt}(c) = 2^m$. □

Codul Reed-Muller $R(1, 5)$ a fost folosit pentru comunicaţii din spaţiul cosmic în 1972, cînd sonda Mariner a transmis fotografii cu Marte.

Construcţia $(u, u + v)$ poate fi folosită pentru a defini recursiv codurile Reed-Muller binare de ordin r:

7 Definiţie. Pentru $r \in \mathbb{N}$ şi orice $m \geq r$, definim *codul binar Reed-Muller de ordin r,* $R(r, m)$:

a) $R(0, m)$ este codul binar de repetiţie de lungime 2^m. Este un cod tip $[2^m, 1, 2^m]$.

b) $R(r, r)$ este întreg spaţiul $\mathbb{F}_2^{2^r}$ (codul binar tip $[2^r, 2^r, 1]_2$).

c) Pentru orice $r > 0$ şi $r + 1 \le m$,

$$R(r, m) := R(r, m-1)|R(r-1, m-1).$$

Fie $G(r, m)$ o matrice generatoare a lui $R(r, m)$. Din definiţiile de mai sus rezultă că putem pune:

$$G(0, m) = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}; \; G(m, m) = I_{2^m}$$

Corolarul **4** permite să scriem:

$$G(r, m) = \begin{bmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{bmatrix}$$

Propunem ca exerciţiu demonstrarea următoarelor fapte despre codurile Reed-Muller folosind această definiţie:

8 Teoremă. *Fie* $r \in \mathbb{N}$ *şi* $m \ge r$. *Atunci* :

a) $R(r, m) \subseteq R(s, m)$ *dacă* $r \le s \le m$.

b) $\dim R(r, m) = \binom{m}{0} + \binom{m}{1} + \dots \binom{m}{r}$.

c) $d(R(r, m)) = 2^{m-r}$.

d) $R(m, m)^{\perp} = 0$.

e) $\forall r < m, R(r, m)^{\perp} = R(m-r-1, m)$. □

Alte construcţii importante (*întreţesere* şi *concatenare*) se vor descrie în capitolul de Aplicaţii.

În continuare descriem o construcţie bazată pe următoarea observaţie. *Fie E un corp cu* q^m *elemente şi F subcorpul său cu q*

elemente. Atunci orice E-spaţiu liniar de dimensiune k poate fi văzut ca un F-spaţiu liniar de dimensiune mk (demonstraţi!).

9 Teoremă. (Subcod determinat de un subcorp) *Fie C un cod* $[N, K, D]$ *peste corpul E cu* q^m *elemente şi F subcorpul său cu q elemente. Definim* $C|_F := C \cap F^N$ (*mulţimea cuvintelor cod cu toate coordonatele în F*). *Atunci* $C|_F$ *este un cod F-liniar de tip* $[n, k, d]$, *unde* $n = N$, $k \geq mK - (m-1)N$ *şi* $d \geq D$. *Dacă* $mK > (m-1)N$, *se poate obţine un cod F-liniar de tip* $[N, mK - (m-1)N, D]$.

Demonstraţie. Faptul că $C|_F$ este F-cod liniar şi că $d(C|_F) \geq d$ este propus spre demonstraţie cititorului. Evident, $N = n$. Avem:
$\dim_F C|_F = \dim_F (C \cap F^N) = \dim_F (C) + \dim_F (F^N) - \dim_F (C + F^N)$
$\geq mK + N - \dim_F (E^N) = mK + N - mN = mK - (m-1)N$.

Aplicînd construcţiile **III** şi **IV** lui $C|_F$, obţinem codul de tip $[N, mK - (m-1)N, D]$. □

Exerciţii

1. Demonstraţi că prin scurtarea unui cod tip $[n, k, d]$ pe o coordonată se obţine un cod tip $[n-1, k', d']$, unde $k - 1 \leq k' \leq k$ şi $d' \geq d$.

2. Presupunem că G este o matrice generatoare în formă standard pentru codul C de tip $[n, k, d]$. Scrieţi o matrice generatoare pentru C scurtat pe prima coordonată.

3. Fie C codul binar cu matricea generatoare

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Scrieţi o matrice generatoare pentru C scurtat pe coordonata 2.

4. Scrieţi toate cuvintele codului $R(1, m)$, pentru $m = 3,\ 4,\ 5$. Demonstraţi că $R(1, 3)$ este autodual.

5. Fie F un corp finit. a) Calculaţi cardinalul maxim al unei mulţimi S de coloane de lungime 2, cu proprietatea că orice două coloane din mulţime sînt liniar independente în F^2.

b) Demonstraţi că afirmaţia „$\forall n \geq 1$, există un cod de tip $[n + 2,\ n,\ 3]$ peste F" este falsă.

c) Demonstraţi că afirmaţia: „Pentru orice corp F şi orice $n,\ k,\ d,$ dacă există un F-cod liniar tip $[n,\ k,\ d]$, atunci există un F-cod liniar tip $[n + 1, k + 1, d]$" este falsă.

d) Demonstraţi că nu există un cod binar tip $[9, 4, 5]$.

e) Demonstraţi că afirmaţia: „Pentru orice corp F şi orice $n,\ k,\ d,$ dacă există un F-cod liniar tip $[n,\ k,\ d]$, atunci există un F-cod liniar tip $[n + 1, k, d + 1]$" este falsă.

6. a) Demonstraţi că există un cod binar $[63,\ 57,\ 3]$.

b) Determinaţi cel mai mic n cu proprietatea că există un cod binar $[n,\ 50,\ 3]$. (Ind. $n \geq 56$ din inegalitatea Hamming. Folosiţi construcţia **V** pentru codul de la a).)

7. a) Demonstraţi că există un cod binar $[67, 60, 3]$.

b) Determinaţi cel mai mic n cu proprietatea că există un cod binar $[n,\ 60, 4]$.

8. Fie $H_{4,\,r}$ un cod Hamming de lungime $(4^r - 1)/3$ peste $\mathbb{F}_4$. Ce informaţii oferă teorema **9** asupra parametrilor lui $H_{4,r}\big|_{\mathbb{F}_2}$? Determinaţi parametrii lui $H_{4,3}\big|_{\mathbb{F}_2}$.

9. Demonstraţi că extinderea codului binar Hamming H de tip [7, 4, 3] este un cod H' de tip [8, 4, 4]. Găsiţi o matrice generatoare în formă standard a lui H'. Demonstraţi că H' este cod autodual.

10. Fie codul binar G_{24} cu matricea generatoare $G = (I_{12} \mid A)$, unde

$$A = \left[\begin{array}{c|cccccccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Observaţi că fiecare din liniile submatricei A' (de tip 11×11 obţinută din A prin suprimarea liniei 1 şi a coloanei 1) este permutare circulară la stînga de linia precedentă. Se mai observă că în prima linie a lui A', în poziţia i este 1 ($i = 0, 1, \ldots, 10$) dacă şi numai dacă $i \in \{0, 1, 3, 4, 5, 9\}$, adică i este un pătrat în $\mathbb{Z}_{11}$ (i este rest pătratic mod 11).

a) Demonstraţi că linia 1 şi linia 2 a lui G sînt ortogonale între ele şi pe orice linie. Deduceţi că G_{24} este autodual.

b) Demonstraţi că şi $(A|I_{12})$ este matrice generatoare a lui G_{24}.

c) Demonstraţi că, $\forall a, b \in (\mathbb{F}_2)^{12}$, $(a, b) \in G_{24} \Leftrightarrow (b, a) \in G_{24}$.

d) Demonstraţi că nu există cuvinte cod de pondere 4 şi că distanţa minimă a lui G_{24} este 8.

e) Prin găurirea lui G_{24} pe prima coordonată, demonstraţi că există un cod binar G_{23} de tip [23, 12, 7].

Codul G_{24} se numeşte *codul binar Golay extins*, iar G_{23} se numeşte *codul binar Golay*. Demonstraţi că G_{23} este perfect.

VI. Coduri ciclice

Clasa codurilor ciclice este obţinută prin impunerea unei structuri suplimentare codurilor liniare. Aceasta permite o descriere mai precisă, o construcţie uşoară, compactă şi algoritmi eficienţi de codare şi decodare. Fixăm un corp finit F cu q elemente.

1 Definiţie. Un cod liniar C peste F se numeşte *ciclic* dacă, pentru orice $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, rezultă că *permutarea ciclică la dreapta a lui c*, adică $(c_{n-1}, c_0, \ldots, c_{n-2})$ este tot în C.

Codurile ciclice au o structură algebrică suplimentară:

2 Teoremă. *Fie C un cod liniar peste F şi fie R_n inelul factor $F[X]/(X^n - 1)$. Fie x clasa lui X modulo $(X^n - 1)$ şi fie submulţimea lui R_n:*

$$I_C := \{c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} | (c_0, c_1, \ldots, c_{n-1}) \in C\}.$$

Atunci: C este ciclic dacă şi numai dacă I_C este un ideal în R_n.

Demonstraţie. Fie C cod ciclic. I_C este clar parte stabilă la adunare în R_n. Fie $(c_0, c_1, \ldots, c_{n-1}) \in C$. Atunci avem, în R_n:

$x(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) = c_0 x + c_1 x^2 + \ldots + c_{n-1} x^n = c_{n-1} + c_0 x + \ldots + c_{n-2} x^{n-1} \in I_C$

Am folosit că în R_n are loc $x^n = 1$. Pentru orice $u = b_0 + b_1x + \ldots + b_mx^m \in R_n$ şi $v \in I_C$, uv este o combinaţie liniară de elemente de forma $x^t(c_0 + c_1x + \ldots + c_{n-1}x^{n-1})$, care sînt în I_C (se foloseşte o inducţie, cazul $t = 1$ a fost demonstrat).

Dacă I_C este ideal, atunci, $\forall(c_0, c_1, \ldots, c_{n-1}) \in C$, avem

$x(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = c_{n-1} + c_0x + \ldots + c_{n-2}x^{n-1} \in I_C$,

deci $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. □

3 Exerciţiu. Dacă I este ideal în R_n, cum îi putem asocia un cod liniar ciclic de lungime n peste F? Demonstraţi că *există o bijecţie între codurile liniare ciclice de lungime n peste F şi idealele lui* $R_n = F[X]/(X^n - 1)$.

Demonstraţia de mai sus arată că este util să vedem *cuvintele unui cod ciclic de lungime n peste F ca polinoame* $\bmod(X^n - 1)$; astfel, vom identifica cuvîntul $(c_0, c_1, \ldots, c_{n-1}) \in C$ cu $c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ din $R_n = F[X]/(X^n - 1)$.

Studiul codurilor ciclice de lungime n peste F este aşadar echivalent cu studiul idealelor lui $F[X]/(X^n - 1)$.

