UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

CODIS ALGEBRAICS

Autor: Axel Gómez Paredes

Director: Dr. Carlos D'Andrea
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 13 de juny de 2022

Resum

En el procés de transmissió d'informació es produeixen errors degut als canals pel quals viatja el missatge. En aquest treball presentem mitjans per poder detectar els errors produïts i corregir-los per tal de garantir la correcta transmissió de la informació. En aquest context, presentarem el funcionament dels codis lineals donant tant eines de codificació com de descodificació. El primer procés de descodificació que treballarem serà el conegut com el del "síndrome" i, a continuació, donarem la teoria sobre codis lineals, centrant-nos en els codis de Hamming i els seus beneficis referents a la detecció i correcció d'errors comesos.

Una segona part del treball estarà focalitzada en els codis cíclics, subconjunt dels codis lineals, que aporten més eficiència en el procés de codificació. Entre aquests trobem els codis de Reed-Solomon del qual extraurem una nova eina per a la seva descodificació. A més, veurem com la idea de codis cíclics es pot estendre en anells de polinomis en diverses variables.

Abstract

Errors occur during the process of information transmission due to the channels through which the information travels. In this project we present methods through which to detect the given errors and correct them so as to guarantee the correct transmission of information. In this context, we will present the functioning of the lineal codes giving the codification tools as well as the decodification ones. The first decodification process we will work on is the one known as that of the "syndrome", and after that we will present the theory about lineal codes, focussing the Hamming codes and their benefits when it comes to the detection and correction of the commited errors.

The second part of the project will focus on cyclic codes, a subset of lineal codes that bring more efficiency to the codification process. Among these we can find the Reed-Solomon codes, and at the same time we will give a new tool for their decodification. Moreover, we will observe that the cyclic codes idea can be extended to polynomial rings in multiple variables.

.

2020 Mathematics Subject Classification. 11T71, 94B05, 94B15, 94B35

Agraïments

Sense l'ajuda del doctor Carlos D'Andrea, la seva paciència i constància, aquesta feina hauria estat més feixuga. Els seus consells van ser sempre útils quan no sortien del meu pensament les idees per escriure allò que avui he aconseguit. Gràcies per les teves orientacions.

Els meus amics i companys de viatge, avui culminen aquesta meravellosa aventura i no puc deixar de recordar quantes tardes i hores de feina ens hem ajuntat al llarg de la nostra formació. Avui ens toca tancar un capítol meravellós en aquesta història de vida i no puc deixar d'agrair-los pel seu suport i perseverança, en estar a les hores més difícils, per compartir hores d'estudi. Gràcies per ser-hi sempre.

Per últim, m'agradaria agrair el recolzament desinteressat que he rebut a casa. Aquest treball és fruit del vostre amor. Gràcies.

Índex

1 Introducció

El nostre objecte d'estudi són els diferents mètodes per enviar de manera eficient i precisa informació d'un lloc a un altre. Una idea intuïtiva del procés de comunicació ve donada pel següent diagrama:

$$\text{Emissor} \xrightarrow{\text{missatge}} \text{Codificador} \xrightarrow{\text{paraula codi}} \text{canal de comunicació} \xrightarrow[\text{soroll}]{\text{paraula codi amb errors}}$$

$$\longrightarrow \text{descodificador} \xrightarrow{\text{missatge descodificiat}} \text{Receptor}$$

on el codificador i el descodificador són aparells que permeten enviar el nostre missatge a través del canal de comunicació. Freqüentment trobarem interferències en el canal de comunicació del missatge i, per tant, caldrà considerar els possibles errors per tal de solucionar-los. Dissenyar codis capaços de detectar i corregir errors així com trobar formes efectives de codificar i descodificar és un dels principals objectius de la teoria de codis.

Per poder treballar sobre els missatges a enviar caldrà definir conjunts finits que prenguin el paper dels abecedaris i, per comoditat, prendrem com a conjunt de lletres els elements dels cossos finits de q elements, que denotarem per $\mathbb{F}_q$. Per tant, els abecedaris seran els cossos finits i les paraules a enviar, vectors de dimensió k sobre el cos. A causa de l'ús del llenguatge binari dels aparells electrònics, prendrem com a cos el $\{0, 1\}$.

Centrarem l'estudi en un tipus concret de codis: aquells en els quals la informació a codificar està formada per tires o paraules de llargada k i en el qual tots els missatges codificats estan formats per tires anomenades paraules del codi de llargada de bloc fixa n prenent símbols del mateix alfabet. Per poder detectar i corregir errors caldrà incloure certa redundància i, per tant, $k < n$.

Anomenarem procés de codificació d'una tira del missatge a una aplicació injectiva $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$. Definim el conjunt de paraules del codis, o simplement codi, com $C = E(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$. Per altra banda, definim el procés de descodificació com l'aplicació $D : \mathbb{F}_q^n \to \mathbb{F}_q^k$ verificant $D \circ E = Id$ a $\mathbb{F}_q^k$. Gràcies als possibles errors produïts en la transmissió del missatge, la funció D haurà de retornar el missatge corregint aquest i, per tant, a la pràctica, no serà tan simple com trobar la inversa de la funció de codificació.

Treballarem els codis lineals, aquells on les paraules del codi formen un subespai vectorial de $\mathbb{F}_q^n$. Aquests codis presenten l'avantatge que es poden codificar utilitzant funcions de codificació que correspondran a aplicacions lineals entre $\mathbb{F}_q^k$ i $\mathbb{F}_q^n$. Al tractar-se d'aplicacions lineals entre espais vectorials, podrem utilitzar les eines d'àlgebra lineal per definir i estudiar les propietats d'aquests codis. Anomenarem matriu generadora d'un codi a la matriu de l'aplicació lineal codificadora.

Dotarem d'una estructura algebraica addicional als codis lineals per formar una família de codis coneguda com codis cíclics. S'afegirà la propietat de ser tancats per a permutacions cícliques dels elements del codi. D'aquesta manera, veurem que els codis cíclics es poden tractar com a ideals i, per tant, podrem aprofitar aquesta caracterització per donar representacions i algoritmes de codificació i descodificació concrets. Com a exemple d'aquesta família estudiarem els codis de Reed-Solomon i donarem un algoritme per descodificar-los.

Com a base per realitzar aquest treball he seguit principalment els llibres [CLO13] i [CLO05].

2 Preliminars

Per tal de desenvolupar la teoria de codis presentada en aquest treball ens caldrà parlar prèviament de cossos finits, submòduls d'anells de polinomis i bases de Gröebner d'aquests. Desenvoluparem més extensament l'apartat de cossos finits donat que formen la base sobre la que construïm els "abecedaris"per poder enviar els missatges.

2.1 Cossos finits

Definició 2.1. *Sigui R un conjunt no buit i dues operacions binàries anomenades suma i producte que denotarem com $+$ i $\cdot$ respectivament. Direm que la terna $(R, +, \cdot)$ és un anell si es verifiquen les següents propietats:*

- *$(R, +)$ verifica que, $\forall\, a, b, c \in R$:*
  1. *$a + (b + c) = (a + b) + c$;*
  2. *$a + 0 = 0 + a = a$;*
  3. *$a + (-a) = (-a) + a = 0$;*
  4. *$a + b = b + a$;*
- *(Propietat associativa) $\forall\, a, b, c \in R$,*

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

- *(Propietat distributiva) $\forall\, a, b, c \in R$,*

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

Notació 1. *És freqüent identificar la terna $(R, +, \cdot)$ amb el conjunt R.*

Definició 2.2. *Sigui R un anell, direm que $a \in R$ és invertible si $\exists\, b \in R$ tal que $a \cdot b = b \cdot a = 1$.*

Definició 2.3. *Direm que un anell k és un cos si $0 \neq 1$ i tot element no nul és invertible*

Definició 2.4. *Donat R un anell, definim l'anell de polinomis sobre R:*

$$R[x_1, \ldots, x_n] := \{ \sum_{\alpha_1, \ldots, \alpha_n \in \mathbb{N}} a_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid a_{\alpha_1, \ldots, \alpha_n} \in R \text{ i el sumatori sigui finit} \}$$

Definició 2.5. *Direm que un cos és finit si té un nombre finit d'elements. Denotarem el cos finit amb q elements com $\mathbb{F}_q$.*

Definició 2.6. *Sigui R un anell, direm que un subconjunt $I \subseteq R$ és un ideal si verifica:*

- *$\forall\, a, b \in I$, $a - b \in R$;*
- *$\forall\, c \in R$ i $\forall\, a \in I$, $c \cdot a \in I$;*

Definició 2.7. *Diem que un ideal J és maximal si els únics ideals que contenen J són el propi J i el total.*

Teorema 2.8 (Teorema fonamental dels homomorfismes d'anells)**.** *(Capítol 2 secció 7 de [Jac12]). Siguin R i R' dos anells, $\phi : R \longmapsto R'$ un homomorfisme, aleshores $ker(\phi)$ és un ideal de R i existeix un únic morfisme $\overline{\phi} : R/ker(\phi) \longmapsto R'$ tal que $\phi = \overline{\phi}\pi$, on π és la projecció natural de R en $R/ker(\phi)$ i $\overline{\phi}$ és injectiva.*

Corołari 2.9. *Donats R i R' dos anells i $\phi : R \longmapsto R'$ un homomorfisme, aleshores $R/ker(\phi) \cong Im(\phi)$.*

Lema 2.10. *Sigui k un cos qualsevol, aleshores l'anell de polinomis $k[x]$ és domini d'ideals principals.*

Demostració. Sigui $I \subseteq k[x]$ ideal no nul. Sigui $q(x) \in I$ un element no nul de grau mínim. Veurem que $I = (q(x))$. Sigui $p(x) \in I$. Com $q(x)$ és de grau mínim, podem realitzar la divisió euclidiana de $p(x)$ respecte $q(x)$: $p(x) = c(x)q(x) + r(x)$ amb $gr(r(x)) < gr(q(x))$. Per tant, reorganitzant tenim $r(x) = p(x) - c(x)q(x) \in I$, però $gr(r(x)) < gr(q(x))$, amb el que cal que $r(x) = 0$ i $p(x) = c(x)q(x)$ i, per tant, I és ideal principal. □

Lema 2.11. *(Teorema 6.6.15 de [Tra17]). Tot domini d'ideals principals és domini de factorització única.*

Corołari 2.12. *$k[x]$ és domini de factorització única.*

Lema 2.13. *(Proposicions 1.1 de [AM89]). Sigui R anell. Aleshores R és cos $\iff$ els únics ideals són els trivials, és a dir, 0 i R*

Lema 2.14. *(Proposicions 1.1 i 1.2 de [AM89]). Tenim la correspondència bijectiva entre els conjunts:*

$$\{\textit{ideals que contenen } I\} \longleftrightarrow \{\textit{ideals de } {}^{A}\!/_{I}\}$$

Com a conseqüència immediata d'aquests dos lemes obtenim:

Lema 2.15. *Sigui R anell, I ideal maximal de R. Aleshores ${}^{R}\!/_{I}$ és un cos.*

Demostració. Com I és maximal, els únics ideals que el contenen són els trivials i, per tant, pel lema 2.13, els únics ideals de ${}^{R}\!/_{I}$ són també els trivials i, pel lema 2.14, tenim que el quocient és, en definitiva, un cos. □

Teorema 2.16. *(Teorema 2.6 de [Jac12]). Siguin R i R' anells, $\pi : R \mapsto R'$ epimorfisme. Sigui H un conjunt de R tal que $ker(\pi) \subseteq H$. Aleshores H és ideal $\iff$ $\pi(H)$ és ideal. A més, si I és un ideal que conté el $ker(\pi)$, tenim:*

$${}^{R}\!/_{I} \cong {}^{R'}\!/_{\pi(I)}$$

Proposició 2.17. *Sigui k un cos, $g \in k[x]$ un polinomi irreductible, aleshores $\langle g \rangle \subseteq k[x]$ és un ideal maximal.*

Demostració. Suposem que $\langle g \rangle$ no és maximal. Aleshores $\exists I = \langle f \rangle$ ideal tal que $\langle g \rangle \subsetneq \langle f \rangle$. Aleshores, $g \in \langle f \rangle \implies \exists\, h \in k[x]$ tal que $g = hf$. Però g és irreductible, per tant, cal que h o f siguin unitats. En el primer cas, $h = c \in k \implies \langle f \rangle = \langle g \rangle$. En l'altre cas, $f = c \neq 0 \in k \implies \langle f \rangle = k$. □

Corołari 2.18. *Sigui k un cos, $g \in k[x]$ un polinomi irreductible, aleshores $k[x]/\langle g \rangle$ és un cos.*

Demostració. Com $\langle g \rangle$ és maximal, pel lema 2.15, $k[x]/\langle g \rangle$ és cos. □

Observació 2.19. Sigui $\mathbb{F} = \mathbb{F}_p[x]/\langle g \rangle$ amb g irreductible. Els elements de $\mathbb{F}$ estan en correspondència un a un amb els residus de la divisió respecte g.

Notació 2. *Freqüentment utilitzarem α per representar la classe de x.*

Exemple 2.20. Sigui $g = x^4 + x + 1$ polinomi de $\mathbb{F}_2[x]$.

1. Veiem que g és irreductible a $\mathbb{F}_2[x]$ i busquem quin és el nombre d'elements de $\mathbb{F} = \mathbb{F}_2[x]/\langle g \rangle$.

   g irreductible: com $g(0) = 1 \neq 0$, $g(1) = 1+1+1 = 3 = 1 \neq 0$, g no té arrels a $\mathbb{F}_2$ i, per tant, no es pot escriure com un producte de polinomis de grau 1. Veiem que no es pot escriure tampoc com a producte de 2 polinomis irreductibles de grau 2. Els polinomis de grau dos a $\mathbb{F}$ són: $x^2 + x + 1$, x^2, $x^2 + 1$ i $x^2 + x$. Les úniques opcions possibles són aquells que contenen algun terme independent, és a dir, els següents productes:

   $(x^2 + 1) \cdot (x^2 + 1) = x^4 + 1 \neq g$

   $(x^2+1)\cdot(x^2+x+1) = (x^2+x+1)\cdot(x^2+1) = x^4+x^3+x^2+x^2+x+1 = x^4+x^3+x+1 \neq g$

   $(x^2 + x + 1) \cdot (x^2 + x + 1) = (x^2 + x + 1) \cdot (x^2 + 1) = x^4 + x^2 + 1 \neq g$

   Per tant, g és irreductible.

   Calculem ara el nombre d'elements. Sabem que estan en correspondència amb els residus dividint entre g. Les possibilitats són els polinomis $ax^3 + bx^2 + cx + d$ amb $a, b, c, d \in \mathbb{F}_2$. Per tant, tenim 2 possibilitats per a cada coeficient, és a dir, $2^4 = 16$ combinacions.

2. Prenent α per a la classe de x, computem les potències d'α.

   Sabem que tenim la identitat $g(\alpha) = 0 \implies \alpha^4 + \alpha + 1 = 0 \implies -\alpha^4 = \alpha + 1 \implies \alpha^4 = \alpha + 1$ on l'última implicació ve donada pel fet que a $\mathbb{F}_2$ es compleix la igualtat $1 = -1$.

α	α^2	α^3
$\alpha^4 = \alpha + 1$	$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^2 + \alpha$	$\alpha^6 = \alpha^5 \cdot \alpha = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha \cdot \alpha^6 = \alpha^3 + \alpha + 1$	$\alpha^8 = \alpha^7 \cdot \alpha = \alpha^2 + 1$	$\alpha^9 = \alpha^3 + \alpha$
$\alpha^{10} = \alpha^2 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha^+1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	$\alpha^{14} = \alpha^3 + 1$	$\alpha^{15} = 1$

3. Comprovem que $k = \{0, 1, \alpha^5, \alpha^{10}\}$ és un cos de 4 elements contingut a $\mathbb{F}$.

   Per veure que k és un subcòs cal comprovar 3 propietats:

   - $a, b \in k \implies a - b \in k$:

     Notem primer que $a - b = a + b$ a $\mathbb{F}$. El cas en què a o b sigui zero, clarament tenim el resultat buscat. Estudiem ara els altres tres casos. $\alpha^5+1 = \alpha^2+\alpha+1 = \alpha^{10} \in k$. $\alpha^5 + \alpha^{10} = \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = 1 \in k$. $\alpha^{10} + 1 = \alpha^2 + \alpha + 1 + 1 = \alpha^2 + \alpha = \alpha^5 \in k$.

- $a, b \in k \implies a \cdot b \in k$:
  Si a o b és 0 o 1, es verifica. Per altra banda, $\alpha^5 \cdot \alpha^{10} = \alpha^{15} = 1 \in k$.
- Tot element diferent del zero té invers. Donat que $\alpha^5 \cdot \alpha^{10} = \alpha^{15} = 1$, tenim que verifica la condició donada.

Més endavant demostrarem que $\mathbb{L}$ és subcòs de $\mathbb{F}$ si i només si $\mathbb{L}$ té 2^n elements amb n divisor de 4. Per tant, podrem afirmar, per exemple, que existeix un subcòs de $\mathbb{F}$ amb 8 elements.

Proposició 2.21. *Sigui $\mathbb{F}$ és un cos de p^n elements, aleshores $\mathbb{F}$ té un subcòs $k = \{0, 1, 2 \cdot 1, ..., (p-1) \cdot 1\}$ isomorf a $\mathbb{F}_p$.*

Demostració. $\mathbb{F}$ és cos i es verifica $p \cdot 1 = 1 + \cdots_p + 1 = 0$. Vegem $k \subseteq \mathbb{F}$ i k és cos.

Denotem per $r_p(l)$ al residu respecte la divisió de l entre p.

- Com $\mathbb{F}$ cos $\implies 1 \in \mathbb{F}, 1 + 1 \in \mathbb{F}, \cdots \implies k \subseteq \mathbb{F}$.
- Sigui $i \cdot 1, j \cdot 1 \in k$; $i \cdot 1 \cdot j \cdot 1 = i \cdot j \cdot 1 = r_p(i \cdot j) \cdot 1 \in k$.
- Sigui $i \cdot 1, j \cdot 1 \in k$; $i \cdot 1 + j \cdot 1 = (i + j) \cdot 1 = r_p(i + j) \cdot 1 \in k$.
- Sigui $i \cdot 1 \neq 0$. Volem veure que $\exists j \cdot 1$, $j \in \{1, \ldots, p-1\}$ tal que $i \cdot 1 \cdot j \cdot 1 = 1$. Com $\mathbb{F}_p$ és cos, $\exists j \in \{1, \ldots, p-1\}$ tal que $i \cdot j = 1$. D'aquesta forma, $i \cdot 1 \cdot j \cdot 1 = r_p(i \cdot j) \cdot 1 = 1$.

Veiem per últim que k i $\mathbb{F}_p$ són isomorfs. Definim el morfisme

$$\begin{array}{ccc} \mathbb{F}_p & \longrightarrow & k \\ i & \longmapsto & i \cdot 1 \end{array}$$

Aquesta aplicació és injectiva, exhaustiva i preserva sumes i productes. □

Proposició 2.22. *$\mathbb{F}_{p^n}$ conté un subcòs $\mathbb{F}_{p^m} \iff m|n$.*

Sigui $k \subseteq \mathbb{F} = \mathbb{F}_{p^n}$ un cos, aleshores $k^* \subseteq \mathbb{F}^*$ i k^* és, doncs, un subgrup cíclic del grup cíclic $\mathbb{F}^*$ que és d'ordre $p^n - 1$ pel teorema 2.32. Per tant, k^* té ordre divisor de $p^n - 1$. Veurem doncs $p^m - 1 | p^n - 1 \iff m|n$.

Demostració.
- $\Leftarrow\rfloor$ Suposem $m|n$. Per tant, $\exists\, k$ tal que $n = km$. $p^n - 1 = p^{mk} - 1 = (p^m)^k - 1 = (p^m - 1)((p^m)^{k-1} + \cdots + p^m + 1)$. Tenim doncs que $p^m - 1 \,|p^n - 1$.
- $\Rightarrow\rfloor$ Sigui $n = a \cdot m + b$. Veurem que necessàriament $b = 0$. Tenim $p^n - 1 = p^{m \cdot a + b} - 1 = p^{m \cdot a + b} - p^{m \cdot a} + (p^{m \cdot a} - 1) = p^{m \cdot a}(p^b - 1) + (p^{m \cdot a} - 1) \equiv p^{m \cdot a}(p^b - 1)$ mòdul $p^m - 1$ (utilitzant l'apartat previ i el fet que $m | m \cdot a$).

