

BUTLLETÍ

DE LA SOCIETAT CATALANA
DE MATEMÀTIQUES
Institut d'Estudis Catalans

í n d e x

- ☐ *Esther Barrabés i Mercè Ollé*
Dinàmica de varietats espacials: les autopistes de l'univers 97
- ☐ *Ramsès Fernàndez-València*
Isogènies, codis i reticles en criptografia postquàntica 125
- ☐ *Jordi Marzo*
Punts d'energia mínima i empaquetaments d'esferes 153
- ☐ *Lluís Vena*
Caracteritzant els codis de Gauss: només cal girar la cantonada 169
- ☐ English summaries 209



Volum 34 • Número 2 • Any 2019



Institut
d'Estudis
Catalans

BUTLLETÍ

DE LA SOCIETAT CATALANA

DE MATEMÀTIQUES

Institut d'Estudis Catalans

Volum 34 • Número 2 • Desembre 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

ESTHER BARRABÉS I MERCÈ OLLÉ	
Dinàmica de varietats espacials: les autopistes de l'univers	97
RAMSÈS FERNÀNDEZ-VALÈNCIA	
Isogènies, codis i reticles en criptografia postquàntica	125
JORDI MARZO	
Punts d'energia mínima i empaquetaments d'esferes	153
LLUÍS VENA	
Caracteritzant els codis de Gauss: només cal girar la cantonada	169
English summaries	209

Dinàmica de varietats espacials: les autopistes de l'univers

ESTHER BARRABÉS I MERCÈ OLLÉ

C'est par la logique qu'on démontre, c'est par l'intuition qu'on invente.

Henri Poincaré (1854–1912)

Resum: En aquest article volem il·lustrar com la comprensió de la dinàmica d'alguns models de la mecànica celeste permet explicar alguns fenòmens astronòmics i dissenyar missions realistes a l'espai. El model paradigmàtic usat és el problema restringit de tres cossos, en el qual els objectes que tenen un paper essencial són les varietats invariants de les anomenades *òrbites de libració*, és a dir, òrbites periòdiques i quasiperiòdiques al voltant dels anomenats *punts d'equilibri col·lineals del model*. Descriurem alguns d'aquests fenòmens i esmentarem algunes missions concretes. Finalment, comentarem altres models també útils (i més sofisticats) a l'astrodinàmica i acabarem amb algun comentari de com les eines de sistemes dinàmics es poden traslladar del món macroscòpic (celeste) al microscòpic, com per exemple el de la física atòmica clàssica.

Paraules clau: problema restringit, varietats invariants, punts d'equilibri, òrbites periòdiques, òrbites quasiperiòdiques, connexions homoclíniques, connexions heteroclíniques.

Classificació MSC2010: 70F07, 70F10, 70F15, 70H12, 70H33, 70K44.

1 Introducció

La teoria de sistemes dinàmics comença a les darreries del segle XIX amb Poincaré, el qual estudia els sistemes d'equacions de manera global, en comptes d'abordar les solucions de manera particular. La idea és usar mètodes qualitatius i quantitativs per obtenir una imatge global de l'evolució dels estats del sistema. En aquesta imatge, els actors principals són els objectes invariants del sistema: començant pels punts d'equilibri, seguint amb solucions

periòdiques i quasiperiòdiques, i les varietats invariants associades a tots els anteriors quan aquests són hiperbòlics. En el camp de la mecànica celeste, el problema de tres cossos restringit és el model paradigmàtic en el qual s'han explotat principalment les idees i tècniques dels sistemes dinàmics. En particular, la comprensió d'aquest model ha permès, en el camp de l'astrodinàmica, donar una empenta enorme al disseny de missions espacials, basat inicialment en l'assaig i error amb posterior refinament per obtenir la trajectòria desitjada. El resultat d'aplicar els mètodes de càlcul de solucions periòdiques i quasiperiòdiques, i també de parametrització de varietats invariants, ha permès poder determinar amb eficiència determinades trajectòries i incrementar enormement la capacitat de dissenyar-ne de noves que anteriorment eren impensables.

Aquestes trajectòries són solucions particulars de l'anomenat *problema de n cossos*. Considerem un sistema de referència inercial. El problema de n cossos de la mecànica clàssica correspon a la descripció del moviment de n masses puntuals $m_1, m_2, \dots, m_n$ sota la llei d'atracció gravitatòria de Newton:

$$m_k \ddot{\mathbf{r}}_k = G \sum_{j=1, j \neq k}^n \frac{m_j m_k}{r_{jk}^3} (\mathbf{r}_j - \mathbf{r}_k), \quad k = 1, 2, \dots, n,$$

on $\mathbf{r}_k$, $k = 1, \dots, n$, és la posició de cada cos, $r_{jk} = |\mathbf{r}_j - \mathbf{r}_k|$ la distància entre els cossos de massa m_j i m_k , i G la constant gravitatòria. Fixada una condició inicial per a cada cos (posició i velocitat), la solució $(\mathbf{r}_1(t), \dots, \mathbf{r}_n(t))$ del sistema d'equacions conté la trajectòria o *òrbita* $\mathbf{r}_k(t)$ de cadascun.

El model més senzill és el problema de dos cossos, que es pot reformular com el problema de Kepler:

$$\ddot{\mathbf{r}} = G(m + M) \frac{\mathbf{r}}{r^3},$$

on $\mathbf{r}$ és el vector de posició relativa d'un cos respecte a l'altre. Aquest problema és integrable; això vol dir que tenim suficients integrals primeres (constants sobre les trajectòries), de forma que cada trajectòria és intersecció de les hipersuperfícies de nivell i, per tant, tenim una equació (en general implícita) per a la trajectòria. Les seves solucions, conegudes com a *òrbites keplerianes*, són còniques: els dos cossos es mouen en òrbites circulars, el·líptiques, parabòliques o hiperbòliques.

El primer pas en el disseny de missions espacials comporta prendre un model prou senzill (però alhora prou acurat) que permeti el càlcul d'una trajectòria que segueixi el camí desitjat. La primera estratègia per dissenyar viatges interplanetaris consisteix en el que s'anomena *còniques empalmades* (*patching conics*): el problema de n cossos que representa el Sistema Solar es divideix en múltiples problemes de dos cossos encadenats, en cadascun dels quals intervenen el Sol o un planeta i el satèl·lit artificial, de manera que la trajectòria d'aquest últim és una seqüència d'òrbites keplerianes. Quan aquest es troba molt a prop d'un planeta, només es té en compte l'atracció gravitatòria

d'aquest cos, mentre que quan se n'allunya, la força gravitatòria que es té en compte és la del Sol. Això fa que la trajectòria del satèl·lit es pugui definir a trossos, en cadascun dels quals aquesta segueix una solució d'un problema keplerià adient (Sol-satèl·lit o planeta-satèl·lit). Per exemple, una missió a Mart consistiria primer a dissenyar una òrbita hiperbòlica respecte a la Terra fins que el satèl·lit abandonés l'esfera d'influència del planeta. A continuació seguiria una òrbita el·líptica respecte al Sol fins a trobar-se en l'esfera d'influència de Mart, on de nou seguiria una òrbita hiperbòlica respecte a aquest. Els passos propers a algun planeta es coneixen com a *assistències gravitacionals* (també anomenades *flybys* en anglès), degut al fet que provoquen un canvi significatiu en la trajectòria prèvia i permeten canviar d'una òrbita el·líptica (respecte al Sol) a una altra de diferent.

En l'últim quart del segle xx ja queda palès que el problema de dos cossos és insuficient i que les missions requereixen òrbites més sofisticades. I el model que ha permès avançar en la comprensió de la dinàmica i el disseny de trajectòries amb itineraris prescrits és el *problema restringit de tres cossos* (PRTC), que descriurem al llarg d'aquest article. Un paper cabdal el tindran els punts d'equilibri inestables d'aquest problema, així com les varietats invariants associades no només als mateixos punts d'equilibri, sinó també a òrbites periòdiques i quasiperiòdiques que hi ha al seu voltant. Els treballs de Poincaré ja mostren que, malgrat que en un entorn dels punts d'equilibri inestables del PRTC no és possible predir exactament la trajectòria d'una solució, sí que és cert que les diferents trajectòries es poden agrupar en conjunts o famílies que tenen un comportament similar. Aquests conjunts són com tubs que s'allunyen o s'acosten als punts d'equilibri (o a les òrbites periòdiques o quasiperiòdiques properes) i formen precisament les seves varietats invariants associades. Seguint-los, buscant les seves interseccions amb altres tubs que connecten amb altres punts (o òrbites properes), es poden obtenir trajectòries interessants, no només des del punt de vista del disseny de missions espacials, sinó també per a la comprensió d'alguns fenòmens naturals.

Per exemple, el PRTC circular Sol-Terra-satèl·lit és el model de referència de la ISEE-3 llançada el 1978 per a l'estudi de les interaccions Sol-Terra i de l'anomenat *space weather*. La trajectòria dissenyada seguia una transferència directa a una òrbita quasiperiòdica al voltant d'un dels punts d'equilibri del PRTC (vegeu la figura 1). De fet, en les dues últimes dècades, el nombre de missions espacials al voltant dels punts d'equilibri del problema (amb objectius científics diversos) ha crescut enormement. I això ha estat possible gràcies a l'ampli i profund estudi del model des del punt de vista de sistemes dinàmics, i que descriurem breument a continuació. El nombre d'autors i referències és extensa, però citarem com a bàsiques els treballs per a l'Agència Espacial Europea (ESA) de Gómez, Jorba, Llibre, Martínez, Masdemont, Simó ([22, 23, 19, 20]). D'altra banda, el PRTC també permet donar una explicació d'alguns fenòmens astronòmics com són la trajectòria del cometa Oterma, els asteroides troians, o el moviment en forma de ferradura de les llunes Janus i Epimeteu de Saturn o dels asteroides Cruithne o el 2002 AA29 al voltant de la Terra.

bòlic. En aquesta secció i la següent, ens concentrarem en el cas circular, en què els primaris descriuen òrbites circulars de velocitat angular constant. Per a més detalls sobre el PRTC, us recomanem [14] i [48].

Resulta especialment útil prendre un sistema de coordenades $q = (x, y, z)$ en rotació (anomenat *sinòdic*) que giri a la mateixa velocitat angular que els primaris, de manera que el nou sistema d'equacions sigui autònom. En aquest sistema, els primaris es troben fixos sobre l'eix de les x , i amb un canvi d'unitats de temps, massa i distància adequats, les equacions del problema es poden escriure com

$$\begin{aligned}\ddot{x} - 2\dot{y} &= \Omega_x, \\ \ddot{y} + 2\dot{x} &= \Omega_y, \\ \ddot{z} &= \Omega_z,\end{aligned}\tag{1}$$

on

$$\Omega(x, y, z) = \frac{1}{2}(x^2 + y^2) + \frac{1-\mu}{r_1} + \frac{\mu}{r_2},\tag{2}$$

$\mu = m_2/(m_1 + m_2) \in (0, 1/2]$ és l'anomenat *paràmetre de masses* (podem pensar que $m_1 \geq m_2$), i r_1, r_2 són les distàncies del cos infinitesimal als primaris que estan fixos a les posicions $(\mu, 0, 0)$ i $(\mu - 1, 0, 0)$ (vegeu la figura 2).

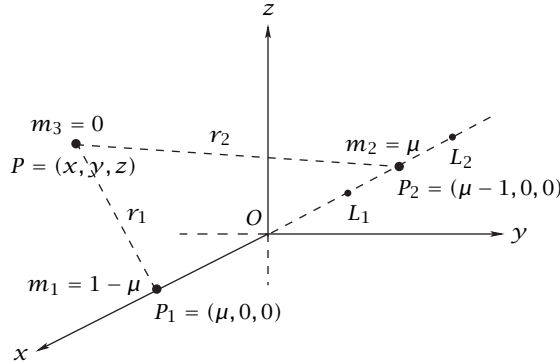


FIGURA 2: Sistema sinòdic de coordenades del problema restringit de tres cossos. Els punts collineals L_1 i L_2 també estan representats.

El PRTC té estructura hamiltoniana i en termes de posicions $q = (x, y, z)$ i moments $p = (p_x, p_y, p_z)$, on $p_x = \dot{x} - y$, $p_y = \dot{y} + x$, $p_z = \dot{z}$, les equacions es poden escriure de la forma

$$\dot{q}_i = \frac{\partial H}{\partial p_i}, \quad \dot{p}_i = -\frac{\partial H}{\partial q_i}, \quad i = 1, 2, 3,$$

amb el hamiltonià (o la funció hamiltoniana) associat definit per

$$H(x, y, z, p_x, p_y, p_z) = \frac{1}{2}(p_x^2 + p_y^2 + p_z^2) + yp_x - xp_y - \frac{1-\mu}{r_1} - \frac{\mu}{r_2}.\tag{3}$$

El problema, que depèn del paràmetre de masses μ , és no integrable i presenta una dinàmica molt rica i complicada. Una característica important és deguda al seu caràcter hamiltonià: el sistema d'equacions posseeix una integral primera. El valor de la funció hamiltoniana (3) és constant sobre cada solució del problema. Aquest valor $h = H(x, y, z, p_x, p_y, p_z)$ s'anomena *energia de l'òrbita* (o de la solució) i és l'energia Kepler (cinètica més potencial) menys el moment angular. Si $\mu = 0$, es conserven ambdues quantitats per separat; si $\mu \neq 0$, només es conserva el hamiltonià, que és la diferència. Aquesta propietat permet estudiar el problema per nivells d'energia: fixat un valor de h , s'estudia el comportament de les solucions que *viuen* en aquell valor de l'energia, i d'aquesta manera es rebaixa el problema en una dimensió. En posicions i velocitats, l'energia també és coneguda com a *constant de Jacobi* i s'escriu com

$$\dot{x}^2 + \dot{y}^2 + \dot{z}^2 = 2\Omega(x, y, z) - C_J, \quad (4)$$

on Ω està definida en (2). La relació entre l'energia i la constant de Jacobi és $h = -2C_J$.

La clau per a l'estudi de la dinàmica del model del PRTC circular està en el fet que el sistema d'equacions diferencials (1) presenta cinc punts d'equilibri denotats per L_i , $i = 1, \dots, 5$. Aquests es troben en el mateix pla de moviment que el dels primaris i són els punts crítics de la funció Ω . De fet, aquests punts d'equilibri són *solucions homogràfiques* del problema de tres cossos i foren descoberts per Euler (1767, configuració col·lineal que correspon a tres cossos en línia) i Lagrange (1772, formant una configuració triangular amb tres cossos en els vèrtexs d'un triangle equilàter). Així doncs, L_1 , L_2 i L_3 són els punts col·lineals, i estan situats entre els dos primaris ($\mu - 1 < x_{L_1} < \mu$), a l'esquerra del primari petit ($x_{L_2} < \mu - 1$), i a la dreta del primari gran ($x_{L_3} > \mu$), respectivament. Els altres dos punts són els anomenats *triangulars*, L_4 i L_5 , i formen un triangle equilàter amb els primaris. Vegeu la figura 3.

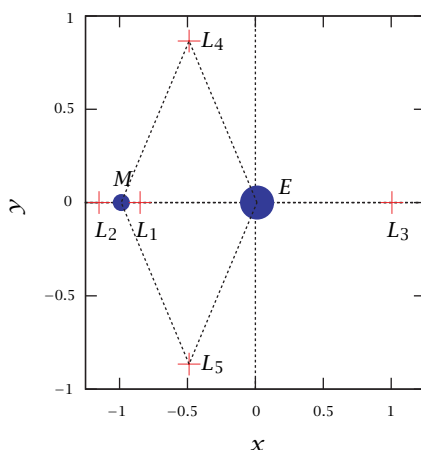


FIGURA 3: Punts d'equilibri del PRTC en el pla (x, y) en el model Terra-Lluna.

La constant de Jacobi ens permet introduir una altra característica del problema. Depenent del nivell d'energia, o valor de C_J , el tercer cos no pot bellugar-se lliurement per tot l'espai. A partir de (4), tenim definides les regions admissibles de moviment per al cos infinitesimal en l'espai (x, y, z) , donat que $2\Omega(x, y, z) - C_J \geq 0$: s'anomenen *regions de Hill*, i estan delimitades per les *superfícies de velocitat zero* definides per $2\Omega(x, y, z) - C_J = 0$. La topologia de les regions de Hill varia a mesura que el valor de C_J disminueix (o l'energia augmenta) i canvia quan C_J pren els valors corresponents als punts d'equilibri $C_J(L_i)$, $i = 1, \dots, 5$. En el pla (x, y) , les regions de Hill estan delimitades per les *corbes de velocitat zero*. Per a $C_J > C_J(L_1)$, la regió de Hill té tres components: dues d'acotades, on el moviment està confinat al voltant dels primaris, i una component no acotada, fora de la superfície de velocitat zero més externa. A $C_J(L_1)$ les dues components acotades es toquen en L_1 i per a $C_J(L_2) < C_J < C_J(L_1)$ hi ha un *coll d'ampolla* que connecta les regions al voltant dels dos primaris (figura 4, esquerra). Per a $C_J = C_J(L_2)$ les fronteres externa i interna es toquen en L_2 i per a $C_J(L_3) < C_J < C_J(L_2)$ apareix un nou coll d'ampolla que connecta la regió al voltant del primari petit amb l'exterior, tot i que encara hi ha la regió prohibida en forma de ferradura (figura 4, central). A $C_J(L_3)$ les corbes es toquen en L_3 i per a $C_J < C_J(L_3)$ ja és possible el moviment al voltant dels primaris i els punts col·lineals (figura 4, dreta). Per a valors de $C_J(L_{4,5}) < C_J < C_J(L_3)$ queda encara una regió prohibida de moviment al voltant dels punts d'equilibri triangulars, que en el pla acaba desapareixent per a $C_J < C_J(L_{4,5})$. Per a aquests valors encara queda una regió de moviment prohibida per a $z \neq 0$.

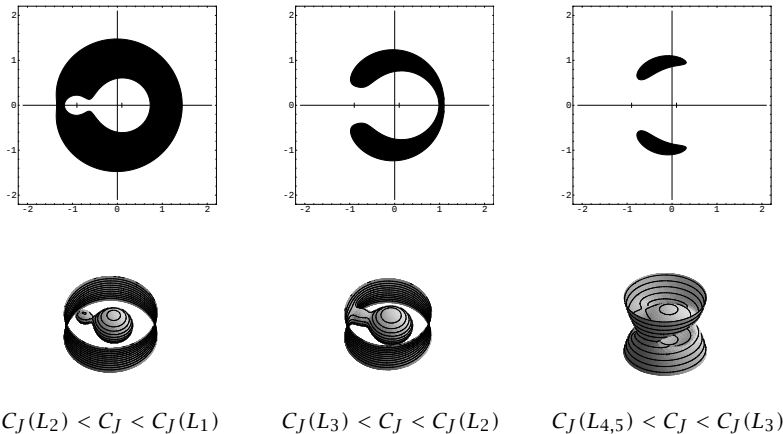


FIGURA 4: A dalt: regions de Hill (blanc) i regions prohibides de moviment (negre) al pla $z=0$. A baix: superfícies de velocitat zero a l'espai (x, y, z) .

Com avançàvem a la introducció, l'estudi de la dinàmica al voltant dels punts d'equilibri del PRTC circular i l'aplicació de la teoria de sistemes dinàmics han estat determinants tant per comprendre fenòmens naturals (l'existència dels

asteroides troians, el moviment de Janus i Epimeteu, satèl·lits de Saturn, o l'explicació de moviments coorbitals a la Terra com el de l'asteroide Cruithne) com per dissenyar missions espacials més sofisticades. El primer pas natural és estudiar l'estabilitat lineal dels punts d'equilibri i extreure la informació dinàmica que se'n deriva. Aquesta informació es troba en els valors propis de la matriu jacobiana Df del camp d'equacions (1) expressat com a sistema de primer ordre. Per al cas dels punts L_i , $i = 1, 2, 3$, els valors propis associats a la matriu diferencial del camp són

$$\text{Spec } Df(L_i) = \{\pm i\omega_1, \pm i\omega_2, \pm\lambda\},$$

on $\omega_i, \lambda > 0$ ($i = \sqrt{-1}$). Diem que els punts d'equilibri col·lineals són del tipus centre $\times$ centre $\times$ sella. Prenent l'aproximació lineal de les equacions (1), les solucions al voltant dels punts d'equilibri es poden escriure de la forma

$$Q(t) = L_i + C \begin{pmatrix} \alpha_1 \cos(\omega_1 t + \theta_1) \\ -\alpha_1 \sin(\omega_1 t + \theta_1) \\ \alpha_2 \cos(\omega_2 t + \theta_2) \\ -\alpha_2 \sin(\omega_2 t + \theta_2) \\ \xi_1 e^{\lambda t} \\ \xi_2 e^{-\lambda t} \end{pmatrix}, \quad (5)$$

on C és la matriu de vectors propis associats als valors propis (prendrem la part real i imaginària dels vectors per a valors propis complexos). Essencialment, el comportament és el de dos oscil·ladors inestables, on ω_1 és la freqüència plana (en el pla de moviment dels primaris) i ω_2 és la freqüència vertical (moviment fora del pla (x, y)). El sistema lineal, doncs, exhibeix òrbites periòdiques de freqüència ω_i , $i = 1, 2$, òrbites quasiperiòdiques (si ω_1 i ω_2 no són commensurables), i òrbites d'escapament (en temps futur i passat) associades als valors propis reals. D'una banda, aplicant el teorema de Liapunov (vegeu, per exemple, [39]), quan els valors propis no són proporcionals entre si, de cada punt col·lineal neixen dues famílies uniparamètriques d'òrbites periòdiques, conegudes com a *famílies de Liapunov planes* (dins del mateix pla de moviment dels primaris) i *verticals* (viuen a $\mathbb{R}^3$), on el paràmetre de les famílies és l'energia (o C_J). Per tant, per a cada valor fixat de h , existeixen dues òrbites periòdiques, una de plana i una de vertical, almenys per a valors de h propers al valor en el punt d'equilibri. A més, a cada nivell d'energia proper a l'energia del punt col·lineal, existeix una família biparamètrica de tors 2-dimensionals, recorreguts per les anomenades *òrbites de Lissajous*, que connecten les dues famílies de Liapunov. Vegeu la figura 5. Quan prenem tots els nivells d'energia (en un cert rang proper al del punt d'equilibri), obtenim una varietat 4-dimensional, anomenada *varietat central*, on viuen tant les òrbites periòdiques com les quasiperiòdiques. Observem que si prenem $\xi_1 = \xi_2 = 0$ en l'expressió (5) obtenim una parametrització (d'ordre 1) de les condicions inicials de totes aquestes òrbites.

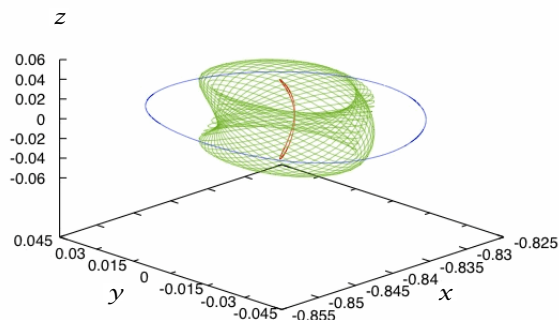


FIGURA 5: Òrbites periòdiques plana i vertical de Liapunov i òrbita quasiperiòdica de Lissajous al voltant del punt d'equilibri L_1 . (Figura cortesia de J. M. Mondelo.)

D'altra banda, degut a la sella associada als valors propis reals $\pm\lambda$, el punt col·lineal té un comportament hiperbòlic (o inestable) i apareixen les varietats invariants 1-dimensionals estable i inestable, $W^u(L_i)$, $W^s(L_i)$ respectivament, associades al punt (l'aproximació lineal s'obté de (5) fent $\alpha_{1,2} = 0$). En donarem la definició i en parlarem amb més detall a la propera secció. De retruc, les òrbites periòdiques de Liapunov hereten la hiperbolicitat i són inestables, de manera que cada òrbita té associades varietats invariants estable i inestable, ara 2-dimensionals. Aquesta inestabilitat fa difícil que ens fem una idea de com és l'espai de fases al voltant dels punts d'equilibri col·lineals. Observem que, en el cas d'un sistema hamiltonià de dos graus de llibertat, una estratègia numèrica per veure com és l'espai de fase consisteix a considerar iterats de l'aplicació de Poincaré fixat un valor de l'energia. L'aplicació de Poincaré es defineix com l'aplicació de retorn, via el flux del sistema d'equacions, a una secció fixada —anomenada *secció de Poincaré*. Usant l'energia i la secció, rebaixem la dimensió a dos, de manera que podem fer representacions gràfiques en un pla. En el cas de tenir òrbites periòdiques estables, veuríem típicament zones fitades corresponents a torsi invariants. Però en el cas de punts i òrbites inestables, per a una condició inicial arbitrària a prop, els iterats s'escapen i el mapa de Poincaré no dona informació. Així doncs, per tal d'obtenir un bon retrat de la dinàmica corresponent a les òrbites periòdiques i quasiperiòdiques al voltant dels punts d'equilibri col·lineals, s'usen tècniques analítiques com la *reducció a la varietat central*, consistent a reduir el hamiltonià per tal d'eliminar les direccions hiperbòliques (vegeu [27]), o bé mètodes numèrics explícits (vegeu [24]).

En incrementar el valor de l'energia i seguir la família d'òrbites planes de Liapunov, la freqüència i l'estabilitat de les òrbites canvien. Quan les freqüències de les òrbites plana i vertical són iguals apareix una bifurcació que dona lloc a dues famílies d'òrbites espacials simètriques respecte al pla $y = 0$, que

s'anomenen *òrbites halo* (vegeu [24], on es fa una descripció àmplia de la dinàmica al voltant dels punts d'equilibri). El seu nom prové del fet que, si prenem el PRTC amb el Sol i la Terra com a primaris, i mirem des de la Terra la projecció en el pla (y, z) d'una d'aquestes òrbites, es veu com un halo al voltant del Sol.

Les òrbites al voltant dels punts d'equilibri col·lineals L_1 i L_2 , periòdiques i quasiperiòdiques (Liapunov, halo i Lissajous) també s'anomenen *òrbites de libració*, i són el destí final de moltes missions espacials. Per exemple, les missions Genesis, ISEE-3 i SOHO són algunes de les missions on els satèl·lits han estat transferits a òrbites halo al voltant del punt L_1 del PRTC Sol-Terra.

Pel que fa als punts triangulars L_i , $i = 4, 5$, la tipologia dels valors propis de la matriu jacobiana depèn de μ : si $0 < \mu < \mu_R = \frac{1}{2}(1 - \frac{\sqrt{69}}{9}) = 0.0381 \dots$ (conegut com a *valor de Routh*), llavors $\text{Spec } Df(L_i) = \{\pm i\omega_1, \pm i\omega_2, \pm i\}$, $\omega_i > 0$. És a dir, el punt és centre $\times$ centre $\times$ centre, i quan podem aplicar de nou el teorema de Liapunov, tenim l'existència de tres famílies d'òrbites periòdiques: dues de planes —una família d'òrbites anomenades de *període curt* i una família d'òrbites anomenades de *període llarg*— i la família d'òrbites verticals. Quan $\mu = \mu_R$, es té un centre degenerat, ja que $\omega_1 = \omega_2$, i per a $\mu > \mu_R$, els valors propis són $\text{Spec } Df(L_i) = \{\pm a \pm ib, \pm i\}$, de manera que té una part de sella complexa en el pla (x, y) , el punt passa a ser inestable i té lloc una bifurcació de Hopf (vegeu, per exemple, [39, 42]).

Tot i que per a $\mu < \mu_R$ els punts $L_{4,5}$ són linealment estables, en el PRTC els punts d'equilibri triangulars són inestables ([34, 35]). Tot i això, hi ha estudis que mostren l'existència d'una regió de confinament efectiva, és a dir, que el cos de massa infinitesimal roman al voltant d'aquests punts per a intervals molt grans de temps. Els responsables d'aquest confinament són les varietats invariants (estable i inestable) de la varietat central associada al punt L_3 ([46]). Una aplicació real dels punts $L_{4,5}$ la trobem en els asteroides troians, conjunt d'asteroides localitzats al voltant dels punts $L_{4,5}$ del PRTC Sol-Jupiter, per al qual $\mu \approx 10^{-3}$ (vegeu, per exemple, [18]).

3 Varietats invariants en el PRTC circular

3.1 Definició i càlcul

Formalment, si Γ és un objecte invariant (punt d'equilibri, òrbita periòdica...) i $\phi_t(\mathbf{q})$ és la solució a temps t del PRTC circular amb condició inicial $\mathbf{q}$, definim les varietats inestable, $W^u(\Gamma)$, i estable, $W^s(\Gamma)$, associades a Γ , com a:

$$W^u(\Gamma) = \{\mathbf{q} \in \mathbb{R}^6 \mid \lim_{t \rightarrow -\infty} d(\phi_t(\mathbf{q}), \Gamma) = 0\},$$

$$W^s(\Gamma) = \{\mathbf{q} \in \mathbb{R}^6 \mid \lim_{t \rightarrow +\infty} d(\phi_t(\mathbf{q}), \Gamma) = 0\},$$

on $d(\phi_t(\mathbf{q}), \Gamma)$ és la distància entre $\phi_t(\mathbf{q})$ i el conjunt Γ .

Com hem explicat, els punts d'equilibri col·lineals L_i , $i = 1, 2, 3$, del PRTC tenen varietats invariants associades de dimensió 1. Conley, a [13], prova que cada varietat té dues branques, això és, cada varietat està formada per dues solucions del problema que tendeixen (temps endavant o endarrere) al punt d'equilibri. Concretament, usant l'aproximació lineal (5) i prenent $\alpha_1 = \alpha_2 = 0$, obtenim una parametrització d'ordre 1 de les varietats que es pot escriure com

$$\phi(\xi) = L_i + \xi v,$$

per a valors de ξ petits, on v és un vector propi unitari associat al valor propi λ (per a la varietat $W^u(L_i)$) o $-\lambda$ (per a la varietat $W^s(L_i)$). Escollint adequadament v , i per a valors de ξ petits, les branques $W_-^{u/s}$ s'allunyen cap al semiespai $x < x_{L_i}$ per a ξ negatiu, mentre que les branques $W_+^{u/s}$ s'allunyen cap a $x > x_{L_i}$ per a ξ positiu. Integrant el sistema diferencial, temps endavant o enrere amb aquestes condicions inicials, s'obtenen les varietats inestable i estable respectivament. Vegeu la figura 6.

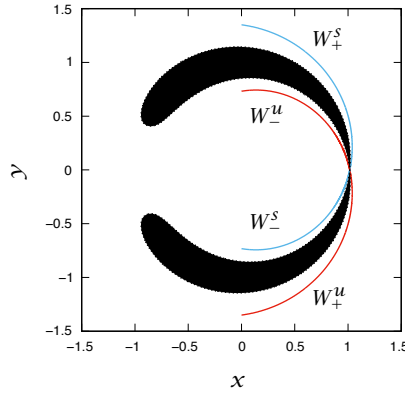


FIGURA 6: Projectió en el pla de configuracions (x, y) de les varietats invariants 1-dimensionals associades al punt d'equilibri L_3 del PRTC circular. Les internes són $W_-^{u/s}$ i les externes $W_+^{u/s}$.

