

BUTLLETÍ

DE LA SOCIETAT CATALANA
DE MATEMÀTIQUES
Institut d'Estudis Catalans

— í n d e x —

- ☐ *Miriam Alcalá Vicente*
L'inici de la geometria no euclidiana a Itàlia 5
- ☐ *Cristina Dalfó i Miquel Àngel Fiol*
El mètode de les línies per a la resolució numèrica d'equacions
en derivades parcials 33
- ☐ *Mercè Villanueva i Cristina Fernández-Córdoba*
Codis detectors i correctors d'errors i algunes de les seves
aplicacions a la societat de la informació 53
- ☐ English summaries 91



Volum 34 • Número 1 • Any 2019



Institut
d'Estudis
Catalans

BUTLLETÍ

DE LA SOCIETAT CATALANA

DE MATEMÀTIQUES

Institut d'Estudis Catalans

Volum 34 • Número 1 • Juny 2019

BARCELONA
2019

© dels autors dels articles

Editat per la Societat Catalana de Matemàtiques
filial de l'Institut d'Estudis Catalans
Carrer del Carme, 47
08001 Barcelona

Text revisat lingüísticament
per la Unitat de Correcció del Servei Editorial de l'IEC.

Imprès a Open Print, SL

ISSN: 0214-316-X
Dipòsit Legal: B 19272-1987

Són rigorosament prohibides, sense l'autorització escrita dels titulars del *copyright*, la reproducció total o parcial d'aquesta obra per qualsevol procediment i suport, incloent-hi la reprografia i el tractament informàtic, la distribució d'exemplars mitjançant lloguer o préstec comercial, la inclusió total o parcial en bases de dades i la consulta a través de xarxa telemàtica o d'Internet. Les infraccions d'aquests drets estan sotmeses a les sancions establertes per les lleis.

Índex

MIRIAM ALCALÁ VICENTE	
L'inici de la geometria no euclidiana a Itàlia.....	5
CRISTINA DALFÓ I MIQUEL ÀNGEL FIOL	
El mètode de les línies per a la resolució numèrica d'equacions en derivades parcials.....	33
MERCÈ VILLANUEVA I CRISTINA FERNÁNDEZ-CÓRDOBA	
Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació.....	53
English summaries	91

L'inici de la geometria no euclidiana a Itàlia

MIRIAM ALCALÁ VICENTE

Resum: La geometria no euclidiana és, probablement, la teoria matemàtica més revolucionària del segle XIX. Després de passar desapercebuda durant més de trenta anys, el 1860 s'inicia un procés de renaixença, que va ser impulsat per la labor de dos matemàtics, G. Jules Hoüel i Giuseppe Battaglini.

En aquest article tractarem el procés de difusió, desenvolupament i acceptació de la nova geometria, centrant-nos en el context italià. En particular, mostrarem que l'aportació de Battaglini en aquest camp va més enllà de la divulgació. Al final del seu article «Sulla geometria immaginaria di Lobatschewsky» ens trobem amb una inesperada coincidència entre la descripció que fa del pla no euclidià i el model del disc donat més tard per Eugenio Beltrami. Ens proposem justificar la semblança entre les dues interpretacions.

Paraules clau: història de la geometria, geometria no euclidiana, Hoüel, Battaglini, Beltrami.

Classificació MSC2010: 01A55, 51-03, 53-03.

1 Introducció

Ens situem en el moment de la renaixença de la geometria no euclidiana, que es va iniciar a Europa l'any 1860. Aquest procés culmina amb la presentació del model del disc de Beltrami, el 1868, i del model projectiu de Klein, el 1871, que van aportar les raons necessàries per admetre la validesa de la nova teoria, ja que constitueixen una prova de la seva consistència relativa a la geometria euclidiana o projectiva, respectivament. L'acceptació de la geometria no euclidiana va suposar un trencament amb el pensament matemàtic anterior i va provocar una crisi en els fonaments de les matemàtiques, que no va ser resolta fins a finals de segle amb la reformulació de la geometria donada per Hilbert. Podríem dir, doncs, que es tracta de la descoberta més transcendent del segle XIX, no només en l'àmbit matemàtic, sinó també filosòfic.

L'objectiu d'aquest article serà veure com arriba, de la mà de G. J. Hoüel¹ i G. Battaglini,² la nova geometria a Itàlia i el seu posterior desenvolupament en els treballs d'E. Beltrami.³ A la vegada, explicarem les diferents posicions en el debat sobre la seva acceptació.

La data, 1860, que ha passat a considerar-se el començament d'aquesta renaixença ve donada per ser l'any en què es comença a publicar la correspondència de C. F. Gauss.⁴ Les cartes del cèlebre matemàtic van desvelar que s'havia ocupat durant molts anys del postulat de les paral·leles, tot i no haver publicat mai res,⁵ i que les seves recerques coincidien amb les publicades per J. Bolyai i N. I. Lobatxevski.⁶ No només això, també declara la seva aprovació i admiració pels treballs dels dos geòmetres⁷ i s'inclina a acceptar la nova geometria.⁸

1 Guillaume Jules Hoüel (Thaon, 1823 - Périers, 1886) va estudiar primer a Caen i després a Rollin, abans d'ingressar a l'École normale supérieure l'any 1843. En acabar el seus estudis va ensenyar matemàtiques a diferents liceus fins que, el 1855, finalitza el seu doctorat en mecànica celeste a la Facultat de Ciències de la Sorbona de París. El 1859 obté la càtedra de matemàtiques pures de la Facultat de Ciències de Bordeus, succeint Le Besgue, i donant classe de càlcul infinitesimal. A més de les seves aportacions en geometria, és destacable la seva feina en la creació i revisió de taules de càlcul.

2 Giuseppe Battaglini (Nàpols, 1826 - 1894) va assistir a l'escola privada de matemàtiques de Tucci i d'Angelis, deixebles de Fergola, on es va preparar per a l'admissió a la Regia Scuola di Ponti e Strade, en la qual es va llicenciar l'any 1848. Dos anys més tard comença com a alumne en l'Observatori de Capodimonte, feina que aviat es veurà obligat a deixar per negar-se a signar la petició del rei Borbó per abolir la constitució. L'any 1854 es presenta al concurs per a una càtedra a la Universitat de Nàpols, sense aconseguir la plaça. Donarà, llavors, classes a l'estudi de Tucci fins a l'expulsió dels Borbons l'any 1860, quan va passar a ocupar la nova càtedra de geometria superior a la Universitat de Nàpols. El 1871 es trasllada a la Universitat de Roma, fins al 1885, quan torna a la de Nàpols.

3 Eugenio Beltrami (Cremona, 1835 - Roma, 1900) prové d'una família de reconeguts ideals del Risorgimento, per la qual cosa vivien una situació difícil sota el govern austríac. Va començar a estudiar matemàtiques a la Universitat de Pavia, però va haver d'abandonar els estudis abans de llicenciar-se per qüestions econòmiques. Obligat a treballar en feines administratives per a l'enginyer Diday, descobreix la seva vocació matemàtica i refà del tot la seva educació científica. El 1862, Brioschi el fa nomenar per decret professor extraordinari a la Universitat de Bolonya. Un any més tard, E. Betti li ofereix la càtedra de geodèsia a la Universitat de Pisa. Degut a la insistència de Cremona, que va ser el seu amic i mentor durant molts anys, torna a la Universitat de Bolonya, el 1866, i es trasllada després a Roma, el 1873. Descontent a la capital i per la salut de la seva dona, intentarà un trasllat a la Universitat de Pàdua, que fracassà per l'oposició de Cremona. L'any 1876 aconsegueix la càtedra de física matemàtica a la Universitat de Pavia, on trobarà el seu amic Felice Casorati, però la mort prematura d'aquest el farà decidir a tornar a Roma el 1891.

4 La primera de publicar-se va ser la que mantenia amb Schumacher, editada per C. A. F. Peters en sis volums que apareguren entre els anys 1860-1865 [41].

5 Vegeu la carta de Gauss a Schumacher amb data 17.5.1831 editada per Peters, a [41, 1861, vol. 2, p. 261] o a *Werke* [24, 1900, vol. 8, p. 212].

6 Hoüel, en la seva traducció de l'article de Battaglini [5, p. 217], afirma a peu de pàgina que, de fet, seria més just anomenar a la teoria de les paral·leles de Lobatxevski la teoria de Gauss, ja que la correspondència mostra que va ser el primer a inventar-la.

7 Vegeu, per exemple, sobre el treball de Janos Bolyai, la carta de Gauss a Gerling del 14.2.1832 (a Schaefer [45, p. 387] o a *Werke* [24, 1900, vol. 8, p. 220]), o l'escrita al pare de Janos, Farkas, el 6.3.1832 (a *Werke* [24, vol. 8, p. 220-221], o a la transcripció digitalitzada a <https://gauss.adw-goe.de>). Sobre el treball de Lobatxevski, vegeu per exemple la carta a Schumacher del 28.11.1846 (a Peters [41, 1863, vol. 5, p. 246-247] o a *Werke* [24, 1900, vol. 8, p. 239]).

8 Gauss reconeix per primer cop que no troba res d'absurd en la hipòtesi no euclidiana a la

Gauss, deliberadament, no va fer públiques aquestes opinions; només les havia compartit amb alguns amics i col·legues interessats en la qüestió, conscient que la comunitat matemàtica, fortament influenciada per la filosofia kantiana, no acceptaria les noves idees.⁹ Sense el suport de Gauss, les massa innovadores recerques de J. Bolyai i N. I. Lobatxevski no van tenir la repercussió que calia esperar davant la solució d'un problema que havia mantingut ocupats els matemàtics des de la mateixa aparició dels *Elements* d'Euclides.

Recordem que, en aquesta recopilació, el matemàtic grec construeix tot el coneixement geomètric de l'època de manera rigorosa, fent servir la deducció lògica i partint de cinc postulats o axiomes que havien de ser tan evidents que ningú no en pogués discutir la veracitat. Però la complexa redacció del cinquè postulat, el de les paral·leles, que contrasta amb la senzillesa dels quatre anteriors, va portar a la creença que es devia poder demostrar a partir dels altres, i va passar a ser considerat com un teorema.¹⁰ Durant els segles posteriors molts matemàtics van intentar demostrar el teorema sense èxit, arribant sempre a una *petitio principii*, és a dir, en algun moment de la prova suposaven com a cert un fet, aparentment evident, que en el fons era un enunciat equivalent al postulat. En els seus treballs, independents, Bolyai i Lobatxevski parteixen de la negació del postulat de les paral·leles, i aconsegueixen construir un sistema geomètric sense cap contradicció lògica. D'aquesta manera, consideren que han provat la impossibilitat de demostrar el postulat a partir dels anteriors, a la vegada que han trobat una nova geometria possible diferent de l'euclidiana.¹¹

Aquest resultat desvelador va passar pràcticament desapercbut, en part, perquè els autors no es movien en els principals cercles acadèmics, però sobretot, com bé sabia Gauss, perquè contradeia l'epistemologia de Kant. En la seva *Crítica a la raó pura*, Kant explica que no tot el coneixement prové de l'experiència, hi ha conceptes que són innats a la raó humana. L'ésser humà, en observar la realitat, organitza les seves percepcions en l'espai i el temps. Aquestes són, doncs, dues condicions *a priori* de l'experiència sensible. La geometria euclidiana, en descriure les propietats de l'espai, és un coneixement *a priori*, és la nostra manera de percebre la realitat, per tant, és l'única geometria possible. L'aparició d'una geometria basada en la negació d'un axioma i lògicament coherent desmunta completament la visió kantiana del món. La

seva carta a Gerling de l'11.4.1816 (a Schaefer [45, p. 122], o a *Werke* [24, vol. 8, p. 168-169]), i es mostra cada vegada més convençut en la correspondència posterior. Vegeu per exemple la carta a Schumacher del 12.7.1831 (a Peters [41, 1861, vol. 2, p. 269] o a *Werke* [24, 1900, vol. 8, p. 215-218]).

9 Abardia, Reventós i Rodríguez, a «What did Gauss read in the Appendix?» [1], mostren que Gauss intentava buscar una superfície que fes el paper d'esfera imaginària en el seu estudi de superfícies corbes. Segurament, en no trobar-la, no es va decidir a publicar res sobre la qüestió, ja que no tenia una solució convincent.

10 De fet, ja en temps d'Aristòtil, hi havia discussions sobre el postulat de les paral·leles. Aquesta és probablement la raó per la qual Euclides va elaborar un enunciat tan complex i va decidir, encertadament, incloure'l entre els axiomes. Vegeu l'article d'Imre Toth «Non-Euclidean Geometry before Euclid» [47].

11 El 3 de novembre del 1823, Bolyai escriu al seu pare: «del no-res he creat un univers nou». Podem llegir la versió anglesa de la carta a Bonola [15, p. 98] i la traducció al català a *Una lectura del Disquisitiones*, de Reventós i Rodríguez [42, p. 110].

realitat podria no ser euclidiana, després de tot. I encara que ho fos, només es podria corroborar mitjançant l'experiència, veient quina de les dues geometries s'adapta millor a la realitat sensible. Com diu Lobatxevski, «res no autoritza, a part de les observacions directes, a suposar que en un triangle la suma dels angles és igual a dos angles rectes».¹²

La qüestió de les paral·leles va caure en l'oblit i, durant els anys següents, el postulat va passar a considerar-se de la mateixa manera que la quadratura del cercle o el moviment perpetu, problemes que s'han mantingut irresolubles al llarg de la història. La referència a aquests problemes clàssics¹³ mostra, però, un canvi de mentalitat; entre els matemàtics es va començar a instaurar la idea que el cinquè postulat no es podia demostrar a partir dels altres quatre, cosa que va donar una certa predisposició a acceptar les noves idees proposades per Bolyai i Lobatxevski.

L'autoritat de Gauss va despertar ràpidament l'interès per les poc conegudes obres d'aquests autors.¹⁴ Aviat van aparèixer les traduccions franceses i italianes, fetes respectivament per G. J. Hoüel i G. Battaglini.¹⁵ Aquests dos matemàtics van impulsar el procés de renaixença de la nova geometria, no només amb les seves traduccions, sinó també amb la divulgació i el suport que van donar a les noves idees. El seu paper va ser fonamental en el posterior desenvolupament de la geometria no euclidiana.

2 Context polític i social a Itàlia

Ens trobem en els últims anys del Risorgimento (1815-1870), que va finalitzar amb la unificació dels diferents estats italians en un sol país, sota el govern del rei Víctor Manuel. Molts matemàtics italians van participar en aquest moviment, formant part de les revoltes contra el règim polític establert,¹⁶ i compartien l'ideal de la construcció del nou estat. Amb la unificació, van passar a ocupar càrrecs a les noves institucions, des d'on es van poder implicar en les reformes de l'educació pública i la universitat que va iniciar el nou govern. Els matemàtics

12 «... j'ai atâché de prouver que rien n'autorise, si ce ne sont les observations directes, de supposer dans un triangle rectiligne la somme des angles égale à deux angles droits...» A «Géométrie imaginaire» [36, p. 295].

13 Vegeu R. Baltzer, *Die Elemente der Mathematik* [3, p. III], i G. J. Hoüel, «Quelques réflexions au sujet de la ligne de longueur minimum sur la sphère» [28, p. 78].

14 Voelke, a [48, p. 50], assenyalà les cartes de Gauss a Schumacher amb dates 28.11.1846 i 12.7.1831 (a Peters [41, 1863, vol. 5, p. 246-247 i 1861, vol. 2, p. 269] o a *Werke* [24, 1900, vol. 8, p. 238-239 i p. 215-218]) com els principals desencadenants de la renaixença de la geometria no euclidiana; Battaglini es refereix, a més, a la del 17.5.1831 (a Peters [41, vol. 2, p. 258-261]) en la seva carta a Genocchi del 14.5.1867, a [19, p. 167-168]. El pes de l'opinió de Gauss ve confirmat pels comentaris de Baltzer en el prefaci de *Die Elemente der Mathematik* [3, p. III], i de Hoüel en *Sur l'axiôme XI d'Euclide* [27, nota VI de l'apèndix, p. 72].

15 El 1866 es publica la traducció del *Geometrische Untersuchungen zur Theorie der Parallellinien* de Lobatxevski al francès [37], i l'any següent la de la «Pangeometria» a l'italià [38]. Les traduccions de l'*Appendix* de Bolyai, francesa [14] i italiana [13], són de 1868.

16 Per exemple, Cremona va participar en la defensa de la República de Venècia fins a la seva rendició l'agost del 1849; Brioschi va lluitar a les Cinc Jornades de Milà, en les quals els habitants insurgents van vèncer les tropes ocupants del govern austríac; Betti va pertànyer al batalló dels universitaris pisans a la batalla de Curtatone i Montara el 1848; i Beltrami va ser acomiadat de l'administració ferroviària lombardoveneta el 1859, per les seves idees polítiques.

més influents en l'àmbit polític van ser Luigi Cremona (1830–1903),¹⁷ Francesco Brioschi (1824–1897) i Enrico Betti (1823–1892).¹⁸

El Govern va crear també nous centres de recerca i noves càtedres, com les de geometria superior, assignades per reial decret a Cremona a Bolonya i a Battaglini a Nàpols. Van aparèixer escoles tècniques destinades a formar enginyers, com el Politecnico di Milano, fundat per Brioschi el 1863, i la Scuola di Applicazioni per gli Ingegneri a Roma, dirigida per Cremona, on també van donar classe Battaglini i Beltrami. La darrera formava part del projecte de convertir la recent proclamada capital en el principal centre científic i de formació del país. Amb aquesta idea es va crear també una escola normal per formar professors,¹⁹ i es va cridar els personatges més il·lustres i reputats a treballar a la universitat. Roma, però, no es va acabar imposant com a centre de recerca matemàtica a Itàlia.²⁰

El projecte per promoure el desenvolupament de la matemàtica va seguir diverses línies d'actuació,²¹ entre les quals la internacionalització de la recerca italiana. Amb aquest propòsit, allotjats a casa de Placido Tardy, a Gènova, en les vacances de Pasqua del 1858, es troben Genocchi, Betti i Brioschi; els darrers es van conèixer en aquell moment. La reunió era per parlar de la nova revista *Annali di Matematica Pura ed Applicata*, que es començaria a editar aquell any. Amb l'entrada dels tres matemàtics en la direcció, la publicació havia de substituir els *Annali di scienze matematiche e fisiche*, que es publicaven des del 1850 sota la direcció de Barnaba Tortolini i que ja difonien gran part de la recerca feta a Itàlia. L'objectiu era mantenir els matemàtics informats també sobre la recerca que es duia a terme fora del seu país, iniciant una feina de traducció i divulgació de les principals obres europees. La iniciativa era compartida pel *Giornale di Matematiche*, dirigit per Battaglini a Nàpols, que es va convertir en la principal via de difusió de la geometria no euclidiana.

En la trobada, Betti, Brioschi i Genocchi projecten fer un viatge a les principals universitats estrangeres. Pretenen, principalment, conèixer les últimes novetats en recerca per tal de publicar-les a la nova revista i posar-les a l'abast dels matemàtics italians, així com presentar les investigacions dels darrers. Al viatge, hi va acabar anant Felice Casorati (1835–1890), llavors assistent de Brioschi, en lloc de Genocchi, i van visitar, entre els mesos de setembre i novembre, les principals universitats de França i Alemanya, països de considerable tradició en la formació de grans matemàtics. A Alemanya, van anar a Göttingen, on van conèixer Dedekind i Riemann, però no els va ser possible trobar-se amb Dirichlet. També van viatjar a Berlín, on van conèixer Weierstrass, Kummer i Kronecker, a Leipzig i a Dresden. A París, van conèixer Bertrand i Hermite, però malauradament no van poder trobar-se amb Liouville.

17 Va ser senador, ministre d'Instrucció Pública i vicepresident del Senat.

18 Tots dos van ser diputats, senadors i secretaris generals del Ministeri d'Instrucció Pública. La seva col·laboració és considerada el principal potenciador del desenvolupament de les matemàtiques postunitàries, vegeu «New perspectives on Beltrami's life and work» [46, p. 469].

19 Vegeu la carta de Beltrami a Hoüel, Bolonya 8.10.1873, a [12, p. 176].

20 En les cartes de Battaglini a Hoüel s'evidencien els problemes que sorgiren; vegeu, per exemple, la del 25.1.1872, a [19, p. 126–127].

21 R. Tazzioli enumera les línies d'actuació que es van dur a terme a «New perspectives on Beltrami's life and work» [46, p. 469].

Betti quedà força impressionat de la trobada amb Riemann. De seguida va traduir la seva *Inauguraldisseration*, del 1851 [43], i es va encarregar de promocionar les seves idees. Entre els dos matemàtics va sorgir una gran amistat i Riemann va passar llargues temporades a la Universitat de Pisa convidat per Betti. Durant aquests anys, Beltrami era professor de geodèsia a la mateixa universitat però, com confessa a Hoüel,²² en les seves freqüents xerrades, Riemann mai no va parlar de les innovadores idees exposades a la seva memòria pòstuma.²³

Els matemàtics italians van mantenir el contacte amb les universitats estrangeres i es van esforçar a enviar-hi els joves a especialitzar-se. Va ser, per exemple, el cas de Gregorio Ricci-Curbastro (1853-1925) i Luigi Bianchi (1856-1928), que van assistir a les classes de Klein a la Universitat de Munic, o Ulisse Dini (1845-1918), alumne de Betti, que va estudiar un any a París amb Hermite.

Els esforços per potenciar la investigació van comportar l'obertura de nous camps de recerca i van propiciar un entorn científic que aconseguí formar una nova generació de matemàtics italians reconeguda internacionalment. Pertanyen a aquesta generació, a cavall entre els segles XIX i XX, Ricci-Curbastro i el seu deixeble Tullio Levi-Civita (1873-1941), formats a la Scuola Normale Superiore de Pisa, dirigida per Betti. També va ser molt destacable l'escola italiana de geometria algebraica, iniciada per Corrado Segre (1863-1924) i Eugenio Bertini (1846-1933) seguint la línia dels treballs de Cremona, que té com a màxims representants Guido Castelnuovo (1865-1952), Federico Enriques (1871-1946), Francesco Severi (1879-1961) i Giuseppe Veronese (1854-1917).

La reforma en l'educació va portar a una revisió de l'ensenyament de les matemàtiques a les escoles. Seguint les indicacions de Cremona, el 1867, el ministre d'educació proposa tornar a utilitzar els *Elements* d'Euclides per ensenyar la geometria.²⁴ Aquell mateix any, Betti i Brioschi publiquen una revisió dels *Elements* [11], amb alguns comentaris i una sèrie d'exercicis al final de cada llibre,²⁵ pensat perquè es fes servir com a llibre de text. El manual seguia un estil purament euclidià, conservant el llenguatge característic i sense fer ús de l'àlgebra o de l'aritmètica. La seva intenció era contraposar-se als tractats comuns que seguien la línia dels *Elements de Legendre*.²⁶ L'ús de mètodes exclusivament geomètrics havia estat reivindicat per Hoüel a l'*Essai critique*,²⁷ que insistia en la necessitat d'abandonar la metodologia de Legendre en considerar que els procediments moderns que s'introdueixen són del tot innecessaris en l'exposició.

22 Vegeu la carta de Beltrami a Hoüel, Bolonya 4.12.1868, a [12, p. 69].

23 Es tracta de l'*Habilitationsvortrag*, la dissertació feta per Riemann, el 1854, per obtenir la qualificació postdoctoral necessària per donar classe a les universitats alemanyes, titulada «Über die Hypothesen, welche der Geometrie zu Grunde liegen» [44]. La memòria es va publicar per primer cop el 1868, dos anys després de la mort de Riemann.

24 Estratto dal Decreto Coppino (10.10.1867), *Supplemento alla Gazzetta Ufficiale del Regno d'Italia*, Florència 24 d'octubre de 1867.

25 Segons explica Forti a Hoüel a la seva carta del 3.12.1867, que es troba al *Dossier Hoüel* dels Archives de l'Académie des Sciences de París.

26 Tal com els mateixos autors especifiquen al prefaci [11, p. VI-VII].

27 Hoüel exposa les seves opinions sobre com hauria d'estructurar-se l'ensenyament de les matemàtiques a la nota *Réflexions sur l'enseignement de la géométrie élémentaire* de l'apèndix de l'*Essai critique*, a [27, p. 81-85] o a [32, p. 88-91]. Al seu manual, Betti i Brioschi es refereixen al treball de Hoüel en diverses ocasions.

El text no va tenir, però, una bona acceptació entre el professorat, degut a la seva complexitat i a la manca d'aportacions didàctiques, i va passar a engrandir la discussió, encetada pel decret ministerial, entre partidaris i detractors de fer servir els *Elements* com a llibre de text. Els primers defensaven el rigor d'Euclides, que consideraven perdut, i creien que era una bona manera d'ensenyar el raonament lògic. Els segons el consideraven antiquat, perquè no incloïa els descobriments recents que s'havien fet en aquesta disciplina, i pel llenguatge complicat que s'hi utilitza.

La polèmica es va revifar amb la traducció de la memòria de J. M. Wilson, «Euclid as a text-book of elementary geometry»,²⁸ publicada al *Giornale di Matematiche* sota la signatura R. R., darrere la qual s'amagava el professor Raffaele Rubini, de la Universitat de Nàpols.²⁹ L'escrit fa una crítica contundent del text d'Euclides i conclou que és «antiquat, artificial, il·lògic i inapropiat» com a llibre per a l'ensenyament.³⁰ La reacció dels partidaris del text d'Euclides no es va fer esperar. Battaglini publicarà al *Giornale* la rèplica de Brioschi i Cremona, defensant la mesura governamental [16] i un fragment de la carta que va rebre de Hoüel [29]. Tot i així, sembla que l'editor compartia més les opinions de Rubini.³¹ En les seves cartes a Hoüel, Battaglini accepta la necessitat del rigor lògic i que cal desenvolupar els conceptes sense recórrer a l'àlgebra,³² però també diu que el text d'Euclides s'hauria de fer servir només en «primer lloc», sempre suposant que se li donés un format modern i que fos rectificat en alguns punts.³³ Creiem que el que en realitat està dient, amb molta diplomàcia, és que considera el text antiquat i que el troba insuficient per a conèixer en profunditat la geometria, segurament pensant en els nous descobriments. La nostra interpretació es confirma en la carta que el napolità escrigué a Genocchi, on es mostra contundent en el seu desacord amb l'ús del text d'Euclides:

... non ho ritengo a dire che, con tutto rispetto pel merito dell'Euclide, ritengo i suoi Elementi come libro inadatto all'insegnamento, tanto se si ha in miral l'ammaestramento nella *Geometria* (per la povertà di quel libro) quanto se si riguarda il solo lato educativo, poichè credo che quel libro sia più adatto ad addormentare la mente dei ragazzi, che a svolgere le loro facoltà.³⁴

[... no tinc reserves a dir que, amb tot el respecte pel mèrit d'Euclides, considero els seus *Elements* com a llibre inadequat per a l'ensenyament, tant pel que fa al coneixement de la *Geometria* (per la pobresa d'aquest llibre) com si es mira només el cantó pedagògic, ja que crec que aquest llibre és més adequat per adormir la ment dels nois que no pas per desenvolupar les seves facultats.]

[Battaglini a Genocchi, 7.2.1869]

²⁸ *The Educational Times*, 1868, p. 125-128.

²⁹ Tal com revela Forti a Hoüel a la seva carta, Pisa 25.2.1869, que es troba al *Dossier Hoüel* dels Archives de l'Académie des Sciences de Paris.

³⁰ Vegeu la traducció de Rubini, a [49, p. 368].

³¹ Segons diu Beltrami en la seva carta a Hoüel amb data Bolonya 23.1.1870, a [12, p. 126-127].

³² Carta de Battaglini a Hoüel, Nàpols 19.7.1871, a [19, p. 116].

³³ Carta de Battaglini a Hoüel, Nàpols 2.2.1869, a [19, p. 78].

³⁴ A [19, p. 169-170].

Aquesta declaració pot semblar molt radical en aquest context, però si pensem que el llibre anava destinat a estudiants d'institut d'entre 10 i 15 anys, la posició de Battaglini se'ns revela força equilibrada.

Més endavant, Beltrami, qui comparteix la posició de Cremona,³⁵ en formar part d'algunes inspeccions als instituts, tindrà l'oportunitat de conèixer els resultats que estava tenint la mesura del govern, i valorar que els professors reticents a canviar de mètode eren del tipus que només demanen estereotipar l'ensenyament. A la vegada, es queixa de la manca de manuals de qualitat des del punt de vista científic i didàctic i de la poca preparació del professorat de les escoles secundàries.³⁶ Conscients d'aquests problemes, els matemàtics italians es van ocupar en la traducció de manuals europeus i en la creació de nous. També s'instauraran, l'any 1875, les escoles de magisteri per tal de donar coneixements actualitzats al professorat i un entrenament apropiat en qüestions pedagògiques.

3 El paper de G. J. Hoüel

En la recerca històrica, la correspondència entre els protagonistes té un interès especial. En les seves pàgines s'expressen intuïcions encara no concretes, es plantegen i es resolen dubtes, se segueixen discussions... en definitiva, ens permeten conèixer els pensaments dels matemàtics de la seva pròpia mà. La figura de G. Jules Hoüel es revela, per aquesta raó, molt rellevant en la història de la geometria no euclidiana. El francès es cartejava amb una llarga llista de matemàtics, molts d'ells italians, i es conserva una gran quantitat de cartes rebudes per Battaglini i Beltrami.³⁷

La seva contribució és reconeguda per les traduccions de les obres de Bolyai i Lobatxevski, amb les quals va introduir la nova geometria a França. També va mantenir els matemàtics francesos informats sobre el desenvolupament de la qüestió traduint els treballs de Battaglini, Beltrami i Klein. Però la seva aportació no és només la de divulgador; els seus escrits sobre els fonaments de les matemàtiques proporcionen un suport filosòfic per acceptar la nova geometria. De fet, Hoüel va ser el principal difusor i defensor de la geometria no euclidiana a França, on, en general, es van rebre amb bastanta apatia i reticència. La reacció dels matemàtics francesos es devia a la gran influència d'A.-M. Legendre (1752-1833), qui havia presentat una prova nova del postulat a cadascuna de les successives edicions dels seus *Eléments de géométrie*, la primera del 1794.

Els anys com a professor d'institut van portar Hoüel a interessar-se per la geometria elemental i pel seu ensenyament. Veient una debilitat axiomàtica en els tractats de geometria, en l'«*Essai d'une exposition rationnelle des principes fondamentaux de la géométrie élémentaire*» [26], del 1863, es proposa revisar els fonaments per establir una base sòlida sobre la qual construir aquesta disciplina. Els *Essai critique* del 1867 i del 1883, [27] i [32], seran versions més

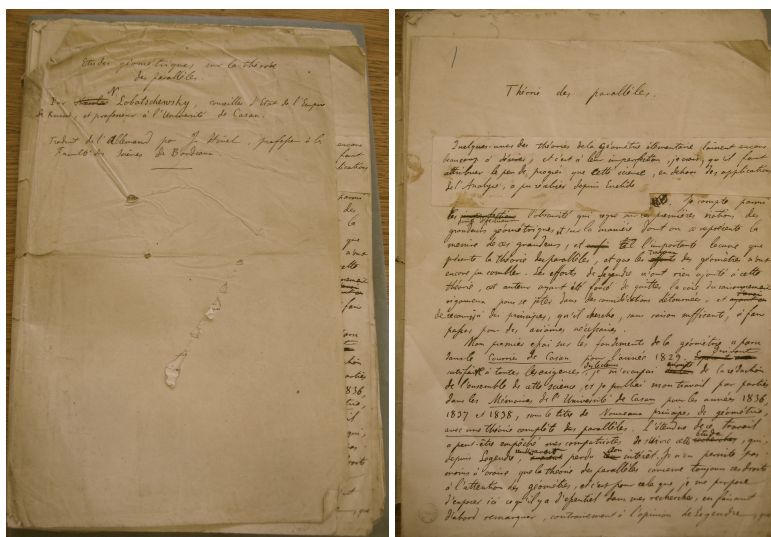
35 Vegeu la carta de Beltrami a Hoüel amb data Bolonya 23.1.1870, a [12, p. 126-127].

36 Vegeu la carta de Beltrami a Hoüel amb data Bolonya 12.6.1870, a [12, p. 141-142].

37 Les cartes rebudes per Hoüel es troben al *Dossier Hoüel* dels Archives de l'Académie des sciences de Paris, tret d'algunes d'inèdites que vam poder consultar a la Biblioteca Municipal de Caen i que actualment es troben a la Biblioteca Alexis de Tocqueville del mateix municipi.

completes d'aquest primer treball, en què ja parlarà de les aportacions de Lobatxevski i Bolyai sobre la teoria de les paral·leles.

Les primeres reflexions de Hoüel sobre la geometria de Lobatxevski les trobem en unes anotacions fetes en el sobre d'una carta timbrada l'any 1866, que es troba intercalat a les pàgines d'una versió de l'*Essai*.³⁸ Hoüel va conèixer l'existència dels treballs del geòmetra rus i de Bolyai per R. Baltzer,³⁹ qui havia introduït per primer cop les nocions no euclidianes a un tractat de geometria elemental.⁴⁰ El juliol d'aquell any, l'alemany li escriu per proposar-li divulgar a França aquestes idees desconegudes.⁴¹ Hoüel publicarà de seguida els *Études géométriques sur la théorie des parallèles* de N. I. Lobatxevski [37]. La traducció de l'*Appendix* de Bolyai [14] trigarà, en canvi, un parell d'anys, degut a les dificultats que hi havia per fer-se amb un exemplar. Va ser gràcies a l'arquitecte hongarès Franz Schmidt⁴² que va aconseguir-ne dues còpies, i en va enviar una a Battaglini.⁴³ Schmidt havia trobat, per casualitat, una còpia de l'*Essai* del 1863 i, volent continuar amb els seus estudis de matemàtiques, li va escriure per demanar-li consell. En la seva resposta, Hoüel li demana ajut per aconseguir la rara publicació dels Bolyai i material per a les seves biografies, que va acabar escrivint el mateix Schmidt.



Manuscrit dels *Études géométriques*. Archive Hoüel,
Biblioteca Alexis de Tocqueville, Caen.

38 Brunel situa el manuscrit a la biblioteca universitària de Bordeus, i transcriu les anotacions del sobre a [18, p. 25-31].