4 Lemă. *a) Fie R inel şi I un ideal în R. Atunci orice ideal al inelului factor R/I se poate scrie unic sub forma* $J/I = \{j + I \mid j \in J\}$, *unde J este un ideal al lui R care include I. Mai precis, aplicaţia* $J \mapsto J/I$ *este o bijecţie care păstrează incluziunile între mulţimea idealelor lui R care includ I şi mulţimea idealelor lui R/I.*

b) Idealele lui $F[X]$ *sînt de forma* $(g) = \{gh \mid h \in F[X]\}$, *cu* $g \in F[X]$. *Pentru un ideal nenul I al lui* $F[X]$, *avem* $I = (g)$, *dacă g*

este un polinom nenul din I de grad minim. Un astfel de polinom g este numit generator *al lui I.*

Demonstraţie. a) Dacă B este ideal în R/I, atunci $I_B := \{r \in R \mid r + I \in B\}$ este ideal în R şi $B = I_B/I$ (demonstraţi!).

b) Fie I un ideal nenul în $F[X]$ şi fie $g \in I$ un polinom monic al cărui grad e cel mai mic printre gradele polinoamelor nenule din I. Dacă $f \in I$, atunci $f = gq + r$, unde $q,\ r \in K[X]$, grad $r <$ grad g (sau $r = 0$). Cum $r = f - gq$ şi I is an ideal, avem $r \in I$; grad $r <$ grad g implică $r = 0$. Deci $f = gq \in (g)$, $\forall f \in I$. □

5 Teoremă. *Pentru orice ideal I al lui* $R_n = F[X]/(X^n - 1)$, *există un unic polinom monic* $g \in F[X]$ *astfel încît* $g|(X^n - 1)$ *şi* $I = (g)/(X^n - 1) = \{hg \bmod (X^n - 1) \mid h \in F[X]\}$.

Demonstraţie. Lema de mai sus spune că $I = J/(X^n - 1)$, pentru un ideal al lui $F[X]$ care include $(X^n - 1)$. Dar J este de forma (g), unde $(g) \supseteq (X^n - 1)$, i.e. $g|(X^n - 1)$. □

Conchidem că un cod ciclic C este unic determinat de generatorul monic g din demonstraţia de mai sus, numit *polinomul generator al codului C*. Deci, polinomul monic $g \in F[X]$ este polinomul generator al codului ciclic C de lungime n dacă şi numai dacă $g|(X^n - 1)$ şi

$$C = \{hg \bmod (X^n - 1) \mid h \in F[X]\}.$$

(Identificăm cuvintele din C cu polinoamele mod $(X^n - 1)$!)

6 Propoziţie. *Fie C cod ciclic de lungime n şi fie g polinomul său generator. Atunci orice cuvînt din C poate fi unic scris sub forma hg, cu* $h \in F[X]$, grad $h <$ $n -$ grad g *:*

$$C = \{hg \bmod (X^n - 1) \mid h \in F[X], \text{ grad } h < n - \text{grad } g\}.$$

În particular, dimensiunea lui C este k = n – grad g.

Demonstraţie. Deoarece $g|(X^n - 1)$, există $d \in F[X]$ astfel încît $X^n - 1 = gd$. Fie $h \in F[X]$ oarecare. Din teorema împărţirii cu rest există $q,\ r \in F[X]$ cu $h = dq + r$, grad $r <$ grad $d = n -$ grad g. Deci (egalităţile sînt mod$(X^n - 1)$):

$$hg = (dq + r)g = gdq + rg = (X^n - 1)q + rg = rg \bmod (X^n - 1). \ \square$$

Fie C un cod ciclic $[n, k, d]$ şi fie g polinomul său generator. Propoziţia de mai sus spune că o bază pentru C este $g,\ xg, \ldots, x^{k-1}g$. Presupunem că $g = a_0 + a_1 X + \ldots + a_n X^{n-k}$. Aşadar, o matrice generatoare a lui C este:

$$\begin{bmatrix} a_0 & a_1 & \ldots & a_{n-k} & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_{n-k} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & a_0 & a_1 & \ldots & \ldots & a_{n-k} \end{bmatrix} \in \mathrm{M}(k, n, F)$$

Presupunem de acum înainte că $(q, n) = 1$.

Această presupunere e necesară deoarece avem nevoie de o extindere a lui $\mathbb{F}_q$ în care $X^n - 1$ se descompune în factori liniari *distincţi* (adică $X^n - 1$ nu are rădăcini multiple; din criteriul cu derivata formală, aceasta echivalează cu $(X^n - 1,\ nX^{n-1}) = 1 \Leftrightarrow nX^{n-1} \neq 0 \Leftrightarrow (q, n) = 1$). Dacă o astfel de extindere F există, F are q^m elemente. Cum rădăcinile lui $X^n - 1$ formează un subgrup de ordin n şi F^* are ordin $q^m - 1$, din teorema lui Lagrange rezultă $n \mid q^m - 1$. Fie ω un generator al lui F^* (*un element primitiv al lui F*); atunci $\alpha = \omega^{(q^m-1)/n}$ are ordin n in F^* (este o *rădăcină primitivă de ordinul n a unităţii în F*) şi avem:

$$X^n - 1 = \prod_{i=0}^{n-1} \left(X - \alpha^i \right)$$

Deoarece generatorul g divide $X^n - 1$, rezultă că:

$g = \prod_{i \in I} \left(X - \alpha^i \right)$, pentru o submulţime $I \subseteq \{0, 1, \ldots, n-1\}$.

Mulţimea I se numeşte *mulţimea de definiţie a lui* C (în raport cu α).

7 Observaţie. Cu notaţiile de mai sus, I este mulţimea de definiţie a lui C dacă şi numai dacă are loc: $\forall c \in F[X]/(X^n - 1)$, $c \in C \Leftrightarrow c(\alpha^i) = 0, \forall i \in I$.

Nu orice submulţime a lui $\{0, 1, \ldots, n-1\}$ este mulţime de definiţie pentru un cod ciclic, deoarece g trebuie să aibă coeficienţi în $\mathbb{F}_q$. Avem nevoie de următorul rezultat din teoria Galois.

8 Propoziţie. *Fie* $F \subseteq E$ *o extindere de corpuri finite,* $|F| = q$, $|E| = q^m$. *Atunci* $F = \{x \in E \mid x^q = x\}$. *Fie* $\varphi : E \to E$, $\varphi(x) = x^q$. *Extindem* φ *la* $\psi : E[X] \to E[X]$,

$$\psi(a_0 + a_1 X + \ldots + a_n X^n) = \varphi(a_0) + \varphi(a_1) X + \ldots + \varphi(a_n) X^n$$

Atunci ψ *este un morfism de inele şi* $f \in F[X]$ *dacă şi numai dacă* $\psi(f) = f$.

Demonstraţie. Faptul că $F = \{x \in E \mid x^q = x\}$ e demonstrat la Teorema **III.16**.b). Cum φ este automorfism (este o putere a automorfismului Frobenius), un calcul direct arată că ψ este automorfism. Avem:

$\psi(a_0 + a_1 X + \ldots + a_n X^n) = a_0 + a_1 X + \ldots + a_n X^n \Leftrightarrow \varphi(a_0) = a_0$, $\ldots$, $\varphi(a_n) = a_n \Leftrightarrow a_0, \ldots, a_n \in F \Leftrightarrow a_0 + a_1 X + \ldots + a_n X^n \in F[X]$. □

Aplicînd acest rezultat la $g = \prod_{i \in I} \left(X - \alpha^i \right)$, avem: $g \in F[X] \Leftrightarrow g = \psi(g) = \prod_{i \in I} \left(X - \alpha^{iq} \right)$. Am obţinut următoarea:

9 Propoziţie. *Mulţimea* $I \subseteq \{0, 1, \ldots, n-1\}$ *este mulţime de definiţie pentru un anumit cod ciclic* C *dacă şi numai dacă are proprietatea că, pentru orice* $i \in I$, *rezultă că* $iq \pmod n$ *este tot în* I. □

Se observă că g factorizează într-un produs de polinoame ireductibile peste $\mathbb{F}_q$, alese dintre factorii lui $X^n - 1$. Cum $X^n - 1$ nu are rădăcini multiple, g este produs de polinoame ireductibile distincte. Un astfel de polinom ireductibil este de fapt polinomul minimal m_i al unui α^i pentru un i, $0 \le i < n$, şi trebuie să aibă şi rădăcinile obţinute aplicînd automorfismul $z \mapsto z^q$, adică α^i, α^{iq}, α^{iq^2}, … . În concluzie, g este produs de polinoame minimale distincte m_i.

Unul din cele mai importante exemple de coduri ciclice (foarte folosit în practică) este următorul:

10 Definiţie. Fie $\mathbb{F}_q \setminus \{0\} = \{1, \alpha, \ldots, \alpha^{q-2}\}$ unde α este un element primitiv al lui $\mathbb{F}_q$ (deci α este de ordin $q-1$ în $\mathbb{F}_q^*$) şi $1 \le k \le q-1$. *Codul Reed-Solomon* $RS(k, q)$ este codul următor de lungime $n = q - 1$:

$$RS(k,q) := \{(f(1), \ldots, f(\alpha^{q-2})) \in \mathbb{F}_q^{q-1} \mid f \in \mathbb{F}_q[X], \operatorname{grad} f \le k-1\}$$

11 Teoremă. *RS*(*k, q*) *este cod liniar ciclic tip* [$q-1$, k, $q-k$] (*cod MDS*).

Demonstraţie. $\{f \mid f \in \mathbb{F}_q[X],\ \operatorname{grad} f \le k-1\} =: L_{k-1}$ este un subspaţiu liniar al lui $\mathbb{F}_q[X]$ de dimensiune k. *RS*(*k, q*) poate fi văzut ca imaginea funcţiei de evaluare $ev : L_{k-1} \to \mathbb{F}_q^{\,q-1}$, $ev(f) = (f(1),\ \ldots, f(\alpha^{q-2}))$. Deci *RS*(*k, q*) este subspaţiu liniar, căci *ev* este liniară. Dimensiunea este k, deoarece *ev* este injectivă: orice $f \in L_{k-1}$ cu $ev(f) = (0,\ \ldots,\ 0)$ are $q-1 > \operatorname{grad} f$ rădăcini şi trebuie să fie 0).

Dacă $\mathrm{wt}(f(1),\ \ldots, f(\alpha^{q-2})) < q-1-k+1$, atunci numărul de coordonate i cu $f(\alpha^i) = 0$ este mai mare decît $k-1$. Deci f are mai multe rădăcini decît gradul, i.e $f = 0$. Astfel, ponderea minimă a cuvintelor lui *RS*(*k, q*) este $d = q-k$, adică este un *cod MDS*.

Orice cod Reed-Solomon este ciclic. Într-adevăr, o bază a subspaţiului k-dimensional *RS*(*k, q*) este $\{ev(X^j) \mid 0 \le j \le k-1\}$, unde $ev(X^j) = ((\alpha^j)^0, \ldots, (\alpha^j)^{q-2})$. Permutînd ciclic la dreapta acest cuvînt cod obţinem $((\alpha^j)^{q-2}, (\alpha^j)^0, \ldots, (\alpha^j)^{q-3}) = \alpha^{-j} ev(X^j)$, care aparţine *RS*(*k, q*) (vezi şi exerciţiul **1**). □

Codurile Reed-Solomon au aplicaţii practice importante, fiind folosite la schemele de codare pentru corectarea de erori la medii de stocare (CD, DVD, Blu-Ray), la transmisii de date (DSL, WiMAX), DVB (Digital Video Broadcast), la anumite implementări ale RAID 6.