  Com $p^m - 1 | p^n - 1$ i $p^{m \cdot a} \nmid p^m - 1$, $(p^b - 1) = r \cdot (p^m - 1)$ per a un cert r. Però no és possible ja que $0 < b < m$. Per tant, cal $b = 0$ i $r = 0$ i $m|n$.

□

Proposició 2.23. *Sigui $\mathbb{F}$ un cos finit. Aleshores $|\mathbb{F}| = p^n$ amb p primer i $n \geq 1$.*

Demostració. Sigui 1 el neutre respecte el producte al grup $(\mathbb{F}, \cdot)$. Com $\mathbb{F}$ és finit i és grup amb la suma, 1 ha de tenir ordre finit. Anomenem característica de $\mathbb{F}$ al menor primer p tal que $p \cdot 1 = 1 + ... + 1 = 0$. La característica ha de ser un nombre primer donat que, altrament, $p = m \cdot n$, i es compleix $p \cdot 1 = (m \cdot 1) \cdot (n \cdot 1) = 0$ i tindríem doncs divisors de zero al cos $\mathbb{F}$. Prenem ara el subcòs $k = \{m \cdot 1; m = 0, ..., p-1\}$. Per la proposició 2.21 tenim $k \cong \mathbb{F}_p$.

Aplicant l'axiomàtica dels cossos tenim que si considerem l'operació additiva de $\mathbb{F}$ juntament amb el producte escalar d'elements de $\mathbb{F}$ per elements de $k \subseteq \mathbb{F}$, aleshores $\mathbb{F}$ té estructura de k-e.v.

Com $\mathbb{F}$ és un conjunt finit, també ho serà com k-e.v. Sigui $dim_k \mathbb{F} = n$. Podem prendre una base $\{a_1, ..., a_n\} \subseteq \mathbb{F}$. Aleshores tot element de $\mathbb{F}$ es pot escriure de manera única com a combinació lineal amb coeficients a k, $c_1 \cdot a_1 + ... + c_n \cdot a_n$, obtenim un total de p^n combinacions. □

Observació 2.24. Per construir cossos finits, considerarem els quocients ${}^{\mathbb{F}_p[x]}\!/_{\langle g \rangle}$ amb g polinomi irreductible de $\mathbb{F}_p[x]$. Al teorema 2.37 hem vist que sempre podrem prendre aquesta consideració.

Veurem ara que $\forall p$ primer i $\forall n \geq 1$ existeix un cos finit amb p^n elements tot comptant els polinomis irreductibles d'un grau determinat a $\mathbb{F}_p[x]$. Prendrem únicament polinomis mònics donat que podem prendre sempre representants que ho siguin. D'aquests hi ha p^n donat que són de la forma $x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0$ amb els coeficients $a_i \in \mathbb{F}_p$, $\forall\, i \in \{0, ..., n-1\}$.

Considerem ara la funció generatriu per aquesta enumeració per graus, és a dir, la sèrie formal (sumatori infinit sense haver de considerar convergències) de potències els coeficients dels quals codifiquen informació sobre una successió $\{a_i\}_i$, en aquest cas codifica el nombre de polinomis mònics de cada grau. Per tant, tenim la sèrie formal $\sum_{n=0}^{\infty} p^n \cdot u^n$.

La sèrie geomètrica formal produeix:

$$\sum_{n=0}^{\infty} p^n \cdot u^n = \frac{1}{1 - p \cdot u}. \tag{2.1}$$

Coms $\mathbb{F}_p[x]$ és domini de factorització única, cada polinomi mònic factoritza de manera única a $\mathbb{F}_p[x]$. Definim N_n, $n \in \mathbb{N}$, com el nombre de polinomis mònics irreductibles de grau n a $\mathbb{F}_p[x]$. Aleshores, donat un polinomi $g \in \mathbb{F}_p[x]$, $g = g_1 \cdot ... \cdot g_m$ on els g_i's són irreductibles de grau n_i no necessàriament diferents. El grau total de g és la suma dels graus dels factors. Per a cada factor g_i tenim N_{n_i} opcions.

Comptant factoritzacions com abans, tenim que els polinomis mònics de grau n, és a dir, p^n, també es pot expressar com els coeficients de u^n al producte formal infinit $(1 + u + u^2 + ...)^{N_1} \cdot (1 + u^2 + u^4 + ...)^{N_2} \cdot ... = \prod_{k=1}^{\infty} \frac{1}{(1-u^k)^{N_k}}$.

Agrupant les igualtats obtenim:

$$\prod_{k=1}^{\infty} \frac{1}{(1-u^k)^{N_k}} = \frac{1}{1 - p \cdot u}. \tag{2.2}$$

Proposició 2.25. $p^n = \sum_{k|n} k \cdot N_k$

Demostració. Per veure la igualtat caldrà prendre logaritmes i multiplicar per u la igualtat (2.2):

$$\log(\prod_{k=1}^{\infty} \frac{1}{(1-u^k)^{N_k}}) = \log \frac{1}{1-p\cdot u} \iff \sum_{k=1}^{\infty} \log \frac{1}{(1-u^k)^{N_k}} = \log \frac{1}{1-p\cdot u} \iff$$

$$(-1)\sum_{k=1}^{\infty} \cdot(N_k)\cdot \log(1-u^k) = (-1)\cdot\log(1-p\cdot u) \iff \sum_{k=1}^{\infty} N_k \cdot \log(1-u^k) = \log(1-p\cdot u)$$

Derivant la igualtat respecte u obtenim:

$$\sum_{k=1}^{\infty} N_k \frac{1}{(1-u^k)} \cdot (-k)\cdot u^{k-1} = \frac{1}{1-p\cdot u}\cdot(-p) \iff \sum_{k=1}^{\infty} \frac{k\cdot N_k}{1-u^k}\cdot u^{k-1} = \frac{p}{1-p\cdot u}$$

Multiplicant finalment per u, desenvolupant la sèrie geomètrica formal 2.1 i comparant els coeficients dels termes u^n obtenim el resultat buscat

$$\sum_{k=1}^{\infty} \frac{k\cdot N_k}{1-u^k}\cdot u^k = \frac{p\cdot u}{1-p\cdot u} \iff \sum_{k=1}^{\infty} k\cdot N_k \cdot (u^k + u^{2k} + ...) = p\cdot u + p^2\cdot u^2 + p^3\cdot u^3 + ...$$

□

Notació 3. *Utilitzarem $\lfloor A \rfloor$ per denominar el major enter menor o igual a A.*

Proposició 2.26. $N_n > 0$, $\forall\, n \geq 1$.

Demostració.

- Cas $n = 1$: $\forall\, \beta \in \mathbb{F}_p$, $x - \beta$ és irreductible. Per tant, tenim $N_1 = p$.
- Cas $n = 2$: per la proposició prèvia i aïllant N_2 obtenim $N_2 = \frac{p^2-p}{2} > 0$.
  De la mateixa manera obtenim els casos $n = 3, 4$:
- Cas $n = 3$: $N_3 = \frac{p^3-p}{3} > 0$.
- Cas $n = 4$: $N_4 = \frac{p^4-p^2}{2} > 0$.
- Cas $n \geq 5$: aplicarem contradicció
  Suposem $\exists\, n \geq 5$ tal que $N_n = 0$. Per la proposició prèvia tenim:

$$p^n = \sum_{k|n, 0<k<n} k \cdot N_k$$

Recordem primer la fórmula de la suma geomètrica finita:

$$\sum_{k=0}^{j} p^k = \frac{p^{j+1}-1}{p-1}$$

Per arribar a la contradicció, aproximarem el costat dret de la igualtat:
Sabem $N_k \leq p^k\ \forall\, k$ i a més $k \leq \lfloor \frac{n}{2} \rfloor$ donat que $k|n$.

Per tant, $p^n \leq \lfloor \frac{n}{2} \rfloor \cdot \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} p^k \leq \lfloor \frac{n}{2} \rfloor \cdot \frac{p^{\lfloor \frac{n}{2} \rfloor}-1}{p-1} \leq \lfloor \frac{n}{2} \rfloor \cdot p^{\lfloor \frac{n}{2} \rfloor + 1}$. Dividint els dos extrems entre $p^{\lfloor \frac{n}{2} \rfloor}$ obtenim

$$p^{n-\lfloor \frac{n}{2} \rfloor} \leq \lfloor \frac{n}{2} \rfloor \cdot p.$$

Fet que és fals $\forall\, n \geq 5$. És a dir, $N_n > 0\ \forall\, n$.

Veiem per finalitzar aquesta darrera afirmació. Si $n \geq 5$, aleshores $\lfloor \frac{n}{2} \rfloor \geq 2$. Veurem que es verifica la desigualtat contrària, és a dir, $p^{n-\lfloor \frac{n}{2} \rfloor} > \lfloor \frac{n}{2} \rfloor \cdot p$ o, equivalentment, $p^{n-\lfloor \frac{n}{2} \rfloor - 1} > \lfloor \frac{n}{2} \rfloor$. Prenent logaritmes en base p obtenim $n - \lfloor \frac{n}{2} \rfloor - 1 > \log_p \lfloor \frac{n}{2} \rfloor$. Notem primer $n - \lfloor \frac{n}{2} \rfloor - 1 \geq \lfloor \frac{n}{2} \rfloor - 1$. Anomenem x a $\lfloor \frac{n}{2} \rfloor$. Demostrarem $x - 1 > \log_p x$. Per a $x = 3$ es verifica $p^{x-1} > x$ i derivant respecte x tenim $p^{x-1} \cdot ln(p) > 1$, $\forall\, x \geq 3$. Per tant, es verifica la desigualtat inicial per a tot $x \geq 3$.

En el cas $x = 2$ i $p \neq 2$, tenim la desigualtat $p^{x-1} = p > 2 = x$. Cal, per últim, estudiar el cas $x = 2$, $p = 2$. Anant directament a $n - \lfloor \frac{n}{2} \rfloor - 1 > \log_p \lfloor \frac{n}{2} \rfloor$ i avaluant obtenim $2 > \log_2 2 = 1 \iff 2^2 > 2$ com volíem.

□

Teorema 2.27. *$\forall\, p$ primer i $\forall\, n \geq 1$, existeix un cos $\mathbb{F}$ tal que $|\mathbb{F}| = p^n$.*

Demostració. Per a cada p primer, com $N_n > 0$, podem prendre un polinomi g irreductible de grau n i el cos $\mathbb{F}_p[x]/\langle g \rangle$ té p^n elements com buscàvem. □

Proposició 2.28. *Siguin γ_1 i γ_2 elements d'un grup abelià finit d'ordres n_1 i n_2 respectivament tals que n_1 i n_2 siguin coprimers. Aleshores, $\gamma_1 \cdot \gamma_2$ té ordre $n_1 \cdot n_2$.*

Demostració. $(\gamma_1 \cdot \gamma_2)^{n_1 \cdot n_2} = \gamma_1^{n_1 \cdot n_2} \cdot \gamma_2^{n_1 \cdot n_2} = 1^{n_2} \cdot 1^{n_1} = 1$. Sigui m l'ordre de $\gamma_1 \cdot \gamma_2$. Tenim doncs, $m | n_1 n_2$

Llavors, $(\gamma_1 \cdot \gamma_2)^m = 1 \implies \gamma_2^m = \gamma_1^{-m}$ i, per tant, γ_2^m pertany a la òrbita de γ_1 i de γ_2 alhora. Suposem que γ_2^m té ordre r, aleshores $(\gamma_2^m)^r = 1$ i com pertany a l'òrbita dels dos, $r | n_1$ i $r | n_2$ però aquests són coprimers i, per tant, necessàriament $r = 1$. Tenim doncs $\gamma_2^m = 1$ i com és de l'òrbita de γ_1 i γ_2, $n_1 | m$ i $n_2 | m$. Com són coprimers, $n_1 n_2 | m$. En conclusió, $m = n_1 n_2$. □

Teorema 2.29 (Lagrange per a grups finits)**.** *(Teorema 1.5 de [Jac12]). Donat un grup finit G i un subgrup H l'ordre de H és un divisor de l'ordre de G.*

Corołari 2.30. *Si G és un grup finit d'ordre n, aleshores $x^n = 1$ per a tot $x \in G$.*

Demostració. Sigui $x \in G$ un element d'ordre m, és a dir, $x^m = 1$. Pel teorema 2.29 $m | n \implies \exists\, r$ tal que $n = mr$. Tenim doncs $x^n = x^{mr} = (x^m)^r = 1^r = 1$ □

Proposició 2.31. *Sigui G un grup cíclic i $g \in G$ un element d'ordre n. Aleshores g^k té ordre $\frac{n}{mcd(k,n)}$.*

Demostració. Sigui m l'ordre de g^k i sigui $d = mcd(k, n)$, aleshores $n = dn'$ i $k = dk'$. $(g^k)^{n'} = g^{kn'} = g^{k'dn'} = g^{k'n} = (g^n)^{k'} = 1$. Per tant $m \leq n'$. Per altra banda $(g^k)^m = g^{km} = 1$ i com l'ordre de g és n, $n | km \implies n'd | k'dm \implies n' | k'm$ i com $mcd(n', k') = 1$, aleshores $n' | m$ i, per tant, $n' \leq m$. Ajuntant els dos resultats, obtenim $m = n'$. □

Teorema 2.32. *Sigui $\mathbb{F} = \mathbb{F}_{p^n}$ un cos finit. El grup multiplicatiu d'elements no nuls de $\mathbb{F}$, denotat per $\mathbb{F}^*$, és un grup cíclic d'ordre $p^n - 1$.*

Demostració. L'ordre és clar donat que només estem ometent el 0. Sigui $m = p^n - 1$. Pel teorema de Lagrange per a grups finits tenim $\forall\, \beta \in \mathbb{F}\backslash\{0\}$ és arrel de $x^m = 1$ i l'ordre multiplicatiu de cada és divisor de m. Falta veure que existeix un element d'ordre m. Factoritzem m en primers: $m = q_1^{e_1} \cdot ... \cdot q_k^{e_k}$. Sigui $m_i = m/q_i$. Com $x^{m_i} = 1$ té com a màxim m_i arrels, aleshores existeix $\beta_i^{m_i} \neq 1$. Per la proposició 2.31, $\gamma_i = \beta_i^{m/q_i^{e_i}}$ té ordre $q_i^{e_i}$. Es segueix de la proposició 2.28 que $\gamma_1 \cdot ... \cdot \gamma_k$ té ordre exactament m donat que els $q_i^{e_i}$'s són coprimers 2 a 2. □

Definició 2.33. *Anomenarem element primitiu a un generador del grup multiplicatiu $\mathbb{F}^*$.*

Exemple 2.34. Estudiem $\mathbb{F}_9$. Prenem el polinomi irreductible $g = x^2 + x + 2$ a $\mathbb{F}_3[x]$. Aleshores, $\mathbb{F}_9 \cong {}^{\mathbb{F}_3[x]}\!/_{\langle g \rangle}$. Tenim la relació $\alpha^2 = 2\alpha + 1$. Computem les potències de α arrel de g.

α	$\alpha^2 = 2\alpha + 1$	$\alpha^3 = 2\alpha + 2$
$\alpha^4 = 2$	$\alpha^5 = 2\alpha$	$\alpha^6 = \alpha + 2$
$\alpha^7 = \alpha + 1$	$\alpha^8 = 1$	0

Es comprova que α és element primitiu de $\mathbb{F}_9^*$.

Observació 2.35. No sempre tindrem que l'arrel del polinomi sigui element primitiu. El següent exemple il·lustra aquest fet.

Exemple 2.36. Sigui $g = x^2 + 1 \in \mathbb{F}_3[x]$. Veiem si té arrels a $\mathbb{F}_3$: $g(0) = 1$, $g(1) = 2$, $g(2) = 5 = 2$. Per tant, és irreductible. Tal com hem vist, per tant, $k = {}^{\mathbb{F}_3[x]}\!/_{\langle g \rangle}$ és un cos amb 9 elements. Tot i així, la classe de x, que notarem per α, a k no és element primitiu.

$\alpha^2 = -1 = 2$, $\alpha^3 = 2 \cdot \alpha$, $\alpha^4 = 2 \cdot \alpha^2 = 2 \cdot 2 = 1$. Per tant α té ordre 4 i no 8 com caldria.

Podríem pensar que, com hi ha més d'un polinomi irreductible donat un grau n, no hi ha unicitat de cossos ${}^{\mathbb{F}_p[x]}\!/_{\langle g \rangle}$ tot i tenir els mateixos elements. El següent resultat ens assegura el contrari.

Teorema 2.37. *Tot cos finit $\mathbb{F}$ és isomorf a un quocient $\mathbb{F} = {}^{\mathbb{F}_p[x]}\!/_{\langle g \rangle}$ amb g irreductible a $\mathbb{F}_p[x]$.*

Demostració. Sigui $\mathbb{F}$ un cos finit tq $|\mathbb{F}| = p^n$ (pel teorema 2.27 l'existència està assegurada). Sigui α un element primitiu de $\mathbb{F}$. Considerem l'homomorfisme d'anells definit per:

$$\begin{aligned} \varphi : \mathbb{F}_p[x] &\longrightarrow \mathbb{F} \\ x &\longmapsto \alpha \end{aligned} \tag{2.3}$$

Veiem primer que és un homomorfisme exhaustiu. Sigui $\beta \in \mathbb{F}$, com α és element primitiu $\Longrightarrow\ \exists\, j \in \{0, ..., p^n - 1\}$ tal que o bé $\alpha^j = \beta$ o bé $\beta = 0$. En el primer cas, β és imatge de x^j per ser φ homomorfisme. En el segon cas és imatge del 0 per ser també homomorfisme.

Passem a estudiar l'estructura del $ker(\varphi)$ tot veient que és de la forma $ker(\varphi) = \langle g \rangle$ per a algun $g \in \mathbb{F}_p[x]$ polinomi irreductible mònic. Pel teorema 2.8 sabem que $ker(\varphi)$ és un ideal de $\mathbb{F}_q[x]$. Els elements del nucli són de la forma $\sum_{j=0}^{n} a_j \cdot x^j$ tals que $\varphi(\sum_{j=0}^{n} a_j \cdot x^j) = 0$. sigui $g \in \mathbb{F}_p[x]$ tal que $g(\alpha) = 0$ amb g irreductible. Notem que el ker no pot ser trivial

donat que aleshores φ seria un isomorfisme i $\mathbb{F}_p[x]$ és un cos infinit mentre que $\mathbb{F}$ és un cos finit. Per tant hi ha com a mínim un element. Com $ker(\varphi)$ és ideal de $\mathbb{F}_p[x]$ i aquest és DIP, necessàriament $ker(\varphi) = \langle g \rangle$ amb g irreductible de $\mathbb{F}_p[x]$ ja que si no ho fos, $g = f_1 \cdot ... \cdot f_k \implies f_1(\alpha) \cdot ... \cdot f_k(\alpha) = g(\alpha) = 0$ i com $\mathbb{F}_p[x]$ domini d'integritat (per ser $\mathbb{F}$ cos) $\exists i \in \{1, .., k\}$ tal que $f_i(\alpha) = 0$ però aleshores $f_i \in \langle g \rangle = ker(\varphi)$ i $grau(f_i) < grau(g)$ i arribem a contradicció.

Finalment, el teorema fonamental 2.8 ens permet afirmar $\mathbb{F}[x]/_{ker(\varphi)} \cong Im(\varphi)$. Com φ és exhaustiva, $Im(\varphi) = \mathbb{F}$ i tal com hem vist $Ker(\varphi) = \langle g \rangle$ amb g polinomi mònic irreductible. □

Definició 2.38. *Anomenarem polinomi mínim de α sobre $\mathbb{F}_p[x]$ al polinomi mònic irreductible que genera $ker(\varphi)$ on φ és el morfisme (2.3) vist a la demostració anterior.*

Proposició 2.39. *Sigui k un cos amb p^n elements, aleshores $x^{p^n} - x$ descompon completament en factors lineals a $k[x]$.*

Demostració. Pel teorema 2.32, k^* és grup cíclic d'ordre $p^n - 1$ i per tant $\forall\, \alpha \in k^*$ es verifica $\alpha^{p^n-1} = 1$, és a dir, α és arrel del polinomi $x^{p^n-1} - 1$. Hem trobat doncs $p^n - 1$ arrels de $x^{p^n-1} - 1$ i per tant descompon en factors lineals a $k[x]$. Afegint l'arrel 0, trobem p^n arrels de $x^{p^n} - x$ a k i $x^{p^n} - x$ descompon en factors lineals a $k[x]$. □

Definició 2.40. *Donat $f = a_0 + \cdots + a_m x^m$ i $g = b_0 + \cdots b_l x^l$ dos polinomis de $k[x]$, definim la resultant de f i g com el determinant de la matriu*

$$\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & & a_0 & b_l & & b_0 \\ a_m & & a_1 & & \ddots & \vdots \\ & \ddots & \vdots & & & b_l \\ & & a_m & & & \end{pmatrix} \in M_{(m+l)\times(m+l)}(k)$$

i es denota per $res(f, g, x)$.