39 Com explica en aquest manuscrit i a l'*Essai critique* [27, p. viii].

40 En la segona edició de *Die Elemente der Mathematik* [3].

41 Carta de Baltzer a Hoüel 19.7.1866, citada per Voelke a [48, p. 60, n. 3].

42 Vegeu la nota del traductor a *La science absolue de l'espace* [14] i la biografia de Hoüel escrita per Halsted [25, p. 100-101].

43 Vegeu les cartes de Battaglini a Hoüel, Nàpols 13.6.1867 i 17.6.1867, on li agraeix que les hagi enviat, a [19, p. 66-67].

Al contrari que la comunitat científica del seu país, Hoüel accepta immediatament la geometria no euclidiana. La seva predisposició a favor de les noves idees prové de la seva recerca sobre els fonaments, que ja l'havia portat a creure que el postulat de les paral·leles no es podia demostrar. A l'*Essai* del 1863 valora que, si les recerques de tants «esperits eminents» no havien arribat a cap resultat satisfactori, era, probablement, perquè estaven escometent un «problema irresoluble».⁴⁴ En l'opuscle de Lobatxevski veurà confirmada definitivament aquesta impressió.⁴⁵

En els seus treballs, Hoüel assenyala que s'està partint d'un «fals punt de vista metafísic» en considerar que la geometria és una ciència de raonament pur,⁴⁶ i que l'experiència sí que intervé en la tria dels axiomes. Les propietats geomètriques se'ns revelen per mitjà dels sentits, però com que algunes ens resulten tan clares, hem acabat creient-les innates a l'intel·lecte humà i declarant que són axiomes *a priori*. Les ciències exactes es basen en primer lloc en l'observació, que ens permet establir, per inducció, les lleis i principis «indefinibles i indemostrables» a partir dels quals es deduiran, mitjançant la lògica, fets nous.⁴⁷ Partir del reconeixement que la geometria no és una ciència *a priori* suposa una diferència epistemològica fonamental per poder acceptar la teoria de Lobatxevski, ja que significa que l'euclidiana no ha de ser l'única geometria possible.

Hoüel continua admetent que, en partir de l'observació experimental, que no és d'una exactitud rigorosa, es podria donar el cas que es triés un axioma equivocat. L'error el reconixeríem quan, en seguir les deduccions lògiques, arribéssim a resultats que estan en «desacord amb la realitat objectiva».⁴⁸ Aquesta és, precisament, la situació en la qual ens trobem quan es pren com a axioma la negació del postulat de les paral·leles, cosa que porta a concloure que la geometria no euclidiana és físicament falsa. Però, puntualitza Hoüel, això no vol pas dir que no sigui «absolutament certa». El que realment importa en una ciència racional i abstracta és que els axiomes inicials, que poden ser triats arbitràriament, siguin compatibles, és a dir, no contradictoris entre ells, i independents els uns dels altres, garantint a més, que el nombre seleccionat sigui el mínim possible. Qualsevol ciència construïda amb aquesta base i que obté els seus resultats seguint la deducció lògica és certa des del punt de vista abstracte, tot i que no concordi amb els fets reals que pretenia representar.⁴⁹ Ara bé, si el que es vol és aplicar aquesta teoria científica a una determinada realitat i que condueixi a resultats pràctics, llavors els principis s'han de triar en conformitat a aquesta realitat observada. La geometria no euclidiana és, per tant, certa, però com que no sembla que es pugui aplicar a l'espai que ens

44 En la introducció [26, p. 171].

45 Vegeu la carta de Hoüel a De Tilly del 21.2.1875, citada per Voelke a [48, p. 61].

46 Introducció de l'*«Essai»* del 1863 [26, p. 171-178].

47 *Du rôle de l'expérience dans les sciences exactes*, la nota es recull a l'apèndix de la segona edició de l'*Essai critique*, 1883 [32, p. 63-70].

48 *Du rôle de l'expérience* [32, nota 1 de l'apèndix, p. 63].

49 *Du rôle de l'expérience* [32, nota 1 de l'apèndix, p. 66]. Vegeu també els fragments de les cartes de Hoüel a De Tilly, amb dates 9.12.1873 i 4.1.1873, citades per Voelke, a [48, p. 71].

envolta, l'hem de considerar com una teoria abstracta que només existeix al nostre pensament,⁵⁰ el seu interès és purament filosòfic.⁵¹ És a dir, Hoüel fa una distinció clara entre la consistència lògica d'una teoria abstracta i la seva validesa experimental.⁵²

4 La geometria imaginària de G. Battaglini

La labor de Giuseppe Battaglini com a difusor de la geometria no euclidiana a Itàlia ha estat sovint reconeguda pels historiadors. Va traduir les obres de Lobatxevski i Bolyai, que li va proporcionar Hoüel,⁵³ i sota la seva direcció, el *Giornale di Matematiche* era la revista que més articles publicava sobre la qüestió. Però, com veurem, la seva contribució al desenvolupament de la geometria no euclidiana va molt més enllà.

Battaglini mostra un ràpid interès per les idees de Lobatxevski i accepta immediatament la nova geometria, entrant en conflicte amb els seus col·legues a la facultat de Nàpols, on la rebuda no va ser gens favorable. En la seva carta a Genocchi per informar-lo sobre la nova geometria, escriu:

... sono *in guerra* con tutta la facoltà di matematica di Napoli, per essermi fatto propugnatore di queste nuove idee...⁵⁴

[... estic *en guerra* amb tota la facultat de matemàtiques de Nàpols, per haver-me fet defensor d'aquestes noves idees...]

Aquestes posicions oposades es fonamentaven en les dues tendències filosòfiques que llavors coexistien a la universitat, el positivisme de Comte i l'idealisme absolut de Hegel.⁵⁵

El suport inqüestionable a la nova geometria per part de Battaglini, que trobem en la correspondència, malauradament no ve acompanyat d'arguments que el justifiquin. Les seves raons se'ns desvelaran, però, en entendre les idees implícites en el seu article «Sulla geometria immaginaria di Lobatschewsky»,⁵⁶ publicat poc després de traduir Lobatxevski, i en algunes línies de les seves cartes.

50 Lobatxevski va arribar a aquesta mateixa conclusió després de realitzar una sèrie d'experiments per comprovar si en la realitat es complia el postulat de les paral·leles o la seva negació, i per això va posar a la nova geometria el nom de *geometria imaginària*.

51 *Sur l'axiome XI (dit postulatum) d'Euclide, Essai critique*, 1867 [27, p. 77-78] o 1883 [32, p. 85].

52 D'aquesta diferència en parla a la carta a De Tilly amb data 21.8.1876, citada per Voelke a [48, p. 70-71].

53 Vegeu les cartes de Battaglini a Hoüel escrites entre abril i juliol del 1867, a [19, p. 66-67], i les del 21.07.1867, 23.11.1867, 2.4.1868, 1.8.1868, a [2, p. 211-212, 214-216].

54 Battaglini a Genocchi, Nàpols 14.5.1867, a [19, p. 167-168].

55 El positivisme d'August Comte creu en el mètode científic com a via de coneixement, basat en la percepció objectiva i la inducció. D'altra banda, la filosofia de Hegel té un concepte de l'*a priori* pròxim al de Kant.

56 Es publicaran a *Rendiconti dell'Accademia delle Scienze di Napoli*, vol. VI (1867), 157-173 i al *Giornale di Matematiche* [4].

El 1854, en la seva carta de presentació a Betti, Battaglini havia expressat que creia que la geometria projectiva és la teoria més general, i que amb ella es tenen tots els mitjans per estudiar les propietats de l'espai.⁵⁷ De fet, el napolità va ser, junt amb Cremona, dels primers italians a interessar-se per la projectiva. En el debat entre partidaris del mètode sintètic o de l'analític, Battaglini s'inclina pel procediment analític, seguint la línia dels seus mestres a l'Escola de Ponts i Camins, Tucci i De Angelis, que es contraposava a la forta tendència sintètica que s'imposava a la Universitat de Nàpols degut a la influència de l'escola de Fergola. Comparteix, doncs, la mateixa posició que Riemann i Beltrami, o en el cas concret de la projectiva, que Möbius i Plücker. Així, en el seu article «Sulla geometria immaginaria», es proposa estudiar la geometria imaginària de Lobatxevski fent servir les eines de la geometria projectiva i seguint una metodologia analítica. Aquest plantejament mostra per primer cop la possibilitat de considerar la nova geometria com a inclosa en la projectiva.

La principal dificultat que un es troba en la lectura de l'article és la complexitat de la seva exposició, que ha fet que se li atribuís falta de rigor. Per exemple, el seu alumne D'Ovidio valora el procediment com a «més feliç que rigorós»⁵⁸ i el mateix Battaglini reconeix a Hoüel que caldria que el desenvolupés amb més claredat.⁵⁹ En una opinió més recent, Voelke qualifica el raonament de «matemàticament insatisfactori» i considera que està «seriosament hipotecat des del principi».⁶⁰ El seu argument és que la deducció, que exposarem a continuació, de la fórmula (1), a partir de la qual Battaglini dedueix gran part dels seus resultats, és incorrecta.

$$\frac{\sinh m\omega}{\sinh \omega n} = \lambda \frac{\sin M\Omega}{\sin \Omega N}. \quad (1)$$

Mencionem primer que l'article s'inicia partint de la rotació d'una recta Ω entorn a un punt p . La funció $F(z)$ que expressa aquesta rotació ha de ser periòdica i compleix, a més, la propietat $F(x + y) = F(x)F(y)$, és a dir, és una funció exponencial. Per tal que la funció exponencial sigui periòdica cal prendre l'exponencial complexa $F(z) = e^{ikz}$, introduint així la variable complexa com Lobatxevski. Les funcions circulars les definirà fent servir el desenvolupament de Taylor de la funció exponencial.

Battaglini considera, llavors, el sistema de punts ω de la recta L i les corresponents rectes Ω que els uneixen amb un punt p , exterior a la recta.

⁵⁷ Vegeu la carta de Battaglini a Betti, Nàpols 8.11.1874, a [19, p. 179–180].

⁵⁸ «In verità più felice che rigoroso può dirsi il procedimento del Battaglini». A [21, p. 588].

⁵⁹ «Je sais que ma Note sur la Géométrie de Lobatschewsky aurait besoin d'être plus clairement développée.» Battaglini a Hoüel, Nàpols 6.8.67, Biblioteca Alexis de Tocqueville, Caen; transcripció a [2, p. 212].

⁶⁰ Voelke és qui ha aprofundit més en l'anàlisi de l'article «La méthode de Battaglini est mathématiquement insatisfaisante», a [48, p. 75]. «La méthode de Battaglini est sérieusement hypothéquée dès le début», a [48, p. 77].

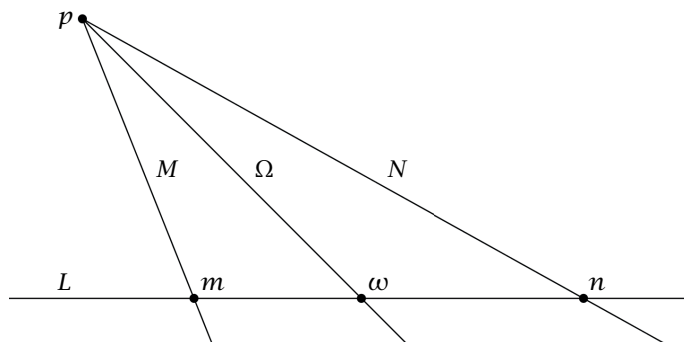


FIGURA 1: Representació de la situació descrita per Battaglini.

Prenent dues posicions fixades dels punts n i m i les respectives rectes M i N , com es mostra a la figura 1, s'obtenen les bijeccions següents:⁶¹

$$\omega \longleftrightarrow \frac{\sinh m\omega}{\sinh \omega n} =: r(\omega),$$

$$\Omega \longleftrightarrow \frac{\sin M\Omega}{\sin \Omega N} =: R(\Omega),$$

$$\omega \longleftrightarrow \Omega.$$

La composició d'aquestes funcions ens dona una bijecció entre les dues raons, que ens porta, segons Battaglini, «evidentment», a la relació:

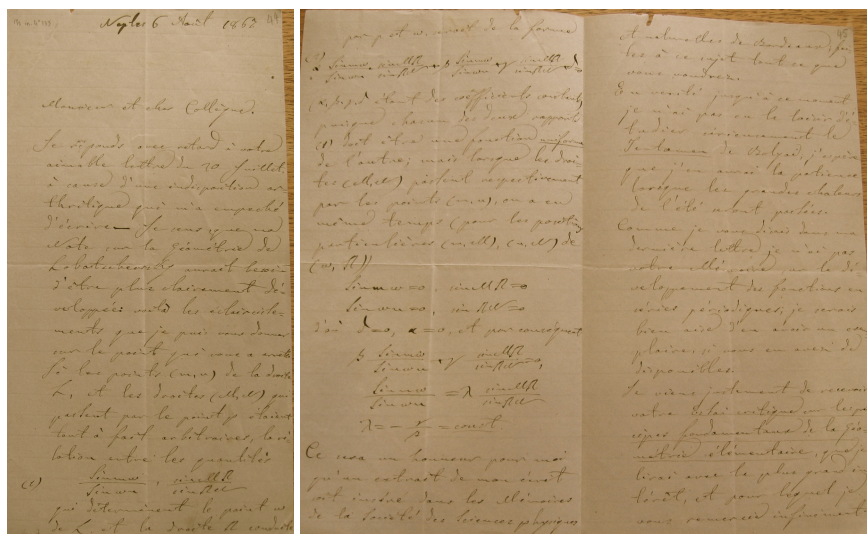
$$r(\omega) = \lambda R(\Omega),$$

és a dir, a la fórmula (1).

Certament, l'equació planteja més dificultats de les que accepta Battaglini. El mateix Hoüel es va encallar en aquest punt i va demanar més explicacions a Battaglini, qui en la seva carta del 6 d'agost del 1867⁶² li enviarà una sèrie de càlculs per justificar-ne el resultat.

⁶¹ L'última bijecció resulta òbvia per la mateixa construcció. Les dues primeres afirmen que cada una de les dues raons tindrà un valor únic i determinat segons la posició del punt ω o la recta Ω , i viceversa. Es poden demostrar fent servir les definicions de sinus circular i hiperbòlic mitjançant l'exponencial.

⁶² La carta inèdita es troba a l'*Archive Hoüel*, Biblioteca Alexis de Tocqueville, Caen. Vegeu-ne la transcripció a [2, p. 212-213].



Carta de Battaglini a Hoüel, Nàpols 6.8.1867. *Archive Hoüel*,
Biblioteca Alexis de Tocqueville, Caen.

Els aclariments, amb el vistiplau de l'autor,⁶³ apareixeran a la traducció francesa [5] en què, a més, se'ns remet a un teorema⁶⁴ que considerem que resol la qüestió de la veracitat de la fórmula. Per tal d'aplicar-lo cal que la funció de partida sigui bijectiva i holomorfa. En l'exposició queda clara la bijectivitat, però no es fa menció a l'holomorfia. No sabem si Battaglini es devia parar a demostrar-la, però és clar que es compleix, ja que es tracta de fraccions entre funcions hiperbòliques i circulars, on les úniques singularitats es trobarien quan s'anul·len els denominadors, que són justament els casos límit contemplats en els aclariments fets a Hoüel.⁶⁵

Battaglini arriba al concepte fonamental de la teoria de Lobatxevski considerant les rectes que passen per un punt p exterior a una recta donada L , i trobant les fórmules següents per a la distància del punt de tall amb L al peu de la perpendicular per p :

$$\theta = \frac{1}{2k} \log \frac{\tan \Delta + \tan \Theta}{\tan \Theta - \tan \Delta}, \quad (2)$$

$$\theta = \frac{1}{2k} \log \frac{\tan \Delta + \tan \Theta}{\tan \Theta - \tan \Delta} + \frac{i\pi}{2k}, \quad (3)$$

on Θ és l'angle que forma la recta que passa per p amb la perpendicular i $k \in \mathbb{R}$.

⁶³ Vegeu la carta de Battaglini a Hoüel 5.8.1868, a [19, p. 74].

⁶⁴ Tota funció monòdroma i monògena, que admet un nombre limitat d'infinitos, és una fracció racional, teorema enunciat al manual de Briot i Bouquet, *Théorie des fonctions doublement périodiques* [17, capítol 4 del llibre I, p. 40].

⁶⁵ Per a més detalls, vegeu «El desenvolupament de la geometria no euclidiana a Itàlia» [2, p. 121-126].

Quan el valor de la distància és infinit obté les dues paral·leles de Lobatxevski, que separen les rectes que tallen en punts situats a distància real finita, donada per la fórmula (2), de les que ho fan en punts situats a distància ideal, donada per la fórmula (3), tal com es mostra a la figura 2. Els darrers els considera com a punts de la recta que estan «més enllà de l'infinit».

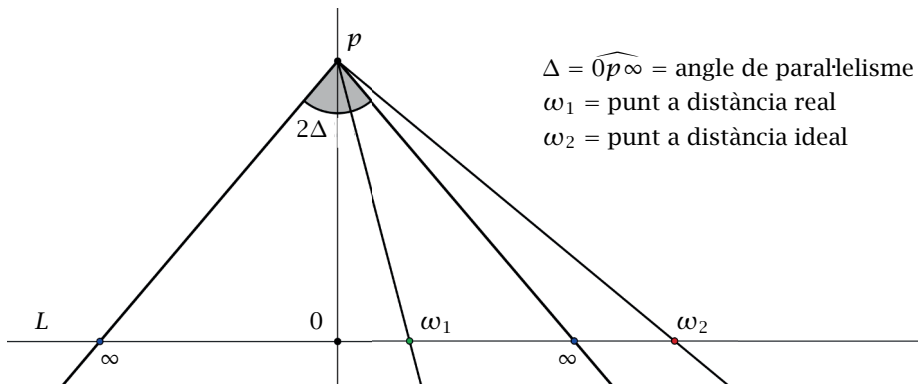


FIGURA 2: Els diferents tipus de recta segons la descripció de Battaglini.

Observant, llavors, que la geometria euclidiana està inclosa en la imaginària, assenyala que la principal diferència entre les dues geometries és que, en l'euclidiana, les rectes són com cercles, ja que els dos punts a l'infinit són coincidents, mentre que en la imaginària són diferents i entre ells es troben infinits punts ideals.⁶⁶ Battaglini no només introdueix el concepte projectiu de punt a l'infinit, sinó que a més ha afegit els anomenats *punts ideals a la recta*. A l'article, també apareix el concepte projectiu de pol d'una recta, definit com el punt en què es tallen totes les seves perpendiculars.

A l'inici de la última secció se'ns presenta una idea d'allò més interessant. Battaglini passa les seves observacions sobre la recta al pla, fent girar el feix de rectes que passen per un punt exterior a la recta donada, tal com il·lustra la figura 3, i fa la sorprenent observació següent:

Nel sistema della Geometria *non-euclidiana* il piano è una superficie indefinita essendo i suoi punti all'infinito tutti *distinti* tra loro ed appartenenti ad una *circonferenza di circolo*, che ha per centro un punto *qualunque* del piano ed il raggio infinito; similmente per lo spazio, i punti all'infinito sono tutti *distinti* tra loro ed appartengono ad una *superficie sferica*, che ha per centro un punto *qualunque* ed il raggio infinito.⁶⁷

[En el sistema de la geometria *no euclidiana* el pla és una superfície indefinida, tots els seus punts de l'infinit són *diferents* entre si i pertanyen a una *circumferència de cercle*, que té per centre un punt *qualsevol* del pla i radi infinit; anàlogament per a l'espai, els punts de l'infinit són tots *diferents* entre si i pertanyen a una *superfície esfèrica* que té per centre un punt *qualsevol* i radi infinit.]

⁶⁶ «Sulla geometria immaginaria» [4, p. 223].

⁶⁷ A «Sulla geometria immaginaria» [4, p. 229].

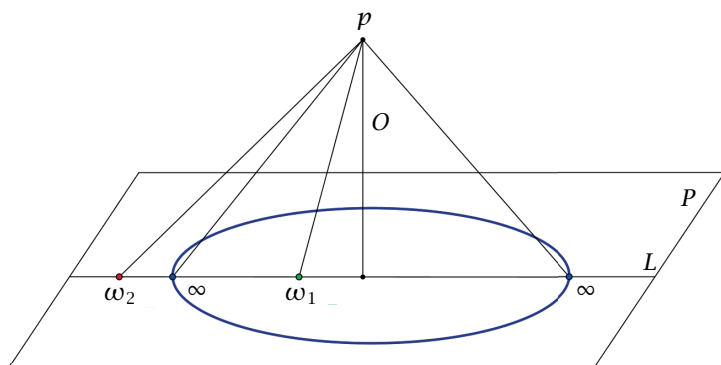


FIGURA 3: Representació gràfica de la descripció de Battaglini del pla hiperbòlic.

La descripció del pla no euclidià com la regió limitada per un cercle sense frontera dins del pla euclidià coincideix, clarament, amb els models donats per Beltrami uns mesos després i Klein uns anys més tard.

Aquesta reflexió de Battaglini no ha estat analitzada en profunditat, tot i que, en la nostra opinió, porta a preguntar-se quina relació hi ha entre els estudis dels tres autors. L'enigma el resoldrem en el següent apartat. Veurem que el plantejament de Battaglini no va suposar una influència en el treball de Beltrami, tot i que J. M. Montesinos així ho creu.⁶⁸ Beltrami parteix d'un altre enfocament. Klein, en canvi, sí que segueix la línia projectiva, i serà en la seva recerca on trobarem la justificació de la similitud entre les tres descripcions del pla hiperbòlic.

5 La interpretació de la geometria no euclidiana d'E. Beltrami i F. Klein

La contribució d'Eugenio Beltrami a la geometria no euclidiana és de les més destacables en la història d'aquesta matèria. La seva interpretació de la geometria no euclidiana, com la que farà Klein uns anys més tard, es pot reformular segons el que actualment anomenem *teoria de models*, solucionant el problema de la seva consistència. En la matemàtica moderna, es considera que una teoria abstracta és vàlida si es construeix seguint deduccions lògiques a partir d'un conjunt d'axiomes independents i consistents. La consistència queda demostrada si es pot proporcionar un model on són vàlids els axiomes de la teoria, ja que, si hi hagués una contradicció a la nova teoria, també es donaria en el model, i aquest s'ha fet a partir d'una teoria que ja es considera acceptada.

⁶⁸ Vegeu el seu article «La cuestión de la consistencia de la geometría hiperbólica» [40, p. 221].

El punt clau per entendre els treballs de Beltrami és llegir-los en el context de la geometria diferencial, introduïda per Gauss al «Disquisitiones generales circa superficies curvas» [23]. La gran aportació de Gauss és que proposa estudiar les superfícies sense pensar-les com a incloses en l'espai real, sinó de manera intrínseca, és a dir, com ho farien habitants bidimensionals que visquessin dins de la superfície. Aquesta idea serà desenvolupada posteriorment per Riemann i és el principi en què es fonamenta l'obra de Beltrami.

La geometria intrínseca de les superfícies tracta les propietats que no varien en doblegar una superfície sense estirar-la ni trencar-la. Aquestes propietats venen determinades per la fórmula de l'element de longitud, que és la que defineix com mesuren els habitants de la superfície. Posem, per exemple, un pla i un cilindre; podem doblegar el pla per fer un cilindre o obrir el cilindre sobre el pla, són localment desenvolupables l'un sobre l'altre. Per tant, tindran el mateix element de longitud i la mateixa geometria intrínseca; diem que són superfícies isomètriques.

Una de les propietats invariants per flexions és la curvatura de Gauss. Si una superfície es desenvolupa sobre una altra, la curvatura de Gauss en punts corresponents és la mateixa. El recíproc només és cert quan la curvatura és constant: si dues superfícies tenen la mateixa curvatura de Gauss constant, llavors es pot desenvolupar localment l'una sobre l'altra. El pla i el cilindre tenen, doncs, la mateixa curvatura, zero, i qualsevol altra superfície que tingui curvatura zero es podrà desenvolupar localment sobre un pla i tindrà com a geometria intrínseca l'euclidiana. De la mateixa manera, totes les superfícies de curvatura constant positiva es desenvolupen localment sobre una esfera i tenen com a geometria intrínseca l'esfèrica. La genialitat de Beltrami serà descobrir que la geometria de Lobatxevski és la de les superfícies de curvatura constant negativa, que ell anomena «pseudoesfèriques».

Durant els anys que va ser professor de geodèsia a la Universitat de Pisa (1864–1866), Beltrami es va dedicar a l'estudi de les cartes geogràfiques. Un comentari fet per Lagrange⁶⁹ el va portar a plantejar-se la possibilitat de representar una superfície sobre un pla de manera que les geodèsiques de la superfície es corresponguin amb rectes del pla. Beltrami troba l'element de longitud de les superfícies que compleixen aquesta propietat, i en calcular a partir d'ell la curvatura, veu que ha de ser constant.⁷⁰ Segons explica a la seva correspondència, és aquest estudi el que el conduirà a topar-se amb la geometria no euclidiana gairebé per casualitat.⁷¹

En el «Saggio d'interpretazione della geometria non euclidea» [7], publicat el 1868,⁷² parteix de l'element de longitud que havia trobat per a l'esfera i

69 A l'article «Sur la construction des cartes géographiques», del 1779 [35].

70 A l'article «Risoluzione del problema: “Riportare i punti di una superficie sopra un piano in modo che le linee geodetiche vengano rappresentate da linee rette”» [6].

71 En la seva carta a D'Ovidio del 25.12.1872, Beltrami explica detalladament la seva via de descobriment. Vegeu el fragment citat per G. Loria a [39, p. 421–423]; la carta va ser publicada per primer cop per D'Ovidio a la seva commemoració de Beltrami [22]. Vegeu també la carta de Beltrami a Houël, Bolonya 18.11.1868, a [12, p. 65].

72 Tot i que el va escriure un any abans, Beltrami no es decidia a publicar-lo degut a una objecció

canvia la constant R del radi per iR , i obté una curvatura constant negativa igual a $-1/R^2$.

Beltrami veu llavors que la geometria intrínseca definida per aquesta mètrica és precisament la desenvolupada per Lobatxevski. Després mostra com aquestes superfícies pseudoesfèriques es poden representar en el pla mitjançant un disc, de manera que les geodèsiques de la superfície s'apliquen a les cordes del disc. Obté, així, un model de la planimetria no euclidiana.

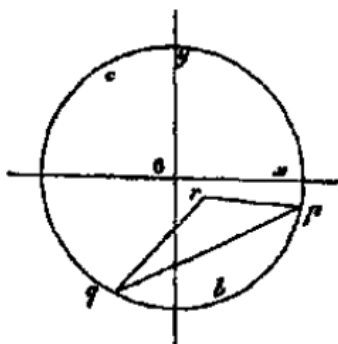
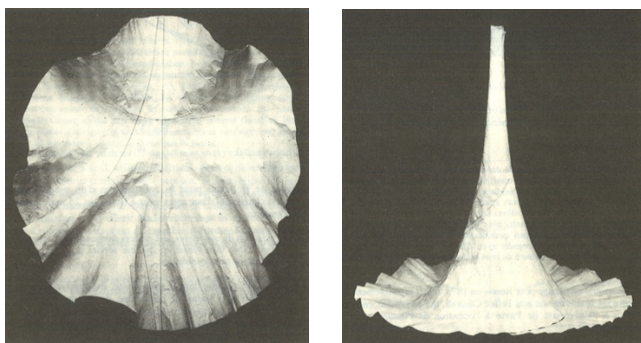


FIGURA 4: Model del disc presentat per Beltrami al «Saggio».

Continua veient que es pot aplicar una part de la superfície pseudoesfèrica en la superfície de revolució generada per la corba tractiu, coneguda amb el nom de *pseudoesfera*. Beltrami es va preocupar de construir materialment aquesta superfície per poder estudiar-ne millor les propietats.



Construcció material de la pseudoesfera feta per Beltrami.
Model conservat al Departament de Matemàtiques de la Universitat de Pavia.

feta per Cremona, referida a si es podia utilitzar l'anàlisi ordinària, fonamentada en la geometria euclidiana, per tractar nocions de geometria no euclidiana. Les seves reticències desapareixeran quan llegeixi la memòria pòstuma de Riemann. Beltrami ho explica a les seves cartes a Genocchi del 9.6.1868 i del 23.7.1868, a [39, p. 415-416], i a Hoüel del 18.11.1868, a [12, p. 66].

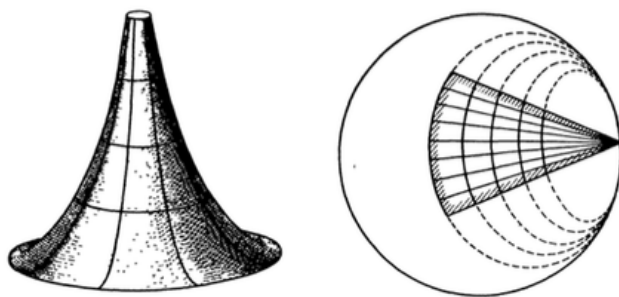


FIGURA 5: Dibuix de Klein per mostrar l'aplicació entre la pseudoesfera i el disc, presentat en el *Vorlesungen über Nicht-Euklidische Geometrie*, del 1928.

La pseudoesfera, però, només és localment isomètrica a la superfície pseudoesfèrica de què parla Beltrami. És a dir, podem tallar-la i obrir-la i posar-la sobre un tros del disc de Beltrami, de la mateixa manera que podem tallar i obrir un cilindre i dir que és igual que un tros de pla, però un cilindre no és un pla! No s'ha de confondre, doncs, la superfície abstracta de Beltrami, que avui anomenaríem *varietat de Riemann de dimensió 2 de curvatura constant negativa*, amb la pseudoesfera, que és una superfície de l'espai real. Aquesta confusió era molt comuna entre els seus contemporanis, que no havien comprès completament les teories de Gauss i Riemann, com podem veure en les moltes cartes a Hoüel on dona explicacions sobre el tema.⁷³

Beltrami finalitza l'article reflexionant que no és possible donar una interpretació real per a l'estereometria no euclidiana de la mateixa manera que ho acaba de fer amb la planimetria, és a dir, no es pot trobar un model. No obstant, veu possible donar una interpretació analítica, sense suport geomètric, simplement introduint una variable més en la mètrica inicial. Així, a «Teoria fondamentale» [8], el 1869, estén els resultats per a superfícies de curvatura constant negativa de dimensió arbitrària, i conclou dient que «la teoria de Lobatxevski coincideix, tret del nom, amb la de l'espai de tres dimensions de curvatura constant negativa».⁷⁴

Pocs anys després de les publicacions de Beltrami apareixen les dues memòries de Klein «Ueber die sogenannte Nicht-Euklidische Geometrie» [33] i [34], el 1871 i el 1873, respectivament, on l'alemany aporta també un nou model per a la geometria no euclidiana, aquesta vegada seguint el punt de vista projectiu suggerit per Battaglini.⁷⁵

⁷³ Vegeu, per exemple, les editades a [12], amb dates 13.3.1869, p. 79; 1.4.1869, p. 87-88; 22.4.1869, p. 92; 12.10.1869, p. 100; 25.10.1869, p. 102-103; 19.12.1869, p. 108.

⁷⁴ «[...] la teoria di Lobatschewsky coincide, salvo nei nomi, colla geometria dello spazio a tre dimensioni di curvatura costante negativa» [8, p. 425].

⁷⁵ Sabem que Klein havia llegit el «Sulla geometria immaginaria», ja que el cita atribuint a Battaglini la introducció del concepte de punt ideal i l'observació que les perpendiculars a una recta són concurrents en el pol d'aquesta respecte a la cònica fonamental. Vegeu [33, p. 290].

Els seus estudis parteixen de la teoria de l'Absolut d'Arthur Cayley (1821–1895). Recordem que la geometria projectiva estudia les posicions relatives entre els elements geomètrics, en lloc d'estudiar les propietats mètriques, com fa la geometria euclidiana, ja que les darreres no es conserven en fer projeccions i seccions. A la seva memòria del 1859, «A sixth memoir upon quantics» [20], el britànic aportava una mètrica a la geometria projectiva, definint la distància de manera que queda invariant per a transformacions que deixen fixa una cònica que anomena *Absolut*. Veia, llavors, que la geometria euclidiana és el cas particular en què l'Absolut és una cònica degenerada formada per un parell de punts.

Klein donarà una nova definició de distància a partir de la raó doble, un invariant projectiu, i distingirà també els casos en què l'Absolut és real i imaginari, que es corresponen amb la geometria de Lobatxevski i la geometria esfèrica, respectivament. D'aquesta manera, demostra que les tres geometries de curvatura constant, que ell anomena *parabòlica*, *hiperbòlica* i *el·líptica*, es poden estudiar com a casos particulars d'una teoria més general, la geometria projectiva. En prendre els punts interiors de la cònica real de l'Absolut, Klein obté el model de Beltrami, li proporciona, a més, una fórmula per a la distància i assenjala que el disc també podria ser una el·lipse.

El 1873, Beltrami escriu l'«Osservazione» [9], en què relaciona també els seus estudis anteriors amb la teoria de l'Absolut de Cayley. La realitat, però, és que feia temps que era conscient d'aquest vincle entre les superfícies de curvatura constant i la geometria projectiva. El 1869 escriu a Hoüel, sobre un afegit que voldria fer a les seves memòries, si aconseguís concretar la idea:

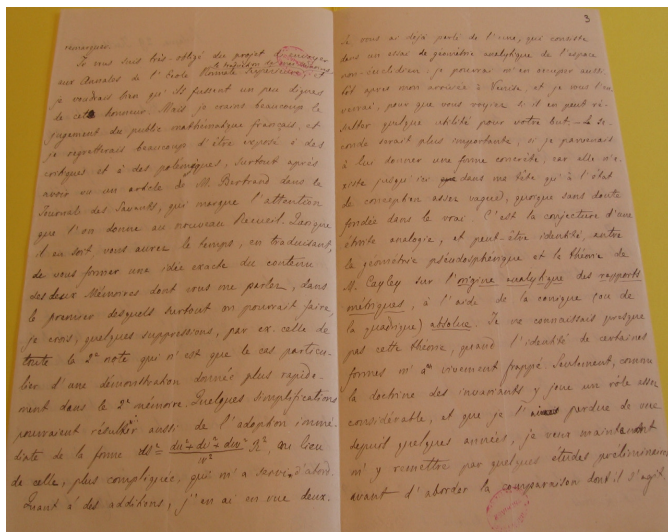
C'est la conjecture d'une étroite analogie, et peut-être identité, entre la géométrie pseudosphérique et la théorie de M. Cayley sur l'*origine analytique des rapports métriques*, à l'aide de la conique (ou de la quadrique) *absolue*. Je ne connaissais presque pas cette théorie, quand l'identité de certaines formes m'a vivement frappé.⁷⁶

[Es tracta de la conjectura d'una estreta analogia, i potser identitat, entre la geometria pseudoesfèrica i la teoria del Sr. Cayley sobre l'*origen analític de les relacions mètriques*, amb l'ajut de la cònica (o quàdrica) *absoluta*. Amb prou feines coneixia aquesta teoria, quan la identitat de certes formes m'ha impressionat profundament.]