Si ara ens situem en un nivell d'energia h a prop i per sobre del nivell dels punts d'equilibri col·lineals, tenim una òrbita periòdica plana, una de vertical i una família d'òrbites de Lissajous (quasiperiòdiques), cadascuna de les quals té associades les seves varietats invariants, en aquest cas de dimensió 2 (per a les òrbites periòdiques) i dimensió 3 (per a les òrbites quasiperiòdiques), les quals hereten el comportament (al voltant de l'òrbita periòdica) de les varietats 1-dimensionals dels punts d'equilibri. Podem pensar que el punt d'equilibri s'ha engreixat i ha donat lloc a una òrbita periòdica (o quasiperiòdica) i que les varietats invariants que abans eren 1d ara s'han engreixat i han passat a varietats 2d (o 3d). En el cas d'una òrbita periòdica Γ , $W^{u/s}(\Gamma)$, són varietats 2-dimensionals foliades per solucions del PRTC circular, totes elles

en el mateix nivell d'energia que l'òrbita periòdica. Geomètricament es poden veure com tubs que s'acosten (endavant o endarrere en el temps) cap a l'òrbita periòdica. Cadascuna de les varietats posseeix també dues branques, $W_{\pm}^{u/s}$, en un comportament similar al de les varietats dels punts d'equilibri. Vegeu la figura 7.

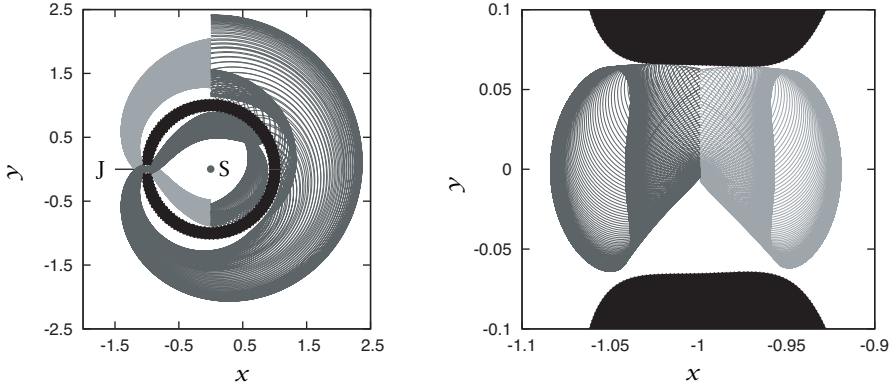


FIGURA 7: En el PRTC Sol-Júpiter, projecció en el pla de configuracions (x, y) de les branques $W_{\pm}^{u/s}(\Gamma_i)$ associades a Γ_i òrbita periòdica al voltant de L_i , $i = 1, 2$. Esquerra: branques internes $W_{+}^{u/s}(\Gamma_1)$ i branques externes $W_{-}^{u/s}(\Gamma_2)$. Dreta: detall de la regió al voltant de Júpiter, on es mostra la branca $W_{-}^u(\Gamma_1)$ i la branca $W_{+}^s(\Gamma_2)$. En gris fosc les varietats estables, en gris clar les inestables.

Anàlogament al cas de les varietats dels punts d'equilibri, per calcular numèricament les varietats invariants d'una òrbita periòdica prenem una aproximació lineal de la parametrització de la varietat, vàlida en un entorn de l'òrbita:

$$\psi(\theta, \xi) = \phi_{\frac{\theta}{2\pi}T}(\mathbf{q}_0) + \xi \Lambda^{-\theta/(2\pi)} D\phi_{\frac{\theta}{2\pi}T}(\mathbf{q}_0) \mathbf{v}, \quad (6)$$

on $\phi_t(\mathbf{q}_0)$ és la solució del PRTC començant a la condició inicial $\mathbf{q}_0$ de l'òrbita periòdica, T és el seu període, i Λ i $\mathbf{v}$ són el valor i el vector propi de la matriu de monodromia $D\phi_T(\mathbf{q}_0)$ corresponents a la varietat (estable o inestable). Aquesta aproximació d'ordre 1 de la parametrització de les varietats és invariant pel flux, excepte termes d'ordre dos en ξ , ja que

$$\phi_t(\psi(\theta, \xi)) = \psi(\theta + t\omega, e^{t\lambda}\xi) + \mathcal{O}(\xi^2), \quad (7)$$

on $\omega = 2\pi/T$, $\lambda = (\omega \ln \Lambda)/(2\pi)$. Partint de l'aproximació lineal (local) i mitjançant integració numèrica, obtenim la varietat global.

De manera similar podem calcular l'aproximació lineal de les corresponents parametritzacions de les varietats invariants associades a òrbites quasiperiòdiques, i globalitzar-les mitjançant integració numèrica.

Hi ha situacions, però, en les quals per tal de tenir una bona aproximació cal començar molt a prop del punt d'equilibri o de l'òrbita periòdica (ξ molt

petit), i llavors el temps d'integració per allunyar-se'n és molt gran. En aquest cas, és convenient expressar la parametrització ψ de la varietat com una expansió en sèrie de potències. En el cas dels punts d'equilibri, el mètode de la parametrització permet trobar ψ fins a un ordre desitjat resolent una equació d'invariància associada a les equacions. En el cas de les òrbites periòdiques, un mètode per obtenir aproximacions de qualsevol ordre de les parametritzacions consisteix a veure cada punt de l'òrbita periòdica com un punt fix d'una aplicació (el flux per a un temps igual al del període de l'òrbita) i aplicar el mètode de la parametrització per a punts fixos de difeomorfismes.

El mètode de la parametrització s'inicia cap a finals del segle xx i es desenvolupa a principis del xxi com un nou enfocament al càlcul de varietats invariants. Tot i que alguns trets del mètode remunten a Poincaré, els articles que estableixen els fonaments teòrics amb resultats rigorosos són [9, 10, 11]. Una referència recent en què es fa un recull dels desenvolupaments de la teoria, amb referències a autors diversos i les seves contribucions, així com la descripció de la metodologia numèrica aplicada concretament a varietats de punts fixos, tors invariants i al context general de varietats normalment hiperbòliques és [25]. Altres mètodes per al càlcul de varietats invariants consisteixen a obtenir altres expansions en sèries, per exemple, usant el mètode de Lindstedt-Poincaré o expandint el hamiltonià usant la reducció a forma normal (vegeu, per exemple, [38]).

3.2 Òrbites de trànsit i no trànsit, i connexions homoclíniques i heteroclíniques

Considerem el PRTC circular pla, això és, el tercer cos es mou només en el mateix pla que els primaris. Com hem dit, el problema restringit de tres cossos es pot estudiar fixant el nivell d'energia. Per a cada valor de h , les corbes de velocitat zero delimiten les regions admissibles de moviment en el pla de configuracions. En concret, per a un rang de h entre els valors de l'energia corresponents a L_1 i L_2 , es poden distingir clarament tres regions de moviment: al voltant del primari principal (regió interior), al voltant del secundari, i una zona «externa» lluny dels dos (essencialment r gran, vegeu la figura 4).

Fixada una òrbita periòdica al voltant dels punts d'equilibri col·lineals, en el cas del PRTC circular pla, les varietats invariants associades tenen codimensió 1, ja que en fixar l'energia ens situem en un espai de dimensió 3. Per tant, les varietats separen comportaments, això és, solucions a «costats» diferents de les varietats tenen comportaments diferents. Conley ([13]) defineix les òrbites de *trànsit* i de *no trànsit* de la manera següent: les primeres són solucions que s'apropen al coll d'ampolla determinat per la corba de velocitat zero i passen de la regió $\{x < x_{L_i}\}$ a la regió $\{x > x_{L_i}\}$, o a l'inrevés, mentre que les segones són solucions que s'acosten al coll d'ampolla però retornen cap al mateix semiespai. Perquè una òrbita que s'apropa cap a la regió on viu l'òrbita periòdica Γ sigui de trànsit és suficient i necessari que la solució corresponent estigui *dins* de la branca $W^s(\Gamma)$ de la mateixa regió, mentre que si està *fora* retorna cap a la mateixa regió. Vegeu la figura 8.

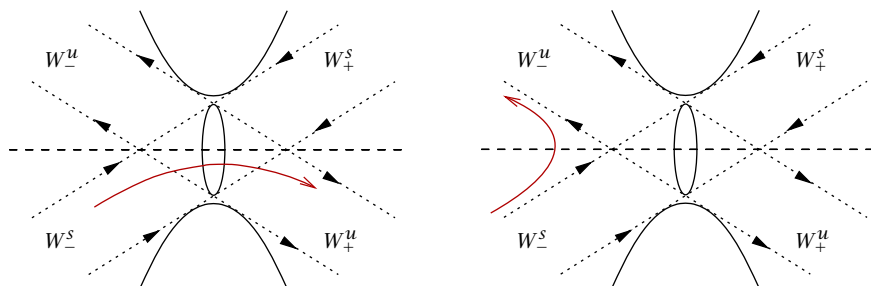


FIGURA 8: En el pla (x, y) , esquema de la dinàmica de trànsit i no trànsit en la regió de coll d'ampolla al voltant d'una òrbita periòdica inestable nascuda en un punt d'equilibri.

Per exemple, suposem que tenim el sistema restringit de tres cossos Sol-Júpiter (o qualsevol altre planeta) i que el tercer cos es troba orbitant a la regió exterior més enllà de l'òrbita de Júpiter. Perquè aquest pugui transitar cap a la regió interior (més a prop del Sol), primer cal un trànsit per la zona de L_2 per passar a la regió de Júpiter, i seguidament, un trànsit per la zona de L_1 per passar cap a la regió interior (vegeu la figura 9, esquerra). El primer trànsit es realitza dins la branca $W_-^s(\Gamma_2)$ (associada a una òrbita plana Γ_2 al voltant de L_2), i surt per l'interior de la branca $W_+^u(\Gamma_2)$, i en el segon trànsit, el tercer cos s'acosta primer al següent coll d'ampolla dins $W_-^s(\Gamma_1)$ i surt després per dintre de $W_+^u(\Gamma_1)$ (on Γ_1 és una òrbita periòdica al voltant de L_1 que viu en el mateix nivell d'energia que la primera). Un altre exemple de doble trànsit el tindríem si el tercer cos primer estigués donant voltes al voltant de Júpiter, escapés a través de la regió de L_1 a fer una (o diverses) voltes al Sol, i tornés a la regió de Júpiter. En aquest cas, la trajectòria ha de trobar-se primer dins $W_+^u(\Gamma_1)$ i després dins $W_-^s(\Gamma_1)$ (vegeu la figura 9, dreta).

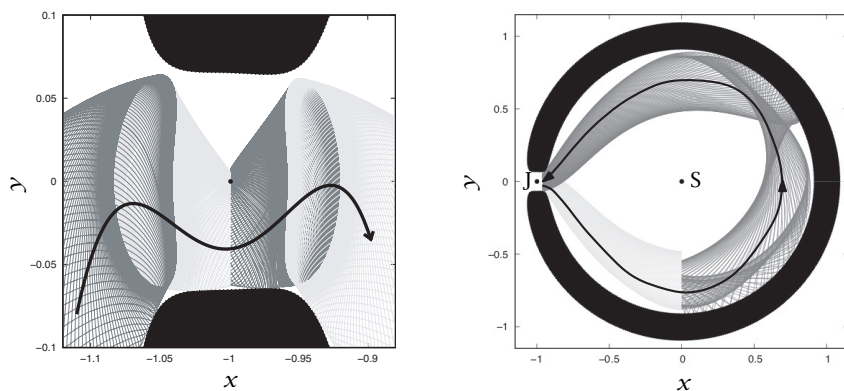


FIGURA 9: En el pla (x, y) . Esquerra: ampliació de la regió al voltant de Júpiter (punt marcat al centre), i esquema del doble trànsit des de la regió exterior fins a la interior al voltant del Sol. Dreta: doble trànsit del cos que comença a la regió al voltant de Júpiter, passa a la regió interior i torna a la primera regió.

Clarament, doncs, perquè hi pugui haver trànsit d'una regió a una altra, és necessari que dues branques, una de cadascuna d'algunes varietats estable i inestable, s'intersequin. Si les dues branques que es tallen estan associades a òrbites periòdiques diferents (com en el cas de la figura 9, esquerra), tindrem una connexió heteroclínica, això és, una solució del PRTC que temps endavant i endarrere tendeix a una òrbita periòdica diferent (figura 10, esquerra). En cas que les dues branques que es troben estiguin associades a la mateixa òrbita periòdica (figura 10, dreta), tindrem una connexió homoclínica.

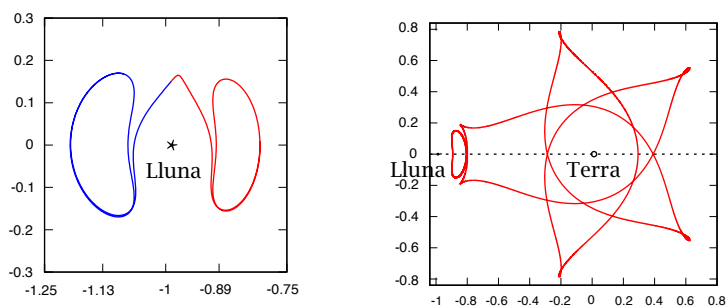


FIGURA 10: Exemples de connexions homo-heteroclíniques en el PRTC Terra-Lluna en l'espai de configuracions (x, y) . Esquerra: connexió heteroclínica entre dues òrbites periòdiques de Liapunov al voltant de L_1 i L_2 . Dreta: connexió homoclínica d'una òrbita periòdica de Liapunov al voltant de L_1 . (Figura cortesia de J. M. Mondelo.)

Una metodologia numèrica per calcular solucions homo-heteroclíniques consisteix a seguir un cert nombre de trajectòries sobre cadascuna de les branques de les varietats invariants involucrades fins que aquestes creuen una determinada secció de Poincaré. Donat que estem sobre un nivell d'energia fixat, el problema queda reduït a dos graus de llibertat i és fàcil comprovar visualment si les dues varietats s'intersequen o no. Un cop trobada una primera connexió, es pot dissenyar un mètode de continuació numèrica prenent l'energia com a paràmetre, per tal de trobar famílies de connexions homo-heteroclíniques. El procés requereix, per a cada pas corresponent a un nivell d'energia fix, resoldre un sistema d'equacions que té com a solució les noves òrbites periòdiques i la connexió entre elles ([5, 6]).

L'estudi de l'existència d'òrbites de trànsit i no trànsit, homoclíniques i heteroclíniques, i el seu càlcul són fonamentals tant per al disseny de trajectòries amb recorreguts específics, com per explicar fenòmens astronòmics reals. Per exemple, la construcció de cadenes de solucions heteroclíniques permet propostes com el *Petit grand tour*, que visita diverses llunes de Júpiter ([21, 30]), o l'existència de connexions homoclíniques permet calcular òrbites periòdiques properes amb un comportament semblant, com el cas dels cicles entre la Terra i la Lluna (òrbites que passen a prop dels dos cossos i d'interès per al suport de les telecomunicacions, la navegació, etc.); vegeu la figura 10, dreta, i [12]. La concatenació de trànsits i connexions homo-heteroclíniques que exhibeixen determinades ressonàncies permet explicar ressonàncies orbitals com les del

cometa Oterma ([29]). És desitjable, doncs, construir mapes de connexions homo-heteroclíniques entre objectes invariants (tant d'òrbites periòdiques com quasiperiòdiques) que ens permetin tenir una idea general de possibles connexions.

Per acabar, volem fer un esment al PRTC espacial. En aquest cas, les varietats invariants associades a òrbites periòdiques són objectes 2d dins d'un espai de dimensió 5 (pensem que sempre ens reduïm a l'espai d'energia constant), i, per tant, no separen comportaments. D'altra banda, hem de tenir en compte que també apareixen, a més de les òrbites planes, les òrbites periòdiques verticals i les òrbites quasiperiòdiques. Pel que fa a les òrbites de trànsit i no trànsit, a [44] es dona una condició necessària i suficient que caracteritza una òrbita de trànsit en el problema espacial. Pel que fa a les connexions homo-heteroclíniques, la metodologia explicada de continuació de famílies de connexions és adaptable al cas espacial, amb un increment de la complexitat del sistema a resoldre, molt especialment en el cas de connexions de tors. Vegeu, per exemple, [21, 38].

3.3 Altres varietats

Tot i que ens hem concentrat en el paper que fan les varietats invariants de punts d'equilibri i òrbites periòdiques i quasiperiòdiques, volem fer notar que el sistema d'equacions diferencials del PRTC té dues singularitats amb varietats associades que poden esdevenir importants a l'hora de descriure altres tipus de particularitats.

D'una banda, una de les singularitats correspon a la col·lisió amb un dels primaris. En aquest cas, mitjançant la tècnica de la regularització (que consisteix a introduir un canvi de coordenades i de temps) podem obtenir equacions diferencials que són regulars a un entorn dels primaris. En el cas del PRTC espacial, s'acostumen a utilitzar les coordenades de Kustaanheimo-Stiefel ([47]), i en el cas pla, es prenen típicament les anomenades coordenades de Levi-Civita i/o les de McGehee ([48, 33]). Utilitzant les coordenades de McGehee en el PRTC pla, la col·lisió es pot veure com un tor amb dues circumferències de punts d'equilibri inestables, que tenen varietats invariants associades estable i inestable, de manera que moure's al llarg d'aquestes varietats correspon a òrbites que surten o arriben a col·lidir amb el primari (amb temps asimptòticament grans, [43]). Per tant, una connexió heteroclínica entre dos punts d'equilibri de la varietat de col·lisió seria una òrbita d'ejecció-col·lisió amb el primari, mentre que una solució heteroclínica, per exemple, amb una òrbita de Liapunov, seria una trajectòria que connectaria el primari amb l'òrbita periòdica. Observem que la cerca de connexions heteroclíniques de col·lisió amb la Terra i una òrbita destí pot esdevenir útil per a possibles missions espacials.

D'altra banda, esmentem la singularitat de l'infinit. També en aquest cas, amb canvis de coordenades i temps adequats (típicament el canvi de coordenades de McGehee trasllada l'infinit a l'origen), podem estudiar les varietats de cert tipus d'òrbites que neixen de l'origen i que també tenen varietats invariants associades (tot i que les òrbites són parabòliques en lloc d'hiperbòliques, [37]). Aquestes varietats poden esdevenir un mecanisme per explicar el possible transport de matèria des de l'exterior del Sistema Solar cap al seu interior.

4 Camins celestes

Si mirem al cel, on són totes aquestes òrbites i les seves varietats invariants? Què ens expliquen o de què ens serveixen? Volem mostrar com les varietats invariants expliquen alguns fenòmens observables i com poden utilitzar-se per a la navegació espacial.

4.1 Viatges espacials

El nombre de viatges per explorar el Sistema Solar creix contínuament. L'estratègia bàsica per als viatges interplanetaris des de les missions *Pioneer* i *Voyager* dels anys setanta fins a les missions *Galileo* o *Mars Observer* dels noranta consisteix a aproximar una solució del problema de n cossos concatenant i enllaçant solucions de diferents problemes de dos cossos —l'anomenat mètode de *patching conics* esmentat a la introducció. El fet que les missions siguin cada cop més exigents quant a la trajectòria que es vol seguir fa que es necessitin millors aproximacions, i el problema restringit de tres cossos ha donat resposta a aquesta demanda.

Moure's a través del Sistema Solar requereix energia. En una missió espacial, la majoria de combustible es consumeix en el moment de l'enlairament i sortida de l'atmosfera terrestre. Per a la missió *Apollo 11* a la Lluna del 1969, varen fer falta uns 3 600 000 litres de combustible (la meitat només per a la primera part de sortida de l'atmosfera). Des de llavors, la tecnologia ha permès que avui dia un coet com el *Falcon 9* necessiti només un 15 % del que va consumir el coet *Saturn V*. Però això és només per arribar a la distància de la Lluna. Un cop superat el pas inicial (sortir de l'atmosfera), per moure'ns cap al nostre destí necessitarem algun mecanisme que ens propulsi i ens faci canviar la trajectòria. És el que es coneix com a Δv (delta- v), un increment de velocitat per aconseguir-ho. La transferència de Hohmann ([8]) és la maniobra d'aquest tipus més senzilla i consisteix essencialment a passar d'una òrbita circular a una altra seguint una solució el·líptica del problema de dos cossos (el cost és major si l'òrbita inicial i final no estan al mateix pla). Per això cal un impuls inicial per sortir de l'òrbita inicial i un de final per inserir-se a l'òrbita d'aparcament. Per exemple, per arribar al punt d'equilibri L_1 del sistema Terra-Lluna sortint d'una òrbita LEO (*low earth orbit*), on es troben, per exemple, l'*Estació Espacial Internacional* (ISS), alguns satèl·lits d'observació terrestre o la constel·lació *Iridium* de 66 satèl·lits de comunicació telefònica, cal que $\Delta v = 3.15$ km/s. Per arribar a Mart amb una transferència de Hohmann, cal aproximadament $\Delta v = 5.5$ km/s, i a Júpiter $\Delta v = 14.5$ km/s. Aquest valor està al límit del que el coet més potent actualment podria assolir, i no hem tingut en compte la sortida de la Terra.

Afortunadament per a l'exploració espacial, existeixen els anomenats *camins de baix cost* (*low energy transfers*) que permeten moure's d'un lloc a un altre sense despesa en combustible (excepte un impuls inicial i un de final per entrar en el camí adequat, i maniobres de correcció). Aquests camins, que anomenarem *autopistes*, estan estretament relacionats precisament amb les

varietats invariants associades a òrbites periòdiques o quasiperiòdiques del model PRTC circular. Aquestes varietats ens donen l'esquelet bàsic que permet construir les trajectòries reals en el model complet del Sistema Solar. Viatges a cost baix energèticament parlant, però que, com tota autopista, tenen un peatge: el temps de viatge. En general, seguir aquests camins comporta temps llargs, i per dissenyar missions realistes (en temps) cal trobar punts intermedis on concatenar trajectòries diferents, usar mecanismes d'impuls puntuals (*low-thrust*), etc.

Les primeres aplicacions de l'existència i comportament de les varietats invariants serien les transferències a òrbites de libració, és a dir, òrbites periòdiques o quasiperiòdiques al voltant d'un punt d'equilibri. Per obtenir una trajectòria natural per a una missió que vulgui anar de la Terra a una òrbita de libració, primer haurem de posar el satèl·lit en una òrbita d'estacionament al voltant de la Terra de manera que aquesta intersequi la varietat estable de l'òrbita final de libració. Amb una Δv adequada, la nau s'insereix en la varietat estable, i aquesta anirà a l'òrbita de destí sense la necessitat de fer cap control ni maniobres amb costos addicionals durant el viatge. Des d'aquest punt de vista naveguem per una de les autopistes de l'espai. Així mateix, l'existència de connexions homoclíniques i heteroclíniques permet enllaçar unes autopistes amb altres i construir itineraris que comencen i acaben en entorns de diferents punts d'equilibri.

Posarem només alguns exemples de missions espacials que fan ús de la diversitat d'òrbites que exhibeix el PRTC circular:

- Les dues primeres missions a òrbites de libració al voltant d'un punt d'equilibri foren la ISEE-3 i SOHO. Aquesta última missió conjunta de l'ESA i la NASA, iniciada el 1995, ha estat especialment reexida: va ser dissenyada per arribar a una òrbita halo al voltant del punt L_1 del sistema Sol-Terra i estar-s'hi dos anys, però la transferència fou quasiperfecta i la inserció va requerir un consum de combustible tan baix que porta més de vint anys orbitant i actualment encara continua explorant l'helioesfera i el vent solar i transmetent imatges i dades de l'activitat solar (*space weather*). Vegeu la figura 11.

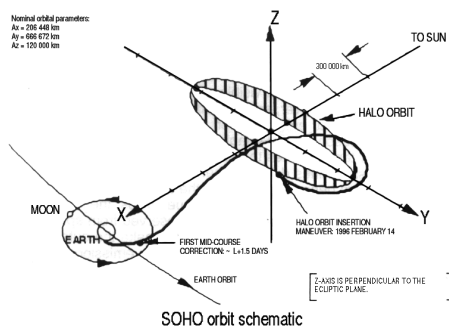


FIGURA 11: Esquema de la transferència de la missió SOHO a una òrbita halo al voltant del punt L_1 del sistema Sol-Terra. (Font: NASA.)

- Per commemorar que enguany fa cinquanta anys de la visita a la Lluna, parlarem d'alguna missió a punts d'equilibri del sistema Terra-Lluna. El 2007 es va iniciar la missió Themis, consistent en el llançament de cinc satèl·lits que es van posar en òrbita al voltant del punt de Lagrange L_2 del sistema Terra-Lluna per estudiar les tempestes espacials i les aurores. El 2010, dos dels satèl·lits es van reconvertir en la missió Artemis: un es va quedar orbitant al voltant del punt L_2 i l'altre va ser transferit al voltant del punt L_1 per poder fer observacions des de costats oposats. La transferència d'un costat a l'altre fou possible seguint una connexió heteroclínica entre dues òrbites al voltant de L_1 i L_2 respectivament. Prenent el PRTC circular amb la Terra i la Lluna com a primaris, mitjançant la metodologia numèrica descrita, s'obté la connexió heteroclínica entre dues òrbites periòdiques al voltant de L_1 i L_2 del sistema (com la que es mostra a la figura 10, esquerra), i és aquest tipus de connexió, amb l'ajut d'alguna maniobra addicional, la que s'utilitza per a la transferència. Vegeu la figura 12, esquerra.

Una altra missió que ha fet ús de *low energy transfers* en el sistema Terra-Lluna és Hiten (1990, de l'Institut de les Ciències de l'Espai i l'Astronàutica del Japó), en la qual es va llançar una sonda que va ser inserida en una òrbita lunar i més tard va visitar els punts d'equilibri L_4 i L_5 .

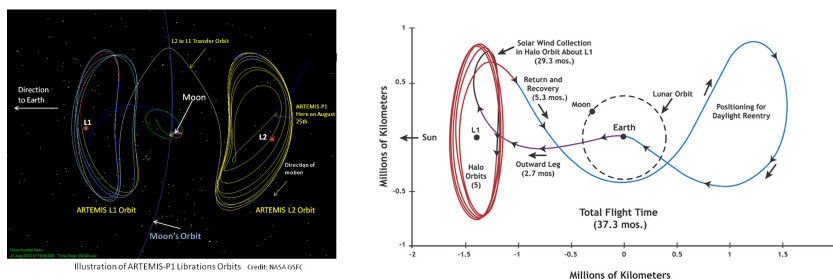


FIGURA 12: Projecció en el pla sinòdic (x, y) de les trajectòries de dues missions a punts de Lagrange: Artemis, en el sistema Terra-Lluna (esquerra), i Genesis, en el sistema Sol-Terra (dreta). (Font: NASA.)

- La missió Genesis (2001-2004) és considerada la primera que es va dissenyar usant la teoria moderna de sistemes dinàmics. Prenent ara com a model el sistema Sol-Terra, la missió fou definida de manera que, un cop la nau va ser inserida en una trajectòria cap a una òrbita quasiperiòdica al voltant de L_1 , no varen fer falta maniobres addicionals per arribar a la seva òrbita de destí. Això és possible si la trajectòria triada pertany a la varietat invariant estable de l'òrbita. El camí de tornada va fer ús de la varietat inestable de la mateixa òrbita i de l'existència de connexions heteroclíniques amb l'entorn del punt L_2 . Vegeu la figura 12, dreta.

Altres exemples de missions, en aquest cas amb el punt L_2 del sistema Sol-Terra com a destí, són Gaia (ESA, 2013), que des d'una òrbita al voltant del punt L_2 en el sistema Sol-Terra està fent un cens d'aproximadament 1 000 mi-

lions d'estrelles, o Herschel i Planck (ESA, 2009). Més recentment, tenim la sèrie Chang'e del programa d'exploració de la Lluna de l'agència espacial xinesa, anomenada així pel nom de la Lluna en la mitologia xinesa, de la qual, el Chang'e 2 (2010) ha estat estacionada en algun moment en una òrbita halo al voltant del punt L_2 .

4.2 Fenòmens naturals

El coneixement de la dinàmica del PRTC circular permet també entendre i donar una explicació a alguns fenòmens naturals per als quals el model de dos cossos és massa simple. Ja hem explicat el cas dels asteroides troians, els quals es troben confinats en una regió al voltant dels punts triangulars del problema Sol-Júpiter. La dinàmica al voltant dels punts col·lineals també ens permet explicar altres fenòmens.

Un d'aquests és el cometa Oterma. En aquest cas, l'existència de connexions homoclíniques i heteroclíniques i trànsits a través de les regions determinades per les corbes de velocitat zero ens permet explicar el moviment d'aquest cometa. S'ha observat que fins al 1980 el cometa segueix una trajectòria externa a la de Júpiter al voltant del Sol (amb una ressonància propera a 2:3, 2 voltes del cometa per 3 de Júpiter al voltant del Sol), passa prop de Júpiter per seguir una òrbita més interna a la del planeta (ara en ressonància 3:2), i torna a fer un pas cap a la regió exterior. Prenent el PRT3C circular amb el Sol i Júpiter, d'una banda existeixen connexions homoclíniques d'òrbites a l'entorn dels punts L_2 i L_1 amb aquestes ressonàncies i molt properes a les trajectòries externa i interna del cometa, respectivament, i d'altra banda, connexions heteroclíniques entre una òrbita al voltant de L_2 i una al voltant de L_1 (vegeu-ne un exemple a la figura 10, esquerra) que expliquen el trànsit de la zona externa a Júpiter a la interna (seguint la idea mostrada a la figura 9). Són justament aquestes connexions les que constitueixen l'esquelet o canal dinàmic, molt a prop del qual s'observa la trajectòria d'Oterma. Per a més detalls, citem les referències [29] i [6] (en aquesta última es donen rangs d'energia per als quals les transicions entre diferents ressonàncies és possible).

Un altre fenomen natural que s'explica per l'existència de varietats invariants és el de llunes i asteroides amb moviment coorbital o de ferradura. L'exemple més conegut és el de les llunes de Saturn, Janus i Epimeteu. En un sistema en rotació adequat, les òrbites que segueixen les dues llunes tenen forma de ferradura com la que es mostra a la figura 13, esquerra. Altres moviments semblants són els d'alguns asteroides propers a la Terra, com el Cruithne o el 2002 AA29, figura 13, dreta. Aquests asteroides segueixen una òrbita al voltant del Sol amb un semieix proper al de la Terra, que en un sistema en rotació té forma de ferradura, i s'acosten a la Terra dues vegades cada volta.