Proposició 2.41. *(proposició 3 capítol 6 de [CLO13]) Siguin $f, g \in k[x]$ polinomis no nuls. f i g tenen una arrel en comú si i només si $Res(f, g, x) = 0$.*

Proposició 2.42. *Sigui $\mathbb{F} = \mathbb{F}_p[x]/_{\langle g \rangle}$ un cos finit, aleshores g divideix $x^{p^n} - x$ a $\mathbb{F}_p[x]$*

Demostració. Sigui β element primitiu de $\mathbb{F}$. Sabem doncs $\beta \in \mathbb{F}^*$, pel teorema 2.32 tenim doncs $\beta^{p^n-1} = 1$. Per tant β és arrel del polinomi $x^{p^n-1} = 1$ i per tant també ho és de $x^{p^n} = x$. Com $g(\beta) = 0$ i g és irreductible, necessàriament $g | x^{p^n} - x$ ja que al tenir una arrel en comú la resultant dels dos polinomis és nul·la i per tant $gcd(g, x^{p^n} - x) \neq 1$ i l'única opció és el propi g per ser irreductible. □

Teorema 2.43. *Siguin k i $\mathbb{L}$ dos cossos tals que $|k| = |\mathbb{L}| = p^n$. Aleshores k i $\mathbb{L}$ són isomorfs.*

Demostració. Siguin k i $\mathbb{L}$ dos cossos amb p^n elements. Sigui β un element primitiu de $\mathbb{L}$, i sigui $g \in \mathbb{F}_p[x]$ el polinomi mínim de β a $\mathbb{F}_p$. Tenim doncs $\mathbb{L} \cong \mathbb{F}_p[x]/_{\langle g \rangle}$.

Observem primer que $x^{p^n} - x$ descompon en factors lineals a $k[x]$. Sigui $\alpha \in k^*$, aleshores, com k té p^n elements, α pertany al grup cíclic k^* d'ordre $p^n - 1$. Per tant, verifica $\alpha^{p^n} = \alpha$. Tot element de k^* és doncs solució de l'equació $x^{p^n} = x$ i, a més, el zero també la verifica.

Veiem ara que hi ha algun $\gamma \in k$ que és arrel de $g = 0$. Suposem que no. Per la proposició 2.42, $h = x^{p^n} - x = g \cdot f$ amb $f \in \mathbb{F}_p[x]$. Com $h(\gamma) = 0 \ \forall \gamma \in k \implies g(\gamma) \cdot f(\gamma) = 0 \ \forall \alpha \in k$. Si $g(\gamma) \neq 0 \ \forall \gamma \in k$ aleshores, $f(\gamma) = 0 \ \forall \gamma \in k$ i, per tant, $f = h \cdot A$ amb A unitat. Per tant, $h = g \cdot f = g \cdot h \cdot A \implies 1 = g \cdot A$ i g ha de ser unitat.

Seguirem els raonaments descrits 2.37. Definim el morfisme injectiu

$$\begin{aligned} \varphi : \mathbb{F}_p[x] &\longrightarrow k \\ x &\longmapsto \gamma \end{aligned}$$

Com $g(\gamma) = 0$, $g \in ker(\varphi)$ i, per tant, $\langle g \rangle \subseteq ker(\varphi)$. Sigui $h \in \mathbb{F}_p[x]$ polinomi irreductible tal que $\langle h \rangle = ker(\varphi)$. Com $g \in \langle h \rangle$, h divideix g i, com tot dos són irreductibles, són múltiples respecte unitats. Per tant, $\langle g \rangle = \langle h \rangle = ker(\varphi)$. Pel teorema 2.8,

$$k \cong {}^{\mathbb{F}_p[x]}\!\diagup_{\langle g \rangle} \cong \mathbb{L}$$

□

El següent exemple il·lustra el cas particular de $p = 2$ i $n = 3$:

Exemple 2.44. Aïllant n_k de la igualtat obtinguda a la proposició 2.25, sabem que hi ha $\frac{2^3-2}{3} = 2$ polinomis mònics irreductibles de grau 3 a $\mathbb{F}_2[x]$, que són $g_1 = x^3 + x + 1$ i $g_2 = x^3 + x^2 + 1$. Tenim doncs els següents cossos finits amb 8 elements:

$$\begin{aligned} k_1 &= {}^{\mathbb{F}_2[x]}\!\diagup_{g_1} \\ k_2 &= {}^{\mathbb{F}_2[x]}\!\diagup_{g_2} \end{aligned}$$

Sigui α la classe de x a k_1, aleshores $g_1(\alpha) = 0$ i, per tant, $\alpha^3 + \alpha + 1 = 0$. Tenint en compte la relació prèvia, $g_2(\alpha + 1) = (\alpha + 1)^3 + (\alpha + 1)^2 + 1 = (\alpha^2 + 2\alpha + 1)(\alpha + 1) + (\alpha^2 + 2\alpha + 1) + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + 1 = \alpha^3 + \alpha + 1$ a k_1. Per tant, donada una arrel α del polinomi g_1, tenim $\alpha + 1$ com arrel de g_2.

Definim ara el morfisme d'anells

$$\begin{aligned} \varphi : \mathbb{F}_2[x] &\longrightarrow \mathbb{F}_2[x] \\ x &\longmapsto x + 1 \end{aligned}$$

Veiem que es tracta d'un morfisme d'anells i té com a morfisme invers

$$\begin{aligned} \varphi^{-1} : \mathbb{F}_2[x] &\longrightarrow \mathbb{F}_2[x] \\ x &\longmapsto x - 1 \end{aligned}$$

Per tant, es tracta d'un isomorfisme d'anells. Aquest morfisme envia g_1 a g_2. Per tant, $\varphi(\langle g_1 \rangle) = \langle g_2 \rangle$ i, pel teorema 2.16, tenim l'isomorfisme buscat.

Lema 2.45. *Sigui $\beta \in \mathbb{F}_{p^n}$ tal que β no és ni 0 ni 1. Aleshores*

$$\sum_{j=0}^{p^n-2} \beta^j = 0.$$

Demostració. $\frac{x^m-1}{x-1} = \frac{(x^{p^n-1}-1)}{(x-1)} = \sum_{j=0}^{p^n-2} x^j$. Sabem que $\forall\, \beta \neq 0 \in \mathbb{F}$ es verifica $\beta^m = 1$. Per tant, si $\beta \neq 0, 1$ tenim $\sum_{j=0}^{m-1} \beta^j = \frac{\beta^m - 1}{\beta - 1} = 0$ □

Observació 2.46. Notem que al construir $\mathbb{F}_p[x]/\langle g \rangle$ la classe de x esdevé una arrel de l'equació $g = 0$.

Lema 2.47. *Sigui $\mathbb{F}_q$ un cos finit. Tot parell x, $y \in \mathbb{F}_q$ verifica:*

$$(x+y)^q = x^q + y^q$$

Demostració. Desenvolupem la potència.

$$(x+y)^q = \sum_{k=0}^{q} \binom{q}{k} \cdot x^{q-k} \cdot y^k = \sum_{k=0}^{q} \frac{q!}{k!\cdot(q-k)!} x^{q-k} \cdot y^k.$$

Com la característica del cos és p, tenim que $\frac{q!}{k!\cdot(q-k)!} = 0$ si i només si $k \neq 0, q$ i altrament el quocient pren valor 1.

Per tant, $(x+y)^q = x^q + y^q$. □

2.2 Bases de Gröebner

En aquesta secció $R = k[x]$ serà l'anell de polinomis en una variable sobre k un cos i I un ideal d'aquest.

Definició 2.48. *Un ordre monomial a $(\mathbb{Z}_{\geq 0})^n$ (exponents de monomis de R) és una relació $>$ a $(\mathbb{Z}_{\geq 0})^n$ tal que:*

1. *$>$ és un ordre total (és a dir, si $\alpha \neq \beta \implies \alpha > \beta$ o $\beta > \alpha$).*
2. *si $\alpha > \beta \implies \forall\, \gamma \in (\mathbb{Z}_{\geq 0})^n$, $\alpha + \gamma > \beta + \gamma$*
3. *$>$ és un bon ordre (és a dir, $\forall\, S \subseteq\in (\mathbb{Z}_{\geq 0})^n$ tal que $S \neq \emptyset$, aleshores $\exists\, \alpha^o \in S$ tal que $\alpha > \alpha^o\ \forall\, \alpha \in S$).*

Proposició 2.49. *(Lema 2 del capítol 2 de [CLO13]). Sigui $>$ una relació, aleshores és bon ordre si i només si tota successió estrictament decreixent estaciona en un nombre finit de passos.*

Definició 2.50. *Sigui $f = \sum a_\alpha x^\alpha \in K[x_1, \cdots, x_n]$, $f \neq 0$ i $>$ un ordre monomial. Aleshores:*

- *El multigrau de f és $multideg(f) = max_>\{\alpha \in (\mathbb{Z}_>)^n) | a_\alpha \neq 0\}$.*
- *El coeficient principal de f és $LC(f) = a_{multideg(f}$.*
- *El monomi principal de f és $LM(f) = x^{multideg(f)}$.*

- *El terme principal de f és $LT(f) = L(f) \cdot LM(f)$.*

Definició 2.51. *Sigui I ideal. Definim el conjunt de termes principals com:*

$$LT(I) = \{a_\alpha x^\alpha | \exists\, f \in I : LT(f) = a_\alpha x^\alpha\}$$

Definició 2.52. *Fixat un ordre monomial a $K[x_1, \cdots, x_n]$, sigui I un ideal, un conjunt $\{g_1, \cdots, g_s\}$ de I és base de Gröebner si:*

$$\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_s)\rangle$$

Lema 2.53. *(Proposició 4 del capítol 5 de [CLO13]). Sigui k un cos i $I \subset k[x_1, \cdots, x_n]$ ideal. Aleshores $k[x_1, \cdots, x_n]/I$ és isomorf com a k-espai vectorial al espai vectorial generat per $\{x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle\}$*

Tot i que es podria haver estret aquesta secció com a un cas particular de la següent, és més il·lustratiu considerar les definicions restringides a $R = k[x]$ donat que prenen un paper important en alguns codis.

2.3 Submòduls d'anells de polinomis en diverses variables

Per veure un dessenvolupament més extens consultar capítol 5 de [CLO05].

Definició 2.54. *Sigui R un anell commutatiu unitari. Anomenarem R-mòdul a la terna $(M, +, \cdot)$ on:*

- *M és un conjunt.*
- *$+ : M \times M \mapsto M$*
- *$\cdot : R \times M \mapsto M$*

Que satisfà:

1. *$(M, +)$ és un grup abelià.*
2. *$a \cdot (f + g) = a \cdot f + a \cdot g$; $\forall\, a \in R$, $\forall\, f, g \in M$.*
3. *$(a + b) \cdot f = a \cdot f + b \cdot f$; $\forall\, a, b \in R$, $f \in M$.*
4. *$(a \cdot b) \cdot f = a \cdot (b \cdot f)$; $\forall\, a, b \in R$, $f \in M$.*

Definició 2.55. *Sigui R un anell, M un R-mòdul. Direm que una terna $(N, +, \cdot)$ és un submòdul de $(M, +, \cdot)$ si:*

- *$N \subseteq M$ com a conjunts.*
- *$(N, +, \cdot)$ és un R-mòdul.*

Notació 4. *És freqüent denotar el mòdul $(M, +, \cdot)$ com a M.*

Definició 2.56. *Sigui M un R-mòdul. Direm que un conjunt $F \subset M$ genera M si $\langle F\rangle = M$. Si F és un conjunt finit, aleshores direm que M és finit generat. Anomenarem generadors als elements de F.*

Definició 2.57. *Sigui $F = \{f_1, \cdots, f_n\} \subset M$, direm que és linealment independent sobre R si $\forall\, a_i \in R$, $f_i \in F$, $i = 1, \cdots, n$:*

$$a_1 f_1 + \cdots + a_n f_n = 0 \in M \implies a_i = 0 \quad \forall\, i = 1, \cdots, n$$

Direm que F és una base de M: si genera M i és linealment independent.

Proposició 2.58. *Sigui M un R-mòdul. Un conjunt F és una base de M si i només si tot element $f \in M$ es pot escriure de manera única com a combinacions lineals respecte R d'elements de F.*

Definició 2.59. *Donat M un R-mòdul, direm que és un mòdul lliure si admet una base.*

Observació 2.60. Podem pensar R^m com:

$$R^m = R \oplus R \oplus \cdots \oplus R$$

és a dir, com a una suma directa de còpies del propi R. És fàcil veure que

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots e_n = (0, 0, \ldots, 1)$$

és una base de R^m que anomenarem base estàndard.

A partir d'ara considerarem k un cos, $R = k[x_1, \cdots, x_n]$ l'anell de polinomis en n variables. Treballarem amb submòduls M de la forma $M \subset R^m$ per a cert $m \geq 1$.

Definició 2.61. *Un monomi a R^m és un element de la forma $x^\alpha e_i$ per a algun $i \in \{1, \cdots, m\}$.*

Observació 2.62. Tot element de R^m es pot escriure com a única combinació de monomis. Aquest fet és conseqüència que els e_i's formin una base de R^m.

Donat un polinomi $f \in R^m$, aquest és de la forma $f = \sum_{i=1}^n f_i e_i$ amb $f_i \in R$ per a $i = 1, \ldots, n$. Alhora, els f_i's descomponen en monomis de R, $f_i = \sum_j a_j x^j$. D'aquesta forma, podem expressar el polinomi f com a combinacions de monomis de R^m, $f = \sum_{i=0}^t c_i m_i$ amb m_i's monomis.

Definició 2.63. *Definirem un ordre monomial $>$ a R^m com una relació d'ordre als monomis de R^m que verifica:*

1. *$>$ és relació total (és a dir, si a, b són monomis de R^m tals que $a \neq b \implies a > b$ o $b > a$);*
2. *Per a tot parell de monomis $a, b \in R^m$ tals que $a > b$, aleshores $x^\alpha a > x^\alpha b$ per a tot $x^\alpha \in R$;*
3. *$>$ és un bon ordre (és a dir, tot subconjunt no buit de monomis té un mínim element).*

Proposició 2.64. *La condició 3 és equivalent a veure que $x^\alpha m > m$ per a tot monomi $m \in R^m$ i $x^\alpha \in R$ tal que $x^\alpha \neq 1$.*

Definició 2.65. *Donat un ordre monomial $>$ a R^m i $f = \sum_{i=0}^t c_i m_i \in R^m$, $c_i \in k$, $m_i \in R^m$ $i = 1, \ldots t$ podem definir:*

- *El monomi principal de f com $LM_>(f) = max_>\{m_1, \ldots, m_t\}$.*
- *El coeficient principal es correspondrà al coeficient del monomi $LM_>(f)$ i es denotarà per $LC(f)$.*
- *El terme principal serà $LT_>(f) = LC_>(f) \cdot LM_>(f)$.*

Teorema 2.66. *Donat un ordre monomial $>$ a R^m i un conjunt $F = \{f_1, \ldots, f_s\}$ una s-tupla ordenada d'elements de R^m. Aleshores, tot $f \in R^m$ s'escriu de manera única com:*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

on $a_i \in R$, $\forall\, i = 1, \ldots, s$; $r \in R^m$ tal que $LT(a_i f_i) \leq LT(f)$ i, a més, $r = 0$, o bé és combinació k-lineal de monomis no divisibles per $LM(f_i)$ $i = 1, \ldots, s$. Anomenarem residu a r.

Definició 2.67. *Anomenarem residu de f respecte F al element r del teorema anterior. El denotarem per $r_F(f)$.*

Proposició 2.68 (algoritme de divisió a R^m)**.** *(Teorema 3 capítol 2 de [CLO13]). Donat un ordre monomial a R^m i $\{f_1, \ldots, f_s\}$ una s-tupla ordenada d'elements de R^m, el següent algoritme calcula la $s+1$-tupla mencionada al teorema anterior que verifica la igualtat.*

- *Input:*$\{f_1, \ldots, f_s\}, f$.
- *Output:* $\{q_1, \ldots, q_s\}, r$.
  - $q_1 := 0,\ \ldots q_s := 0,\ r := 0,\ p := f$.
  - *While $p \neq 0$ do:*
    - $i := 0$
    - $divisio := FALSE$
    - *While $i \leq s$ i $divisio = FALSE$ do:*
      - *si $LT(f_i)$ divideix $LT(p)$ aleshores:*
      - $q_i := q_i + LT(p)/LT(f_i)$
      - $p := p - (LT(p)/LT(f_i))f_i$
      - $divisio := TRUE$
      - *Altrament*
      - $i := i + 1$
    - *If $divisio = FALSE$ aleshores:*
      - $r := r + LT(p)$
      - $p := p - LT(p)$

    Return $q_1, \ldots, q_s, r$.

Definició 2.69. *Sigui M un R-mòdul, $>$ un ordre monomial. Denotarem per $\langle LT(M)\rangle$ el submòdul monomial generat per els termes principals dels elements de M respecte $>$.*

Anomenarem base de Gröebner de M al conjunt $\mathcal{G} = \{g_1, \ldots, g_s\} \subset M$ tal que

$$\langle LT(M)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle.$$

Proposició 2.70. *Sigui $\mathcal{G}$ una base de Gröebner d'un submòdul $M \subset R^m$. Aleshores:*

- *Donat $f \in R^m$, $f \in M$ si i només si $r_{\mathcal{G}}(f)$ és zero.*
- *$M = \langle \mathcal{G} \rangle$.*

Observació 2.71. Tot i que una base de Gröebner d'un mòdul és un conjunt generador del mòdul, no és cert en general que aquest conjunt sigui una base donat que no està assegurada la independència lineal sobre R.

Corołari 2.72. *Tot submòdul de R^m és finit generat.*

Demostració. Prèviament hem vist que R^m admet com a base de Gröebner $\{e_1, \ldots, e_m\}$ i tot submòdul serà doncs finit generat. □

Definició 2.73. *Donats $f, g \in R^m$ i un ordre monomial $>$ a R^m, anomenarem mínim comú múltiple de f i g al element*

$$LCM(f,g) = max_{>}\{h \in R^m \mid r_f(h) = 0 \; i \; r_g(h) = 0\}.$$

Definició 2.74. *Fixat un ordre monomial $>$ i donats $f, g \in R^m$ definim el S-polinomi de f i g com:*

$$S(f,g) = \frac{LCM(LM(f),LM(g))\cdot f}{LT(f)} - \frac{LCM(LM(f),LM(g))\cdot g}{LT(g)}$$

Teorema 2.75. *(criteri de Buchberger per a submòduls) Un conjunt $\mathcal{G} = \{g_1, \ldots, g_s\} \subset R^m$ és una base de Gröebner del mòdul que generen si i només si*

$$r_{\mathcal{G}} S(g_i, g_j) = 0 \quad \forall \, i, j \; i \neq j$$

Teorema 2.76. *[algoritme de Buchberger per a submòdul]: El següent algoritme permet computar una base de Gröebner d'un submòdul M a partir d'un sistema de generadors d'aquest.*

- *Input: $\{f_1, \ldots, f_s\}$ conjunt generador de M.*
- *output:$\{g_1, \ldots, g_t\} = \mathcal{G}$ base de Gröebner de M.*
  - *$G := F$*
  - *Repeat:*
    - *$\mathcal{G}' := \mathcal{G}$*
    - *$\forall p, q \in \mathcal{G}'$, $p \neq q$ do:*
      - *$S := r_{\mathcal{G}'}(S(p,q))$*
      - *if $S \neq 0 \implies \mathcal{G} := \mathcal{G} \cup \{S\}$*

    While $\mathcal{G} = \mathcal{G}'$

Definició 2.77. *Una base reduïda de Gröebner d'un submòdul M és un conjunt $\mathcal{G}$ tal que:*

- *$\mathcal{G}$ és base de Gröebner.*
- *$LC(g) = 1 \; \forall \, g \in \mathcal{G}$.*
- *$\forall \, g \in \mathcal{G}$, cap terme de g pertany a $\langle LT(\mathcal{G} \backslash \{g\}) \rangle$.*

Proposició 2.78. *Tot submòdul de R^m admet una única base reduïda de Gröebner donat un ordre monomial $>$.*

3 Codis correctors d'errors

Definició 3.1. *Anomenarem alfabet a un conjunt finit no buit. Prendrem com a alfabet* $\mathbb{F}_q$ *amb* $q = p^n$ *amb* p *primer* $n \geq 1$.