[Beltrami a Hoüel, 29.7.1869]

Recordem ara el cercle límit descrit per Battaglini en el paràgraf que hem destacat abans del «Sulla geometria immaginaria», i observem que no és altra cosa que la cònica real de l'Absolut. És probable que, precisament per no tenir gaires coneixements en projectiva, Beltrami no veiés aquesta al·lusió implícita a l'Absolut feta per Battaglini.

⁷⁶ A [12, p. 96–97]. Vegeu també la carta a D'Ovidio del 25.12.1872, esmentada anteriorment.



Carta de Beltrami a Hoüel, Bolonya 29.7.1869. Dossier Hoüel, Archives de l'Académie des Sciences, Paris.

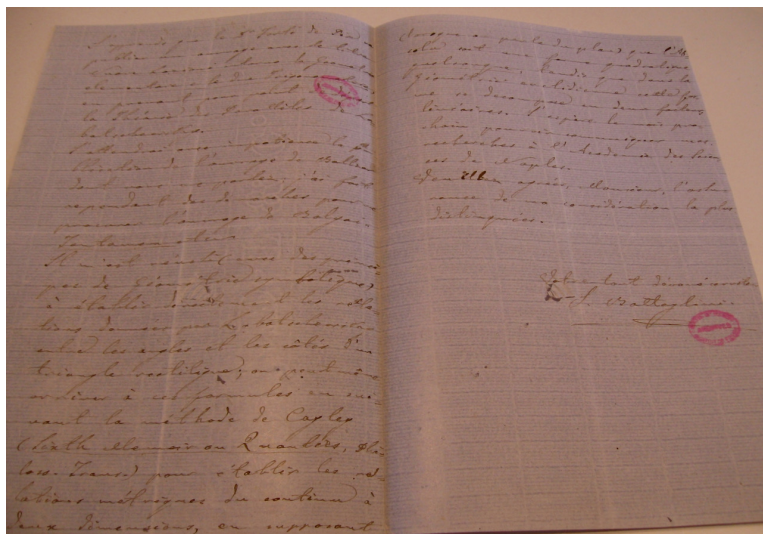
La qüestió que hom es planteja immediatament és si Battaglini ja tenia al cap, llavors, el model projectiu de Klein, com suggereix Montesinos.⁷⁷ La resposta la trobem en les següents línies escrites a Hoüel quan treballava en l'article:

Il m'est réussi (avec des principes de Géométrie iperbolique [sic]) à établir des relations données par Lobatschewsky entre les angles et les côtés d'un triangle rectiligne; on peut même arriver à ces formules en suivant la méthode de Cayley (A sixth memoir upon quantics, Philos. Trans) pour établir les relations métriques du continu à deux dimensions, en supposant (lorsque on parle du plan) que l'*Absolu* soit une forme quadratique *quelconque*, tandis que dans la Géométrie euclidienne cette forme se décompose en deux facteurs linéaires. J'espère le mois prochain pouvoir communiquer mes recherches à l'Académie des Sciences de Naples.⁷⁸

[He aconseguit (amb els principis de geometria hiperbòlica) establir les relacions entre els angles i els costats d'un triangle rectilini donades per Lobatxevski; també es pot arribar a aquestes fórmules seguint el mètode de Cayley («A sixth memoir upon quantics», *Philos. Trans*) per establir les relacions mètriques del continu en dues dimensions, suposant (quan parlem del pla) que l'*Absolut* sigui una forma quadràtica *qualsevol*, mentre que en la geometria euclidiana aquesta forma es descompon en dos factors lineals. Espero poder comunicar les meves recerques el mes que ve a l'Acadèmia de les Ciències de Nàpols.]

[Battaglini a Hoüel, Nàpols 21.5.1867]

⁷⁷ Vegeu «La cuestión de la consistencia de la geometría hiperbólica» a [40, p. 218].
⁷⁸ A [19, p. 63–64].



Carta de Battaglini a Hoüel, Nàpols 21.5.1867. Dossier Hoüel,
Archives de l'Académie des Sciences, Paris.

Observem que també fa servir el terme *geometria hiperbòlica*, que després utilitzarà Klein. Segurament, l'alemany, amb els seus coneixements de geometria projectiva, sí que va entendre el nou enfocament de Battaglini, i sembla bastant probable que veiés que la circumferència de punts a l'infinit és la cònica real de l'Absolut.

6 L'acceptació de la geometria no euclidiana

En aquest apartat presentarem breument la reacció de la comunitat matemàtica davant la reaparició de la geometria no euclidiana i de les noves aportacions de Beltrami. La difusió feta per Hoüel i Battaglini de la nova geometria va desencadenar un interessant debat sobre si havia de ser reconeguda o no com una teoria vàlida. La discussió es va prolongar fins i tot després de la publicació dels treballs de Beltrami, que van rebre moltes crítiques.

Des d'un inici els principals defensors van ser Hoüel i Battaglini. Com veurem, Beltrami només la va acceptar completament després de llegir Riemann. Per què Battaglini va acceptar de manera tan immediata la nova geometria, és una qüestió que, en un principi, sembla no estar clara, ja que, a diferència de Hoüel, mai no explica concretament les seves raons. Un pot pensar, simplement, que era un home d'acord amb el moment històric, obert a idees noves i revolucionàries... Ara bé, l'anàlisi que exposem en els apartats anteriors del seu article i de la seva correspondència mostra que la resposta a aquesta pregunta està sòlidament basada en arguments matemàtics. En la nostra lectura del «Sulla geometria immaginaria» hem vist que Battaglini decideix estudiar la nova geometria des del punt de vista projectiu. Descobrim a més, en la seva carta a Hoüel, que era plenament conscient que correspon al cas particular en

què la cònica de l'Absolut és real. Per tant, en entendre que la geometria no euclidiana està inclosa en la projectiva, que és una teoria totalment acceptada, de seguida va veure fora de dubte la seva validesa i no és estrany que l'aproves sense recances. De fet, les seves inquietuds estan més aviat relacionades amb les repercussions que pot tenir la nova teoria. Conscient que suposa una ruptura amb el pensament matemàtic tradicional, Battaglini assenyala que cal un replantejament de la doctrina de l'espai. En aquesta nova concepció es mostra partidari de seguir el camí proposat per Riemann.⁷⁹ També creu que és fonamental disposar d'uns *Elements* de la geometria no euclidiana per tal d'introduir-la a l'ensenyament. La seva personalitat idealista li fa sentir la responsabilitat d'ensenyar la revolució científica, de donar als joves instruments per trencar amb les metodologies establertes i mantenir la ment oberta davant noves vies de recerca.

En el debat, superada la influència kantiana, es contraposaven dues posicions: la de Hoüel, partidari d'acceptar-la com a certa a un nivell abstracte, i la dels realistes, que consideraven que la veritat s'havia de fonamentar en la realitat i no pas en la consistència lògica.

A França, el principal defensor d'aquesta darrera opinió era Joseph Bertrand. El desembre del 1869 va presentar a l'Académie des Sciences una demostració del postulat feta per Jules Carton,⁸⁰ que, naturalment, es basa en una petició de principi en suposar que les línies rectes no es desvien en cap moment, i que va suscitar força polèmica. Davant les crítiques, Bertrand argumenta que, en el cas del postulat, cal recórrer a l'«evidència». La demostració és, en el fons, innecessària, ja que és l'observació la que ens el mostra com a cert. El que es pretén, en donar una prova rigorosa, és convèncer aquells que no el veuen tan evident com la resta d'axiomes. Per tant, Carton aconsegueix el propòsit en partir només d'una evidència totalment irrecusable.⁸¹ La demostració, però, va produir justament l'efecte contrari en el reconegut geòmetra Gaston Darboux que, en analitzar-la i veure'n el defecte, es va acabar de convèncer de la impossibilitat de demostrar el postulat.⁸²

També a Itàlia, reconeguts matemàtics, com Giusto Bellavitis i Angelo Genocchi, compartien l'opinió de Bertrand.⁸³ En les nombroses cartes a Hoüel, Bellavitis exposa la seva posició, dient que no pot admetre un món creat només a partir del raonament; la ciència serveix per explicar la realitat, i la realitat és la que és. La idea de «mons possibles» li resulta incomprensible; les coses o són certes o són impossibles.⁸⁴

79 Vegeu la carta de Battaglini a Hoüel amb data Nàpols 5.8.1868, a [19, p. 74].

80 «Nouveau moyen de lever la difficulté de la théorie des parallèles», *Comptes Rendus hebdomadaires des séances de l'Académie des Sciences de Paris*, 69 (1869), p. 44.

81 Vegeu «Sur la somme des angles d'un triangle» [10, p. 1265-1266].

82 Vegeu la carta de Darboux a Hoüel citada per Voelke a [48, p. 9].

83 Vegeu la carta de Bellavitis a Hoüel del 20.3.1870, al *Dossier Hoüel*, Archive de l'Académie des Sciences, París. Beltrami també ho diu a la carta a Hoüel del 8.7.1870, a [2, p. 220-221]. D'altra banda, Hoüel diu a De Tilly el 9.10.1873, a [48, p. 184-185], que Genocchi comparteix l'opinió de Bellavitis.

84 Vegeu la carta de Bellavitis a Hoüel amb data 2.7.1872, p. 4, al *Dossier Hoüel*, Archives de l'Académie des Sciences, París.

L'aparició del «Saggio» de Beltrami respon a aquesta crida a trobar una interpretació real de la nova teoria, que alguns reclamaven per acceptar-la. El mateix Beltrami l'havia considerat necessària, i veient que no podia donar una interpretació geomètrica de l'estereometria no euclidiana com la que havia aconseguit per a la planimetria, inicialment no l'havia acceptat.⁸⁵ Va ser en llegir la memòria de Riemann que es va adonar que no necessitava trobar una interpretació d'aquest tipus. Les noves aportacions del matemàtic alemany li proporcionaven un fonament analític per explicar la geometria no euclidiana en qualsevol dimensió; aquesta no és més que la geometria intrínseca d'una varietat n -dimensional de curvatura constant negativa.

Seguint el nou concepte de varietat de Riemann, n'hi ha prou de donar una expressió quadràtica de les coordenades, que sigui l'element de longitud a una superfície abstracta, per poder fer geometria. No cal preocupar-se de com seria aquesta superfície en la realitat, o de si es pot o no realitzar com una superfície de $\mathbb{R}^3$. Per a aquells que no comprenien el punt de vista de Riemann, en canvi, l'acceptació de la geometria no euclidiana depenia de trobar una superfície real de l'espai on es complissin les propietats de la geometria no euclidiana. Segons Abardia, Reventós i Rodríguez, Gauss havia intentat trobar aquesta superfície sense èxit.⁸⁶ Bellavitis i Genocchi, simplement, no creien que pogués existir i, com demostrarà Hilbert un any després de la mort de Beltrami, no anaven equivocats. El més proper que podem aconseguir a una realització de superfície de curvatura constant negativa és la pseudoesfera, però només és localment isomètrica al pla no euclidià, per tant, com assenyalava Genocchi, presenta tota una sèrie de problemes.

Per Beltrami, però, l'existència o no de la realització en l'espai real no afecta en absolut la validesa de la geometria no euclidiana. Les superfícies pseudoesfèriques existeixen en el sentit donat per Riemann. La geometria diferencial, de la qual no es discuteix la certesa, engloba les tres geometries: euclidiana, esfèrica i pseudoesfèrica. La darrera, doncs, és exactament igual de vàlida que la geometria intrínseca de qualsevol altra superfície.

Amb la intenció de resoldre definitivament la qüestió, Hoüel publica, a finals de l'any 1870, «Note sur l'impossibilité de démontrer par une construction plane le principe des parallèles, dit Postulatum d'Euclide»,⁸⁷ en què aclareix per què no és possible demostrar el postulat d'Euclides. Es remet també als treballs de Beltrami, assegurant que dissipen qualsevol dubte que es pugui tenir sobre l'acceptació de la nova geometria. De fet, després de les publicacions de Beltrami, només alguns matemàtics, generalment pertanyents a la generació anterior, continuaren veient la necessitat de trobar una superfície real on es donés la geometria no euclidiana. La resta n'havia tingut prou que es fonamentés en una teoria acceptada.

85 Vegeu les dues cartes a Genocchi amb dates Bolonya 9.6.1868 i 23.7.1868 citades per G. Loria a [39, p. 415-416], i la carta a Hoüel del 18.11.1868, a [12, p. 65-66].

86 Com deïem a la nota 9 de la pàgina 7. Vegeu l'article «What did Gauss read in the Appendix?» [1].

87 Amb el mateix títol Hoüel va publicar en vuit revistes diferents, però hi ha només dues versions de l'article; nosaltres les hem consultat en les *Mémoires de la Société des sciences physiques et naturelles de Bordeaux* [30], i en els *Nouvelles annales de mathématiques* [31].

Agraïments

El present article es basa en la tesi doctoral de l'autora, «El desenvolupament de la geometria no euclidiana a Itàlia», presentada el juny del 2017 i realitzada sota la direcció del professor Agustí Reventós i Tarrida, a qui agraeixo el seu suport i les seves inestimables aportacions.

Referències

- [1] ABARDIA, J.; REVENTÓS, A.; RODRÍGUEZ, C. J. «What did Gauss read in the Appendix?». *Historia Math.*, 39 (3) (2012), 292–323.
- [2] ALCALÁ, M. «El desenvolupament de la geometria no euclidiana a Itàlia». Tesi doctoral. Universitat Autònoma de Barcelona, 2017.
- [3] BALTZER, R. *Die Elemente der Mathematik*. Vol. 2. 2a ed. Dresden: B. G. Teubner, 1867.
- [4] BATTAGLINI, G. «Sulla geometria immaginaria di Lobatschewsky». *Giornale di Matematiche*, 5 (1867), 217–231.
- [5] BATTAGLINI, G. «Sur la géométrie imaginaire de Lobatcheffsky». *Nouvelles annales de mathématiques*, 2e série, 7 (1868), 209–221, 265–277. [Traducció de [4] per J. Hoüel]
- [6] BELTRAMI, E. «Risoluzione del problema: “Riportare i punti di una superficie sopra un piano in modo che le linee geodetiche vengano rappresentate da linee rette”». *Annali di Matematica Pura ed Applicata*, serie I, 7 (1865), 185–204.
- [7] BELTRAMI, E. «Saggio d'interpretazione della geometria non euclidea». *Giornale di Matematiche*, 6 (1868), 284–312. També disponible en línia a: <http://www.caressa.it/pdf/beltrami01.pdf>.
- [8] BELTRAMI, E. «Teoria fondamentale degli spazii di curvatura costante». *Annali di Matematica Pura ed Applicata*, serie II, 2 (1868–69), 232–255.
- [9] BELTRAMI, E. «Osservazione sulla precedente Memoria del sig.r prof. Schläfli». *Annali di Matematica Pura ed Applicata*, serie II, 5 (1871–73), 194–198.
- [10] BERTRAND, J. «Sur la somme des angles d'un triangle». *Comptes Rendus hebdomadaires des séances de l'Académie des Sciences de Paris*, 69 (1869), 1265–1269.
- [11] BETTI, E.; BRIOSCHI, F. *Gli Elementi d'Euclide, con note, aggiunte ed esercizi ad uso de' ginnasi e de' licei*. Florència: Le Monnier, 1867.
- [12] BOI, L.; GIACARDI, L.; TAZZIOLI, R. *La découverte de la géométrie non euclidienne sur la pseudosphère : Les lettres d'Eugenio Beltrami à Jules Hoüel (1868–1881)*. Paris: Albert Blanchard, 1998.
- [13] BOLYAI, G. «Sulla scienza dello spazio assolutamente vera, ed indipendente dalla verità o dalla falsità dell'assioma XI di Euclide (giammai da potersi decidere a priori)». *Giornale di Matematiche*, 6 (1868), 97–115. [Traducció de G. Battaglini]

- [14] BOLYAI, J. *La science absolue de l'espace indépendante de la vérité ou de la fausseté de l'Axiôme XI d'Euclide (que l'on ne pourra jamais établir a priori); suivie de la quadrature géométrique du cercle, dans le cas de la fausseté de l'Axiôme XI*. París: Gauthier-Villars, 1868. [Traducció de J. Höüel]
- [15] BONOLA, R. *Non-Euclidean Geometry. A Critical and Historical Study of its Developments*. Nova York: Dover, Inc., 1955. [Traducció amb apèndixs addicionals per H. S. Carslaw. Suplement que conté «The theory of parallels», de N. Lobachevski «The science of absolute space», de J. Bolyai]
- [16] BRIOSCHI, F.; CREMONA, L. «Al signor Direttore del Giornale di Matematiche ad uso degli studenti delle Università italiane — Napoli». *Giornale di Matematiche*, 7 (1869), 51–54.
- [17] BRIOT, M.; BOUQUET, M. *Théorie des fonctions doublement périodiques et, en particulier, des fonctions elliptiques*. París: Mallet-Bachelier, 1859.
- [18] BRUNEL, G. «Notice sur l'influence scientifique de Guillaume-Jules Höüel». *Mémoires de la Société des sciences physiques et naturelles de Bordeaux*, 3e série, 1er cahier, 4 (1888), 1–78.
- [19] CASTELLANA, M.; PALLADINO, F. *Giuseppe Battaglini. Raccolta di lettere (1854–1891) di un matematico al tempo del Risorgimento d'Italia*. Bari: Levante, 1996.
- [20] CAYLEY, A. «A sixth memoir upon quantics». *Philosophical Transactions of the Royal Society of London*, 149 (1859), 61–90; *The Collected Mathematical Papers*. Vol. 2. Cambridge: Cambridge University Press, 1889.
- [21] D'OVIDIO, E. «Commemorazione del Socio Giuseppe Battaglini». *Mem. Reale Accad. Lincei Cl. Sci. Fis.* (5), 1 (1895), 558–610.
- [22] D'OVIDIO, E. «Eugenio Beltrami». *Atti della Reale Accademia delle scienze di Torino*, 35 (1900), 541–546.
- [23] GAUSS, C. F. «Disquisitiones generales circa superficies curvas». *Commentationes Societatis Regiae Scientiarum Göttingensis Recentiores Classis Mathematicae*, VI (1828), 99–146. [Presentat el 8 d'octubre del 1827. Vegeu també [24, vol. 4, p. 217–258]]
- [24] GAUSS, C. F. *Carl Friedrich Gauss Werke*. Vol. 1–12. B. G. Teubner, Leipzig: Königlichen Gesellschaft der Wissenschaften zu Göttingen, 1870–1927. [Les cartes de Gauss es poden consultar també a: <https://gauss.adw-goe.de>]
- [25] HALSTED, G. B. «Biography: Guillaume Jules Höüel». *Amer. Math. Monthly*, 4 (4) (1897), 99–101.
- [26] HOÜEL, G. J. «Essai d'une exposition rationnelle des principes fondamentaux de la géométrie élémentaire». *Archiv der Mathematik und Physik*, 40 (1863), 171–211.
- [27] HOÜEL, J. *Essai critique sur les principes fondamentaux de la géométrie élémentaire ou commentaire sur les XXXII premières propositions des Éléments d'Euclide*. París: Gauthier-Villars, 1867.

- [28] HOÜEL, J. «Quelques réflexions au sujet de la ligne de longueur minimum sur la sphère». *Nouvelles annales de mathématiques*, 2e série, 7 (1868), 73-78.
- [29] HOÜEL, J. «Estratto di una lettera del Prof. Hoüel al redattore». *Giornale di Matematiche*, 7 (1869), 50.
- [30] HOÜEL, J. «Note sur l'impossibilité de démontrer par une construction plane le principe des parallèles, dit Postulatum d'Euclide». *Mémoires de la Société des sciences physiques et naturelles de Bordeaux*, 8 (1867), 11-18.
- [31] HOÜEL, J. «Note sur l'impossibilité de démontrer par une construction plane le principe des parallèles, dit Postulatum d'Euclide». *Nouvelles annales de mathématiques*, 2e série, 9 (1870), 93-96.
- [32] HOÜEL, J. *Essai critique sur les principes fondamentaux de la géométrie élémentaire ou commentaire sur les XXXII premières propositions des Éléments d'Euclide*. París: Gauthier-Villars, 1883.
- [33] KLEIN, F. «Ueber die sogenannte Nicht-Euklidische Geometrie». *Mathematische Annalen*, 4 (4) (1871), 573-625. [Traducció francesa de M. L. Laugel, «Sur la géométrie dite non euclidienne». *Annales de la faculté des sciences de Toulouse*, 1re série, 11 (4) (1897), G1-G62; traducció anglesa de J. Stillwell, *Sources of Hyperbolic Geometry*. Providence, RI: American Mathematical Society; Londres: London Mathematical Society, 1996. (History of Mathematics; 10)]
- [34] KLEIN, F. «Ueber die sogenannte Nicht-Euklidische Geometrie. (Zweiter Aufsatz.)». *Mathematische Annalen*, 6 (2) (1873), 112-145.
- [35] DE LAGRANGE, J. L. «Sur la construction des cartes géographiques». (Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, année 1779). *Œuvres complètes*. Vol. 4. París: Gauthier-Villars, 1867-1892, 637-692.
- [36] LOBATSCHESKY, N. «Géométrie imaginaire». *Journal für die Reine und Angewandte Mathematik*. [Crelle's Journal], 17 (1837), 295-320.
- [37] LOBATSCHESKY, N. I. *Études géométriques sur la théorie des parallèles*. París: Gauthier-Villars, 1866. [Traducció de l'alemany per J. Hoüel]
- [38] LOBATSCHESKY, N. «Pangeometria, o sunto di geometria fondata sopra una teoria generale e rigorosa delle parallele». *Giornale di Matematiche*, 5 (1867), 273-336. [Traducció de G. Battaglini]
- [39] LORIA, G. «Eugenio Beltrami e le sue opere mathematiche. (Mit Bildnis.)». *Bibliotheca Mathematica*, 3e série, 2 (1901), 392-440.
- [40] MONTESINOS AMILIBIA, J. M. «La cuestión de la consistencia de la geometría hiperbólica». A: *Historia de la matemática en el siglo XIX*. Parte 2. Madrid: Real Academia de Ciencias Exactas, Físicas y Naturales, 1994, 213-232.
- [41] PETERS, C. A. F. (ED.). *Briefwechsel zwischen C.F. Gauss und H.C. Schumacher*. 6 vol. Altona: G. Esch, 1860-1865; Hildesheim; Nova York: G. Olms, 1975. [Versió digital de les cartes a: <https://gauss.adw-goe.de>]

- [42] REVENTÓS, A.; RODRÍGUEZ, C. J. *Una lectura del Disquisitiones generales circa superficies curvas de C. F. Gauss*. Barcelona: Institut d'Estudis Catalans. Societat Catalana de Matemàtiques, 2006. 201 p. (Publicacions de la SCM; 4)
- [43] RIEMANN, B. «Fondamenti di una teorica generale delle funzioni di una variabile complessa». *Annali di Matematica Pura ed Applicata*, 2 (1) (1859), 288–304. [Títol original: *Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse*. Inauguraldissertation, Göttingen, 1851]
- [44] RIEMANN, B. «Über die Hypothesen, welche der Geometrie zu Grunde liegen». Habilitationsvortrag (1854); *Abhandlungen der Königl. Gesellschaft der Wissenschaften zu Göttingen*, 13 (1868), 309–326.
- [45] SCHAEFER, C. *Briefwechsel zwischen Carl Friedrich Gauss und Christian Ludwig Gerling*. Berlín: O. Elsner, 1927. [Reimpressió: Hildesheim; Nova York: G. Olms, 1975. Versió digital de les cartes a: <https://gauss.adw-goe.de>]
- [46] TAZZIOLI, R. «New perspectives on Beltrami's life and work – considerations based on his correspondence». A: COEN, S. (ed.). *Mathematicians in Bologna 1861–1960*. Basilea: Birkhäuser, 2012, 465–517.
- [47] TOTH, I. «Non-Euclidean Geometry before Euclid». *Scientific American*, 221 (5) (1969), 87–101.
- [48] VOELKE, J.-D. *Renaissance de la géométrie non euclidienne entre 1860 et 1900*. Berna: Peter Lang, 2005.
- [49] WILSON, J. M. «Euclide come testo di geometria elementare». *Giornale di Matematiche*, 6 (1868), 361–368.

El mètode de les línies per a la resolució numèrica d'equacions en derivades parcials

CRISTINA DALFÓ I MIQUEL ÀNGEL FIOU

Resum: En aquest treball es descriu un mètode numèric semidiscret per a la resolució d'un tipus d'equacions en derivades parcials. És conegut com el *mètode de les línies* (MOL, per les sigles en anglès), i es basa en la discretització de totes les variables involucrades, excepte una. Il·lustrem l'aplicació del MOL amb la resolució de l'equació de Laplace en coordenades cartesianes. Els conceptes matemàtics que hi apareixen es comparen amb els corresponents al mètode analític de separació de variables. A més, mostrem que els resultats obtinguts amb el MOL són bones aproximacions de les solucions analítiques.

Paraules clau: equacions en derivades parcials, discretització d'una variable contínua, anàlisi numèrica.

Classificació MSC2010: 65M20.

1 Introducció

El mètode de les línies, també anomenat *mètode de semidiscretització* per Zuazua [14], és un mètode per a la resolució d'equacions en derivades parcials (EDP) amb condicions de contorn i en regions amb una certa simetria. Es basa a discretitzar totes les variables, excepte una (si el problema ho permet, sovint es discretitzen les variables espacials i es manté contínua la variable temporal). Això condueix a un sistema d'equacions diferencials ordinàries (EDO), les quals es poden resoldre pels mètodes numèrics habituals per a EDO amb condicions inicials. Aquest mètode va ser introduït a principis dels anys seixanta i, des de llavors, la seva exactitud i estabilitat han fet que es generessin una bona quantitat d'articles (vegeu, per exemple, Zafarullah [13] i Verwer i Sanz-Serna [11]).

Per tant, el *mètode de les línies* (MOL) és un enfocament diferencial i de diferències finites per resoldre equacions en derivades parcials. Aquest mètode té moltes aplicacions en la resolució de problemes en física i enginyeria. Per exemple, ha estat usat àmpliament per experts en tècniques computacionals

en problemes d'electromagnetisme; vegeu, per exemple, Berardi i Vurro [1], Diestel [4], Sadiku [6, capítol 9], Sadiku i Obiozor [7], o Shakeri i Dehghan [9].

En aquest treball il·lustrem el mètode de les línies amb l'equació de Laplace en el pla, per simplicitat. El procés a seguir consta dels passos següents:

1. Discretització de l'equació diferencial en una direcció: contracció de la regió de solucions a un conjunt de línies, i aproximació de les derivades corresponents.
2. Obtenció d'un sistema d'equacions diferencials ordinàries acoblades.
3. Transformació per obtenir un sistema d'equacions diferencials ordinàries desacoblades.
4. Resolució de les equacions diferencials.
5. Transformació inversa i introducció de les condicions de contorn.
6. Resolució del sistema d'equacions lineals obtingut en el pas anterior.

A més de les seves múltiples aplicacions, per exemple, com ja s'ha dit, en electromagnetisme, aquest mètode involucra moltes idees, conceptes i tècniques de la matemàtica discreta, juntament amb els mètodes bàsics de l'anàlisi diferencial. De fet, en el desenvolupament del mètode ens trobem amb els conceptes i els resultats següents: les equacions diferencials en derivades parcials (el·líptiques, parabòliques i hiperbòliques), amb les seves aplicacions; l'estudi dels problemes de contorn (amb condicions de Dirichlet o de Neumann); les tècniques numèriques d'interpolació polinòmica i l'aproximació de derivades; la teoria de matrius tridiagonals semidefinides positives (les quals també apareixen en els grafs distància-regulars); la teoria de matrius circulants i la seva relació amb els grafs de Cayley sobre grups cíclics; la diagonalització de matrius i els algorismes del càlcul dels valors propis i vectors propis; el teorema dels cercles de Gershgorin (per localitzar els valors propis); els polinomis ortogonals de variable discreta (també importants en els grafs distància-regulars); l'estudi de condicions d'ortogonalitat en el cas discret respecte del cas continu; les transformacions discretes (canvis de base) com, per exemple, la transformada discreta de Fourier (DFT); la resolució de les recurrències lineals i les diferències finites; la resolució d'equacions diferencials ordinàries (EDO) lineals; l'aproximació i càlcul d'errors; i, finalment, la representació gràfica i la interpretació de les solucions.

2 El mètode de les línies (MOL): l'equació de Laplace

La transferència de calor a l'estat estacionari en sòlids segueix l'equació de Laplace i ha estat resolta directament per diversos mètodes numèrics, com el mètode successiu de sobrerelaxació, el mètode implícit de direcció alternativa i el mètode de transitoris falsos. Aquests mètodes són alternatius al MOL, que veurem a continuació i que consisteix a discretitzar totes les variables excepte una. De vegades, el MOL també és anomenat *mètode semianalític* (vegeu Subramanian i White [10]).

2.1 L'equació de Laplace en un domini rectangular

Considerem l'equació de Laplace per a la funció potencial $V(x, y)$ en una regió rectangular $a \times b$.

$$\nabla^2 V = \frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} = 0, \quad x \in (0, a), \quad y \in (0, b), \quad (1)$$

amb condicions de frontera que, per simplicitat, establim com a

$$V(0, y) = V(a, y) = 0, \quad y \in (0, b), \quad (2)$$

$$V(x, 0) = 0, \quad V(x, b) = f(x), \quad x \in (0, a). \quad (3)$$

El primer pas és discretitzar la variable $x \in (0, a)$ en els N punts $x_j = j\Delta x$, per a $j = 1, 2, \dots, N$, on el «pas» $h = \Delta x = \frac{a}{N+1}$ correspon a la distància entre dues de les N línies resultants de la discretització, segons mostrem a la figura 1.

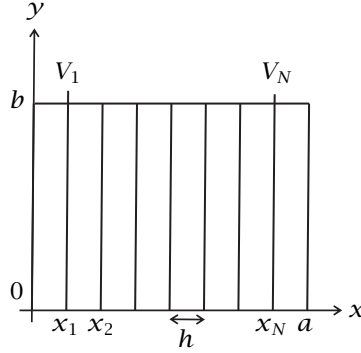


FIGURA 1: Discretització de la variable x .

Ara iterem l'aproximació lineal de la derivada en dos punts successius,

$$V'(x_j) \simeq \frac{V(x_{j+1}) - V(x_j)}{h},$$

i obtenim l'anomenada *aproximació centrada* de la segona derivada

$$V''(x_j) \simeq \frac{V'(x_j) - V'(x_{j-1}))}{h} \simeq \frac{V(x_{j+1}) - 2V(x_j) + V(x_{j-1}))}{h^2},$$

amb error $|\epsilon_j| \leq Ch^2$, per a una C constant, que correspon a un mètode de segon ordre. Amb notació simplificada,

$$\frac{\partial^2 V}{\partial x^2} \simeq \frac{V_{j+1} - 2V_j + V_{j-1}}{h^2}, \quad (4)$$

on V_j denota la funció $V(x_j, y)$. Si substituïm (4) a (1), obtenim les N equacions diferencials

$$\frac{\partial^2 V}{\partial y^2} + \frac{1}{h^2}(V_{j+1} - 2V_j + V_{j-1}) = 0, \quad j = 1, \dots, N. \quad (5)$$

Aleshores, si reemplacem $V(x, y)$ pel vector columna $V = (V_1, \dots, V_N)^\top$, podem escriure (5) en forma matricial com a

$$\frac{\partial^2 V}{\partial y^2} - \frac{1}{h^2} QV = 0, \quad (6)$$

on Q és una matriu tridiagonal, és a dir,

$$\begin{pmatrix} \frac{\partial^2 V_1}{\partial y^2} \\ \frac{\partial^2 V_2}{\partial y^2} \\ \vdots \\ \frac{\partial^2 V_{N-1}}{\partial y^2} \\ \frac{\partial^2 V_N}{\partial y^2} \end{pmatrix} - \frac{1}{h^2} \begin{pmatrix} q_l & -1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 & 0 \\ 0 & -1 & 2 & \dots & 0 & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & \dots & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & -1 & q_r \end{pmatrix} \begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_{N-1} \\ V_N \end{pmatrix} = 0, \quad (7)$$

on els valors q_l i q_r depenen de les condicions de contorn a $x = 0$ i $x = a$. Si la condició de contorn és de Dirichlet per l'esquerra (respectivament, per la dreta), aleshores $q_l = 2$ (respectivament, $q_r = 2$); si la condició de contorn és de Neumann per l'esquerra (respectivament, per la dreta), aleshores $q_l = 1$ (respectivament, $q_r = 1$).

Per resoldre el sistema (6) d'equacions diferencials ordinàries (EDO) lineals de segon ordre acoblades necessitem transformar-lo en un sistema d'EDO desacoblades. Aleshores, la solució és diagonalitzar la matriu Q . En aquest sentit, notem que Q és simètrica i, per tant, els seus valors propis $\lambda_1, \dots, \lambda_N$ són reals. A més, el teorema de Gershgorin¹ ens assegura la no negativitat, ja que han de complir $|\lambda_k - 2| \leq 2$, de manera que utilitzarem la notació $\lambda_k = \omega_k^2$ per a $k = 1, \dots, N$. De fet, com s'explica a la subsecció 3.2, la matriu tridiagonal Q té tots els valors propis diferents, i dona lloc a una successió de Sturm de polinomis ortogonals, els quals estan relacionats estretament amb els corresponents vectors propis (vegeu, per exemple, Godsil [5, §8,5]).