Exerciţii

1. Fie C cod liniar şi fie $\{u_1, \ldots, u_k\}$ o bază în C. Demonstraţi că C este ciclic dacă şi numai dacă permutările ciclice la dreapta ale oricărui u_i sînt cuvinte cod în C.

2. Fie $g \in F[X]$ polinomul generator al unui cod ciclic de lungime n astfel încît $(X-1) \nmid g$. Demonstraţi că

$$C' = \{(c_0, \ldots, c_{n-1}) \in F^n \mid (c_0, \ldots, c_{n-1}) \in C,\ c_0 + \ldots + c_{n-1} = 0\}$$

este cod ciclic şi are polinom generator $(X-1)g$. Ce se întîmplă dacă $(X-1) \mid g$?

3. Fie C cod binar ciclic şi g polinomul generator. Demonstraţi că toate cuvintele lui C au pondere pară dacă şi numai dacă g este divizibil cu $X-1$.

4. Fie $g = 1 + X^2 + X^5 \in \mathbb{F}_2[X]$. Demonstraţi că g generează un cod ciclic C de tip [31, 26, 3]. Demonstraţi că mulţimea cuvintelor de pondere pară ale lui C este codul din exemplul **5**. Scrieţi polinomul generator.

5. Fie C cod liniar ciclic. Demonstraţi că $C^\perp$ este ciclic.

6. Fie $g = a_0 + a_1 X + \ldots + a_m X^m$ polinomul generator al codului ciclic C, de lungime n. Definim *reciprocul* lui g:

$$g_R := a_m + a_{m-1} X + \ldots + a_0 X^n.$$

Fie $h \in F[X]$ astfel încît $gh = X^n - 1$. Demonstraţi că h_R generează codul dual $C^\perp$. (*Ind.* Fie $g = g_0 + g_1 X + \ldots + g_{n-1} X_{n-1}$ şi $h = h_0 + h_1 X + \ldots + h_{n-1} X_{n-1}$, cu g_{n-1} şi h_{n-1} posibil 0. Calculaţi gh mod $(X^n - 1)$ şi comparaţi coeficienţii. Conchideţi că h_R (ca vector în F^n) este ortogonal pe $(g_0, g_1, \ldots, g_{n-1})$ şi pe toate permutările sale ciclice).

7. Descompuneţi în factori polinomul $X^8 - 1 \in \mathbb{F}_3[X]$. Calculaţi numărul codurilor ciclice de lungime 8 peste $\mathbb{F}_3$.

VII. Coduri BCH

Codurile Reed-Solomon sînt o subclasă a unei clase de coduri ciclice cunoscute drept coduri BCH (numele este un acronim format cu numele celor care le-au inventat: R.C. Bose şi D.K. Ray-Chaudhuri în 1960 şi, independent, A. Hocquenghem în 1959). Interesul pentru aceste coduri este dat de faptul că această construcţie permite crearea de coduri care au o distanţă minimă prescrisă. Menţinem presupunerea că $(q, n) = 1$, adică $X^n - 1$ se descompune în factori liniari *distincţi* într-o anumită extindere a lui $\mathbb{F}_q$.

1 Definiţie. Fie $n \geq 2$ şi $t \in \mathbb{N}^*$. Fie α o rădăcină primitivă de ordin n a unităţii într-o extindere $\mathrm{GF}(q^m)$ a lui $\mathrm{GF}(q)$ şi fie I mulţimea de definiţie a unui cod ciclic $C \subseteq \mathrm{GF}(q)^n$.

Codul C se numeşte *cod BCH de distanţă din design* t dacă I conţine $t - 1$ numere consecutive. Dacă $\{1, \ldots, t - 1\} \subseteq I$, atunci C se numeşte cod BCH *în sens restrîns*. Dacă $n = q^m - 1$ (adică α este element primitiv al lui $\mathrm{GF}(q^m)$), atunci C este numit *primitiv*.

Echivalent spus, un cod BCH de distanţă din design t este un *cod ciclic cu generator egal cu cel mai mic multiplu comun al polinoamelor minimale ale* α^j, α^{j+1}, …, α^{j+t-2} pentru un $j \geq 0$.

2 Exerciţiu. $RS(k, q)$ este cod BCH primitiv în sens restrîns, de lungime $q-1$ (deci $m=1$ şi $n=q-1$ în definiţia de mai sus). Generatorul său este $g=(X-\alpha)\ldots(X-\alpha^{q-k-1})$.

Denumirea de *cod BCH de distanţă din design t* este justificată:

3 Teoremă (**inegalitatea BCH**, **BCH bound**) *Distanţa minimă d a unui cod BCH cu distanţă din design t este cel puţin t.*

Demonstraţie. Fie $j, j+1, \ldots, j+t-2$ în mulţimea de definiţie a lui C şi fie $c=\sum_{s=1}^{d} c_{i_s} x^{i_s}$ un cuvînt cod nenul în C de pondere d (unde $c_{i_j} \neq 0, \ \forall j$). Presupunem prin absurd că $d<t$. Deoarece $c(\alpha^i)=0, \forall i, j \leq i \leq j+t-2$, avem $Ac=0$, unde

$$A=\begin{bmatrix} \alpha^{i_1 j} & \alpha^{i_2 j} & \ldots & \alpha^{i_d j} \\ \alpha^{i_1 (j+1)} & \alpha^{i_2 (j+1)} & \ldots & \alpha^{i_d (j+1)} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{i_1 (j+d-1)} & \alpha^{i_2 (j+d-1)} & \ldots & \alpha^{i_d (j+d-1)} \end{bmatrix}, \ c=\begin{bmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_d} \end{bmatrix}$$

Avem:

$$\det A = \alpha^{i_1 j}\alpha^{i_2 j}\ldots\alpha^{i_d j} \cdot \det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \ldots & \alpha^{i_d} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{i_1 (d-1)} & \alpha^{i_2 (d-1)} & \ldots & \alpha^{i_d (d-1)} \end{bmatrix} \neq 0,$$

(ultimul determinant este tip Vandermonde). Deci $c=0$, contradicţie. □

4 Observaţie. Există multe coduri ciclice cu distanţa minimă mai mare decît cea garantată de inegalitatea BCH. O cale de a îmbunătăţi estimarea distanţei pentru un cod ciclic este următoarea: să observăm că mulţimea de definiţie I a codului ciclic C depinde de alegerea rădăcinii primitive de ordin n a unităţii α din F. Orice altă rădăcină primitivă de ordin n a unităţii β este de forma $\beta = \alpha^a$, cu $(a, n) = 1$. Fie $b \in \mathbb{N}$ astfel încît $ab = 1 \pmod n$; atunci $1 = \left(\alpha^a\right)^b = \beta^b$. Mulţimea de definiţie a lui C relativă la β este $J = \{bi \pmod n \mid i \in I\} := bI$. Se poate întîmpla ca bI să aibă mai multe elemente consecutive decît I. Deci, cînd estimăm cu inegalitatea BCH distanţa minimă a unui cod ciclic de mulţime de definiţie I, un *multiplicator* (un număr întreg b prim cu n) poate fi aplicat lui I.

5 Exemplu. Construim un cod ciclic binar C de lungime 31 a cărui mulţime de definiţie conţine 0 şi 3. Deci $q = 2$ şi $n = 31$. Cel mai mic m astfel încît $31 \mid 2^m - 1$ este 5; o rădăcină primitivă de ordin 31 a unităţii, $\alpha \in \mathbb{F}_{32}$, este de fapt un element primitiv al $\mathbb{F}_{32}$. Mulţimea de definiţie a lui C trebuie să conţină 3, $3 \cdot 2 = 6$, $6 \cdot 2 = 12$, $12 \cdot 2 = 24$, $24 \cdot 2 = 48 = 17$, $17 \cdot 2 = 34 = 3$ (calcule mod 31). Deci mulţimea de definiţie este $I = \{0, 3, 6, 12, 24, 17\}$, care furnizează $d(C) \geq 2$. Cum apar multipli de 3 consecutivi, alegem multiplicatorul să fie $21 = 3^{-1} \pmod{31}$; obţinem $21I = \{0, 1, 2, 4, 8, 16\}$, care dă $d(C) \geq 4$. Cît este dim C?

Multe coduri Hamming (în particular codurile Hamming binare) sunt de fapt coduri BCH:

6 Propoziţie. *Fie* $n = (q^r - 1)/(q - 1)$, *cu* $(r, q - 1) = 1$. *Fie C codul BCH cu generator polinomul minimal al lui* α, *rădăcină primitivă de ordin n a unităţii într-o extindere a lui* $\mathbb{F}_q$. *Atunci C este codul Hamming* $H_{q,r}$.

Demonstraţie. Arătăm că $(n, q - 1) = 1$. Pentru aceasta, observăm că $n - r$ este multiplu de $q - 1$:

$$n = \frac{q^r - 1}{q - 1} = 1 + q + \ldots + q^{r-1} = 1 + q - 1 + 1 + q^2 - 1 + 1 + \ldots + q^{r-1} - 1 + 1$$
$$= r + (q - 1) \cdot c$$

de unde rezultă $(n, q - 1) = (r, q - 1) = 1$.

Fie γ un element primitiv în GF(q^r) şi $\alpha \in$ GF(q^r), ord $\alpha = n$. Cum ord $\gamma = q^r - 1$, putem lua $\alpha = \gamma^{\frac{q^r - 1}{n}} = \gamma^{q-1}$.

Codul C are ca generator polinomul minimal al lui α peste GF(q). Observăm că singura putere a lui α care aparţine lui GF(q)* este 1. Într-adevăr, dacă $i \in \{0, \ldots, n-1\}$ şi $\alpha^i \in$ GF(q)*, atunci $(\alpha^i)^{q-1} = 1$. Cum ord $\alpha = n$, rezultă $n \mid i(q - 1)$. Însă $(n, q - 1) = 1$, deci $n \mid i$, şi $i = 0$.

Deci, în GF(q^r), văzut ca GF(q) – spaţiu vectorial, elementele mulţimii $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$ sunt două câte două liniar independente (niciunul nu este multiplu scalar de celălalt).

Ştim că:

$C = \{(c_0, c_1, \ldots, c_{n-1}) \in (\mathrm{GF}(q))^r \mid c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} = 0\}$.