Definició 3.2. *Un codi* C *de llargada* k *sobre un alfabet* $\mathbb{F}_q$ *és un subconjunt de* $\mathbb{F}_q^k$. *Anomenarem paraules als elements de* C.

Exemple 3.3. Per la naturalesa dels aparells electrònics es freqüent considerar un alfabet binari $\{0, 1\}$ i identificar-lo amb $\mathbb{F}_2$.

Anomenarem codis detector i correctors d'errors als codis capaços de detectar i corregir una quantitat determinada d'errors produïts en la transmissió del codi.

Presentarem una classe de codis que presenten propietats molt còmodes per al procés de codificació i descodificació. Aquests són els codis lineals.

3.1 Codis lineals

Definició 3.4. *Un codi lineal es aquell en el que el conjunt de paraules del codi* C *forma un subespai vectorial de* $\mathbb{F}_q^n$.

Observació 3.5. Podem prendre com a funció codificant $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$ aquelles funcions lineals que tinguin com a imatge C. Com es tracta d'una funció lineal podem prendre la matriu de l'aplicació E respecte les bases estàndards, és a dir, les bases que es deriven de l'element primitiu.

Definició 3.6. *Donat un codi lineal* $C = E(\mathbb{F}_q^k)$, *anomenarem matriu generadora de* C *a la matriu de l'aplicació lineal* E.

Podem prendre G com les matrius de dimensió $k \times n$ i rang k i pensar el procés de codificació d'un vector w com el producte per la dreta d'aquest respecte la matriu G. Les files de G formen una base de C donat que són la imatge dels elements de la base.

Com C és un subespai vectorial i G aplicació lineal, podem descriure C com el conjunt de solucions del sistema de $n - k$ equacions lineals independents. Ens referirem com a matriu de control de paritat de C a la matriu construïda amb els coeficients d'aquest sistema d'equacions.

Exemple 3.7. Prenem el codi lineal C amb $n = 4$, $k = 2$ donat per la matriu generadora G.

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Donat que només hi ha els dos escalars $0, 1 \in \mathbb{F}_2$ per fer les combinacions lineals, hi ha exactament 4 elements a C i són:

$$(0,0) \cdot G = (0,0) \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (0,0,0,0).$$

$$(1,0) \cdot G = (1,0) \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (1,1,1,1).$$

$$(0,1)\cdot G = (0,1)\cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (1,0,1,0).$$
$$(1,1)\cdot G = (1,1)\cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = (0,1,0,1).$$

Veiem que

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

és una funció de control de paritat per a C tot veient que $xH = 0$ per a tot $x \in C$.

$$(0,0,0,0)\cdot H = (0,0,0,0)\cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = (0,0).$$
$$(1,1,1,1)\cdot H = (1,1,1,1)\cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = (0,0).$$
$$(1,0,1,0)\cdot H = (1,0,1,0)\cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = (0,0).$$
$$(0,1,0,1)\cdot H = (0,1,0,1)\cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = (0,0).$$

Exemple 3.8. Sigui $\mathbb{F}_4 = {}^{\mathbb{F}_2[\alpha]}\!/_{\langle \alpha^2+\alpha+1\rangle}$, i sigui C el codi lineal a $\mathbb{F}_4^5$ amb matriu generadora

$$G = \begin{pmatrix} \alpha & 0 & \alpha+1 & 1 & 0 \\ 1 & 1 & \alpha & 0 & 1 \end{pmatrix}.$$

El conjunt de paraules del codi correspondrà a la imatge de $\mathbb{F}_4^2$ per al codi lineal donat. La base estàndard de $\mathbb{F}_4^2$ és $\{(1,0),(0,1)\}$. L'espai de paraules del codi serà el generat per la imatge de la base estàndard. Per tant és l'espai vectorial $< (\alpha,0,\alpha+1,1,0),(1,1,\alpha,0,1) >$ i aquest espai té $4^2 = 16$ elements donat que $\mathbb{F}_4$ té com a elements $0,1,\alpha,\alpha^2 = \alpha+1$.

$$
\begin{aligned}
(1,0) &: (\alpha, 0, \alpha+1, 1, 0) & (0,1) &: (1, 1, \alpha, 0, 1)\\
(\alpha,0) &: (\alpha+1, 0, 1, \alpha, 0) & (0,\alpha) &: (\alpha, \alpha, \alpha+1, 0, \alpha)\\
(\alpha+1,0) &: (1, 0, \alpha, \alpha+1, 0) & (0,0) &: (0, 0, 0, 0, 0)\\
(\alpha+1,\alpha+1) &: (\alpha, \alpha+1, \alpha+1, \alpha+1, \alpha+1) & (1,\alpha) &: (0, \alpha, 0, 1, \alpha)\\
(\alpha,1) &: (\alpha, 1, \alpha+1, \alpha, 1) & (\alpha+1,1) &: (0, 1, 0, \alpha+1, 1)\\
(1,\alpha+1) &: (1, \alpha+1, \alpha, 1, \alpha+1) & (\alpha,\alpha+1) &: (0, \alpha+1, 0, \alpha, \alpha+1)\\
(\alpha+1,\alpha) &: (\alpha+1, \alpha, 1, \alpha+1, \alpha) & (\alpha,\alpha) &: (1, \alpha, \alpha, \alpha, \alpha)\\
(1,1) &: (\alpha+1, 1, \alpha, 1, 1) & (0,\alpha+1) &: (\alpha+1, \alpha+1, 1, 0, \alpha+1)
\end{aligned}
$$

Podem prendre com a matriu de control de paritat

$$
\begin{pmatrix}
\alpha & 0 & 0\\
0 & \alpha & 0\\
1 & \alpha & 1\\
1 & 1 & \alpha^2\\
0 & 1 & \alpha
\end{pmatrix}
$$

donat que és de rang 3 i verifica $G \cdot H = 0$.

Per estudiar la capacitat de correcció d'un codi necessitarem mesurar la distància a la qual es troben els elements de $\mathbb{F}_q^n$.

Definició 3.9. *Siguin $x, y \in \mathbb{F}_q^n$. Definim la distància de Hamming entre x i y com $d(x,y) = |\{i, 1 \leq i \leq n : x_i \neq y_i\}|$.*

Anomenem pes de x a la distància $d(x,0)$ on 0 denota al vector zero a $\mathbb{F}_q^n$. Denotarem el pes per $wt(x)$.

Lema 3.10. *La distància de Hamming té les propietats d'una mètrica a $\mathbb{F}_q^n$.*

1. $d(x,y) \geq 0$, $\forall\, x, y \in \mathbb{F}_q^n$.
2. $d(x,y) = d(y,x)$, $\forall\, x, y \in \mathbb{F}_q^n$.
3. $d(x,y) \leq d(x,z) + d(z,y)$ $\forall\, x, y, z \in \mathbb{F}_q^n$.

Demostració.

1. Surt automàticament de la definició donat que és el cardinal d'un conjunt i aquest valor sempre és major o igual a zero.

2. El nombre de components diferents no depèn de l'ordre en que triem els dos punts i, per tant, és simètrica.

3. Sigui d(x,y)=i. Aleshores existeixen i components en les que difereixen. Suposem, sense pèrdua de generalitat, que es tracta de les primeres i components, és a dir, $x_j \neq y_j$ $\forall\, j = 1, ..., i$. Fixat ara $j \in \{1, .., i\}$ tenim que o bé $z_j = x_j \implies z_j \neq y_j$ o bé $z_j = y_j \implies z_j \neq x_j$ o bé $x_j \neq z_j \neq y_j$. Per tant, comparant les primeres i components ja podem afirmar $d(x,z) + d(z,y) \geq i = d(x,y)$.

□

Definició 3.11. *Donat $x \in \mathbb{F}_q^n$ definim la bola tancada de radi r respecte la distància de Hamming centrada a x com:*

$$B_r(x) = \{y \in \mathbb{F}_q^n | d(x,y) \leq r\}.$$

Definició 3.12. *Donat un codi C definim la distància mínima del codi com:*

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

Passem doncs a veure quines utilitats tenen aquests conceptes introduïts.

Proposició 3.13. *Sigui C un codi amb distància mínima d. Tots els errors amb pes $\leq d-1$ es poden detectar. A més, si $d \geq 2t+1$, aleshores tots els errors de pes $\leq t$ es poden corregir prenent la paraula del codi més pròxima.*

Demostració. Sigui e el vector error, z el missatge obtingut i x l'enviat, aleshores $z = x+e$. $wt(e) = d(z-x,0) = |\{i | z_i - x_i \neq 0\}| = |\{i | z_i \neq x_i\}| = d(z,x)$. Com $wt(e) \leq d-1$, tenim $d(z,x) \leq d-1$. Per tant, z no pot ser un element de C donat que la distància mínima es d. En conseqüència, z no és del codi.

Suposem ara $d \geq 2t+1$ i $wt(e) \leq t$. Com que la distància mínima és d i $d-1 \geq 2t$, tenim que, donat $x, y \in C$, $B_t(X) \cap B_t(y) = \emptyset$.

Per tant, si $wt(e) = d(z,x) \leq t$, tenim que z s'ha de trobar dins de la bola tancada de radi t del missatge original $x \in C$. Per corregir el missatge z cal doncs prendre l'element de C tal que $d(z,x) = min\{d(z,y) | y \in C\}$. □

Proposició 3.14. *Per a qualsevol codi lineal C la distància mínima d és equivalent a prendre $min_{x \in C \setminus \{0\}} |\{i \mid x_i \neq 0\}|$.*

Demostració. $d(x-y,0) = |\{i \mid x_i - y_i \neq 0\}| = |\{i \mid x_i \neq y_i\}| = d(x,y)$. Per tant, la distància entre tota parella d'elements diferents del zero del codi es pot escriure com la distància d'un altre element del codi al zero. Buscar la mínima distància és buscar el mínim entre els parells d'elements diferents entre ells i tots aquests termes és poden reescriure com $d(z,0)$ amb un $z \in C$.

En definitiva: $d = min\{d(x,y) \mid x \neq y \in C\} = min\{d(x-y,0) \mid x \neq y \in C\} = min\{d(z,0) \mid z \neq 0 \in C\} = min_{z \in C \setminus 0} |\{i \mid z_i \neq 0\}|$ □

Presentem ara un exemple d'un codi i les seves característiques així com les seves capacitats de detecció i correcció d'errors.

Exemple 3.15. Els codis de Hamming són una família de codis amb interessants propietats de correcció d'errors que estudiarem més endavant. Un d'aquests és el codi sobre $\mathbb{F}_2$ amb $k=4$, $n=7$ i matriu generadora

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{3.1}$$

Notem que al codificar un vector $w \in \mathbb{F}_2^4$, $E(w) = w \cdot G$ el nou vector sempre tindrà com a les primeres 4 components el propi w. Vegem ara que la matriu

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

és de comprovació de paritat. Per fer-ho veurem que el rang de la matriu és 3 i que $G \cdot H = 0$. Són condicions suficients donat que per definició, una matriu de control de paritat són els coeficients d'un sistema de $n - k$ equacions tals que els punts de C són solució del sistema. En aquest cas, $n - k = 3$ i a més, com les files de G són una base de l'espai vectorial, com $G \cdot H = 0$ aleshores és compleix que tot element w de l'espai verificarà $w \cdot H = 0$ com volíem.

Prenent el menor 3×3 corresponent a les últimes 3 files veiem que té rang 3.

$$G \cdot H = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

El codi és $< (1,0,0,0,0,1,1), (0,1,0,0,1,0,1), (0,0,1,0,1,1,0), (0,0,0,1,1,1,1) >$ i, per tant, té com a elements:

$(1,0,0,0) : (1,0,0,0,0,1,1)$	$(0,1,0,0) : (0,1,0,0,1,0,1)$	$(0,0,1,0) : (0,0,1,0,1,1,0)$
$(0,0,0,1) : (0,0,0,1,1,1,1)$	$(1,1,1,1) : (1,1,1,1,1,1,1)$	$(0,0,0,0) : (0,0,0,0,0,0,0)$
$(1,0,0,1) : (1,0,0,1,1,0,0)$	$(1,0,1,0) : (1,0,1,0,1,0,1)$	$(1,1,0,0) : (1,1,0,0,1,1,0)$
$(0,1,0,1) : (0,1,0,1,0,1,0)$	$(0,1,1,0) : (0,1,1,0,0,1,1)$	$(1,1,1,0) : (1,1,1,0,0,0,0)$
$(0,0,1,1) : (0,0,1,1,0,0,1)$	$(1,0,1,1) : (1,0,1,1,0,1,0)$	$(0,1,1,1) : (0,1,1,1,1,0,0)$
	$(1,1,0,1) : (1,1,0,1,0,0,1)$	

A partir d'aquesta llista és fàcil veure que el nombre mínim de components no nul·les és 3. Utilitzant la proposició 3.14 tenim que la distància mínima és 3.

Utilitzant la proposició 3.13 tenim que podem detectar qualsevol error de pes 1 o 2 i corregir qualsevol error de pes 1 prenent el veí més proper.

Si ens fixem en el procés de codificació podem observar que en la imatge de cada paraula a codificar, aquesta conté la pròpia paraula.

Definició 3.16. *Anomenarem codificadors sistemàtics al codis tals que les paraules a codificar apareixen sense modificar a alguna component de la paraula del codi. Parlarem de posicions d'informació a aquestes components i de control paritat a la resta de components.*

Aquest codis ens permeten simplificar tant el procés de codificació com el de descodificació. Per codificar només ens caldrà computar el control de paritat i en el procés oposat només caldrà eliminar el control si no tenim errors en la transmissió.

Notem que els codis sistemàtics admeten matrius generadores de la forma $G = (I_k|P)$ amb P una $k \times (n - k)$ matriu. Anomenarem matriu generadora amb forma sistemàtica a les matrius generadores d'aquesta forma.

Proposició 3.17. *Sigui C un codi lineal amb matriu generadora amb forma sistemàtica $G = (I_k|P)$, on I_k és la matriu identitat $k \times k$ i P una $k \times (n-k)$ matriu. La matriu*

$$H = \begin{pmatrix} -P \\ I_{n-k} \end{pmatrix}$$

és de control de paritat per a C.

Demostració. Efectuant el producte per blocs $G \cdot H$ tenim:

$$G \cdot H = (I_k|P) \cdot \begin{pmatrix} -P \\ I_{n-k} \end{pmatrix} = I_k \cdot (-P) + P \cdot I_{n-k} = P - P = 0.$$

Com les files de G formen base del conjunt de paraules del codi, tenim doncs que tot l'element c de C verifiquen l'equació $c \cdot H = 0$ com volíem. □

Notació 5. *Ens referirem a un codi lineal de llargada de bloc n, dimensió k i mínima distància d com a un $[n, k, d]$-codi. Per exemple el codi de Hamming previ era un $[7, 4, 3]$-codi.*

Determinar quines triples $[n, k, d]$ es poden triar per tal que existeixi un $[n, k, d]$-codi sobre un cos finit $\mathbb{F}_q$ així com la seva construcció són dos problemes importants en la teoria de codis. La tria del paràmetre k ve donada per la mida de les paraules que apareguin al missatge original. La distància mínima es prendrà en funció del canal de transmissió i la probabilitat que es produeixi un error en aquest. Per tant, prendrem d tal que la probabilitat que una paraula no pugui ser correctament descodificada sigui considerablement baixa. Queda doncs a determinar quan de gran ha de ser n per tal que existeixi el $[n, k, d]$-codi. Podríem per exemple prendre n molt gran i que el conjunt de paraules del codi fos una cadena de copies de la paraula a enviar. Però el codi resultaria poc útil. Buscarem codis tals que la proporció d'informació k/n no sigui massa petita i a més d sigui relativament gran.

Una forma d'intentar produir bons codis és fixar longitud de bloc n i una mínima distància d i aleshores intentar maximitzar k prenent els paraules del codi un per un tals que mantinguin $d(x, y) \geq d$ per a tot parell $x \neq y$.

La següent proposició estudia alguns resultats de $\mathbb{F}_q^n$ per tal de donar condicions d'existència de codis lineals així com una cota superior de la distància mínima.

Proposició 3.18.

1. *El cardinal de les boles de radi $d-1$ centrades als elements del codi $b = |B_{d-1}(c)|$ ve donat per $b = \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$ per a cada $c \in \mathbb{F}_q^n$.*

2. *Sigui d un enter positiu, i sigui $C \subset \mathbb{F}_q^n$ subconjunt (no necessàriament un codi lineal) tal que $d(x, y) \geq d$ per als parells $x \neq y$ a C. Suposem que $\forall\, z \in \mathbb{F}_q^n \backslash C$, $d(z, c) \leq d-1$ per a algun $c \in C$. Aleshores $b \cdot |C| \geq q^n$ amb b com a l'apartat 1. Aquest resultat dona una forma de la cota de Gilbert-Varshmov. Un enunciat equivalent és el següent: si $b \cdot |C| < q^n$, aleshores existeix z tal que tot parell d'elements diferents a $C \cup \{z\}$ estan separats per com a mínim d.*

3. *Si k satisfà $b < q^{n-k+1}$ aleshores existeix un $[n, k, d]$-codi lineal.*

Demostració. 1. $|B_{d-1}(c)|$ són la suma dels diversos elements que difereixen amb c en des de 1 a $d-1$ components. Suposem que difereixen en i components. Aleshores tenim i components diferents i, per tant, $(q-1)^i$ valors que pot prendre cada forat. Finalment falta veure on poden estar aquestes diferencies. Estem buscant en realitat el nombre de permutacions amb repeticions de i components diferents i $n-i$ bones: $P_n^{i,n-i} = \frac{n!}{i!(n-i)!}$. Per tant, si $i \in \{1, ..., d-1\}$ tenim $\frac{n!}{i!(n-i)!}(q-1)^i = \binom{n}{i}(q-1)^i$ valors i aleshores $|B_{d-1}(c)| = \sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i$.

2. Si prenem $c \in C$, tenim que la bola tancada de radi $d-1$ conté b elements de $\mathbb{F}_q^n$. Tots els elements que no hi siguin a la bola seran aquells que es troben a una distància de com a mínim d. Podem doncs estudiar el nombre d'elements que hi ha en totes les boles tancades de radi $d-1$ amb centre els elements de C. Aquest conjunt té com a màxim $b \cdot |C|$ i és aquest valor si les boles són disjuntes. Com tenim $b \cdot |C| < q^n$, ha d'existir algun element de $\mathbb{F}_q^n$ que està fora de les boles. Aquest element es troba a distància de com a mínim d.

3. Farem inducció sobre k dels codis lineals $[n, k, d]$. En el cas $k = 1$ donat que només tenim una paraula del codi i un missatge possible, necessàriament ha de ser el $\langle 0 \rangle = 0$ que és un espai vectorial sobre $\mathbb{F}_q^n$ com volíem. Suposem que existeix $[n, k-1, d]$-codi C. Tenim doncs $|C| = q^{k-1}$ i com $b < q^{n-k+1}$, aleshores $b \cdot |C| = b \cdot q^{k-1} < q^{n-k+1} \cdot q^{k-1} = q^n$. Podem doncs aplicar l'apartat 2 i tenim que existeix $z \in \mathbb{F}_q^n$ tal que $d(c, z) > d$ per a tot $c \in C$. Prenem ara el codi lineal C' generat per C i z. Veiem finalment que C' té distància mínima d. Sigui $ac + bz \in C'$ amb $a, b \in \mathbb{F}_q^n$ i $c \in C$, volem veure que té pes major o igual a d. $wt(ac + bz) = d(ac + bz, 0) = d(ac, -bz) = d(a'c, z) = d(c', z) \geq d$. Hem utilitzat $ac_i \neq bz_i \iff ab^{-1}c_i \neq z_i$ on podem prendre l'invers de b donat que és un element del cos. Com C és espai vectorial, $a'c = c' \in C$ i, per tant, tenim la última desigualtat.