Per tant, tenim que $T^\top QT = D$, on T és la matriu ortogonal (amb columnes ortonormals corresponents als vectors propis de Q), és a dir, $T^{-1} = T^\top$, i D és la matriu diagonal dels valors propis de Q . Aleshores, $Q = TDT^\top$ que, si substituïm a (6), ens dona

$$\frac{\partial^2 V}{\partial y^2} - \frac{1}{h^2} TDT^\top V = 0.$$

Multiplicant per $T^\top (= T^{-1})$,

$$\frac{\partial^2 T^\top V}{\partial y^2} - \frac{1}{h^2} DT^\top V = 0,$$

¹ Recordem que el teorema de Gershgorin afirma que, donada una matriu $A = (a_{jk}) \in M_n(\mathbb{C})$, si es defineixen els cercles $D_1, \dots, D_n$ amb centre a_{jj} i radi $r_j = \sum_{k \neq j} |a_{jk}|$, els valors propis de la matriu A es troben en la unió dels D_j .

i utilitzant el *potencial transformat* $\bar{\mathbf{V}} := \mathbf{T}^\top \mathbf{V}$, tenim

$$\left(\frac{\partial^2}{\partial y^2} - \frac{1}{h^2} \mathbf{D} \right) \bar{\mathbf{V}} = \mathbf{0}. \quad (8)$$

Per tant, obtenim N equacions diferencials ordinàries (en la variable y), del tipus

$$\bar{V}_j'' = \frac{1}{h^2} \omega_j^2, \quad j = 1, \dots, N,$$

amb solucions (el polinomi característic és $s^2 = \frac{\omega_j^2}{h^2}$, amb arrels $s_{1,2} = \pm \frac{\omega_j}{h}$)

$$\bar{V}_j = \alpha_j e^{\frac{\omega_j}{h} y} + \beta_j e^{-\frac{\omega_j}{h} y} = A_j \cosh \frac{\omega_j y}{h} + B_j \sinh \frac{\omega_j y}{h}, \quad j = 1, \dots, N. \quad (9)$$

Per trobar el vector de potencials per a cada $j = 1, \dots, N$, només cal realitzar la *transformada inversa* de $\bar{\mathbf{V}}$, o sigui,

$$\mathbf{V} = \mathbf{T} \bar{\mathbf{V}}.$$

Finalment, imposen les condicions de contorn i resollem les equacions resultants per determinar les constants α_j , β_j , o A_j , B_j .

3 Diagonalització de la matriu $\mathbf{Q}$ i ortogonalitat

3.1 Valors i vectors propis

Abans de resoldre un exemple concret, en aquesta secció discutim la diagonalització de la matriu $\mathbf{Q}$ i les propietats d'ortogonalitat involucrades. Els resultats obtinguts, els valors propis $\lambda_k = \omega_k^2$ i les matrius de vectors propis $\mathbf{T} = (T_{jk})$, es mostren a la taula 1, segons les condicions de contorn a $x = 0$ i $x = a$.

Esquerra	Dreta	T_{jk}	$\lambda_k = \omega_k^2$
Dirichlet	Dirichlet	$\sqrt{\frac{2}{N+1}} \sin \left(\frac{jk\pi}{N+1} \right)$	$4 \sin^2 \left(\frac{k\pi}{2N+2} \right)$
Dirichlet	Neumann	$\sqrt{\frac{2}{N+0.5}} \sin \left(\frac{j(k-0.5)\pi}{N+0.5} \right)$	$4 \sin^2 \left(\frac{(k-0.5)\pi}{2N+1} \right)$
Neumann	Dirichlet	$\sqrt{\frac{2}{N+0.5}} \cos \left(\frac{(j-0.5)(k-0.5)\pi}{N+0.5} \right)$	$4 \sin^2 \left(\frac{(k-0.5)\pi}{2N+1} \right)$
Neumann	Neumann	$\sqrt{\frac{2}{N}} \cos \left(\frac{(j-0.5)(k-1)\pi}{N} \right)$ si $k > 1$ $\frac{1}{\sqrt{N}}$ si $k = 1$	$4 \sin^2 \left(\frac{(k-1)\pi}{2N} \right)$

TAULA 1: Components de la matriu $\mathbf{T}$ i valors propis $\lambda_k = \omega_k^2$ segons les condicions de contorn a $x = 0$ i $x = a$.

Per al càlcul procedim de la manera següent. L'equació a resoldre és

$$\begin{pmatrix} q_l & -1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 & 0 \\ 0 & -1 & 2 & \dots & 0 & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & \dots & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & -1 & q_r \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{N-1} \\ u_N \end{pmatrix} = \lambda \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{N-1} \\ u_N \end{pmatrix}, \quad (10)$$

d'on

$$(q_l - \lambda)u_1 - u_2 = 0, \quad (11)$$

$$(2 - \lambda)u_j - u_{j-1} = u_{j+1}, \quad j = 2, \dots, N-1 \quad (12)$$

$$(q_r - \lambda)u_N - u_{N-1} = 0, \quad (13)$$

on, per als valors usats de q_l i q_r , el teorema de Gershgorin i el fet que la matriu és simètrica impliquen que els valors propis estan a l'interval $[0, 4]$.

Per resoldre l'equació en diferències (12) podríem usar la solució $u_j = s^j$, però s'obté un resultat més compacte amb $u_j = e^{ij\alpha}$ (és a dir, agafant $s = e^{i\alpha} = \cos \alpha + i \sin \alpha$). Si substituïm aquest valor a (12) i dividim per $e^{i(j-1)\alpha}$ obtenim

$$e^{i\alpha} = (2 - \lambda) - e^{-i\alpha} \Rightarrow 2 - \lambda = 2 \cos \alpha. \quad (14)$$

Per tant, l'equació característica és

$$\lambda = 2(1 - \cos \alpha) = 4 \sin^2 \left(\frac{\alpha}{2} \right), \quad (15)$$

cosa que significa que, per a cada valor propi λ , tenim dos possibles valors de α :

$$\alpha_{1,2} = \pm 2 \arcsin \left(\frac{\sqrt{\lambda}}{2} \right).$$

Així, amb $\alpha = \alpha_1$, la solució general de la recurrència és

$$u_j = Ae^{ij\alpha} + Be^{-ij\alpha}. \quad (16)$$

Per trobar els possibles valors de les constants A , B , i α , imposen les «condicions inicials» (11) i (13). Suposem que tenim condicions de Dirichlet per la dreta i l'esquerra, és a dir, $q_l = q_r = 2$. (Els altres casos es resolen de manera similar.) De la primera equació, s'obté que

$$\begin{aligned} (2 - \lambda)u_1 - u_2 &= 2 \cos \alpha (Ae^{i\alpha} + Be^{-i\alpha}) - Ae^{i2\alpha} - Be^{-i2\alpha} = 0 \\ \Rightarrow A + B &= 0, \end{aligned}$$

on hem aplicat $\cos \alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2}$ i $\sin \alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}$. Per tant, $B = -A$ i, llevat d'una constant multiplicativa, podem suposar que

$$u_j = \sin(j\alpha), \quad j = 1, \dots, N.$$

D'altra banda, de (13) s'obté

$$(2 - \lambda)u_1 - u_2 = 2 \cos \alpha (Ae^{iN\alpha} + Be^{-iN\alpha}) - Ae^{i(N-1)\alpha} - Be^{-i(N-1)\alpha} = 0 \\ \Rightarrow \sin((N+1)\alpha) = 0.$$

Per tant, els possibles valors de α són $\alpha_k = \frac{k\pi}{N+1}$, per a $k = 1, \dots, N$, amb la qual cosa obtenim els valors propis

$$\lambda_k = 4 \sin^2 \left(\frac{k\pi}{2(N+1)} \right), \quad k = 1, \dots, N, \quad (17)$$

els quals compleixen que $\lambda_1 < \lambda_2 < \dots < \lambda_N$, amb els respectius vectors propis

$$\mathbf{u}_k = (u_{jk}) = \left(\sin \left(\frac{k\pi}{N+1} \right), \sin \left(\frac{2k\pi}{N+1} \right), \dots, \sin \left(\frac{Nk\pi}{N+1} \right) \right)^\top. \quad (18)$$

Finalment, com que les columnes de T han de ser ortonormals, tenim

$$\|\mathbf{u}_k\|^2 = \sum_{j=1}^N \sin^2 \left(\frac{jk\pi}{N+1} \right) = \frac{1}{2} \sum_{j=1}^N \left(1 - \cos \left(\frac{2jk\pi}{N+1} \right) \right) = \dots = \frac{N+1}{2},$$

on hem usat que $\sin^2 x = \frac{1}{2}(1 - \cos(2x))$ i la suma d'una sèrie geomètrica $\sum_{j=1}^N r^j = \frac{r(1-r^N)}{1-r}$. Concloem que les components de la matriu T són

$$T_{jk} = (u_{jk}) = \sqrt{\frac{2}{N+1}} \sin \left(\frac{jk\pi}{N+1} \right), \quad j, k = 1, \dots, N, \quad (19)$$

com s'indica a la taula 1.

3.2 Ortogonalitat

Considerem ara les propietats d'ortogonalitat que apareixen en el MOL, i les comparem amb les corresponents del mètode analític. En primer lloc, notem que, per ser una matriu simètrica, els elements de les subdiagonals de la matriu $\mathbf{Q} = (q_{jk})$ satisfan $q_{j,j+1}q_{j+1,j} > 0$ per a $j = 1, \dots, N$ i, per tant, donen lloc a una família de polinomis ortogonals $p_0, p_1, \dots, p_{N-1}$ de variable discreta.² Aquest és també el cas, per exemple, de la matriu quocient d'un graf distància-regular, els polinomis ortogonals del qual corresponen als anomenats *polinomis distància*. Els detalls d'aquesta aplicació, i altres de tipus combinatori, poden trobar-se a l'article de Cámara, Fàbrega, Fiol i Garriga [2].

² És a dir, polinomis ortogonals respecte d'un producte escalar discret en els punts d'una malla $x_1, \dots, x_N \in \mathbb{R}$: $\langle f, g \rangle = \sum_{j=1}^N w_j f(x_j) g(x_j)$ per a uns certs «pesos» $w_j > 0$. Els polinomis ortogonals es poden obtenir amb el mètode de Gram-Schmidt a partir de $1, x, x^2, \dots, x^{N-1}$ amb la normalització adequada.

Els polinomis $p_0, p_1, \dots, p_{N-1}$ constitueixen una successió de Sturm (vegeu Godsil [5, §8.5] o Chihara [3]) i satisfan una relació de recurrència de tres termes (com a l'expressió (12))

$$p_{k+1}(x) = (2-x)p_k(x) - p_{k-1}(x), \quad k = 1, \dots, N-2, \quad (20)$$

inicialitzada amb $p_0(x) = 1$ i $p_1(x) = 2-x$. A més, $p_N(x) = (2-x)p_{N-1}(x) - p_{N-2}(x)$ correspon al polinomi característic de la matriu $\mathbf{Q}$ i, per tant, les seves arrels són els valors propis λ_k , amb vectors propis

$$\mathbf{u}_k = (p_0(\lambda_k), p_1(\lambda_k), \dots, p_{N-1}(\lambda_k))^T, \quad k = 1, \dots, N,$$

trobat anteriorment a (17) i (18) (aquests últims llevat d'una constant multiplicativa). L'ortogonalitat esmentada s'obté respecte d'un producte escalar discret en els punts de la malla $\lambda_1, \lambda_2, \dots, \lambda_N$, amb $\lambda_1 < \lambda_2 < \dots < \lambda_N$. Per tant, un cop normalitzem els vectors $\mathbf{u}_k$, és a dir, $\bar{\mathbf{u}}_k = \mathbf{u}_k / \|\mathbf{u}_k\|$, obtenim de nou els elements de la matriu $\mathbf{T}$ donats a (19):

$$T_{j,k} = (\bar{\mathbf{v}}_k)_j, \quad j, k = 1, \dots, N,$$

és a dir,

$$T_{j,k} = \sqrt{\frac{2}{N+1}} \sin\left(\frac{jk\pi}{N+1}\right) = \frac{p_{j-1}(\lambda_k)}{\left(\sum_{j=0}^{N-1} p_j^2(\lambda_k)\right)^{\frac{1}{2}}}, \quad j, k = 1, \dots, N. \quad (21)$$

Compareu les funcions pròpies de la primera igualtat de (21) amb les del cas analític (23). Observeu que (21) es pot entendre com la versió discreta de (23).

En aquest context, observem que el potencial transformat $\bar{\mathbf{V}} = \mathbf{T}^T \mathbf{V}$ no és més que el vector de coeficients de Fourier obtingut en expressar V en termes d'uns polinomis ortogonals (que, en els punts de la malla, tenen els valors donats per cada fila de $\mathbf{T}$).

Per exemple, en el cas de la matriu $\mathbf{Q}$ a (10) amb $N = 5$ i $q_l = q_r = 2$, s'obtenen els polinomis

$$\begin{aligned} p_0(x) &= 1, \\ p_1(x) &= 2-x, \\ p_2(x) &= x^2 - 4x + 3, \\ p_3(x) &= -x^3 + 6x^2 - 10x + 4, \\ p_4(x) &= x^4 - 8x^3 + 21x^2 - 20x + 5, \\ p_5(x) &= -x^5 + 10x^4 - 36x^3 + 56x^2 - 35x + 6. \end{aligned}$$

Els valors propis de $\mathbf{Q}$ (les arrels de $p_5(x)$) són:

$$\lambda_1 = 2 - \sqrt{3}, \quad \lambda_2 = 1, \quad \lambda_3 = 2, \quad \lambda_4 = 3, \quad \lambda_5 = 2 + \sqrt{3}.$$

A la figura 2 es mostren les gràfiques de $p_j(x)$, per a $j = 0, \dots, 4$. Noteu les paritats (parells i senars) d'aquests polinomis respecte de $x = \lambda_3 = 2$, induïdes per les corresponents simetries de la matriu

$$T = \begin{pmatrix} \sqrt{3}/6 & 1/2 & \sqrt{3}/3 & 1/2 & \sqrt{3}/6 \\ 1/2 & 1/2 & 0 & 1/2 & 1/2 \\ \sqrt{3}/3 & 0 & -\sqrt{3}/3 & 0 & \sqrt{3}/3 \\ 1/2 & -1/2 & 0 & 1/2 & -1/2 \\ \sqrt{3}/6 & -1/2 & \sqrt{3}/3 & -1/2 & \sqrt{3}/6 \end{pmatrix}.$$

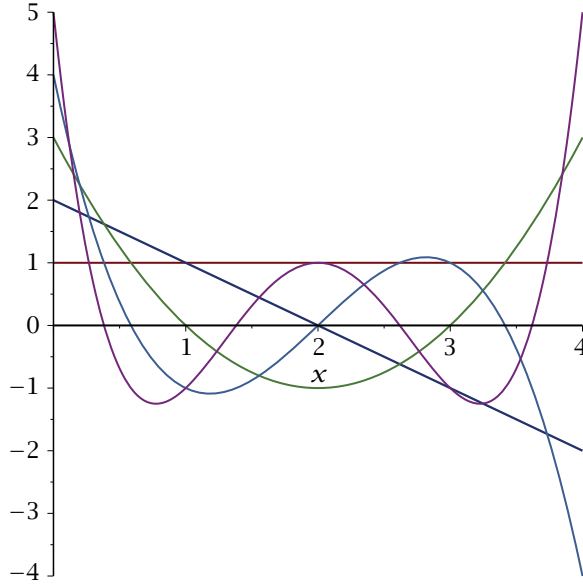


FIGURA 2: Els polinomis ortogonals $p_j(x)$ (de grau j), per a $j = 0, \dots, 4$.

4 Un exemple

Ara vegem com s'aplica el MOL a la resolució d'un problema concret: resoldre l'equació de Laplace (potencial)

$$\frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} = 0,$$

amb condicions de contorn de tipus Dirichlet $V(0, y) = V(a, y) = V(x, 0) = 0$ i $V(x, b) = 100$, amb $a = b = 1$ a la regió representada a la figura 3. També volem calcular el valor del potencial en els punts indicats en aquesta figura.

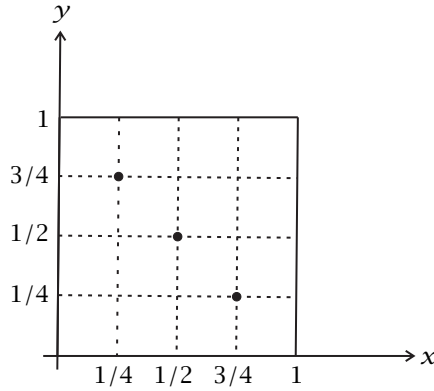


FIGURA 3: Regió on volem resoldre l'equació de Laplace amb el MOL.

La matriu $\mathbf{Q}$ té valors propis $\omega_k^2 = 4 \sin^2 \frac{k\pi}{2N+2}$, per a $k = 1, 2, \dots, N$, i la matriu de vectors propis $\mathbf{T}$ té components $T_{jk} = \sqrt{\frac{2}{N+1}} \sin \frac{jk\pi}{N+1}$ (vegeu la taula 1).

Si escollim $N = 15$, resulta que $h = \Delta x = \frac{1}{16}$, i les abscisses dels punts on volem calcular el potencial són $x_4 = \frac{1}{4}$, $x_8 = \frac{1}{2}$ i $x_{12} = \frac{3}{4}$.

De $V_j = \sum_{k=1}^N T_{jk} \bar{V}_k$, per a $j = 1, 2, \dots, N$, obtenim la solució

$$\begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_N \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1N} \\ T_{21} & T_{22} & \dots & T_{2N} \\ & & \ddots & \\ T_{N1} & T_{N2} & \dots & T_{NN} \end{pmatrix} \begin{pmatrix} A_1 \cosh \frac{\omega_1 y}{h} + B_1 \sinh \frac{\omega_1 y}{h} \\ A_2 \cosh \frac{\omega_2 y}{h} + B_2 \sinh \frac{\omega_2 y}{h} \\ \vdots \\ A_N \cosh \frac{\omega_N y}{h} + B_N \sinh \frac{\omega_N y}{h} \end{pmatrix}.$$

Ara, per determinar les constants A_j i B_j , imposem les condicions de contorn:

- $V(x, 0) = 0 \Rightarrow$

$$\begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_N \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1N} \\ T_{21} & T_{22} & \dots & T_{2N} \\ & & \ddots & \\ T_{N1} & T_{N2} & \dots & T_{NN} \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

d'on $A_j = 0$, per a $j = 1, 2, \dots, N$.

- $V(x, 1) = 100 \Rightarrow$

$$\begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_N \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1N} \\ T_{21} & T_{22} & \dots & T_{2N} \\ & & \ddots & \\ T_{N1} & T_{N2} & \dots & T_{NN} \end{pmatrix} \begin{pmatrix} B_1 \sinh \frac{\omega_1}{h} \\ B_2 \sinh \frac{\omega_2}{h} \\ \vdots \\ B_N \sinh \frac{\omega_N}{h} \end{pmatrix} = \begin{pmatrix} 100 \\ 100 \\ \vdots \\ 100 \end{pmatrix},$$

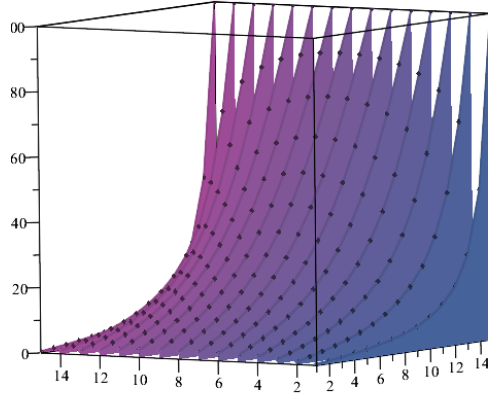


FIGURA 4: Gràfica dels potencials $V_j(y) = V(x_j, y)$, amb $x_j = jh$ i $j = 1, \dots, 15$, per a $V(x, 1) = 100$.

d'on

$$\begin{pmatrix} B_1 \sinh \frac{\omega_1}{h} \\ B_2 \sinh \frac{\omega_2}{h} \\ \vdots \\ B_N \sinh \frac{\omega_N}{h} \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} & \dots & T_{1N} \\ T_{21} & T_{22} & \dots & T_{2N} \\ & & \ddots & \\ T_{N1} & T_{N2} & \dots & T_{NN} \end{pmatrix}^\top \begin{pmatrix} 100 \\ 100 \\ \vdots \\ 100 \end{pmatrix} =: \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix}.$$

Per tant,

$$B_j = \frac{c_j}{\sinh \frac{\omega_j y}{h}}, \quad j = 1, 2, \dots, N.$$

Així, arribem a l'aproximació $\tilde{V}(x_j, y)$ de $V(x_j, y)$:

$$\begin{aligned} \tilde{V}(x_j, y) &= \sum_{k=1}^N T_{jk} B_k \sinh \left(\frac{\omega_k y}{h} \right) = \\ &= \sum_{k=1}^N \sqrt{\frac{2}{N+1}} \sin \left(\frac{jk\pi}{N+1} \right) \frac{c_k}{\sinh \left(\frac{\omega_k}{h} \right)} \sinh \left(\frac{\omega_k y}{h} \right), \end{aligned}$$

la qual està representada a la figura 4.

En els punts que ens interessen, els valors que s'obtenen amb el MOL (calculats amb el programa de la secció 7) són

$$\tilde{V}\left(\frac{1}{4}, \frac{3}{4}\right) = 43.1008, \quad \tilde{V}\left(\frac{1}{2}, \frac{1}{2}\right) = 24.9644, \quad \tilde{V}\left(\frac{3}{4}, \frac{1}{4}\right) = 6.7984$$

que, comparats amb els valors calculats analíticament aplicant la fórmula (24) de la secció 5,

$$V\left(\frac{1}{4}, \frac{3}{4}\right) = 43.2028, \quad V\left(\frac{1}{2}, \frac{1}{2}\right) = 24.9999, \quad V\left(\frac{3}{4}, \frac{1}{4}\right) = 6.7971, \quad (22)$$

demostran ser bones aproximacions.

5 El mètode analític

Ara volem resoldre el problema anterior amb el mètode analític, per poder-lo comparar amb el resultat obtingut amb el MOL. És a dir, ja que podem conèixer la solució analítica, emprem l'equació de Laplace com a test pel mètode de les línies.

Considerem, doncs, de nou l'equació

$$\nabla^2 V = \frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} = 0,$$

per a $x \in (0, a)$ i $y \in (0, b)$, amb condicions de contorn

$$\begin{aligned} V(0, y) &= V(a, y) = V(x, 0) = 0, \\ V(x, b) &= f(x), \end{aligned}$$

com es veu a la figura 5.

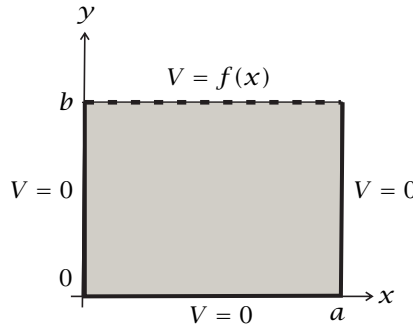


FIGURA 5: Regió on volem resoldre l'equació de Laplace amb el mètode analític.

La solució analítica s'obté per separació de variables, és a dir, suposant que el potencial és de la forma $V(x, y) = X(x)Y(y)$, d'on trobem que X i Y satisfan les equacions

$$\begin{aligned} X''(x) + \omega^2 X(x) &= 0, \\ Y''(y) - \omega^2 Y(y) &= 0. \end{aligned}$$

Imposant les condicions de contorn homogènies, resulta que $\omega = \omega_k = \frac{k\pi}{a}$ per a $k = 1, 2, \dots$ i obtenim les funcions

$$X(x) = B \sin\left(\frac{k\pi}{a}x\right),$$

$$Y(y) = C \sinh\left(\frac{k\pi}{a}y\right),$$

amb B i C constants. Per tant, les solucions del problema homogeni són:

$$V_k(x, y) = A_k \sinh\left(\frac{k\pi}{a}y\right) \sin\left(\frac{k\pi}{a}x\right). \quad (23)$$

Considerem ara una solució en forma de sèrie

$$V(x, y) = \sum_{k=1}^{\infty} A_k \sinh\left(\frac{k\pi}{a}y\right) \sin\left(\frac{k\pi}{a}x\right).$$

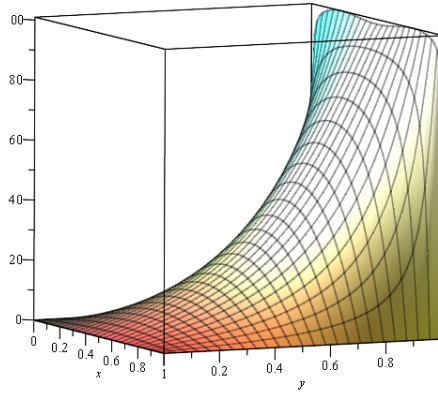


FIGURA 6: Gràfica del potencial $V(x, y)$ en el cas $a = b = 1$, $V(0, y) = V(a, y) = V(x, 0) = 0$ i $V(x, b) = 100$.

Si imposem la condició de contorn no homogènia

$$V(x, b) = f(x) = \sum_{k=1}^{\infty} A_k \sinh\left(\frac{k\pi}{a}b\right) \sin\left(\frac{k\pi}{a}x\right),$$

i considerem que $\{\sin(\frac{k\pi}{a}x) : k = 1, 2, \dots\}$ és una base ortogonal a $(0, a)$, obtenim el corresponent desenvolupament en sèrie de Fourier de $f(x)$, amb coeficients

$$\alpha_k = A_k \sinh\left(\frac{k\pi}{a}b\right) = \frac{2}{a} \int_0^a f(x) \sin\left(\frac{k\pi}{a}x\right) dx.$$

Per tant, la solució analítica és

$$V(x, y) = \sum_{k=1}^{\infty} \alpha_k \frac{\sinh\left(\frac{k\pi}{a}y\right)}{\sinh\left(\frac{k\pi}{a}b\right)} \sin\left(\frac{k\pi}{a}x\right).$$

Observem que les condicions de contorn *iguals* a zero a $x = 0$ i $x = a$ donen solucions periòdiques en *sinus*, mentre que les condicions de contorn *diverses* a $y = 0$ i $y = b$ donen solucions no periòdiques en *sinus hiperbòlics*.

En l'exemple anterior, utilitzant el MOL, consideràvem el cas particular $a = b = 1$ i $f(x) = 100$. En aquest cas, ara obtenim que $\alpha_n = \frac{400}{n\pi}$ per a n senar i $\alpha_n = 0$ per a n parell. Aleshores, la solució analítica és

$$V(x, y) = \frac{400}{\pi} \sum_{k=1}^{\infty} \frac{1}{2k-1} \frac{\sinh((2k-1)\pi y)}{\sinh((2k-1)\pi)} \sin((2k-1)\pi x), \quad (24)$$

la representació gràfica de la qual es mostra a la figura 6.

6 Sobre l'error

Podem calcular l'error comès quan utilitzem el mètode de les línies, simplement amb la diferència entre els resultats obtinguts amb el MOL i el mètode analític. De fet, se sap que, sota condicions generals de regularitat de les solucions, l'error del mètode de les línies és de l'ordre de $O(h^2)$ (vegeu, per exemple, Schiesser [8] o Zuazua [14, 15]).

Nosaltres estudiem primer el comportament de l'error en el cas de l'exemple anterior (secció 4). A la figura 7 es representen els errors de les aproximacions de $V(x_j, y)$ per a $j = 1, \dots, 8$; per bé que $N = 15$, per simetria en les condicions de contorn, hi ha set funcions d'error que se superposen a unes altres set.

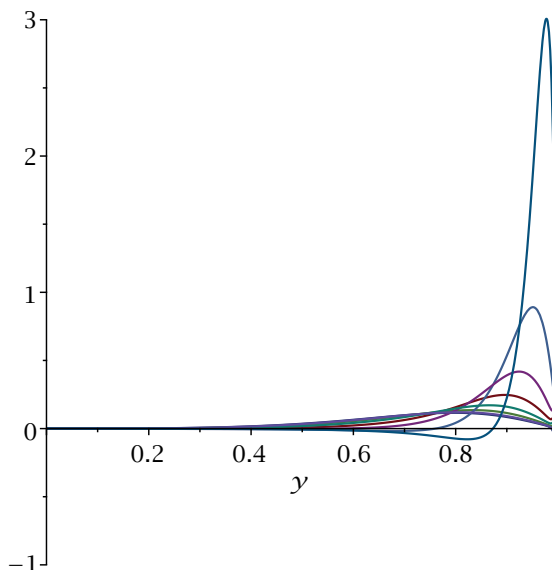


FIGURA 7: Gràfiques dels errors absoluts comesos en calcular el potencial amb el mètode de les línies en l'exemple de la secció 4 en comparació amb el mètode analític (secció 5).

Observem que tenim 8 funcions d'error (per a $x_j = j/16$, $j = 1, \dots, 8$) malgrat que $N = 15$ perquè, per simetria en les condicions de contorn, hi ha 7 funcions d'error que se superposen a altres 7 (i en queda una sense superposar). Com era d'esperar a causa de la discontinuïtat en les condicions de contorn, els errors són més petits quan som més a prop del centre de la gràfica (és a dir, per a $x_8 = 1/2$).

Per obtenir resultats més precisos, considerem ara un altre exemple més senzill, el qual ens permet donar la solució numèrica amb una fórmula tancada. Així, suposem ara que les condicions de contorn són $V(0, y) = V(1, y) = V(x, 0) = 0$, com abans, i que $V(x, 1) = \sinh(\pi) \sin(\pi x)$. Aleshores, per trobar la solució analítica no cal fer l'últim pas del desenvolupament en sèrie de Fourier, i s'obté

$$V(x, y) = \sinh(\pi y) \sin(\pi x), \quad (25)$$

la gràfica de la qual es mostra a la figura 8. Pel que fa al mètode de les línies, esmentem primer que aquest cas va ser resolt computacionalment per Subramanian i White [10] utilitzant matrius exponencials, encara que sense arribar a una expressió tancada. En canvi, les tècniques descrites aquí ens permeten obtenir la solució compacta següent

$$\tilde{V}(x_j, y) = \sinh[\pi \text{sinc}(h)y] \sin(\pi x_j), \quad (26)$$

on $x_j = jh$, $j = 1, \dots, N$, i $\text{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$. Vegeu la figura 9. Notem que, com que $\lim_{h \rightarrow 0} \text{sinc}(h) = 1$, quan $h \rightarrow 0$, $j \rightarrow \infty$, i $jh \rightarrow x$, aleshores $\tilde{V}(x_j, y) \rightarrow V(x, y)$, com era d'esperar. De fet, en aquest cas és fàcil comprovar que, per a cada y , l'error $\epsilon = V(x_j, y) - \tilde{V}(x_j, y)$ és de l'ordre de $O(h^2)$, com ja hem comentat.

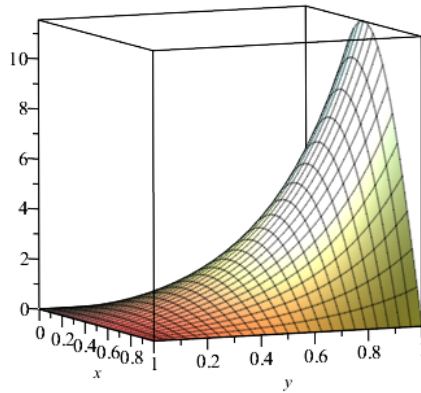


FIGURA 8: Gràfica del potencial $V(x, y)$ en el cas $a = b = 1$, $V(0, y) = V(a, y) = V(x, 0) = 0$ i $V(x, b) = \sinh(\pi) \sin(\pi x)$.

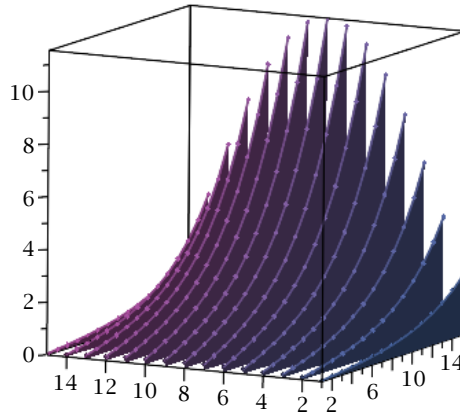


FIGURA 9: Gràfica del potencial $V_j(y) = V(x_j, y)$, $x_j = jh$, $j = 1, \dots, 15$, per a $V(x, b) = \sinh(\pi) \sin(\pi x)$.

7 Programa en MATLAB

A continuació, escrivim en el llenguatge del programa MATLAB les instruccions per calcular el valor del potencial en els tres punts interiors que es consideren a l'exemple de la secció 4.

```
>> AA=1;
>> BB=1;
>> N=15;
>> %Determinem el vector alpha
>> H=AA/(N+1);
>> LAMBDA=2*sin((1:N)*pi*0.5/(N+1));
>> ALPHA=LAMBDA/H;
>> %Calculem la matriu de transformació
>> S=sqrt(2/(N+1));
>> T=zeros(N,N);
>> for J=(1:N)
>>     for K=(1:N)
>>         T(J,K)=S*sin(J*K*pi/(N+1));
>>     end
>> end
>> V=100*ones(N,1);
>> C=inv(T)*V;
>> A=ALPHA';
>> B=C./sinh(BB*A);
>> %Calculem V en els punts donats
>> V1=0; V2=0; V3=0;
>> for K=1:N
```

```

V1=V1+T(4,K)*B(K)*sinh(ALPHA(K)*0.75);
V2=V2+T(8,K)*B(K)*sinh(ALPHA(K)*0.5);
V3=V3+T(12,K)*B(K)*sinh(ALPHA(K)*0.25);
end
>> diary
>> V1, V2, V3
      V1 = 43.1008
      V2 = 24.9644
      V3 = 6.7984
>> diary off

```

8 Altres exemples resolubles amb el MOL

Finalment, detallem alguns altres exemples que es poden resoldre amb el mètode de les línies.

1. L'equació de Laplace en la regió quadrada 1×1 amb condicions de contorn:
 - (a) Dirichlet-Neumann.
 - (b) Neumann-Dirichlet.
 - (c) Neumann-Neumann.

(Els valors a utilitzar de la matriu T i els valors propis ω_k^2 són a la taula 1.)

2. L'equació de Laplace en coordenades cilíndriques $\rho^2 \frac{\partial^2 V}{\partial \rho^2} + \rho \frac{\partial V}{\partial \rho} + \frac{\partial^2 \phi}{\partial \phi^2} = 0$, amb les condicions de contorn $V(\rho, \phi) = 0$ per a $0 \leq \rho \leq a$ i $V(\rho, \phi) = V_0$ per a $a < \rho \leq b$, amb la discretització de la coordenada angular ϕ . La solució analítica és $V(\rho) = V_0 \frac{\ln(\frac{\rho}{a})}{\ln(\frac{b}{a})}$.
3. L'equació d'ona $\frac{\partial^2 v}{\partial t^2} - \frac{\partial^2 v}{\partial x^2} = q(x, t)$, amb $0 \leq x \leq L$ i $0 \leq t \leq T$, les condicions inicials $v(x, 0) = f_1(x)$ i $\frac{\partial v}{\partial t}(x, 0) = f_2(x)$ per a $0 \leq x \leq L$, la condició de contorn de Dirichlet $v(0, t) = g_1(x)$ i la condició no local $\int_0^L v(x, t) dx = g_2(x)$ per a $0 \leq t \leq T$. A la taula següent hi ha alguns casos particulars amb la corresponent solució analítica.