Aquests tipus d'òrbites es poden explicar a partir de les varietats invariants del punt L_3 i de les òrbites de Liapunov planes al seu voltant. Aquestes varietats s'autointersequen i donen lloc a òrbites homoclíniques. Al voltant d'aquestes connexions s'acumulen una infinitat d'òrbites periòdiques (fenomen conegut com a *blue sky catastrophe*, [15]) que ressegueixen un camí semblant. Aquest mecanisme seria el que explicaria l'existència d'aquest moviment de ferradura ([4, 32]).

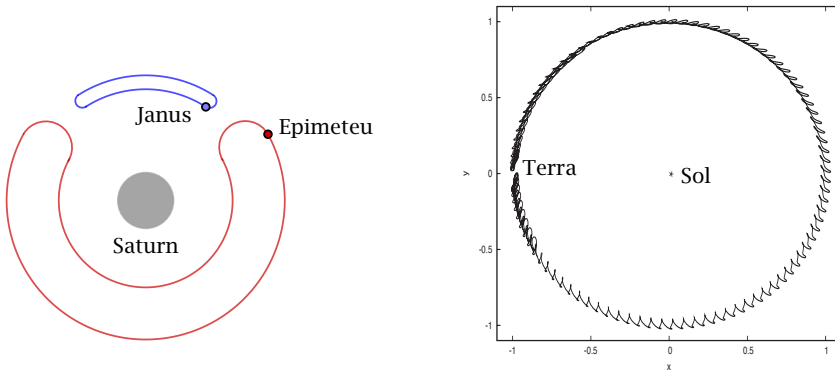


FIGURA 13: Esquerra: esquema aproximat de les trajectòries que descriuen Janus i Epimeteu. Dreta: òrbita de tipus ferradura descrita per l'asteroide 2002 AA29, en un PRTC Sol-Terra. (Font: referència [4].)

5 Altres models de la mecànica celeste

Fins ara ens hem concentrat principalment en el PRTC circular, i ja hem vist que era prou adequat per a diferents propòsits. No obstant, quan aquest model no és suficient, se'n consideren d'altres que s'ajusten millor a les situacions corresponents.

- El PRTC el·líptic: una de les primeres millores és tenir present que els primaris es mouen en òrbites el·líptiques (en lloc de circulars) al voltant del llur centre de masses, amb una excentricitat $e \neq 0$. En aquest cas, prenent unes coordenades adequades, rotatòries i pulsants (es divideix per la distància entre els primaris al llarg del temps), el sistema d'equacions diferencials que s'obté és no autònom, però periòdic. Aquest problema depèn de dos paràmetres $\mu \in (0, 0.5]$ i $e \in (0, 1]$, i té els mateixos punts d'equilibri L_i , $i = 1, \dots, 5$, tot i que canvia l'estabilitat depenent de μ i e ([48]). També deixa de tenir la integral primera, i les òrbites periòdiques apareixen aïllades (per a valors de μ i e fixats) en lloc d'agrupar-se en famílies (com passa al problema circular). Aquest model, per exemple, s'usa per a l'estudi dels asteroides troians a partir de la dinàmica al voltant dels punts L_4 i L_5 ([31]).
- El PRTC parabòlic, on ara els primaris descriuen òrbites parabòliques: introduint canvis adequats en les coordenades i en el temps, el sistema d'equacions és autònom i de tipus quasigradient (és a dir, presenta una funció monòtona a trossos). Una conseqüència important és que aquest problema no té òrbites periòdiques. Amb aquest problema es pot modelar de manera simple l'encontre entre dues galàxies. En particular es poden estudiar els mecanismes que expliquen el desplaçament de matèria (mo-

delada com a conjunts de partícules) del voltant d'una galàxia a l'altra, i explicar la formació de ponts i cues de matèria entre galàxies que s'observen a la realitat. Aquest mecanisme precisament es basa en connexions heteroclíniques entre la col·lisió amb un primari i un punt d'equilibri ([2]).

- El problema restringit de quatre cossos bicircular: és, de fet, un problema restringit de quatre cossos, obtingut del PRTC afegint un tercer primari. Més concretament, suposem dos primaris de masses m_1 i m_2 que descriuen òrbites circulars al voltant del centre de masses (localitzat a l'origen) i un tercer primari de massa m_3 que gira descrivint una òrbita circular al voltant de l'origen. El problema bicircular consisteix a descriure el moviment d'un cos de massa infinitesimal que es mou sota l'atracció dels tres primaris. En aquest cas, en coordenades adequades, el model és hamiltonià amb tres graus de llibertat i no autònom, però periòdic. Els punts d'equilibri col·lineals del PRTC amb primaris m_1 i m_3 es converteixen, en el problema bicircular, en òrbites periòdiques inestables, OPL_i , $i = 1, 2, 3$, amb les corresponents varietats invariants associades.

Remarquem que aquest model no és coherent en el sentit que les trajectòries circulars que suposem per als tres primaris no satisfan l'equació de Newton del problema de tres cossos. Malgrat aquest fet, és un problema que dona una primera aproximació força acurada d'alguns problemes de quatre cossos. Per exemple, podem considerar el model bicircular com una primera ampliació del model PRTC, en el qual, a més dels dos cossos primaris, s'afegeix com a tercer primari el següent cos del Sistema Solar de rellevància: en el sistema Terra-Lluna, afegim l'efecte gravitatori del Sol, o en el sistema Sol-Terra, si volem estudiar a prop de la Terra, afegim l'efecte de la Lluna, o en un sistema Sol-Júpiter, el següent cos a tenir en compte seria Saturn. El model bicircular també permet explicar el transport de matèria (cometes, asteroides i petites partícules) des dels planetes exteriors als interiors en el Sistema Solar. Considerem aquest com una concatenació de models bicirculars: primer Sol-Júpiter-Neptú, després Sol-Júpiter-Urà, etc., i en cadascun d'ells les varietats invariants associades a les òrbites OPL_i . La intersecció de les varietats invariants d'aquests models dona lloc a canals naturals de trànsit des del Sistema Solar exterior cap a l'interior ([3]).

- El problema bicircular coherent: és un problema restringit de quatre cossos on els tres primaris sí que es mouen seguint una solució del problema de tres cossos. Aquest model, en què s'obté un sistema hamiltonià no autònom, fou desenvolupat originalment per M. A. Andreu i C. Simó per tal d'estudiar el moviment al voltant del punt L_2 del sistema Terra-Lluna tenint en compte també l'efecte del Sol ([1]). Posteriorment s'ha aplicat per estudiar el moviment al voltant de les òrbites periòdiques substituïdes dels punts d'equilibri col·lineals del sistema Terra-Lluna tenint en compte a més el Sol (vegeu, per exemple, [26]), o al voltant dels triangles per estudiar els asteroides troians en el sistema Sol-Júpiter pertorbat per Saturn ([17]).

És clar que qualsevol dels models esmentats no s'ajusta exactament a la realitat i que, tenint en compte altres efectes, per exemple, l'aixafament d'un planeta, els efectes de radiació, o el nombre de cossos, o el moviment de tots ells, podem considerar altres models més complexos i sofisticats. Per exemple, el mètode JPL consisteix a prendre un problema de N cossos en què les trajectòries dels planetes estan donades per les efemèrides que publica la NASA. Un altre model d'aplicació a l'astrodinàmica és el PRTC en què el satèl·lit porta una *vela solar*, una superfície reflectant que s'aprofita de la pressió de radiació com a impuls extra ([16]). En general, una millora del PRTC porta a un model no autònom, en el qual el camp depèn periòdicament del temps, i un repte ha estat adequar les eines d'estudi a aquests nous models ([28]). No obstant, fins a la data d'avui, el PRTC, de formulació clarament més senzilla, ja proporciona un model força acurat per dissenyar determinades missions i explicar alguns fenòmens.

D'altra banda, a l'hora d'abordar altres problemes de tipus astronòmic, certament cap dels problemes anteriors no és suficient. Esmentem, per exemple, la modelització d'una galàxia barrada, on cal buscar una distribució de densitat de massa que approximi prou bé la seva lluminositat. El que és remarcable, però, és que, prenent altres models, també els punts d'equilibri, les òrbites periòdiques inestables i les seves varietats (del model resultant) tenen un paper cabdal a l'hora d'explicar una determinada fenomenologia. Esmentem l'article publicat en aquest *Butlletí* ([45]), en què els autors presenten una teoria que unifica la formació de braços espirals i anells en galàxies barrades.

Ja per acabar, és interessant observar com les eines de la teoria de sistemes dinàmics (concretades aquí en el rol de les varietats invariants) aplicades al macrocosmos (problemes de mecànica celeste i astronomia) es poden traslladar al món a escala atòmica. En les darreres dècades, s'han publicat diferents treballs que estudien, des del punt de vista de la mecànica clàssica, diverses qüestions rellevants a l'hora de descriure la dinàmica de determinats àtoms. Per esmentar-ne algun exemple concret, si es considera l'àtom d'hidrogen en un camp de microones circularment polaritzat, es plantegen algunes qüestions de manera natural: sota quines condicions ionitzarà l'electró? Com s'explica el seu moviment aparentment erràtic? Podem donar regions de comportament regular i d'altres de comportament caòtic? És possible que l'electró arribi a xocar amb el nucli? Totes elles es poden respondre a partir del comportament de certes varietats invariants d'un sistema d'equacions que té una forma semblant al sistema del PRTC ([7, 40, 41]).

Agraïments

E. Barrabés ha rebut el suport dels ajuts MTM2016-80117-P (MINECO/FEDER) i 2017 SGR 1374, i a M. Ollé se li han atorgat els ajuts MTM2015-65715 (MINECO/FEDER) i 2017SGR1049. Ambdues han rebut l'ajut PGC2018-100928-B-100.

Referències

- [1] ANDREU, M. «The quasi-bicircular problem». Tesi de màster. Universitat de Barcelona, 1999.

- [2] BARRABÉS, E.; CORS, J. M.; GARCÍA-TABERNER, L.; OLLÉ, M. «Tails and bridges in the parabolic restricted three-body problem». *Mon. Not. R. Astron. Soc.*, 472 (3) (2017), 2554–2568.
- [3] BARRABÉS, E.; GÓMEZ, G.; MONDELO, J. M.; OLLÉ, M. «Pseudo-heteroclinic connections between bicircular restricted four-body problems». *Mon. Not. R. Astron. Soc.*, 462 (1) (2016), 740–750.
- [4] BARRABÉS, E.; MIKKOLA, S. «Families of periodic horseshoe orbits in the restricted three-body problem». *A & A*, 432 (3) (2005), 1115–1129.
- [5] BARRABÉS, E.; MONDELO, J. M.; OLLÉ, M. «Numerical continuation of families of homoclinic connections of periodic orbits in the RTBP». *Nonlinearity*, 22 (12) (2009), 2901–2918.
- [6] BARRABÉS, E.; MONDELO, J. M.; OLLÉ, M. «Numerical continuation of families of heteroclinic connections between periodic orbits in a Hamiltonian system». *Nonlinearity*, 26 (10) (2013), 2747–2765.
- [7] BARRABÉS, E.; OLLÉ, M.; BORONDO, F.; FARRELLY, D.; MONDELO, J. M. «Phase space structure of the hydrogen atom in a circularly polarized microwave field». *Phys. D*, 241 (4) (2012), 333–349.
- [8] BATE, R. R.; MUELLER, D. D.; WHITE, J. E. *Fundamentals of Astrodynamics*. Nova York: Dover Publications, Inc., 1971.
- [9] CABRÉ, X.; FONTICH, E.; DE LA LLAVE, R. «The parameterization method for invariant manifolds. I. Manifolds associated to non-resonant subspaces». *Indiana Univ. Math. J.*, 52 (2) (2003), 283–328.
- [10] CABRÉ, X.; FONTICH, E.; DE LA LLAVE, R. «The parameterization method for invariant manifolds. II. Regularity with respect to parameters». *Indiana Univ. Math. J.*, 52 (2) (2003), 329–360.
- [11] CABRÉ, X.; FONTICH, E.; DE LA LLAVE, R. «The parameterization method for invariant manifolds. III. Overview and applications». *J. Differential Equations*, 218 (2) (2005), 444–515.
- [12] CASOLIVA, J.; MONDELO, J. M.; VILLAC, B. F.; MEASE, K. D.; BARRABÉS, E.; OLLÉ, M. «Two classes of cycler trajectories in the earth-moon system». *J. Guid. Control Dynam.*, 33 (5) (2010), 1623–1640.
- [13] CONLEY, C. C. «Low energy transit orbits in the restricted three-body problem». *SIAM J. Appl. Math.*, 16 (4) (1968), 732–746.
- [14] DANBY, J. M. A. *Fundamentals of Celestial Mechanics*. 2a ed. Richmond, VA: Willmann-Bell, Inc., 1988.
- [15] DEVANEY, R. L. «Blue sky catastrophes in reversible and Hamiltonian systems». *Indiana Univ. Math. J.*, 26 (2) (1977), 247–263.
- [16] FARRÉS, A.; JORBA, À. «Periodic and quasi-periodic motions of a solar sail close to SL_1 in the Earth-Sun system». *Celestial Mech. Dynam. Astronom.*, 107 (1-2) (2010), 233–253.

- [17] GABERN, F.; JORBA, À. «A restricted four-body model for the dynamics near the Lagrangian points of the Sun-Jupiter system». *Discrete Contin. Dyn. Syst. Ser. B*, 1 (2) (2001), 143-182.
- [18] GIORGILLI, A.; SKOKOS, C. «On the stability of the Trojan asteroids». *A & A*, 317 (1997), 254-261.
- [19] GÓMEZ, G.; JORBA, À.; SIMÓ, C.; MASDEMONT, J. *Dynamics and Mission Design near Libration Points. Vol. III. Advanced Methods for Collinear Points*. River Edge, NJ: World Scientific Publishing Co., Inc., 2001. (World Scientific Monograph Series in Mathematics; 4)
- [20] GÓMEZ, G.; JORBA, À.; SIMÓ, C.; MASDEMONT, J. *Dynamics and Mission Design near Libration Points. Vol. IV. Advanced Methods for Triangular Points*. River Edge, NJ: World Scientific Publishing Co., Inc., 2001. (World Scientific Monograph Series in Mathematics; 5)
- [21] GÓMEZ, G.; KOON, W. S.; LO, M. W.; MARSDEN, J. E.; MASDEMONT, J.; ROSS, S. D. «Connecting orbits and invariant manifolds in the spatial restricted three-body problem». *Nonlinearity*, 17 (5) (2004), 1571-1606.
- [22] GÓMEZ, G.; LLIBRE, J.; MARTÍNEZ, R.; SIMÓ, C. *Dynamics and Mission Design Near Libration Points. Vol. I. Fundamentals: The Case of Collinear Libration Points*. River Edge, NJ: World Scientific Publishing Co., Inc., 2001. (World Scientific Monograph Series in Mathematics; 2)
- [23] GÓMEZ, G.; LLIBRE, J.; MARTÍNEZ, R.; SIMÓ, C. *Dynamics and Mission Design Near Libration Points. Vol. II. Fundamentals: The Case of Triangular Libration Points*. River Edge, NJ: World Scientific Publishing Co., Inc., 2001. (World Scientific Monograph Series in Mathematics; 3)
- [24] GÓMEZ, G.; MONDELO, J. M. «The dynamics around the collinear equilibrium points of the RTBP». *Phys. D*, 157 (4) (2001), 283-321.
- [25] HARO, À.; CANADELL, M.; FIGUERAS, J.-L.; LUQUE, A.; MONDELO, J.-M. *The Parameterization Method for Invariant Manifolds. From Rigorous Results to Effective Computations*. Cham: Springer, 2016. (Applied Mathematical Sciences; 195)
- [26] HOWELL, K. C.; GUZMÁN, J. J. «Spacecraft trajectory design in the context of a coherent restricted four-body problem with application to the map mission». A: *51st International Astronautical Congress* (2-6 octubre 2000, Rio de Janeiro, Brasil). Paper IAF-00-A.5.06.
- [27] JORBA, À.; MASDEMONT, J. «Dynamics in the center manifold of the collinear points of the restricted three body problem». *Phys. D*, 132 (1-2) (1999), 189-213.
- [28] JORBA, M. «Periodic time dependent Hamiltonian systems and applications». Tesi de màster. Universitat de Barcelona, 2019.
- [29] KOON, W. S.; LO, M. W.; MARSDEN, J. E.; ROSS, S. D. «Heteroclinic connections between periodic orbits and resonance transitions in celestial mechanics». *Chaos*, 10 (2) (2000), 427-469.

- [30] KOON, W. S.; MARSDEN, J. E.; ROSS, S. D.; LO, M. W. «Constructing a low energy transfer between Jovian moons». A: *Celestial Mechanics*. Providence, RI: Amer. Math. Soc., 2002, 129–145. (Contemp. Math.; 292)
- [31] LHOTKA, CH.; EFTHYMIOPOULOS, C.; DVORAK, R. «Nekhoroshev stability at L_4 or L_5 in the elliptic-restricted three-body problem - application to Trojan asteroids». *Mon. Not. R. Astron. Soc.*, 384 (3) (2008), 1165–1177.
- [32] LLIBRE, J.; OLLÉ, M. «The motion of Saturn coorbital satellites in the Restricted Three-Body Problem». *A & A*, 378 (3) (2001), 1087–1099.
- [33] MCGEHEE, R. «Triple collision in the collinear three-body problem». *Invent. Math.*, 27 (1974), 191–227.
- [34] MCKENZIE, R.; SZEBEHELY, V. «Nonlinear stability around the triangular libration points». *Celestial Mech.*, 23 (3) (1981), 223–229.
- [35] MARKEEV, A. P. «Stability of the triangular Lagrangian solutions of the restricted three-body problem in the three-dimensional circular case». *Soviet Astronom. AJ*, 15 (1971), 682–686 (1972).
- [36] MARTÍNEZ BARCHINO, R. «Aplicació dels sistemes dinàmics a l'estudi d'òrbites de cometes i naus espacials». *Butlletí de la Societat Catalana de Matemàtiques*, 16 (1) (2001), 87–100.
- [37] MARTÍNEZ, R.; SIMÓ, C. «Invariant manifolds at infinity of the RTBP and the boundaries of bounded motion». *Regul. Chaotic Dyn.*, 19 (6) (2014), 745–765.
- [38] MASDEMONT, J. J. «High-order expansions of invariant manifolds of libration point orbits with applications to mission design». *Dyn. Syst.*, 20 (1) (2005), 59–113.
- [39] MEYER, K. R.; HALL, G. R. *Introduction to Hamiltonian Dynamical Systems and the N-body Problem*. Nova York: Springer-Verlag, 1992. (Applied Mathematical Sciences; 90)
- [40] OLLÉ, M. «To and fro motion for the hydrogen atom in a circularly polarized microwave field». *Commun. Nonlinear Sci. Numer. Simul.*, 54 (2018), 286–301.
- [41] OLLÉ, M.; PACHA, J. R. «Hopf bifurcation for the hydrogen atom in a circularly polarized microwave field». *Commun. Nonlinear Sci. Numer. Simul.*, 62 (2018), 27–60.
- [42] OLLÉ, M.; PACHA, J. R.; VILLANUEVA, J. «Motion close to the Hopf bifurcation of the vertical family of periodic orbits of L_4 ». *Celestial Mech. Dynam. Astronom.*, 90 (1–2) (2004), 89–109.
- [43] OLLÉ, M.; RODRÍGUEZ, Ò.; SOLER, J. «Ejection-collision orbits in the RTBP». *Commun. Nonlinear Sci. Numer. Simul.*, 55 (2018), 298–315.
- [44] REN, Y.; SHAN, J. «Numerical study of the three-dimensional transit orbits in the circular restricted three-body problem». *Celestial Mech. Dynam. Astronom.*, 114 (4) (2012), 415–428.

- [45] ROMERO-GÓMEZ, M.; SÁNCHEZ-MARTÍN, P.; MASDEMONT, J. J. «Com les varietats invariants formen espirals i anells en galàxies barrades». *Butlletí de la Societat Catalana de Matemàtiques*, 29 (1) (2014), 51-75.
- [46] SIMÓ, C.; SOUSA-SILVA, P.; TERRA, M. «Practical stability domains near $L_{4,5}$ in the restricted three-body problem: some preliminary facts». A: *Progress and Challenges in Dynamical Systems*. Heidelberg: Springer, 2013, 367-382. (Springer Proc. Math. Stat.; 54)
- [47] STIEFEL, E. L.; SCHEIFELE, G. *Linear and Regular Celestial Mechanics. Perturbed Two-body Motion, Numerical Methods, Canonical Theory*. Nova York; Heidelberg: Springer-Verlag, 1971. (Die Grundlehren der mathematischen Wissenschaften; 174)
- [48] SZEBEHELY, V. *Theory of Orbits. The Restricted Problem of Three Bodies*. Nova York; Londres: Academic Press, Inc., 1967.

ESTHER BARRABÉS VERA
DEPARTAMENT D'INFORMÀTICA, MATEMÀTICA APLICADA I ESTADÍSTICA
UNIVERSITAT DE GIRONA
17003, GIRONA
esther.barrabes@udg.edu

MERCÈ OLLÉ TORNER
DEPARTAMENT DE MATEMÀTIQUES
UNIVERSITAT POLITÈCNICA DE CATALUNYA
08028, BARCELONA
merce.olle@upc.edu

Isogènies, codis i reticles en criptografia postquàntica

RAMSÈS FERNÀNDEZ-VALÈNCIA

Que feliç que era la cigala a l'estiu! El sol
lluïa, les flors desprenien la seva aroma em-
briagadora i la cigala cantava i cantava. El
futur no la preocupava gens: el cel era tan
blau sobre el seu cap i les seves cançons
tan alegres... però l'estiu no és etern.

Isop (620–564 a. C.)

Resum: En aquest article presentem una breu introducció a alguns dels conceptes i de les tècniques matemàtiques que estan essent utilitzades en criptografia postquàntica. S'introdueixen la teoria de reticles, la teoria de codis i la teoria d'isogènies de corbes el·líptiques supersingulars.

Paraules clau: reticle, codi, isogènia, corba el·líptica supersingular.

Classificació MSC2010: 11T71, 14G50, 94A60.

1 Introducció

Actualment qualsevol transferència de dades comporta un procés de xifratge per tal de fer aquesta informació inintelligible quan s'envia a través de canals que no sempre són segurs. Els mecanismes de xifratge que més s'estan utilitzant, com RSA, ElGamal o ECC, fonamenten la seva seguretat i resistència principalment en els problemes següents:

1. Factorització en producte de dos primers: donat un número $a \in \mathbb{Z}$, trobar dos números primers $p, q \in \mathbb{Z}$ tals que $a = p \cdot q$.
2. Logaritmes discrets: donats un grup $(G, \cdot)$ i dos elements $a, b \in G$, trobar $k \in \mathbb{Z}$ tal que $a = b^k$.

Se sap que aquests dos problemes són computacionalment complexos per als ordinadors actuals, la qual cosa vol dir que els mètodes de xifratge que recolzen sobre aquests problemes resistirien atacs informàtics amb l'objectiu de desxifrar els missatges xifrats sempre que la implementació fos correcta, fet que pot assolir-se, per exemple, fent servir els números primers adequats.

Fins ara s'ha considerat que els mètodes de xifratge fonamentats en els problemes 1 i 2 són segurs però, a començament dels anys vuitanta, Richard Feynman i Yuri Manin, entre d'altres, van començar a teoritzar sobre la possibilitat de fer servir idees de la física quàntica en computació.

El món de la ciberseguretat va viure amb una certa tranquil·litat fins que Peter Shor va presentar un algorisme quàntic que resolvia en temps polinomial no només el problema de la factorització en primers, sinó també el problema del logaritme discret [19]. De sobte, els problemes sobre els quals recolzaven els sistemes criptogràfics més emprats deixaven de ser, teòricament, computacionalment complexos: tan bon punt arribés una computadora quàntica programable capaç d'executar l'algorisme de Shor, tots els missatges xifrats podrien ser desxifrats.

D'ençà que es va presentar l'algorisme de Shor, la preocupació per mantenir la privadesa de les dades mitjançant nous algorismes ha anat creixent fins al punt de passar de ser una petita preocupació a una prioritat en algunes empreses. Per què? Degut a la possibilitat de tenir ordinadors quàntics en qüestió de pocs anys. Actualment Microsoft, Google, IBM i D-Wave Systems són les empreses que lideren la recerca en l'anomenada *supremacia quàntica*; de fet, D-Wave Systems ha creat ordinadors quàntics, tot i que cal aclarir que són ordinadors que resolten un tipus concret de problema. L'objectiu final de la supremacia quàntica és la creació d'un ordinador quàntic universal, capaç de resoldre qualsevol tipus de problema; en aquesta direcció IBM i Microsoft estan fent passes cada cop més grans, amb tècniques que involucren conceptes de la topologia algebraica en el cas de la recerca duta a terme per Microsoft.

Davant l'aparició imminent dels primers ordinadors quàntics, cal buscar les eines matemàtiques adequades per generar algorismes de xifratge resistents als atacs d'un ordinador quàntic. Si abans la teoria de nombres era la font principal d'eines per a la creació d'algorismes criptogràfics, ara ho és la geometria algebraica. En són exemples:

1. La teoria de reticles: els problemes del vector més curt i del vector més proper estan generant algorismes de xifratge de clau pública, de signatura digital i d'intercanvi de claus.
2. La teoria de codis algebraics: bàsicament parlem de codis de Goppa. L'algorisme més famós fonamentat en aquesta teoria és el McEliece.
3. La teoria d'isogènies de corbes el·líptiques supersingulars: és un camp nou en criptografia, però molt prometedor. Els algorismes que se'n deriven són focus de recerca actual en l'àmbit de la seguretat.

La criptografia postquàntica ha esdevingut un camp de recerca molt actiu que ha obert una gran quantitat de fronts, tant en l'àmbit aplicat com en el teòric, que atrauen un nombre creixent d'empreses, centres tecnològics i grups de recerca.

L'objectiu d'aquestes notes és concentrar en una font única les principals tècniques matemàtiques involucrades en criptografia postquàntica. En particular estudiarem les tres teories esmentades abans: les teories de reticles, d'isogènies i de codis.

És important observar dos aspectes pel que fa a aquest article: d'una banda, aquestes notes no inclouen un estudi entre la complexitat computacional dels problemes que es deriven de les diferents tècniques matemàtiques i la seva resistència a la computació quàntica. Els interessats en aquests aspectes trobaran una molt bona introducció en [17]. D'una altra banda, la secció sobre els codis s'estudia àmpliament a [18] i [25]. Els interessats en els codis correctors d'errors poden complementar la informació que trobin en aquestes notes amb l'estudi contingut en la referència.

2 Reticles

2.1 Definicions fonamentals

Un reticle és un subconjunt discret i additiu $\Lambda \subseteq \mathbb{R}^n$, és a dir, tal que:

- (1) és tancat respecte de la suma i de la resta: $x \pm y \in \Lambda$, $\forall x, y \in \Lambda$, i
- (2) existeix $\epsilon > 0$ tal que $\forall x, y \in \Lambda$, $x \neq y$, se satisfà $\|x - y\| \geq \epsilon$. Dit d'una altra manera, $\forall x \in \Lambda$ existeix una bola tancada $B_\epsilon(x)$ amb centre en x i amb radi $\epsilon > 0$ tal que $\Lambda \cap B_\epsilon(x) = \{x\}$.

EXEMPLE. El conjunt $\mathbb{Q}^n \subseteq \mathbb{R}^n$ és un subconjunt tancat respecte de la suma i de la resta, però no és un reticle ja que $\mathbb{Q}$ no és discret. L'exemple de reticle més senzill és $\mathbb{Z}^n$.

Donat un conjunt $B = \{b_1, \dots, b_m\}$ amb m vectors linealment independents de $\mathbb{R}^n$, el reticle generat per B és:

$$\Lambda(B) := \left\{ \sum_{i=1}^m z_i b_i \mid z_i \in \mathbb{Z} \right\}.$$

Habitualment B s'anomena *base del reticle* $\Lambda(B)$ i es diu que Λ és generat per B . Anomenarem *rang de* Λ el valor m , i *dimensió de* Λ el valor n . Quan $m = n$ parlem de *reticles de rang màxim*.

Si pensem en el conjunt B com una matriu $n \times m$

$$B = \begin{pmatrix} b_{1,1} & \dots & b_{m,1} \\ \vdots & \ddots & \vdots \\ b_{1,n} & \dots & b_{m,n} \end{pmatrix},$$

amb columnes formades pels vectors $\{b_1, \dots, b_m\}$, aleshores s'escriu

$$\Lambda := \Lambda(B) = \{B \cdot z \mid z \in \mathbb{Z}^m\} = B \cdot \mathbb{Z}^m.$$

Donada una base B per a un reticle Λ , definim

$$\text{span}(\Lambda) := \text{span}(B) = \{B \cdot \gamma \mid \gamma \in \mathbb{R}^m\}.$$

OBSERVACIÓ. La principal diferència entre $\Lambda(B)$ i $\text{span}(\Lambda)$ és que en el primer cas es fan servir elements enters, i en el segon en fem servir de reals.

Centrem tot seguit la nostra atenció en les bases que generen el mateix reticle.

LEMA 1 ([15, lema 2.5]). *Dues bases $B = \{b_1, \dots, b_m\}$ i $B' = \{b'_1, \dots, b'_m\}$ de $\mathbb{R}^n$ generen el mateix reticle Λ si, i només si, existeix una matriu unimodular U (i.e. invertible a $M_{m \times m}(\mathbb{Z})$) tal que $B = B' \cdot U$. En aquest cas direm que les bases B i B' són equivalents.*

COROLLARI 2 ([11, teorema 2]). *Si dues bases B, B' generen el mateix reticle de rang màxim, aleshores $\det(B) = \pm \det(B')$.*

COROLLARI 3. *Dues bases B, B' generen el mateix reticle de rang màxim si, i només si, $(B')^{-1}B$ és unimodular.*

PROVA. En efecte, suposem que U és una matriu unimodular d'ordre n . Aleshores: $\Lambda(B) = \Lambda(B') \Leftrightarrow B = B' \cdot U \Leftrightarrow (B')^{-1}B = U$. $\square$

2.2 Regions fonamentals

Donat un reticle Λ , una *regió fonamental* de Λ és un subconjunt $F \subseteq \mathbb{R}^n$ tal que $\forall x \in \Lambda$ el conjunt $x + F = \{x + y \mid y \in F\}$ genera una partició de $\mathbb{R}^n$, és a dir: $\bigsqcup_{x \in \Lambda} x + F = \mathbb{R}^n$.

Donat un reticle $\Lambda(B)$, definim el *paralelepípede fonamental* associat a B com el conjunt $P(B) = \{\sum_i z_i b_i \mid z_i \in [0, 1)\}$.