Alegem un $\mathbb{F}_q$-izomorfism $\varphi : \mathrm{GF}(q)^r \to \mathrm{GF}(q^r)$ (pentru că GF(q^r) are dimensiunea r, ca GF(q)-spaţiu vectorial). Relaţia de liniară dependenţă $c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} = 0$ este echivalentă (via φ) în GF(q)^r cu $c_0\varphi(\alpha^0) + \ldots + c_{n-1}\varphi(\alpha^{n-1}) = 0$. Aşadar,

$C = \{(c_0, c_1, \ldots c_{n-1}) \in \mathrm{GF}(q)^r \mid c_0\varphi(\alpha^0) + \ldots + c_{n-1}\varphi(\alpha^{n-1}) = 0\}$ este codul cu matricea de paritate $(\varphi(\alpha^0), \ldots, \varphi(\alpha^{n-1}))$ de tip $r \times n$ peste GF(q), care este matrice de tip Hamming de paritate a codului C. (Amintim că o matrice de paritate pentru codul Hamming $H_{q,r}$ se obţine prin alegerea în GF(q) a $(q^r - 1)/(q - 1)$ coloane astfel încât oricare două să fie liniar independente.) □

Algoritmul Petersen-Gorenstein-Ziegler

Fie C un cod BCH de lungime n peste corpul GF(q) (cu q o putere a numărului prim p) şi $m \in \mathbb{N}$ astfel încît GF(q^m) conţine un element α de ordin n. Presupunem că C are distanţa minimă din design d, deci C poate corecta $t = [(d - 1)/2]$ erori. Pentru simplificarea notaţiilor, presupunem că C este în sens restrîns, adică mulţimea de definiţie T a lui C în raport cu α include $\{1, 2, \ldots, d - 1\}$.

Fie $c \in C$ un cuvînt transmis şi y cuvîntul recepţionat. Ca de obicei, c şi y sunt presupuse a fi polinoame de grad cel mult $n - 1$ din GF(q)[x]. Deci $y = c + e$, unde e este *vectorul (polinomul) eroare*, de pondere $\mathrm{wt}(e) = v$. Presupunem că $v \le t$, adică au avut loc cel mult t erori. Dacă poziţiile în care apar erori sunt $k_1, \ldots, k_v$, atunci:

$$e(x) = e_{k_1} x^{k_1} + \ldots + e_{k_v} x^{k_v}.$$

Scopul nostru este de a afla e, ceea ce permite determinarea cuvîntului transmis: $c = y - e$. Pentru aceasta, e suficient să determinăm *localizările erorilor* (error locations) $k_1, \ldots, k_v$ şi *valorile erorilor* (error magnitudes) $e_{k_1}, \ldots, e_{k_v}$. Observăm că v nu este cunoscut.

Amintim că, $\forall c \in \mathrm{GF}(q)[X]/(X^n - 1)$, avem $c \in C \Leftrightarrow c(\alpha^i) = 0$, $\forall i \in T$. Deci:

$$y(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i),\ \forall i \in T$$

Notăm cu $S_i = y(\alpha^i) \in \mathrm{GF}(q^m)$, $1 \le i \le 2t$, *sindroamele* lui y. Primul pas al algoritmului calculează aceste sindroame. În acest calcul următoarea proprietate poate fi utilă:

7 Propoziţie: $S_{iq} = S_i^q$, $\forall i \in T$.

Demonstraţie. $S_{iq} = y(\alpha^{iq}) = y(\alpha^i)^q$ (deoarece calculele sunt în corpuri de caracteristică p, iar coeficienţii lui y sunt în GF(q)). □

Avem $\forall i$, $1 \le i \le 2t$:

$$S_i = y(\alpha^i) = e(\alpha^i) = e_{k_1}(\alpha^i)^{k_1} + \ldots + e_{k_v}(\alpha^i)^{k_v} =$$
$$= e_{k_1}(\alpha^{k_1})^i + \ldots + e_{k_v}(\alpha^{k_v})^i$$

Vom simplifica notaţiile. Fie, pentru orice $1 \le j \le v$,

$E_j = e_{k_j}$ („valorile erorilor”, *error magnitudes*)

$X_j = \alpha^{k_j}$ („numerele” asociate localizărilor erorilor, *error location numbers*)

Observăm că X_j determină în mod unic k_j. Aşadar:

$S_i = E_1 X_1^{\,i} + \ldots + E_v X_v^{\,i}$, pentru orice i, $1 \le i \le 2t$.

Obţinem sistemul:

$$\begin{aligned} S_1 &= E_1 X_1 + \ldots + E_v X_v \\ S_2 &= E_1 X_1^{\,2} + \ldots + E_v X_v^{\,2} \\ &\ldots \\ S_{2t} &= E_1 X_1^{\,2t} + \ldots + E_v X_v^{\,2t} \end{aligned} \qquad \text{(N)}$$

Pentru a rezolva acest sistem (neliniar) cu $2v$ necunoscute X_j şi E_j $(1 \le j \le v)$, definim noile variabile $\sigma_1, \ldots, \sigma_v$ şi *polinomul de localizare a erorilor* $\sigma(x)$ prin:

$$\sigma(x) = (1 - xX_1)\ldots(1 - xX_v) = 1 + \sigma_1 x + \ldots + \sigma_v x^v \qquad (\sigma)$$

Rădăcinile lui $\sigma(x)$ sînt $X_1^{-1}, \ldots, X_v^{-1}$, deci avem ecuaţiile:

$$\sigma(X_j^{-1}) = 1 + \sigma_1 X_j^{-1} + \ldots + \sigma_v X_j^{-v} = 0,\ 1 \le j \le v$$

Prin înmulţire cu $E_j X_j^{i+v}$, obţinem:

$$E_j X_j^{i+v} + \sigma_1 E_j X_j^{i+v-1} + \ldots + \sigma_v E_j X_j^i = 0,\ \forall i$$

Sumînd după j de la 1 la v, rezultă

$$\sum_{j=1}^{v} E_j X_j^{i+v} + \sigma_1 \sum_{j=1}^{v} E_j X_j^{i+v-1} + \ldots + \sigma_v \sum_{j=1}^{v}, E_j X_j^i = 0,\ \forall i$$

Se observă că sumele sunt exact sindroamele $S_{i+v}, \ldots, S_i$ (dacă $i \ge 1$ şi $i + v \le 2t$). Astfel, pentru orice $i \le v$, ecuaţia de mai sus se scrie:

$$\sigma_1 S_{i+v-1} + \sigma_2 S_{i+v-2} + \ldots + \sigma_v S_i = -S_{i+v}$$

Scrise matricial, aceste ecuaţii devin:

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{v-1} & S_v \\ S_2 & S_3 & \cdots & S_v & S_{v+1} \\ & & \vdots & & \\ S_v & S_{v+1} & \cdots & S_{2v-2} & S_{2v-1} \end{bmatrix} \begin{bmatrix} \sigma_v \\ \sigma_{v-1} \\ \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ \\ -S_{2v} \end{bmatrix} \qquad (S)$$

Pasul 2 al algoritmului va rezolva acest sistem, aflînd $\sigma_1, \ldots, \sigma_v$. Mai întîi însă, trebuie să aflăm v, *numărul de erori produse*. Folosim faptul că sistemul (S) trebuie să aibă o soluţie unică, adică matricea sistemului trebuie să fie nesingulară.

8 Lemă. *Pentru orice $v \le b \le t$, fie M_b matricea cu elemente în* GF(q^m):

$$M_b = \begin{bmatrix} S_1 & S_2 & \cdots & S_{b-1} & S_b \\ S_2 & S_3 & \cdots & S_b & S_{b+1} \\ & & \vdots & & \\ S_b & S_{b+1} & \cdots & S_{2b-2} & S_{2b-1} \end{bmatrix}$$

Atunci M_b este inversabilă dacă $b = v$ şi neinversabilă dacă $b > v$.

Demonstraţie. Presupunem că $b \ge v$. Punem $X_j = E_j = 0$ pentru j între $v + 1$ şi b. Notăm:

$$A_b = \begin{bmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_b \\ & & \vdots & \\ X_1^{b-1} & X_2^{b-1} & \dots & X_b^{b-1} \end{bmatrix} \quad B_b = \begin{bmatrix} E_1X_1 & 0 & \dots & 0 \\ 0 & E_2X_2 & \dots & 0 \\ & & \vdots & \\ 0 & 0 & \dots & E_bX_b \end{bmatrix}.$$

Un calcul direct arată că $M_b = A_b B_b A_b^{\mathrm{T}}$. Deci $\det M_b = \det A_b \cdot \det B_b \cdot \det A_b$. Dacă $b > v$, atunci $\det B_b = 0 = \det M_b$. Dacă $b = v$, atunci $\det B_b = E_1X_1 \cdot \ldots \cdot E_vX_v \ne 0$ şi $\det A_b \ne 0$ (este determinant Vandermonde cu $X_1, \ldots, X_b$ distincte). □

Lema arată că *numărul de erori v este*

$$v = \max \{b \mid b \le t, \det M_b \ne 0\}.$$

Pasul 2 al algoritmului determină numărul de erori v, folosind lema de mai sus. Astfel, iniţializăm $b = t$. Dacă $\det M_b = 0$, punem $b = b - 1$ şi reluăm calculul, pînă obţinem o matrice nesingulară M_b. Pentru acest b, punem $v = b$ şi rezolvăm sistemul (S). Se obţin $\sigma_1, \ldots, \sigma_v$ şi deci polinomul $\sigma(x)$.

La Pasul 3 se determină rădăcinile lui $\sigma(x)$. Cum rădăcinile lui σ sunt de forma α^i, $1 \le i < n$, ele se pot determina prin încercări

succesive, calculînd $\sigma(\alpha^i)$, $1 \le i < n$. Apoi se găsesc X_i, inversele acestor rădăcini.

Pasul 4 determină valorile erorilor, E_1, …, E_v. Pentru aceasta se rezolvă sistemul liniar (N) cu necunoscutele E_1, …, E_v, în care cunoaştem S_i şi X_i. E suficient să ne limităm la primele v ecuaţii, deoarece determinantul sistemului este nenul:

$$\begin{aligned} E_1X_1 + \ldots + E_vX_v &= S_1 \\ E_1X_1^{\,2} + \ldots + E_vX_v^{\,2} &= S_2 \\ &\ldots \\ E_1X_1^{\,v} + \ldots + E_vX_v^{\,v} &= S_v \end{aligned} \qquad \text{(S1)}$$

Sumarizînd, se obţine:

Algoritmul Petersen-Gorenstein-Ziegler de decodare a codurilor BCH

Pas 1. Calculează sindroamele $S_i = y(\alpha^i) \in \mathrm{GF}(q^m)$, $1 \le i \le 2t$. Dacă $S_i = 0$, $\forall i \in T$, atunci nu au avut loc erori. Dacă nu, treci la pasul 2.

Pas 2. Se caută, în ordine descrescătoare, începînd cu $b = t$, continuînd cu $b = t-1$, …, prima valoare pentru care M_b este nesingulară. Punem $v = b$ şi se rezolvă (S), obţinîndu-se $\sigma(x)$.

Pas 3. Se determină rădăcinile lui σ (eventual prin încercarea directă a tuturor α^i, $1 \le i < n$). Se determină X_j (localizarea erorilor) ca inversele acestor rădăcini.