□

Teorema 3.19 (cota de Singleton)**.** *Tot codi lineal verifica $d \leq n-k+1$. Aquest resultat es coneix com a cota de Singleton.*

Demostració. Sigui C un $[n, k, d]$-codi lineal i sigui H una matriu de control de paritat. Aleshores, el rang de la matriu H és $n-k$ i tota combinació de $n-k+1$ files de H és linealment depenent. Siguin $F_1, \ldots, F_{n-k+1}$ les primeres $n-k+1$ files de H i $x_1, \ldots, x_{n-k+1} \in \mathbb{F}_q$ tals que $x_1F_1 + \cdots + x_{n-k+1}H_{n-k+1} = 0$. Aleshores, $x = (x_1, \ldots, x_{n-k+1}, 0, \ldots, 0)$ verifica $xH = x_1F_1 + \cdots + x_{n-k+1}H_{n-k+1} = 0$ i, per tant, x és del codi i $d \leq wt(x) = n-k+1$ □

Definició 3.20. *Direm que un codi amb distància mínima $d = 2t+1$ és perfecte si la unió de les boles de radi t centrades a les paraules del codi és $\mathbb{F}_q^n$.*

Exemple 3.21. El $[7, 4, 3]$-codi de Hamming presentat a l'exemple 3.15 és perfecte, és a dir, Les boles de radi 1 centrades a cada paraula del codi són disjuntes 2 a 2 i cobreixen $\mathbb{F}_2^7$ completament.

Per veure aquest resultat utilitzarem l'apartat 1 de la proposició 3.18 que ens diu $b = |B_{d-1}(c)|$ ve donat per $b = \sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i$ per a cada $c \in \mathbb{F}_q^n$. Tenim doncs que per a cada $c \in C$, $|B_1(c)| = \sum_{i=0}^{1}\binom{7}{i}(2-1)^i = \binom{7}{0}1 + \binom{7}{1}1 = 8 = 2^3$.

Suposem que les boles no són disjuntes, aleshores existeixen $c_1, c_2 \in C$ $x \in \mathbb{F}_2^7$ tals que $d(c_1, x) \leq 1$, $d(c_2, x) \leq 1$ però per la desigualtat triangular tenim $d(c_1, c_2) \leq d(c_1, x) + d(c_2, x) \leq 2$ però la distància mínima és 3.

Tenim doncs que les boles són disjuntes i cadascuna conté 2^3 elements. Per tant, cobreixen $b \cdot |C| = 2^3 2^4 = 2^7$ que és el total d'elements de $\mathbb{F}_2^7$.

Proposició 3.22. *Sigui C un codi lineal i H una matriu de control de paritat del codi. Si no hi ha cap col·lecció de $\delta - 1$ files diferents de H tals que siguin un subconjunt linealment dependent de $\mathbb{F}_q^{n-k}$, aleshores la distància mínima d de C satisfà $d \geq \delta$*

Demostració. Utilitzarem el resultat vist a la proposició 3.14 que caracteritza la distància mínima com a components no nul·les. Sigui $x \in C$ una paraula del codi no nul·la. A partir de l'equació $xH = 0$ a $\mathbb{F}_q^{n-k}$, podem pensar les components de x com a els coeficients en una combinació lineal de les files de H:

$$(x_1 \cdots x_n) \cdot \begin{pmatrix} H_1 \\ \vdots \\ H_n \end{pmatrix} = 0.$$

Com no hi ha cap combinació de $\delta - 1$ files és linealment dependent, aleshores x ha de tenir com a mínim δ components no nul·les i, per tant, $d \geq \delta$. □

3.1.1 Descodificació del síndrome

Passem ara a estudiar una mica més les funcions de codificació. Com hem pogut veure, estudiar la codificació de codis lineals és relativament simple. Només ens cal la matriu generadora del codi i tots els càlculs es poden fer amb àlgebra lineal. En canvi, per a un codi arbitrari C de mida q^k no tenim gaire més alternativa que presentar tot el conjunt de paraules del codi. Per tant, si sabem que el nostre codi és lineal, només cal donar imatge als vectors base de C a diferencia de tot el conjunt de paraules del codi.

El procés de descodificació d'un codi lineal és també més simple. Un mètode comú és el conegut com a descodificació del síndrome. Es basa en la següent observació.

Observació 3.23. Si $c = wG$ és una paraula del codi i $e \in \mathbb{F}_q^n$ un error en la transmissió i el missatge rebut és x=c+e. Aleshores xH només depèn de l'error.

Demostració. Com $c \in C$, $cH = 0$ amb H matriu de control de paritat. Tenim doncs, $xH = (c + e)H = cH + eH = 0 + eH = eH$. Per tant, xH només depèn de l'error. □

Definició 3.24. *Els possibles valors per a $eH \in \mathbb{F}_q^{n-k}$ es coneixen com a síndromes.*

Teorema 3.25. *Sigui C un $[n, k, d]$ codi lineal amb matriu de control de paritat H. Els possibles valors de $yH \in \mathbb{F}_q^{n-k}$ (els síndromes) estan en correspondència un a un amb les classes de C a $\mathbb{F}_q^n$ (o elements del quocient $\mathbb{F}_q^n / C \cong \mathbb{F}_q^{n-k}$). D'aquest fet es deprèn que hi ha q^{n-k} possibles síndromes.*

Demostració. Utilitzarem el teorema d'isomorfia per a anells presentat al corol·lari 2.9. Com H és matriu d'una aplicació lineal, $H : \mathbb{F}_q^n \mapsto \mathbb{F}_q^{n-k}$ que envia $x \to Hx$, té sentit prendre el $ker(H)$. Aquest és, com hem vist, C. Com el rang de H és q^{n-k}, és també aplicació exhaustiva.

Per tant, pel teorema d'isomorfia tenim $\mathbb{F}_q^n/C = \mathbb{F}_q^n/ker(H) \cong im(\mathbb{F}_q^n) = \mathbb{F}_q^{n-k}$. □

El procés de descodificació del síndrome segueix els següents passos. Primer ens cal computar una taula, amb els possibles valors dels síndromes $s = xH$ com a index, dels element/s de la corresponent classe amb el menor nombre de components no nul·les o equivalentment, amb el menor pes.

Definició 3.26. *Els elements de menor pes de cada classe de C a $\mathbb{F}_q^n$ s'anomenen líders de la classe.*

Proposició 3.27. *Sigui $d = 2t + 1$, sabem que podem corregir qualsevol error de pes t o inferior. Si hi ha algun element d'alguna classe de C amb t o menys elements no nuls, aleshores només hi ha un únic element d'aquest tipus i, per tant, el lider de la classe és únic.*

Demostració. Suposem que hi ha dos elements x i y d'una classe donada que tenen t o menys elements no nuls. tenim doncs, $[x] = [y] \cong xH = yH \implies (x - y)H = 0 \iff x - y \in C$. Aleshores $wt(x - y) = d(x, y) \leq d(x, 0) + d(y, 0) = wt(x) + wt(y) \leq t + t = 2t < 2t + 1$. Però la distància mínima és de $2t + 1$ i arribem a contradicció. Per tant, només pot haver un element amb aquestes característiques i el lider de la classe és únic. □

Si rebem $x \in \mathbb{F}_q^n$, computem primer $x = xH$ i busquem el corresponent lider o líders de la classe. Si només hi ha un únic lider, substituïm x per $x' = x - l$. Aquest element x' és de C donat que $x'H = xH - lH \cong [l] - [l] = [0]$ (Per l'isomorfisme construït al teorema 3.25, tenim $lH \cong [l] = l + C$) .

Altrament direm que hi ha un error. Per la proposició 3.13, si no han passat més de t errors a x, hem trobat una única classe de paraules del codi més pròxima x i retornem el veí més pròxim de x'. L'avantatge ha estat que no ens ha calgut calcular la distància de x a tots els q^k elements del codi, només ha aquells de la classe.

Tot i això, encara ens cal molta informació per seguir aquest procediment, en concret la taula dels líders de classe per a cada q^{n-k} classes de C.

Exemple 3.28. Calculem la taula de líders de classe del $[7, 4, 3]$-codi de Hamming donat al exemple 3.15 i utilitzant el procés de descodificació del síndrome, descodifiquem el missatge rebut $(1, 1, 0, 1, 1, 1, 0)$. Recordem que

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

Computem primer les possibles classes. Per l'exemple 3.15, sabem que la distància mínima del codi és 3 i, per tant, tots els errors de pes menor que 1 són líders de classe. En total, tenim $2^{7-4} = 2^3 = 8$ classes al quocient. Tenim que hi ha $P_7^{1,6} = \frac{7!}{1!6!} = 7$ líders de classe de pes 1 i afegint l'element 0 ja tenim els 8 buscats. En definitiva, són:

$$(0,0,0,0,0,0,0),\ (0,0,0,0,0,0,1),\ (0,0,0,0,0,1,0),(0,0,0,0,1,0,0),$$
$$(0,0,0,1,0,0,0),\ (0,0,1,0,0,0,0),\ (0,1,0,0,0,0,0),\ (1,0,0,0,0,0,0).$$

Finalment calculem els síndromes dels líders de classe per tal de classificar-los:

$$\begin{array}{lll} (0,0,0,0,0,0,0) & \to & (0,0,0) \\ (0,0,0,0,0,1,0) & \to & (0,1,0) \\ (0,0,0,1,0,0,0) & \to & (1,1,1) \\ (0,1,0,0,0,0,0) & \to & (1,0,1) \end{array} \qquad \begin{array}{lll} (0,0,0,0,0,0,1) & \to & (0,0,1) \\ (0,0,0,0,1,0,0) & \to & (1,0,0) \\ (0,0,1,0,0,0,0) & \to & (1,1,0) \\ (1,0,0,0,0,0,0) & \to & (0,1,1) \end{array}$$

Passem a descodificar el missatge $(1,1,0,1,1,1,0)$. Busquem primer el síndrome. Com només hi ha un líder de cada classe, trobant el síndrome del missatge rebut podrem descodificar-lo.
$(1,1,0,1,1,1,0)\cdot H = (1,1,1)$.
Aquest es correspon amb el síndrome de $(0,0,0,1,0,0,0)$. Retornem doncs $(0,0,0,1,0,0,0)$ com a missatge corregit.

Exemple 3.29. Donem ara un altre exemple de codi lineal, aquest cop sobre $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle \alpha^2+\alpha+1\rangle$. Sigui C el codi lineal amb $n=8$, $k=3$ sobre $\mathbb{F}_4$ generat per

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}. \tag{3.2}$$

Tot i no tenir la matriu G en forma sistemàtica, podem obtenir-ne una que ho sigui tot fent reducció Gaussiana. Aquest procés correspon a un canvi en la base de C i no modifica la imatge de la funció de codificació E. Aquest procés no és essencial per poder codificar però pot facilitar algunes operacions com veurem més endavant.

Després d'efectuar Gauss-Jordan obtenim la matriu

$$\text{G'}= \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha+1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & \alpha+1 & \alpha \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \end{pmatrix},$$

on hem tingut en consideració que $\alpha^2 = \alpha+1$.

Observant les matrius, podem donar una cota superior de la distància mínima del codi, és a dir, $d \leq 5$. Per donar la distància mínima, però, cal computar els $4^3-1 = 63$ elements no nuls del codi i obtenim $d=5$.

Quan el nombre de paraules del codi no nul·les q^k-1 és gran, el càlcul de la distància mínima és dificulta considerablement. Podem però donar una cota inferior de la distància mínima per poder tenir millor idea de com es aquesta.

3.2 Codis duals

Definició 3.30. *Considerem el producte formal intern a $\mathbb{F}_q^n$ definit per:*

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i.$$

(Una aplicació bilineal simètrica de $\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ sense considerar la noció de ser positiu en el nostre cas). Donat un codi C, definim:

$$C^\perp = \{x \in \mathbb{F}_q^n \quad | \quad \langle x, y\rangle = 0 \quad \forall\, y \in C\}$$

el subespai ortogonal a C que viu a $\mathbb{F}_q^n$.

Observació 3.31. Si C és de dimensió k, aleshores $C^\perp$ és un codi lineal de llargada de bloc n i dimensió $n-k$ anomenat codi dual de C.

Proposició 3.32. *Sigui G la matriu generadora d'un codi lineal C, podem prendre com a matriu generadora de $C^\perp$ la matriu $G' = H^t$ on H és una matriu de control de paritat del codi C.*

Demostració. Les files de G generen C. Si busquem elements ortogonals a les files de G, l'espai generat per aquests elements serà ortogonal a C. Podem prendre com a matriu generadora G' del codi dual qualsevol matriu de dimensió $(n-k)\times n$ i rang $n-k$ verificant $G \cdot G'^t = 0_{k\times n-k}$. Observem que les matrius de control de paritat verifiquen les condicions necessàries per ser la transposada de les matrius generadores de codis duals. □

Observació 3.33. Sigui $G = (I_k|P_{k\times n-k})$ la matriu d'un codificador sistemàtic C. Per la proposició 3.17 tenim com a matriu de paritat de C

$$H = \begin{pmatrix} -P \\ I_{n-k} \end{pmatrix}.$$

Per tant, $G' = H^t$ és matriu generadora del codi dual.

Notació 6. *Nota de terminologia: alguns textos sobre teoria de codis defineixen la matriu de control de paritat H d'un codi lineal com la transposada de la que hem definit en aquest text. D'aquesta forma, les files de la matriu H formen una base del codi dual de C.*

Exemple 3.34. Trobem matrius generadores i determinem els paràmetres $[n, k, d]$ dels duals dels dos codis generats per les matrius (3.1) i (3.2).

- El $[7, 4, 3]$-codi de Hamming té per matriu generadora:

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

  Hem vist prèviament que podem prendre com a matriu de control de paritat:

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

Així doncs,

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

és matriu generadora del codi dual.

- Podem prendre per matriu generadora:

$$G = (I_3|P) = \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha & \alpha+1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & \alpha+1 & \alpha \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \end{pmatrix}.$$

Podem aplicar l'apartat previ i tenim com a matriu generadora del codi dual H^t amb

$$H = \begin{pmatrix} -P \\ I_5 \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha+1 & 1 & 0 \\ 1 & 1 & 0 & \alpha+1 & \alpha \\ 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

3.3 Codis de Hamming

Definició 3.35. *Sigui q una potencia d'un primer i $m \geq 1$. Anomenarem a un conjunt S de vectors a $\mathbb{F}_q^m$ subconjunt maximal linealment independent per parells si S té la propietat que cap parell d'elements diferents de S són múltiples escalars entre ells i, a més, és maximal respecte l'inclusió.*

Proposició 3.36. *Si S és subconjunt maximal linealment independent per parells de $\mathbb{F}_q^m$, aleshores S té exactament $(q^m-1)/(q-1)$ elements. (Que són exactament el nombre de punts de l'espai projectiu $\mathbb{P}^{m-1}$ sobre $\mathbb{F}_q$).*

Demostració. Definim la relació $x \sim y \iff \exists\, \lambda \in \mathbb{F}_q^* \quad tal\ que \quad x = \lambda \cdot y$. Aplicarem el teorema de Lagrange per veure el resultat. Veiem primer que la relació definida és d'equivalència:

- $x \sim x$: prenent $1 \in \mathbb{F}_q$ tenim $x = 1 \cdot x$.
- $x \sim y \iff y \sim x$: $x \sim y \implies \exists\, \lambda \in \mathbb{F}_q^*$ tal que $x = \lambda \cdot y$. Com $\mathbb{F}_q$ és cos, l'element λ és invertible i, per tant, $\lambda^{-1} \cdot x = y$ i $y \sim x$.
- $x \sim y$, $y \sim z \implies x \sim z$: $x \sim y \implies \exists \lambda \in \mathbb{F}_q^*$ tal que $x = \lambda \cdot y$, $y \sim z \implies \exists \mu \in \mathbb{F}_q^*$ tal que $y = \mu \cdot z$. Per tant, $x = \lambda \cdot y$ i $y = \mu \cdot z$ i, aleshores, $x = \lambda \cdot \mu \cdot z \implies x \sim z$.

Tenim doncs que la relació definida és d'equivalència. Notem que per definició de S aquest és ${\mathbb{F}_q^m}^*/\sim$, on hem hagut de treure l'element nul de $\mathbb{F}_q^m$ donat que tots els elements estan relacionat amb aquest i, per tant, no pot estar en S. Passem a veure quants elements té cada conjunt de la relació d'equivalència. El nombre d'elements de $\mathbb{F}_q^*$ és $q-1$. Donat un element $x \in \mathbb{F}_q^m$ tenim doncs $q-1$ elements relacionats amb aquest, incloent el propi x. Per tant, cada classe conté $q-1$ elements. També sabem que $\mathbb{F}_q^{m^*}$ té q^m-1 elements i, per tant, pel teorema de Lagrange, sabem que el conjunt $S = {\mathbb{F}_q^m}^*/\sim$ té $(q^m-1)/(q-1)$ elements.

□

Observació 3.37. Com les files de H han de formar un subconjunt maximal linealment independent per parells, necessàriament s'ha de complir $n = (q^m-1)/(q-1)$.

Observació 3.38. Per cada parell (q,m) podem construir un codi lineal C prenent una matriu de control de paritat $H \in M_{n\times m}(\mathbb{F}_q)$ tal que les seves files formin un subconjunt de $\mathbb{F}_q^m$ maximal linealment independent per parells i prenent com a $C \subset \mathbb{F}_q^n$ el conjunt de solucions del sistema lineal d'equacions $xH = 0$.

Definició 3.39. *Anomenarem codis de Hamming als codis obtinguts mitjançant el procés descrit a l'observació 3.38.*

Proposició 3.40. *Els codis de Hamming descrits per una $n \times m$ matriu de control de paritat H és de dimensió $k = n - m$ i longitud de bloc n.*

Demostració. Sabem que el nostre codi C té com a matriu de control de paritat H. A la proposició 3.32 hem vist que H^t és matriu generadora del codi dual de C. Per tant, el codi $C^\perp$ té longitud de bloc n i dimensió m. A més ${C^\perp}^\perp = C$ i, per tant, el codi C té longitud de bloc n i dimensió $k = n - m$. □

Proposició 3.41. *La distància mínima d'un codi de Hamming és sempre 3. Tenim doncs que podem detectar qualsevol error de pes com a màxim 2 i corregir qualsevol error de pes 1.*

Demostració. Com les files formen un conjunt maximal linealment independent per parells, cap parell de files són dependents. Per tant, prenent $2 = \delta - 1$ tenim que, per la proposició 3.22, la distància mínima verifica $d \geq 3$.

Com les files de H formen un sistema maximal linealment independent per parelles, donades tres files qualssevol, existeixen $x_1, x_2, x_3 \in \mathbb{F}_q$ diferents de zero tals que $X_1F_1 + x_2F_2 + x_3F_3 = 0$, on F_i representa la fila i de la matriu H. Si no fos així, el vector $x_1F_1 + x_2F_2$ seria linealment independent a totes les files de H i, per tant, les files de H no formarien un sistema maximal respecte la inclusió. A més, ha de ser linealment depenent a una fila diferent de F_1 i F_2 donat que si no, F_1 i F_2 no serien linealment independents.

Prenent doncs el vector $x = (x_1, x_2, x_3, 0, \ldots, 0) \in \mathbb{F}_q^n$ aquest verifica $xH = x_1F_1 + x_2F_2 + x_3F_3 = 0$ i és, per tant, del codi. Com x té pes 3, la distància mínima és $d \leq 3$.

Agrupant les dues desigualtats arribem al resultat $d = 3$. □

Proposició 3.42. *Els codis de Hamming són perfectes.*

Demostració. Seguirem els mateixos raonaments que al exercici 3.21. Veiem primer que les boles de radi 1 són disjuntes i, seguidament, que cobreix tot $\mathbb{F}_q^n$. Suposem que no són disjuntes, aleshores existeixen $c_1, c_2 \in C$ $x \in \mathbb{F}_q^n$ tals que $d(c_1, x) \leq 1$, $d(c_2, x) \leq 1$ però per la desigualtat triangular tenim $d(c_1, c_2) \leq d(c_1, x) + d(c_2, x) \leq 2$ però la distància mínima és 3. Per la proposició 3.18 sabem que cada bola de radi 1 centrades $x \in C$ conté $|B_1(x)| = \sum_{i=0}^{1} \binom{n}{i}(q-1)^i = 1+n\cdot(q-1)$ elements. Per tant, les boles de radi 1 centrades en punts de C cobreixen

$$|C|\cdot|B_1(x)| = q^k\cdot(1+n\cdot(q-1)) = q^k\cdot(1+((q^{n-k}-1)/(q-1))\cdot(q-1)) = q^k\cdot q^{n-k} = q^n.$$

□

Exemple 3.43. Donem ara una matriu de control paritat per a $q = 3$, $k = 2$.

Per la proposició 3.40 i 3.37, tenim que $k = n - m$ i $n = (q^m - 1)/(q - 1)$. En el nostre cas, $n = (3^m - 1)/2$ i $2 = n - m$. Agrupant aquestes dues equacions obtenim que s'ha de verificar $5 + 2m = 3^m$, que té com solució $m = 2$ i $n = 4$. Construïm ara una matriu de control de paritat $H_{4\times 2}$ tal que les seves files siguin un conjunt maximal linealment independent per parelles.