LEMA 4 ([15, lema 2.10]). *Considerem un reticle $\Lambda(B)$ i una regió fonamental F del reticle $\mathbb{Z}^n$. Aleshores el conjunt $B \cdot F = \{B \cdot z \mid z \in F\}$ és una regió fonamental de $\Lambda(B)$. En particular, $P(B)$ és una regió fonamental de $\Lambda(B)$.*

El resultat següent ens permet establir una condició per determinar si un conjunt format per vectors linealment independents de Λ n'és una base:

LEMA 5 ([16, lema 1]). *Donat un reticle Λ de rang màxim i $B = \{b_1, \dots, b_n\}$ un conjunt de vectors de Λ linealment independents, aleshores B és una base de Λ si, i només si, $\Lambda \cap P(B) = \{0\}$.*

Per a un reticle $\Lambda = \Lambda(B)$ generat per una base B , definim el seu determinant com el volum del paralelepípede fonamental associat a B i el denotarem per $\text{vol}(P(B))$ o bé $\det(\Lambda)$. El resultat següent és immediat:

PROPOSICIÓ 6 ([11, proposició 2]). *Per a qualsevol base $B = \{b_1, \dots, b_m\}$, amb $b_i \in \mathbb{R}^n$, tenim la igualtat $\det(\Lambda(B)) = \sqrt{|\det(B^T B)|}$. En particular, si $B \in M_{n \times n}(\mathbb{R})$ és no singular, aleshores: $\det(\Lambda) = |\det(B)|$.*

OBSERVACIÓ. Notem l'abús de notació: escrivim B tant per denotar la base com la matriu associada.

El resultat següent prova que el volum és un invariant reticular:

COROL·LARI 7. *Donades dues bases equivalents B_1 i B_2 , el volum dels paral·lelepípedes associats és el mateix.*

PROVA. En efecte, com que les bases són equivalents existeix una matriu unimodular U tal que $B_2 = B_1 \cdot U$. Es dedueix el resultat tot calculant determinants. $\square$

2.3 Ortogonalització de Gram-Schmidt

El procediment d'ortogonalització de Gram-Schmidt té un paper important en la teoria de reticles necessària en criptografia ja que s'empra en la creació de bases que es fan servir com a clau privada en alguns algorismes, com el GGH [28].

Recordem que el procés permet trobar, a partir d'un conjunt de vectors B , un conjunt de vectors B^* tal que els seus elements són ortogonals entre si i tal que $\text{span}(B^*) = \text{span}(B)$.

Si tenim $B = \{b_1, \dots, b_n\}$, amb $b_i \in \mathbb{R}^n$, els elements de B^* es calculen fent

$$b_1^* = b_1, \quad b_i^* = b_i - \sum_{j < i} \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^* = b_i - \sum_{j < i} \mu_{i,j} b_j^*, \quad i \geq 2. \quad (1)$$

El procés el podem interpretar com la descomposició de la matriu B en forma $B = B^* \cdot M$, on M és la matriu triangular superior tal que $\text{diag}(M) = \{1, \dots, 1\}$ i $m_{i,j} = \mu_{j,i}$ per a $j < i$. Com que $B^* T B^* = D^2$, on D és la matriu diagonal amb entrades $\|b_i^*\|$ per a $i \in \{1, \dots, n\}$, s'obté també la descomposició de B^* com $B^* = QD$, amb Q matriu ortogonal.

PROPOSICIÓ 8 ([15, lema 2.1]). *Per a tot reticle $\Lambda = \Lambda(B)$ de rang màxim tenim la igualtat $\det(\Lambda) = \prod_i \|b_i^*\|$.*

Considerem ara, per a cada i , l'aplicació $\pi_i: \mathbb{R}^n \rightarrow \text{span}(b_1, \dots, b_{i-1})^\perp$ definida com

$$\pi_i(v) = \sum_{j=i}^n \frac{\langle v, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*.$$

Observem que $\pi_1(b_1), \pi_2(b_2), \dots, \pi_n(b_n)$ són els vectors ortogonals entre si, obtinguts mitjançant el procediment de Gram-Schmidt (1), de $\{b_1, \dots, b_n\}$.

2.4 Forma normal d'Hermite

De la mateixa manera que el procés de Gram-Schmidt genera bases que es fan servir com a claus privades en alguns algorismes de xifratge, la forma normal d'Hermite té un paper rellevant en aquests algorismes degut a la seva importància a l'hora de crear les claus públiques [11].

Una matriu $B \in M_{m \times n}(\mathbb{R})$ està en forma normal d'Hermite (escriurem HNF) si, i només si, per a tot $1 \leq i, j \leq m$ tenim

$$\begin{cases} b_{i,j} = 0 & \text{si } i < j, \\ b_{i,j} \geq 0 & \text{si } i \geq j, \\ b_{i,j} \leq b_{j,j} & \text{si } i > j. \end{cases}$$

Els resultats següents són estàndard (vegeu [11]):

LEMA 9. *Per a tota matriu B i tota matriu unimodular U existeix una matriu H en HNF tal que $H = BU$.*

LEMA 10. *Si dues matrius H_1 i H_2 estan en HNF i són equivalents, aleshores $H_1 = H_2$.*

2.5 Reticle dual

Donat un reticle $\Lambda(B)$ generat per una base $B = \{b_1, \dots, b_m\}$ amb $b_i \in \mathbb{R}^n$, el *reticle dual* associat és el conjunt

$$\widehat{\Lambda(B)} := \{y \in \text{span}(B) \mid \langle x, y \rangle \in \mathbb{Z}, \forall x \in \Lambda(B)\}.$$

Mantenint les notacions, la *base dual* de B és el conjunt $D = \{d_1, \dots, d_m\} \subseteq \mathbb{R}^n$ tal que:

- (1) $\text{span}(B) = \text{span}(D)$ i
- (2) $B^T D = \text{Id}_m$.

Utilitzant (1) i (2), tenim que $D = B \cdot (B^T B)^{-1}$.

El resultat següent dona al reticle dual, tal com indica el seu nom, l'estructura de reticle:

PROPOSICIÓ 11 ([16, afirmació 11]). *Si D és la base dual de B , aleshores tenim $\widehat{\Lambda(B)} = \Lambda(D)$.*

A continuació presentem una afirmació habitual en espais vectorials duals:

LEMA 12 ([16, afirmació 2]). *El doble dual d'un reticle és el reticle original: $\widehat{\widehat{\Lambda(B)}} = \Lambda(B)$.*

LEMA 13 ([11, proposició 6]). *Per a tot reticle de rang màxim tenim la igualtat $\det(\widehat{\Lambda(B)}) = (\det(\Lambda(D)))^{-1}$.*

La relació existent entre la base dual i el procés de Gram-Schmidt és estreta i s'estableix mitjançant els resultats següents, el primer dels quals prova que el procés d'ortogonalització no afecta la dualitat:

PROPOSICIÓ 14 ([11, proposició 12]). *Si considerem dues bases $B = \{b_1, \dots, b_n\}$ i $D = \{d_1, \dots, d_n\}$ duals, les bases $B' = \{\pi_i(b_i), \dots, \pi_i(b_n)\}$ i $D' = \{d_i, \dots, d_n\}$ també són duals, per a tot $i \in \{1, \dots, n\}$.*

PROPOSICIÓ 15 ([16, afirmació 7]). *Considerem $B = \{b_1, \dots, b_n\}$ una base i la seva base ortogonal, obtinguda mitjançant el procediment de Gram-Schmidt, $B^* = \{b_1^*, \dots, b_n^*\}$. Considerem també la base dual $D = \{d_1, \dots, d_n\}$ de B i la seva base ortogonal, obtinguda mitjançant el procediment de Gram-Schmidt, $D^* = \{d_1^*, \dots, d_n^*\}$. Aleshores, per a tot $i \in \{1, \dots, n\}$ es compleix $d_i^* = \frac{b_i^*}{\|b_i^*\|^2}$.*

2.6 Reticles q -aris

Els reticles q -aris tenen un paper important en criptografia basada en reticles ja que permeten relaxar les hipòtesis sobre els reticles sense perdre propietats relatives a la seguretat. Els sistemes que recolzen sobre aquesta mena de reticle tenen una complexitat computacional similar a la de problemes com el SIS o LWE [13], dels quals se sap que són tan complexos com els problemes més complexos en teoria de reticles.

Donat un enter q , un reticle Λ s'anomena q -ari si existeix $q \in \mathbb{Z}$ tal que $q \cdot \mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$, és a dir, Λ defineix un subgrup del grup additiu $\mathbb{Z}_q^n$.

LEMA 16 ([11, teorema 3]). *Si $B \in M_{n \times n}(\mathbb{Z})$ és una matriu no singular, aleshores $\det(\Lambda(B)) \cdot \mathbb{Z}^n \subseteq \Lambda(B)$.*

Donat un enter q , dos naturals $m < n$ i una matriu $A \in M_{n \times m}(\mathbb{Z})$ de rang màxim per columnes, considerem els reticles q -aris

- $\Lambda_q(A) = \{x \in \mathbb{Z}^n \mid x \equiv Ay \pmod{q} \text{ per a un cert } y \in \mathbb{Z}^m\} = A \cdot \mathbb{Z}^m + q\mathbb{Z}^n = \Lambda(A) + q\mathbb{Z}^n$.
- $\Lambda_q^\perp(A) = \{x \in \mathbb{Z}^n \mid A^T x = 0 \pmod{q}\}$.

LEMA 17 ([12, proposició 9]). *Amb les notacions anteriors tenim:*

$$(1) \quad q \cdot \widehat{\Lambda_q^\perp(A)} = \Lambda_q(A).$$

$$(2) \quad q \cdot \widehat{\Lambda_q(A)} = \Lambda_q^\perp(A).$$

PROVA. Només demostrarem el punt (1). La prova del punt (2) és anàloga:

$$\begin{aligned} \Lambda_q^\perp(A) &= \{y \in \mathbb{Z}^m \mid Ay \equiv 0 \pmod{q}\} = \{y \in \mathbb{Z}^m \mid A^T Ay = A^T qx, x \in \mathbb{Z}^n\} = \\ &= \{y \in \mathbb{Z}^m \mid y = (A^T A)^{-1} A^T qx, x \in \mathbb{Z}^n\}. \end{aligned}$$

De manera que la base de $\Lambda_q^\perp(A)$ és $(A^T A)^{-1} A^T q$, per tant, la base per a $q \cdot \Lambda_q^\perp(A)$ és $(A^T A)^{-1} A^T$. Si $(A^T A)^{-1} A^T$ és la base de $q \cdot \Lambda_q^\perp(A)$, la seva dual serà:

$$(A^T A)^{-1} A^T ((A^T A)^{-1} A^T)^T (A^T A)^{-1} A^T = \dots = A^T,$$

que és la base de $\Lambda_q(A)$. □

2.7 Mínims successius

Considerem, donat un reticle Λ , la longitud del vector no nul més curt de Λ , i denotem-la per $\lambda_1(\Lambda)$:

$$\lambda_1(\Lambda) := \min_{v \in \Lambda - \{0\}} \|v\| = \min_{x \neq y \in \Lambda} \|x - y\|.$$

Observem que $\lambda_1(\Lambda)$ és el paràmetre r més petit tal que els punts de Λ que pertanyen a una bola tancada de radi r generen un espai vectorial de dimensió 1. Podem generalitzar aquest concepte i introduir el concepte de mínims successius. Donat un reticle Λ de rang n , definim el i -èsim mínim successiu com:

$$\lambda_i(\Lambda) := \inf\{r \in \mathbb{R} \mid \dim(\text{span}(\Lambda \cap \overline{B}_r(0))) \geq i\}, \quad i \in \{1, \dots, n\}.$$

Les proposicions següents ens permetran fitar $\lambda_1(\Lambda)$, tant superiorment com inferior. La primera de les proposicions estableix una fita inferior:

PROPOSICIÓ 18 ([16, teorema 5]). *Per a qualsevol base B i la seva ortogonal per Gram-Schmidt associada B^* tenim $\lambda_1(\Lambda) \geq \min_{i \in \{1, \dots, n\}} \|b_i^*\|$.*

PROPOSICIÓ 19 (BLICHFELD, [11, teorema 5]). *Donats un conjunt $S \subseteq \mathbb{R}^n$ i un reticle $\Lambda(B)$ de rang màxim tals que $\text{vol}(S) > \det(\Lambda)$, existeix un parell de punts $z_1, z_2 \in S$ tal que $z_1 - z_2 \in \Lambda$.*

PROPOSICIÓ 20 (COS CONVEX DE MINKOWSKI, [16, teorema 9]). *Mantenint les notacions de la proposició anterior, si $S \subseteq \mathbb{R}^n$ és un subconjunt simètric (i. e. $x \in S \Rightarrow -x \in S$), convex tal que $\text{vol}(S) > 2^n \det(\Lambda)$, aleshores $\exists x \neq 0$ tal que $x \in S \cap \Lambda(B)$.*

El resultat anterior ens assegura l'existència d'un punt de Λ dintre d'un conjunt convex i simètric S , sempre que S sigui prou gran. Com a corollari de les dues proposicions anteriors obtenim aquesta fita superior per a $\lambda_1(\Lambda)$:

PROPOSICIÓ 21 ([16, corollari 2]). *Per a qualsevol reticle $\Lambda(B)$ de rang màxim n tenim $\lambda_1(\Lambda) \leq \sqrt[n]{n \det(\Lambda)}$.*

2.8 Problemes en teoria de reticles

Els problemes en teoria de reticles poden dividir-se principalment en dos blocs: els problemes resolubles de forma eficient i aquells que són computacionalment complexos. Començarem descrivint breument els problemes que són resolubles de forma eficient per encarregar-nos després d'estudiar amb més detall els problemes computacionalment complexos, que són font de propostes criptogràfiques postquàntiques.

2.8.1 Problemes resolubles eficientment

1. El problema de la base: a partir d'un conjunt de vectors B , determinar un subconjunt que generi una base B' per a Λ . Aquest és un problema que es pot resoldre, en temps polinòmic, calculant $\text{HNF}(B)$.
2. El problema de les bases equivalents: donades dues bases reticulars B i B' , determinar si són equivalents. Aquest problema es pot resoldre, en temps polinòmic, calculant $H = \text{HNF}(B)$, $H' = \text{HNF}(B')$ i comprovant si $H = H'$.
3. El problema de la unió: donades dues bases reticulars B i B' , determinar una base per al reticle més petit que contingui tant $\Lambda(B)$ com $\Lambda(B')$. El reticle mínim és generat per $B'' := B \cup B'$, de manera que podem determinar una base si calculem $\text{HNF}(B'')$.
4. El problema de la subbase: donades dues bases reticulars B i B' , determinar si $\Lambda(B') \subseteq \Lambda(B)$. Aquest problema es pot reduir als problemes de la unió i de les bases equivalents; en efecte: $\Lambda(B') \subseteq \Lambda(B)$ si, i només si, $\Lambda(B \cup B') = \Lambda(B)$. Si volem comprovar la inclusió, només cal calcular $\text{HNF}(B \cup B')$, $\text{HNF}(B)$ i comprovar si les formes coincideixen.
5. Pertinença a un reticle: donat $v \in \mathbb{Z}^n$, determinar si $v \in \Lambda(B)$. Aquest problema pot reduir-se al problema de la subbase tot comprovant si $\Lambda(v) \subseteq \Lambda(B)$. El problema es pot resoldre per a un conjunt de vectors $\{v_1, \dots, v_k\}$ tot calculant $\text{HNF}(B)$, calculant després, per a cada $i \in \{1, 2, \dots, k\}$, $\text{HNF}(B \cup v_i)$, i comprovant si $\text{HNF}(B) = \text{HNF}(B \cup v_i)$.
6. El problema del nucli: donada una base $A \in M_{n \times m}(\mathbb{Z})$, determinar una base que generi $\Lambda(A)$ a partir de $\ker(A)$. Aquest problema es redueix al problema de la base un cop determinat un conjunt generador de $\ker(A)$. Observem que el mateix procediment resol el problema següent.
7. El problema del nucli modular: donats una matriu $A \in M_{n \times m}(\mathbb{Z})$ i $q \in \mathbb{Z}$, determinar una base que generi el reticle $\Lambda_q^\perp(A)$.

2.8.2 Problemes computacionalment complexos Entre els problemes que són computacionalment complexos destaquen:

1. Vector més curt: en el problema del vector més curt (escriurem SVP) es vol determinar, per a una base B i un reticle $\Lambda(B)$, el vector no trivial més curt de Λ . Aquest problema té dues versions:
 - La versió exacta, en què es pretén resoldre alguna de les preguntes següents:
 - Decisió: per a $0 < d \in \mathbb{R}$, decidir si $\lambda_1(\Lambda(B)) \leq d$ o bé si $\lambda_1(\Lambda(B)) > d$.
 - Càlcul: determinar $\lambda_1(\Lambda(B))$.
 - Cerca: trobar $v \in \Lambda(B) - \{0\}$ tal que $\|v\| = \lambda_1(\Lambda(B))$.

- La versió aproximada (escriurem SVP_γ), en la qual tenim una funció real $\gamma = \gamma(\dim(\Lambda)) \geq 1$, en què es pretén resoldre alguna de les preguntes següents:
 - Decisió: per a $0 < d \in \mathbb{R}$, decidir si $\lambda_1(\Lambda(B)) \leq d$ o bé si $\lambda_1(\Lambda(B)) > \gamma \cdot d$.
 - Estimació: trobar $d \in [\lambda_1(\Lambda(B)), \gamma \cdot \lambda_1(\Lambda(B))]$.
 - Cerca: trobar $v \in \Lambda(B) - \{0\}$ tal que $\|v\| = \gamma \cdot \lambda_1(\Lambda(B))$.
- 2. Vector més proper: en el problema del vector més proper (escriurem CVP) volem trobar, per a una base B , un reticle $\Lambda(B)$ i un vector $w \in \mathbb{R}^n$, el vector $v \in \Lambda(B)$ més proper a w . Com en el cas anterior, aquest problema admet dues versions:
 - La versió exacta, en la qual es pretén resoldre alguna de les preguntes següents:
 - Decisió: donat un nombre real $r \in \mathbb{R}$, decidir si $\text{dist}(w, \Lambda(B)) \leq r$ o bé si $\text{dist}(w, \Lambda(B)) > r$, on $\text{dist}(w, \Lambda(B)) = \min_{v \in \Lambda(B)} \|w - v\|$.
 - Càlcul: trobar $r \in \mathbb{R}$ tal que $r = \text{dist}(w, \Lambda(B))$.
 - Cerca: trobar $v \in \Lambda(B)$ tal que $\text{dist}(w, v) \leq \text{dist}(w, \Lambda(B))$.
 - La versió aproximada (escriurem CVP_γ), en la qual tenim una funció real $\gamma = \gamma(\dim(\Lambda)) \geq 1$, en què es pretén resoldre alguna de les preguntes següents:
 - Decisió: donat un nombre real $r \in \mathbb{R}$, decidir si $\text{dist}(w, \Lambda(B)) \leq r$ o bé si $\text{dist}(w, \Lambda(B)) > \gamma \cdot r$.
 - Càlcul: trobar $r \in \mathbb{R}$ tal que $r \in [\text{dist}(w, \Lambda(B)), \gamma \cdot \text{dist}(w, \Lambda(B))]$.
 - Cerca: trobar $v \in \Lambda(B)$ tal que $\text{dist}(w, v) \leq \gamma \cdot \text{dist}(w, \Lambda(B))$.
- 3. Enters petits: en el problema de la solució mitjançant enters petits (escriurem SIS) considerem un enter $q \in \mathbb{Z}$, una matriu $A \in M_{n \times m}(\mathbb{Z}_q)$ i $\beta \in \mathbb{R}$ amb l'objectiu de trobar un vector $z \in \mathbb{Z}^m - \{0\}$ tal que $Az \equiv 0 \pmod{q}$ amb $\|z\| \leq \beta$.

El lema següent garanteix, sota certes condicions, l'existència de solucions per al problema SIS.

LEMA 22 ([12, lema 5.2]). *Per a tot $q \in \mathbb{Z}$, $A \in M_{n \times m}(\mathbb{Z}_q)$ i $\beta \geq \sqrt{m} \sqrt[n]{q^n}$ existeix $z \in \mathbb{Z}^m - \{0\}$ tal que $\|z\| \leq \beta$ i $Az \equiv 0 \pmod{q}$.*

El problema SIS admet una variant anomenada *no homogènia* (escriurem ISIS) en la qual, donats $q \in \mathbb{Q}$, una matriu $A \in M_{n \times m}(\mathbb{Z}_q)$, $\beta \in \mathbb{R}$ i $u \in \mathbb{Z}_q^n$ es vol trobar $z \in \mathbb{Z}_q^m$ tal que $Az \equiv u \pmod{q}$ i $\|z\| \leq \beta$.

2.8.3 Relació entre SVP i CVP El problema CVP pot interpretar-se com una versió no homogènia del problema SVP ja que, mentre que en el problema SVP busquem un punt del reticle proper a l'origen, en el problema CVP busquem un punt del reticle proper a un punt arbitrari.

La diferència principal entre SVP i CVP la trobem en el fet que, mentre que la solució del SVP no pot ser el vector nul, el CVP sí que l'admet. Aquest fet fa que puguem fer servir el problema CVP per trobar el vector més proper al vector 0 per tal de resoldre el problema SVP.

El problema SVP pot reduir-se al problema CVP. Aquest procés es fonamenta en els resultats següents. Considerem un reticle $\Lambda(B)$, de rang màxim, generat per una base $B = \{b_1, \dots, b_n\}$:

LEMA 23 ([9, proposició 3]). *Considerem $0 \neq v = \sum_{i=1}^n c_i b_i$ un vector més curt d'un reticle $\Lambda(B)$. Existeix un índex $i \in \{1, \dots, n\}$ tal que c_i és senar.*

Considerem un índex $j \in \{1, \dots, n\}$ i definim les bases per a $\Lambda(B)$ següents: $B^{(j)} := \{b_1, \dots, b_{j-1}, 2b_j, b_{j+1}, \dots, b_n\}$. Aleshores tenim:

PROPOSICIÓ 24 ([9, proposició 4]). *Considerem $v = \sum_{i=1}^n c_i b_i$ un vector de $\Lambda(B)$ per al qual existeix $j \in \{1, \dots, n\}$ tal que c_j és senar. Aleshores el vector $u := \frac{c_j+1}{2} 2b_j + \sum_{i \neq j} c_i b_i = 2c'_j b_j + \sum_{i \neq j} c_i b_i$ és un vector de $\Lambda(B^{(j)})$ tal que $\text{dist}(u, b_j) = \|v\|$.*

PROPOSICIÓ 25 ([9, proposició 5]). *Considerem $u = 2c'_j b_j + \sum_{i \neq j} c_i b_i$ un vector de $\Lambda(B^{(j)})$. Aleshores $v = (2c'_j - 1)b_j + \sum_{i \neq j} c_i b_i$ és un vector no nul de $\Lambda(B)$ tal que $\text{dist}(u, b_j) = \|v\|$.*

Observem que el lema 23, juntament amb la proposició 24, ens permet deduir l'existència, per a cada $j \in \{1, \dots, n\}$, d'un vector de $\Lambda(B^{(j)})$ tal que la distància amb el vector objectiu b_j coincideix amb la norma d'un vector més curt de $\Lambda(B)$. Finalment, fent servir la proposició 25, es pot determinar un vector de $\Lambda(B)$ tal que la distància amb el vector objectiu coincideix amb la norma d'un vector més curt de $\Lambda(B)$. Formalment, tenim:

TEOREMA 26 ([9, teorema 6]). *Donat $y = y(n) \in \mathbb{R}$, el problema SVP_y pot reduir-se al problema CVP_y .*

2.9 L'algorisme Lenstra-Lenstra-Lóvasz

Considerem $B = \{b_1, \dots, b_m\} \subset \mathbb{R}^n$ una base i $B^* = \{b_1^*, \dots, b_m^*\}$ la seva base associada obtinguda amb el procediment de Gram-Schmidt. Direm que B és δ -LLL reduïda, per a $\frac{1}{4} < \delta < 1$, si satisfà les condicions següents:

1. Condició de mida: $\forall 1 \leq i \leq n$ i $j < i$: $|\mu_{i,j}| \leq \frac{1}{2}$, on $\mu_{i,j}$ són els coeficients involucrats en el procediment de Gram-Schmidt.
2. Condició de Lóvasz: $\forall 1 \leq i < n$: $\delta \|b_i^*\|^2 \leq \|\mu_{i+1,i} b_i^* + b_{i+1}^*\|^2$.

L'algorisme Lenstra-Lenstra-Lóvasz (LLL) és un algorisme de reducció que retorna, donada una base, una base constituïda per vectors curts que satisfan la condició de Lóvasz. Pot entendre's com una versió vectorial de l'algorisme d'Euclides per al càlcul del màxim comú divisor. El funcionament essencial de

l'algorisme LLL es fonamenta en el procediment de Gram-Schmidt (vegeu la secció 6.12 de [10]).

TEOREMA 27 ([10, teorema 6.68]). *Sigui $\{v_1, \dots, v_n\}$ una base per a un reticle Λ . L'algorisme LLL ([10, figura 6.7]) acaba en un nombre finit de passos i retorna una base δ -LLL reduïda per a Λ . En particular, l'algorisme LLL és un algorisme polinòmic.*

Tot i que l'aplicació original de l'algorisme era la factorització de polinomis sobre $\mathbb{Q}$, les aplicacions més destacables de l'algorisme LLL també inclouen la criptoanàlisi dels sistemes criptogràfics basats en reticles ja que l'algorisme LLL resol la versió exacta del problema SVP en temps $2^{O(n^2)}$ [1] i també té un paper important en la resolució de la versió aproximada del problema CVP en temps d'ordre $2^{O(n)}$ (vegeu [10, teorema 6.73] per a una referència).

3 Codis

3.1 Conceptes bàsics

Un *missatge* és una seqüència finita d'elements d'un cos finit $\mathbb{F}_q$ d'ordre q , per a $q = p^r$ on p és un nombre primer i $r \in \mathbb{N}$. Un *codi* C de longitud n és un conjunt $C \subset \mathbb{F}_q^n$. Si C només té un element, direm que C és un codi trivial. Si prenem $q = 2$ parlarem de codis binaris. Els elements $c \in C$ s'anomenen *paraules codi*.

El procés de codificació d'un missatge es pot interpretar com una aplicació injectiva, que anomenem *codificador*, $f: \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$, per a $n > k > 0$. Un codi de longitud n és la imatge $f(\mathbb{F}_q^k) := C \subset \mathbb{F}_q^n$. Un codificador té associada una funció injectiva $g: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^k$ tal que $g \circ f = \text{Id}$,¹ que anomenarem *descodificador*.

EXEMPLE. Per tal de motivar els propers conceptes ens centrarem en una situació en què volem codificar un missatge $a \in \mathbb{F}_q^k$ mitjançant un codificador $f: \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$. El resultat és un element $f(a) \in C$, que és enviat a través d'un canal. El codi arriba al descodificador associat g , que retorna un missatge amb la forma $g(b) \in \mathbb{F}_q^k$. Sigui $q = 2$, $k = 1$, $n = 3$ i $C = \{(0, 0, 0), (1, 1, 1)\} \subset \mathbb{F}_2^3$. Suposem que el missatge «No» es correspon amb 0 i que es codifica com $f(0) = (0, 0, 0)$. Suposem que un missatge «Sí» es correspon amb 1 i que es codifica com $f(1) = (1, 1, 1)$. Enviem un «No» a través d'un canal que genera interferències tals que el descodificador rep el codi $(0, 1, 0)$. És raonable pensar que el descodificador retorni el missatge «No» ja que l'element $(0, 1, 0) \in \mathbb{F}_2^3$ és més semblant a $(0, 0, 0)$ que no pas a $(1, 1, 1)$ ja que $(0, 1, 0)$ i $(0, 0, 0)$ només difereixen en una component, mentre que $(0, 1, 0)$ i $(1, 1, 1)$ difereixen en dues. En aquest cas direm que el codi ha corregit un error.

¹ Observem que la composició és la identitat amb una certa probabilitat que depèn de la longitud de la *paraula codi* ([24, secció 2.1]).

Considerem $x \in \{x_1, \dots, x_n\} \in \mathbb{F}_q^n$. El pes $w(x)$ és el nombre de components no nul·les de x . En l'exemple anterior $w(f(0)) = 0$, $w(f(1)) = (1, 1, 1) = 3$, $w((0, 1, 0)) = 1$.

Donats dos elements $x, y \in \mathbb{F}_q^n$, la *distància de Hamming* és

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

EXEMPLE. Per a $x = (1, 1, 1)$ i $y = (0, 1, 0)$ tenim $d(x, y) = w(1, 0, 1) = 2$.

Si C és un codi no trivial, la distància mínima de C és $\min_{x \neq y \in C} d(x, y)$; el pes mínim és $\min_{x \in C - \{0\}} w(x)$.

Un (n, m, d) -codi és un codi amb longitud n , m paraules codi i distància mínima d . El codi C de l'exemple és un $(3, 2, 3)$ -codi.

El radi de cobriment d'un codi C és $\rho(C) = \max_{x \in \mathbb{F}_q^n} \min_{c \in C} d(x, c)$. Observem que el concepte formalitza la idea de com d'allunyat està un element rebut $x \in \mathbb{F}_q^n$ de la *paraula codi* més propera.

Donat un codi $C \subset \mathbb{F}_q^n$ de longitud n , el *codi estès* associat és

$$\overline{C} := \left\{ (c_1, \dots, c_{n+1}) \mid (c_1, \dots, c_n) \in C, c_{n+1} = \sum_{i=1}^n c_i \right\}.$$

Un *codi lineal* és un subespai vectorial de $\mathbb{F}_q^n$. Una forma alternativa de definir-lo és mitjançant successions exactes, la qual cosa ens conduirà a alguns conceptes fonamentals. En efecte, considerem la successió exacta curta:

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{A} \mathbb{F}_q^n \xrightarrow{B} \mathbb{F}_q^{n-k} \longrightarrow 0.$$

Per ser exacta, tenim $rk(A) = k$, $rk(B) = n - k$ i $B \circ A = 0$. D'una altra banda:

1. Definim $C := A(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$. L'aplicació lineal A es descriu amb una matriu de mida $n \times k$. Les seves columnes formen una base de C . La matriu A^T s'anomena *matriu generatriu*.
2. Per ser una successió exacta, $C = \ker(B)$, per tant, $x \in C \Leftrightarrow Bx = 0$. L'aplicació B es defineix amb una matriu de mida $(n - k) \times n$, les files de la qual són les relacions que defineixen C . La matriu B rep el nom de *matriu de paritat* o *de control*. Donat un element $x \in \mathbb{F}_q^n$, la *síndrome* de x és $Bx \in \mathbb{F}_q^{n-k}$.

Com que els espais són tots de dimensió finita, la successió anterior indueix una successió curta dual

$$0 \longrightarrow \mathbb{F}_q^{n-k} \xrightarrow{B^T} \mathbb{F}_q^n \xrightarrow{A^T} \mathbb{F}_q^k \longrightarrow 0.$$

Aquesta successió, de forma anàloga, ens permet definir un codi $\hat{C} := B^T(\mathbb{F}_q^{n-k})$ anomenat *codi dual* o *codi ortogonal* de C . Si $\dim(C) = k \Rightarrow \dim(\hat{C}) = n - k$.