L	T	$q(x, t)$	$f_1(x)$	$f_2(x)$	$g_1(t)$	$g_2(t)$	$v(x, t)$ analítica
1	4	0	0	$\pi \cos(\pi x)$	$\sin(\pi t)$	0	$\cos(\pi x) \sin(\pi t)$
1	5	$-2(x-t)e^{-x-t}$	0 0	xe^{-x}	0 0	$-2te^{-t-1} + te^{-t}$	xte^{-x-t} xte^{-x-t}
1	4	0	$\cos(\pi x)$	0	$\cos(\pi t)$	0	$\frac{1}{2} \cos(\pi(x+t)) + \frac{1}{2} \cos(\pi(x-t))$
1	5	$2x^5 + 2x^3 - 2x^2 - (20x^3 + 6x - 2) \cdot (t^2 - t)$	0	$-x^5 - x^3 + x^2$	0	$\frac{t(t-1)}{12}$	$(x^5 + x^3 - x^2) \cdot (t^2 - t)$

9 Conclusions

El mètode de les línies ha demostrat ser una bona eina per resoldre alguns tipus d'equacions en derivades parcials amb condicions de contorn. Com que es basa a discretitzar totes les variables excepte una, es pot utilitzar directament en l'equació de Laplace, la qual hem fet servir com a exemple il·lustratiu. Una alternativa és aplicar el mètode de les falses transicions, afegint una derivada temporal i discretitzant les variables espacials. Si estem al pla xy , l'error d'aquest mètode alternatiu és de l'ordre de $\Delta_x^2 + \Delta_y^2$. Per tant, és millor aplicar el mètode semidiscret (o semianalític), que és el que hem aplicat, i en el qual hem vist que l'error és de l'ordre de Δ_x^2 .

Per una altra banda, es pot estudiar com canvia l'error si, en comptes de prendre línies equiespaiades, considerem línies situades als zeros dels polinomis de Tchebixov (els quals tenen un millor comportament respecte de l'error). En aquest context, es pot consultar el treball de Youssef i Shukur [12]. Finalment, proposem el següent problema obert: Estudiar les semblances i les diferències entre el MOL i la integració al llarg de les rectes característiques de l'equació en derivades parcials de primer ordre $\frac{\partial V}{\partial t} + c \frac{\partial V}{\partial x} = f(x, t)$, amb $c > 0$.

Agraïments

Els autors volen agrair els comentaris i suggeriments del revisor anònim, els quals han contribuït considerablement a millorar aquest treball.

Aquest treball ha estat parcialment finançat per l'AGAUR del govern català amb el projecte 2017SGR1087 i pel MICINN del govern espanyol amb el projecte PGC2018-095471-B-I00.

La primera autora també ha estat parcialment finançada pel MICINN amb el projecte MTM2017-83271-R i pel projecte de la Unió Europea Marie Skłodowska-Curie 734922 dins del programa Horizon 2020. 

Referències

- [1] BERARDI, A.; VURRO, M. «The numerical solution of Richards' equation by means of method of lines and ensemble Kalman filter». *Math. Comput. Simulation*, 125 (2016), 38-47.
- [2] CÁMARA, M.; FÀBREGA, J.; FIOL, M. A.; GARRIGA, E. «Some families of orthogonal polynomials of a discrete variable and their applications to graphs and codes». *Electron. J. Combin.*, 16 (1) (2009). (Research Paper; 83, 30 p.)
- [3] CHIHARA, T. S. *An Introduction to Orthogonal Polynomials*. Nova York; Londres; París: Gordon and Breach Science Publishers, 1978. (Mathematics and its Applications; 13)
- [4] DIESTEL, H. «Analysis of planar multiconductor transmission-line systems with the method of lines». *Arch. Elektron. Übertragungstechn.*, 41 (3) (1987), 169-175.

- [5] GODSIL, C. D. *Algebraic Combinatorics*. Nova York: Chapman & Hall, 1993. (Chapman and Hall Mathematics Series)
- [6] SADIKU, M. N. O. *Computational Electromagnetics with Matlab*. 4a ed. Boca Raton; Londres; Nova York: CRC Press, 2018.
- [7] SADIKU, M. N. O.; OBIOZOR, C. N. «A simple introduction to the method of lines». *Int. J. Elec. Eng. Educ.*, 37 (3) (2000), 282–296.
- [8] SCHIESSER, W. E. *The Numerical Method of Lines. Integration of Partial Differential Equations*. San Diego, CA: Academic Press, Inc., 1991.
- [9] SHAKERI, F.; DEHGHAN, M. «The method of lines for solution of the one-dimensional wave equation subject to an integral conservation condition». *Comput. Math. Appl.*, 56 (9) (2008), 2175–2188.
- [10] SUBRAMANIAN, V. R.; WHITE, R. E. «Semianalytical method of lines for solving elliptic partial differential equations». *Chem. Eng. Sci.*, 59 (4) (2004), 781–788.
- [11] VERWER, J. G.; SANZ-SERNA, J. M. «Convergence of method of lines approximations to partial differential equations». *Computing*, 33 (3–4) (1984), 297–313.
- [12] YOUSSEF, I. K.; SHUKUR, A. M. «The line method combined with spectral Chebyshev for space-time fractional diffusion equation». *Appl. Comput. Math.*, 3 (6) (2014), 330–336.
- [13] ZAFARULLAH, A. «Application of the method of lines to parabolic partial differential equations with error estimates». *J. Assoc. Comput. Mach.*, 17 (1970), 294–302.
- [14] ZUAZUA, E. «Introducción al análisis numérico de ecuaciones en derivadas parciales de evolución». Notes d'un curs introductori al càlcul numèric d'equacions diferencials. Universidad Autónoma de Madrid, 2003. http://verso.mat.uam.es/web/ezuazua/documentos_public/archivos/personal/comites/1_anedpde2.pdf.
- [15] ZUAZUA, E. «Métodos numéricos de resolución de ecuaciones en derivadas parciales». Basque Center for Applied Mathematics (BCAM), 2009. Notes.

CRISTINA DALFÓ
 DEPARTAMENT DE MATEMÀTICA
 UNIVERSITAT DE LLEIDA
 IGUALADA (BARCELONA), CATALUNYA
cristina.dalfo@matematica.udl.cat

MIQUEL ÀNGEL FIOL
 DEPARTAMENT DE MATEMÀTIQUES
 BARCELONA GRADUATE SCHOOL OF MATHEMATICS
 UNIVERSITAT POLITÈCNICA DE CATALUNYA
 BARCELONA, CATALUNYA
miguel.angel.fiol@upc.edu

Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació

MERCÈ VILLANUEVA I CRISTINA FERNÁNDEZ-CÓRDOBA

«Maleït sigui! Si les màquines poden detectar un error, per què no podem localitzar la posició de l'error i corregir-lo?», 1947.

Richard W. Hamming (1915–1998)

Resum: En les transmissions digitals d'informació d'un emissor a un receptor a través d'un canal, normalment es produeixen errors. En aquest article s'exposen els conceptes i resultats més importants de la teoria de codis detectors i correctors d'errors, que estudia mètodes eficients per garantir una transmissió exacta de la informació. Primer es descriuen alguns exemples quotidians de codis detectors d'errors inclosos en el DNI, l'ISBN, l'IBAN i l'EAN. A continuació, es presenta la teoria clàssica dels codis correctors d'errors, que inclou els codis lineals i, dins d'aquests, els codis cíclics, que resulten més eficients a l'hora de codificar. També es descriuen les dues famílies més importants de codis cíclics, els BCH i Reed-Solomon, que permeten descodificar també de forma eficient. Finalment, es mostren dues aplicacions històriques, en les memòries d'ordinador i en la transmissió de fotografies a l'espai, i dues aplicacions més recents, en els codis QR i en l'emmagatzematge distribuït.

Paraules clau: detecció d'errors, correcció d'errors, codis lineals, codis cíclics, BCH, Reed-Solomon, aplicacions.

Classificació MSC2010: 94B05, 94B15, 11T71.

1 Introducció

Cap a l'any 1948, Claude E. Shannon va formular en els seus treballs el problema de la transmissió d'informació en termes estadístics, utilitzant models probabilístics per a les fonts d'informació i els canals de comunicació [41]. Amb aquests treballs va néixer un nou camp anomenat *teoria de la informació* [1], dins del qual es troba la teoria matemàtica de la comunicació digital, que estudia la transmissió de la informació entre un emissor i un receptor a través d'un

canal. En molts casos, els canals que es fan servir són insegurs i amb soroll, com, per exemple, en la comunicació entre dos telèfons mòbils via satèl·lit, on la informació viatja per l'espai a través d'ones.

Així, en general, la informació pot ser interceptada i manipulada per tercers. A més, es poden produir errors i interferències que alteren el senyal transmès, cosa que fa que el receptor no rebi exactament la mateixa informació que havia enviat l'emissor. Altres exemples de comunicació digital es troben en la televisió digital, l'emmagatzematge de dades en diferents dispositius (memòries, CD, Blu-ray, etc.), Internet, Internet de les coses (IoT), etc.

En la transmissió d'informació es consideren diferents mecanismes, de manera que es pugui garantir que la comunicació entre l'emissor i el receptor sigui eficient, segura i exacta. La figura 1 mostra un esquema general d'un sistema de comunicació digital a través d'un canal insegur i amb soroll. Per tal que la transmissió sigui més eficient, s'aplica un compressor que permet reduir la mida de les dades que volem enviar aprofitant la redundància que aquestes presenten. També es pot realitzar un procés de xifratge (també conegut com a *encriptació*) per tal d'evitar que un tercer pugui accedir a les dades i garantir així la seva confidencialitat i/o autenticitat. Finalment, per assegurar una comunicació fiable i exacta, es codifiquen fent servir codis correctors d'errors. És en aquesta darrera fase, estudiada dins de l'anomenada *teoria de la codificació*, en la qual ens centrarem en aquest article.

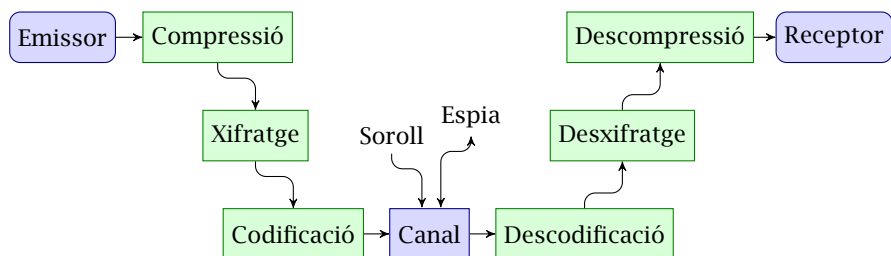


FIGURA 1: Sistema de comunicació digital.

Inicialment, la teoria de la codificació es trobava dins de l'àmbit de l'enginyeria electrònica o informàtica. A més, els canals considerats eren binaris i, per tant, els codis estudiats estaven definits sobre el cos $\mathbb{Z}_2$. A poc a poc, la teoria de la codificació s'ha anat endinsant més en l'àmbit matemàtic. Per una banda, s'ha anat dotant els codis de certa estructura algebraica que ha anat fent més eficient el procés de codificar i decodificar; i, per una altra banda, s'han considerat codis sobre alfabetos diferents. Primer, es van començar a estudiar codis sobre cossos finits. A partir del 1994, arran de l'article [18], on es van estudiar codis sobre $\mathbb{Z}_4$, van començar a tenir més importància els codis sobre anells en general. També s'han considerat codis sobre alfabetos mixtos (les coordenades es troben en diferents anells) [5]. Actualment, dins del camp de la teoria de la codificació, hi ha una vessant més d'enginyeria que estudia l'aplicació de mètodes de codificació i decodificació a diferents

sistemes de comunicació, i una altra vessant més matemàtica que estudia les diferents estructures algebraïques, geomètriques i combinatòries dels codis, la construcció de nous codis, l'existència de codis amb certes propietats, i la seva classificació.

Durant la transmissió de dades digitals (normalment en forma de seqüència de bits) a través de canals amb soroll, es poden produir errors i, per tant, no rebre a la sortida del canal exactament les mateixes dades que s'havien enviat. Per exemple, pot haver-hi soroll tèrmic generat per l'equipament electrònic. Els codis correctors d'errors tenen com a objectiu detectar aquests errors i corregir-los. Aquest procés permet, per exemple, rebre bones imatges des dels satèl·lits, o gaudir de la música emmagatzemada en un CD encara que el disc estigui ratllat. El preu que s'ha de pagar per corregir els errors és afegir una certa redundància a les dades que es volen transmetre.

No només en les transmissions d'informació, on el canal és un cable, l'aire o l'espai, és necessari disposar de mecanismes que puguin permetre la detecció i, si és possible, la correcció d'errors. Si considerem, per exemple, que el canal és el paper o un disc dur, ens podem plantejar si en escriure i emmagatzemar algun número llarg, volem poder detectar possibles errors. En aquests canals, els errors més freqüents són equivocar-se introduint algun dígit o bé intercanviant dos dígitos. Per poder detectar aquests tipus d'errors, usualment s'afegeix redundància incorporant un nou símbol al número. Així és com s'han dissenyat codis tan quotidians com el codi del document nacional d'identitat o DNI, l'*International Standard Book Number* o ISBN dels llibres, l'*International Bank Account Number* o IBAN i el Codi de Compte Corrent o CCC dels comptes bancaris, i l'*European Article Number* o EAN, que formen part dels coneguts codis de barres, que descriurem en la secció 2.

En la secció 3, introduïrem els conceptes de la teoria clàssica dels codis correctors d'errors. Primer ens centrarem en els codis lineals basats en conceptes d'àlgebra. A continuació, descriurem els codis lineals cíclics o codis cíclics que permeten codificar la informació de forma més eficient. Finalment, presentarem les dues famílies més importants de codis cíclics, els codis BCH i Reed-Solomon, que permeten també descodificar de forma eficient i que, per tant, són els que es fan servir en moltes situacions en què és necessari poder corregir errors i evitar una retransmissió de les dades.

Els primers codis lineals, els codis de Hamming, s'expliquen en la secció 4, on es veu la seva aplicació en les primeres memòries d'ordinador. En la secció 5, es descriuen els codis de Reed-Muller de primer ordre, coneguts també com a *codis de Hadamard*. A més, es mostra com alguns d'aquests codis es van utilitzar per millorar la transmissió de fotografies a l'espai. En la secció 6, ens centrarem en l'aplicació dels codis BCH i Reed-Solomon dins dels coneguts *codis QR (Quick Response)*, que representen una evolució dels codis de barres, d'una a dues dimensions. Finalment, en la secció 7, veurem una aplicació recent dels codis correctors d'errors en el camp de l'emmagatzematge distribuït.

2 Exemples quotidians de codis detectors d'errors

En aquesta secció, descriurem alguns dels codis detectors d'errors més coneguts, ja esmentats en la introducció: el codi associat al DNI, l'ISBN dels llibres, l'IBAN i el CCC dels comptes bancaris, i l'EAN o codi de barres. Tots ells són força quotidians i ens els trobem tot sovint en el dia a dia. A més, tots estan basats en l'aritmètica modular i detecten, però no permeten, corregir els errors. A part d'aquests, n'hi ha molts més, com els que apareixen en les targetes de crèdit, els bitllets d'avió o els serveis de missatgeria, entre d'altres.

2.1 Codi DNI

El codi del document nacional d'identitat (DNI) consisteix en un número de 8 xifres decimals seguit d'una lletra. Aquesta lletra, de fet, representa la redundància que permetrà detectar els errors més freqüents en escriure el número. La lletra s'assigna segons el valor que resulta de calcular el número del DNI a $\mathbb{Z}_{23}$, o el que és el mateix, segons el residu que s'obté en dividir-lo per 23, d'acord amb les equivalències que es mostren en la taula 1.

0	1	2	3	4	5	6	7	8	9	10	11
T	R	W	A	G	M	Y	F	P	D	X	B
12	13	14	15	16	17	18	19	20	21	22	
N	J	Z	S	Q	V	H	L	C	K	E	

TAULA 1: Assignació de lletres per al DNI.

El càlcul es realitza a $\mathbb{Z}_{23}$. Es pren un número primer per tal de treballar en un cos finit. A més, s'exclouen les lletres I, O i U, perquè aquestes es poden confondre més fàcilment amb l'1, el 0 i la lletra V, respectivament. Podem simplificar els càlculs si tenim precalculades les potències de 10 a $\mathbb{Z}_{23}$. Així, com que $10^2 = 8$, $10^3 = 11$, $10^4 = 18$, $10^5 = 19$, $10^6 = 6$ i $10^7 = 14$ a $\mathbb{Z}_{23}$, calcular el número del DNI a $\mathbb{Z}_{23}$ equival a calcular $x_0 + 10x_1 + 8x_2 + 11x_3 + 18x_4 + 19x_5 + 6x_6 + 14x_7$ a $\mathbb{Z}_{23}$, on $x_7x_6x_5x_4x_3x_2x_1x_0 = \sum_{i=0}^7 10^i x_i$ representa el número del DNI.

EXEMPLE 1. La lletra del DNI corresponent al número 34149351 és D, ja que $34149351 = 9$ a $\mathbb{Z}_{23}$, o equivalentment, $14 \cdot 3 + 6 \cdot 4 + 19 \cdot 1 + 18 \cdot 4 + 11 \cdot 9 + 8 \cdot 3 + 10 \cdot 5 + 1 = 9$ a $\mathbb{Z}_{23}$, i la lletra corresponent al valor 9 és D d'acord amb la taula 1.

Aquest codi permet detectar si hi ha hagut un error en un dels dígit del DNI, o bé si hi ha hagut una transposició entre dos dígit [6]. En canvi, si n'hi ha dos o més, no sempre es poden detectar. També permet recuperar un dels dígit si aquest no es visualitza correctament, simplement resolent una equació lineal a $\mathbb{Z}_{23}$.

EXEMPLE 2. Continuant amb el DNI de l'exemple 1, què passa si en escriure el DNI ens equivoquem en un dígit i escrivim, per exemple, 34249351D? Com

que $34249351 = 5$ a $\mathbb{Z}_{23}$ i la lletra corresponent al 5 és la M, podem detectar que hi ha hagut un error, i repassar l'escriptura d'aquest DNI.

I si ens equivoquem en dos dígitos que s'han intercanviat de posició, i escrivim, per exemple, 34419351D? En aquest cas, de nou, en calcular $34419351 = 12$ a $\mathbb{Z}_{23}$, podem detectar l'error ja que 12 correspon a la lletra N.

Finalment, què podem fer si un dels dígitos és borrós, per exemple, si tenim 341493□1D on el setè dígit no es reconeix? En aquest cas, podem plantejar l'equació lineal següent a $\mathbb{Z}_{23}$, $14 \cdot 3 + 6 \cdot 4 + 19 \cdot 1 + 18 \cdot 4 + 11 \cdot 9 + 8 \cdot 3 + 10 \cdot x_1 + 1 = 9$, o sigui $10x_1 = 4$ a $\mathbb{Z}_{23}$. Com que l'invers de 10 és 7, tenim que $x_1 = 4 \cdot 7 = 28 = 5$ a $\mathbb{Z}_{23}$. Per tant, el dígit de la posició setena és 5 i obtenim el DNI 34149351D.

2.2 Codi ISBN

Cada llibre porta associat un identificador únic, l'anomenat *International Standard Book Number* (ISBN) [27], que consisteix en una seqüència de 10 símbols en què cadascun pot ser un element de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$ i X representa el 10. Les operacions es realitzen a $\mathbb{Z}_{11}$, a diferència del codi DNI, que eren a $\mathbb{Z}_{23}$. El darrer símbol representa la redundància i es calcula a partir dels anteriors. Aquest codi també permet detectar si, durant la transcripció d'aquest identificador, s'ha produït un error en algun dels seus dígitos o la transposició de dos d'ells [6, 12].

EXEMPLE 3. Els identificadors 0-444-85010-4 i 84-732-9114-X corresponen als codis ISBN dels llibres *The Theory of Error-Correcting Codes*, de Florence J. MacWilliams i Neil J. A. Sloane, en l'editorial North-Holland, i *Mirall trencat*, de Mercè Rodoreda, en l'editorial Club Editor, respectivament.

Dels 10 símbols, els que apareixen abans del primer guió fan referència a l'idioma/país, els símbols entre el primer i el segon guió identifiquen l'editorial, els següents identifiquen el llibre dins de l'editorial, i finalment el darrer representa la redundància. A partir dels nou primers símbols, denotats per $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$, es calcula la redundància x_{10} com a $x_{10} = x_1 + 2x_2 + 3x_3 + \dots + 9x_9$ a $\mathbb{Z}_{11}$. Si el resultat és 10, escrivim el símbol X.

EXEMPLE 4. Continuant amb el primer ISBN que apareix en l'exemple 3, si en escriure'l ens equivoquem en un símbol i escrivim, per exemple, 0-444-85510-4, aleshores en calcular x_{10} obtenim que $x_{10} = 6$ en comptes de 4. Per tant, podem detectar que hi ha hagut un error, i repassar-ne la transcripció. De forma similar, si ens equivoquem en dos símbols consecutius que s'han intercanviat de posició, i escrivim per exemple, 0-444-58010-4, de nou en calcular x_{10} obtenim que $x_{10} = 7 \neq 4$ i així detectem que hi ha hagut algun error. Finalment, és fàcil veure que si un dels símbols no es reconeix, podem obtenir-lo resolent una equació lineal a $\mathbb{Z}_{11}$.

2.3 Codi IBAN i CCC

Els comptes bancaris tenen associat un codi, anomenat *International Bank Account Number* (IBAN), que consisteix en una seqüència d'un màxim de 34 ca-

ràcters alfanumèrics que identifiquen, de forma única, un compte bancari d'una determinada entitat financera [24]. Els dos primers caràcters identifiquen el país. Els dos següents són dígit de control que es calculen a partir de la resta, com veurem tot seguit. La resta corresponen al número de compte bancari i permeten identificar també l'entitat i l'oficina, en la majoria de països.

EXEMPLE 5. La seqüència BG18RZBB91550123456789 correspon al codi IBAN d'un possible compte bancari a Bulgària, i la seqüència ES021234567806011155555 a un a Espanya. A Bulgària tots els codis IBAN tenen exactament 22 caràcters i a Espanya en tenen 24.

Per calcular els dos dígit de control, situats en les posicions tercera i quarta de la seqüència, es procedeix de la forma següent. Les dues primeres lletres corresponents al país es traslladen a les dues darreres posicions, s'eliminen els dos dígit de control i s'afegeixen dos zeros al final. Els caràcters se substitueixen per un número de dues xifres d'acord amb la taula 2 i es calcula el número obtingut a $\mathbb{Z}_{97}$. Finalment, per evitar utilitzar com a dígit de control el 00 i 01, es resta el valor obtingut a 98, i s'obtenen els dos dígit de control. Si el resultat conté un únic dígit, s'afegeix un zero al davant.

10	11	12	13	14	15	16	17	18	19	20	21	22
A	B	C	D	E	F	G	H	I	J	K	L	M
23	24	25	26	27	28	29	30	31	32	33	34	35
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

TAULA 2: Assignació numèrica per a l'IBAN.

EXEMPLE 6. Els dos dígit de control de l'IBAN BG18RZBB91550123456789 són 18. A continuació comprovem que és correcte. Primer, traslladem les dues primeres lletres al final, eliminem els dos dígit de control i afegim dos zeros al final, per tant, obtenim RZBB91550123456789BG00. A continuació, substituint els caràcters per valors numèrics segons la taula 2, arribem al número 2735111191550123456789111600, que és igual a 80 a $\mathbb{Z}_{97}$. Els dígit de control són efectivament $98 - 80 = 18$.

Com en els dos codis anteriors, el DNI i l'ISBN, el codi IBAN també permet detectar possibles errors produïts en una única posició o transposicions de dos caràcters, així com recuperar-ne un que aparegui il·legible.

A Espanya, el codi IBAN es va implantar definitivament l'1 de febrer del 2014 aprofitant l'antic codi de compte corrent (CCC). De fet, el codi IBAN es construeix a partir del codi CCC, que té 20 xifres decimals, afegint al davant els dos caràcters ES corresponents al país i els dos dígit de control que hem explicat abans, fins a completar els 24 caràcters.

El codi CCC està format per 20 dígit. Els 4 primers dígit identifiquen l'entitat bancària, els 4 següents identifiquen l'oficina, els 2 següents són dígit de control, i finalment els darrers 10 descriuen el número de compte bancari.

Així, aquest codi el podem representar de la manera següent:

$$x_3x_4x_5x_6 \quad x_7x_8x_9x_{10} \quad c_1c_2 \quad y_1y_2y_3y_4y_5y_6y_7y_8y_9y_{10}.$$

El primer dígit de control c_1 es calcula a partir dels 8 díigits anteriors, d'acord amb l'equació següent $c_1 = -\sum_{i=3}^{10} 2^{i-1}x_i = 7x_3 + 3x_4 + 6x_5 + x_6 + 2x_7 + 4x_8 + 8x_9 + 5x_{10}$ a $\mathbb{Z}_{11}$, i el segon c_2 , a partir dels 10 díigits següents com a $c_2 = -\sum_{i=1}^{10} 2^{i-1}y_i = 10y_1 + 9y_2 + 7y_3 + 3y_4 + 6y_5 + y_6 + 2y_7 + 4y_8 + 8y_9 + 5y_{10}$ a $\mathbb{Z}_{11}$. Si en fer aquests càlculs obtenim un 10 a $\mathbb{Z}_{11}$, assignem el dígit 1. Fixem-nos que en els dos casos la fórmula és la mateixa considerant que $x_1 = x_2 = 0$ per al càlcul de c_1 . Aquests codis tenen les mateixes propietats per detectar errors o corregir un esborrall (dígit borrós que no es reconeix) que els codis anteriors, excepte en alguns casos en què en fer els càlculs obtenim $c_i \in \{1, 10\}$.

EXEMPLE 7. El codi CCC, corresponent al codi IBAN ES0212345678060111555555, és 12345678060111555555, on 1234 representaria una entitat bancària i 5678 una oficina d'aquesta entitat. Si a l'hora de transcriure aquest compte bancari, escrivim 12345678060111655555, aleshores en calcular els díigits de control c_1 i c_2 obtenim que $c_1 = 0$ però $c_2 = 1$ en comptes de 6. Per tant, haurem detectat que hi ha algun error, i que aquest es troba dins dels darrers 10 díigits.

2.4 Codi EAN

La majoria dels productes comercials porten associat un número de 13 xifres decimals anomenat *European Article Number* (EAN) o, més recentment, *International Article Number*. L'EAN apareix just a sota d'un codi de barres que serveix per facilitar-ne la lectura. Els dos o tres primers díigits identifiquen l'estat o associació a la qual està registrat el fabricant, els següents de 5 a 8 díigits identifiquen l'empresa, els següents fins al 12è, el producte, i finalment el darrer és el dígit de control [25, 20].

El dígit de control es calcula a partir dels anteriors. Si l'EAN de 13 xifres el denotem per $x_1x_2 \dots x_{13}$, aleshores x_{13} es calcula de la manera següent: $x_{13} = -\sum_{i=1}^6 (x_{2i-1} + 3x_{2i}) = 9x_1 + 7x_2 + 9x_3 + 7x_4 + 9x_5 + 7x_6 + 9x_7 + 7x_8 + 9x_9 + 7x_{10} + 9x_{11} + 7x_{12}$ a $\mathbb{Z}_{10}$. Igual que els codis detectors que hem vist en les subseccions anteriors, el codi EAN permet detectar si s'ha produït un error en un dels díigits, però en canvi no permet detectar sempre la transposició de dos díigits. Concretament, si s'intercanvien dos díigits diferents, x_i i x_j , tals que i i j tenen la mateixa paritat, o bé $x_i - x_j = 5$, la transposició no es detecta [6, 20]. També és fàcil veure que podem recuperar un dígit il·legible, ja que l'1 i el 3 (o equivalentment, els seus oposats, el 9 i el 7) són invertibles a $\mathbb{Z}_{10}$.

EXEMPLE 8. Si l'empresa utilitza el codi EAN de l'Associació Espanyola de Codificació Comercial (AECOC), els dos primers díigits són 84. En canvi, en altres països com Alemanya els primers díigits són números del 400 al 440.

Si tenim el número següent 1512345678909, de 13 xifres, podem comprovar fàcilment que és un codi EAN vàlid. Si es produeix un error en un dels dígit, i obtenim per exemple 1518345678909, podem detectar l'error, ja que el dígit de control hauria de ser 1 en lloc de 9. Si s'intercanvien dos dígit no sempre es detecta. Per exemple, si obtenim 1512340678959 degut a un intercanvi entre les posicions 7a i 12a, podem comprovar que el dígit de control és correcte i per tant l'error no es detecta. En canvi, si l'intercanvi es produeix entre les posicions 1a i 6a, es detectaria, ja que 4512315678909 hauria de tenir el 5 com a dígit de control.

3 Teoria clàssica sobre codis correctors d'errors

En la subsecció 3.1, veurem els conceptes bàsics de la teoria dels codis correctors d'errors. Descriurem els tres paràmetres més importants que defineixen un codi i especificarem quan aquest és òptim. A continuació, en la subsecció 3.2, ens centrarem en els codis que són lineals i els mètodes generals per codificar i descodificar aquests codis. En la subsecció 3.3, descriurem els codis lineals cíclics que permeten codificar i descodificar de forma més eficient. Finalment, en la subsecció 3.4, ens centrarem en dues famílies importants de codis cíclics: els anomenats *codis BCH* i *Reed-Solomon*. Si es vol aprofundir en aquesta teoria clàssica dels codis correctors d'errors, es pot consultar, per exemple, [23, 31, 38].

3.1 Codis q -aris lineals i no lineals

Com hem dit, si volem detectar i/o corregir els possibles errors que es produeixen en les transmissions a través de canals amb soroll, hem d'afegir certa redundància a la informació que volem transmetre, expandint-la de forma que hi hagi certa «distància» entre dues informacions diferents, que serà la que ens permetrà corregir errors i aconseguir així una transmissió al més fiable i exacta possible.

EXEMPLE 9. Suposem que volem transmetre una seqüència de bits a través d'un canal binari simètric amb probabilitat d'error p , BSC(p), on p és la probabilitat que el bit de sortida sigui diferent al d'entrada i satisfà que $0 < p < 1/2$. Per tal de reduir aquesta probabilitat p , en comptes d'enviar un 0 o un 1, enviem 000 o 111, respectivament. Per exemple, si volem transmetre 1101, enviem 111111000111 a través del canal BSC(p). Suposem que a la sortida del canal rebem 101100001111. A continuació, descodifiquem segons el nombre de zeros i uns que hi ha en cada bloc de 3 bits. Per exemple, si rebem 101, com que hi ha més uns que zeros, descodifiquem per 111. Així, obtenim 111000000111, o sigui 1001. Observem que alguns errors s'han corregit i altres no. En tot cas, aquest mètode permet reduir la probabilitat d'error fins a $p' = p^3 + 3p^2(1 - p) = p^2(3 - 2p)$. Per exemple, si $p = 0.02$, aleshores $p' = 0.001184$, i diem que hem obtingut un guany de $10 \log_{10}(p/p') \approx 12.28$ dB. El preu que paguem és que hem triplicat el nombre de símbols que s'envien pel canal i per tant es fa més lenta la transmissió.

Considerem un alfabet amb q elements. Normalment es tria que q sigui una potència d'un nombre primer i l'alfabet un cos finit $\mathbb{F}_q$. Un *codi q -ari* C és un conjunt finit de vectors o seqüències sobre $\mathbb{F}_q$, anomenades *paraules codi*. Si totes les seqüències són de la mateixa longitud n , aleshores diem que C és un *codi bloc* de longitud n . En aquest cas, $C \subseteq \mathbb{F}_q^n$, on $\mathbb{F}_q^n$ és un espai vectorial sobre $\mathbb{F}_q$. A partir d'ara ens centrarem en els codis bloc i suposarem que la informació a transmetre està representada per una seqüència d'elements de l'alfabet $\mathbb{F}_q$. En una transmissió fent servir codis bloc, la informació que volem transmetre es divideix primer en blocs de k símbols de $\mathbb{F}_q$. Després, a cadascun d'aquests blocs, se li assigna una paraula codi de longitud n del codi q -ari C . Per tant, C ha d'estar format per un mínim de q^k paraules codi; en particular, cal que $k \leq n$. Aquest procés d'assignació s'anomena *codificació*.

És fàcil veure que com més separades estiguin aquestes paraules codi entre elles, més errors permetrà corregir el codi. Així, es defineix la *distància (de Hamming)* entre dos vectors $v = (v_1, \dots, v_n)$ i $w = (w_1, \dots, w_n)$, que denotarem per $d_H(v, w)$, com el nombre de coordenades que tenen diferents. El *pes (de Hamming)* d'un vector $v = (v_1, \dots, v_n)$, denotat per $\text{wt}_H(v)$, és el nombre de coordenades diferents de zero i, per tant, $\text{wt}_H(v) = d_H(v, \mathbf{0})$, on $\mathbf{0}$ és el vector zero. La distància de Hamming defineix una mètrica a $\mathbb{F}_q^n$ [38, p. 114]. La descodificació per mínima distància tria la paraula codi més propera al vector rebut, d'acord amb aquesta distància. Aquest mètode minimitza la probabilitat mitjana d'error, i coincideix amb la descodificació per màxima versemblança [38, p. 128], si cada símbol de l'alfabet té la mateixa probabilitat d'error p i la mateixa probabilitat d'aparèixer. Un canal amb aquestes dues propietats s'anomena *canal q -ari simètric*. Quan $q = 2$, s'anomena *canal binari simètric* o BSC(p).

La *distància mínima* d'un codi q -ari C és $d(C) = \min\{d_H(v, w) : v, w \in C, v \neq w\}$. En general, calcular la distància mínima d'un codi és computacionalment difícil i s'ha demostrat que és un problema NP-difícil [44]. Si un codi q -ari C de longitud n sobre $\mathbb{F}_q$ conté M paraules codi i té distància mínima $d = d(C)$, direm que és un codi q -ari (n, M, d) . La *taxa de transmissió* de C és $R = \log_q(M)/n$ i mesura la proporció d'informació que conté cada paraula codi.