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

on α és element primitiu de $\mathbb{F}_3$. Aquesta matriu és de rang 3 i verifica la condició que cap fila és múltiple d'una altra i a més qualsevol subconjunt de 3 files no és linealment independent.

Observació 3.44. Si $q = 2$, podem prendre com a files de H tots els vectors no nuls de $\mathbb{F}_2^k$ donat que aquest formen un conjunt maximal linealment independent per parelles.

4 Codis cíclics

Considerarem ara més classes de conjunts de codis lineals amb noves estructures i veurem com podem aplicar les eines estudiades a les altres seccions per operar aquest codis. El primer que considerarem són els codis cíclics.

Definició 4.1. *Donat un vector* $(a_0, \cdots, a_{n-1}, a_n) \in \mathbb{F}_q^n$ *definim la permutació cíclica* $\pi : (a_0, \cdots, a_{n-1}, a_n) \longrightarrow (a_n, a_0, \cdots, a_{n-1})$.

Definició 4.2. *Un codi cíclic és un codi lineal tal que el conjunt de paraules del codi és tancat per a la permutació* π.

Observació 4.3. Com tota permutació cíclica es pot escriure com a composicions successives de π, ser cíclic és equivalent a ser tancat per a tota permutació cíclica de tots els elements.

Exemple 4.4. A $\mathbb{F}_2^3$ considerem el codi lineal C amb matriu generadora

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Vegem que es tracta d'un codi cíclic. Els elements del codi són les imatges dels vectors de $\mathbb{F}_2^2$ i, per tant, $C = \{(0,0,0),(0,1,1),(1,1,0),(1,0,1)\}$. Aquest conjunt és tancat respecte π i és doncs un codi cíclic.

Si prenem l'isomorfisme estàndard entre $\mathbb{F}_q^n$ i l'espai de polinomis de grau com a molt $n-1$ amb coeficients a $\mathbb{F}_q$ donat per:

$$(a_0, a_1, \cdots, a_{n-1}) \longleftrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

aleshores, podem identificar un codi cíclic C amb la corresponent col·lecció de polinomis.

Hi ha diverses formes de representar l'espai de polinomis de $\mathbb{F}_q[x]$ de grau com a molt $n-1$ però el següent resultat ens pot ajudar a decidir quina representació pot ser-nos útil per facilitar els càlculs.

Proposició 4.5. *Multiplicar el polinomi $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ per x, i després prendre el residu de la divisió per $x^n - 1$ dona un polinomi tal que els coeficients són els mateixos que els de $p(x)$ però cíclicament desplaçats una posició cap a la dreta.*

Demostració. $x \cdot p(x) = a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n$. efectuant la divisió respecte $x^n - 1$ obtenim:

$$x \cdot p(x) = a_{n-1}(x^n - 1) + a_{n-1} + a_0 x + \cdots + a_{n-2}x^{n-1},$$

i prenent mòdul $x^n - 1$ tenim el resultat buscat. □

Aquesta propietat ens permet caracteritzar els codis cíclics donat que tot cicle el podrem escriure com a composicions d'aquest. En treballar amb codis cíclics considerarem els polinomis de grau com a molt $n-1$ com els elements de l'anell quocient $R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^n - 1\rangle}$. D'aquesta forma, els codis cíclics seran els subespais vectorials de l'anell R tancats sota la multiplicació per $[x]$ a R.

Proposició 4.6. *Si un subespai $C \subseteq R$ és tancat sota la multiplicació per $[x]$, aleshores és tancar sota la multiplicació per tota classe $[h(x)] \in R$.*

Demostració. Suposem que $[h(x)] = [\sum_{i=0}^{n-1} a_i x^i]$, $a_i \in \mathbb{F}_q \quad \forall\, i \in \{0, \cdots, n-1\}$. Sigui $[p(x)] \in C$. Aleshores, $[h(x)] \cdot [p(x)] = [h(x) \cdot p(x)] = [\sum_{i=0}^{n-1} a_i x^i p(x)] = \sum_{i=0}^{n-1} a_i [x^i p(x)]$. Com C és tancat pel producte per $[x]$, $[x^i p(x)] \in C$ per a tota i. Com és espai vectorial, aquesta combinació lineal d'elements de C també és de C. En conclusió, el producte $[h(x)] \cdot [p(x)]$ pertany a C. □

Proposició 4.7. *Un subespai vectorial $C \subseteq R$ és un codi cíclic si i només si C és un ideal de l'anell R.*

Demostració.

- $\Rightarrow\rfloor$ Suposem C és codi cíclic. Veiem que és un ideal. Com C és espai vectorial, és tancat per a la suma d'elements del propi codi. A més, hem vist que l'espai C és tancat també per a la multiplicació sota $[h(x)] \in R$. Per tant, C és un ideal.

- $\Leftarrow\rfloor$ Suposem C ideal de R. Volem veure que és tancat per a permutacions, és a dir, tancat per la multiplicació per $[x]$ a R però, com C és ideal, aquest producte sempre serà un element de C.

□

Proposició 4.8. *Cada ideal $I \subseteq R$ és principal, generat per la classe d'un únic element f de grau $n-1$ o menys. Encara més, f és divisor de $x^n - 1$.*

Demostració. Tal com hem vist al lema 2.14, hi ha una correspondència bijectiva entre els conjunts

$$\{\text{ideals que contenen } \langle x^n - 1\rangle\} \longleftrightarrow \{\text{ideals de } R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^n - 1\rangle}\}$$

Sigui I un ideal de R. Aleshores $\exists\, J \in \mathbb{F}_q[x]$ que està en correspondència amb l'ideal I. Com J és un ideal d'un domini d'ideals principals (lema 2.10), $\exists\, f \in \mathbb{F}_q[x]$ tal que $\langle f\rangle = J$. A més, $\langle x^n - 1\rangle \subseteq J = \langle f\rangle \implies f | x^n - 1$.

Tenim doncs que l'ideal és $I = {}^{J}\!/_{\langle x^n - 1\rangle}$ està generat per la classe de f. □

Definició 4.9. *Sigui C un codi cíclic. Anomenarem polinomi generador del codi C al polinomi f tal que $C = \langle f\rangle$. La seva existència és clara per la proposició 4.8.*

Exemple 4.10. Identificant les 4-tuples $(a, b, c, d) \in \mathbb{F}_2^4$ amb $[a + bx + cx^2 + dx^3] \in R = {}^{\mathbb{F}_2[x]}\!/_{\langle x^4 - 1\rangle}$, demostrem que el codi cíclic a $\mathbb{F}_2^4$ amb matriu generadora

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

el podem pensar com l'ideal generat per la classe de $f = 1 + x^2$ a R.

Avaluant en G obtenim que el codi és $C = \{(1,1,1,1), (0,0,0,0), (1,0,1,0), (0,1,0,1)\}$. Aquest és poden identificar amb els elements de R pel morfisme:

$$(a_0, \cdots, a_{n-1}) \longmapsto a_0 + \cdots + a_{n-1}x^{n-1}$$

Tenim doncs a R l'espai vectorial format pels elements

$$J = \{[0], [1 + x^2], [x + x^3], [1 + x + x^2 + x^3]\}.$$

Notem que aquest conjunt és tancat pel producte per $[x]$:

$[x] \cdot [0] = [0]$;

$[x] \cdot [1 + x^2] = [x + x^3]$;

$[x] \cdot [x + x^3] = [x^2 + x^4] = [1 + x^2]$;

$[x] \cdot [1 + x + x^2 + x^3] = [x + x^2 + x^3 + x^4] = [1 + x + x^2 + x^3]$.

Donem l'element generador de l'ideal. Notem que $1 + x^2$ divideix a la resta d'elements i, per tant, tots pertanyen a l'ideal $\langle 1 + x^2\rangle$, és a dir, $J \subseteq \langle 1 + x^2\rangle$. Com l'altre inclusió és immediata, $J = \langle 1 + x^2\rangle$. A més també veiem que es verifica que $x^2 + 1$ divideix $x^4 - 1$ tal com enunciàvem a la proposició 4.8.

Exemple 4.11. Prenem una altra vegada $R = {}^{\mathbb{F}_2[x]}\!/_{\langle x^4-1\rangle}$, trobem els paraules del codi del codi cíclic generat per $1+x$ a R.

Els elements de R són:

$$\begin{array}{cccc} [0] & [1] & [x] & [x+1] \\ [x^2] & [x^2+1] & [x^2+x] & [x^2+x+1] \\ [x^3] & [x^3+1] & [x^3+x] & [x^3+x^2] \\ [x^3+x^2+1] & [x^3+x^2+x] & [x^3+x+1] & [x^3+x^2+x+1] \end{array}$$

Efectuem el producte per $x+1$ i prenem residu respecte x^4-1 i obtenim respectivament els elements:

$$\begin{array}{cccc} [0] & [x+1] & [x^2+x] & [x^2+1] \\ [x^3+x^2] & [x^3+x] & [x^3+x^2+x+1] & [x^3+1] \\ [x^3+1] & [x^2+x+1] & [x^2+1] & [x^3+x] \\ [x+1] & [x^2+x] & [x^3+x^2] & [0] \end{array}$$

que és equivalent al conjunt

$$\{[0],[x+1],[x^2+1],[x^2+x],[x^2+x+1],[x^3+1],[x^3+x],[x^3+x^2],[x^3+x^2+x+1]\}.$$

4.1 Codis de Reed-Solomon

Estudiarem ara un subconjunt dels codis cíclics anomenats codis de Reed-Solomon. Definirem els codis de Reed-Solomon a partir de les matrius generadores i seguidament veurem que són cíclics veient la invariància sota cicles.

En aquesta secció considerarem $\alpha \in \mathbb{F}_q$ element primitiu del cos finit $\mathbb{F}_q$ i $n = q-1$.

Definició 4.12. *Definim*

$$L_{k-1} = \{\textstyle\sum_{i=0}^{k-1} a_i t^i \quad | \quad a_i \in \mathbb{F}_q\}$$

l'espai vectorial de polinomis de grau com a molt $k-1$ a $\mathbb{F}_q[t]$.

Definició 4.13. *Sigui $k \geq 1$, definim el codi de Reed-Solomon $RS(q,k)$ com el conjunt*

$$C = \{(f(1), \cdots, f(\alpha^{q-2})) \quad | \quad f \in L_{k-1}\}.$$

Les paraules del codi seran aleshores avaluar els diferents polinomis L_{k-1} als $q-1$ elements no nuls de F_q.

Observació 4.14. Notem que C és espai vectorial donat que és imatge d'un espai vectorial per una aplicació lineal.

Observació 4.15. Per donar una matriu generadora de C només cal prendre l'imatge d'una base de L_{k-1}, és a dir, avaluar la base en els diferents elements de $\mathbb{F}_q$. La base més simple per a L_{k-1} és $\{1, t, t^2, \cdots, t^{k-1}\}$.

Exemple 4.16. Sigui $\mathbb{F}_4$, $n = 3$ i $k = 2$. Sigui $\alpha \in \mathbb{F}_4$ element primitiu. Aleshores una base de L_2 és $\{1, t\}$ i la matriu generadora del codi RS(3,4) és

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}.$$

Prenent la matriu generadora en funció de la base de monomis de L_2 ens ajuda a visualitzar la propietat d'invariància per a cicles. Per exemple, la permutació resultant de moure cap a la dreta cada component de la segona fila és equivalent a multiplicar aquesta per l'escalar α^2. Notem doncs, que qualsevol cicle és equivalent a prendre el producte per un escalar.

Observació 4.17. En general, la matriu del codi $RS(k, q)$ respecte la base de monomis de L_{k-1} és de la forma:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2n-2} \\ & & \vdots & & \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{n(k-1)} \end{pmatrix}.$$

Proposició 4.18 (matriu de Vandermonde i el seu determinant)**.** *(Corol·lari 2.37 de [Kna07]). Sigui R anell. Donats $r_1, \cdots, r_n \in R$, aleshores:*

$$det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ r_1^2 & r_2^2 & \cdots & r_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \cdots & r_n^{n-1} \end{pmatrix} = \prod_{j>i}(r_j - r_i).$$

Proposició 4.19. *El $RS(k, q)$ codi té dimensió k.*

Demostració. Notem que les primeres k columnes formen una matriu de Vandermonde amb determinant $\prod_{j>i}(\alpha^j - \alpha^i)$ i aquest és no nul. Per tant, el rang de la matriu generadora del codi $RS(k, q)$ és k.

□

Proposició 4.20. *La permutació cíclica $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ que envia $(a_0, a_1, \cdots, a_{n-1}) \longmapsto (a_{n-1}, a_0, \cdots, a_{n-2})$ és una aplicació lineal.*

Demostració. Veiem les propietats d'aplicació lineal:

- Siguin $a, b \in \mathbb{F}_q^n$;
  $\pi(a + b) = \pi(a_0 + b_0, a_1 + b_1, \cdots, a_{n-1} + b_{n-1}) = (a_{n-1} + b_{n-1}, a_0 + b_0, \cdots, a_{n-2} + b_{n-2}) = (a_{n-1}, a_0, \cdots, a_{n-2}) + (b_{n-1}, b_0, \cdots, b_{n-2}) = \pi(a) + \pi(b)$.
- Siguin $\lambda \in \mathbb{F}_q, a \in \mathbb{F}_q^n$;
  $\pi(\lambda \cdot a) = \pi(\lambda a_0, \lambda a_1, \cdots, \lambda a_{n-1}) = (\lambda a_{n-1}, \lambda a_0, \cdots, \lambda a_{n-2}) = \lambda \cdot (a_{n-1}, a_0, \cdots, a_{n-2}) = \lambda \cdot \pi(a)$.

□

Observació 4.21. Notem que desplaçar una posició les components de la fila i-èssima és equivalent a multiplicar la pròpia fila per l'escalar α^{i-1} ja que $\alpha^{q-1} = 1$. Aquest fet es desprèn del teorema 2.32 prenent $n = q - 1$. Com π és pot escriure com a composicions successives d'aquesta aplicació, π també verificarà aquesta propietat.

Teorema 4.22. *El codi lineal $RS(k, q)$ és un codi cíclic.*

Demostració. Veurem que donat $c \in RS(k, q)$, aleshores $\pi(c) \in RS(k, q)$. Siguin $e_1, \cdots, e_n$ les files de la matriu generadora en la base $\{1, t, t^2, \cdots, t^{n-1}\}$. Sabem que aquestes files són generadores de l'espai vectorial $RS(k, q)$ i alhora verifiquen que $\pi(e_i) = \lambda_i e_i$ per a algun $\lambda_i \in \mathbb{F}_q$. Com que $c \in RS(k, q)$, llavors $\exists\, \beta_1, \cdots, \beta_n \in \mathbb{F}_q$ tals que $c = \beta_1 e_1 + \cdots + \beta_n e_n$. Per tant, $\pi(c) = \pi(\beta_1 e_1 + \cdots + \beta_n e_n) = \beta_1 \pi(e_1) + \cdots + \beta_n \pi(e_n) = \beta_1 \lambda_1 e_1 + \cdots + \beta_n \lambda_n e_n$. Com $\pi(c)$ és combinació lineal dels generadors de C, $\pi(c) \in RS(k, q)$. Per tant, el codi $RS(k, q)$ és invariant per al cicle π i és doncs un codi cíclic.

□

Exemple 4.23. Sigui

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix}$$

matriu generadora del codi de Reed-Solomon $RS(3, 9)$ respecte la base $\{1, t, t^2\}$. Veiem que les files de G tenen la propietat que les transformacions cícliques de qualsevol fila són equivalents a multiplicar per un escalar la pròpia fila i, en conseqüència, és cíclic.

Per a cada fila, veurem que moure una posició a l'esquerra és equivalent a multiplicar per un escalar i, com tot cicle es pot escriure com a composició successiva d'aquest, el codi serà cíclic. Per a la primera fila aquest escalar és 1, per a la segona és α i per a la última, com $\alpha^8 = 1$ (teorema 2.32), l'escalar és α^2.

Definició 4.24. *Donat un codi lineal C direm que té distància màxima separable (MDS) si $d = n - k + 1$, és a dir, si assoleix la cota superior $d \leq n - k + 1$ presentada a la proposició 3.18.*

Proposició 4.25. *Els codis de Reed-Solomon són codis que tenen distància màxima separable.*

Demostració. Com $n = q - 1$, $d \leq q - k$. Per altra banda, els elements del codi són per construcció de la forma $(f(1), \cdots, f(\alpha^{q-2}))$ amb $f \in L_{k-1}$. Si una paraula del codi té k o més components nul·les, aleshores $\exists\, f \in L_{k-1}$ tal que s'anul·la per a k o més elements, però els polinomis de grau com a molt $k - 1$ tenen com a màxim $k - 1$ arrels. Per tant, aquest polinomi ha de ser el nul. Tenim llavors que tot element diferent del zero té menys de k zeros i, per tant, $wt(c) \geq (q - 1) - (k - 1) = q - k$. Per la proposició 3.14, tenim $d \geq q - k$ i, en conclusió, $d = q - k$. □

4.1.1 Polinomi generador d'un codi de Reed-Solomon

Fins ara hem vist com definir el codis $RS(k, q)$ tot trobant la matriu generadora, veiem ara com definir-lo a partir del polinomi generador f.

Observació 4.26. De la proposició 4.8 sabem que el polinomi generador f ha de ser divisor de $x^n - 1$. En el nostre cas $f \mid x^{q-1} - 1$. Per la proposició 2.39 sabem que el polinomi $x^{q-1} - 1$ descompon en factors lineals a $\mathbb{F}_q[x]$, és a dir,

$$x^{q-1} - 1 = \prod_{\beta \in \mathbb{F}_q^*} (x - \beta).$$

Per tant, el polinomi generador ha de ser de la forma $\prod_{\beta \in S}(x-\beta)$ per a un subconjunt $S \subseteq \mathbb{F}_q^*$.

Lema 4.27. *Sigui $I = \langle g \rangle$ ideal a $R = {}^{F_q[x]}\!/_{\langle x^n - 1 \rangle}$. Si $gr(g) = l$ llavors I té dimensió $n - l$ com a $\mathbb{F}_q$ espai vectorial. És més,*

$$I = \langle g \rangle = \{r \cdot g \mid gr(r) < n - l\}.$$

Demostració. Com $g | x^n - 1 \implies \exists\, h \in \mathbb{F}_q[x]$ tal que $x^n - 1 = g \cdot h$ i $gr(h) = n - l$. Els elements de I són de la forma $f \cdot g$ amb $f \in R$, passem a veure que la classe $[f \cdot g]$ és la mateixa a una classe $[r \cdot g]$ amb $gr(r) < n - l$. si $gr(f) < n - l$ llavors prenent $r = f$ acabem. Suposem doncs $gr(f) \geq n - l$. Aleshores podem efectuar la divisió euclidiana respecte h, $f = q \cdot h + r$ amb $q, r \in R$ i $gr(r) < n - l$. Multiplicant per g obtenim $f \cdot g = q \cdot h \cdot g + r \cdot g = r \cdot g$.

Notem ara que el conjunt $\{r \cdot g \mid gr(r) < n - l\}$ és pot generar amb el conjunt $\{g, x \cdot g, x^2 \cdot g, \cdots, x^{n-l-1} \cdot g\}$ com a $\mathbb{F}_q$ espai vectorial. A més, els elements del conjunt són linealment independents. En conclusió, I com a $\mathbb{F}_q$ espai vectorial és de dimensió $n - l$. □

Proposició 4.28. *Un codi lineal de dimensió k a $R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^{q-1} - 1 \rangle}$ és cíclic si i només si les paraules del codi, vistes com a polinomis de grau com a molt $q - 2$, tenen algun conjunt S de $q-k-1$ arrels comunes a $\mathbb{F}_q^*$. Notem que si les paraules del codi tenen els elements de S com a arrels, aleshores cada paraula és divisible per $g(x) = \prod_{\beta \in S}(x-\beta)$ amb $gr(g) = q - k - 1$.*

Demostració.

- $\Rightarrow\rfloor$ Suposem que C és un codi cíclic de dimensió k a $R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^{q-1} - 1 \rangle}$. Per la propsosició 4.7 i 4.8, C és un ideal principal de l'anell R i, a més, el polinomi generador és un divisor de $x^{q-1} - 1$. Acabem de veure a l'observació 4.26 que aquest polinomi descompon en factors lineals $x^{q-1} - 1 = \prod_{\beta \in \mathbb{F}_q^*}(x - \beta)$. Per tant, $f \mid \prod_{\beta \in \mathbb{F}_q^*}(x - \beta) \implies f = \prod_{\beta \in S}(x - \beta)$ amb $S \subseteq \mathbb{F}_q^*$. Volem veure que el grau de f ha de ser $q - k - 1$. Suposem que $gr(f) = r \neq q - k - 1$, aleshores, pel lema 4.27, el codi té dimensió $q - 1 - r = k$ i necessàriament $r = q - 1 - k$. Per tant, $gr(f) = q - k - 1$.