Pas 4. Se rezolvă (S1) şi se află E_j (valorile erorilor).

9 Exemplu. a) Construim un cod BCH binar în sens restrîns de lungime 15 cu distanţă din design 7 (deci algoritmul corectează

pînă la $t = 3$ erori). Avem nevoie de o extindere a lui $\mathbb{F}_2$ care conţine o rădăcină primitivă de ordin 15. Fie $\alpha \in \mathbb{F}_{16}$, rădăcină a polinomului ireductibil $1 + X + X^4$; α este element primitiv (verificaţi!). În prealabil este necesară exprimarea elementelor din $\mathbb{F}_{16}$ ca puteri ale lui α. Cum distanţa din design este 7 şi codul este în sens restrîns, mulţimea de definiţie I include {1, 2, 3, 4, 5, 6}; rezultă că $I = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 9\}$. Ce dimensiune are codul?

Să presupunem că au apărut două erori, pe poziţiile 4 şi 11 ale cuvîntului transmis. Ele reprezintă polinomul eroare $e = X^3 + X^{10}$.

Folosind lista elementelor lui $\mathbb{F}_{16}$ ca puteri ale lui α, putem calcula sindroamele $S_1, \ldots, S_6$:

$S_1 = e(\alpha) = \alpha^3 + \alpha^{10} = \alpha^{12}$

$S_2 = e(\alpha^2) = e(\alpha)^2 = (S_1)^2 = \alpha^{24} = \alpha^9$

$S_3 = e(\alpha^3) = \alpha^9 + \alpha^{30} = \alpha^9 + 1 = \alpha^7$

$S_4 = (S_2)^2 = \alpha^{18} = \alpha^3$

$S_5 = e(\alpha^5) = \alpha^{15} + \alpha^{50} = \alpha^0 + \alpha^5 = \alpha^{10}$

$S_6 = (S_3)^2 = \alpha^{14}$.

Observăm că într-o situaţie reală se cunoaşte doar sindromul cuvîntului recepţionat:

$$S = (S_1, S_2, S_3, S_4, S_5, S_6) = (\alpha^{12}, \alpha^9, \alpha^7, \alpha^3, \alpha^{10}, \alpha^{14})$$

Calculăm numărul de erori v. Conform pasului 2:

$$\det M_3 = \begin{vmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{vmatrix} = \begin{vmatrix} \alpha^{12} & \alpha^9 & \alpha^7 \\ \alpha^9 & \alpha^7 & \alpha^3 \\ \alpha^7 & \alpha^3 & \alpha^{10} \end{vmatrix} = 0$$

(Era de aşteptat, sînt 2 erori, deci $\det M_3 = 0$). Avem $\det M_2 = \begin{vmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & \alpha^7 \end{vmatrix} = \alpha^7 \neq 0$. Astfel, $v = 2$ şi sistemul (S) devine:

$$\begin{cases} S_1\sigma_2 + S_2\sigma_1 = S_3 \\ S_2\sigma_2 + S_3\sigma_1 = S_4 \end{cases} \Leftrightarrow \begin{cases} \alpha^{12}\sigma_2 + \alpha^9\sigma_1 = \alpha^7 \\ \alpha^9\sigma_2 + \alpha^7\sigma_1 = \alpha^3 \end{cases}$$

Rezolvînd, se obţine $\sigma_1 = \alpha^{12}$, $\sigma_2 = \alpha^{13}$.

Deci $\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 = 1 + \alpha^{12}x + \alpha^{13}x^2$. Are ca rădăcini (prin încercări) pe α^{12} şi α^5. Deci $X_1 = \alpha^{-12} = \alpha^3$, $X_2 = \alpha^{-5} = \alpha^{10}$.

Am redescoperit astfel cele două localizări ale erorilor, poziţiile 4 şi 11. Codul fiind binar, corectarea se face modificînd biții de pe pozițiile 4 și 11 din cuvîntul recepționat.

Exerciţii

1. Scopul exerciţiului este de a construi un cod C, BCH, ternar de lungime 13, distanţă minimă 5 şi dimensiune maxim posibilă.

a) Demonstraţi că $\min\{m \in \mathbb{N} \mid \mathrm{GF}(3^m)$ conţine o rădăcină primitivă de ordin 13 a unităţii$\}$ este 3. Fie $\omega \in \mathrm{GF}(3^3)$ o rădăcină primitivă de ordin 13 a unităţii.

b) Scrieţi coseturile 3-ciclotomice mod 13, C_i, $0 \le i \le 12$. Fie μ_i polinomul minimal al lui ω^i peste GF(3). Exprimaţi μ_i în funcţie C_i şi polinomul generator al lui C în funcţie de μ_i. Demonstraţi că dim $C = 6$.

c) Construiţi GF(3^3), găsiţi un element primitiv α şi demonstraţi că putem lua $\omega = \alpha^2$.

d) Calculaţi polinomul generator al codului *C*.

e) Decodaţi cuvîntul (0, – 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0),

2. Construiţi un polinom generator şi o matrice de paritate pentru un cod binar BCH care corectează două erori, de lungime 15.

3. Găsiţi o matrice generatoare a unui cod RS tip [10, 6] peste $\mathbb{Z}_{11}$ şi calculaţi distanţa sa minimă.

4. Construiţi un cod BCH care să corecteze 3 erori, de lungime 31 şi dimensiune 16.

VIII. Aplicaţii: pachete de erori, Compact Disc, CRC

Ipoteza că erorile de comunicare apar la întîmplare (ca la canalul *qSC*) nu este îndeplinită în toate aplicaţiile practice: există canale la care erorile tind să apară una lîngă alta (*pachete de erori*, *burst errors*). Această situaţie este des întîlnită la stocarea pe bandă sau medii optice (CD, DVD), comunicaţii radio etc.

Ca întotdeauna, F este un corp finit fixat.

1 Definiţie. Un *pachet de erori de lungime b*, pe scurt *b-pachet de erori* (*burst of length b*, *b-burst*) este un vector u în F^n ale cărui coordonate nenule se găsesc pe b poziţii consecutive, din care prima şi ultima sînt nenule. Codul $C \subseteq F^n$ se numeşte *corector de b-pachete de erori* dacă nu există cuvinte cod distincte $c_1, c_2 \in C$ şi pachete de erori u_1, u_2 de lungimi cel mult b astfel încît $c_1 + u_1 = c_2 + u_2$. Pentru un cod liniar C, aceasta e echivalent cu:

Pentru orice pachet de erori u de lungime $\leq b$, cosetul $u + C$ nu conţine alt pachet de erori de lungime $\leq b$.

Avertizare: a nu se face confuzie între *lungimea unui pachet de erori u* definită ca mai sus (care este *b*) şi *lungimea lui u* văzut ca *vector* în F^n (care e, desigur, *n*).

2 Teoremă. *Fie C un cod liniar corector de b-pachete de erori tip* [*n, k, d*]. *Atunci:*

a) C nu conţine pachete de erori de lungime $\leq 2b$.

b) (Inegalitatea Reiger, Reiger Bound) $n - k \geq 2b$.

Demonstraţie. a) Presupunem că $c \in C$ este un pachet de erori de lungime $\leq 2b$ ale cărui componente nenule sînt în poziţiile de la i pînă la $i + t$ (cu $t \leq 2b - 1$): $c = 0\ldots0c_i\ldots c_{i+t}0\ldots0$, unde $c_j \in F$, $c_i \neq 0$, $c_{i+t} \neq 0$.

Fie $u = 0\ldots c_i\ldots c_{i+b-1}0\ldots0$, $v = 0\ldots0c_{i+b}\ldots c_{i+t}0\ldots0$; deci $c = u + v$. Atunci $0 + v = c + (-u)$, cu $0, c \in C$ şi $-u, v$ pachete de erori de lungime $\leq b$, contradicţie.

b) Afirmăm că C conţine pachete de erori de lungime $\leq n - k + 1$. (Din prima parte, aceasta va implica $n - k + 1 > 2b \Leftrightarrow n - k \geq 2b$.) Să demonstrăm afirmaţia. Fie H o matrice de paritate a lui C şi fie $h_1, \ldots, h_n$ coloanele sale. Avem $h_i \in F^{n-k}$, deci $h_1, \ldots, h_{n-k+1}$ sînt liniar dependente: există $c_1, \ldots, c_{n-k+1} \in F$, nu toţi zero, astfel încît $c_1h_1 + \ldots + c_{n-k+1}h_{n-k+1} = 0$.

Atunci $c_1\ldots c_{n-k+1}0\ldots0 \in C$, şi este pachet de erori de lungime $\leq n - k + 1$. □

Tehnicile de *concatenare* şi *întreţesere* sînt folosite la proiectarea de coduri cu capacităţi bune de corectare de pachete de erori.

Dacă informaţia vine în cuvinte de m simboluri binare, acestea pot fi văzute ca elemente ale corpului cu 2^m elemente. Folosind un cod Reed-Solomon cu $q = 2^m$, un pachet de b erori în simbolurile binare devine un pachet de b/m erori în cuvintele cod, care poate fi corectat dacă $b/m < e$ (capacitatea de corectare a codului). Aceasta este un exemplu de *concatenare*.

3 Definiţie (Concatenarea a două coduri, *Concatenation of two codes*). Fie A un cod liniar $[n, k, d]$ peste $\mathbb{F}_q$. Atunci A este $\mathbb{F}_q$-spaţiu liniar de dimensiune k; deoarece corpul cu $Q := q^k$ elemente este tot $\mathbb{F}_q$-spaţiu liniar de dimensiune k, există un $\mathbb{F}_q$-*izomorfism* $\varphi : \mathbb{F}_Q \to A$. Fie B un cod liniar $[N, K, D]$ peste $\mathbb{F}_Q$. Un cuvînt oarecare al lui B este de forma $b = (b_1, \ldots, b_N)$, $b_i \in \mathbb{F}_Q$. Dacă înlocuim fiecare b_i cu imaginile lor în A prin φ (care sînt cuvinte de lungime n peste $\mathbb{F}_q$), obţinem un cuvînt de lungime Nn peste $\mathbb{F}_q$. Toate cuvintele obţinute astfel formează un nou cod C. Formal:

$$C = \{(\varphi(b_1), \ldots, \varphi(b_N)) \in \mathbb{F}_q^{Nn} \mid (b_1, \ldots, b_N) \in B\}$$

Codul C se numeşte cod *concatenat*, cu A *codul interior* (the *inner code*) şi B *codul exterior* (the *outer code*). A se observa că C depinde şi de alegerea $\mathbb{F}_q$-izomorfismului $\varphi : \mathbb{F}_Q \to A$.