Trobar algorismes de descodificació eficients és una de les àrees d'investigació més importants en la teoria de codis ateses les seves aplicacions pràctiques. Si en enviar una paraula codi $c \in C$ es rep el vector $w \in \mathbb{F}_q^n$, diem que $e = w - c$ és el *vector d'error*. La descodificació consisteix a trobar el vector d'error e a partir de w , que equival a trobar la paraula codi c enviada. Entre tots els possibles vectors d'errors triem el de pes menor, que equival a triar la paraula codi a menor distància de w .

Direm que un codi C *detecta* el vector d'error e si i només si $c + e \notin C$ per a qualsevol $c \in C$, i direm que *corregeix* el vector d'error e si i només si per a tot $c \in C$, $c + e$ és més proper a c que a qualsevol altra paraula codi. Si un codi C corregeix tots els vectors d'error de pes com a molt t , i no en pot corregir com a mínim un de pes $t + 1$, direm que és *t -corrector* o que t és la *capacitat correctora* de C . De forma similar es defineix la *capacitat detectora*.

i que el nombre de paraules codi M també sigui gran per codificar el major nombre de missatges. Aquestes condicions no es poden assolir totes alhora ateses les relacions que hi ha entre aquests paràmetres. Per exemple, tenim que $M \leq q^n$. També es compleix l'anomenada *fita de Singleton*, $M \leq q^{n-d+1}$; i la *fita de Hamming*,

$$M \cdot \sum_{i=0}^t \binom{n}{i} (q-1)^i \leq q^n, \quad (1)$$

on $t = \lfloor (d-1)/2 \rfloor$ és la capacitat correctora del codi [31, p. 20]. Es diu que un codi és *òptim* si té els millors paràmetres possibles n, M, d, q , és a dir, al mateix temps no es pot incrementar M per a valors de n, d, q fixats, i no es pot incrementar d per a valors de n, M, q fixats.

3.2 Codis lineals

Direm que un codi q -ari C de longitud n sobre un cos finit $\mathbb{F}_q$ és *lineal* si és un subespai de $\mathbb{F}_q^n$. De fet, qualsevol subespai de $\mathbb{F}_q^n$ és un codi q -ari lineal. Si $k = \dim(C)$ i $d = d(C)$, direm que és un codi $[n, k, d]_q$ o $[n, k]_q$ en comptes d'un codi q -ari (n, q^k, d) . En aquest cas, la taxa de transmissió és $R = k/n$, ja que $M = q^k$. A més, és fàcil veure que si C és lineal, aleshores $d = \min\{\text{wt}_H(v) : v \in C, v \neq \mathbf{0}\}$, o sigui, la distància mínima coincideix amb el pes mínim [38, p. 125].

Una matriu quadrada sobre $\mathbb{F}_q$ és *monomial* si té exactament una entrada diferent de zero en cada fila i columna. Diem que dos codis lineals C i C' sobre $\mathbb{F}_q$ de la mateixa longitud n són *equivalents* si existeix una matriu monomial M de mida $n \times n$ sobre $\mathbb{F}_q$ i un automorfisme γ de $\mathbb{F}_q$ tal que $C' = \{\gamma(cM) : c \in C\}$, on γ s'aplica coordenada a coordenada [23, p. 24]. És clar que si dos codis són equivalents, aleshores tenen els mateixos paràmetres $[n, k, d]_q$ i R .

Si C és un codi lineal $[n, k]_q$, una *matriu generadora* G de C és una matriu $k \times n$ sobre $\mathbb{F}_q$ que conté com a files una base de C . En la codificació fent servir codis lineals, a cada vector d'informació $i \in \mathbb{F}_q^k$ li podem assignar la paraula codi $c = iG \in C \subseteq \mathbb{F}_q^n$. Si la matriu G conté la matriu identitat de mida k com a submatriu, aleshores les coordenades de i apareixen en les coordenades de $c = iG$, exactament en les mateixes posicions on es troben les columnes de la matriu identitat dins de G . En aquest cas, direm que la matriu G és *sistemàtica* o que la codificació és *sistemàtica* en aquestes coordenades.

Segui G una matriu generadora d'un codi C lineal $[n, k]_q$. Observem que tota matriu que tingui per files una base de C és una matriu generadora de C . Per tant, sempre podem triar una matriu generadora de C sistemàtica. En canvi, si permutem les columnes de G , obtenim una nova matriu G' que genera un nou codi C' equivalent al codi C . És fàcil veure que qualsevol codi lineal C és equivalent a un codi C' generat per una matriu de la forma $G' = (I_k \ A)$, on I_k és la matriu identitat de mida k i A és una matriu $k \times (n-k)$ sobre $\mathbb{F}_q$. En aquest cas, direm que la matriu G' està en *forma estàndard* i que la codificació

és sistemàtica en les k primeres coordenades. La utilització del codi C' amb matriu generadora G' simplifica el procés d'obtenir la informació després de la correcció d'errors, ja que aquesta està localitzada directament en les primeres k coordenades.

EXEMPLE 12. Dels codis de l'exemple 11, tenim que C_1 és un codi lineal $[3, 1, 3]_2$ amb matriu generadora $G_1 = (1 \ 1 \ 1)$. En canvi, el codi C_2 no és lineal, ja que $(1, 2, 1, 2) + (1, 1, 2, 2) = (2, 0, 0, 1) \notin C_2$. El codi C_3 és lineal amb paràmetres $[5, 2, 3]_3$ i pot ser generat a partir de la matriu generadora següent:

$$G_3 = \begin{pmatrix} 2 & 1 & 0 & 2 & 0 \\ 2 & 1 & 1 & 1 & 2 \end{pmatrix}.$$

Així, abans d'enviar a través d'un canal ternari la seqüència d'informació, primer la dividim en blocs de $k = 2$ elements de $\mathbb{F}_3$ i a continuació multipliquem cada bloc per G_3 i obtenim blocs de $n = 5$ elements. Per exemple, si la informació és 10 21 22 11, enviem $(1, 0)G_3$, $(2, 1)G_3$, $(2, 2)G_3$ i $(1, 1)G_3$, o sigui 21020 00122 21201 12102, a través del canal. És fàcil veure que C_3 és equivalent (permutant la 2a i 3a coordenades i realitzant combinacions lineals de files) a un codi C'_3 generat per la matriu següent en forma estàndard:

$$G'_3 = (I_2 \ A) = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 & 2 \end{pmatrix}.$$

Si codifiquem la mateixa informació, utilitzant la matriu G'_3 , obtenim 10210 21112 22101 11202. Fixem-nos que, en aquest cas, la codificació és sistemàtica en les dues primeres coordenades, o sigui, la informació està localitzada en les dues primeres coordenades de cada paraula codi.

Per descriure el mètode general de descodificació per a codis lineals, necessitem definir el codi ortogonal (o dual) i la matriu de control. El producte escalar entre dos vectors, $v = (v_1, \dots, v_n)$ i $w = (w_1, \dots, w_n)$, és $\langle v, w \rangle = \sum_{i=1}^n v_i w_i$. El *codi ortogonal* (o *dual*) d'un codi C lineal $[n, k]_q$, denotat per $C^\perp$, és $C^\perp = \{v \in \mathbb{F}_q^n : \langle v, c \rangle = 0 \ \forall c \in C\}$. És fàcil veure que $C^\perp$ és un codi lineal $[n, n - k]_q$. Qualsevol matriu generadora H del codi $C^\perp$ s'anomena *matriu de control* de C . A més, si $G = (I_k \ A)$, aleshores una matriu de control és $H = (-A^t \ I_{n-k})$, on A^t denota la matriu transposada de A . També tenim que, a partir d'una matriu de control, es pot determinar la distància mínima d'un codi, tal com mostra la proposició 13. Tot i aquest resultat, calcular la distància mínima d'un codi lineal continua sent un problema NP-difícil [44].

PROPOSICIÓ 13 ([38, p. 125]). *La distància mínima d'un codi lineal C coincideix amb el mínim nombre de columnes linealment dependents que hi ha en una matriu de control de C .*

EXEMPLE 14. En l'exemple 12, hem vist que el codi C_3 és equivalent al codi C'_3 generat per la matriu $G'_3 = (I_2 \ A)$ en forma estàndard. Per tant, el codi ortogonal $C_3'^\perp$ està generat per la matriu següent:

$$H'_3 = (-A^t \ I_3) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

que és també una matriu de control de C'_3 . Com que hem obtingut C'_3 a partir de C_3 permutant la 2a i 3a coordenades, podem obtenir una matriu de control de C_3 , desfent la permutació que havíem fet; és a dir, permutant la 2a i la 3a columnes de H'_3 . Així, la matriu següent és una matriu de control de C_3 :

$$H_3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Com que el mínim nombre de columnes linealment dependents de H_3 és 3, per exemple, les columnes 1, 2 i 4, podem veure que $d(C_3) = 3$ per la proposició 13.

El mètode general per descodificar codis lineals s'anomena *descodificació via síndrome* [23, p. 61]. Com que un codi lineal C es pot veure com un subgrup del grup additiu $\mathbb{F}_q^n$, les diferents classes d'equivalència $C + v$ representen una partició de $\mathbb{F}_q^n$ en q^{n-k} conjunts de mida q^k . Dos vectors v_1 i v_2 estan en la mateixa classe si i només si $v_1 - v_2 \in C$. Suposem que enviem una paraula codi $c \in C$ i rebem el vector $w = c + e \in \mathbb{F}_q^n$. En la descodificació, volem trobar la paraula codi c' més propera a w , o equivalentment, el vector d'error e' de pes mínim dins de la classe $C + w$ que conté w . Un vector de pes mínim en una classe s'anomena *líder de la classe* i no necessàriament és únic. El vector zero és l'únic líder de la classe C . De forma més general, si el pes del líder de la classe és menor o igual a la capacitat correctora t , aleshores aquest líder és únic.

La *síndrome* d'un vector $v \in \mathbb{F}_q^n$, respecte a una matriu de control H d'un codi lineal C , és el vector $Hv^t \in \mathbb{F}_q^{n-k}$. Els vectors que tenen com a síndrome el vector zero són exactament els corresponents a totes les paraules codi. Com que H té rang $n - k$, qualsevol vector de $\mathbb{F}_q^{n-k}$ és una síndrome. A més, com que tots els vectors d'una mateixa classe tenen la mateixa síndrome, existeix una bijecció entre les classes mòdul C i les seves síndromes. Per tant, podem construir l'anomenada *taula de síndromes*, que assigna a cada síndrome un líder de la classe corresponent (si no és únic se'n tria un de forma aleatòria). Fixem-nos que la descodificació via síndrome requereix una taula amb q^{n-k} entrades, que pot ser molt menor comparat amb una taula amb q^n vectors mostrant quina paraula codi és la més propera a cada vector de l'espai.

En una descodificació completa s'assigna una paraula codi a cada vector rebut $w \in \mathbb{F}_q^n$. Per això, primer calculem la síndrome de w . Si és zero, sabem

que no hi ha hagut cap error. En canvi, si és diferent de zero, utilitzem la taula de síndromes per trobar l'error e' i la paraula codi $c' = w - e' \in C$. En una descodificació incompleta podem reduir la taula de síndromes considerant només aquelles síndromes que tenen un líder amb pes menor o igual a la capacitat correctora t , o sigui quan el líder de la classe és únic. En aquest cas, quan la síndrome del vector rebut no es troba en la taula, es demana retransmetre aquest vector.

EXEMPLE 15. Considerem el codi C'_3 donat a l'exemple 12 i la seva matriu de control H'_3 donada a l'exemple 14. Per descodificar, utilitzant aquesta matriu de control H'_3 , primer construïm la taula 3 de síndromes.

líder	síndrome	líder	síndrome	líder	síndrome
00000	000	00001	001	20002	212
10000	120	00002	002	22000*	202
20000	210	12000	112	11000*	101
01000	022	21000	221	00102	102
02000	011	10002*	122	00201	201
00100	100	01100	111	20200*	110
00200	200	02200	222	10100*	220
00010	010	01200*	211	02020*	012
00020	020	10001	121	01010*	021

TAULA 3: Taula de síndromes per al codi C'_3 amb matriu de control H'_3 .

Suposem que hem codificat la informació utilitzant la matriu G'_3 . Com que la capacitat correctora de C'_3 és $t = 1$, si el vector d'error té pes 1, l'error es corregeix. En canvi, si el vector d'error té pes 2, segons quin sigui, pot passar que el vector rebut es descodifiqui correctament o que es descodifiqui com si s'hagués produït un altre error de pes 1 o 2. En la taula 3, apareixen marcats amb un * aquells líders que no són únics.

Si volem transmetre la informació 10 21 22 11, enviem a través del canal la seqüència codificada 10210 21112 22101 11202 calculada a l'exemple 12. Suposem que a la sortida del canal rebem 20210 20012 22211 01002. Per a cada bloc w de longitud $n = 5$ calculem la síndrome, el vector d'error e' a partir de la taula 3, i la paraula codi c' corresponent:

c	e	$w = c + e$	síndrome	líder e'	$c' = w - e'$
10210	10000	20210	120	10000	10210
21112	02200	20012	222	02200	21112
22101	00110	22211	110	20200	02011
11202	20100	01002	010	00010	01022

TAULA 4

Observem que en els dos primers blocs l'error s'ha corregit, tant el de pes 1 com el de pes 2, ja que els líders de les dues classes corresponents són únics. En el tercer bloc, el líder de la classe no és únic i se n'ha triat un de diferent al de l'error real e per a la construcció de la taula de síndromes. En el quart bloc, el líder és únic però el vector d'error e de pes 2 té la mateixa síndrome que un de pes 1, i es tria el de menor pes, o sigui una paraula codi a menys distància del vector rebut. Finalment, després d'intentar corregir els errors, s'obté la informació associada a cada paraula codi, que en aquest cas està situada en les dues primers coordenades, ja que s'ha codificat amb la matriu generadora G'_3 que està en forma estàndard. O sigui, obtenim que la informació enviada era 10 21 02 01.

Hi ha molts codis importants que s'obtenen modificant o combinant altres codis. Això es pot fer de diverses maneres, i a continuació en descriurem algunes. Per exemple, és possible crear codis més llargs, afegint noves coordenades. Concretament, donat un codi C lineal $[n, k, d]_q$, el seu *codi estès* (*extended code*), denotat per $\hat{C}$, és el codi

$$\hat{C} = \left\{ (x_1, \dots, x_n, x_{n+1}) : (x_1, \dots, x_n) \in C \text{ i } \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

El codi estès $\hat{C}$ és un codi lineal $[n+1, k, \hat{d}]_q$, on $\hat{d} \in \{d, d+1\}$ [23, p. 15]. Aquest procés també es coneix com afegir un dígit de control de paritat. Fixem-nos que si C és un codi binari, aleshores totes les paraules codi de $\hat{C}$ tenen pes parell. Per tant, $\hat{d} = d$ si d és parell i $\hat{d} = d+1$ si d és senar. En general, podem obtenir una matriu generadora de $\hat{C}$ afegint a una matriu generadora de C una columna extra, de forma que la suma de totes les coordenades de cada fila sigui zero. Si H és una matriu de control de C , aleshores la matriu $\hat{H}$ següent és una matriu de control del codi $\hat{C}$:

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

El *codi punxat* (*punctured code*) en la j -èsima coordenada d'un codi C lineal $[n, k, d]_q$, denotat per C^j , és el codi format per les paraules codi de C després d'eliminar la coordenada j -èsima de cada una. Aquest és un codi lineal $[n-1, k, d']_q$, on $d' \in \{d, d-1\}$, si $d > 1$ [23, p. 13]. Si G és una matriu generadora de C , aleshores podem obtenir una matriu generadora de C^j eliminant la columna j (i eliminant també possibles files repetides o de zeros) de G .

Finalment, per definir el *codi escurçat* (*shortened code*) en la j -èsima coordenada d'un codi C lineal $[n, k, d]_q$, denotat per C_0^j , definim primer el subcodi $C_0 \subseteq C$ format per les paraules codi de C que tenen un 0 en la coordenada

j -èsima. El codi C_0^j és el codi C_0 després d'eliminar la j -èsima coordenada de totes les seves paraules codi, o sigui, és el codi punxat de C_0 en la coordenada j -èsima. A més, fixem-nos que és un subcodi de C^j , és a dir, $C_0^j \subseteq C^j$, i és un codi $[n-1, k', d']_q$, on $k' \in \{k-1, k\}$ i $d \leq d'$ [23, p. 16].

EXEMPLE 16. Sigui C el codi $[7, 3, 3]_2$ amb la matriu generadora següent:

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

El codi estès $\hat{C}$ és el codi $[8, 3, 4]_2$ generat per $\hat{G}$; el codi punxat C^5 en la 5a coordenada és el codi $[6, 3, 2]_2$ generat per G^5 , i el codi escurçat C_0^5 en la 5a coordenada té paràmetres $[6, 2, 4]_2$ i està generat per G_0^5 , on

$$\hat{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad G^5 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

$$G_0^5 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3.3 Codis cíclics

Donat un vector $v = (v_1, \dots, v_n) \in \mathbb{F}_q^n$, definim la seva permutació cíclica $\pi(v)$ com el vector $\pi(v) = (v_n, v_1, \dots, v_{n-1})$. Direm que un codi q -ari lineal C de longitud n és *cíclic* si la permutació cíclica de qualsevol paraula codi torna a ser una paraula codi, o sigui, $\pi(c) \in C$ per a tot $c \in C$. Fixem-nos que, per linealitat, és suficient veure que la permutació cíclica de qualsevol fila d'una matriu generadora pertany al codi per afirmar si un codi lineal és cíclic o no.

EXEMPLE 17. Considerem els codis C_1 , C_2 i C_3 de l'exemple 11. El codi lineal C_1 és cíclic, ja que $\pi(c) = c \in C_1$ per a tot $c \in C_1$. El codi C_2 no és lineal, tal com s'ha vist a l'exemple 12, i, per tant, no pot ser un codi cíclic. Finalment, el codi lineal C_3 , amb matriu generadora G_3 donada en l'exemple 12 i matriu de control H_3 calculada en l'exemple 14, no és cíclic. Si considerem, per exemple, la paraula codi c corresponent a la primera fila de G_3 , $\pi(c) = \pi(2, 1, 0, 2, 0) = (0, 2, 1, 0, 2) \notin C_3$ ja que $H_3(0, 2, 1, 0, 2)^t = (2, 1, 0)^t \neq (0, 0, 0)^t$.

Un codi q -ari cíclic de longitud n es pot descriure en termes més algebraics, relacionant-lo amb l'anell de polinomis $R_{q,n} = \mathbb{F}_q[x]/(x^n - 1)$. Per fer-ho, considerem la bijecció següent:

$$\mathbb{F}_q^n \rightarrow R_{q,n}$$

$$v = (v_1, v_2, \dots, v_n) \mapsto v(x) = v_1 + v_2x + \dots + v_nx^{n-1}.$$

Fixem-nos que el polinomi associat a la permutació cíclica d'un vector $v \in \mathbb{F}_q^n$, $\pi(v)(x)$, és $xv(x)$. Sigui $C \subseteq \mathbb{F}_q^n$ un codi q -ari qualsevol. A partir d'ara, C denotarà indistintament tant el codi a $\mathbb{F}_q^n$ com la seva imatge per la bijecció anterior. Així, tenim que un codi lineal C és cíclic si i només si $xc(x) \in C$ per a tot $c(x) \in C$. Per linealitat, també tenim que C és cíclic si i només si $a(x)v(x) \in C$ per a tot $a(x) \in R_{q,n}$. Per tant, els codis cíclics a $\mathbb{F}_q^n$ es corresponen amb els ideals de $R_{q,n}$.

Sabem que els ideals de l'anell $R_{q,n}$ són principals [30] i, per tant, estan generats per només un element. Si C és un codi cíclic, aleshores existeix un únic polinomi mònic $g(x) \in \mathbb{F}_q[x]$ tal que $g(x) \mid (x^n - 1)$ i $C = \langle g(x) \rangle$ [23, capítol 4]. Aquest polinomi s'anomena *polinomi generador* de C i coincideix amb l'únic polinomi mònic de grau mínim del codi.

TEOREMA 18 ([23, CAPÍTOL 4]). *Sigui C un codi q -ari cíclic de longitud n i $g(x) \in \mathbb{F}_q[x]$ el polinomi generador de C . Aleshores,*

- (i) *la dimensió de C és $k = n - \text{grau}(g(x))$,*
- (ii) *una base de C és $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$, i*
- (iii) *una matriu generadora de C és*

$$G = \begin{pmatrix} g_1 & g_2 & \dots & g_{n-k+1} & 0 & 0 & \dots & 0 \\ 0 & g_1 & g_2 & \dots & g_{n-k+1} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & g_1 & g_2 & \dots & g_{n-k+1} \end{pmatrix}. \quad (2)$$

És fàcil veure que si C és un codi cíclic, aleshores el seu codi ortogonal, $C^\perp$, també ho és. A continuació, veiem que una matriu generadora i el polinomi generador de $C^\perp$ es poden donar en funció del polinomi generador de C . Definim el polinomi $h(x) = (x^n - 1)/g(x)$. Diem que $h(x) = h_1 + h_2x + \dots + h_{k+1}x^k$ és el *polinomi de control* de C , ja que $c(x) \in C$ si i només si $h(x)c(x) = 0$ a $R_{q,n}$. A partir d'aquesta darrera igualtat de polinomis, tenim que una matriu de control de C és

$$H = \begin{pmatrix} h_{k+1} & h_k & \dots & h_1 & 0 & 0 & \dots & 0 \\ 0 & h_{k+1} & h_k & \dots & h_1 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & h_{k+1} & h_k & \dots & h_1 \end{pmatrix}. \quad (3)$$

El *polinomi recíproc* de $h(x)$, denotat per $h^*(x)$, és el polinomi mònic que té els mateixos coeficients que $h(x)$, però en ordre invers i dividits per h_1 ; és a dir, $h^*(x) = x^k h(x^{-1})/h_1$. Com que H també és una matriu generadora de $C^\perp$, tant el conjunt $\{h_1 h^*(x), h_1 x h^*(x), \dots, h_1 x^{n-k-1} h^*(x)\}$ com el conjunt $\{h^*(x), x h^*(x), \dots, x^{n-k-1} h^*(x)\}$ són una base de $C^\perp$. Per tant, el

polinomi $h^*(x)$ és de fet el divisor de $x^n - 1$ que genera el codi $C^\perp$, o sigui $C^\perp = \langle h^*(x) \rangle$ [38, p. 146].

EXEMPLE 19. El polinomi $g(x) = 1 + x + x^3$ divideix $x^7 - 1 \in \mathbb{F}_2[x]$. Aleshores, $C = \langle g(x) \rangle$ és un codi binari cíclic de longitud 7 i dimensió $7 - 3 = 4$. El polinomi de control del codi és $h(x) = (x^7 - 1)/(1 + x + x^3) = 1 + x + x^2 + x^4$ i el polinomi generador de $C^\perp$ és $h^*(x) = 1 + x^2 + x^3 + x^4$. A partir d'aquests polinomis, obtenim, respectivament, les matrius generadora i de control de C següents:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \text{i} \quad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Utilitzar codis cíclics suposa un avantatge en el procés de codificar respecte dels codis lineals, tant des del punt de vista de l'espai de memòria com de la seva implementació física a través dels circuits LFSR (*linear feedback shift register*) [38, p. 148]. Sigui $C = \langle g(x) \rangle \subseteq R_{q,n}$ un codi cíclic i $i = (i_1, \dots, i_k) \in \mathbb{F}_q^k$ un vector d'informació que volem codificar. A continuació, veurem diverses maneres de codificar la informació i , és a dir, d'assignar a i una paraula codi de C .

Atès que C és un codi lineal, es pot codificar multiplicant per una matriu generadora. Per exemple, podem assignar a i la paraula codi $c = iG$, on G és la matriu (2). També podem fer combinacions lineals per files en la matriu G fins a obtenir una matriu generadora G' en forma estàndard, i assignar a i la paraula codi $c = iG'$. Aquesta seria una codificació sistemàtica en les primeres k coordenades.

També es pot codificar utilitzant el polinomi generador $g(x)$. Considerem el polinomi associat al vector d'informació, $i(x) = i_1 + i_2x + \dots + i_kx^{k-1}$. Per exemple, podem assignar a i la paraula codi c corresponent al polinomi $c(x) = i(x)g(x) \in R_{q,n}$. En aquest cas, la codificació de i seria igual a l'obtinguda fent iG . En canvi, si volem una codificació sistemàtica, aleshores podem assignar a i la paraula codi c corresponent a $c(x) = i(x)x^{n-k} - r(x)$, on $r(x)$ és el residu de dividir $i(x)x^{n-k}$ per $g(x)$. Aquesta darrera codificació s'anomena CRC (*cyclic redundancy check*), és fàcil veure que és sistemàtica en les darreres k coordenades i es pot implementar fàcilment fent servir circuits LFSR.

Finalment, podem codificar utilitzant el polinomi recíproc de $h(x)$, $h^*(x) = h_1^* + h_2^*x + \dots + h_k^*x^{k-1} + x^k$. A partir de la igualtat $Hc^t = \mathbf{0}$, on H és la matriu (3), obtenim que podem assignar a i la paraula codi $c = (i_1, \dots, i_k, c_{k+1}, \dots, c_n)$, on $c_i = -\sum_{j=1}^k h_j^* c_{i-k+j-1}$ per $i \in \{k+1, \dots, n\}$ [23, p. 129]. Clarament, aquesta codificació és sistemàtica en les primeres k coordenades.

EXEMPLE 20. Considerem el codi $C = \langle g(x) \rangle$, on $g(x) = 1 + x + x^3$, de l'exemple 19. A continuació, codifiquem el vector d'informació $i = (1, 0, 1, 1)$ de diverses maneres.

A partir de la matriu generadora G donada en l'exemple 19, la codificació de i seria $c = iG = (1, 1, 1, 1, 1, 1)$. Aquesta coincideix amb multiplicar $i(x)$ per $g(x)$ a $R_{q,n}$, ja que $i(x) = 1 + x^2 + x^3$ i $c(x) = i(x)g(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$. Ara bé, si fem servir el mètode CRC tenim que $r(x) = 1$ i $c(x) = (1 + x^2 + x^3)x^3 - 1 = 1 + x^3 + x^5 + x^6$, que es correspon amb el vector $c = (1, 0, 0, 1, 0, 1, 1)$. Podem veure que en aquest cas la codificació és sistemàtica en les quatre darreres posicions. Finalment, fent servir $h^*(x) = 1 + x^2 + x^3 + x^4$, tenim que $c = (1, 0, 1, 1, c_5, c_6, c_7)$ i, aplicant la fórmula $c_i = -\sum_{j=1}^4 h_j^* c_{i+j-5}$, per $i \in \{5, 6, 7\}$, obtenim $c_5 = 1$, $c_6 = 0$ i $c_7 = 0$. Així, el vector codificat és $c = (1, 0, 1, 1, 1, 0, 0)$.

Hem vist que els codis cíclics de longitud n són ideals de l'anell $R_{q,n}$ i el polinomi generador és, de fet, un polinomi mònic divisor de $x^n - 1$ a $\mathbb{F}_q[x]$. Per tant, per a l'estudi d'aquests codis, s'utilitza la factorització de $x^n - 1$ a $\mathbb{F}_q[x]$ [30].

Sigui m l'enter positiu més petit tal que $n \mid q^m - 1$; o sigui, l'ordre multiplicatiu de q mòdul n . Així, $\mathbb{F}_{q^m}$ és el mínim cos de característica q que conté totes les arrels de $x^n - 1$ i s'anomena *cos de descomposició* de $x^n - 1$. Les arrels de $x^n - 1$ formen un subgrup cíclic del grup multiplicatiu de $\mathbb{F}_{q^m}$. Per tant, $x^n - 1 = \prod_{j=0}^{n-1} (x - \alpha^j)$, on $\alpha \in \mathbb{F}_{q^m}$ és una arrel n -èsima primitiva de la unitat [23, 31].

Ara que ja tenim la factorització de $x^n - 1$ a $\mathbb{F}_{q^m}[x]$, donarem la seva factorització a $\mathbb{F}_q[x]$. Donat un enter s , $0 \leq s \leq n - 1$, la *classe q -ciclotòmica de s mòdul n* és $C_s = \{s, sq, sq^2, \dots, sq^{m-1}\}$, on $sq^m \equiv s \pmod{n}$. El conjunt $\{0, \dots, n - 1\}$ es pot escriure com la unió disjunta de classes q -ciclotòmiques. El *polinomi mínim de α^s* , $M_{\alpha^s}(x)$, és el polinomi mònic de menor grau a $\mathbb{F}_q[x]$ que té α^s com a arrel. Tenim que $M_{\alpha^s}(x) = \prod_{j \in C_s} (x - \alpha^j)$ és irreductible a $\mathbb{F}_q[x]$. Per tant, qualsevol polinomi $g(x) \mid (x^n - 1)$ a $\mathbb{F}_q[x]$ es pot escriure com a $g(x) = \prod_{j \in K} (x - \alpha^j)$, on K és la unió de classes q -ciclotòmiques.

EXEMPLE 21. Considerem el polinomi $x^7 - 1 \in \mathbb{F}_2[x]$. En aquest cas, l'ordre multiplicatiu de 2 mòdul 7 és $m = 3$. Per tant, el cos de descomposició de $x^7 - 1$ és $\mathbb{F}_8$. Sigui $\mathbb{F}_8 = \mathbb{F}_2[x]/(1 + x + x^3)$ i α una arrel de $1 + x + x^3$ que és també una arrel 7-èsima primitiva de la unitat. Així, la factorització a $\mathbb{F}_8[x]$ és $x^7 - 1 = \prod_{j=0}^6 (x - \alpha^j)$. Les classes 2-ciclotòmiques mòdul 7 són $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ i $C_3 = \{3, 5, 6\}$. Per tant, la factorització a $\mathbb{F}_2[x]$ és $x^7 - 1 = M_1(x) \cdot M_\alpha(x) \cdot M_{\alpha^3}(x) = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$.

Continuant amb l'exemple 19, considerem el codi binari cíclic $C = \langle g(x) \rangle$, on $g(x) = 1 + x + x^3$. Tenim que $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$, o sigui, $g(x) = M_\alpha(x)$ i en aquest cas $K = C_1$. De la mateixa manera, si considerem el codi binari cíclic $C^\perp$ que hem vist que està generat pel polinomi $h^*(x) = 1 + x^2 + x^3 + x^4$, tenim que $h^*(x) = (x - 1)(x - \alpha)(x - \alpha^2)(x - \alpha^4) = M_1(x) \cdot M_\alpha(x)$ i $K = C_0 \cup C_1$.

Sigui $C = \langle g(x) \rangle$ un codi cíclic, on $g(x) = \prod_{j \in K} (x - \alpha^j)$. Pel teorema 18, la dimensió de C és $n - |K|$, i tenim que $c(x) \in C$ si i només si $c(\alpha^j) = 0$ per a

tot $j \in K$. Aquesta propietat ens permet definir la següent matriu de control de C a partir de les arrels del polinomi generador $g(x)$:

$$H = \begin{pmatrix} 1 & \alpha^{j_1} & \alpha^{2j_1} & \dots & \alpha^{(n-1)j_1} \\ 1 & \alpha^{j_2} & \alpha^{2j_2} & \dots & \alpha^{(n-1)j_2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{j_{n-k}} & \alpha^{2j_{n-k}} & \dots & \alpha^{(n-1)j_{n-k}} \end{pmatrix},$$

on $K = \{j_1, \dots, j_{n-k}\}$.

El fet de considerar el polinomi generador d'un codi cíclic tenint en compte les seves arrels a $\mathbb{F}_{q^m}$ permet dissenyar codis cíclics amb una distància mínima superior o igual a un valor fixat, δ , anomenat *distància mínima prevista*, tal com mostra el resultat següent.

TEOREMA 22 ([23, p. 151]). *Sigui $C = \langle g(x) \rangle$ un codi q -ari cíclic de longitud n , amb $g(x) = \prod_{j \in K} (x - \alpha^j)$, on $\alpha \in \mathbb{F}_{q^m}$ és una arrel n -èsima primitiva de la unitat i m l'ordre multiplicatiu de q mòdul n . Si K conté $\delta - 1$ enters consecutius, aleshores la distància mínima d satisfà $d \geq \delta$.*

EXEMPLE 23. Considerem de nou el codi binari cíclic C de longitud 7 generat per $g(x) = 1 + x + x^3$ de l'exemple 19. Com hem vist a l'exemple 21, les arrels de $g(x)$ a $\mathbb{F}_8$ són α , α^2 i α^4 . Per tant, com que hi ha dues arrels amb exponents consecutius, podem assegurar que la distància mínima de C és $d \geq 3$ pel teorema 22. En aquest cas, de fet, tenim que la distància mínima és $d = 3$, ja que per exemple la primera fila de la matriu generadora G és una paraula codi de pes 3.

3.4 Codis BCH i Reed-Solomon

Dues famílies importants de codis cíclics són els codis BCH i Reed-Solomon. Els codis BCH van ser introduïts per Hocquenghem i, independentment, per Bose i Chaudhuri, el 1960. El mateix any, van ser introduïts els codis Reed-Solomon o RS per Reed i Solomon. Tots aquests codis es poden construir fent servir el teorema 22 per assegurar que la distància mínima (i, per tant, la capacitat correctora) sigui com a mínim un valor fixat. Els codis RS, a més, satisfan la fita de Singleton amb igualtat i, per tant, es diu que són codis MDS (*Maximum Distance Separable*). Aquesta propietat, que $d = n - k + 1$, no la compleixen en general els codis BCH.