- $\Leftarrow\rfloor$ Suposem C un codi lineal tal que tots els elements són divisibles per $g = \prod_{\beta \in S}(x-\beta)$ per un $S \subset \mathbb{F}_q$ conjunt de $q-k-1$ elements. Sigui $f \in C \implies g | f \implies f \in \langle g \rangle \implies C \subseteq \langle g \rangle$. Acabem de veure que aquest codi coincideix amb el codi cíclic amb polinomi generador g tot veient que $g \in C$. Pel lema 4.27, el codi $\langle g \rangle$ té dimensió k, per tant, tenim $dim C = dim \langle g \rangle$ com a $\mathbb{F}_q$ espais vectorials i alhora $C \subseteq \langle g \rangle$. Aleshores, podem prendre la mateixa base d'elements $\{p_1, \cdots, p_k\}$ per generar tant C com $\langle g \rangle$. Com $g \in \langle g \rangle$, $\exists \lambda_1, \cdots, \lambda_k \in \mathbb{F}_q$ tal que $g = \lambda_1 p_1 + \cdots + \lambda_k p_k$.

Hem escrit doncs g com a combinació lineal d'elements de C i al ser C espai vectorial, $g \in C$.

□

Tenim ara eines per poder trobar el polinomi generador d'un codi $RS(k,q)$.

Proposició 4.29. *Sigui $\mathbb{F}_q$ un cos finit i $k \geq 1$, el codi $RS(k,q)$ és de la forma:*

$$g = (x-\alpha)\cdots(x-\alpha^{q-k-1}) = (x-\alpha)\cdots(x-\alpha^{d-1}).$$

on α és element primitiu de $\mathbb{F}_q^*$.

Demostració. Sigui $f(t) = \sum_{i=0}^{k-1} a_j t^j \in L_{k-1}$, una paraula del codi es pot prendre com el polinomi $c(x) = \sum_{i=0}^{q-2} c_i x^i$ on $c_i = f(\alpha^i)$ per a $i = 0, \cdots, k-1$. Suposem $1 \leq l \leq q-k-1$, aleshores:

$$c(\alpha^l) = \sum_{i=0}^{q-2} c_i(\alpha^l)^i = \sum_{i=0}^{q-2}(\sum_{j=0}^{k-1} a_j(\alpha^i)^j)\alpha^l i = \sum_{j=0}^{k-1} a_j(\sum_{i=0}^{q-2}\alpha^{i(l+j)}).$$

Per lema 2.45, tenim $\sum_{j=0}^{p^n-2} \beta^j = 0$ si $\beta \in \mathbb{F}_{p^n}$. Per tant, el sumatori interior és zero i $c(\alpha^l) = 0$. Hem trobat doncs un conjunt $S = \{\alpha, \alpha^2, \cdots, \alpha^{q-k-1}\}$ de $q-k-1$ elements d'arrels comunes i, per tant, el codi lineal $RK(k,q)$ de dimensió k, tal com hem vist a la proposició 4.28, és un codi cíclic. A més, hem vist que el polinomi $\prod_{\beta\in S}(x-\beta)$ és el polinomi generador del codi cíclic i en el cas dels codis de Reed-Solomon tenim a més la igualtat $d = q-k = n-k+1$. En conseqüència

$$g = (x-\alpha)\cdots(x-\alpha^{q-k-1}) = (x-\alpha)\cdots(x-\alpha^{d-1}).$$

□

4.2 Algoritme de descodificació de Reed-Solomon

En aquesta secció considerarem $R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^{q-1}-1\rangle}$, $C \subset R$ un $RS(k,q)$ codi de Reed-Solomon amb polinomi generador $g = (x-\alpha)\cdots(x-\alpha^{d-1})$ i, per tant, $C = \langle g\rangle$. Recordem també $d = q-k$. Per simplificar prendrem $d = 2t+1$. En cas contrari treballaríem amb $t = \lfloor d/2\rfloor - 1$.

L'objectiu d'aquesta secció és donar eines per saber identificar si s'ha produït un error de pes com a màxim t i poder corregir-lo per tal de poder descodificar el missatge rebut. És a dir, donat una paraula del codi $c = \sum_{j=0}^{q-2} c_j x^j \in C$ i suposem que es produeix un error $e = \sum_{i\in I} e_i x^i$, l'objectiu serà, rebut un missatge $y = c+e$, retornar $E^{-1}(y-e)$ Anomenarem ubicacions de l'error al conjunt I i valors de l'error als coeficients e_i.

Com g és divisor de tota paraula del codi, podrem utilitzar les arrels d'aquest per tal d'obtenir informació de l'error. D'aquesta forma, els escalars $E_j = y(\alpha^j)$, $j = 1, \cdots d-1$ només dependran de l'error: $E_j = y(\alpha^j) = c(\alpha^j) + e(\alpha^j) = e(\alpha^j)$ donat que $g|c \implies c(\alpha^j) = 0$ per a $j = 1, \cdots, d-1$.

Definició 4.30. *Definim el síndrome polinomial com el polinomi*

$$S(x) = \sum_{j=1}^{d-1} E_j x^{j-1}.$$

Notem que aquest polinomi és de grau com a molt $d-2$.

Si estenem la definició de E_j *per a tot* j*, podem definir també el polinomi*

$$E(x) = \sum_{j=1}^{\infty} E_j x^{j-1}.$$

Notem que els coeficients de E *són periòdics de període com a molt* q *donat que* $\alpha^q = \alpha$.

Suposem $e(x) = \sum_{i\in I} e_i x^i$, aleshores $E_j = \sum_{i\in I} e_i(\alpha^j)^i = \sum_{i\in I} e_i(\alpha^i)^j$.

$$E(x) = \sum_{j=1}^{\infty} E_j x^{j-1} = \sum_{j=1}^{\infty}\sum_{i\in I} e_i(\alpha^i)^j x^{j-1} = \sum_{i\in I}\sum_{j=1}^{\infty} e_i(\alpha^i)^j x^{j-1} = \sum_{i\in I}\sum_{k=0}^{\infty} e_i(\alpha^i)^{k+1} x^k = \sum_{i\in I} e_i\alpha^i \sum_{k=0}^{\infty}(\alpha^i)^k x^k.$$

Aplicant la fórmula de la suma geomètrica obtenim la igualtat

$$E(x) = \sum_{i\in I} \frac{e_i\alpha^i}{1-\alpha^i x} = \frac{\Omega(x)}{\Lambda(x)},$$

on

$$\Omega = \sum_{i\in I} e_i\alpha^i \prod_{j\neq i, j\in I}(1-\alpha^j x) \qquad \Lambda(x) = \prod_{i\in I}(1-\alpha^i x).$$

Proposició 4.31. *Els polinomis* $\Omega(x)$ *i* $\Lambda(x)$ *són coprimers*

Demostració. Les arrels de $\Lambda(x)$ són els α^{-i} per a $i \in I$ mentre que

$$\Omega(\alpha^{-i}) = \textstyle\sum_{i\in I} e_i\alpha^i \prod_{j\neq i, j\in I}(1-\alpha^j\alpha^{-i}) \neq 0.$$

A més,

$$gr(\Omega) \leq gr(\Lambda) - 1.$$

□

Notem que les arrels de Λ ens permeten trobar els elements del conjunt I, és a dir, les localitzacions dels errors. Per aquest motiu, anomenem Λ polinomi localitzador d'errors.

Teorema 4.32. $\Omega \equiv \Lambda S \ mod\ x^{2t}$.

Demostració. Considerant la "cua" de la sèrie geomètrica E i utilitzant la igualtat (2.1) obtenim:

$$E(x) - S(x) = \sum_{j=d}^{\infty} E_j x^{j-1} = \sum_{j=d}^{\infty} \sum_{i \in I} e_i (\alpha^i)^j x^{j-1} = \sum_{i \in I} \sum_{j=d}^{\infty} e_i (\alpha^i)^j x^{j-1} =$$
$$\sum_{i \in I} \sum_{k=0}^{\infty} e_i (\alpha^i)^{k+d} x^{k+d-1} = x^{d-1} \sum_{i \in I} e_i \alpha^{id} \sum_{k=0}^{\infty} (\alpha^i)^k x^k = x^{d-1} \sum_{i \in I} \frac{e_i \alpha^{id}}{1 - \alpha^i x} =$$
$$x^{d-1} \frac{\Gamma(x)}{\Lambda(x)}.$$

on

$$\Gamma(x) = \sum_{i \in I} e_i \alpha^{id} \prod_{j \neq i, j \in I} (1 - \alpha^j x).$$

Notem que $gr(\Gamma)$ és com a molt $gr(\Lambda) - 1$.

Per tant,

$$\frac{\Omega}{\Lambda} - S = x^{d-1} \frac{\Gamma}{\Lambda}.$$

Prenent $d = 2t - 1$ i reordenant obtenim la igualtat

$$\Omega = \Lambda S + x^{2t} \Gamma.$$

□

Aquest teorema ens dona una relació entre els termes coneguts S, x^{2t} i els buscats Ω, Λ.

Definició 4.33. *Anomenarem equació clau a la congruència $\Omega \equiv \Lambda S \bmod x^{2t}$. A vegades, també ens referirem a la igualta $\Omega = \Lambda S + x^{2t}\Gamma$ com a equació clau.*

Teorema 4.34. *Sigui S el síndrome polinomial per a un missatge rebut y amb un error de pes com a molt t. Llevat d'escalar, existeix una única solució de l'equació clau que satisfà*

$$\begin{cases} gr(\Lambda) \leq t \\ gr(\Omega) < gr(\Lambda) \end{cases} \tag{4.1}$$

i Ω i Λ són coprimers.

Demostració. Existència: el localitzador de l'error Λ i el corresponent Ω són solució de l'equació.

Unicitat: Sigui $(\overline{\Omega}, \overline{\Lambda})$ una altre solució. Aleshores tenim les congruències

$$\Omega \equiv \Lambda S \bmod x^{2t}$$
$$\overline{\Omega} \equiv \overline{\Lambda} S \bmod x^{2t}$$

Multiplicant per $\overline{\Lambda}$ i Λ respectivament i per transitivitat obtenim

$$\Omega \overline{\Lambda} \equiv \overline{\Omega} \Lambda \bmod x^{2t}$$

Com els polinomis verifiquen la condició (4.1), tenim que tant $\Omega\overline{\Lambda}$ com $\overline{\Omega}\Lambda$ són polinomis de grau com a molt $2t - 1$. Per tant,

$$\Omega\overline{\Lambda} = \overline{\Omega}\Lambda$$

Com Ω i Λ són coprimers de la mateixa forma que $\overline{\Omega}$ i $\overline{\Lambda}$ ho són, necessàriament $\Lambda|\overline{\Lambda}|\Lambda$ i $\Omega|\overline{\Omega}|\Omega$ d'on es conclou la unicitat llevat escalar. □

Observació 4.35. A partir de les solucions de l'equació clau podem determinar les localitzacions de l'error buscant les arrels del polinomi $\overline{\Gamma}$. Si el polinomi localitzador té com arrel $\alpha^{-}i$, aleshores $i \in I$ és una localització de l'error.

Proposició 4.36. *Sigui* (Ω, Λ) *una solució de l'equació clau on el polinomi corrector de l'error* Λ *(amb terme constant 1) apareix. Si* $i \in I$*, aleshores*

$$\Omega(\alpha^{-i}) = e_i\alpha^i\chi_i(\alpha^{-i}) \tag{4.2}$$

on $\chi_i(x) = \prod_{j\neq i}(1-\alpha^j x)$

Demostració. $\Omega(\alpha^{-i}) = \sum_{k\in I} e_k\alpha^k \prod_{j\neq k, j\in I}(1-\alpha^j\alpha^{-1})$. Si $k \neq i$, aleshores un dels factors de $\prod_{j\neq k,j\in I}(1-\alpha^j\alpha^{-1})$ és $(1-\alpha^i\alpha^{-i}) = 1-1 = 0$ donat que $j = i \neq k$; $j \in I$.

En conclusió, $\Omega(\alpha^{-i}) = \sum_{k\in I} e_k\alpha^k \prod_{j\neq k,j\in I}(1-\alpha^j\alpha^{-1}) = e_i\alpha^i \prod_{j\neq i,j\in I}(1-\alpha^j\alpha^{-i})$. □

Observació 4.37. A partir de la proposició prèvia podem conèixer els valors de l'error e_i de les localitzacions trobades prèviament.

Corołari 4.38. *Resoldre l'equació clau és equivalent a resoldre el problema de descodificació.*

Definició 4.39. *Donat un enter* t *i* $S \in \mathbb{F}_q[x]$*, considerem el conjunt de solucions de l'equació clau*

$$K = \{(\Omega, \Lambda) \mid \Omega \cong \Lambda S \mod x^{2t}\}.$$

Proposició 4.40. K *és* $\mathbb{F}_q[x]$*-submòdul de* $\mathbb{F}_q[x]^2$*.*

Demostració. Clarament $K \subset \mathbb{F}_q[x]^2$. Comprovem les condicions de $\mathbb{F}_q[x]$-mòdul:

- Tancat per a la suma d'elements de K:

  Definim $+ : K \times K \mapsto K$ que envia $((\Omega, \Lambda), (\overline{\Omega}, \overline{\Lambda})) \longrightarrow (\Omega + \overline{\Omega}, \Lambda + \overline{\Lambda})$.

  Veiem que està ben definida, és a dir, que $(\Omega+\overline{\Omega}, \Lambda+\overline{\Lambda}) \in K$. Cal demostrar $\Omega+\overline{\Omega} \cong (\Lambda + \overline{\Lambda})S \mod x^{2t}$ però es clar donat que cada parell verifica la congruència.

- Tancat pel producte per elements de $\mathbb{F}_q[x]$:

  Definim $\cdot : \mathbb{F}_q[x] \times K \mapsto K$ que envia $(h, (\Omega, \Lambda)) \longrightarrow (h\Omega, h\Lambda)$.

  Veiem que està ben definida, és a dir, que $(h\Omega, h\Lambda) \in K$. Cal demostrar la congruència $h\Omega \cong h\Lambda S \, mod \, x^{2t}$. Com $\Omega - \Lambda S \cong 0 \implies h(\Omega - \Lambda S) \cong 0 \implies h\Omega \cong h\Lambda S$.

□

Proposició 4.41. *Tot element de* K *és pot escriure com a combinació, amb polinomis com a coeficients, dels generadors:*

$$g_1 = (x^{2t}, 0) \quad g_2 = (S, 1)$$

Demostració. Veiem finalment que $g_1 = (x^{2t}, 0) \quad g_2 = (S, 1)$ són generadors de K. Considerem $\overline{K} = \{(\Omega, \Lambda, \Gamma) | \Omega = \Lambda S + x^{2t}\Gamma\}$. Demostrarem $\overline{K} = \langle (x^{2t}, 0, 1), (S, 1, 0) \rangle$ i com la projecció $\pi : \overline{K} \mapsto K$ que envia $(\Omega, \Lambda, \Gamma) \longrightarrow (\Omega, \Lambda)$ és exhaustiva, la imatge del generador $\{(x^{2t}, 0, 1), (S, 1, 0)\}$ de $\overline{K}$ serà generador de K i és $\{g_1, g_2\}$.

- $\supseteq\rfloor$ $g_1 = (x^{2t}, 0, 1)$ verifica $x^{2t} = 0 + x^{2t} \implies g_1 \in \overline{K}$. Anàlogament es veu $g_2 \in \overline{K}$. Per tant, $\langle g_1, g_2 \rangle \subseteq \overline{K}$.
- $\subseteq\rfloor$ Sigui $(\Omega, \Lambda, \Gamma) \in \overline{K}$. Aleshores, $\Omega = \Lambda s + x^{2t}\Gamma \implies (\Omega, \Lambda, \Gamma) = (\Lambda s + x^{2t}\Gamma, \Lambda, \Gamma) = \Gamma(x^{2t}, 0, 1) + \Lambda(S, 1, 0) \implies (\Omega, \Lambda, \Gamma) \in \langle g_1, g_2 \rangle$.

□

Proposició 4.42. *Sigui k un cos, M un submòdul de $k[x]^2$. Sigui $>$ un ordre monomial a $K[x]^2$. Aleshores els següents enunciats són equivalents:*

- *El k espai vectorial ${}^{k[x]^2}\!/_M$ és finit dimensional.*
- *$\langle LT(M) \rangle$ conté elements de la forma $x^u e_1 = (x^u, 0)$ i $x^v e_2 = (0, x^v)$ per a alguns u, v.*

Demostració. Utilitzarem el lema (2.53) tot adaptant-lo per a submòduls de $k[x]^2$. Suposem que ${}^{k[x]^2}\!/_M$ és finit dimensional. Aleshores, pel lema, l'espai generat pel conjunt de monomis que no pertanyen a $\langle LT(M) \rangle$ ha de ser finit i això només passa si $LT(M)$ conté alguns monomis de la forma $(x^u, 0)$ i $(0, x^v)$. Si per exemple no contingués algun monomi $(x^u, 0)$, aleshores $(x^\beta, 0)$ seria de l'espai de monomis que no pertanyen $\forall\, \beta \in \mathbb{Z}_{\geq 0}$ i ${}^{k[x]^2}\!/_M$ seria infinit. □

A partir d'ara considerarem només $k[x]^2$-submòduls tals que $dim({}^{k[x]^2}\!/_M)$ siguin finits.

Definició 4.43. *Sigui $r \in \mathbb{Z}$, definim un ordre monomial $>_r$ a $k[x]^2$ com:*

- *$x^\alpha e_i >_r x^\beta e_i$ si $\alpha > \beta$, $i = 1, 2$;*
- *$x^\alpha e_2 > x^\beta e_1 \iff \alpha + r \geq \beta$.*

Expressat d'una altra forma:

- $(u, 0) >_r (v, 0) \iff u > v$;
- $(0, u) >_r (0, v) \iff u > v$;
- $(0, u) >_r (v, 0) \iff u + r \geq v$.

Proposició 4.44. *L'ordre definit és un ordre monomial.*

Demostració. Veiem les propietats d'ordre monomial:

1. Ordre total: Siguin a, b monomis de $k[x]^2$. Suposem $a = (u, 0)$:

   - Si $b = (v, 0)$, o bé $u > v$ o bé $v > u$ (altrament $a = b$) i, per tant, $a > b$ o $b > a$ respectivament.
   - Si $b = (0, v)$, o bé $v + r \geq u$ o bé $u > v + r$ i, per tant, $a > b$ o $b > a$ respectivament.
   - La resta de cassos són anàlegs.

2. $a > b \implies x^\alpha a > x^\alpha b$ amb x^α monomi de $k[x]$.

   Suposem $a = (u, 0)$:

   - Si $b = (v, 0)$, aleshores $(u, 0) > (v, 0) \implies u > v \implies u + \alpha > v + \alpha \implies x^\alpha(u, 0) > x^\alpha(v, 0)$.
   - Si $b = (0, v)$, aleshores $(u, 0) > (0, v) \implies u > v+r \implies u+\alpha > v+r+\alpha \implies x^\alpha(u, 0) > x^\alpha(0, v)$.
   - La resta de cassos són anàlegs.

3. Bon ordre: Per la proposició 2.64, és suficient veure que donat un monomi qualsevol $a \in k[x]^2$, el monomi $x^\alpha a$ verifica $x^\alpha > a$.

   Sigui $a \in k[x]^2$ monomi. Suposem que és de la forma $(u, 0)$. Aleshores $x^\alpha(u, 0) > (u, 0) \iff \alpha + m > m$ i la segona desigualtat sempre es verifica per a x^α monomi de $k[x]$.

   L'altre cas és anàleg.