4 Teoremă. *a) C este cod liniar peste $\mathbb{F}_q$, de lungime Nn, dimensiune Kk şi distanţă minimă cel puţin Dd.*

b) Păstrăm notaţiile din definiţia de mai sus şi punem $A = \mathbb{F}_q^n$ (*cod tip* $[n, n, 1]$ *peste* $\mathbb{F}_q$). *Atunci codul concatenat C* cu *cod interior A şi cod exterior B poate corecta pachete de erori de*

lungime $\le (e-1)n+1$, *unde* $e = \lfloor (D-1)/2 \rfloor$, *capacitatea de corectare a lui B*.

Demonstraţie. a) Lema următoare spune că B este un $\mathbb{F}_q$-spaţiu liniar de dimensiune Kk. Definim aplicaţia $\mathbb{F}_q$-linară $\Phi: \mathbb{F}_Q^N \to \mathbb{F}_q^{Nn}$, $\Phi(b_1, \ldots, b_N) = (\varphi(b_1), \ldots, \varphi(b_N))$, pentru orice $(b_1, \ldots, b_N) \in \mathbb{F}_Q^N$. Acesta este un $\mathbb{F}_q$-izomorfism. Deoarece C este imaginea lui B prin izomorfismul Φ, $\dim C = \dim B = Kk$ (ca $\mathbb{F}_q$-spaţii liniare).

Orice cuvînt nenul din C este de forma $(\varphi(b_1), \ldots, \varphi(b_N))$, unde $(b_1, \ldots, b_N)$ este un cuvînt nenul din B; deci are cel puţin D componente nenule. Deoarece orice $\varphi(b_i)$ nenul are pondere cel puţin d, $\mathrm{wt}(\varphi(b_1), \ldots, \varphi(b_N)) = \mathrm{wt}(\varphi(b_1)) + \ldots + \mathrm{wt}(\varphi(b_N)) \ge Dd$.

b) Fie $u \in \mathbb{F}_q^{Nn}$ un pachet de erori de lungime $\le an+1$. Atunci u coresponde prin Φ^{-1} unui vector $v \in \mathbb{F}_Q^N$. O examinare rapidă arată că v este pachet de erori de lungime $\le a+1$. Deci, dacă punem $a = e-1$, atunci v este pachet de erori de lungime $\le e$ şi poate fi corectat de B. □

5 Lemă. *Fie* $F \subseteq E$ *o extindere de corpuri,* $\dim_F E = k$. *Dacă* V *este un* E*-spaţiu vectorial de dimensiune* N, *atunci* E *este un* F*-spaţiu vectorial de dimensiune* kN.

Demonstraţie. Fie $v_1, \ldots, v_N$ o E-bază a lui V şi fie $e_1, \ldots, e_k$ o F-bază a lui E. Atunci $\{e_i v_j \mid 1 \le i \le k,\ 1 \le j \le N\}$ este o F-bază a lui V. □

6 Definiţie (Întreţesere, *Interleaving*). Fie C un cod liniar $[n, k, d]$ peste F care poate corecta pachete de erori de lungime $\le b$.

Definim codul tip [*nt, kt*] *I*(*C, t*) (*numit C întreţesut la adînimea t, C interleaved to depth t*) astfel: pentru orice $c_{ij} \in F$, $(1 \le i \le t, 1 \le j \le n)$*:*

$c_{11}c_{21}\ldots c_{t1}c_{12}c_{22}\ldots c_{t2}\ldots\ldots c_{1n}c_{2n}\ldots c_{tn} \in I(C, t) \Leftrightarrow c_{11}c_{12}\ldots c_{1n} \in C$, $c_{21}c_{22}\ldots c_{2n} \in C, \ldots, c_{t1}c_{t2}\ldots c_{tn} \in C$.

Aşadar, pentru a obţine un cuvînt cod de lungime *nt* în *I*(*C, t*), se aleg *t* cuvinte cod $c_1, c_2, \ldots, c_t \in C$, $c_i = c_{i1}c_{i2}\ldots c_{in}$ şi se formează matricea ale cărei *linii* sînt cele *t* cuvinte:

$$\begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ & & \vdots & \\ c_{t1} & c_{t2} & \ldots & c_{tn} \end{bmatrix}$$

Citind pe *coloane*, obţinem un cuvînt cod din *I*(*C, t*).

Întreţeserea la adîncime *t* multiplică de *t* ori capacitatea de corectare de pachete de erori:

7 Teoremă. *Dacă C este un cod liniar* [*n, k, d*]*, corector de b-pachete de erori, atunci I*(*C, t*) *este cod tip* [*nt, kt, d*]*, corector de bt-pachete de erori.*

Demonstraţie. Un pachet de erori de lungime *bt* sau mai mică $c_{11}c_{21}\ldots c_{t1}c_{12}c_{22}\ldots c_{t2}\ldots\ldots c_{1n}c_{2n}\ldots c_{tn}$ este distribuit în pachete de erori de lungime cel mult *b* în cele *t* linii ale matricei de mai sus. □

Codarea pentru compact disc

Schema de codare petru Compact Disc audio foloseşte două coduri Reed-Solomon scurtate şi două forme de întreţesere. Din Prop. **V.1**, ştim că scurtarea unui cod tip $[n, k, n-k+1]$ (cod

MDS) pe r coordonate produce un cod MDS tip $[n - r, k - r, n - k + 1]$.

Exerciţiu. Construiţi un cod Reed–Solomon de lungime 255 şi distanţă minimă 5 peste corpul cu 256 elemente. Explicaţi cum se obţin două coduri Reed–Solomon scurtate: C_2 de tip $[32, 28, 5]$ şi C_1 de tip $[28, 24, 5]$.

Descriem acum (urmînd în linii mari [9]) schema de codare şi decodare folosită pentru compact disc audio (CD audio), pentru a da o idee asupra dificultăţilor ce apar şi a tehnicilor folosite în implementările concrete ale codurilor corectoare de erori.

Descriere generală. Un CD este un disc gros de 1,2 mm, din policarbonat, cu diametrul de 120 mm. Un strat subţire de aluminiu (sau, mai rar, aur) este aplicat pe suprafaţă, ceea ce o face reflectorizantă. Metalul este protejat de un film de lac. Discul conţine o pista spirală de aproximativ 5 km (care începe dinspre centru), care e scanată optic de un laser cu AlGaAs de lungime de undă 780 nm (infraroşu apropiat), la o viteză liniară constantă de aprox. 1,2 m/s. Pe pistă sînt indentări (numite *pit-uri*) şi zone plate intre pit-uri, numite *lands*. Lăţimea unui pit este de aprox. 500 nm, adîncimea de 100 nm; lungimea variază între 850 nm şi 3500 nm. Pasul spiralei este 1,6 μm. Laserul este reflectat cu intensităţi diferite de pit-uri şi land-uri din cauza interferenţei. Prin măsurarea schimbărilor de intensitate cu o fotodiodă, datele pot fi citite de pe disc. Pit-urile sît mai apropiate de faţa etichetată a discului, ceea ce face ca defectele şi impurităţile de pe faţa care este scanată optic să fie neclare (nefocusate) în timpul citirii. Deci este mai probabilă deteriorarea CD-urilor prin partea etichetată a discului. Informaţia

conţinută de pit-uri şi land-uri este afectată de erori provenind de la particule de praf pe disc, bule de aer în învelişul de plastic, amprente, zgîrieturi etc. Aceste erori sînt cel mai adesea pachete de erori şi sînt corectate cu un sistem de codare şi decodare foarte eficient.

Codarea. Semnalul audio este eşantionat prin măsurare de 44,100 ori pe secundă. Fiecare eşantion este tradus într-un număr pe 16 biţi (deci amplitudinea semnalului va fi aproximată cu unul din cele $2^{16} = 65536$ nivele posibile); deoarece sunetul este stereo, sînt două eşantioane simultane (unul pentru fiecare canal). Astfel, o eşantionare produce 4 octeţi (bytes) (un *octet*/*byte* este un cuvînt de 8 biţi, adică un element al $\mathbb{F}_2^8$). Pentru fiecare secundă de sunet se generează aşadar $44\,100 \cdot 4 = 176\,400$ octeţi.

Pentru a coda octeţii se folosesc două coduri Reed–Solomon scurtate, C_1 şi C_2, şi două forme de întreţesere. Această schemă se numeşte *CIRC (cross-interleaved Reed–Solomon code, cod Reed-Solomon întreţesut-încrucişat)*. Scopul întreţeserii încrucişate, care este o variantă de întreţesere, este să „împrăştie" pachetele lungi de erori.

Şase eşantioane de 4 octeţi fiecare sînt grupate pentru a forma un *cadru (frame)*. Un cadru are deci 24 octeţi:

$$L_1R_1L_2R_2\ldots L_6R_6\,,$$

unde L_i ($\in \mathbb{F}_2^{16}$) semnifică cei *doi octeţi* corespunzători canalului stîng din eşantionul i al cadrului, iar R_i sînt cei doi octeţi corespunzători de la canalul drept.

Octeţii sînt rearanjaţi astfel: eşantioanele impare (L_1R_1, L_3R_3, L_5R_5) se grupează cu eşantioanele pare $L''_2R''_2$ $L''_4R''_4$ $L''_6R''_6$ *luate cu două cadre mai tîrziu*, în ordinea următoare:

$$L_1L_3L_5R_1R_3R_5L''_2L''_4L''_6\,R''_2R''_4R''_6$$

Se obţine un cuvînt mesaj de 24 octeţi. Eşantioanele care erau iniţial consecutive în timp sînt acum la două cadre distanţă. Aceasta va uşura „disimularea erorilor” (vezi partea de decodare).

Identificăm octeţii cu elemente ale corpului $\mathbb{F}_{256}$ *cu* $2^8 = 256$ *elemente*. Un codor sistematic pentru codul Reed Solomon scurtat tip $[28, 24, 5]_{256}$ C_1 (vezi **Exerciţiu** mai sus) codează mesajul de 24 octeţi într-un cuvînt de 28 octeţi, care e format din mesajul original la care se adaugă 4 octeţi „de paritate” notaţi P_1 şi P_2 (P_1 şi P_2 au cîte *doi* octeţi, ca şi L_i). Formăm cuvîntul cod de 28 octeţi prin plasarea P_1 şi P_2 la mijloc:

$$L_1L_3L_5R_1R_3R_5P_1P_2L''_2L''_4L''_6\,R''_2R''_4R''_6$$

Cuvintele cod de 28 octeţi din C_1 sînt întreţesute la o adîncime de 28 folosind o „întîrziere” de 4 cadre (*4-frame delay interleaving*). Mai precis, fie $c_1, \ldots, c_n, \ldots$ cuvintele cod din C_1 în ordinea în care au fost generate, şi fie $c_i = c_{i1}\ldots c_{i28} \in \mathbb{F}_{256}^{28}$. Formăm următoarea matrice M cu 28 linii şi un număr suficient de coloane ca să conţină toate cadrele:

1	$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{5,1}$	$c_{6,1}$	$c_{7,1}$	$c_{8,1}$	$c_{9,1}$	$c_{10,1}$	$c_{11,1}$	$c_{12,1}$	$c_{13,1}$	…	$c_{109,1}$	…
2	0	0	0	0	$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{5,2}$	$c_{6,2}$	$c_{7,2}$	$c_{8,2}$	$c_{9,2}$	…	$c_{105,2}$	…
3	0	0	0	0	0	0	0	0	$c_{1,3}$	$c_{2,3}$	$c_{3,3}$	$c_{4,3}$	$c_{5,3}$	…	$c_{101,3}$	…
4	0	0	0	0	0	0	0	0	0	0	0	0	$c_{1,4}$	…	$c_{97,4}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮	
28	0	0	0	0	0	0	0	0	0	0	0	0	0	…	$c_{1,28}$	…

Matricea M obţinută prin întreţesere cu întîrziere de 4 cadre (4-frame delay interleaving)

Linia i (foarte lungă) se obţine prin plasarea octeţilor i ai cuvintelor cod c_1, …, c_n, …, în această ordine; apoi se translatează la dreapta linia 2 cu 4 poziţii, linia 3 cu 8 poziţii, ..., linia 28 cu $27 \cdot 4 = 108$ poziţii; se completează cu zerouri unde e necesar. Cuvîntul cod c_i poate fi citit din această matrice prin parcurgerea în diagonală cu panta $-1/4$ începînd din poziţia i a liniei 1.