Sigui n un enter, $n \geq 1$, i m l'enter positiu més petit tal que $n \mid q^m - 1$. Sigui $\alpha \in \mathbb{F}_{q^m}$ una arrel n -èsima primitiva de la unitat. Definim el *codi q -ari BCH* (o RS) amb distància mínima prevista $\delta \geq 1$ i paràmetres (m, δ) com el codi cíclic sobre $\mathbb{F}_q$ (o $\mathbb{F}_{q^m}$) generat pel polinomi de menor grau sobre $\mathbb{F}_q[x]$ (o $\mathbb{F}_{q^m}[x]$), que té com a arrels, $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$, per algun enter $b \geq 1$. Per als codis BCH, el polinomi generador és $g(x) = \text{mcm}(M_{\alpha^b}(x), \dots, M_{\alpha^{b+\delta-2}}(x)) \in \mathbb{F}_q[x]$. Aquest polinomi també es pot escriure com a $g(x) = \prod_{j \in K} (x - \alpha^j)$, on $K = C_b \cup \dots \cup C_{b+\delta-2}$. En el cas dels codis BCH, la distància mínima d satisfà $d \geq \delta$. D'altra banda, per als codis RS, el polinomi generador és

$g(x) = \prod_{j=b}^{b+\delta-2} (x - \alpha^j) \in \mathbb{F}_{q^m}[x]$ i la distància mínima és $d = \delta$. Finalment, per als dos casos, quan $b = 1$, el codi s'anomena *BCH o RS en sentit estricte*, i quan $n = q^m - 1$, s'anomena *BCH o RS primitiu*. En aquest darrer cas, la taxa de transmissió és la màxima entre tots els codis BCH o RS amb la mateixa capacitat correctora.

EXEMPLE 24. Construïm el codi binari BCH amb paràmetres (4, 7) primitiu i en sentit estricte. Com que $q = 2$ i $m = 4$, considerem el cos finit $\mathbb{F}_{16} = \mathbb{F}_2[x]/(1 + x + x^4) = \{0, \alpha^0, \alpha, \dots, \alpha^{15}\}$, on α és una arrel 15-èsima primitiva de la unitat. La taula 5 mostra els vectors de $\mathbb{F}_{16}$ en forma potencial.

potencial	vectorial	potencial	vectorial
$\alpha^{-\infty} = 0$	(0, 0, 0, 0)	α^7	(1, 1, 0, 1)
α^0	(1, 0, 0, 0)	α^8	(1, 0, 1, 0)
α^1	(0, 1, 0, 0)	α^9	(0, 1, 0, 1)
α^2	(0, 0, 1, 0)	α^{10}	(1, 1, 1, 0)
α^3	(0, 0, 0, 1)	α^{11}	(0, 1, 1, 1)
α^4	(1, 1, 0, 0)	α^{12}	(1, 1, 1, 1)
α^5	(0, 1, 1, 0)	α^{13}	(1, 0, 1, 1)
α^6	(0, 0, 1, 1)	α^{14}	(1, 0, 0, 1)

TAULA 5: Representació potencial i vectorial a $\mathbb{F}_{16} = \mathbb{F}_2[x]/(1 + x + x^4)$.

Com que volem un codi primitiu, la longitud ha de ser $n = 2^4 - 1 = 15$. Les classes 2-ciclotòmiques mòdul 15 són $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$ i $C_7 = \{7, 14, 13, 11\}$. Com que volem un codi en sentit estricte i $\delta = 7$, llavors $K = \bigcup_{i=1}^6 C_i = C_1 \cup C_3 \cup C_5 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$ i $g(x) = \prod_{j \in K} (x - \alpha^j)$. També podem obtenir $g(x)$ a partir d'alguns polinomis mínims, ja que $g(x) = \text{mcm}(M_\alpha(x), \dots, M_{\alpha^6}(x))$, on $M_\alpha(x) = M_{\alpha^2}(x) = M_{\alpha^4}(x) = 1 + x + x^4$, $M_{\alpha^3}(x) = M_{\alpha^6}(x) = 1 + x + x^2 + x^3 + x^4$ i $M_{\alpha^5}(x) = 1 + x + x^2$. Així, el polinomi generador és $g(x) = M_\alpha(x) \cdot M_{\alpha^3}(x) \cdot M_{\alpha^5}(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10} \in \mathbb{F}_2[x]$ i el codi BCH és $C = \langle 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10} \rangle$.

Volem codificar el primer vector d'informació de la seqüència binària 10110100... Com que el codi C té longitud $n = 15$ i el grau de $g(x)$ és $n - k = 10$, aleshores la dimensió del codi és $k = 5$ i el primer vector d'informació és $i = (1, 0, 1, 1, 0)$. La codificació de $i(x) = 1 + x^2 + x^3$ fent servir el mètode CRC és $c(x) = i(x)x^{10} - r(x)$, on $r(x) = x + x^3 + x^8 + x^9$ i $c(x) = x + x^3 + x^8 + x^9 + x^{10} + x^{12} + x^{13}$. Per tant, la codificació de $i = (1, 0, 1, 1, 0)$ és $c = (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$.

EXEMPLE 25. Construïm el codi binari RS amb paràmetres (4, 7) primitiu i en sentit estricte. Com que $q = 2$ i $m = 4$, considerem també el cos finit $\mathbb{F}_{16}$ com en l'exemple 24. Perquè sigui primitiu, la longitud del codi ha de ser $n = 2^4 - 1 = 15$. Com que ha de ser en sentit estricte i $\delta = 7$, el polinomi generador és $g(x) = \prod_{j=1}^6 (x - \alpha^j) = \alpha^6 + \alpha^9 x + \alpha^6 x^2 + \alpha^4 x^3 + \alpha^{14} x^4 + \alpha^{10} x^5 + \alpha^6 x^6 \in \mathbb{F}_{16}[x]$.

Volem codificar el primer vector d'informació de la seqüència binària 101101000010110100001000111110101... En aquest cas, com que la longitud és $n = 15$ i el grau de $g(x)$ és $n - k = 6$, la dimensió del codi és $k = 9$. Per codificar necessitem un vector d'informació de longitud 9 a $\mathbb{F}_{16}$, o equivalentment, una seqüència binària de $4 \cdot 9 = 36$ bits. Prenem els 36 primers bits de la seqüència a codificar, agrupats en blocs de 4 bits 1011 0100 0010 1101 0010 1110 0001 0001 1111, i considerem els corresponents elements a $\mathbb{F}_{16}$ d'acord amb la taula 5: $\alpha^{13} \alpha \alpha^2 \alpha^7 \alpha^2 \alpha^{10} \alpha^3 \alpha^3 \alpha^{12}$. Així, tenim que $i(x) = \alpha^{13} + \alpha x + \alpha^2 x^2 + \alpha^7 x^3 + \alpha^2 x^4 + \alpha^{10} x^5 + \alpha^3 x^6 + \alpha^3 x^7 + \alpha^{12} x^8$. Codificant amb el mètode CRC tenim que $c(x) = \alpha + \alpha^{14} x^2 + \alpha^9 x^3 + \alpha^{11} x^5 + \alpha^{13} x^6 + \alpha x^7 + \alpha^2 x^8 + \alpha^7 x^9 + \alpha^2 x^{10} + \alpha^{10} x^{11} + \alpha^3 x^{12} + \alpha^3 x^{13} + \alpha^{12} x^{14}$. Així, la codificació dels 36 primers bits és la seqüència binària de longitud 60, 0100 0000 1001...0001 1111, corresponent a la paraula codi c de longitud 15 sobre $\mathbb{F}_{16}$.

La descodificació per a codis cíclics és tan complexa com la descodificació per a codis lineals en general. En canvi, per als codis BCH i RS existeix un mètode eficient de descodificació, àmpliament utilitzat i conegut com a algorisme de Berlekamp-Massey, que està basat en l'algorisme d'Euclides estès [32]. A continuació, veurem com s'aplica aquest mètode als codis BCH i RS primitius i en sentit estricte.

Suposem que en la transmissió d'informació d'una paraula codi c de longitud n es produeixen errors. Es rep el vector u , o equivalentment el polinomi $u(x)$, que consisteix en la paraula codi enviada més els errors que s'han produït. Si s'han produït esborralls, aleshores se substitueix cadascun d'ells per un valor arbitrari del cos, per exemple, el 0. A partir de $u(x)$, calculem el *polinomi síndrome* $S(x) = u(\alpha) + u(\alpha^2)x + \dots + u(\alpha^{\delta-1})x^{\delta-2}$. Com que $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ són arrels del polinomi generador del codi, tenim que $S(x) = 0$ si i només si u correspon a una paraula codi i , per tant, no s'ha produït cap error.

Si $S(x) \neq 0$, aleshores el vector rebut u conté errors que volem corregir. Sigui J el conjunt que conté els valors j tals que s'ha produït un error a la coordenada $(j + 1)$ -èsima i J' el conjunt que conté els valors j tals que s'ha produït un esborrall a la coordenada $(j + 1)$ -èsima. Definim el *polinomi localitzador d'esborralls* $\sigma_b(x) = \prod_{j \in J'} (1 - \alpha^j x)$ i el *polinomi localitzador d'errors* $\sigma_e(x) = \prod_{j \in J} (1 - \alpha^j x)$. Així, el *polinomi localitzador d'errors i esborralls* és $\sigma(x) = \sigma_b(x) \cdot \sigma_e(x)$. A partir de $S(x)$ i δ , plantejem l'equació següent, anomenada *equació clau*:

$$w(x) = \sigma(x)S(x) \pmod{x^{\delta-1}}.$$

Fent servir l'algorisme d'Euclides, estès a partir dels polinomis $S(x)$ i $x^{\delta-1}$, podem resoldre aquesta equació i obtenir dos polinomis $\sigma(x)$ i $w(x)$ tals que $\text{mcd}(\sigma(x), w(x)) = 1$, $0 < \text{grau}(\sigma(x)) \leq \lfloor (\delta - 1)/2 \rfloor$ i $\text{grau}(w(x)) \leq \lfloor (\delta - 1)/2 \rfloor$ [38, p. 179]. El polinomi $w(x)$ s'anomena *polinomi avaluador d'errors i esborralls*. A continuació, calculem les arrels de $\sigma(x)$ a $\mathbb{F}_{q^m}$ i la derivada de $\sigma(x)$, $\sigma'(x)$. Per a cada arrel α^{-j} de $\sigma(x)$, el coeficient de x^j del

polinomi $e(x)$ és $e_j = -\frac{w(\alpha^{-j})}{\sigma'(\alpha^{-j})}$. Finalment, a partir de $e(x)$ obtenim el vector d'error e i, per tant, la paraula codi enviada és $c = u - e$. En aquest procés de descodificació, el més costós computacionalment és l'obtenció de les arrels de $\sigma(x)$ a $\mathbb{F}_{q^m}$.

EXEMPLE 26. Considerem el codi BCH amb paràmetres (4, 7) de l'exemple 24. Suposem que a la sortida del canal rebem 101000110101100, corresponent a un vector u de longitud 15. El polinomi associat és $u(x) = 1 + x^2 + x^6 + x^7 + x^9 + x^{11} + x^{12}$. A partir de $u(x)$, calculem el polinomi síndrome $S(x) = u(\alpha) + u(\alpha^2)x + \dots + u(\alpha^6)x^5$. Tenim que $u(\alpha) = 1 + \alpha^2 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{11} + \alpha^{12} = \alpha^{14}$, $u(\alpha^2) = \alpha^{13}$, $u(\alpha^3) = \alpha$, $u(\alpha^4) = \alpha^{11}$, $u(\alpha^5) = \alpha^5$ i $u(\alpha^6) = \alpha^2$. Per tant, el polinomi síndrome és $S(x) = \alpha^{14} + \alpha^{13}x + \alpha x^2 + \alpha^{11}x^3 + \alpha^5x^4 + \alpha^2x^5$. Com que $S(x) \neq 0$, sabem que s'han produït errors. Aleshores, resollem l'equació clau $w(x) = \sigma(x)S(x) \pmod{x^6}$. Aplicant l'algorisme d'Euclides estès, obtenim que $\sigma(x) = \alpha^{11} + \alpha^{10}x + \alpha^{10}x^2$ i $w(x) = \alpha^{10}$. La derivada de $\sigma(x)$ és $\sigma'(x) = \alpha^{10}$. Les arrels de $\sigma(x)$ són $\alpha^7 = \alpha^{-8}$ i $\alpha^9 = \alpha^{-6}$ i, per tant, els coeficients diferents de zero de $e(x)$ són els corresponents a x^8 i x^6 . Els valors d'aquests coeficients són $e_8 = \frac{w(\alpha^{-8})}{\sigma'(\alpha^{-8})} = \frac{\alpha^{10}}{\alpha^{10}} = 1$ i $e_6 = \frac{w(\alpha^{-6})}{\sigma'(\alpha^{-6})} = \frac{\alpha^{10}}{\alpha^{10}} = 1$. Així, $e(x) = x^6 + x^8$, el vector d'error és $e = (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$ i la paraula codi enviada és $c = u - e = (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$. Si s'ha codificat utilitzant el mètode CRC, aleshores la informació es troba en les darreres $k = 5$ coordenades, o sigui, és 01100.

EXEMPLE 27. Considerem el codi RS amb paràmetres (4, 7) de l'exemple 25. Suposem que a la sortida del canal rebem una seqüència binària de longitud 60 corresponent a una paraula codi amb possibles errors. Fent blocs de 4 bits, i considerant els corresponents elements a $\mathbb{F}_{16}$ d'acord amb la taula 5, obtenim un vector u de longitud 15 a $\mathbb{F}_{16}$. Considerem $u(x)$ el polinomi associat. Igual que a l'exemple 26, calculem el polinomi síndrome $S(x)$ i resollem l'equació clau $w(x) = \sigma(x)S(x) \pmod{x^6}$. A partir de les arrels del polinomi localitzador d'errors $\sigma(x)$, obtenim les posicions de les coordenades diferents de zero del vector d'error. A partir del polinomi avaluador d'errors, obtenim els valors d'aquestes coordenades. Així, construïm el vector d'error e a $\mathbb{F}_{16}$. Finalment, calculem la paraula codi a $\mathbb{F}_{16}$, $c = u - e$, i tornem a considerar cada coordenada de c com 4 bits d'acord amb la taula 5. Si s'ha codificat utilitzant el mètode CRC, aleshores la informació es troba en els darrers $4k = 4 \cdot 9 = 36$ bits.

Els codis BCH i RS s'utilitzen en molts àmbits [46]. A part de les aplicacions en el camp de les memòries dels dispositius electrònics, les comunicacions espacials, la representació d'informació en forma de codis de barres bidimensionals i l'emmagatzematge distribuït, que es comentaran en les properes seccions, aquests codis també es fan servir en l'emmagatzematge de dades dels discs òptics. En aquest cas, la codificació i correcció d'errors permeten la lectura de les dades encara que el disc òptic no estigui en perfecte estat. Inicialment, es van emprar per a l'escriptura de dades en els CD i, posteriorment, s'ha estès a la resta de dispositius d'emmagatzematge en discs òptics, com el DVD i el Blu-ray.

Una generalització dels codis BCH i RS són els codis algebraics geomètrics, que es defineixen usant corbes algebraïques sobre cossos finits [35, capítol 10]. Entre aquests, cal destacar els codis de Goppa, que, en el cas binari, s'han aplicat en sistemes criptogràfics de clau pública basats en codis, com per exemple el criptosistema de McEliece i el de Niederreiter. Dins de l'estudi de la criptografia postquàntica, s'ha demostrat que aquests algorismes criptogràfics són segurs envers atacs efectuats mitjançant computació quàntica [2, 40].

4 Codis de Hamming en les memòries d'ordinadors

El 1947, per tal de millorar la fiabilitat dels ordinadors de l'època i no haver de reiniciar els programes des de zero quan es detectava un error, Richard W. Hamming va plantejar per primera vegada la necessitat no només de detectar errors sinó de corregir-los. Ell va ser qui va construir el primer codi corrector, el codi lineal $[7, 4, 3]_2$, que apareix publicat tres anys més tard [17], ja que els Laboratoris Bell on treballava van sol·licitar-ne la patent. Aquest codi va ser generalitzat per Marcel J. E. Golay l'any 1949 i va donar lloc als coneguts *codis de Hamming* [14].

En aquesta secció descriurem els codis de Hamming i n'analitzarem les propietats. Veurem que permeten corregir un únic error, però la correcció es pot realitzar de forma molt eficient, tant en temps com en memòria. També mostrarem que el codi està d'un codi de Hamming, a més de corregir un error, permet detectar fins a dos errors, i com aquest tipus de codi s'aplica en les memòries d'ordinador.

Diem que un codi lineal sobre $\mathbb{F}_q$ és un *codi de Hamming* si les columnes de la seva matriu de control formen un conjunt maximal de vectors de longitud $t \geq 2$ sobre $\mathbb{F}_q$ linealment independents dos a dos. Per la proposició 13, aquesta condició garanteix que la distància mínima és $d = 3$ i, per tant, són codis 1-correctors. Per construcció, són codis lineals $[n, n - t, 3]_q$, on $n = (q^t - 1)/(q - 1)$. A més, d'entre tots els codis 1-correctors, aquests són els que tenen la major longitud n i, per tant, també la major taxa de transmissió $R = (n - t)/n$. Donat un cos finit $\mathbb{F}_q$ i un nombre enter $t \geq 2$, és fàcil veure que existeix un únic codi de Hamming, denotat per $\mathcal{H}_{q,t}$, llevat d'equivalències.

EXEMPLE 28. En el cas binari, si $t = 3$, aleshores una matriu de control per al codi de Hamming $\mathcal{H}_{2,3}$, que té paràmetres $[7, 4, 3]_2$, podria ser la següent:

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

En canvi, si l'alfabet és $\mathbb{F}_4$ i $t = 2$ una matriu de control per al codi de Hamming $\mathcal{H}_{4,2}$, que té paràmetres $[5, 3, 3]_4$, podria ser

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

on α és un element primitiu del cos finit $\mathbb{F}_4$.

Alguns dels codis de Hamming també es poden considerar com a codis cíclics. De fet, el codi de Hamming $\mathcal{H}_{q,t}$ és equivalent a un codi cíclic si i només si els valors t i $q - 1$ són coprimsers [4, p. 114]. D'aquest fet es desprèn que tot codi binari de Hamming és equivalent a un codi cíclic.

Els codis de Hamming són perfectes en el sentit que compleixen la fita de Hamming (1) amb igualtat. Per això, només cal veure que les boles de radi 1 centrades en cadascuna de les paraules codi recobreixen tot l'espai $\mathbb{F}_q^n$ [23, p. 48]. Aquest fet facilita la construcció de la taula de síndromes, ja que el conjunt de síndromes coincideix amb les columnes de la matriu de control i els seus múltiples. A més, totes les classes d'equivalència diferents de la classe del zero tenen un únic líder que és de pes 1, i el conjunt de líders (diferents de zero) coincideix amb el conjunt de tots els vectors de pes 1.

La correcció d'errors també resulta eficient, ja que en aquest cas, un cop rebem un vector $w \in \mathbb{F}_q^n$, calculem Hw^t i busquem en quina columna de la matriu de control H es troba aquesta síndrome o un múltiple seu. Així, si $Hw^t = rh_i$, on $r \in \mathbb{F}_q$ i h_i és la columna i -èsima de H , direm que l'error és el vector de pes 1, amb r en la i -èsima coordenada i zeros en la resta. En el cas binari, només cal trobar la columna de H que coincideixi amb la síndrome. Per tant, si ordenem les columnes de H de manera que la columna i -èsima coincideixi amb la representació en base 2 de i , la descodificació és més ràpida.

El codi estès d'un codi de Hamming és un codi lineal $[n + 1, n - t, 4]_2$, on $n = (q^t - 1)/(q - 1)$. Aquest codi continua sent 1-corrector, però a diferència del codi de Hamming, a més de corregir un error, pot simultàniament detectar-ne dos. Fixem-nos que les classes d'equivalència diferents de la classe del zero tenen o bé un líder de pes 1 que és únic, o bé un líder de pes 2 que no és únic. En aquest cas, si optem per una descodificació completa, podem decidir per exemple que el líder de pes 2 sigui el que tingui un 1 en la darrera posició.

EXEMPLE 29. El codi estès del codi de Hamming $[7, 4, 3]_2$, amb matriu de control H donada en l'exemple 28, és el codi $[8, 4, 4]_2$ que té la matriu de control següent:

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

Suposem que hem codificat la informació amb aquest codi i que rebem el vector $w = (1, 1, 0, 0, 0, 1, 1, 1)$. Per descodificar, calculem $\hat{H}w^t = (1, 0, 1, 0)$. Com que $(1, 0, 1, 0)$ coincideix amb la 2a columna de $\hat{H}$, l'error és $e = (0, 1, 0, 0, 0, 0, 0, 0)$ i, per tant, la paraula codi és $c = w - e = (1, 0, 0, 0, 0, 1, 1, 1)$. En aquest cas, com que les columnes de H estan ordenades, ens podem estalviar la cerca dins de la matriu $\hat{H}$. A partir de $(1, 0, 1, 0)$, eliminant el primer bit, com que 010 és el 2 en base 2, sabem que l'error està en la 2a posició. En canvi, si rebem el vector $w' = (0, 0, 0, 1, 0, 1, 1, 1)$, com que la síndrome és $(0, 1, 0, 1)$ i no coincideix amb cap de les columnes de $\hat{H}$, podem detectar que s'han produït dos o més errors. També és fàcil de veure-ho analitzant la paritat del

vector rebut: si és senar, direm que s'ha produït un error que es podrà corregir; i si és parell, detectarem que n'hi ha hagut com a mínim dos. Si apliquem una descodificació completa, com la que hem definit abans, l'error associat al vector w' seria $e' = (0, 0, 0, 0, 1, 0, 0, 1)$, ja que 101 és 5 en base 2. Per tant, la paraula codi seria $c' = w' - e' = (0, 0, 0, 1, 1, 1, 1, 0)$.

Les memòries dels ordinadors estan construïdes a partir de xips de silici. Un xip de memòria és bàsicament una matriu quadrada de cel·les que emmagatzemen bits. Per exemple, un xip de 64 kilobits emmagatzema $64 \cdot 2^{10} = 2^{16}$ bits, o un de 256 kilobits emmagatzema 2^{18} bits. En el de 64 kilobits, els bits s'organitzen en una matriu de $2^8 \times 2^8$. S'accedeix a cada bit a partir de dos valors de 0 a $2^8 - 1 = 255$ que representen la fila i la columna. Com que els valors de 0 a 255 es poden representar a partir de 8 bits, es necessiten $8 + 8 = 16$ bits per descriure la posició d'un bit en el xip. En un xip de 256 kilobits es necessitarien 18 bits per localitzar la posició d'un bit.

El bit que s'emmagatzema en una posició del xip es representa a partir de la presència o l'absència de càrrega elèctrica negativa. Quan s'emmagatzema un 0, el forat del potencial de l'electró és omplert amb electrons, i quan s'emmagatzema un 1, es deixa buit. Es considera que hi ha un 0 si, mesurant la seva càrrega negativa, aquesta és superior a un cert valor llindar. Per tant, si una posició perd la seva càrrega negativa, aleshores es llegeix de forma incorrecta i diem que s'ha produït un error. Aquests tipus d'errors són força freqüents i no es poden evitar.

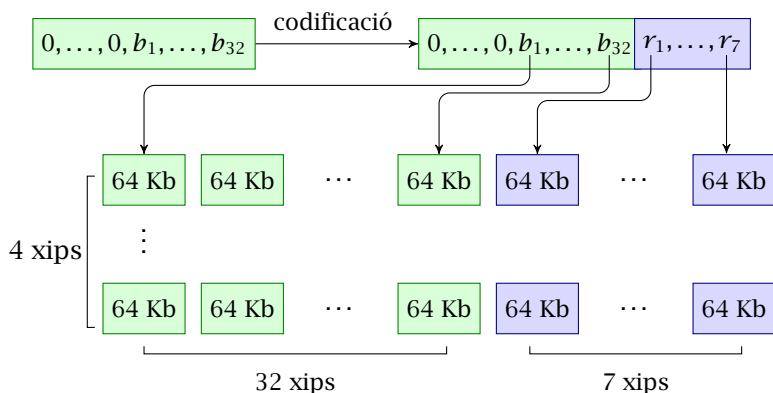


FIGURA 3: Esquema de configuració en memòries d'ordinadors.

Per tal de corregir els errors descrits, inicialment es van fer servir codis de Hamming estesos de la forma següent. Per exemple, si tenim 128 xips de 64 kilobits, aquests s'organitzen en 4 files de 32 xips cadascuna. La informació es divideix en paraules de 32 bits, on cadascun dels 32 bits s'extreu d'un dels 32 xips. Per corregir els errors, s'afegeixen 7 xips al final de cadascuna de les 4 files de 32 xips, obtenint un total de $128 + 7 \cdot 4 = 156$ xips. Així, dels 39 xips

que conté cadascuna de les 4 files, els darrers 7 contenen la redundància i són utilitzats per corregir els errors. La figura 3 mostra un esquema d'aquesta configuració. En aquest cas, s'utilitza el codi binari estès de Hamming $[64, 57, 4]_2$, encara que només s'aprofiten 32 dels 57 bits d'informació.

Part de la informació sobre aquesta aplicació s'ha extret de [29]. L'aplicació d'altres codis en diferents tipus de memòries d'ordinador i dispositius electrònics es pot trobar, per exemple, a [42, capítols 2 i 3] o [47]. En aquest àmbit, a part dels codis de Hamming, es fan servir els codis BCH i RS, i més recentment els codis LDPC (*low-density parity-check*).

5 Codis Reed-Muller per a la transmissió de fotografies a l'espai

En aquesta secció descriurem alguns codis que van aparèixer poc després dels codis de Hamming. A més, veurem com alguns es van aplicar per millorar la qualitat de les fotografies dels planetes del sistema solar enviades a la terra a través de sondes espacials.

Sigui $\mathcal{H}_{q,t}$ el codi de Hamming $[n, n - t, 3]_q$, on $n = (q^t - 1)/(q - 1)$. L'ortogonal d'un codi de Hamming, $\mathcal{H}_{q,t}^\perp$, s'anomena *codi simplex* i és un codi amb paràmetres $[n, t, q^{t-1}]_q$, on totes les paraules codi diferents de zero tenen pes q^{t-1} . El *codi Reed-Muller de primer ordre*, també anomenat *codi de Hadamard lineal*, és el codi $(\widehat{\mathcal{H}_{q,t}})^\perp$, o sigui l'ortogonal del codi estès de Hamming. Aquest codi té paràmetres $[n + 1, (n + 1)q, (q^t + q - 2)/q]_q$, per tant, per a $q = 2$ són codis lineals $[2^t, t + 1, 2^{t-1}]_2$ [21, p. 83]. En general, els codis Reed-Muller d'ordre r , $1 \leq r \leq n$, van ser descrits per primera vegada per David E. Muller el 1954 [33]; el mateix any, Irving S. Reed va proposar el primer algorisme eficient per descodificar-los [36].

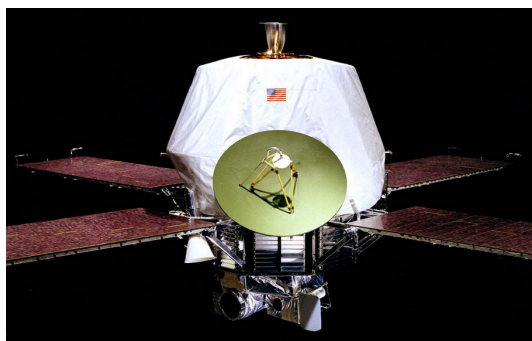
Recordem que els codis de Hamming són codis perfectes en el sentit que compleixen la fita de Hamming (1) amb igualtat. De fet, tots els codis 1-perfectes lineals són codis de Hamming. Com que són codis 1-correctors, també es diu que són codis 1-perfectes. En general, es diu que un codi és *t-perfecte* si satisfà la fita de Hamming amb igualtat, o equivalentment, si tot vector $w \in \mathbb{F}_q^n$ està a distància com a màxim t d'exactament una paraula codi. Per definició, els codis *t-perfectes* són codis *t-correctors*. El 1973, es va demostrar que els únics codis perfectes no trivials són els següents: els codis q -aris de repetició $[n, q, n]_q$ amb n senar; els codis q -aris 1-perfectes (no necessàriament lineals); el codi binari de Golay [23, 12, 7]₂, i el codi ternari de Golay [11, 6, 5]₃; vegeu [43, 49]. Tots aquests, excepte els 1-perfectes no lineals, són únics llevat d'equivalències [31]. En canvi, hi ha molts codis 1-perfectes no lineals que no són equivalents entre ells [11, 19, 34].

El 1962 van començar les primeres missions espacials per fotografiar els planetes Mercuri, Venus i Mart, a través del programa Mariner. Inicialment les imatges es van dividir en 200×200 elements o píxels, i a cadascun d'aquests se li assignava un vector binari de longitud 6 per indicar un nivell en l'escala

de grisos, del 000000 que representava el blanc al 111111 que representava el negre. Com que la probabilitat d'error d'un bit enviat a través de l'espai era $p = 0.05$, la probabilitat d'error d'un píxel era $1 - (1 - p)^6 \approx 0.265$. O sigui, més del 26% de la imatge contenia errors. Aquest percentatge era força inacceptable i es va estudiar la manera de reduir-lo.

A partir del disseny de les sondes espacials Mariner 6 i 7, llançades el 1969 per fotografiar el planeta Mart, es van començar a incorporar codis correctors d'errors. Calia, però, tenir en compte certes restriccions de pes, consum d'energia, emmagatzematge i capacitat de computació. Per això, com que es van dividir les imatges en 700×832 píxels, aquests píxels ja codificats no podien excedir de 30 bits aproximadament. També calia que el procés de codificació i descodificació fos ràpid per poder així redirigir la càmera a partir de les fotografies rebudes.

Finalment, es va decidir fer servir el codi de Hadamard lineal $[32, 6, 16]_2$ que permet corregir fins a $\lfloor (16-1)/2 \rfloor = 7$ errors cada 32 bits. D'aquesta manera, es va aconseguir reduir l'error en les imatges d'un 26% a un 0.01%, ja que la probabilitat d'error d'un píxel es va reduir fins a $1 - \sum_{i=0}^7 \binom{32}{i} p^i (1-p)^{32-i} \approx 0.00014$. La codificació per a codis lineals resultava ràpida i no requeria memòria. La descodificació es podia accelerar utilitzant la transformada ràpida de Fourier que es va implementar dins de la circuiteria de la sonda, coneguda com a «Green Machine» (no pel seu color, sinó pel seu dissenyador, R. R. Green). Més informació sobre aquesta aplicació dels codis es pot consultar amb detall a [35, capítol 25] o breument a [29, 21]. A [21] es descriuen moltes altres aplicacions dels codis de Hadamard.



La sonda Mariner 9.

En la sonda Mariner 9, llançada el 1971, les dades instrumentals que requereien una major protecció contra els errors van ser codificades afegint abans de forma concatenada un codi RS $[6, 4]$ sobre $\mathbb{F}_{26}$. Es considera que aquest va ser el primer disseny d'un sistema de codis concatenats. En les sondes Voyager 1 i 2, llançades el 1977 per enviar fotografies en color de Júpiter i Saturn, part de les dades es van codificar fent servir el codi estès de Golay $[24, 12, 8]_2$ concatenat amb un codi convolucional. A partir del 1968, amb la missió espacial Pioneer 9

per a l'estudi del sol, es van començar a fer servir codis convolucionals com a part d'un experiment. Posteriorment, dins dels estàndards de transmissió per l'espai CCSDS (*Consultative Committee for Space Data Systems*), s'han dissenyat sistemes de codis convolucionals concatenats amb codis RS. Per a més informació sobre codis aplicats en aquest camp, es pot consultar [35, capítol 25] o [46, capítol 3], i per a més informació sobre codis convolucionals o convolucionals Reed-Solomon, [35, capítol 12] o [10], respectivament.

6 Codis BCH i Reed-Solomon en el QR

En la secció 2 s'ha explicat el codi EAN, utilitzat per identificar productes comercials. Aquest és un tipus de codi de barres unidimensional (1D) o lineal. En general, té poca capacitat i només permet detectar errors. En canvi, els codis bidimensionals (2D) o matricials tenen més capacitat, o sigui, permeten representar més quantitat de dades, i alhora corregir errors, des d'un 5 % fins a un 35 % segons el tipus. Dins dels codis 2D trobem el MaxiCode, el HanXin, el Data Matrix, l'HCC2D i el QR, entre d'altres [3]. En aquesta secció descriurem els codis QR, ja que són els més coneguts i utilitzats, i a més uns dels millors tant des del punt de vista de la capacitat per representar dades com per corregir errors.

El codi QR (de l'anglès *Quick Response*) va ser creat el 1994 per la companyia japonesa Denso Wave i va ser estandarditzat el 2000 [26]. Actualment, el seu ús és de caràcter públic, ja que l'empresa va renunciar als seus drets d'autor. Inicialment, aquest codi es va utilitzar per fer el seguiment de les peces en la fabricació de vehicles. Avui en dia, però, s'utilitza en molts llocs, tant en l'àmbit comercial com particular. Es pot fer servir per mostrar un missatge de text, obrir una pàgina web o un gestor de correu, afegir un contacte al mòbil, etc.



FIGURA 4: Exemple d'un QR amb la URL d'una pàgina web.

En els codis QR la unitat mínima per representar les dades és el mòdul, un quadrat que representa un 1 a $\mathbb{Z}_2$ quan és negre o un 0 quan és blanc. La versió original o model 1 era capaç de representar només fins a 1167 caràcters numèrics amb una matriu de 73×73 mòduls. Actualment, s'utilitza el model 2,

que permet representar fins a 7089 caràcters numèrics amb una matriu de 177×177 mòduls. Dins d'aquest model, en podem trobar versions diferents. La versió 1 està formada per 21×21 mòduls i la versió 40 per 177×177 . Per passar d'una versió a la següent s'incrementen en 4 el nombre de mòduls de cada costat.

Cada versió disposa de quatre nivells segons la capacitat correctora: el nivell *L* té una capacitat correctora d'aproximadament el 7%, el *M* té una capacitat del 15%, el *Q* en té una del 25% i finalment el *H* en té una del 30%. La capacitat màxima depèn de la versió i el nivell de correcció. Per exemple, el màxim que es pot representar amb un codi QR són 7089 caràcters numèrics (o 4296 d'alfanumèrics) amb la versió 40 del nivell *L*.

La figura 4 mostra un exemple d'un codi QR (versió 2 amb nivell de correcció *L*) amb la URL de la pàgina web del *Butlletí de la Societat Catalana de Matemàtiques*. Fixem-nos que està format per 25×25 mòduls, ja que correspon a un codi de la versió 2. A més, el nivell de correcció és el més baix, o sigui, permet corregir només un 7% dels mòduls, aproximadament.