Si definim, donats $x, y \in \mathbb{F}_q^n$, $x \cdot y := \sum_i x_i y_i$, obtenim la següent caracterització de $\hat{C}$:

LEMA 28 ([7, lema 1.1]). *Es compleix $\hat{C} = \{\gamma \in \mathbb{F}_q^n \mid x \cdot \gamma = 0, \forall x \in C\}$.*

Un codi binari C és *parell* si el pes $w(x)$ és divisible entre 2 per a tot $x \in C$; s'anomena *doblement parell* si el pes $w(x)$ és divisible entre 4.

El grup simètric Σ_n actua sobre $\mathbb{F}_q^n$ mitjançant permutacions de coordenades. Dos codis C, C' sobre $\mathbb{F}_q^n$ són *equivalents* si $\exists \sigma \in \Sigma_n$ tal que $\sigma(C) = C'$.

3.2 Codis cíclics

La importància dels codis cíclics en criptografia postquàntica rau en el fet que les seves propietats els fan particularment útils a l'hora de dur a terme implementacions i calcular síndromes.

Un codi lineal C de longitud n s'anomena *cíclic* si per a qualsevol paraula codi $c = (c_0, \dots, c_{n-1}) \in C$, $c' = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$. Podem identificar les paraules codi d'un codi cíclic amb cinc classes de polinomis de $\mathbb{F}_q^n[x]/(x^n - 1)$ mitjançant el següent isomorfisme:

$$\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n[x]/(x^n - 1), \quad (c_0, \dots, c_{n-1}) \longmapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

El resultat següent aporta una definició alternativa per al concepte de codi cíclic i en motiva el nom:

TEOREMA 29 ([24, teorema 6.1.3]). *Un codi lineal C de longitud n és cíclic si, i només si, és un ideal de $\mathbb{F}_q^n[x]/(x^n - 1)$.*

Si C és un codi cíclic, aleshores tenim que, com que és un ideal de $\mathbb{F}_q^n[x]/(x^n - 1)$: $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in C \Rightarrow x \cdot c(x) \in C$, ara bé:

$$x \cdot c(x) = c_{n-1} + c_0x + \dots + c_{n-2}x^{n-2}.$$

Per ser un ideal principal, existeix un polinomi mònic $g \in \mathbb{F}_q^n[x]/(x^n - 1)$ amb grau mínim que genera l'ideal. Aquest polinomi rep el nom de *polinomi generador*.

La descomposició en factors irreductibles de $x^n - 1 = f_1(x) \cdot \dots \cdot f_t(x)$ ens porta al concepte de *codi cíclic maximal*, que és un codi generat per $f_i(x)$ i que denotarem per M_i^+ , per a $i = 1, \dots, t$. Els codis generats per $\frac{x^n - 1}{f_i(x)}$ reben el nom de *codis cíclics minimal*s i els denotarem per M_i^- .

TEOREMA 30 ([24, teorema 6.4.1]). *Per a tot codi cíclic C existeix un element $c \in C$ únic, anomenat idempotent, que és el neutre del producte de C .*

TEOREMA 31 ([24, teorema 6.4.3]). *Si C_1, C_2 són codis cíclics amb idempotents c_1 i c_2 respectivament, aleshores:*

- (1) *El codi $C_1 \cap C_2$ té idempotent $c_1 \cdot c_2$.*
- (2) *El codi $C_1 + C_2$ té idempotent $c_1 + c_2 - c_1 \cdot c_2$.*

L'idempotent d'un codi minimal M_i^- s'anomena *idempotent primitiu* i el denotem per $\theta_i(x)$. El lema següent en dona una caracterització:

LEMA 32 ([24, teorema 6.4.4]). *Amb les notacions anteriors, els idempotents primitius satisfan:*

- (1) Si $i \neq j$, aleshores $\theta_i(x)\theta_j(x) = 0$.
- (2) $\sum_{i=1}^t \theta_i(x) = 1$.
- (3) L'idempotent generador del codi $f_{i_1}(x) \cdots f_{i_r}(x)$ és $1 + \theta_{i_1}(x) + \cdots + \theta_{i_r}(x)$.

3.3 Codis de Goppa i la seva descodificació

Sigui $L = \{y_0, y_1, \dots, y_{n-1}\} \subset \mathbb{F}_q$ tal que $g(y_i) \neq 0$ per a $0 \leq i \leq n-1$, essent $g(x)$ un polinomi mònic de grau t sobre $\mathbb{F}_q$. Un *codi de Goppa* $\Gamma(L, g)$, amb *polinomi de Goppa* associat $g(x) = \sum_{i=0}^t g_i x^i$, és el conjunt $(c_0, \dots, c_{n-1}) \in \mathbb{F}_p^n$ tals que $\sum_{i=0}^{n-1} \frac{c_i}{x-y_i} \equiv 0 \pmod{g(x)}$. Si fem $h_j := (g(y_j))^{-1}$, una matriu de paritat per a $\Gamma(L, g)$ és (vegeu [24]):

$$B = \begin{pmatrix} h_0 & h_1 & \dots & h_{n-1} \\ h_0 y_0 & h_1 y_1 & \dots & h_{n-1} y_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_0 y_0^{t-1} & h_1 y_1^{t-1} & \dots & h_{n-1} y_{n-1}^{t-1} \end{pmatrix}.$$

TEOREMA 33 ([24, teorema 9.2.7]). *Amb les notacions anteriors, un codi de Goppa $\Gamma(L, g)$ té distància mínima més gran o igual que $t+1$ i dimensió més gran o igual que $n - mt$.*

Considerem un codi de Goppa $\Gamma(L, g)$, una *paraula codi* $c = (c_0, c_1, \dots, c_{n-1}) \in \Gamma(L, g)$ i un missatge $r = (r_0, r_1, \dots, r_{n-1}) \in \mathbb{F}_p^n$. Sigui $e = r - c = (e_0, e_1, \dots, e_{n-1})$. Considerem $M := \{0 \leq i \leq n-1 \mid e_i \neq 0\}$. Suposem que $\deg(g(x)) = t$ i que $\#M = e \leq t/2$. Considerem un polinomi $S(x)$ tal que

$$\begin{cases} S(x) \equiv \sum_{i=0}^{n-1} \frac{e_i}{x-y_i} \pmod{q}, \\ \deg(S(x)) < t. \end{cases}$$

Definim el polinomi *localitzador d'errors* com $\sigma(x) := \prod_{i \in M} x - y_i$. Definim el *polinomi avaluador d'errors* com $\omega(x) := \sum_{i \in M} e_i \prod_{j \in M - \{i\}} (x - y_j)$.

Considerem el producte $S\sigma$:

$$S(x)\sigma(x) = \sum_{i=0}^{n-1} \frac{e_i}{x-y_i} \prod_{i \in M} x - y_i \equiv \sum_{i=0}^{n-1} e_i \prod_{j \in M - \{i\}} x - y_j \equiv \omega(x) \pmod{g(x)}.$$

Si assumim que tenim un algorisme capaç de calcular un polinomi mònic no nul $\sigma_1(x)$ i un polinomi $\omega_1(x)$ tals que $S(x)\sigma_1(x) \equiv \omega_1(x) \pmod{g(x)}$,

on $\sigma_1(x)$ té el grau més baix entre tots els polinomis mòncics no nuls que satisfan la congruència, i $\deg(\omega_1(x)) < \deg(\sigma_1(x))$, aleshores pot deduir-se

$$\omega_1(x)\sigma(x) - \omega(x)\sigma_1(x) \equiv 0 \pmod{g(x)}.$$

Observem que aquest polinomi té grau menor que el grau de $g(x)$, de manera que $\omega_1(x)\sigma(x) - \omega(x)\sigma_1(x) = 0$. Com que els polinomis σ , ω no tenen factors comuns, la igualtat implica $\sigma | \sigma_1$, d'on es dedueix $\sigma = \sigma_1$. Una vegada es coneixen σ i ω podem recuperar el vector e i descodificar la *paraula codi* c .

3.4 Relació entre codis i reticles

Considerem un reticle $\mathbb{Z}^n \subset \mathbb{R}^n$ i l'aplicació

$$\pi: \mathbb{Z}^n \longrightarrow \mathbb{F}_2^n, \quad (x_1, \dots, x_n) \longmapsto (\bar{x}_1, \dots, \bar{x}_n).$$

Considerem C un (n, k, d) -codi lineal de $\mathbb{F}_2^n$. Com que $\mathbb{F}_2^n / C \cong \mathbb{F}_2^{n-k}$, podem deduir que C és un subgrup de $\mathbb{F}_2^n$ amb cardinalitat 2^k . Per tant,

$$\pi^{-1}(C) = \{x + 2k \mid x \in C, k \in \mathbb{Z}\}$$

és un subgrup de $\mathbb{Z}^n$ d'índex 2^{n-k} . Tenim que $\pi^{-1}(C)$ és un reticle de $\mathbb{R}^n$ pel fet de ser un conjunt discret tancat per a la suma i la resta.

El reticle associat al codi C es defineix com $\Lambda_C = \frac{1}{\sqrt{2}}\pi^{-1}(C)$. Dos elements qualssevol de Λ_C tenen la forma

$$\begin{cases} x = \frac{1}{\sqrt{2}}(c + 2z), \\ y = \frac{1}{\sqrt{2}}(c' + 2z') \end{cases}$$

per a $c, c' \in \{0, 1\}^n$ i $z, z' \in \mathbb{Z}^n$. Cometem un abús de notació tot identificant $\mathbb{F}_2^n \leftrightarrow \{0, 1\}^n$ i escrivint $c, c' \in C$. Tenim

$$\begin{cases} x^2 = \frac{1}{2}(c^2 + 4cz + 4z^2), \\ x \cdot y = \frac{1}{2}(c \cdot c'). \end{cases}$$

És immediat deduir que per a tot $x, y \in \Lambda_C$ es compleix:

$$x \cdot y \in \mathbb{Z} \iff c \cdot c' \in 2\mathbb{Z}, \quad \forall c, c' \in C.$$

Per tant, Λ_C és un reticle integral (i.e. en el qual per a tot $x, y \in \Lambda_C$ es compleix $x \cdot y \in \mathbb{Z}$) si, i només si, $C \subset \hat{C}$. A més a més, $x^2 \in 2\mathbb{Z} \iff c^2 \in 4\mathbb{Z}$ per a tot $c \in C$, de manera que Λ_C és parell si, i només si, C és doblement parell. Finalment, si $k = n/2$, aleshores $\text{vol}(\mathbb{R}^n / \pi^{-1}(C)) = 2^{\frac{n}{2}} \iff \text{vol}(\mathbb{R}^n / \Lambda_C) = 1$, de manera que C és autodual (i.e. $C = \hat{C}$) si, i només si, Λ_C és autodual. Tot plegat prova el resultat següent:

PROPOSICIÓ 34 ([7, proposició 1.3]). *Per a un codi lineal C tenim:*

- (1) $C \subset \hat{C} \Leftrightarrow \Lambda_C$ és un reticle integral.
- (2) C és doblement parell si, i només si, Λ_C és parell.
- (3) C és autodual si, i només si, Λ_C és autodual.

3.5 Apunt final sobre problemes computacionalment complexos

A diferència del que passa amb la teoria de reticles i, com veurem tot seguit, amb la teoria d'isogènies de corbes el·líptiques supersingulares, la teoria de codis no té una llista de problemes computacionalment complexos. La seguretat dels algorismes que recolzen sobre la teoria de codis la fonamentem en el fet que tant el problema de la descodificació de codis lineals com el problema del càlcul de pesos de codis lineals són tots dos problemes NP-complets [2]. Cal destacar que, fins ara, no s'han presentat algorismes capaços de resoldre els problemes en un temps inferior a l'exponencial; no es coneixen encara algorismes quàntics que puguin fer-ho.

4 Isogènies de corbes el·líptiques supersingulares

Sigui $\mathbb{K}$ un cos, una *corba el·líptica* és un parell (E, O_E) , on E és una corba a $\mathbb{P}_{\mathbb{K}}^2$ no singular de gènere 1 i $O_E \in E$ és un punt distingit. Si $\mathbb{K}$ és tal que $\text{char}(\mathbb{K}) \neq 2, 3$, una corba el·líptica pot ser descrita² mitjançant l'equació de Wierstrass

$$E := \{(x : y : z) \in \mathbb{P}_{\mathbb{K}}^2 \mid y^2 z = x^3 + axz + bz^3\},$$

on $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$. Aquesta darrera condició és necessària per tal d'evitar singularitats. En aquest cas, $O_E = (0 : 1 : 0)$.

Si fem el canvi de variables $\frac{x}{z} \mapsto x$, $\frac{y}{z} \mapsto y$ obtenim la *forma afi*

$$E = \{(x, y) \in \mathbb{A}_{\mathbb{K}}^2 \mid y^2 = x^3 + ax + n\}.$$

Per a una corba el·líptica E , descrita per una equació de Weierstrass, es defineix el j -invariant com

$$j(E) = j(a, b) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

PROPOSICIÓ 35 ([22, proposició 1.4]). *Dues corbes el·líptiques E_1, E_2 són isomorfes en la clausura algebraica $\overline{\mathbb{K}}$ si, i només si, $j(E_1) = j(E_2)$.*

EXEMPLE. Donat un $j_0 \in \overline{\mathbb{K}} - \{0, 1728\}$, la corba el·líptica

$$E : y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0}$$

satisfà $j(E) = j_0$.

² Existeixen altres formes de descriure una corba el·líptica, com l'equació de Huff o la d'Edwards; vegeu [14] per a una referència.

Per tal de definir el concepte de morfisme entre corbes el·líptiques ens cal introduir alguns conceptes bàsics de caire tècnic.

Sigui C una corba projectiva plana donada per $f(x, y, z) = 0$ amb $f \in \mathbb{K}[x, y, z]$ irreductible sobre la clausura algebraica. El *cos de funcions* $\mathbb{K}(C)$ és el conjunt de funcions racionals $\frac{g}{h}$ tal que

- Els polinomis g, h són homogenis a $\mathbb{K}[x, y, z]$ i tenen el mateix grau.
- $f \nmid h$.
- $\frac{g_1}{h_1} \equiv \frac{g_2}{h_2} \Leftrightarrow f \mid (g_1 h_2 - g_2 h_1)$.

Donada una corba projectiva plana C , direm que una funció racional $f = \frac{g}{h}$, amb $g, h \in \mathbb{K}[x, y, z]$, és definida, o que és *regular*, en un punt $P \in C(\overline{K})$ si $h(P) \neq 0$.

Si C_1, C_2 són corbes projectives planes definides sobre $\mathbb{K}$, una aplicació racional $\phi: C_1 \rightarrow C_2$ és una terna $\phi = (\phi_x : \phi_y : \phi_z) \in \mathbb{P}_{\mathbb{K}(C_1)}^2$ tal que per a tot punt $P \in C_1(\mathbb{K})$ on ϕ és regular tenim $\phi(P) \in C_2(\mathbb{K})$.

Considerem un parell de corbes projectives planes C_1, C_2 . Una aplicació racional $\phi: C_1 \rightarrow C_2$ regular en tot $P \in C_1(\mathbb{K})$ s'anomena *morfisme entre C_1 i C_2* .

4.1 Conceptes fonamentals sobre isogènies

Donades dues corbes el·líptiques $(E_1, O_1), (E_2, O_2)$, una *isogènia* entre elles és un morfisme $\phi: E_1 \rightarrow E_2$ tal que $\phi(O_1) = O_2$. Dues corbes el·líptiques són *isògeniques* si existeix una isogènia entre elles.

LEMA 36 ([23, lema 5.21]). *Siguin E_1, E_2 corbes el·líptiques sobre $\mathbb{K}$. Una isogènia $\phi: E_1 \rightarrow E_2$ admet la representació*

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)} y \right),$$

on $p, q, s, t \in \mathbb{K}[x]$ són polinomis tals que p, q i s, t són primers entre ells dos a dos.

LEMA 37 ([8, lema 9.6.3]). *Si $\phi: E_1 \rightarrow E_2$ és una isogènia no nul·la entre E_1 i E_2 , corbes el·líptiques sobre $\mathbb{K}$, aleshores $\phi: E_1(\mathbb{K}) \rightarrow E_2(\mathbb{K})$ és una aplicació exhaustiva.*

El *grau* d'una isogènia $\phi: E_1 \rightarrow E_2$ és $\deg(\phi) := \max\{p(x), q(x)\}$. Si la isogènia és tal que $\frac{d}{dx} \frac{p(x)}{q(x)} \neq 0$ direm que ϕ és *separable*. Altrament direm que ϕ és *inseparable*.

EXEMPLE. Considerem un cos finit $\mathbb{F}_q$ d'ordre q . Donada una corba el·líptica E sobre $\mathbb{F}_q$, l'aplicació de Frobenius $\pi_E: E \rightarrow E, (x, y) \mapsto (x^q, y^q)$ és una isogènia de grau q .

Mantenint les notacions de l'exemple, la traça de l'aplicació de Frobenius es defineix com $\tau_E = q + 1 - \#E(\mathbb{F}_q)$. El polinomi característic de Frobenius associat a E és el polinomi $p_E(x) = x^2 - \tau_E x + q$.

El resultat següent aporta un criteri de molta utilitat a l'hora de determinar si dues corbes el·líptiques són isogèniques:

TEOREMA 38 (TEOREMA DE LA ISOGÈNIA DE TATE). *Amb les notacions anteriors, dues corbes el·líptiques E_1 i E_2 són isogèniques si, i només si, tenen el mateix polinomi característic de Frobenius. En particular, E_1 i E_2 són isogèniques si, i només si, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

El nucli d'una isogènia $\phi: (E_1, O_1) \rightarrow (E_2, O_2)$ és el conjunt

$$\ker(\phi) := \{P \in E_1(\overline{\mathbb{K}}) \mid \phi(P) = O_2\}.$$

La relació entre el nucli d'una isogènia i el seu grau és forta, com podem comprovar en el resultat següent:

PROPOSICIÓ 39 ([27, proposició 12.8]). *Si $\phi: E_1 \rightarrow E_2$ és una isogènia separable, aleshores $\deg(\phi) = \#\ker(\phi)$. Si és inseparable, aleshores $\deg(\phi) > \#\ker(\phi)$.*

PROPOSICIÓ 40 ([22, corollari 4.8]). *Si $\phi: E_1 \rightarrow E_2$ és una isogènia no nul·la entre corbes el·líptiques (E_1, O_1) , (E_2, O_2) , aleshores $\ker(\phi) = \phi^{-1}(O_2)$ és un subgrup finit de $E_1(\overline{\mathbb{K}})$.*

EXEMPLE. Considerem (E, O_E) una corba el·líptica i $n \in \mathbb{Z}$, aleshores l'aplicació $[n]: E \rightarrow E$, $P \mapsto [n]P = \underbrace{P + \dots + P}_{n \text{ vegades}}$ és una isogènia.

EXEMPLE. El *problema del logaritme discret sobre corbes el·líptiques* requereix trobar $n \in \mathbb{Z}$ tal que $Q = [n](P)$, donats dos punts P, Q en una corba el·líptica E . Aquest problema es pot reformular com el problema de trobar, donats P i Q de $E(\overline{\mathbb{K}})$, la isogènia $\phi: E \rightarrow E$ tal que $\phi(P) = Q$. L'algorisme de Shor resol el problema del logaritme discret amb un algorisme polinòmic en un ordinador quàntic.

El problema de la determinació d'isogènies entre corbes el·líptiques, del qual el logaritme discret és un exemple bàsic, té algorismes quàntics capaços de resoldre'l en temps subexponencials en el cas de corbes el·líptiques ordinàries [5]. En el cas de considerar corbes el·líptiques supersingulars, només existeix un algorisme quàntic capaç de resoldre el problema en temps exponencial [3].

Denotarem el conjunt d'isogènies entre dues corbes el·líptiques E_1, E_2 per $\text{Hom}(E_1, E_2) = \{\phi: E_1 \rightarrow E_2 \mid \phi \text{ és una isogènia}\}$. Per a $\phi, \psi \in \text{Hom}(E_1, E_2)$ i $P \in E_1(\overline{\mathbb{K}})$ definim $(\phi + \psi)(P) := \phi(P) + \psi(P)$. La suma d'isogènies dona a $\text{Hom}(E_1, E_2)$ estructura de grup.

Si a més definim el producte d'isogènies $\phi \cdot \psi$ com la composició $\phi \circ \psi$, podem dotar el conjunt $\text{End}(E) = \text{Hom}(E, E)$ d'endomorfismes amb estructura d'anell. Els elements amb invers multiplicatiu de $\text{End}(E)$ formen el grup d'automorfismes $\text{aut}(E)$.

Considerem les corbes el·líptiques E_1, E_2 i les isogènies $\phi: E_1 \rightarrow E_2$ i $\phi': E_2 \rightarrow E_1$. Direm que E_1 i E_2 són isomorfes si $\phi \circ \phi' = \text{Id}_{E_2}$ i $\phi' \circ \phi = \text{Id}_{E_1}$; ho denotarem per $E_1 \cong E_2$.

PROPOSICIÓ 41 ([22, proposició 4.2]). *Si E_1, E_2 són corbes el·líptiques, aleshores el grup d'isogènies $\text{Hom}(E_1, E_2)$ és un $\mathbb{Z}$ -mòdul lliure de torsió: donats $a \in \mathbb{Z}$ i $\phi \in \text{Hom}(E_1, E_2)$, aleshores $[a] \circ \phi = 0 \Rightarrow a = 0$ o bé $\phi = 0$.*

Els divisors de zero a $\text{End}(E)$ són isogènies no nul·les $\phi: E \rightarrow E$ tals que la seva composició amb una altra isogènia no nul·la $\psi: E \rightarrow E$ és 0.

PROPOSICIÓ 42 ([22, proposició 4.2]). *Donada una corba el·líptica E , $\text{End}(E)$ és un anell no necessàriament abelià i sense divisors de zero.*

PROPOSICIÓ 43 ([22, corollari 4.11]). *Considerem una isogènia $\phi: E_1 \rightarrow E_2$ no constant i separable i ψ una isogènia no constant. Aleshores $\ker(\phi) \subset \ker(\psi) \Rightarrow \exists! \lambda \in \text{Hom}(E_2, E_3) : \psi = \lambda \circ \phi$.*

TEOREMA 44. *Considerem $\phi \in \text{Hom}(E_1, E_2)$ una isogènia de grau m . Existeix una única isogènia $\hat{\phi} \in \text{Hom}(E_2, E_1)$, anomenada isogènia dual, tal que:*

- (1) $\hat{\phi} \circ \phi = [m]: E_1 \rightarrow E_1$ i $\phi \circ \hat{\phi} = [m]: E_2 \rightarrow E_2$.
- (2) $\forall \psi \in \text{Hom}(E_2, E_3), \widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ i $\widehat{\psi + \phi} = \hat{\phi} + \hat{\psi}$.
- (3) $\deg(\phi) = \deg(\hat{\phi})$.
- (4) $\hat{\hat{\phi}} = \phi$.

El següent resultat estableix un dels punts clau de la criptografia basada en isogènies: les isogènies factoritzen. A la pràctica aquest fet es tradueix en el fet que hom pot definir una isogènia de grau alt com una composició d'isogènies amb grau petit, la qual cosa fa que sigui més fàcil de manipular.

PROPOSICIÓ 45 ([23, corollari 6.18]). *Una isogènia separable $\phi: E \rightarrow E'$ descompon com la composició d'isogènies $\phi = \phi_0 \circ \phi_1 \circ \dots \circ \phi_n$ tals que $\phi_i: E_i \rightarrow E_{i+1}$ té grau primer per a tot $i \in \{0, \dots, n\}$, posant $E_0 \cong E$ i $E_{n+1} \cong E'$.*

4.2 Fórmules de Vélu

Com que tota isogènia $\phi \in \text{Hom}(E_1, E_2)$ té associat un nucli $\ker(\phi) = G$ que és un subgrup finit de $E_1(\overline{\mathbb{K}})$, és natural preguntar-se quan la isogènia ϕ queda determinada per G o bé quins subgrups finits de $E_1(\overline{\mathbb{K}})$ són el nucli d'una isogènia. La resposta la dona la proposició següent:

PROPOSICIÓ 46 ([8, teorema 9.6.19]). *Considerem una corba el·líptica E i un subgrup finit $G \subset E(\overline{\mathbb{K}})$. Aleshores existeix una única corba el·líptica E' i una isogènia separable $\phi: E \rightarrow E'$ tal que $\ker(\phi) = G$ i $E' \cong E/\langle G \rangle$.*

Les fórmules de Vélu són expressions que ens permetran construir isogènies a partir d'una corba el·líptica i un subgrup finit. Observem que si combinem el resultat següent amb el teorema anterior deduïm que una isogènia queda completament determinada pel seu nucli. Cal notar que sempre parlem d'isogènies separables.

PROPOSICIÓ 47 ([8, proposició 25.1.6]). *Considerem un subgrup finit $G \subset E(\mathbb{K})$ on E és una corba el·líptica sobre $\mathbb{K}$ donada per l'equació de Weierstrass. Una isogènia separable $\phi: E \rightarrow E'$ amb $\ker(\phi) = G$ es pot escriure com*

$$\phi(P) = \left(x_P + \sum_{Q \in G - \{O_E\}} x_{P+Q} - x_Q, y_P + \sum_{Q \in G - \{O_E\}} y_{P+Q} - y_Q \right),$$

amb $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ i $P + Q = (x_{P+Q}, y_{P+Q})$ i essent la corba $E': y^2 = x^3 + a'x + b'$ on

$$\begin{cases} a' = a - 5 \sum_{Q \in G - \{O_E\}} (3x_Q^2 + a), \\ b' = b - 7 \sum_{Q \in G - \{O_E\}} (5x_Q^3 + 2ax_Q + b). \end{cases}$$

4.3 Polinomis modulars

Els polinomis modulars són una forma alternativa per al càlcul de nuclis. Donat un enter $l > 2$, un polinomi modular és un polinomi $\Phi_l(x, y) \in \mathbb{K}[x, y]$ per al qual un parell $j_1, j_2 \in \mathbb{K}$ satisfà $\Phi_l(j_1, j_2) = 0$ si, i només si, existeixen corbes el·líptiques E_1, E_2 sobre $\mathbb{K}$ tals que $j(E_1) = j_1$, $j(E_2) = j_2$ i per a les quals existeix $\phi \in \text{Hom}(E_1, E_2)$ de grau l .

És immediat observar que, donada una corba el·líptica E , hom pot trobar j -invariants de corbes l -isogèniques³ trobant les arrels, a $\mathbb{K}$, del polinomi $\Phi_l(j(E), y) \in \mathbb{K}[y]$.

4.4 Corbes el·líptiques supersingulars

Un polinomi de divisió és un element $\psi \in \mathbb{K}[x, y, a, b, (2y)^{-1}]$, on a i b són els coeficients de l'equació de Weierstrass definida sobre $\mathbb{K}$. Els definim de forma recursiva:

- $\psi_1 = 1$.
- $\psi_2 = 2y$.
- $\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$.
- $\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$.
- Per a $m \geq 2$: $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$.
- Per a $m \geq 3$: $\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$.

³ Fem notar l'abús de llenguatge: les isogènies involucrades són de grau l .

TEOREMA 48 ([20, teorema 1.8]). Si $\text{char}(\mathbb{K}) \nmid m$, aleshores

$$[m](x, y) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x, y)} \right),$$

on $\phi_m := x\psi_m^2 - \psi_{m+1}\psi_{m-1}$ i $\omega_m := \psi_{m+2}\psi_{m-1}^2 + \psi_{m-2}\psi_{m+1}^2$.

Els punts $P \in E(\overline{\mathbb{K}})$ d'ordre m són aquells tals que $[m]P = O_E$. Formen un subgrup de $E(\overline{\mathbb{K}})$ amb la suma i el producte anomenat *subgrup de m -torsió*, que denotem per $E[m]$. El subgrup de torsió de E és el conjunt $E_{\text{tors}} = \bigcup_{m \geq 1} E[m]$.

La relació entre els polinomis de divisió i el subgrup de m -torsió queda determinada pel lema següent:

LEMA 49 ([20, corollari 1.10]). Donada una corba el·líptica E sobre un cos $\mathbb{K}$ tenim: si $\text{char}(\mathbb{K}) \nmid m$, aleshores un punt $P \in E(\overline{\mathbb{K}})$ és una arrel ψ_m si, i només si, $P \in E[m]$.

Pel que fa a l'estructura del subgrup de m -torsió, tenim:

LEMA 50. En les condicions del lema anterior, $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$.

El resultat següent aporta una primera caracterització de les corbes el·líptiques supersingulars:

TEOREMA 51 ([8, teorema 9.11.2]). Considerem una corba el·líptica (E, O_E) sobre un cos finit $\mathbb{F}_q$, amb $q = p^m$ i p primer. Les afirmacions següents són equivalents:

- (1) $\#E(\mathbb{F}_q) = q + 1 - \tau_E$ on $p \mid \tau_E$.
- (2) $E[p] = O_E$.
- (3) $\text{End}_{\overline{\mathbb{F}_q}}(E)$ té estructura d'anell no commutatiu.
- (4) El polinomi característic de Frobenius de E factoritza sobre $\mathbb{C}$ amb arrels α_1, α_2 tals que $\frac{\alpha_i}{\sqrt{q}}$ és una arrel de la unitat per a $i \in \{1, 2\}$.

Una corba que satisfà qualsevol dels punts anteriors rep el nom de *supersingular*. Altrament s'anomena *ordinària*.

OBSERVACIÓ. Una forma accessible de definir una corba el·líptica supersingular és com a corba tal que compleix qualsevol de les condicions següents:

1. $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$.
2. $\tau_E \equiv 0 \pmod{p}$.

Ambdues condicions es dedueixen immediatament del teorema anterior.

La condició d'ésser supersingular o ordinària és un invariant isogènic. En efecte:

PROPOSICIÓ 52 ([23, teorema 14.1]). Donada una isogènia $\phi: E_1 \rightarrow E_2$ entre corbes el·líptiques, E_1 és supersingular (resp. ordinària) si, i només si, E_2 és supersingular (resp. ordinària).

4.5 Relació entre reticles i corbes el·líptiques

Un *reticle complex* és un subconjunt discret i additiu $\Lambda \subseteq \mathbb{C}^n$. Considerem $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ l'anell d'enters gaussians. Donat un conjunt amb m vectors linealment independents de $\mathbb{C}^n$, $\{v_1, \dots, v_m\}$, un *reticle complex de rang m i dimensió n* és un conjunt generat per aquests vectors:

$$\Lambda(v_1, \dots, v_m) := \left\{ \sum_{i=1}^m c_i v_i \mid c_i \in R \right\}.$$

EXEMPLE. Donat un reticle complex Λ , l'espai quocient $\mathbb{T} = \mathbb{C}^n / \Lambda$ s'anomena *tor complex*.