Am obţinut pînă acum o matrice M ale cărei coloane sînt elemente din $\mathbb{F}_{256}^{28}$. Folosim acum codul Reed–Solomon scurtat C_2, tip $[32, 28, 5]_{256}$, pentru a coda aceşti vectori de lungime 28 în cuvinte cod de lungime 32. Aceste cuvinte cod sînt iarăşi întreţesute: simbolurile de pe poziţii impare de la un cuvînt sînt grupate cu simbolurile de pe poziţii pare ale cuvîntului următor; se obţine un şir de segmente de 32 octeţi. Această întreţesere mai împrăştie eventualele pachetele de erori care mai există. La sfîrşitul fiecărui astfel de segment este adăugat un al 33-lea octet (de control şi display). Astfel, fiecare cadru de 6 eşantioane a produs în final 33 octeţi. O schemă detaliată a codării folosind C_1 şi C_2 poate fi găsită în [19].

Fiecare octet obţinut trebuie acum imprimat pe disc. O tranziţie land-pit sau pit-land semnifică un 1, în timp ce un pit sau land semnifică un şir de 0. Lungimea pit-ului (land-ului) determină numărul de 0-uri, după regula că fiecare bit corespunde la 300 nm. De exemplu, un pit de lungime 1500 nm urmat de un land de lungime 900 nm corespunde şirului 10000100: pit-ul de 1500 nm semnifică $1500/300 = 5$ biţi, din care primul e 1, adică 10000; landul de 900 nm semnifică şirul de trei biţi 100.

Din motive tehnice, fiecare land sau pit trebuie să fie între 900 şi 3300 nm, adică fiecare pereche de 1 trebuie să fie separată de cel

puţin două 0-uri şi cel mult zece 0-uri. Cel mai scurt pit (land) reprezintă 3 biţi (100), şi cel mai lung 11 biţi (10000000000). Deci, cei 256 octeţi posibili trebuie convertiţi în şiruri de biţi care satisfac această condiţie. Se poate arăta că cea mai mică lungime *l*, astfel încît există cel puţin 256 cuvinte binare de lungime *l* cu proprietatea că fiecare 1 este separat de cel puţin două 0-uri şi cel mult zece 0-uri, este 14. De fapt, sînt 267 cuvinte de lungime 14 cu această proprietate; 11 din acestea nu sînt folosite. Această conversie de la octeţi la cuvinte de lungime 14 se numeşte EFM (*eight-to-fourteen modulation, modulaţie opt la paisprezece*), şi se realizează folosind un tabel de conversie. Mai este o problemă: două cuvinte succesive de 14 biţi pot să nu satisfacă condiţia de separare de mai sus. Din acest motiv, trei biţi suplimentari (*merge bits*, *biţi de fuzionare*) sînt adăugaţi la sfîrşitul fiecărui cuvînt de 14-biţi pentru a obţine şiruri care satisfac condiţia. De exemplu, şirurile 10010000000100 şi 00000000010001, scrise succesiv, ar produce un şir de 11 zerouri; dacă adăugăm 001 după primul şir, obţinem 10010000000100001000000000010001, care satisface condiţia.

Astfel, cadrul iniţial de 6 eşantioane corespunde la 33 octeţi; fiecare octet e convertit în 17 biţi. La fiecare aceşti 33·17 biţi, se adaugă 24 biţi plus trei biţi de fuzionare; astfel, fiecare cadru de 6 eşantioane produce 588 biţi.

Decodarea şi corectarea de erori. Mai întîi se elimină biţii de sincronizare, control şi display şi de fuzionare. Se realizează apoi conversia din formatul EFM în octeţi folosind o tabelă; acum informaţia este un şir de octeţi. Apoi se rearanjează octeţii în ordinea normală. Şirul e împărţit în segmente de 32 octeţi. Fiecare

din aceste segmente de 32 octeţi conţine octeţii de pe poziţii impare dintr-un cuvînt cod (cu posibile erori) şi octeţii de pe poziţiile pare ale următorului cuvînt cod. Octeţii sînt regrupaţi în poziţiile iniţiale şi sînt furnizaţi decodorului pentru C_2. Dacă un pachet scurt de erori a apărut pe disc, pachetul va fi divizat în pachete mai mici prin această regrupare.

Decodarea cu C_2. Deoarece C_2 este cod tip [32, 28, 5] peste $\mathbb{F}_{256}$, poate corecta două erori la nivel de octeţi. Totuşi, este folosit doar pentru a *corecta o eroare* şi pentru a *detecta prezenţa de erori multiple*. Dacă s-a produs o singură eroare, C_2 poate corecta eroarea prin căutarea unui cuvînt cod în sfera de rază 1 centrată în cuvîntul recepţionat. Dacă găseşte unul, eroarea este corectată; dacă nu, înseamnă că două sau trei erori au avut loc şi C_2 a detectat aceste erori (dar nu va fi folosit pentru corectarea lor).

E important să estimăm probabilitatea ca C_2 să nu detecteze 4 sau mai multe erori cînd e folosit să corecteze 1 eroare. O astfel de situaţie apare dacă erorile se produc la un cuvînt cod încît vectorul ce rezultă se află într-o sferă de rază 1 centrată în alt cuvînt cod. Presupunînd că toţi vectorii sînt la fel de probabili, probabilitatea ca această situaţie să apară este aproximativ egală cu raportul dintre numărul de vectori din sferele de rază 1 centrate în cuvinte cod şi numărul total de vectori din $\mathbb{F}_{256}^{32}$:

$$\frac{256^{28}\cdot\left[1+32(256-1)\right]}{256^{32}}=\frac{8161}{256^{4}}\approx 1.9\cdot 10^{-6}$$

Pe de altă parte, dacă am utiliza C_2 la capacitatea maximă de corectare de erori (toate erorile duble), probabilitatea de eşec în detectarea a trei sau mai multe erori este raportul dintre numărul de

vectori din sferele de rază 2 centrate în cuvinte cod şi numărul total de vectori din $\mathbb{F}_{256}^{32}$:

$$\frac{256^{28}\cdot\left[1+32(256-1)+\binom{32}{2}(256-1)^2\right]}{256^{32}}=\frac{32260561}{256^4}\approx 0.0756$$

Această probabilitate de eşec (cam de 4000 ori mai mare decît precedenta) este motivul pentru care C_2 nu este folosit la capacitatea maximă de corectare.

Decodare cu C_1. Dacă decodorul pentru C_2 găseşte cel mult o eroare într-un şir de 32 octeţi, eroarea eventuală este corectată şi mesajul de 28 octeţi este extras şi trimis mai departe. Dacă C_2 detectează cel puţin două erori, trimite un cuvînt de 28 octeţi cu toate componentele marcate ca „ştersături”. Aceste blocuri de 28 octeţi corespund coloanelor matricei M, cu posibile ştersături. Diagonalele de pantă $-1/4$ sînt transmise ca vectori de 28 octeţi decodorului pentru C_1. Se observă că blocurile de 28 octeţi cu ştersături sînt împrăştiate prin acest proces la blocuri diferite ale codului exterior C_2.

O schemă de decodare foloseşte C_1 doar la corectarea ştersăturilor. Din teorema **I. 12**, C_1 poate corecta pînă la patru ştersături. Datorită întreţeserii, un bloc de 28 octeţi marcat ca ştersătură (de codul interior) corespunde la 28 blocuri (cu cîte un singur octet ştersătură) din codul exterior. Întreţeserea cu întîrziere de 4 cadre, combinată cu capacitatea de corectare a 4 ştersături a lui C_1, permit corectarea unui pachet de erori care afectează 16 şiruri consecutive de 588 biţi fiecare. Un astfel de pachet de erori ocupă aproximativ 2.8 mm în lungul pistei discului.

O altă schemă de decodare foloseşte C_1 la corectarea unei erori (care a scăpat eventual detectării lui C_2) şi a două ştersături. (cf. Teorema **I. 12**)

Interpolare şi disimularea erorilor. Eşantioanele care nu pot fi corectate de schema de mai sus şi sînt detectate ca erori sînt marcate ca ştersături. Deoarece eşantioanele consecutive sînt separate de două cadre înainte de codare, la finalul decodării, cînd aceste eşantioane sînt readuse în ordinea iniţială, este probabil ca eşantioanele vecine să fie corecte sau să fi fost corectate. În acest caz, eşantionul marcat „şters" este aproximat prin interpolare liniară folosind eşantioanele vecine. Testele au arătat că acest proces este practic indedectabil la audiţie. Dacă eşantioanele vecine nu sînt corecte, se foloseşte „muting". Cu 32 eşantioane înaintea pachetului de erori, eşantioanele corecte sînt treptat micşorate pîna la apariţia pachetului de erori, care e înlocuit de eşantioane de valoare zero, iar următoarele 32 eşantioane corecte sînt treptat readuse la valoarea reală.

Detectare de erori cu CRC (Cyclic Redundancy Check)

Matricea generatoare a unui cod ciclic dată la **VI.6** nu este în formă standard, deci codarea corespunzătoare nu e sistematică. Descriem acum o codare sistematică pentru coduri ciclice, care are importante aplicaţii. Codurile *binare* ciclice sînt potrivite pentru detectarea de erori, iar implementarea circuitelor de codare şi de detectare de erori este eficientă (folosind *linear feedback shift registers*).

Fie C un cod ciclic tip $[n, k, d]$ peste corpul F cu q elemente, g polinomul său generator, $\operatorname{grad} g = n - k$. Deoarece $\dim C = k$,

polinomul mesaj este de grad cel mult $k-1$. Folosind teorema împărţirii cu rest, putem scrie

$$X^{n-k}m = gq + r, \text{ cu } q,\ r \in F[X], \text{ grad } r < n-k \text{ sau } r = 0.$$

Astfel, $X^{n-k}m - r = gq \in C$. Dacă codăm m ca $c = X^{n-k}m - r$, aceasta este o codare sistematică, deoarece coeficienţii lui m apar drept coeficienţii lui X^{n-k}, X^{n-k+1}, …, X^{n-1} în c. Practic, la cuvîntul mesaj (coeficienţii lui m) se adaugă la sfîrşit simbolurile de control (coeficienţii lui $-r$).