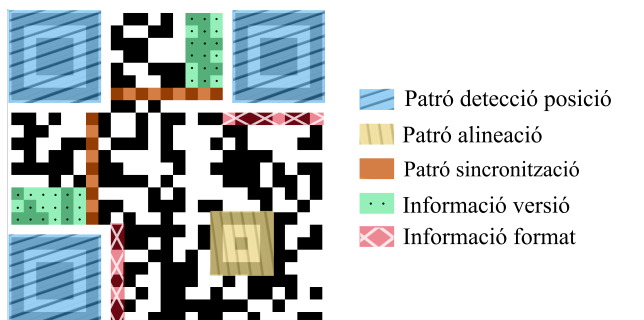


FIGURA 5: Estructura d'un QR de la versió 2.

Els codis QR estan formats per diferents parts, incloent-hi la que conté la informació que es vol representar. En la figura 5 es mostra l'estructura del QR de la figura 4 amb les diferents parts que conté. Al voltant del codi QR hi ha una zona lliure de marques d'una amplada de 4 mòduls. A les cantonades superiors i inferior esquerra hi ha tres patrons idèntics de detecció de posició que permeten que es pugui llegir encara que estigui rotat o hi hagi una reflexió. Al llarg de la fila 7 i de la columna 7 es troben els patrons de sincronització, que estan formats per mòduls negres i blancs de forma alternada i que serveixen com a referència per determinar les coordenades dels mòduls de dades. Els patrons d'alineació són semblants als de detecció però són més petits, també serveixen per alinear el codi i el seu nombre depèn de la versió. La informació sobre quin és el nivell de correcció o format es codifica amb un codi binari BCH, es duplica i se situa en dos o tres llocs diferents segons la versió. La informació sobre quina és la versió també es codifica amb un codi binari BCH, es duplica i se situa en dues ubicacions diferents. Finalment, la informació que es vol incloure

en el QR es codifica amb un codi RS sobre el cos finit $\mathbb{F}_{2^8}$, en funció del nivell de correcció i versió, i s'organitza en grups de 8 bits cadascun corresponent a un element de $\mathbb{F}_{2^8}$.

En les zones destinades a indicar el nivell de correcció o format i la versió s'utilitza un codi binari BCH. Concretament, el format es representa amb 5 bits (2 per indicar un dels 4 nivells disponibles i 3 per aplicar una màscara per tal d'evitar algunes seqüències de bits de més difícil lectura) que es codifiquen amb un BCH $[15, 5]_2$. Aquesta informació apareix duplicada i situada en dos o tres llocs diferents segons la versió. El número de versió es representa amb 6 bits, que es codifiquen amb un BCH $[18, 6]_2$. Aquesta informació només s'inclou a partir de la versió 7, i també apareix duplicada i ubicada en dos llocs diferents.

Per a les dades que volem incloure en el QR s'utilitzen diferents codis RS, segons quin sigui el nivell de correcció i la versió. Per exemple, en el nivell H de la versió 4, com que hi ha 100 bytes disponibles, s'inclouen 4 paraules codi, codificades amb un RS $[25, 9, 17]_{2^8}$. En aquest cas, com que la distància mínima és $d = 17$, aquest codi permet corregir 8 bytes per cada paraula codi, per tant, un total de $4 \cdot 8 = 32$ bytes dels $4 \cdot 25 = 100$ bytes totals, o sigui, el 32%.

Els codis QR han evolucionat en diverses direccions a través de la mateixa empresa que els va crear. El 1998 es van crear els codis micro QR, més apropiats per a aplicacions on les dades i l'espai són reduïts, mantenint la mateixa facilitat de lectura. El 2007 van aparèixer els SQRC (*security QR code*), preparats per incloure dades encriptades de forma que aquestes només són accessibles per als lectors autoritzats, o sigui, que tinguin les claus per desxifrar. Entre el 2009 i el 2011 es van presentar els codis iQR, que, comparats amb els codis QR, permeten representar més informació (fins a 40 637 caràcters numèrics), reduir l'espai per a una mateixa quantitat d'informació i corregir més errors amb un nou nivell S , que corregeix aproximadament el 50% dels mòduls. A més, aquests codis també permeten comprimir les dades i ser generats en forma rectangular.

7 Codis per a l'emmagatzematge distribuït

En aquesta secció veurem una aplicació dels codis correctors d'errors (o correctors d'esborralls) en el camp de l'emmagatzematge distribuït. Concretament, veurem alternatives a l'emmagatzematge fent servir rèpliques, els problemes que comporten i algunes de les solucions proposades recentment.

És evident que estem totalment immersos dins de la nova era digital. Avui en dia, la majoria dels objectes són digitals o en depenen en gran mesura. El 2011, la International Data Corporation va estimar que la quantitat total de dades al món creixeria el 2012 fins als 2.7 zettabytes (un zettabyte són 10^{21} bytes o 10^9 terabytes) i, per tant, suposaria un increment del 48% respecte al 2011 [7]. Més recentment, la predicció és que creixerà dels 33 zettabytes el 2018 als 175 el 2025 [37]. Això implica que cada dia hi ha més i més dades digitals que es creen i que cal emmagatzemar. A més, volem que estiguin sempre disponibles des de qualsevol lloc, i que siguin de fàcil i ràpid accés.

Actualment, per emmagatzemar grans quantitats de dades es fan servir sistemes distribuïts (*distributed storage systems*). O sigui, les dades s'emmagatzemen en molts servidors diferents que en conjunt es comporten com un únic sistema d'emmagatzematge, conegut com a *centre de dades*. Així, les dades d'un fitxer es divideixen i distribueixen en diverses unitats d'emmagatzematge, anomenades *nodes*, que, simplificant, poden associar-se amb els discs durs. Un node o disc dur pot necessitar ser reparat per diversos motius. Per exemple, el node pot fallar (la probabilitat que un disc dur deixi de funcionar està entre el 2 % i el 4 % l'any), o pot estar ocupat amb altres peticions o en fase de manteniment.

Una primera solució a aquest problema consisteix a fer còpies de seguretat (també conegudes com a *backups*), o sigui, replicar n cops les dades de cada node. Això es pot veure com si en realitat s'estigués fent servir un codi de repetició, com el descrit en l'exemple 9 amb $n = 3$. Si un node falla, podem accedir a les dades d'una de les còpies, descarregar-les i restaurar el node. El nombre de nodes que poden fallar sense que hi hagi cap pèrdua d'informació en el sistema s'anomena *tolerància a fallades*, i en aquest cas és igual a $n - 1$. Normalment s'assumeix que els nodes fallen de forma independent. Finalment, cal destacar que aquest mètode és força ineficient, ja que suposa un elevat cost en termes econòmics i d'espai.

Una primera alternativa consisteix a fer servir altres codis lineals diferents del codi de repetició. En general, si es fa servir un codi lineal $[n, k]_q$, les dades es divideixen en k nodes i s'afegeixen $n - k$ nodes de redundància de forma que assignem cadascun dels n símbols de la paraula codi a cadascun dels n nodes. Si un node falla, això és equivalent a dir que hi ha un esborrall en una de les coordenades. No es considera un error, ja que es pot saber en quin node, o sigui en quina coordenada, s'ha produït. Si la distància mínima del codi és d , el codi permet corregir fins a $d - 1$ esborralls, per tant, la tolerància a fallades del sistema seria $d - 1$. Aquest valor pot ser inferior a l'obtingut amb un codi de repetició $[n, 1]_q$, però l'avantatge és que es pot reduir el nombre de nodes redundants, passant de $n - 1$ a $n - k$. D'aquesta forma es poden obtenir sistemes amb la mateixa fiabilitat, però millorant significativament l'espai i els costos d'emmagatzematge.

En la indústria, s'han anat reemplaçant els sistemes inicials basats en la rèplica d'informació per sistemes on es fan servir codis correctors d'esborralls (*erasure codes*). Normalment s'utilitzen codis Reed-Solomon com els descrits en la subsecció 3.3, ja que són MDS (vegeu la subsecció 3.4). Així, la distància mínima i, per tant, la capacitat per corregir esborralls és la màxima possible fixats els valors de n i k . A més, podem recuperar les dades emmagatzemades connectant-nos a qualsevol subconjunt de k nodes dels n nodes. Per exemple, en el sistema d'emmagatzematge de Linux RAID-6 es fa servir un codi RS $[10, 8]$ i en el Google Colossus un RS $[9, 6]$ [8]. També Facebook en el seu sistema de fitxers va incorporar un RS $[14, 10]$ [45]. La darrera versió del sistema de fitxers distribuïts Hadoop, Hadoop 3.0, incorpora l'opció d'utilitzar aquests codis [48].

Malgrat els seus avantatges respecte als sistemes basats en la rèplica d'informació, els sistemes basats en codis correctors d'esborralls tenen el gran inconvenient que, quan un node falla, el sistema ha d'accedir a k nodes, i descarregar k vegades la quantitat de dades que conté el node que volem restaurar. Per tant, és ineficient tant des del punt de vista de la quantitat de dades que hem de descarregar (*repair bandwidth*) com de la quantitat de nodes que intervenen en la reparació (*repair degree*). Aquest problema ha donat lloc a dues noves famílies de codis: els codis regeneratius (*ReGenerating* o RG) [9] i els localment recuperables (*Locally Recoverable* o LR) [15]. En els codis RG l'objectiu és minimitzar la quantitat de dades que hem de descarregar, mentre que en els codis LR es busca minimitzar el nombre de nodes necessaris en la reparació d'un node. També s'han combinat les idees d'aquestes dues famílies per tal de minimitzar els dos paràmetres amb els anomenats *codis localment regeneratius* (*Locally Regenerating Codes* o LRG) [28]. Altres autors han buscat alternatives per millorar la reparació amb els codis Reed-Solomon [16, 8].

Els codis LR ja es troben implementats en sistemes d'emmagatzematge com el Windows Azure [22] i en l'emmagatzematge de les dades a Facebook [39]. A continuació, descriurem breument la primera d'aquestes dues aplicacions.

EXEMPLE 30. Tal com s'explica a [22], en el sistema d'emmagatzematge Windows Azure, les dades inicialment es van incorporant a un fitxer fins a arribar a una certa mida, per exemple fins a obtenir un fitxer d'1 gigabyte que ja no pot ser modificat. Durant aquest procés, es van mantenint sempre tres còpies d'aquest fitxer.

Un cop el fitxer s'ha omplert, es divideix en $k = 6$ parts que s'emmagatzemen en 6 nodes, $x_0, x_1, x_2, y_0, y_1, y_2$. A continuació, s'afegeixen $n - k = 4$ nodes de redundància, p_0, p_1, p_x, p_y , tal com es mostra en la figura 6. Els dos primers nodes de redundància es calculen a partir dels 6 nodes d'informació i s'anomenen *paritats globals*. Els altres dos nodes de redundància s'anomenen *paritats locals*. El node p_x es calcula a partir de x_0, x_1, x_2 i p_y a partir de y_0, y_1, y_2 .

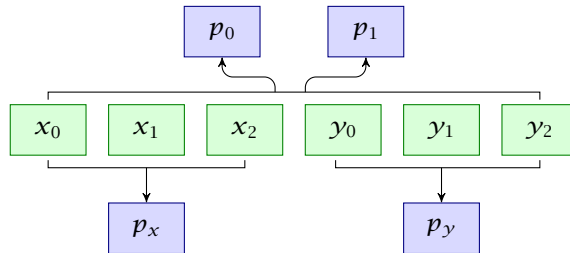


FIGURA 6: Esquema d'un exemple de codi localment recuperable.

Aquest codi LR seria comparable amb un codi Reed-Solomon [9, 6] en termes del cost d'emmagatzematge (*storage overhead*), ja que el codi LR té un cost de $10/6 = 1.66$ i el RS de $9/6 = 1.5$. En l'LR hi hauria 4 nodes de redundància

en comptes dels 3 que hi ha en l'RS. A canvi, si un node falla, es necessitarien només 3 nodes per recuperar les dades, en lloc dels 6 que calen amb el codi RS. Finalment, aquest codi RS pot tolerar fins a la pèrdua de qualssevol 3 nodes, mentre que el codi LR pot tolerar la pèrdua de qualssevol 3 nodes i alguns patrons de 4 nodes. Per exemple, si fallen els nodes x_0, x_1, y_0, y_1 sí que es podrien recuperar a partir de la resta, però no si fossin els nodes x_0, x_1, x_2, p_x .

Per tal de reduir el cost d'emmagatzematge respecte del codi RS [9, 6], s'ha utilitzat un altre codi LR semblant a l'anterior, però amb 14 nodes d'informació i 4 de redundància. Aquest codi LR és comparable amb l'RS respecte al nombre de nodes necessaris per reparar-ne un (*repair degree*), ja que se'n necessiten 7 en lloc de 6. A canvi, s'ha reduït el cost d'emmagatzematge d'1.5 a l'RS a $18/14 = 1.29$ a l'LR, fet que ha suposat un estalvi de milions de dòlars a Microsoft [13].

Agraïments

Les autores volen agrair especialment als companys del grup de recerca Combinatorics, Coding and Security Group (CCSG) del Departament, Joaquim Borges, Jaume Pujol i Josep Rifà, els seus comentaris i aportacions en la millora del redactat final de l'article. Les autores també han tingut l'ajut del projecte MINECO (AEI/FEDER, UE) número MINECO TIN2016-77918-P i del projecte número 2017SGR-00463 de la Generalitat de Catalunya.

Referències

- [1] ASH, R. *Information Theory*. Nova York; Londres; Sydney: Interscience Publishers John Wiley & Sons, 1965. (Interscience Tracts in Pure and Applied Mathematics; 19)
- [2] BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. (ED.). *Post-quantum Cryptography*. Berlín: Springer-Verlag, 2009.
- [3] BHASKAR RAJ, A. S. *BAR CODES: Technology and Implementation*. Nova Delhi: Tata McGraw-Hill Education, 2001.
- [4] BIAHUT, R. E. *Algebraic Codes for Data Transmission*. Nova York: Cambridge University Press, 2003.
- [5] BORGES, J.; FERNÁNDEZ-CÓRDOBA, C.; PUJOL, J.; RIFÀ, J.; VILLANUEVA, M. « $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality». *Des. Codes Cryptogr.*, 54 (2) (2010), 167–179.
- [6] BRUNAT BLAY, J. M.; VENTURA CAPELL, E. *Informació i codis*. Barcelona: Edicions UPC, 2001.
- [7] BUSINESS WIRE. «IDC predicts 2012 will be the year of mobile and cloud platform wars as IT vendors vie for leadership while the industry redefines itself» (1 desembre 2011). <https://www.businesswire.com/news/home/20111201005201/en/IDC-Predicts-2012-Year-Mobile-Cloud-Platform>.

- [8] DAU, H.; DUURSMA, I.; KIAH, H. M.; MILENKOVIC, O. «Repairing Reed-Solomon codes with two erasures». A: *Proceedings of 2017 IEEE International Symposium on Information Theory (ISIT)*. Nova York: IEEE, 2017, 351-355.
- [9] DIMAKIS, A. G.; BRIGHTEN GODFREY, P.; WU, Y.; WAINWRIGHT, M. J.; RAMCHANDRAN, K. «Network coding for distributed storage systems». *IEEE Trans. Inform. Theory*, 56 (9) (2010), 4539-4551.
- [10] EBERT, P. M.; TONG, S. Y. «Convolutional Reed-Solomon codes». *Bell System Tech. J.*, 48 (1969), 729-742.
- [11] ETZION, T. «Nonequivalent q -ary perfect codes». *SIAM J. Discrete Math.*, 9 (3) (1996), 413-423.
- [12] GALLIAN, J. A. «Error detection methods». *ACM Comput. Surveys*, 28 (3) (1996), 504-517.
- [13] GANTENBEIN, D. «A better way to store data». Microsoft Research Blog (5 setembre 2012). <https://www.microsoft.com/en-us/research/blog/better-way-store-data/>.
- [14] GOLAY, M. J. E. «Notes on digital coding». *Proceedings of the IRE*, 37 (6) (1949), 657.
- [15] GOPALAN, P.; HUANG, C.; SIMITCI, H.; YEKHANIN, S. «On the locality of codeword symbols». *IEEE Trans. Inform. Theory*, 58 (11) (2012), 6925-6934.
- [16] GURUSWAMI, V.; WOOTTERS, M. «Repairing Reed-Solomon codes». *IEEE Trans. Inform. Theory*, 63 (9) (2017), 5684-5698.
- [17] HAMMING, R. W. «Error detecting and error correcting codes». *Bell System Tech. J.*, 29 (1950), 147-160.
- [18] HAMMONS, A. R., JR.; KUMAR, P. V.; CALDERBANK, A. R.; SLOANE, N. J. A.; SOLÉ, P. «The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes». *IEEE Trans. Inform. Theory*, 40 (2) (1994), 301-319.
- [19] HEDEN, O. «A survey of perfect codes». *Adv. Math. Commun.*, 2 (2) (2008), 223-247.
- [20] HERNÁNDEZ, L.; MARTÍN, A. «Codificación de información mediante códigos de barras». *Bol. Soc. Esp. Mat. Apl. SeMA*, 27 (2004), 29-48.
- [21] HORADAM, K. J. *Hadamard Matrices and their Applications*. Princeton, NJ: Princeton University Press, 2007.
- [22] HUANG, C.; SIMITCI, H.; XU, Y.; OGUS, A.; CALDER, B.; GOPALAN, P.; LI, J.; YEKHANIN, S. «Erasure coding in Windows Azure Storage». A: *Proceedings of the 2012 USENIX Annual Technical Conference*. Boston: USENIX Association, 2012, 15-26.
- [23] HUFFMAN, W. C.; PLESS, V. *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.
- [24] ISO 13616-1:2007 *Financial services - International bank account number (IBAN) - Part 1: Structure of the IBAN*. 1a ed. Suïssa: International Organization for Standardization, març 2007.

- [25] ISO/IEC 15420:2009(EN) *Information technology - Automatic identification and data capture techniques - EAN/UPC bar code symbology specification*. 2a ed. Suïssa: International Organization for Standardization, desembre 2009.
- [26] ISO/IEC 18004:2015(EN) *Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification*. 3a ed. Suïssa: International Organization for Standardization, febrer 2015.
- [27] ISO 2108:2017, ISO 2108:2005 *Information and documentation - International Standard Book Number (ISBN)*. 7a ed. Suïssa: International Organization for Standardization, desembre 2017.
- [28] KAMATH, G. M.; PRAKASH, N.; LALITHA, V.; KUMAR, P. V. «Codes with local regeneration and erasure correction». *IEEE Trans. Inform. Theory*, 60 (8) (2014), 4637–4660.
- [29] KEY, J. D. «Some error-correcting codes and their applications». A: SHIER, D. R.; WALLINIUS, K. T. (ED.). *Applied Mathematical Modeling: A Multidisciplinary Approach*. Boca Raton: Chapman & Hall/CRC, 1999, 276–299.
- [30] LIDL, R.; NIEDERREITER, H. *Finite fields*. 2a ed. Cambridge: Cambridge University Press, 1997. (Encyclopedia of Mathematics and its Applications; 20)
- [31] MACWILLIAMS, F. J.; SLOANE, N. J. A. *The Theory of Error-Correcting Codes*. I. Amsterdam; Nova York; Oxford: North-Holland Publishing Co., 1977. (North-Holland Mathematical Library; 16)
- [32] MASSEY, J. L. «Shift-register synthesis and BCH decoding». *IEEE Trans. Information Theory*, IT-15 (1969), 122–127.
- [33] MULLER, D. E. «Application of Boolean algebra to switching circuit design and to error detection». *Transactions of the I.R.E. Professional Group on Electronic Computers*, EC-3 (3) (1954), 6–12.
- [34] PHELPS, K. T.; RIFÀ, J.; VILLANUEVA, M. «Kernels and p -kernels of p^r -ary 1-perfect codes». *Des. Codes Cryptogr.*, 37 (2) (2005), 243–261.
- [35] PLESS, V. S.; HUFFMAN, W. C. (ED.). *Handbook of Coding Theory*. Vol. II. Holanda: Elsevier Science B.V., 1998.
- [36] REED, I. S. «A class of multiple-error-correcting codes and the decoding scheme». *Trans. I.R.E.*, PGIT-4 (1954), 38–49.
- [37] REINSEL, D.; GANTZ, J.; RYDNING, J. «Data age 2025: The digitization of the world. From edge to core». A: *International Data Corporation. White Paper*, US44413318 (novembre 2018), 1–28. <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.
- [38] RIFÀ, J.; HUGUET, LL. *Comunicación digital: teoría matemática de la información, codificación algebraica, criptología*. Barcelona: Masson, 1991. (Colección Técnica y Científica de Telecomunicaciones)

- [39] SATHIAMOORTHY, M.; ASTERIS, M.; PAPAILIOPOULOUS, D.; DIMAKIS, A. G.; VADALI, R.; CHEN, S.; BORTHAKUR, D. «XORing elephants: Novel erasure codes for big data». A: *Proceedings of the 39th International Conference on Very Large Data Bases*. Riva del Garda: Curran Associates, 2013, 325-336.
- [40] SAYOLS, N.; XAMBÓ, S. «Codis correctors d'errors i criptografia postquàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 33 (2) (2018), 147-171.
- [41] SHANNON, C. E. «A mathematical theory of communication». *Bell System Tech. J.*, 27 (3) (1948). 379-423.
- [42] STIEVANO, I. (ED.). *Flash Memories*. Londres: IntechOpen, 2011.
- [43] TIETÄVÄINEN, A. «On the nonexistence of perfect codes over finite fields». *SIAM J. Appl. Math.*, 24 (1973), 88-96.
- [44] VARDY, A. «The intractability of computing the minimum distance of a code». *IEEE Trans. Inform. Theory*, 43 (6) (1997), 1757-1766.
- [45] WANG, W.; KUANG, H. «Saving capacity with HDFS RAID». *Facebook Core* (5 juny 2014). <https://code.fb.com/core-data/saving-capacity-with-hdfs-raid/>.
- [46] WICKER, S. B.; BHARGAVA, V. K. (ED.). *Reed-Solomon Codes and their Applications*. Nova York: Wiley-IEEE Press, 1994.
- [47] ZHANG, L.; TAN, Y.-A.; ZHANG, Q.-K. «Identification of NAND flash ECC algorithms in mobile devices». *Digital Investigation*, 9 (1) (2012), 34-48.
- [48] ZHANG, Z.; WANG, A.; ZHENG, K.; MAHESWARA, G.; VINAYAKUMAR, B. «Introduction to HDFS erasure coding in Apache Hadoop». *Cloudera Engineering Blog* (23 setembre 2015). <https://blog.cloudera.com/blog/2015/09/introduction-to-hdfs-erasure-coding-in-apache-hadoop/>.
- [49] ZINOV'EV, V. A.; LEONT'EV, V. K. «Nonexistence of perfect codes over Galois fields». *Problems of Control and Information Theory*, 2 (1973), 123-132.

DEPARTAMENT D'ENGINYERIA DE LA INFORMACIÓ I DE LES COMUNICACIONS
UNIVERSITAT AUTÒNOMA DE BARCELONA
merce.villanueva@uab.cat, cristina.fernandez@uab.cat

English summaries

Miriam Alcalá Vicente

The beginning of non-Euclidean geometry in Italy

Non-Euclidean geometry is probably one of the most revolutionary theories of the 19th century. After remaining unnoticed for over 30 years, from 1860 it underwent a Renaissance process, which was driven by the work of two mathematicians: Jules Hoüel and Giuseppe Battaglini.

This article is about the process of dissemination, development and acceptance of the new geometry, focusing on the Italian context. In particular, we will show that the contribution of G. Battaglini to this area goes far beyond the disclosure. At the end of his article «Sulla geometria immaginaria di Lobatschewsky», we find an unexpected coincidence between his description of the non-Euclidian plane and the subsequent Beltrami's disk model. Our purpose is to justify the similarities between these two interpretations.

Keywords: history of geometry, non-Euclidean geometry, Hoüel, Battaglini, Beltrami.

MSC2010 Subject Classification: 01A55, 51-03, 53-03.

Cristina Dalfó and Miquel Àngel Fiol

The method of lines for numerical solutions of partial differential equations

In this paper, we describe a semi-discrete method for a numerical resolution of a type of partial differential equations called the method of lines (MOL). This method is based on the discretization of all but one of the variables of the problem. We illustrate this method by solving the Laplace equation in Cartesian

coordinates. We compare the concepts used by the MOL with respect to the analytical method of variable separation. We show that the results obtained with the MOL are very good approximations of the analytical solutions.

Keywords: partial differential equations, discretization of a continuous variable, numerical analysis.

MSC2010 Subject Classification: 65M20.

Mercè Villanueva and Cristina Fernández-Córdoba

Error detecting and correcting codes and some of their applications in the information society

In digital transmissions of information from a sender to a receiver through a channel, errors may occur. In this article, the most important concepts and results of the theory of error detecting and correcting codes are discussed. This theory studies efficient methods to guarantee accurate transmission of information. First, some everyday examples of error detecting codes are described, such as the codes included in DNI, ISBN, IBAN and EAN. Next, the classical theory of error correcting codes is presented, particularly considering linear codes and, within them, cyclic codes, which are more efficient for encoding. The two most important families of cyclic codes, the BCH and Reed-Solomon codes, which also make it possible to decode efficiently, are also described. Lastly, two historical applications, in computer memories and the transmission of photographs in space, and two more recent applications, in QR codes and distributed storage, are shown.

Keywords: error detection, error correction, linear codes, cyclic codes, BCH, Reed-Solomon, applications.

MSC2010 Subject Classification: 94B05, 94B15, 11T71.

Instruccions per als autors

Els articles sotmesos a publicació s'han d'enviar als editors o a qualsevol membre del comitè editorial per correu electrònic, preferentment en format PDF. Els originals han de contenir la versió anglesa del títol, un resum breu en català i en anglès, paraules clau en català i en anglès i els codis de la classificació per matèries MSC2010.

Les versions definitives dels articles acceptats s'han de presentar en codi $\text{\TeX}$, preferentment en l'estil $\text{\LaTeX}$ propi del BUTLLETÍ. Aquest estil es pot obtenir a les pàgines web de la Societat Catalana de Matemàtiques (SCM). Fem notar que en aquesta publicació s'utilitza preferentment el punt per a separar decimals, en lloc de la coma recomanada per l'IEC, per a poder facilitar la comprensió de les expressions matemàtiques. Per tal d'accelerar el procés de producció, es prega als autors que segueixin les indicacions contingudes en el document d'exemple.

La versió en paper del BUTLLETÍ s'imprimeix en blanc i negre. Quan un article contingui figures en color i es consideri convenient, l'autor proporcionarà una versió dels gràfics substituint el color per tons de grisos i línies de gruix variable. Així mateix, modificarà els comentaris que facin referència al color de les figures. En qualsevol cas, el BUTLLETÍ publicarà l'original en color en el seu format electrònic.

La propietat intel·lectual dels articles és dels respectius autors.

Els autors, en el moment de lliurar els articles al BUTLLETÍ per a sol·licitar-ne la publicació, accepten els termes següents:

- Els autors cedeixen a la SCM (filial de l'Institut d'Estudis Catalans) els drets de reproducció, comunicació pública i distribució dels articles presentats per a ser publicats al BUTLLETÍ.

- Els autors responen davant la SCM de l'autoria i l'originalitat dels articles presentats.

- És responsabilitat dels autors l'obtenció dels permisos per a la reproducció de tot el material gràfic inclòs en els articles.

- La SCM està exempta de tota responsabilitat derivada de l'eventual vulneració de drets de propietat intel·lectual per part dels autors.

Cada autor rebrà una còpia en PDF d'alta qualitat de la versió digital del seu article i un exemplar imprès del número del BUTLLETÍ en el qual es publiqui.

La correspondència administrativa relacionada amb el BUTLLETÍ s'ha d'adreçar a la SCM.

Pel que fa a la protecció de dades personals, l'Institut d'Estudis Catalans (IEC) compleix el que estableix el Reglament general de protecció de dades de la Unió Europea (Reglament 2016/679, del 27 d'abril de 2016). De conformitat amb aquesta norma, s'informa que, amb l'acceptació de les normes de publicació, els autors autoritzen que les seves dades personals (nom i cognoms, dades de contacte i dades de filiació) puguin ser publicades en el corresponent volum del BUTLLETÍ.

Aquestes dades seran incorporades a un tractament que és responsabilitat de l'IEC amb la finalitat de gestionar aquesta publicació. Únicament s'utilitzaran les dades dels autors per a gestionar la publicació del BUTLLETÍ i no seran cedides a tercers, ni es produiran transferències a tercers països o organitzacions internacionals. Un cop publicat el BUTLLETÍ, aquestes dades es conservaran com a part del registre històric d'autors. Els autors poden exercir els drets d'accés, rectificació, supressió, oposició, limitació en el tractament i portabilitat, adreçant-se per escrit a l'Institut d'Estudis Catalans (carrer del Carme, 47, 08001 Barcelona), o bé enviant un correu electrònic a l'adreça dades.personals@iec.cat, en què s'especifiqui de quina publicació es tracta.

Comitè editorial

Antoni Guillamon (editor en cap)
Departament de Matemàtiques
Universitat Politècnica de Catalunya
antoni.guillamon@upc.edu

Carme Cascante
Dep. de Matemàtiques i Informàtica
Universitat de Barcelona
cascante@ub.edu

Bartomeu Coll
Dep. de Matemàtiques i Informàtica
Universitat de les Illes Balears
tomeu.coll@uib.cat

Núria Fagella
Dep. de Matemàtiques i Informàtica
Universitat de Barcelona
fagella@maia.ub.es

Armengol Gasull
Departament de Matemàtiques
Universitat Autònoma de Barcelona
gasull@mat.uab.cat

Gábor Lugosi
ICREA i Departament d'Economia
Universitat Pompeu Fabra
gabor.lugosi@upf.edu

Rosa Camps (editora adjunta)
Departament de Matemàtiques
Universitat Autònoma de Barcelona
rcamps@mat.uab.cat

Marc Noy
Departament de Matemàtiques
Universitat Politècnica de Catalunya
marc.noy@upc.edu

Francesc Planas
Departament de Matemàtiques
Universitat Politècnica de Catalunya
francesc.planas@upc.edu

Joan Saldaña
Dep. d'Informàtica, Mat. Aplicada i Estadística
Universitat de Girona
joan.saldana@udg.edu

Marta Sanz-Solé
Dep. de Matemàtiques i Informàtica
Universitat de Barcelona
marta.sanz@ub.edu

Gil Solanes
Departament de Matemàtiques
Universitat Autònoma de Barcelona
solanes@mat.uab.cat

Durant el procés d'elaboració d'aquest número s'ha produït el canvi d'editor en cap del BUTLLETÍ. Agraïm a Julià Cufí, antic editor en cap, la tasca realitzada durant tots aquests anys i, en concret, en la primera etapa de la confecció d'aquest número.



Societat Catalana de Matemàtiques

La **Societat Catalana de Matemàtiques (SCM)** és una societat filial de l'Institut d'Estudis Catalans, que continua les activitats de la Secció de Matemàtiques de la Societat Catalana de Ciències, que fou fundada per l'Institut l'any 1931. Les finalitats de la **SCM** són: el conreu de les ciències matemàtiques, l'extensió del seu coneixement en la societat catalana, el foment del seu ensenyament i de la seva investigació teòrica i aplicada, així com la publicació de tota mena de treballs que s'adeqüin a aquests objectius. La **SCM** desenvolupa les seves activitats en les terres de llengua i cultura catalanes. El català és, doncs, la llengua pròpia de la **SCM** i la que és usada normalment en tots els seus actes i publicacions.

La **SCM** edita les publicacions periòdiques *SCM/Notícies* i *Butlletí de la Societat Catalana de Matemàtiques*. Els socis de la **SCM** reben, gratuïtament, aquestes dues publicacions.

La **SCM** té convenis de reciprocitat amb diverses societats matemàtiques d'arreu del món, mitjançant els quals els socis de la **SCM** obtenen una reducció en la quota de soci d'aquestes societats. Així mateix, els socis de la **SCM** poden fer-se socis de la Societat Matemàtica Europea pagant una quota complementària.

La Junta Directiva de la **SCM** està constituïda per les persones següents:

PRESIDENTA: Dolors Herbera i Espinal

VICEPRESIDENT: Josep Vives i Santa-Eulàlia

ADJUNT A LA VICEPRESIDÈNCIA: Abraham de la Fuente Pérez

SECRETÀRIA: Immaculada Baldomà i Barraca

TRESORER: Albert Granados i Corsellas

VOCALS: Albert Avinyó i Andrés, Núria Fagella i Rabionet, Josep Grané i Manlleu, Carles Romero i Chesa, Aleix Ruiz de Villa, Manel Udina i Abelló

DELEGADA DE L'IEC: Pilar Bayer i Isant

L'adreça de la **SCM** és carrer del Carme, 47, 08001 Barcelona. Telèfon: 933 248 583. Fax: 932 701 180. Correu electrònic: scm@iec.cat. Adreça web: <http://scm.iec.cat>.

El Butlletí de la Societat Catalana de Matemàtiques publica, en llengua catalana, exposicions matemàtiques de qualitat, que puguin interessar a un nombre elevat de lectors. Es donarà prioritat a aquells treballs en què destaquin la claredat d'exposició i l'interès general del tema. El Butlletí està obert a tots els camps de la matemàtica i també als aspectes matemàtics de les ciències experimentals, la tecnologia, l'economia, etc., així com a altres àrees, com la història, la didàctica i la filosofia, sempre que els treballs tinguin un component matemàtic important. També tenen cabuda al Butlletí aquells articles que desenvolupin un aspecte significatiu de la problemàtica de la professió matemàtica al nostre país.

El Butlletí publica un volum a l'any, dividit en dos números, que es trameten gratuïtament a tots els socis. El Butlletí es publica també en format electrònic. L'edició electrònica del Butlletí pot obtenir-se des del portal de revistes científiques en línia de l'IEC o al servidor <http://scm.iec.cat>.

La correspondència administrativa s'ha d'adreçar a la Societat Catalana de Matemàtiques.

Editor en cap _____

Antoni Guillaumon

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Editora adjunta _____

Rosa Camps

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Comitè editorial _____

Carne Cascante

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Marc Noy

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Bartomeu Coll

Dep. de Matemàtiques i Informàtica

Universitat de les Illes Balears

Francesc Planas

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Núria Fagella

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Joan Saldaña

Dep. d'Informàtica, Mat. Aplicada i Estadística

Universitat de Girona

Armengol Gasull

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Marta Sanz-Solé

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Gábor Lugosi

ICREA i Departament d'Economia

Universitat Pompeu Fabra

Gil Solanes

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Societat Catalana de Matemàtiques

Carrer del Carne, 47 - 08001 Barcelona

tel. 933 248 583 - fax 932 701 180

scm@iec.cat - <http://scm.iec.cat>