Dos reticles complexos Λ_1, Λ_2 són homotètics si existeix $\alpha \in \mathbb{C} - \{0\}$ tal que $\Lambda_1 = \alpha \Lambda_2$.

Donat un reticle complex Λ , la sèrie d'Eisenstein amb pes $2k$ es defineix com $G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k}$. S'escriu $g_2(\Lambda) = 60G_4(\Lambda)$ i $g_3(\Lambda) = 140G_6(\Lambda)$. El j -invariant modular es defineix com $j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$.

TEOREMA 53 ([21, teorema 4.1]). *Dos reticles complexos són homotètics si, i només si, els j -invariants modulars associats coincideixen.*

El teorema anterior classifica els tors complexos tret d'homotècia ja que sempre podem associar un tor a un reticle. Estableix les condicions sota les quals dos reticles són homotètics, la qual cosa, en el cas dels tors, es tradueix a saber sota quines condicions dos tors són isomorfs.

Tant el j -invariant d'una corba el·líptica com el j -invariant modular d'un reticle són classificadors: en el primer cas classifiquen corbes tret d'isomorfisme, mentre que en el segon cas classifiquen reticles tret d'homotècia. El morfisme $\Lambda \rightarrow \mathbb{C}$, $g_2 \mapsto 4a^3$, $g_3 \mapsto b$ envia $j(\Lambda)$ a $j(E: y^2 = 4x^3 - g_2x - g_3)$. De manera que per a tota classe d'homotècia d'un tor complex tenim una classe d'isomorfia de corbes el·líptiques sobre $\mathbb{C}$. Recíprocament:

TEOREMA 54 (TEOREMA D'UNIFORMITZACIÓ, [21, corollari 4.3]). *Donat un parell $a, b \in \mathbb{C}$ tal que $4a^3 + 27b^2 \neq 0$ existeix un reticle complex Λ únic tal que $g_2(\Lambda) = -4a$ i $g_3(\Lambda) = -4b$.*

Observem que el teorema estableix un morfisme entre corbes el·líptiques i tors complexos de manera que, donada una classe d'isomorfia de corbes el·líptiques complexes, es té una classe d'homotècia de tors complexos. Aquest fet, amb l'observació anterior, defineix una bijecció entre classes d'isomorfia de corbes el·líptiques complexes i classes d'homotècia de tors complexos.

Considerem tot seguit dos reticles complexos Λ_1, Λ_2 per als quals existeix $\alpha \in \mathbb{C}$ tal que $\Lambda_1 \subset \alpha \Lambda_2$. Definim un morfisme $\phi_\alpha: \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$, $z \mapsto \alpha z \bmod \Lambda_2$. El resultat següent estableix que els morfismes de la forma ϕ_α es corresponen amb les isogènies entre les corbes el·líptiques associades:

TEOREMA 55 ([22, teorema 4.1]). *Si E_1, E_2 són corbes el·líptiques complexes i Λ_1, Λ_2 els reticles associats, aleshores existeix una bijecció entre $\text{Hom}(E_1, E_2)$ i el conjunt de morfismes ϕ_α , amb $\alpha \in \mathbb{C}$ tal que $\Lambda_1 \subset \alpha \Lambda_2$.*

4.6 Problemes computacionalment complexos

Els següents problemes són els principals candidats a problema computacionalment complex sobre el qual recolzar protocols criptogràfics.

1. Càlcul d'isogènies: considerant $p \neq l$ números primers i $n \in \mathbb{N}$, trobem les versions següents per al problema del càlcul d'isogènies.
 - Trobar un parell de corbes el·líptiques supersingulars E_1, E_2 sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 , i dues isogènies diferents $f_{1,2}: E_1 \rightarrow E_2$ de grau l^n .
 - Donada una corba el·líptica supersingular E sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 , trobar $f \in \text{End}(E)$ de grau l^{2n} tal que $f \neq [l^n]$.
 - Donades dues corbes el·líptiques supersingulars sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 , trobar una isogènia $f: E_1 \rightarrow E_2$ de grau l^n .
2. Càlcul d'ordres maximals: aquest problema presenta les variants següents.
 - Donat un número primer p , una base estàndard per a l'àlgebra de quaternions $B_{p,\infty}$, ramificada en p i ∞^4 i E , una corba el·líptica supersingular sobre un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 , trobar una base per a l'ordre maximal $\mathcal{O}$ de $B_{p,\infty}$ tal que $\text{End}(E) \cong \mathcal{O}$.
 - Donat un número primer p , una corba el·líptica supersingular E , un cos finit $\mathbb{F}_{p^2}$ d'ordre p^2 i quatre elements $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ en un ordre maximal $\mathcal{O}$ de $B_{p,\infty}$ tals que existeix un isomorfisme $\iota: \text{End}(E) \rightarrow \mathcal{O}$, trobar vuit parells de punts de E , $(P_1, Q_{1r}), (P_2, Q_{2r}), r \in \{1, 2, 3, 4\}$, tals que P_1, P_2 formen una base per a $E[l]$ i tals que $Q_{1r} = \iota^{-1}(\beta_r)(P_1)$ i $Q_{2r} = \iota^{-1}(\beta_r)(P_2)$ per a $r \in \{1, 2, 3, 4\}$.
3. Càlcul de l'anell d'endomorfismes: considerem un número primer p i $n > 0$. Per a una corba el·líptica supersingular E sobre un cos finit $\mathbb{F}_{p^n}$, d'ordre p^n , calcular l'anell d'endomorfismes $\text{End}(E)$.

4.6.1 La correspondència de Deuring Considerem H una $\mathbb{Q}$ -àlgebra finitament generada. Un ordre R de H és un subanell de H que és finitament generat com a $\mathbb{Z}$ -mòdul i tal que $H = R \otimes \mathbb{Q}$.

El resultat següent caracteritza l'anell d'endomorfismes:

TEOREMA 56 ([6, teorema 29]). *Donada una corba el·líptica E sobre un cos $\mathbb{F}$ amb característica p , l'anell d'endomorfismes de E és isomorf a:*

- (1) $\mathbb{Z}$ si $p = 0$, o bé
- (2) un ordre R en una extensió de la forma $\mathbb{Q}[\sqrt{d}]$, per a $d < 0$, o bé
- (3) un ordre maximal en l'àlgebra quaterniònica $B_{p,\infty}$ que ramifica en p i en ∞ .

4 Una referència per a àlgebres quaterniòniques és [26].

TEOREMA 57 (CORRESPONDÈNCIA DE DEURING, [4, teorema 2.1]). *Sigui p un nombre primer i un cos finit $\mathbb{F}_p$ de característica p . Per a tot $j_0 \in \overline{\mathbb{F}_p}$, sigui $E(j_0)$ una corba el·líptica en la classe d'isomorfisme de les corbes amb j -invariant j_0 . Per a tot $j_i \in \overline{\mathbb{F}_p}$ existeix una bijecció entre els ordres maximals de $B_{p,\infty}$ i $\text{End}_{\overline{\mathbb{F}_p}}(E(j_i))$.*

La correspondència de Deuring estableix un diccionari entre isogènies i ordres d'àlgebres quaterniòniques que permet una estratègia interessant per a l'estudi dels problemes relacionats amb la seguretat dels sistemes criptogràfics basats en isogènies. Aquesta estratègia es compon dels passos següents:

1. Traslladar un problema d'isogènies al seu equivalent en ordres;
2. resoldre el problema d'ordres;
3. traslladar la solució d'ordres al seu equivalent en isogènies.

Pel que fa al problema del càlcul de l'anell d'endomorfismes, existeixen dues maneres d'atacar-lo:

1. Determinar $\text{End}(E)$ explicitant les isogènies, la qual cosa no és recomanable ja que isogènies de grau alt requeriran molt d'espai computacional per a la seva descripció.
2. Fer servir la correspondència de Deuring per descriure $\text{End}(E)$ com un $\mathbb{Z}$ -mòdul en una àlgebra quaterniònica.

Agraïments

L'autor desitja agrair els comentaris realitzats pel revisor, que han fet millorar sensiblement aquest article.

Referències

- [1] AGGARWAL, D.; DADUSH, D.; REGEV, O.; STEPHENS-DAVIDOWITZ, N. «Solving the shortest vector problem in 2^n time via discrete Gaussian sampling (extended abstract)». A: *STOC'15—Proceedings of the 2015 ACM Symposium on Theory of Computing*. Nova York: ACM, 2015, 733–742.
- [2] BERLEKAMP, E. R.; MCELIECE, R. J.; VAN TILBORG, H. C. A. «On the inherent intractability of certain coding problems». *IEEE Trans. Information Theory*, IT-24 (3) (1978), 384–386.
- [3] BIASSE, J.-F.; JAO, D.; SANKAR, A. «A quantum algorithm for computing isogenies between supersingular elliptic curves». A: *Progress in cryptology—INDOCRYPT 2014*. Cham: Springer, 2014, 428–442. (Lecture Notes in Comput. Sci.; 8885)
- [4] CERVIÑO, J. M. «Supersingular elliptic curves and maximal quaternionic orders». Preprint, 2004.

- [5] CHILDS, A.; JAO, D.; SOUKHAREV, V. «Constructing elliptic curve isogenies in quantum subexponential time». *J. Math. Cryptol.*, 8 (1) (2014), 1-29.
- [6] DE FEO, L. «Mathematics of isogeny based cryptography». Preprint, 2017.
- [7] EBELING, W. *Lattices and Codes. A Course Partially Based on Lectures by F. Hirzebruch*. 3a ed. Wiesbaden: Springer Spektrum, 2013. (Advanced Lectures in Mathematics)
- [8] GALBRAITH, S. D. *Mathematics of Public Key Cryptography*. Cambridge: Cambridge University Press, 2012.
- [9] GOLDREICH, O.; MICCIANCIO, D.; SAFRA, S.; SEIFERT, J.-P. «Approximating shortest lattice vectors is not harder than approximating closest lattice vectors». *Inform. Process. Lett.*, 71 (2) (1999), 55-61.
- [10] HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H. *An Introduction to Mathematical Cryptography*. Nova York: Springer, 2008. (Undergraduate Texts in Mathematics)
- [11] MICCIANCIO, D. «Lattices Algorithms and Applications». Apunts d'un curs, 2010.
- [12] MICCIANCIO, D.; REGEV, O. «Worst-case to average-case reductions based on Gaussian measures». *SIAM J. Comput.*, 37 (1) (2007), 267-302.
- [13] MICCIANCIO, D.; PEIKERT, C. «Hardness of SIS and LWE with small parameters». A: *Advances in Cryptology—CRYPTO 2013*. Part I. Heidelberg: Springer, 2013, 21-39. (Lecture Notes in Comput. Sci.; 8042)
- [14] MOODY, D.; SHUMOW, D. «Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves». *Math. Comp.*, 85 (300) (2016), 1929-1951.
- [15] PEIKERT, C. «Lattices: ... to Cryptography». Transparències, 2013.
- [16] REGEV, O. «Lattices in Computer Science». Apunts, 2004.
- [17] RUÉ, J.; XAMBÓ, S. «Introducció matemàtica a la computació quàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 28 (2) (2013), 183-231.
- [18] SAYOLS, N.; XAMBÓ, S. «Codis correctors d'errors i criptografia postquàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 33 (2) (2018), 147-171.
- [19] SHOR, P. W. «Algorithms for quantum computation: discrete logarithms and factoring». A: *35th Annual Symposium on Foundations of Computer Science* (Santa Fe, NM, 1994). Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, 124-134.
- [20] SHUMOW, D. «Isogenies of elliptic curves: a computational approach». Preprint, 2009.
- [21] SILVERMAN, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Nova York: Springer-Verlag, 1994. (Graduate Texts in Mathematics; 151)
- [22] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves*. 2a ed. Dordrecht: Springer, 2009. (Graduate Texts in Mathematics; 106)

- [23] SUTHERLAND, A. «Isogeny kernels and division polynomials». Apunts, 2017.
- [24] VAN LINT, J. H. *Introduction to Coding Theory*. 2a ed. Berlín: Springer-Verlag, 1992. (Graduate Texts in Mathematics; 86)
- [25] VILLANUEVA, M.; FERNÁNDEZ-CÓRDOBA, C. «Codis detectors i correctors d'errors i algunes de les seves aplicacions a la societat de la informació». *Butlletí de la Societat Catalana de Matemàtiques*, 34 (1) (2019), 53-89.
- [26] VOIGHT, J. «Quaternion algebras». Apunts d'un curs, 2019.
- [27] WASHINGTON, L. C. *Elliptic Curves. Number Theory and Cryptography*. 2a ed. Boca Raton, FL: Chapman & Hall/CRC, 2008. (Discrete Mathematics and its Applications (Boca Raton))
- [28] ZHAOFEL, T. «GGH Cryptosystem and Lattice Reduction Algorithms». Tesi de màster. McMaster University, 2011.

EURECAT, CENTRE TECNOLÒGIC DE CATALUNYA, UNITAT IT SECURITY
GRUP DE RECERCA EN NOUS MODELS DE CIBERSEGURETAT (2017 SGR 01239)
CARRER DE BILBAO, 72, 08005 BARCELONA, CATALUNYA
ramses.fernandez@eurecat.org

Punts d'energia mínima i empaquetaments d'esferes

JORDI MARZO

Resum: En aquest article tractarem de dos problemes molt interessants i d'una manera de relacionar-los. El primer problema és l'estudi del desenvolupament asimptòtic de l'energia mínima d'un conjunt de punts confinats en una esfera que interaccionen mitjançant un potencial de Riesz. El cas límit d'una de les constants que apareixen en aquest desenvolupament ens portarà al nostre segon problema, el de determinar el millor empaquetament d'esferes a l'espai euclidià, problema en què recentment s'han produït avenços importants.

Paraules clau: energia de Riesz, punts ben distribuïts, empaquetaments d'esferes, programació lineal.

Classificació MSC2010: 31C20, 52C07, 11K36.

1 Problema de Thomson

L'any 1904, amb relació al seu model de nucli atòmic anomenat *púding de panses* (*plum pudding model*), Thomson va plantejar el problema de calcular l'energia mínima d'una configuració d'electrons a la superfície d'una esfera que es repelleixen amb una força determinada per la llei de Coulomb i determinar les disposicions de punts amb energia mínima.

Si denotem com a $\mathbb{S}^2 = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ l'esfera unitat, el problema de Thomson consisteix, doncs, a determinar el valor mínim de

$$\sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \frac{1}{|x_i - x_j|} = \sum_{i \neq j} \frac{1}{|x_i - x_j|}$$

entre totes les eleccions possibles de $x_1, \dots, x_N \in \mathbb{S}^2$ i determinar les que assolixen el mínim.

Aquest escrit està basat en la lliçó inaugural del curs 2018-2019 de la Facultat de Matemàtiques i Informàtica de la Universitat de Barcelona.

Aquest model atòmic es va abandonar ràpidament, però el problema plantejat per Thomson s'ha continuat estudiant. A hores d'ara, però, només s'ha pogut resoldre el problema si el nombre de punts, N , és 1, 2, 3, 4, 5, 6 o 12. El darrer resultat, del 2013, va demostrar que la bipiràmide triangular (5 punts) és minimal amb una prova assistida per ordinador [23].

Un dels problemes és que, a diferència del cercle, on els vèrtexs dels polígons regulars (les arrels de la unitat) minimitzen qualsevol energia raonable, a l'esfera $\mathbb{S}^2$ no hi ha configuracions de punts suficientment bones. Un exemple d'això és que només hi ha 5 poliedres convexos regulars: tetraedre, octaedre, cub, icosaedre i dodecaedre. Aquests poliedres són els anomenats *sòlids platònics* (figura 1), i ja va demostrar Euclides, als *Elements*, que són els únics poliedres convexos regulars. Aquest fet es pot demostrar de manera senzilla utilitzant la característica d'Euler. Així doncs, prendre els vèrtexs dels poliedres convexos regulars no ens permet anar gaire lluny, en termes d'agafar punts (20 punts), però, sorprenentment, fins i tot quan existeixen, els vèrtexs dels poliedres convexos regulars no sempre minimitzen l'energia. En efecte, amb 8 i 20 vèrtexs, que corresponen al cub i al dodecaedre, s'han trobat configuracions de punts que tenen energia menor que les donades pels vèrtexs dels corresponents sòlids platònics.

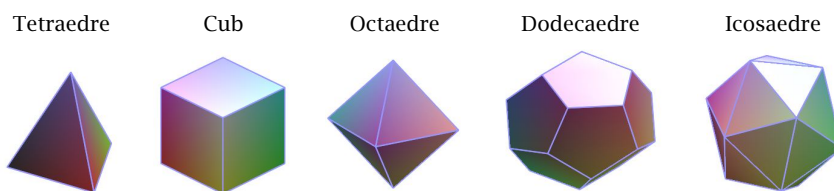


FIGURA 1: Els sòlids platònics.

2 Estimacions asimptòtiques de l'energia mínima

En aquest treball considerarem una generalització del problema de Thompson al context d'esferes en dimensions superiors

$$\mathbb{S}^d = \{(x_1, \dots, x_{d+1}) \in \mathbb{R}^{d+1} : x_1^2 + \dots + x_{d+1}^2 = 1\} \subset \mathbb{R}^{d+1},$$

per a $d \geq 1$ enter, on considerarem conjunts de punts que interaccionen mitjançant energies, anomenades *de Riesz*, que generalitzen la de Coulomb

$$E_s(\mathbb{S}^d, \{x_1, \dots, x_N\}) = \sum_{i=1}^N \sum_{\substack{j=1 \\ j \neq i}}^N \frac{1}{|x_i - x_j|^s} = \sum_{i \neq j} \frac{1}{|x_i - x_j|^s},$$

on $x_1, \dots, x_N \in \mathbb{S}^d$ i $s > 0$. El problema que tractarem serà, no l'energia d'un nombre concret de punts, sinó el comportament asimptòtic de l'energia minimal quan el nombre de punts N creix.

Si considerem els dos valors límit del paràmetre $s \in (0, +\infty)$ obtenim dos problemes particularment interessants. Quan $s \rightarrow 0$ obtenim un potencial logarítmic, en el sentit que $\frac{d}{ds}|_{s=0}(t^{-s}) = -\log t$. Els punts $x_1, \dots, x_N \in \mathbb{S}^d$, que minimitzen l'energia logarítmica

$$\sum_{i \neq j} \log \frac{1}{|x_i - x_j|},$$

són els anomenats *punts de Fekete*. Observem que aquests punts són també aquells que maximitzen el producte de les seves distàncies mútues $\prod_{i \neq j} |x_i - x_j|$, ja que

$$-\log \prod_{i \neq j} |x_i - x_j| = \sum_{i \neq j} \log \frac{1}{|x_i - x_j|}.$$

Quan $s \rightarrow +\infty$ obtenim l'anomenat *problema de Tammes*, o *del millor empaquetament*, que consisteix a trobar les configuracions de N punts $x_1, \dots, x_N \in \mathbb{S}^d$ que fan màxima la distància mínima

$$\min_{1 \leq i \neq j \leq N} |x_i - x_j|.$$

Per tal de limitar una mica el tema, deixarem de banda el cas del potencial logarítmic.

No és difícil demostrar que per a tot $d \geq 2$, N i $s > 0$ hi ha configuracions de punts $x_1^*, \dots, x_N^* \in \mathbb{S}^d$ que assoleixen l'energia mínima, que escrivim $\mathcal{E}_s(\mathbb{S}^d, N)$,

$$\mathcal{E}_s(\mathbb{S}^d, N) = \min_{x_1, \dots, x_N \in \mathbb{S}^d} E_s(\mathbb{S}^d, \{x_1, \dots, x_N\}) = E_s(\mathbb{S}^d, \{x_1^*, \dots, x_N^*\}).$$

En termes físics, aquestes configuracions de punts d'energia mínima són estats fonamentals (*ground states*) si considerem partícules a l'esfera que interaccionen mitjançant el potencial de Riesz (figura 2).

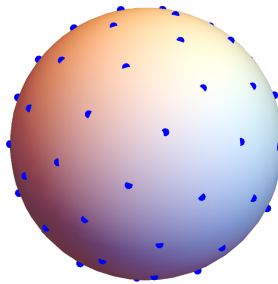


FIGURA 2: Setanta punts minimitzants de l'energia de Coulomb a $\mathbb{S}^2$.

Observem que per a esferes $\mathbb{S}^d$ amb $d \geq 3$ tampoc hi ha configuracions universalment bones. En efecte, Schläfli i Coxeter van demostrar que només hi ha 6 polítops convexos regulars a $\mathbb{R}^4$ i per a $d > 4$ només n'hi ha 3 (les generalitzacions del tetraedre, del cub i de l'octaedre). Una altra mostra d'aquesta falta de bones distribucions és la inexistència, excepte en uns pocs casos, de quadratures de Txeixov minimal a l'esfera [1, 2].

Tal com hem avançat, el nostre objectiu ara és estudiar el comportament asimptòtic, quan $N \rightarrow +\infty$, de l'energia mínima $\mathcal{E}_s(\mathbb{S}^d, N)$. La idea general és que l'energia mínima discreta, si augmenta el nombre de punts, convergeix cap a l'energia mínima contínua. També veurem que hi ha una gran diferència entre potencials de llarg abast $0 < s < d$ i potencials de curt abast $s \geq d$.

Arguments clàssics de teoria del potencial que involucren l'anomenat *diàmetre transfinit generalitzat de Pólya i Szegő* demostren que si $0 < s < d$

$$\lim_{N \rightarrow +\infty} \frac{\mathcal{E}_s(\mathbb{S}^d, N)}{N^2} = \int_{\mathbb{S}^d} \int_{\mathbb{S}^d} \frac{1}{|x - y|^s} d\sigma(x) d\sigma(y),$$

on σ és la mesura de superfície normalitzada a $\mathbb{S}^d$. Per a una demostració més moderna es pot consultar [24, p. 28]. Així, si $x_1^*, \dots, x_N^* \in \mathbb{S}^d$ minimitza l'energia d'exponent $0 < s < d$, una primera aproximació del comportament asimptòtic és

$$\mathcal{E}_s(\mathbb{S}^d, N) = \sum_{i \neq j} \frac{1}{|x_i^* - x_j^*|^s} \approx \left(\int_{\mathbb{S}^d} \int_{\mathbb{S}^d} \frac{1}{|x - y|^s} d\sigma(x) d\sigma(y) \right) N^2. \quad (1)$$

Observem que aquest resultat és cert també per a varietats suaus d dimensionals $X \subset \mathbb{R}^{d+1}$ si considerem l'energia mínima discreta a X i canviem σ per l'anomenada *mesura d'equilibri*, que és la que minimitza el potencial de Riesz continu

$$\int_X \int_X \frac{1}{|x - y|^s} d\mu(x) d\mu(y),$$

entre totes les mesures μ de probabilitat a X .

Els potencials de Riesz per a $0 < s < d$ es diuen *de llarg abast (long range)*, donat que no només els punts propers contribueixen de manera significativa a l'aportació a l'energia d'un punt, sinó que s'han de considerar també els punts llunyans. Observem que, si $s \geq d$, la integral a (1) no convergeix tot i que el terme de l'esquerra és, per a tot N , un valor finit. Si deixem de banda el cas $s = d$, més tècnic, i considerem el cas de potencials de curt abast (*short range potentials*), amb $s > d$, la resposta al comportament asimptòtic de l'energia mínima discreta ve donada per l'anomenat *teorema de la rosquilla amb llavors de rosella (poppy-seed bagel theorem)* [19, 20].

TEOREMA 2.1 (HARDIN, SAFF). *Sigui $X \subset \mathbb{R}^{d'}$ una varietat regular de dimensió d . Sigui*

$$\mathcal{E}_s(X, N) = \sum_{i \neq j} \frac{1}{|x_i^* - x_j^*|^s}$$

l'energia mínima discreta que poden assolir N punts $x_1^, \dots, x_N^* \in X$. Si $s > d$, aleshores*

$$\lim_{N \rightarrow +\infty} \frac{\mathcal{E}_s(X, N)}{N^{1+\frac{s}{d}}} = \frac{C_{s,d}}{\sigma(X)^{s/d}}, \quad (2)$$

on $C_{s,d}$ és una constant positiva independent de X i σ és la mesura de Hausdorff de dimensió d a $\mathbb{R}^{d'}$, normalitzada de manera que el cub unitat $[0, 1]^d$ a $\mathbb{R}^{d'}$ té mesura 1.

Observem el fet remarcable que la constant $C_{s,d}$ del teorema no depèn de la varietat X . Per al cercle $\mathbb{S}^1$ es pot demostrar sense gaire dificultat, [19], que

$$C_{s,1} = 2\zeta(s),$$

on $\zeta(s)$ és la funció zeta de Riemann que es defineix com a

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s},$$

si $\operatorname{Re}(s) > 1$ i s'estén per continuació analítica a tot $\mathbb{C} \setminus \{1\}$.

En general, de cara a determinar el comportament asimptòtic de l'energia mínima $\mathcal{E}_s(\mathbb{S}^d, N)$ quan $N \rightarrow +\infty$, com que la constant $C_{s,d}$ del teorema no depèn de la varietat X , una possible estratègia és considerar varietats més senzilles que $\mathbb{S}^d$ i determinar el comportament de $\mathcal{E}_s(X, N)$ per trobar $C_{s,d}$. Aquesta constant serà, a partir d'ara, el nostre objecte d'estudi principal. Per tal de definir varietats senzilles en dimensions superiors, introduïrem alguns conceptes.

3 Xarxes i tors plans

Definim una *xarxa* o *reticle* com el conjunt

$$\Lambda = \{v_1 k_1 + \dots + v_d k_d : k_i \in \mathbb{Z}\},$$

on $v_1, \dots, v_d$ formen una base de $\mathbb{R}^d$ (figura 3(a)).

Recordem que un problema que tenim per estimar l'energia mínima discreta a l'esfera $\mathbb{S}^d$, quan $d \geq 2$, és que no tenim bones distribucions de punts. Les varietats que considerarem en comptes de l'esfera són els anomenats *tors plans* $\mathbb{R}^d/\Lambda$, que identificarem amb el domini fonamental

$$\{v_1 \alpha_1 + \dots + v_d \alpha_d : \alpha_1, \dots, \alpha_d \in [0, 1)\}$$

(figura 3(b)).

En aquestes varietats sí que podem definir de manera senzilla conjunts de punts clarament ben distribuïts dels quals podem estimar l'energia. Són simplement els reescalats dels punts de la xarxa Λ que cauen al tor $\mathbb{R}^d/\Lambda$ (figura 3(c)). En efecte, si definim els conjunts

$$X_n = \frac{1}{n}\Lambda \cap (\mathbb{R}^d/\Lambda) = \left\{ v_1 \frac{k_1}{n} + \cdots + v_d \frac{k_d}{n} : k_i \in \{0, \dots, n-1\} \right\},$$

tenim que $\#X_n = n^d$ i si denotem tot $x \in X_n$ com a $x = \frac{\lambda}{n}$ amb $\lambda \in \Lambda$ tenim que

$$\sum_{x' \in X_n \setminus \{x\}} |x - x'|^{-s} = n^s \sum_{\substack{\lambda' \in \Lambda \setminus \{\lambda\} \\ \lambda' \in nX_n}} |\lambda - \lambda'|^{-s} \leq n^s \sum_{\lambda' \in \Lambda \setminus \{0\}} |\lambda'|^{-s} = n^s \zeta_\Lambda(s),$$

on, per a $s > d$,

$$\zeta_\Lambda(s) = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{|\lambda|^s}$$

és l'anomenada *funció zeta d'Epstein*. Tenim ara, doncs, que l'energia dels punts reescalats es pot afitar com a

$$E_s(\mathbb{R}^d/\Lambda, X_n) = \sum_{x \in X_n} \sum_{x' \in X_n \setminus \{x\}} \frac{1}{|x - x'|^s} \leq n^{s+d} \zeta_\Lambda(s),$$

i podem deduir que, per a $N \geq 1$ enter, l'energia mínima compleix

$$\mathcal{E}_s(\mathbb{R}^d/\Lambda, N) \leq N^{1+\frac{s}{d}} \zeta_\Lambda(s).$$

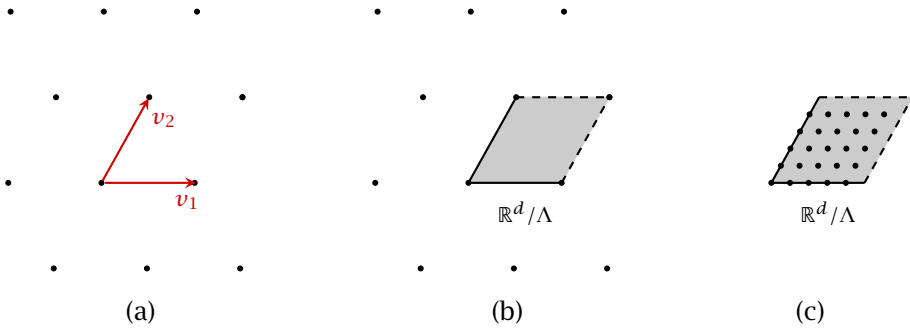


FIGURA 3: (a) Xarxa Λ , (b) domini fonamental, (c) punts reescalats X_n .

Dividint per $N^{1+\frac{s}{d}}$, prenent el límit quan $N \rightarrow +\infty$ i aplicant el teorema 2.1 obtenim que la constant a (2) es pot afitar per

$$C_{s,d} \leq \min_{\Lambda} \text{vol}(\mathbb{R}^d/\Lambda)^{s/d} \zeta_\Lambda(s), \quad (3)$$

on el mínim recorre les xarxes Λ de $\mathbb{R}^d$. Observem que per a $d = 1$ tenim igualtat.

Epstein va definir la funció $\zeta_\Lambda(s)$ l'any 1903 com a generalització de la funció zeta de Riemann, que és $\zeta(s) = \zeta_\mathbb{Z}(s)/2$. Anàlogament al cas de la zeta de Riemann, es pot veure que es pot estendre per continuació analítica a tot $\mathbb{C} \setminus \{d\}$, compleix una equació funcional, té zeros (trivials) als enters parells negatius i té un pol simple a $s = d$ (figura 4), vegeu [25, p. 64]. Tanmateix, se sap que hi ha xarxes per a les quals la corresponent zeta d'Epstein té zeros a l'interval $(0, d)$ i per tant, en general, no es compleix l'anàleg de la hipòtesi de Riemann [26].