În aplicaţii, mesajul m este *binar* şi nu are lungimea fixată k; biţii de control sînt adăugaţi la mesaje de lungime $\le k$. Aceşti biţi de sînt cunoscuţi sub numele de CRC (*Cyclic Redundancy Check*, *Verificare Redundantă Ciclică*) şi se folosesc pentru *detectarea erorilor*. Verificarea de eroare se realizează prin testarea dacă cuvîntul recepţionat (văzut ca polinom) este divizibil cu g. O eroare poate trece nedetectată dacă şi numai dacă un vector eroare e (un polinom de grad mai mic ca n) este adunat cuvîntului cod c de mai sus şi $c + e$ este divizibil cu g. Deoarece $g \mid c$, aceasta are loc dacă şi numai dacă $g \mid e$.

8 Propoziţie. *Un cod ciclic C tip* $[n, k, d]$ *de generator g poate detecta toate pachetele de erori de lungime* $\le n - k$.

Demonstraţie. Fie r un pachet de erori de lungime $\le n - k$ şi să presupunem prin reducere la absurd că r nu este detectat de C, adică $g \mid r$. Fie j cel mai mare număr natural astfel încît $X^j \mid r$. Cum r este pachet de erori de lungime $\le n - k$, aceasta înseamnă că $r = X^j s$, cu grad $s < n - k$. Dar g divide $X^n - 1$, deci g nu este divizibil prin X, adică $(X^j, g) = 1$. Cum $g \mid X^j s$, rezultă că $g \mid s$, imposibil căci grad $g >$ grad s. □

Rezultatul următor estimează proporţia de pachete de erori (mai lungi decît $n - k$) care nu sînt detectate de C:

9 Teoremă. *Din totalul de pachete de erori de lungime $b > n - k$, proporţia celor care nu sînt detectate de un cod ciclic C tip $[n, k, d]$ de generator g este: $q^{-(n-k-1)}/(q-1)$ (dacă $b = n - k + 1$), respectiv $q^{-(n-k)}$ (dacă $b > n - k + 1$).*

Demonstraţie. Fie r un pachet de erori de lungime b care începe în simbolul i: $r = X^i s$, unde grad $s = b - 1$. Numărăm cîte asemenea polinoame s există: sînt $q - 1$ posibilităţi pentru primul coeficient (orice element nenul al lui F), $q - 1$ pentru ultimul, şi q posibilităţi pentru coeficienţii dintre aceştia, deci avem $(q-1)^2 q^{b-2}$ polinoame s.

Eroarea r nu este detectată dacă şi numai dacă $g|s$, adică $s = gh$, cu $h \in K[X]$. Dar grad $g = n - k$, deci grad $h = b - 1 - (n - k)$. Dacă $b - 1 = n - k$, atunci h e o constantă nenulă ($q - 1$ posibilităţi). Astfel, raportul dintre numărul de pachete nedetectate şi numărul total de pachete este

$$(q-1)/((q-1)^2 q^{b-2}) = q^{-(n-k-1)}/(q-1).$$

Dacă $b - 1 > n - k$, sînt $q - 1$ alegeri posibile pentru primul coeficient al lui h, $q - 1$ alegeri pentru ultimul coeficient şi cîte q alegeri pentru fiecare ceficient intermediar. În total rezultă $(q-1)^2 q^{b-1-(n-k)-1}$ polinoame h. Raportul în acest caz este deci $q^{-(n-k)}$. □

Această teoremă afirmă că probabilitatea de eşec în detectarea de erori este proporţională cu $q^{-(n-k)}$ (independentă de lungimea codului sau de cît de zgomotos e canalul). Deci, *probabilitatea de*

apariţie de erori nedetectate e determinată de $n-k$, numărul de simboluri de control.

10 Exerciţiu. Fie $g \in \mathbb{F}_q[X]$ un polinom ireductibil de grad m. Atunci:

a) $g \mid X^n - 1$, unde $n = q^m - 1$ (*Ind:* g are toate rădăcinile în corpul cu q^m elemente).

b) Dacă g este polinomul minimal peste $\mathbb{F}_q$ al unui element primitiv al corpului cu q^m elemente (un astfel de g se numeşte *polinom primitiv*), atunci g este de grad m şi numărul natural min $\{n \in \mathbb{N} \mid g \text{ divide } X^n - 1\}$ (numit *ordinul lui g*) este $q^m - 1$.

c) Dacă α este o rădăcină a lui g într-o extindere E a lui $\mathbb{F}_q$, atunci ordinul lui g este ordinul lui α (în sens de ordin al lui α în grupul multiplicativ E^*). Dacă g are ordin $q^m - 1$, atunci g este primitiv.

d) Pentru orice polinom $h \in \mathbb{F}_q[X]$ astfel încît $(X, h) = 1$, există n astfel încît g divide $X^n - 1$ (cel mai mic număr natural n cu această proprietate se numeşte iarăşi *ordinul* lui h).

Presupunem de acum înainte că F este corpul cu 2 elemente $\mathbb{F}_2$ (cazul *binar*). Din Prop. **8** deducem că orice cod C ciclic tip $[n, k, d]$ cu $k < n$ *detectează o eroare*. Considerăm o *eroare dublă*, în poziţiile $i > j$, deci polinomul eroare este

$$e = X^i + X^j = X^j(X^{i-j} + 1).$$

Cum $(X^j, g) = 1$, e nu este detectat $\Leftrightarrow g \mid e \Leftrightarrow g \mid X^{i-j} + 1$. Dacă lungimea mesajului e mai mică decît ordinul lui g (care este $2^m - 1$ dacă g este primitiv), atunci $X^{i-j} + 1$ nu poate fi divizibil cu g, deci orice eroare dublă este detectată.

Polinoamele generatoare g folosite de obicei în practică pentru CRC sînt de forma $(X+1)h$ unde h este un polinom *primitiv* binar de grad $m-1$. Această alegere are la bază faptul că un cod binar ciclic cu polinomul generator g divizibil cu $X-1$ are toate cuvintele cod de pondere pară (demonstraţi!). Aceasta asigură detectarea tuturor vectorilor eroare care au pondere impară (şi că distanţa minimă a codului este cel puţin 4). Deci orice cod de acest tip are distanţa minimă cel puţin 4, detectează orice pachete de erori de lungime $\leq m$, iar probabilitatea de eşec in detectarea de erori în mesaje complet aleatoare este 2^{-m}.

Polinomul „CRC-5-USB" este $X^5 + X^2 + 1$. Acest polinom e folosit în standardul USB pentru a proteja „pachete token" de 11 biţi.

Polinoame CRC standard pentru $m = 16$:

$$\text{CRC-16} : g = X^{16} + X^{15} + X^2 + 1$$

$$\text{CRC-CCITT} : g = X^{16} + X^{12} + X^5 + 1,$$

Pentru $m = 32$, polinomul CRC standard IEEE 802.3 este

$$g = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

11 Exerciţiu. a) Folosind polinomul CRC-5-USB găsiţi CRC pentru cuvîntul mesaj 10110011101.

b) Presupunem că 1011 0011 101 00001 este un cuvînt de lungime 11 concatenat cu CRC-ul său în raport cu polinomul CRC-5 USB. Verificaţi dacă sînt erori.

Aceste polinoame (şi altele folosite în variate standarde) adesea nu sînt cea mai bună alegere. Mai mulţi autori au contribuit la

efectuarea unei căutări exhaustive în spaţiul polinoamelor binare de grad pînă la 32, găsind exemple de polinoame care se comportă mai bine (au distanţă minimă mai mare pentru o lungime de mesaj dată) decît polinoamele în uz în anumite protocoale. Vezi [5], [10].

Index

D

E

F

G

I

L

M

N

O

P

R

S

T

Bibliografie

1. Bertsekas, D.P, Gallager, R.G, *Data networks*, Prentice Hall, 1987.
2. Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A.,Wassermann, A., *Error-Correcting Linear Codes. Classification by Isometry and Applications*, Springer Verlag, 2006.
3. Castagnoli, G., Braeuer, S. & Herrman, M., *Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits*, IEEE Trans. on Communications, Vol. 41, No. 6, June 1993.
4. *CD-Recordable FAQ*, http://www.cdrfaq.org/
5. Fujiwara, T., Kasami, T., Kitai, A. & Lin, S., „On the undetected error probability for shortened Hamming codes", IEEE Trans. on Communications, vol. 33, no. 6, 1985, pp.570-573.
6. Gherghe, C., Popescu, D., *Criptografie. Coduri. Algoritmi,* Editura Universităţii din Bucureşti, 2005.
7. Grassl, M.*, „Bounds on the minimum distance of linear codes and quantum codes."* Online available at *http://www.codetables.de. Accessed on 2013-09-10.*

8. Hall, J.I, *Notes on Coding Theory*, http://www.mth.msu.edu/~jhall/classes/codenotes/coding-notes.html
9. Huffman, W., Pless, V., *Fundamentals of Error-Correcting Codes*, Cambridge University Press 2003.
10. Koopman, Philip, *32-Bit Cyclic Redundancy Codes for Internet Applications*. The International Conference on Dependable Systems and Networks: 459–468 (July 2002), http://www.ece.cmu.edu/~koopman/networks/dsn02/dsn02_koopman.pdf
11. Lidl, R. and Niederreiter, H., *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.
12. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.
13. Ling, S., Xing, C., *Coding Theory. A First Course, Cambridge University Press,* 2004.
14. MacWilliams, F. J., and Sloane, N. J. A., *The Theory of Error-Correcting Codes,* vol. 1 and 2, North Holland, 1977.
15. Moreira, J. C., Farrell, P.G, *Essentials of Error-Control Coding*, John Wiley & Sons Ltd, 2006.
16. Shannon, C.E., *A Mathematical Theory of Communication*, Bell Systems Technical Journal 27, 623-656 (1948).
17. Shannon, C.E., *Communications in the presence of noise*, Proceedings of the IEEE, 37, 10-21 (1949).
18. Shannon, C.E., *Communication Theory of Secrecy Systems*, (initially "A Mathematical Theory of Cryptography", Memorandum MM 45-110-02, Sept. 1, 1945, Bell Laboratories, confidential report), declassified in *Bell System Technical*

Journal, vol. 28(**4**), page 656–715, 1949. (http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf)

19. Standard ECMA-130, *Data Interchange on Read-only 120 mm Optical Data Disks (CD-ROM)* 2nd edition (June 1996), http://www.ecma-international.org/publications/standards/Ecma-130.htm
20. van Tilborg, H.C.A., *Finite Fields and Error Correcting Codes*, in Handbook of Algebra, vol I, Elsevier Science 1996, p. 397-422.