□

Proposició 4.45. *Sigui M un submòdul de $k[x]^2$, $r \in \mathbb{Z}$. Suposem $\langle LT(M)\rangle$ està generat per $x^u e_1 = (x^u, 0)$ i $x^v e_2 = (0, x^v)$ per a certs $u, v \geq 0$. Aleshores $\mathcal{G} \subset M$ és una base de Gröebner reduïda de M respecte $>_r$ si i només si $\mathcal{G} = \{g_1 = (g_{11}, g_{12}, g_2 = (g_{21}, g_{22})\}$ verificant:*

- *$LT(g_1) = x^u e_1$ i $LT(g_2) = x^v e_2$.*
- *$gr(g_{21}) < u$ i $gr(g_{12}) < v$.*

Demostració. $\Rightarrow\rfloor$ Suposem $\mathcal{G}$ és una base de Gröebner reduïda, aleshores ha de tenir dos elements que anomenarem g_1, g_2. Si $\mathcal{G}$ tingués 3 elements, aleshores necessàriament dos d'ells, que anomenarem a i b, verificarien $LT(a) = x^\alpha e_i$, $LT(b) = x^\beta e_i$ per a la mateixa i i llavors o bé $LT(a) \in \langle LT(b)\rangle$ o bé $LT(b) \in \langle LT(a)\rangle$ i la base no seria reduïda.

Per hipòtesi, $\langle LT(M)\rangle = \langle x^u e_1, x^v e_2\rangle$, per tant, $LT(g_1) = x^u e_1$ i $LT(g_2) = x^v e_2$. Com és base reduïda, cap monomi de g_1 pertany a $\langle LT(\mathcal{G}\backslash\{g_1\})\rangle = \langle LT(g_2)\rangle$. Per tant, $g_{12} \notin \langle LT(g_2)\rangle$ i en conseqüència $gr(g_{12)} < gr(LT(g_2)) = v$. De manera anàloga veiem $gr(g_{21} < u$.

$\Leftarrow\rfloor$ Sigui $\mathcal{G}$ de la forma definida. Aleshores, $\mathcal{G}$ és base de Gröebner donat que $\langle LT(M)\rangle = \langle LT(g_1), LT(g_2)\rangle = \langle x^u e_1, x^v e_2\rangle$. La segona propietat ens assegura que $(0, g_{12})$ no pertany a $\langle LT(g_2)\rangle$ i, per tant, cap monomi de g_1 pertany a $\langle LT(g_2)\rangle$. De la mateixa forma obtenim que cap monomi de g_2 pertany a $\langle LT(g_1)\rangle$ i, per tant, la base és reduïda.

□

Corołari 4.46. *El conjunt generador $\mathcal{G} = \{(S,1),(x^{2t},0)\}$ del mòdul K és una base de Gröebner respecte l'ordre monomial $>=>_{deg(S)}$.*

Demostració. Veiem que el conjunt $\mathcal{G} = \{g_1 = (x^{2t},0), g_2 = (S,1)\}$ verifica les condicions de la proposició anterior. $LT((S,1)) = max_>\{LT(S,0),(0,1)\}$. $LT(S,0) = (LT(S),0)$ on $LT(S)$ és el terme principal del monomi de major grau. Com $1 + gr(S) \geq gr(LT(S)) = gr(S)$, $(0,1) > LT(S,0)$. D'altra banda, $LT(x^{2t},0) = (x^{2t},0)$. Tenim doncs que el conjunt verifica la primera condició.

Passem a veure la segona condició. $gr(S) = g_{21} < u = 2t$ es verifica donat que S és un polinomi de grau com a molt $2t-1$ (recordem que $2t = d-1$). Er altra banda també es cert que $0 = g_{12} < v = 1$. □

Definició 4.47. *Sigui M un submòdul no nul de $k[x]^2$. Anomenarem element mínim de M respecte l'ordre monomial $>$ a $g \in M\backslash\{0\}$ tal que $LT(g)$ sigui mínim respecte $>$.*

Lema 4.48. *$(S,1)$ és un element mínim respecte $>=>_{gr(S)}$.*

Demostració. $(0,1) = LT((S,1)) <_L T((X^{2t},0)) = (x^{2t},0)$ ja que $0 + gr(S) < 2t$. Per altra banda, tot element de $\langle LT(M)\rangle$ és combinació $k[x]^2$-lineal d'aquests i, en conseqüència, tindran termes principals majors o iguals a $LT((S,1))$ respecte $>$. □

Lema 4.49. *Els elements mínims de $M \subset k[x]^2$ són únics llevat de constants.*

Demostració. Siguin f, $g \in M\backslash\{0\}$ dos elements mínims diferents. Com f és mínim, $LT(f) < LT(h)$ per a tot $H \in M\backslash\{0\}$ però aleshores $LT(f) < LT(g)$ amb g mínim, fet que contradiu que g sigui mínim. Com l'ordre no té en compte el coeficient principal per ordenar els elements, aquest és en l'únic terme en el que poden diferir f i g. □

Proposició 4.50. *Donat r, $>_r$ un ordre monomial a $k[x]^2$ i $M \subset k[x]^2$ submòdul, aleshores tota base de Gröebner de M conté un element mínim de M respecte $>_r$.*

Demostració. Sigui $\mathcal{G} = \{g_1,\ldots,g_s\}$ una base de Gröebner de M respecte $>_r$. Com l'ordre és total, podem comparar tots els elements de la base entre ells. D'aquesta forma, podem trobar un element mínim del conjunt $\mathcal{G}$. Com $\langle LT(M)\rangle = \langle LT(g_1),\ldots,LT(g_S)\rangle$, tot element $g \in M$ verifica $LT(g) \in \langle LT(g_1),\ldots,LT(g_S)\rangle$ aleshores $LT(g) \geq_r LT(g_i)$ per a tot i. Per tant, el mínim trobat a la base és un mínim de M. □

Proposició 4.51. *Sigui una solució $g = (\overline{\Omega},\overline{\Lambda})$ de l'equació clau que verifiqui les condicions 4.1 i a més tals que $\overline{\Omega}$ i $\overline{\Lambda}$ siguin coprimers. Aquesta solució és un mínim a K respecte $>_{-1}$.*

Demostració. Sigui $\overline{g} = (\overline{\Omega},\overline{\Lambda}) \in K$, aleshores:

$$gr(\overline{\Lambda}) > gr(\overline{\Omega}) \iff gr(\overline{\Lambda}) - 1 \geq (\overline{\Omega}) \iff LT(0,\overline{\Lambda}) > LT(\overline{\Omega},0) \iff LT(\overline{\Omega},\overline{\Lambda}) = (0,x^{\alpha}) = x^{\alpha}e_2.$$

A més, les solucions tenen la grau mínim respecte Lambda donat que només existeix una solució a K llevat de constant que verifiqui $gr(\overline{\Lambda}) \leq t$.

Suposem que no és mínim arribem a contradicció. Sigui $h = (A,B)$ una solució mínima. Aleshores, $LT(h) <_{-1} LT(\overline{g})$. Com la solució $\overline{g}$ té grau mínim respecte $\overline{\Lambda}$, necessàriament

$LT(h)$ ha de ser de la forma $(x^\gamma, 0) = x^\gamma e_1$. Per tant, $LT(A,0) > LT(0,B) \iff gr(B) - 1 < gr(A) \iff gr(B) \leq gr(A)$. Per altra banda, $LT(h) <_{-1} LT(\overline{g}) \iff LT(A,0) <_{-1} LT(0,\overline{\Lambda}) \iff gr(\Lambda) - 1 \geq gr(A) \iff gr(\Lambda) > gr(A)$. És a dir,

$$gr(\overline{\Lambda}) > gr(A) \geq gr(B).$$

Alhora, tant $\overline{g}$ com h són solucions de l'equació clau

$$A \cong SB \bmod x^{2t}\ \overline{\Omega} \cong \overline{\Lambda}\ mod\, x^{2t}.$$

Multiplicant la primera per Λ i la segona per B i aplicant la transitivitat de les congruències obtenim:

$$\overline{\Lambda}A \cong B\overline{\Omega}\ mod\, x^{2t}.$$

El grau de $\overline{\Lambda}$ és com a molt t (el cardinal màxim de les localitzacions de l'error). Per tant, $gr(\overline{\Lambda}) \leq t$, $gr(A) < t$, $gr(\overline{\Omega}) < t$ i $gr(B) < t$. En definitiva, el terme de l'esquerra és de grau com a molt $2t - 1$ mentre que el de la dreta és estrictament més petit que l'esquerra. □

Observació 4.52. Combinant les proposicions 4.50 i 4.51, obtenim que trobar una solució que verifiqui les condicions del teorema 4.34 es pot resoldre trobant una base de Gröebner respecte $>_{-1}$ i buscant l'element mínim. Aquest element mínim ha de ser necessàriament la solució buscada (si no, tindríem dos elements mínims diferents).

Proposició 4.53. *El següent algoritme calcula l'element mínim del mòdul K solució de l'equació clau respecte l'ordre $>_{-1}$.*

- *Input:* $\mathcal{G} = \{(S,1), (x^{2t}, 0)\}$.
- *Output: element mínim de* $K = \langle \mathcal{G} \rangle$ *respecte* $>_{-1}$
  - $\mathcal{G} := Buchberger(\mathcal{G}, >_{-1}) = \{g_1, \ldots, g_S\}$
  - $: m = g_1$
  - *for:* $i = 2, \ldots, s$
    - *if* $g_i < m$ *then* $m := g_i$
  - *return* m

on $Buchberger(F, >)$ calcula la base de Gröebner de $\langle F \rangle$ respecte l'ordre monomial $>$. Per veure el desenvolupament de l'algoritme de Buchberger mirar teorema 2.76.

4.3 Codis cíclics en altres anells

Una de les preguntes que se'ns podria plantejar ara es com generalitzar la idea de la proposició 4.7 per a anells de polinomis amb diverses variables.

Definició 4.54. *Sigui* $R = {}^{\mathbb{F}_q[x_1,\cdots,x_m]}\!/_{\langle x_1^{n_1}-1,\cdots,x_m^{n_m}-1\rangle}$, $n_1,\cdots,n_m \in \mathbb{N}$. *Anomenarem codis cíclics m-dimensionals als ideals de R.*

Abans de començar a estudiar aquest codis, fem una observació de com obtenir representants de classe dels elements de R.

Observació 4.55. L'ideal $\langle x_1^{n_1}-1,\cdots,x_m^{n_m}-1\rangle$ admet com a base de Gröebner $\mathcal{H} = \{x_1^{n_1}-1,\cdots,x_m^{n_m}-1\}$.

Demostració. Utilitzarem el criteri de Buchberger presentat al teorema 2.75 per veure que el conjunt $\mathcal{H}$ és una base de Gröebner.

Donat un ordre monomial qualsevol i $g_i,\ g_j \in \mathcal{H}$ amb $i \neq j$, aleshores

$$LCM(LM(f), LM(g)) = 0$$

i, per tant, $S(g_i, g_j) = 0$. Pel criteri de Buchberger, $\mathcal{H}$ és una base de Gröebner de l'ideal generat pel conjunt $\mathcal{H}$. □

Per tant, donat un element $[f] \in R$ podem prendre com a representant el resultat d'aplicar l'algoritme de divisió respecte $\mathcal{H}$ a $\mathbb{F}_q[x_1,\cdots x_m]$. Notem que els representants seran polinomis de grau com a molt $n_i - 1$ respecte la variable x_i per a $i = 1,\cdots,m$.

De la mateixa manera que a $J \subseteq R = {}^{\mathbb{F}_q[x]}\!/_{\langle x^n-1\rangle}$ podíem pensar el cicle π que permutava totes les posicions cap a la dreta com el producte per x, ara també podrem pensar el producte per x_1 com a certa permutació dels elements. Més explícitament, si prenem $c(x_1,\cdots,x_m) \in I$, el podem expressar com un polinomi respecte x_1 amb coeficients a $\mathbb{F}_q[x_2,\cdots,x_m]$. Llavors $c = \sum_{j=0}^{n_1-1} c_j(x_2,\cdots,x_m)x_1^j$ i la multiplicació per x_1 seguida de la divisió respecte $\mathcal{H}$ pren com a representant $x_1c = c_{n-1} + c_0x_1 + \cdots c_{n-2}x^{n_1-1} \in I$ (procés anàleg al vist per a una variable). De la mateixa manera podem fer-ho per a la resta de variables.

Si $m = 2$, és freqüent pensar els elements de I com a matrius $n_1 \times n_2$ on la coordenada (i,j) pren el coeficient del monomi $x_1^i x_2^j$.

Per estudiar els representants a podem aprofitar propietats dels ideals a $\mathbb{F}_q[x_1,\cdots,x_m]$. Donat un ideal I amb generadors $\{[f_1],\cdots,[f_s]\} \subset R$, podem prendre el corresponent ideal $J \subset \mathbb{F}_q[x_1,\cdots,x_m]$ definit per

$$J = \langle f_1,\cdots,f_s\rangle + \langle x^{n_1}-1,\cdots x^{n_m}-1\rangle$$

Donat un ordre monomial $\mathbb{F}_q[x_1,\cdots,x_m]$, podem prendre una base de Gröebner $\mathcal{G} = \{g_1,\cdots,g_t\}$.

Proposició 4.56. *Siguin* $R, I, J, \mathcal{G}$ *de la forma definida prèviament, aleshores:*

h és un representant a I $\iff$ $r_{\mathcal{G}}(h)$ *és zero.*

Demostració. Utilitzarem el teorema 2.16. En el nostre cas, $\pi : \mathbb{F}_q[x_1, \cdots, x_m] \mapsto R$ la projecció natural. Com $I = {}^{J}\!/_{\langle x_1^{n_1} - 1, \cdots, x_m^{n_m} - 1\rangle}$ aleshores, $\pi(J) = I$ i, a més, $ker(\pi) = \langle x^{n_1} - 1, \cdots x^{n_m} - 1\rangle \subseteq J$.

Aplicant el teorema, tenim l'isomorfisme

$$ {}^{R}\!/_{I} \cong {}^{\mathbb{F}_q[x_1, \cdots, x_m]}\!/_{J}. $$

□

Observació 4.57. Podem utilitzar el lema 2.53 per estudiar la dimensió del codi ${}^{R}\!/_{I}$ a partir del corresponent ideal ${}^{\mathbb{F}_q[x_1 \ldots, x_m]}\!/_{J}$ tot veient el conjunt de monomis que no pertanyen a $LT(J)$.

Per tal de definir una funció de codificació, necessitarem algunes observacions prèvies.

Definició 4.58. *Sigui $I \subset R$ un codi cíclic de dimensió k. Anomenarem posicions d'informació a les components k de la paraula del codi que contenen una copia del missatge a codificar i posicions de control de paritat a la resta de components. Totes dues components es corresponen a subconjunts de coeficients del polinomi representant de la paraula del codi a R.*

Definició 4.59. *Donat un ideal $J \subset \mathbb{F}_q[x_1, \cdots, x_m]$. Anomenarem monomis no estàndards als monomis pertanyents a $\langle LT(J)\rangle$ i monomis estàndards als monomis que no pertanyen a $\langle LT(J)\rangle$.*

Donat un $m - dim$ codi cíclic $I \subset R = {}^{\mathbb{F}_q[x_1, \cdots, x_m]}\!/_{\langle x_1^{n_1} - 1, \cdots, x^{n_m} - 1\rangle}$, podem definir una funció de codificació amb el següent algoritme:

Teorema 4.60. *Sigui $I \subset R$ un m-dim codi cíclic, $\mathcal{G}$ una base de Gröebner de l'ideal corresponent $J \subset \mathbb{F}_q[x_1, \cdots, x_m]$ respecte un ordre monomial. Aleshores podem construir una funció de codificació de la següent forma:*

- *Input:una base de Gröebner $\mathcal{G}$ de J*
  Una combinació lineal de monomis no estàndards w.
- *Output: $E(w) \in I$*
  - *$\overline{w} := \overline{w}^{\mathcal{G}}$ el residu respecte $\mathcal{G}$*
  - *$E(w) := w - \overline{w}$*

Demostració. Com $I = {}^{J}\!/_{\langle x_1^{n_1} - 1, \cdots, x_m^{n_m} - 1\rangle}$, el ideal I té la mateixa dimensió com a $\mathbb{F}_q$ espai vectorial que l'espai de monomis no estàndards, on x_i apareix amb grau com a molt $n_i - 1$ per a tota i.

Sigui ara w una combinació lineal d'aquests monomis on x_i té grau com a molt $n_i - 1$. Com $\overline{w}$ és una combinació lineal de només monomis estàndards, els termes no estàndards de w no es veuen afectats en efectuar $E(w) := w - \overline{w}$. Per la proposició 4.56, $E(w)$ pertany a l'ideal I i, per tant, E és una funció de codificació. □

En el cas $m = 1$, la base de Gröebner d'ideal J és el propi polinomi generador g. En aquest cas, l'element $\overline{w}$ és el residu de la divisió respecte g.

Exemple 4.61. Sigui $\mathbb{F}_9 = {}^{\mathbb{F}_3[x]}\!/_{\langle x^2+x+1\rangle}$. Hem vist que α arrel de x^2+x+1 és element primitiu. Considerem el $RS(6,9)$. Aquest està generat pel polinomi $g = (x-\alpha)(x-\alpha^2) = x^2-x-\alpha-1$. Pel teorema 4.60, podem prendre com a posicions d'informació els coeficients dels monomis $x^2, x^3, x^4, x^5, x^6, x^7$ com a elements de ${}^{\mathbb{F}_9[x]}\!/_{\langle x^8-1\rangle}$. Suposem que volem codificar la paraula $w = (2+\alpha)x^5 - \alpha x^3$. Efectuant la divisió euclidiana de w respecte g obtenim com a quocient $(-2-\alpha)x^3+(-2-\alpha)x^2+(-2\alpha)x+(-1-\alpha)$ i com a residu $(-1+\alpha)x+\alpha$. Per tant, $\overline{w} = r_g(w) = (-1+\alpha)x+\alpha$. Obtenim doncs,

$$E(w) = w - \overline{w} = (2+\alpha)x^5 - \alpha x^3 + (1-\alpha)x - \alpha.$$

5 Conclusions

En aquest treball hem aconseguit modelitzar i donar solucions a alguns dels problemes que es poden produir en la transmissió de la informació. Per fer-ho, hem introduït conceptes clau en la teoria de codis com són els codis correctors i detectors d'errors. Em centrat l'estudi en codis lineals i, tot definit una mètrica, hem estudiat la relació entre les capacitats de detecció i correcció amb la distància entre els elements del codi. Hem observat que els codis lineals són capaços de detectar, com a molt, la mínima distància entre els elements del codi menys 1 i corregir la part entera de la meitat d'aquest. Hem estudiat condicions necessàries per a l'existència de codis lineals aixi com cotes entre els diferents elements definitoris del codi. Tot seguit, hem profunditzat en la família dels codis de Hamming veient com construir-los i les seves capacitats per a detecció i correcció d'errors de pes 1. Per a un codi lineal qualsevol, hem construït un processos tant de codificació, a partir d'aplicacions lineals entre espais vectorials, com de descodificació, com ho és el conegut del "síndrome".

Hem centrat part del treball en l'estudi d'un subconjunt de codis lineals coneguts com codis cíclics. Aquest són codis lineals tancats per a permutacions cícliques dels elements de les paraules del codi. Hem observat com aquesta caracterització és equivalent a ser ideals sobre anells de polinomis en una variable de grau finit fixat. D'aquesta forma, hem vist que podem definir un codi cíclic a partir d'un polinomi generador. Hem profunditzat aquests resultats a la família de codis cíclics coneguda com a codis de Reed-Solomon. Mitjançant eines de submòduls d'anells de polinomis en diverses variables, hem donat solució al problema de descodificació dels codis de Reed-Solomon.

Per finalitzar, hem estès la noció de codi sobre un anell de polinomis en una variable a polinomis en diverses variables i hem donat mecanismes de codificació per aquests.

Referències

[AM89] Michael Francis Atiyah and Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1989.

[CLO05] David Cox, John Little, and Donal O'shea. *Using algebraic geometry*. Springer New York, NY, 2005.

[CLO13] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[Fit95] Patrick Fitzpatrick. On the key equation. *IEEE Transactions on Information Theory*, 41(5):1290–1302, 1995.

[Hil86] Raymond Hill. *A first course in coding theory*. Oxford University Press, 1986.

[HK03] Toyokazu Hiramatsu and Günter Köhler. *Coding Theory and Number Theory*. Springer Science & Business Media, 2003.

[Jac12] Nathan Jacobson. *Basic algebra I*. Courier Corporation, 2012.

[Kna07] Anthony W Knapp. *Basic algebra*. Springer Science & Business Media, 2007.

[Rom92] Steven Roman. *Coding and information theory*, volume 134. Springer Science & Business Media, 1992.

[Tra17] Artur Travesa. Estructures algebraiques. 2017.

[VFC19] Mercè Villanueva and Cristina Fernández-Córdoba. Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació. In *Butlletí de la societat catalana de matemàtiques volum 34 número 1*. Institut d'estudis catalans, 2019.