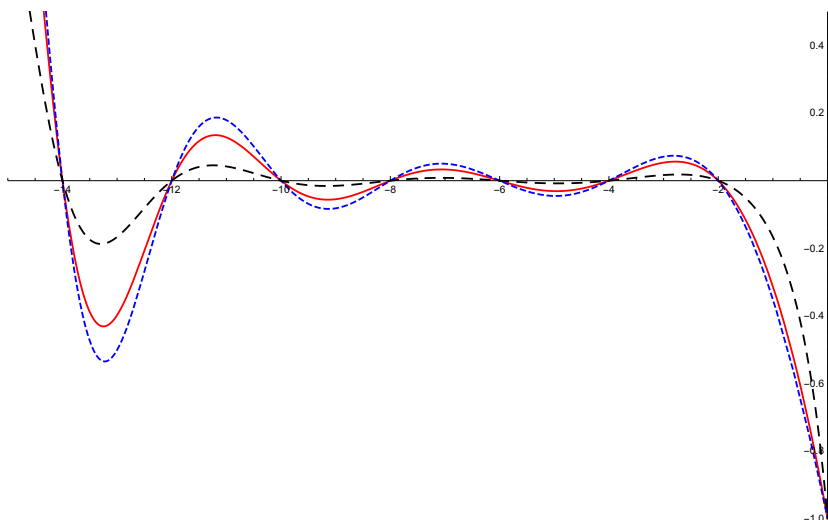


FIGURA 4: Gràfiques de $\zeta_\mathbb{Z}(s)$ (discontinua, trac llarg), $\zeta_{E_8}(s)$ (contínua) i $\zeta_{\Lambda_{24}}(s)$ (discontinua, trac curt).

Donat que sempre podem normalitzar la superfície del tor, si volem donar cotes superiors de la constant $C_{s,d}$ a (3), hem de considerar el problema de la minimització de la funció zeta d'Epstein. Ara bé, de nou, no hi ha gaires resultats coneguts.¹

- Si $d = 2$, la xarxa hexagonal

$$\left\{ k_1 \begin{pmatrix} 2 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix} : k_1, k_2 \in \mathbb{Z} \right\}$$

minimitza $\zeta_\Lambda(s)$ entre totes les xarxes $\Lambda \subset \mathbb{R}^2$ amb volum 1, per a tot $s > 0$ (Rankin [21], Cassels [8]).

¹ Durant la preparació d'aquest treball s'han resolt els casos $d = 8$ i 24 [15], vegeu la darrera secció.

- Si $d = 4, 8$ i 24 , la funció zeta d'Epstein $\zeta_\Lambda(s)$ té un mínim local estricte respectivament a la xarxa de tauler d'escacs

$$D_4 = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : x_1 + x_2 + x_3 + x_4 \text{ parell}\},$$

a la xarxa

$$E_8 = \left\{ (x_1, \dots, x_8) : x_i \in \mathbb{Z} \text{ o } x_i \in \mathbb{Z} + \frac{1}{2} \text{ i } x_1 + \dots + x_8 \text{ parell} \right\},$$

i a la xarxa de Leech Λ_{24} (Sarnak i Strömbergsson [22]).

De fet s'ha conjeatut que en aquestes dimensions privilegiades la constant $C_{s,d}$ s'assoleix en aquestes xarxes, [7, 12], i tenim igualtat a (3).

CONJECTURA 3.1 (BRAUCHART, HARDIN, SAFF [7] I COHN, KUMAR [12]).

$$C_{s,d} = \min_{\Lambda} \text{vol}(\mathbb{R}^d/\Lambda)^{s/d} \zeta_\Lambda(s),$$

per a $d = 2, 4, 8$ i 24 , i el mínim s'assoleix respectivament a les xarxes hexagonal, D_4 , E_8 i Λ_{24} .

4 Empaquetament d'esferes

Hem vist, doncs, que l'únic cas en què es coneix el valor de $C_{s,d}$ és quan $d = 1$. Ara bé, asimptòticament, aquesta constant està relacionada amb una altra constant lligada al segon problema que volem tractar.

TEOREMA 4.1 (BORODACHOV, HARDIN, SAFF [4]).

$$\lim_{s \rightarrow +\infty} C_{s,d}^{1/s} = \frac{1}{2} \left(\frac{\pi^{d/2}}{\Gamma(\frac{d}{2} + 1) \Delta_d} \right)^{1/d},$$

on Δ_d és la major densitat d'un empaquetament d'esferes a $\mathbb{R}^d$.

Un empaquetament d'esferes de $\mathbb{R}^d$ és un conjunt de boles del mateix radi amb interiors disjunts (figura 5) i Δ_d és la fracció de volum màxim de $\mathbb{R}^d$ que podem cobrir amb un empaquetament d'esferes.

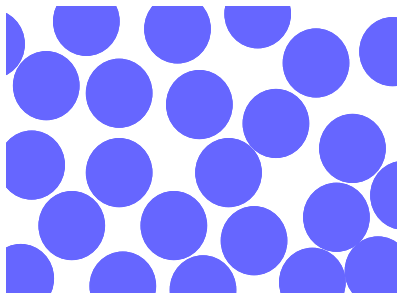


FIGURA 5: Empaquetament d'esferes.

Les esferes dels empaquetaments poden estar centrades en punts no ordenats (figura 5) o estar centrades en punts d'una xarxa (figura 6).

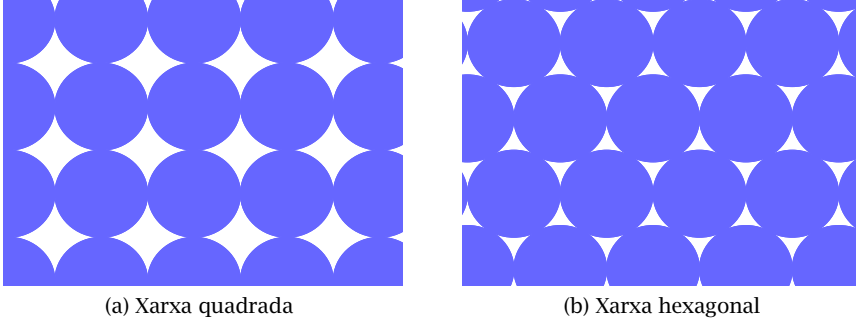


FIGURA 6: Xarxes regulars.

Clarament, la fracció de volum màxim que podem ocupar de $\mathbb{R}$ és $\Delta_1 = 1$, ja que els intervals $[k, k + 1)$ per a $k \in \mathbb{Z}$ cobreixen tot $\mathbb{R}$. Observem que, sabent que $\zeta(s) \approx 1 + \frac{1}{s}$ quan $s \gg 1$, a partir del valor de $C_{s,1}$ efectivament obtenim del teorema 4.1 que $\Delta_1 = 1$. Al pla $\mathbb{R}^2$ es pot veure fàcilment que l'empaquetament quadrat (figura 6(a)) té densitat $\frac{\pi}{4} = 0.7853 \dots$ i, per tant, cobreix un 78.5% de $\mathbb{R}^2$, mentre que l'empaquetament hexagonal (figura 6(b)) té densitat $\frac{\pi}{\sqrt{12}} = 0.9069 \dots$ i cobreix un 90.7% de l'espai. També és fàcil veure que l'empaquetament hexagonal és el millor empaquetament entre els regulars. Ja és una mica més difícil veure que, de fet, és el millor també si considerem tots els empaquetaments de $\mathbb{R}^2$ i que, per tant,

$$\Delta_2 = \Delta_2^* = \frac{\pi}{\sqrt{12}}.$$

Formalment, donat un empaquetament d'esferes $\mathcal{P}$ de $\mathbb{R}^d$ (això és, un conjunt de boles del mateix radi amb interiors disjunts), definim la densitat superior de $\mathcal{P}$ com

$$\limsup_{R \rightarrow \infty} \frac{\text{vol}([-R, R]^d \cap \mathcal{P})}{(2R)^d},$$

i la major densitat d'un empaquetament d'esferes (*sphere packing density*) com

$$\Delta_d = \sup_{\mathcal{P}} \limsup_{R \rightarrow \infty} \frac{\text{vol}([-R, R]^d \cap \mathcal{P})}{(2R)^d},$$

on el suprem recorre els empaquetaments $\mathcal{P}$ de $\mathbb{R}^d$.

Observem que aquesta quantitat és, en principi, més fàcil de calcular en el cas regular. En efecte, donada una xarxa $\Lambda \subset \mathbb{R}^d$, la densitat superior de l'empaquetament format per boles centrades als punts de Λ i radi $r(\Lambda)/2$, on

$$r(\Lambda) = \min\{|\lambda| : \lambda \in \Lambda \setminus \{0\}\}$$

és

$$\frac{\text{vol}(B_{r(\Lambda)/2}^d)}{\text{vol}(\mathbb{R}^d/\Lambda)},$$

ja que al domini fonamental $\mathbb{R}^d/\Lambda$ hi ha exactament una bola de radi $r(\Lambda)/2$ (figura 7).

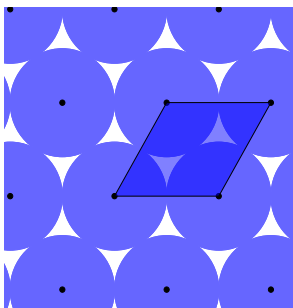


FIGURA 7: Domini fonamental $\mathbb{R}^d/\Lambda$.

Definirem la major densitat dels empaquetaments regulars, això és, d'un empaquetament d'esferes amb centres als punts d'una xarxa, com a

$$\Delta_d^* = \sup_{\Lambda} \frac{\text{vol}(B_{r(\Lambda)/2}^d)}{\text{vol}(\mathbb{R}^d/\Lambda)},$$

on el suprem recorre les xarxes de $\mathbb{R}^d$. Observem que $\Delta_d^* \leq \Delta_d$.

Fins al 2017, mitjançant proves essencialment geomètriques, s'havia pogut trobar el valor de Δ_d per a $d = 2$ i 3 . Algunes dates d'aquesta història són les següents:

- 1773, Lagrange demostra que $\Delta_2^* = \frac{\pi}{\sqrt{12}}$.
- 1910, Thue demostra que $\Delta_2 = \frac{\pi}{\sqrt{12}}$.
- 1611, Kepler conjectura que la xarxa FCC (*face centered cubic*) és òptima i, per tant, que $\Delta_3 = \Delta_3^* = \frac{\pi}{\sqrt{18}}$.
- 1831, Gauss demostra que $\Delta_3^* = \frac{\pi}{\sqrt{18}}$.
- 1953, Fejes Tóth proposa una estratègia per a la conjectura de Kepler de manera que la determinació de Δ_3 es pot reduir a un nombre finit (encara intractable) de casos.
- 1998-2017, Hales prova la conjectura de Kepler amb una demostració per casos utilitzant ordinadors. La demostració va ser acceptada l'any 2017.

Així doncs, finalment, al 2017 s'havia pogut resoldre, en afirmatiu, la conjectura de Kepler amb una prova extremament complexa que donava poques esperances de poder tractar qualsevol altra dimensió més enllà de $\mathbb{R}^3$ [18].

Tanmateix, l'aproximació purament analítica al problema, iniciada per Cohn i Elkies [10], ha donat finalment resultats inesperats, com veurem en la secció següent.

Recordem que hem començat l'article amb el problema de Thomson a l'esfera i que el desenvolupament de l'energia mínima per a potencials de curt abast, de paràmetre $s > d$, ens ha portat a definir la constant $C_{s,d}$, al teorema 2.1. Un nou límit quan $s \rightarrow +\infty$, al teorema 4.1, ens ha fet considerar l'empaquetament d'esferes i la constant Δ_d que hem vist que s'ha pogut determinar per a uns pocs valors de d .

5 Cotes de la densitat amb programació lineal

Per introduir els darrers resultats, necessitarem definir alguns conceptes. Donada una funció prou regular i amb decreixement ràpid, formalment de la classe de Schwartz $f \in S(\mathbb{R}^d)$, definim la seva transformada de Fourier com

$$\hat{f}(y) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i x \cdot y} dx, \quad y \in \mathbb{R}^d.$$

Es pot veure que $\hat{f} \in S(\mathbb{R}^d)$ i que podem recuperar la funció original fent una antitransformada

$$f(x) = \int_{\mathbb{R}^d} \hat{f}(y) e^{2\pi i x \cdot y} dy.$$

En termes físics, si interpretem una funció com un senyal $f(x)$, un so o una imatge, la seva transformada de Fourier $\hat{f}(y)$ ens en dona la freqüència. Entre una funció i la seva transformada hi ha una relació molt estreta. En particular, una funció i la seva transformada no poden estar totes dues ben localitzades. En efecte, es pot veure, per exemple, que si $d = 1$, la transformada d'una funció que és zero fora d'un interval és entera i, per tant, els seus zeros no es poden acumular. Un altre exemple d'aquest comportament és que, per a $\alpha > 0$, si

$$f(x) = e^{-\pi\alpha|x|^2}, \text{ aleshores } \hat{f}(y) = \frac{1}{\alpha^{d/2}} e^{-\pi \frac{|y|^2}{\alpha}},$$

i això ens diu que, tal com es pot veure a la figura 8, la transformada d'una funció gaussiana molt concentrada és una altra gaussiana poc concentrada, i a l'inrevés. De fet, aquesta tensió entre la concentració d'una funció i de la seva transformada es pot quantificar en el principi d'incertesa d'Heisenberg, que, a més, ens diu que les gaussianes són precisament les funcions tals que el parell $f(x), \hat{f}(y)$ està millor concentrat. En general, un principi d'incertesa expressa una relació entre propietats d'una funció (per exemple, la concentració) i propietats de la seva transformada.

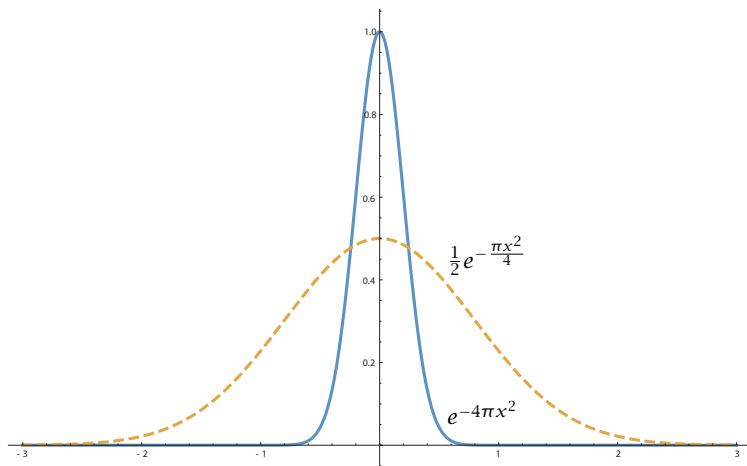


FIGURA 8: Transformades de Fourier.

El següent resultat de Cohn i Elkies és una de les claus dels nous resultats sobre empaquetaments.

TEOREMA 5.1 (COHN, ELKIES [10]). *Si sigui $f \in S(\mathbb{R}^d)$ a valors reals tal que*

- $f(0) = \hat{f}(0) > 0$.
- $\hat{f}(y) \geq 0$, si $y \in \mathbb{R}^d$.
- $f(x) \leq 0$, si $|x| \geq r$ per a un cert $r = r(f) > 0$.

Aleshores, la major densitat d'un empaquetament d'esferes compleix que

$$\Delta_d \leq \text{vol}(B_{r/2}^d) = \frac{\pi^{d/2}}{\Gamma(\frac{d}{2} + 1)} \left(\frac{r}{2}\right)^d.$$

Així doncs, per aprofitar aquest resultat, l'estratègia natural és tractar de trobar funcions $f \in S(\mathbb{R}^d)$ que compleixin les condicions anteriors (podem suposar que són radials) amb $r = r(f)$ tan petit com sigui possible. Aquí trobem, de nou, un principi d'incertesa, ja que les condicions sobre f i $\hat{f}$ van en contra del fet que $r = r(f)$ sigui molt petit. Ara bé, fixada una dimensió, quin és el valor mínim? Es pot assolir? Al seu treball del 2003, Cohn i Elkies només van poder trobar la funció òptima en el cas trivial de dimensió 1, on la funció

$$f(x) = \frac{1}{1-x^2} \left(\frac{\sin \pi x}{\pi x} \right)^2$$

torna a demostrar que $\Delta_1 = 1$.

Donada la dificultat de trobar bones funcions explícitament (excepte per a $d = 1$), en tota una sèrie de treballs Cohn i Elkies [10], Cohn i Kumar [13]

i Cohn i Miller [16] van buscar cotes numèricament amb funcions del tipus $P(|x|)e^{-\pi|x|^2}$, on $P(x)$ és un polinomi. D'aquesta estratègia prové el nom de *programació lineal*. Com a resultat van millorar totes les cotes conegudes prèviament. A més, en alguns casos concrets, $d = 2, 8$ i 24 , les cotes superiors que obtenien coincidien (fins al límit del que podien calcular) amb les cotes inferiors donades per a les xarxes hexagonal, E_8 i Λ_{24} que hem vist abans (figura 9).

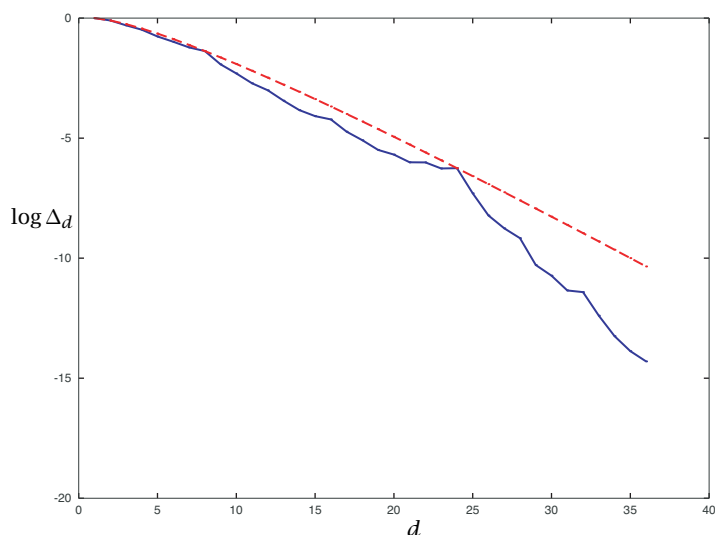


FIGURA 9: Cotes superiors i inferiors de $\log \Delta_d$ calculades amb les dades de [9]. La línia contínua mostra el millor empaquetament conegut, i la discontinua, la cota per programació lineal. Observeu l'aparent coincidència quan $d = 8, 24$.

Això va portar Cohn i Elkies a conjeturar l'existència de funcions que donaven la igualtat al teorema per a aquests valors $d = 2, 8$ i 24 . Però, tot i que des d'un punt de vista numèric les funcions òptimes es podien calcular, no es va poder trobar una expressió explícita i quedava, per tant, la incertesa de si, més enllà del nombre de decimals computables, podia trobar-se una configuració millor que les donades per a aquestes xarxes. Aquest problema es va resoldre finalment l'any 2017 quan Viazovska va construir la funció òptima per a $d = 8$ ([27]) utilitzant formes modulars i va demostrar, per tant, que

$$\Delta_8 = \Delta_8^* = \frac{\pi^4}{384} = 0.253\,669\dots$$

Molt poc temps després, utilitzant les tècniques desenvolupades per Viazovska per a E_8 , Cohn, Kumar, Miller, Radchenko i Viazovska van construir la funció òptima per a $d = 24$ ([14]) i van demostrar que

$$\Delta_{24} = \Delta_{24}^* = \frac{\pi^{12}}{12!} = \frac{\pi^{12}}{479\,001\,600} = 0.001\,929\dots$$

En contrast amb la demostració de Hales per a $\mathbb{R}^3$, aquests treballs no requereixen càlculs informàtics i es basen en eines clàssiques. Ara bé, tal com es pot anticipar veient la figura 9, no és d'esperar que es puguin demostrar altres cotes òptimes utilitzant aquestes tècniques. De fet, sorprenentment, encara s'ha de trobar la funció que demostrï que la xarxa hexagonal és el millor empaquetament a $\mathbb{R}^2$!

Així doncs, tret d'aquest cas ja conegut, semblaria que la història de les cotes per programació lineal acaba aquí, però, com sempre en matemàtiques, una nova solució ens porta a nous problemes. Una vessant molt interessant és precisament interpretar les cotes de Cohn i Elkies com un principi d'incertesa i tractar de trobar les cotes i les funcions òptimes. Seguint aquesta idea Cohn i Gonçalves [11], utilitzant les tècniques desenvolupades per Viazovska, han trobat les cotes òptimes, en dimensió 12, per un principi d'incertesa que van estudiar Bourgain, Clozel i Kahane.

6 Darreres observacions

Els resultats de les primeres seccions d'aquest article tenen una versió dual, en un cert sentit, en termes de configuracions de punts de polarització màxima. Aquest problema és més complex que el de l'energia mínima i té com a límit el problema del millor recobriment (*best-covering*), en comptes del de millor empaquetament [3]. Encara està per desenvolupar, però, una teoria anàloga a la programació lineal per a aquest problema.

Com a actualització de darrera hora, voldria mencionar que els mateixos autors que van demostrar l'optimalitat de la xarxa de Leech han demostrat que E_8 i Λ_{24} són, de fet, universalment òptims, en el sentit que minimitzen no només l'energia donada pel potencial de Riesz, sinó la de tot potencial donat per una funció completament monòtona [15].

Finalment, voldria remarcar que cap dels resultats de què he parlat són meus i només ho és la lectura que he fet dels resultats d'altres. Algunes referències per a aquells que vulguin aprofundir en aquests temes són els articles [6], [19] i [9], i els llibres [17] i [5]. També són molt recomanables les col·leccions de xerrades de Viazovska a l'Institut des Hautes Études Scientifiques (IHES) i les de Carneiro i Gonçalves a l'Instituto de Matemática Pura e Aplicada (IMPA).

Referències

- [1] BANNAI, E.; DAMERELL, R. M. «Tight spherical designs. I». *J. Math. Soc. Japan*, 31 (1) (1979), 199–207.
- [2] BANNAI, E.; DAMERELL, R. M. «Tight spherical designs. II». *J. London Math. Soc.* (2), 21 (1) (1980), 13–30.
- [3] BORODACHOV, S. V.; HARDIN, D. P.; REZNIKOV, A.; SAFF, E. B. «Optimal discrete measures for Riesz potentials». *Trans. Amer. Math. Soc.*, 370 (10) (2018), 6973–6993.

- [4] BORODACHOV, S. V.; HARDIN, D. P.; SAFF, E. B. «Asymptotics of best-packing on rectifiable sets». *Proc. Amer. Math. Soc.*, 135 (8) (2007), 2369–2380.
- [5] BORODACHOV, S. V.; HARDIN, D. P.; SAFF, E. B. *Discrete Energy on Rectifiable Sets*. Nova York: Springer-Verlag, 2019. (Springer Monographs in Mathematics)
- [6] BRAUCHART, J. S.; GRABNER, P. J. «Distributing many points on spheres: Minimal energy and designs». *J. Complexity*, 31 (3) (2015), 293–326.
- [7] BRAUCHART, J. S.; HARDIN, D. P.; SAFF, E. B. «The next-order term for optimal Riesz and logarithmic energy asymptotics on the sphere». A: *Recent Advances in Orthogonal Polynomials, Special Functions, and Their Applications*. Providence, RI: Amer. Math. Soc., 2012, 31–61. (Contemp. Math.; 578)
- [8] CASSELS, J. W. S. «On a problem of Rankin about the Epstein zeta-function». *Proc. Glasgow Math. Assoc.*, 4 (1959), 73–80.
- [9] COHN, H. «A conceptual breakthrough in sphere packing». *Notices Amer. Math. Soc.*, 64 (2) (2017), 102–115.
- [10] COHN, H.; ELKIES, N. «New upper bounds on sphere packings. I». *Ann. of Math. (2)*, 157 (2) (2003), 689–714.
- [11] COHN, H.; GONÇALVES, F. «An optimal uncertainty principle in twelve dimensions via modular forms». *Invent. Math.*, 217 (3) (2019), 799–831.
- [12] COHN, H.; KUMAR, A. «Universally optimal distribution of points on spheres». *J. Amer. Math. Soc.*, 20 (1) (2007), 99–148.
- [13] COHN, H.; KUMAR, A. «Optimality and uniqueness of the Leech lattice among lattices». *Ann. of Math. (2)*, 170 (3) (2009), 1003–1050.
- [14] COHN, H.; KUMAR, A.; MILLER, S. D.; RADCHENKO, D.; VIAZOVSKA, M. «The sphere packing problem in dimension 24». *Ann. of Math. (2)*, 185 (3) (2017), 1017–1033.
- [15] COHN, H.; KUMAR, A.; MILLER, S. D.; RADCHENKO, D.; VIAZOVSKA, M. «Universal optimality of the E_8 and Leech lattices and interpolation formulas». Preprint, 2019. <https://arxiv.org/abs/1902.05438v2>.
- [16] COHN, H.; MILLER, S. D. «Some properties of optimal functions for sphere packing in dimensions 8 and 24». Preprint, 2016. <https://arxiv.org/abs/1603.04759>.
- [17] CONWAY, J. H.; SLOANE, N. J. A. *Sphere Packings, Lattices and Groups*. 3a ed. Nova York: Springer-Verlag, 1999. (Grundlehren der Mathematischen Wissenschaften; 290)
- [18] HALES, T. C. «Cannonballs and honeycombs». *Notices Amer. Math. Soc.*, 47 (4) (2000), 440–449.
- [19] HARDIN, D. P.; SAFF, E. B. «Discretizing manifolds via minimum energy points». *Notices Amer. Math. Soc.*, 51 (10) (2004), 1186–1194.
- [20] HARDIN, D. P.; SAFF, E. B. «Minimal Riesz energy point configurations for rectifiable d -dimensional manifolds». *Adv. Math.*, 193 (1) (2005), 174–204.

- [21] RANKIN, R. A. «A minimum problem for the Epstein zeta-function». *Proc. Glasgow Math. Assoc.*, 1 (1953), 149–158.
- [22] SARNAK, P.; STRÖMBERGSSON, A. «Minima of Epstein's zeta function and heights of flat tori». *Invent. Math.*, 165 (1) (2006), 115–151.
- [23] SCHWARTZ, R. E. «The five-electron case of Thomson's problem». *Exp. Math.*, 22 (2) (2013), 157–186.
- [24] SERFATY, S. *Coulomb Gases and Ginzburg-Landau Vortices*. Zurich: EMS, 2015. (Zurich Lectures in Advanced Mathematics; 21).
- [25] TERRAS, A. *Harmonic Analysis on Symmetric Spaces—Euclidean Space, the Sphere, and the Poincaré Upper Half-Plane*. 2a ed. Nova York: Springer, 2013.
- [26] TERRAS, A. *Harmonic Analysis on Symmetric Spaces—Higher Rank Spaces, Positive Definite Matrix Space and Generalizations*. 2a ed. Nova York: Springer, 2016.
- [27] VIAZOVSKA, M. S. «The sphere packing problem in dimension 8». *Ann. of Math.* (2), 185 (3) (2017), 991–1015.

DEPARTAMENT DE MATEMÀTIQUES I INFORMÀTICA
UNIVERSITAT DE BARCELONA
08007 BARCELONA, SPAIN
jmarzo@ub.edu

Caracteritzant els codis de Gauss: només cal girar la cantonada

LLUÍS VENA

Resum: Aquest document està dedicat a la història, les motivacions i algunes solucions al *problema dels codis de Gauss*.

Una corba tancada al pla pot contenir punts d'autointersecció; en suposem un nombre finit, suposem els talls no tangencials i suposem que la corba recorre cada punt del pla un màxim de dos cops. Si etiquetem els punts de tall amb símbols diferents, triem un punt a la corba, un sentit, i, en recórrer la corba, anotem la seqüència de símbols que anem trobant, aleshores generem una paraula que s'anomena genèricament *codi de Gauss*.

El problema dels codis de Gauss és el de caracteritzar quines són les possibles paraules generades per corbes al pla. Com veurem, les solucions al problema demanen girar la cantonada.

Paraules clau: codis de Gauss, paràgraf de Gauss, caracterització alternativa, cercles de Seifert.

Classificació MSC2010: primària: 05C10; secundària: 57M15, 57M25.

1 Introducció

1.1 Una mica d'història i presentació del problema

Després de la mort de Gauss l'any 1855, i degut a la importància dels seus descobriments, es va decidir de preservar el seu llegat. En l'apartat matematico-literari aquest constava d'una substancial biblioteca i manuscrits variats. Després de catalogar-la, la seva biblioteca personal es va integrar en la de la universitat —amb l'excepció d'aquells volums que contenien nombroses anotacions, que es van classificar com a manuscrits. També es va decidir publicar les seves obres completes; això incloïa tant els treballs ja publicats (el primer volum de les obres completes està dedicat al *Disquisitiones arithmeticae*), com d'altres manuscrits, notes, cartes, fulls solts i quaderns que Gauss havia escrit. La tasca d'editar les obres completes va recaure en Ernst Schering, professor de la Universitat de Göttingen i deixeble de Gauss [7].

Schering era un matemàtic versàtil amb coneixements en diferents àrees de les matemàtiques. Això li va permetre d'editar, fins a la seva mort l'any 1897, sis volums dels treballs complets de Gauss que van ser publicats entre els anys 1863 i 1874 [9, 10, 11, 12, 13, 14]. La resta de volums, fins a completar la dotzena [15, 16, 17, 18, 19, 20], van ser editats per Fricke (anàlisi), Stäckel (geometria), Borsch i Kruger (material geodèsic), Wiechert (física matemàtica), Galle i Geppert, entre d'altres. Brendel, Schlesinger i Klein van prendre el rol d'editors generals per coordinar la tasca en aquesta segona etapa després de la mort de Schering.

Deixant de banda les dificultats inherents a l'edició de treballs no sempre completament finalitzats, en el cas de Gauss s'hi han d'afegir: la manca de dates a molts manuscrits, la gran varietat de formats (llibretes, quaderns, papers solts, anotacions profuses a llibres), així com la diferència en la presentació: tot i que alguns dels manuscrits estan escrits amb lletra clara, d'altres costen més d'entendre i desxifrar.

Després de diverses vicissituds (mort de Schering el 1897, Brendel fou dos anys presoner de guerra a França durant la Primera Guerra Mundial, mort de Klein l'any 1925), els treballs complets de Gauss, dotze volums en total, amb alguns d'ells publicats en diverses parts, es van acabar de publicar l'any 1933. Cal fer notar que la numeració dels volums i les parts no segueix estrictament un ordre cronològic, una dada que indica les dificultats de la tasca.

Nachlass: Zur Geometria Situs. En el volum VIII de les obres completes [16], entre les pàgines 271 i 286, apareixen, agrupades sota el títol genèric de *Geometria Situs*, dues parts dedicades al que avui anomenem *teoria de nusos*. Aquestes parts, que van ser editades per Stäckel, duen per subtítols: [I.] *Zur Geometria Situs* i [II.] *Zur Geometrie der Lage, für zwei raumdimensionen*. La primera part consta de diverses notes trobades en un quadern i presumiblement escrites entre els anys 1822 i 1840 (no estan datades); la segona part va ser escrita l'any 1844.

En la primera part, [I.] *Zur Geometria Situs*, es consideren diverses maneres de descriure la representació plana d'un nus o d'una corba tancada al pla i s'hi tracta el nombre de rotació de les diferents regions en què la corba subdivideix el pla, així com maneres de calcular-lo usant la informació que ens proporcionen la corba i els seus punts d'autointersecció.¹ A la segona nota de la part I hi ha una referència al peu de pàgina on es menciona el problema tractat a la part II i que està datada el 30 de desembre del 1844.

En la segona part, la titulada [II.] *Zur Geometrie der Lage, für zwei raumdimensionen*, Gauss introdueix el problema al qual dediquem la resta de l'article i que queda especificat en la qüestió 1 d'aquest treball. Les qüestions 2 i 3 són reformulacions alternatives del problema.

¹ El nombre de rotació d'un punt del pla respecte d'una corba tancada és el nombre de cops que la corba encercla el punt.

El problema dels codis de Gauss. Sigui γ una corba tancada, al pla, amb un nombre finit de punts d'autointersecció; usarem n per denotar aquest nombre. En aquests punts la corba es talla de manera no tangencial. Assignem, a cada punt d'intersecció, un símbol d'entre $\{s_1, s_2, s_3, \dots\}$ de manera injectiva (cada punt d'intersecció rep un únic símbol), i seleccionem un punt de la corba γ i un sentit per recorre-la. Recorrem la γ i anotem els símbols dels diferents punts d'intersecció que trobem. Això genera una paraula de $2n$ lletres en n símbols (vegeu la figura 1 com a exemple). De manera més general, podem tenir un conjunt de corbes tancades al pla formant un total de n punts de tall; en aquest cas cada corba genera una paraula de, possiblement, diferent llargada, i el conjunt de corbes genera un paràgraf on cada símbol apareix un total de dues vegades ($2n$ lletres entre totes les paraules i n símbols en total). Suposarem que no hi ha corbes isolades i, per tant, no hi ha cap subconjunt estricte de paraules amb aquestes propietats. Més formalment,

DEFINICIÓ 1 (CODI DE GAUSS, PARÀGRAF DE GAUSS). Un *paràgraf de Gauss* ω de mida n està format per un conjunt de $2n$ lletres $L = \{l_1, \dots, l_{2n}\}$, un conjunt de n símbols $S = \{s_1, \dots, s_n\}$, una aplicació dos-a-u $J: L \rightarrow S$ que determina quin parell de lletres correspon a cada símbol, i una aplicació bijectiva $N: L \rightarrow L$ que determina la lletra següent a ω .

Cada òrbita de N és una *paraula*. També demanem que cap subconjunt de paraules sigui un paràgraf de Gauss per si mateix. En el cas de tenir una única paraula usem el terme *codi de Gauss*.

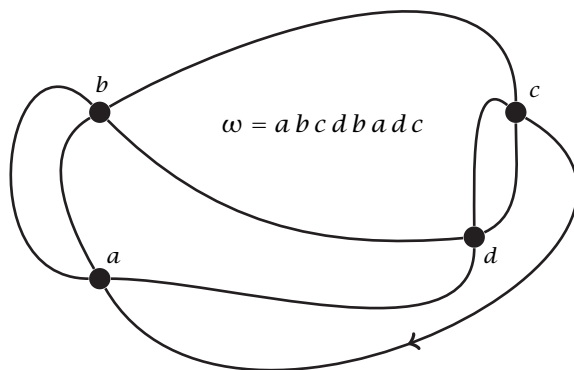


FIGURA 1: Corba representable al pla. El punt inicial està representat per una fletxa que, alhora, n'indica el sentit de recorregut.

Dues paraules donen lloc al mateix codi de Gauss si hi ha una bijecció entre els símbols tal que els dos conjunts de lletres tinguin el mateix ordre cíclic. El problema dels codis de Gauss és el següent:

QÜESTIÓ 1 (PROBLEMA DELS CODIS DE GAUSS). Quines condicions ha de complir una paraula ω de $2n$ lletres, on cada lletra apareix exactament dos cops (codi de Gauss), per tal que existeixi una corba tancada γ , al pla, que la representi?

Condicció de Gauss. Després de presentar el problema de quines paraules de $2n$ lletres en n símbols, on cada símbol apareix 2 cops, són representables per corbes al pla (qüestió 1 en aquest treball), Gauss estableix una condició necessària:

PROPOSICIÓ 2 (CONDICIÓ DE GAUSS). *Si un codi de Gauss no signat és representable al pla, aleshores*

*entre qualsevol parella de lletres del mateix símbol
hi ha un nombre parell de lletres.*

Aquesta condició és bastant natural: una repetició de símbols significa que podem trobar una subcorba tancada que defineix una regió tancada. Sempre que «entrem» a la regió n'hem de «sortir». Tant si entrem a la regió com si en sortim tallarem la corba, per això el nombre de talls és parell.² Posteriorment fa una llista de totes les paraules de 8 lletres o menys (4 símbols diferents, 8 lletres en total) [16, p. 282–283] i veu com aquesta condició, en aquest cas, també és suficient. Després examina totes les paraules de fins a 5 parells de símbols i conclou que la condició no és suficient en aquests casos. Troba que les paraules *abcadcedbe* i *abcadbecde* compleixen la condició de la proposició 2, però amb una simple comprovació manual podem veure que no tenen representació al pla. Així, *abcadcedbe* i *abcadbecde* són les paraules de menys símbols en les que la condició de Gauss no és suficient.³

1.2 Solucions parcials, caracteritzacions i generalitzacions

Nagy [28] va donar una condició necessària més general que la condició de Gauss l'any 1927, tot i que no era suficient. No va ser fins l'any 1936 que Dehn dona la caracterització que veurem més endavant a la secció 4, i que Read i Rosenstiehl [29] van completar fins a la forma que presentem en la mencionada secció com a teorema 8. Altres autors han donat caracteritzacions en termes de subestructures prohibides [26], o d'altres variacions i refinaments a la que presentem a la secció 4 com ara [4, 30, 31, 32, 1, 2]. En aquest treball donem una caracterització diferent, de caire més algorítmic, en forma de teorema 16 a la secció 5 i que es pot trobar de manera més completa a [38]; d'aquest resultat en deduïm la caracterització del teorema 17.

Una primera generalització del problema, desvelat a la definició 1, consisteix a demanar-se per una caracterització quan considerem paràgrafs on cada símbol apareix un total de dos cops. Volem trobar tantes corbes al pla com paraules, i que s'intersequin d'acord amb les lletres en comú en talls no tangencials. La caracterització dels paràgrafs al pla es pot deduir dels arguments de la secció 4; addicionalment, la caracterització de la secció 5 es pot aplicar directament a aquest cas.

² Una demostració més rigorosa de la proposició 2 es pot trobar dins la prova del teorema 8 a la secció 4.

³ A part dels exemples, Godsil i Royle [21, teorema 17.4.2] donen condicions suficients per tal que la condició de Gauss sigui necessària quan permetem que la corba sigui immersa en una superfície orientable qualsevol.

Un cop obtinguda la caracterització dels codis de Gauss o paràgrafs del cas pla, una pregunta natural és demanar-se per la caracterització dels codis de Gauss que es poden representar per corbes en una superfície orientable de gènere g . Tot i que determinar el gènere mínim d'una superfície on el codi es pugui representar és difícil, hi ha resultats positius si la superfície és fixada i s'imposen algunes condicions naturals a les immersions de la corba i que sempre es compleixen en el cas planar [25, 24]. Una altra generalització consisteix a demanar-se per codis o paràgrafs de Gauss on cada símbol pot ser repetit més de dos cops: en aquest cas, cada punt d'intersecció pot ser visitat més de dos cops de manera no tangencial (vegeu [4, secció 5] i [3] per a una solució en el cas de 2 i/o 3 interseccions).

1.3 Resum dels resultats i organització del treball

Com hem descrit de manera breu anteriorment, en aquest article exposem dues solucions a la qüestió 1 que queden condensades en el teorema 8 i els teoremes 16 i 17 de les seccions 4 i 5. El teorema 8 és la primera caracterització que es va trobar; la demostració original és deguda a Dehn [5] i a Read i Rosenstiehl [29, 30, 32]; per a aquest article seguim la presentació [21, teorema 17.7.1].⁴ El teorema 16 es pot trobar a [38].

Les caracteritzacions del teorema 8 i dels teoremes 16 i 17 tenen similituds —les dues utilitzen una estructura combinatòria auxiliar sobre la qual s'imposen restriccions, i aquesta estructura —que és diferent en els dos casos— s'obté mitjançant procediments conceptualment similars sobre la paraula. Més concretament:

- En el primer cas, teorema 8, la caracterització ve donada per la planaritat de l'estructura auxiliar (un diagrama de cordes) més una condició que tot codi de Gauss realitzable satisfà (proposició 2). Aquesta condició addicional ens permet refer, pas per pas, els punts de tall sobre l'estructura auxiliar sense comprometre'n la planaritat. Amb les modificacions pertinents introduïdes per Rosenstiehl i Tarjan a [33], aquesta caracterització dona un algorisme que determina si ω és una paraula representable al pla en temps lineal. Addicionalment, en cas de resposta afirmativa, es construeix una corba que representa ω al pla en temps lineal.
- En el segon cas, teorema 16, dona directament un procediment que, en temps lineal, troba una representació plana, si aquesta existeix, o bé respon que aquesta no existeix. El procediment depèn únicament d'una estructura auxiliar alternativa: el graf d'intersecció d'una col·lecció de cercles en una superfície que es poden intersecar tangencialment, també coneguts com a *cercles de Seifert* [34]. D'aquest algorisme en podem deduir el teorema 17, que seria l'anàleg al teorema 8.

⁴ Cal mencionar que altres caracteritzacions com ara les que usen l'estructura de cicles i el teorema de Mac Lane per a la caracterització dels grafs planars [27, 36] o de subestructures prohibides en la línia de la caracterització dels grafs planars de Kuratowski [26] precedeixen l'argument complet de la presentada com a teorema 8. Per altra banda, també hi ha refinaments de les idees de Dehn, Read i Rosenstiehl que són posteriors, com ara [4, 31] o [2].

Com veurem, les caracteritzacions presentades, teorema 8 i teoremes 16 i 17, són conceptualment similars en el fet que totes dues «desfan» els punts de tall (operació explicada en detall a la secció 3 i resumida en la figura 9) per tal d'obtenir les mencionades estructures auxiliars. A més, ambdues maneres de desfer els punts de tall són les més «naturals» perquè desfan els nusos simplement «girant la cantonada» en arribar a un punt de tall (vegeu la figura 9 i la secció 3 per a més detalls). A la secció 6 veurem com la solució al problema de Gauss també es trobava «girant una altra cantonada», més material que matemàtica.

A la secció 2 presentem els motius que van dur Gauss a considerar aquest problema i introduïm els grafs i mapes auxiliars necessaris per donar les caracteritzacions i que ens permetran de donar una altra perspectiva al problema. A la secció 3 veiem amb detall les operacions que fem al codi de Gauss per tal d'obtenir les mencionades estructures auxiliars. Finalment, les seccions 4, 5 i 6 estan dedicades a donar tres respostes a la qüestió 1.

2 Motivació, reformulacions, grafs i mapes

2.1 Motivació del problema, codis de Gauss signats

La motivació del problema dels codis de Gauss prové de la teoria de nusos. Un *nus* és una immersió de la circumferència S^1 a l'espai tridimensional $\mathbb{R}^3$. Considerem que la circumferència està recorreguda en un sentit determinat i amb un punt inicial donat.⁵ Dos *nusos* són *equivalents* si hi ha una deformació contínua $H(x, t): \mathbb{R}^3 \times [0, 1] \rightarrow \mathbb{R}^3$, tal que per a cada t tenim una immersió d'una circumferència a $\mathbb{R}^3$, de manera que, per a $t = 0$, és el primer nus i, per a $t = 1$, el segon. Si projectem el nus sobre un pla genèric de tal manera que la preimatge de cada punt del pla interseca el nus un màxim de dos cops, aleshores obtenim una corba tancada al pla amb un nombre finit d'interseccions i cada intersecció és no tangent. Si afegim informació sobre els punts d'autointersecció al pla (o punts de tall de la corba) podrem refer el nus. En particular, cal determinar quina de les dues branques de la circumferència passa per sobre i quina per sota; usem la convenció que la branca amb coordenada més petita respecte del pla és la que passa per sota. Així doncs, podem veure un nus com una corba tancada al pla amb la decoració adequada de les branques (quina passa per dalt, quina passa per baix) als punts d'intersecció.

Si ara volem expressar com és la corba al pla, podem assignar un símbol a cada punt d'intersecció, donar una llista de l'ordre en què els recorrem (paraula de $2n$ lletres) per desplegar els trams de corba entre els punts, i com és la situació que ens trobem al punt de tall, o el *signe* del tall. Si prenem un punt arbitrari a la corba i un sentit de recorregut, podem parlar del primer i segon tram de corba que passa per un punt. El primer tram orientat divideix el pla entre esquerra i dreta (segons el sentit de recorregut). Aleshores, el segon tram

⁵ També suposarem que existeix un $\epsilon_0 > 0$, dependent del nus, tal que la intersecció entre la circumferència i tota bola de radi $\epsilon \leq \epsilon_0$ té una única component connexa. També suposarem que la circumferència a $\mathbb{R}^3$ té longitud 1.

pot anar de dreta a esquerra (punt de tall negatiu) o d'esquerra a dreta (punt de tall positiu). Vegeu la figura 2.

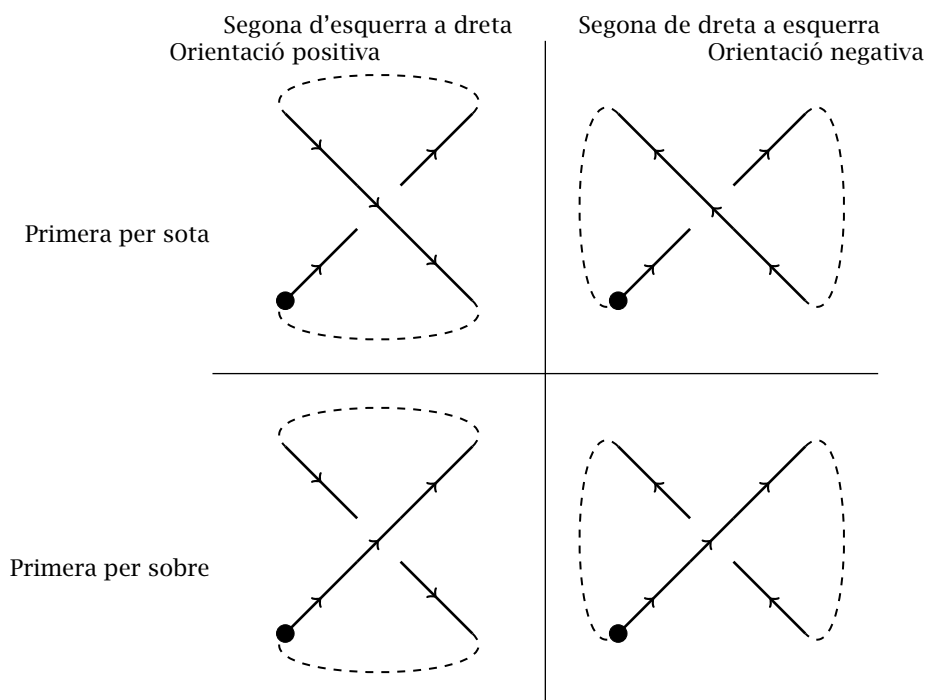


FIGURA 2: Possibles tipus d'interseccions en un nus.

Si assignem un símbol a cada intersecció, $*^{+1}$ si passem per sobre, $+$ si l'altra branca va d'esquerra a dreta, aleshores podem codificar el nus usant n símbols, cadascun d'ells repetit dos cops, amb un signe $+$ o cap signe i un exponent $+1$ o sense exponent (vegeu, per exemple, la part esquerra de la figura 3; per aclarir, usem $-*$ o $*^{-1}$ en comptes de no posar cap signe). Aquesta codificació de la representació del nus s'anomena *codi de Gauss signat estès*. Vegeu la figura 2.⁶

Així doncs, si prescindim dels signes, per a cada nus obtenim un codi de Gauss. La qüestió 1 pot ser reformulada de la manera següent: quins són els codis de Gauss que provenen d'un nus? Tot i que és crucial per determinar si dos nusos són equivalents o no, la informació respecte a si la branca passa per dalt o per baix és irrellevant en aquest cas. Efectivament, si tallem la branca

⁶ Si el primer cop que travessem la intersecció la corba passa per sobre, llavors el segon cop passarà per sota (i al revés). Si el primer cop l'altra branca travessa la corba de dreta a esquerra, el següent cop la travessarà d'esquerra a dreta (i al revés). Per tant, amb la convenció que el primer cop que travessem la intersecció codifiquem el pas sobre/sota i el segon cop codifiquem esquerra/dreta, podem codificar el nus usant n símbols, cadascun repetit dos cops, i amb signe $+$ o sense signe.

que passa per sota just abans i just després del punt de tall s i la canviem per un «pont», obtenim un nou nus amb la mateixa projecció plana on l'únic canvi és el pas sobre/sota de s . Per altra banda, la informació respecte del signe del punt de tall és rellevant per a aquesta pregunta. En particular, no hi ha cap nus que ens doni la projecció plana amb els signes

$$[+a]bca[+b][+c] \text{ o bé } [+a][-b][-c][-a][+b][+c], \quad (1)$$

però sí amb els signes

$$a[+b]c[+a]b[+c] \text{ o bé } [-a][+b][-c][+a][-b][+c],$$

com, per exemple, el nus trèvol (vegeu la figura 3):

$$[a][+b^{+1}][c][+a^{+1}][b][+c^{+1}] \text{ o } [-a^{-1}][+b^{+1}][-c^{-1}][+a^{+1}][-b^{-1}][+c^{+1}].$$

Si prescindim de la informació respecte a si els trossos de corba passen per sobre o per sota, obtenim un *codi de Gauss signat*.

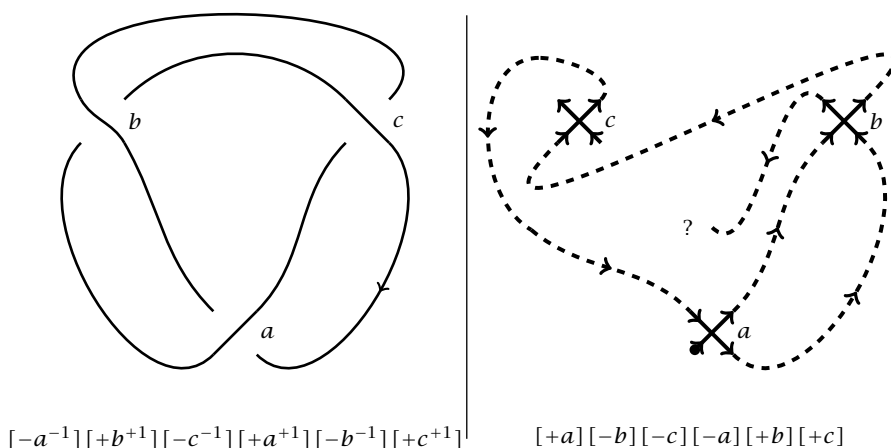


FIGURA 3: Nus trèvol, punt inicial de recorregut a la fletxa, i codi de Gauss no pla.

2.2 Grafs i mapes

En aquest article entendrem un *graf dirigit* com una parella formada per un conjunt de *vèrtexs* V i un multiconjunt d'*arestes* $E = (V \times V, f)$, on $f: V \times V \rightarrow \mathbb{N}$ indica, per a cada parell ordenat $(u, v) \in V \times V$, el nombre d'aparicions a E . Denotem les arestes pels parells ordenats i permetem que el graf tingui llaços, o parells de la forma (u, u) . En el nostre cas, tant V com E són finits.

En un graf dirigit, l'aresta (u, v) denota l'aresta de u a v i és diferent de l'aresta de v a u o (v, u) . Usarem el terme *graf no dirigit* per referir-nos a un graf dirigit on hem oblidat les direccions; en aquest cas denotarem per $\{u, v\}$ l'aresta entre u i v : l'aresta $\{u, v\}$ és present al graf si el graf dirigit

conté l'aresta (u, v) o bé l'aresta (v, u) . Dos vèrtexs u i v es diu que són *adjacents* si (u, v) o bé (v, u) són arestes del graf.

Un graf (dirigit o no dirigit) és *connex* si entre dos vèrtexs diferents qualssevol v_i i v_f hi ha un *camí* entre ells: un conjunt de vèrtexs $v_i = v_1, v_2, \dots, v_{k-1}, v_k = v_f$ tals que l'aresta (v_j, v_{j+1}) o bé l'aresta (v_{j+1}, v_j) pertanyen a E . En el nostre cas només considerem grafs connexos. En certs contextos ens serà útil parlar de diferents orientacions (o direccions) de les arestes en un mateix graf no dirigit; usarem σ per denotar una orientació de les arestes.

En un graf dirigit, un *camí eulerià* és una ordenació de les arestes del graf $E = ((v_1, v_2), (v_3, v_4), \dots, (v_{2|E|-1}, v_{2|E|}))$ tal que $v_{2i} = v_{2i+1}$ i $v_1 = v_{2|E|}$; això és, un camí dirigit passa per totes les arestes del graf un únic cop. Si el graf conté un camí eulerià es diu que el graf és *eulerià*.

Una *immersió d'un graf* G en una superfície Σ és un conjunt de corbes $\mathcal{U}$ (tantes com arestes en E) i punts $\mathcal{P}$ (tants com vèrtexs en V) a Σ tals que la corba (v_1, v_2) té v_1 com a punt inicial, v_2 com a punt final, no passa per cap altre vèrtex, i dues corbes només s'intersequen en vèrtexs. La immersió és *2-cel·lular* si cada peça connexa a $\Sigma \setminus [\mathcal{U} \cup \mathcal{P}]$ (eliminant els punts de la superfície pertanyents al graf) és homeomorfa a un disc obert 2-dimensional. Un *mapa* és un graf immers 2-cel·lularment en una superfície compacta i sense vora. Només considerarem superfícies orientables. Les peces homeomorfes a discs són les *cares* del mapa. Si el graf immers és un graf dirigit (o també dit graf orientat), aleshores podem emfatitzar aquest fet i parlar de *mapa dirigit* o *mapa orientat*; no usarem l'adjectiu si el context deixa clar si el graf immers és orientat o no.

A l'hora de representar els mapes sobre superfícies orientables de manera combinatòria és més còmode dividir les arestes del graf en «meitats d'aresta» o dards. Llavors, un graf es pot veure com un conjunt de vèrtexs V , un conjunt de dards D amb un nombre parell d'elements, una involució $\iota: D \rightarrow D$ sense punts fixos (ι^2 és la identitat) i una aplicació d'*incidència* $A: D \rightarrow V$. L'aplicació ι aparella els dards formant les arestes, i A ens indica a quin vèrtex hem d'adherir el dard. Si l'aresta és dirigida, signem els dards amb «+» o «-» de manera que a l'aresta (v_1, v_2) el dard incident a v_1 és negatiu (sur) i el dard incident a v_2 és positiu (entra). En el cas de mapes orientats, usem σ per denotar l'assignació de signes oposats als dos dards d'una aresta de manera que l'aresta del graf subjacent està dirigida del vèrtex incident al dard negatiu cap al vèrtex incident al dard positiu; per altra banda, una assignació de signes oposats als dos dards d'un mapa genera una orientació de les arestes del graf (del vèrtex incident al dard negatiu cap al vèrtex incident al dard positiu).

Donat el mapa M corresponent a una immersió del graf G a la superfície orientable Σ , podem usar l'orientació de Σ per induir un ordre cíclic dels dards (arestes) al voltant d'un vèrtex de G . Si retallem un disc suficientment petit centrat en un vèrtex de tal manera que el disc conté un únic tros de corba connex per a cada dard, aleshores l'orientació ens permet induir un ordre circular, seguint el sentit antihorari respecte a l'orientació positiva de la superfície, als dards incidents al vèrtex. Vegeu la figura 4. Podem identificar les cares de $\Sigma \setminus G$ amb la seqüència d'arestes en ordre circular que componen

la vora de la cara. Més concretament, podem identificar cada cara amb la seqüència de dards que la deixen a mà esquerra si recorrem la vora de la cara en sentit antihorari i si considerem que els dards tenen com a punt inicial el vèrtex al qual estan adherits. Vegeu la figura 4.

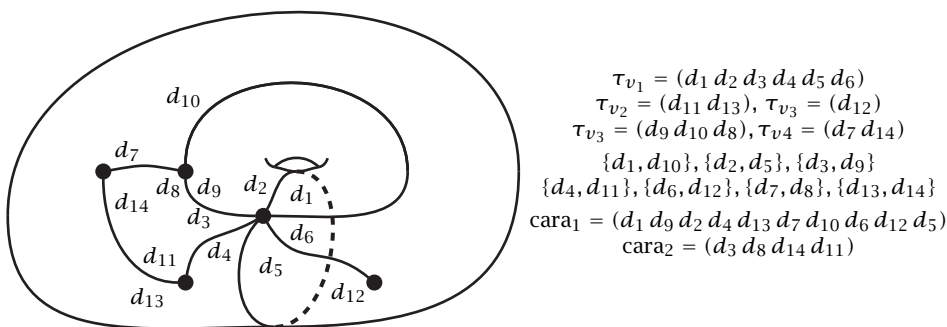


FIGURA 4: Mapa al tor.

Observem que podem revertir aquesta construcció: si per a cada vèrtex v de G donem un ordre cíclic als dards indicents a v , podem generar un mapa M que és la immersió del graf G en una superfície orientable. Codifiquem aquests ordres cíclics com els cicles en què descompon una permutació entre els dards $\tau: D \rightarrow D$: podem identificar els cicles de τ amb els vèrtexs de G . Definim les cares com la seqüència de dards $(d_1, \dots, d_k)$ tal que $d_i = \tau^{-1} \iota d_{i-1}$. És a dir, tenint el dard d_{i-1} , l'aplicació ι ens trasllada a la seva parella (a l'altra banda de l'aresta), i l'aplicació τ^{-1} ens dona l'anterior dard en l'ordre cíclic de dards al voltant del vèrtex corresponent. Si adherim discs a les arestes corresponents a la seqüència de dards que formen les cares esperant-ne l'ordenació, obtenim una superfície compacta sense vora. Vegeu la figura 5.

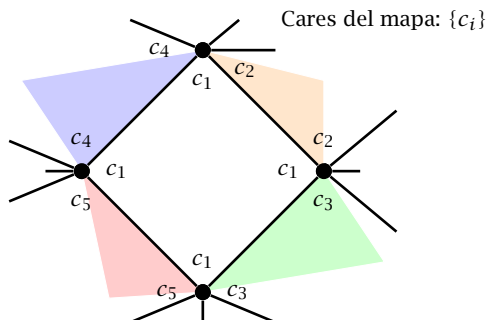


FIGURA 5: Cares d'un mapa.

Amb una mica d'imaginació podem veure que la superfície és orientable i el graf hi està immers 2-cel·lularment i induint el mateix ordre cíclic de les arestes al voltant dels vèrtexs que el donat per τ [8]. Dit d'una altra manera: la immersió de G a Σ determina unívocament un ordre cíclic τ i, a més a més,

la superfície generada per G i l'ordre cíclic τ és homeomorfa a Σ .⁷ El conjunt d'ordres cíclics de les arestes incidents a cada vèrtex s'anomena *sistema de rotacions*.

2.3 Codis de Gauss i mapes

Qualsevol codi o paràgraf de Gauss ens dona, de manera natural, un *graf enriquit* dirigit amb quatre arestes incidents a cada vèrtex, dues entrant i dues sortint. L'enriquiment prové de la informació respecte al camí que la paraula proporciona (en el cas d'un codi de Gauss, aquest camí és eulerià). Més concretament,

DEFINICIÓ 3 (GRAF I GRAF ENRIQUIT D'UN CODI DE GAUSS.). Sigui ω un codi (o un paràgraf) de Gauss no signat en n símbols $\{s_1, \dots, s_n\}$ i $2n$ lletres $\{l_1, \dots, l_{2n}\}$. El *graf de* ω és un graf dirigit 4-regular $\text{Gr}(\omega) = (V, E) = G$ on:

- $V(G)$ són els símbols de ω : $\{s_1, \dots, s_n\}$.
- Posem una (s_j, s_i) si s_i segueix s_j en l'ordre cíclic induït per ω . Més precisament, $E(G)$ és el conjunt d'arestes $\{(J(l_i), J(N(l_i)))\}_{i \in [2n]}$, on $J(\cdot)$ ens dona el símbol de la lletra l_i i $N(\cdot)$ ens dona la següent lletra de ω .

Enriquim el graf G aparellant, per a cada vèrtex s_0 , l'aresta (s_i, s_0) amb (s_0, s_j) si hi ha tres lletres l_1, l_2 i l_3 tals que $J(l_1) = s_i, J(l_2) = s_0, J(l_3) = s_j$ i $l_2 = N(l_1), l_3 = N(l_2)$. És a dir, les tres lletres són consecutives a ω .

EXEMPLE 4. El graf enriquit del codi de Gauss de la figura 6 ve donat pels vèrtexs $V = \{a, b, c, d\}$, les arestes

$$E = \{(a, b), (b, c), (c, d), (d, b), (b, a), (a, d), (d, c), (c, a)\} = \{e_0, e_1, \dots, e_7\}$$

i l'aparellament $\{e_i, e_{i+1}\}$ amb $i \in [0, 7]$ i índexs mòdul 8.

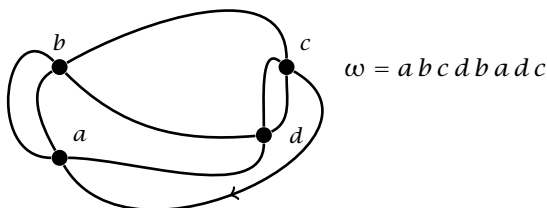


FIGURA 6: Corba representable al pla.

⁷ Si volem considerar mapes en superfícies compactes no orientables, aleshores ho podem fer usant *banderes*, o quarts d'aresta; cada aresta és vista com un rectangle amb un costat més llarg, i les banderes són les quatre cantonades. Tenim un parell de banderes adjuntes a cada vèrtex (és d'un costat curt), un ordre cíclic de les arestes al voltant de cada vèrtex, i un parell d'involucions sense punts fixos: una que intercanvia les dues banderes associades a cada vèrtex (aparella les cantonades dels costats curts) i la que intercanvia els parells associats als dos vèrtexs que conformen l'aresta (intercanvia els parells d'arestes segons el costat llarg del rectangle).

Si el codi o paràgraf de Gauss està signat, aleshores tenim un mapa amb les arestes dirigides de la manera següent:

DEFINICIÓ 5 (MAPA D'UN CODI (PARÀGRAF) DE GAUSS SIGNAT). El mapa del codi de Gauss signat ω^+ , $\text{Gs}(\omega^+) = (V, E)$ ve definit pel graf del codi de Gauss sense signar amb el següent sistema de rotacions τ :

- Si ω^+ és

$$(\dots s_1 [+s_0] s_2 \dots s_3 s_0 s_4 \dots) \quad \text{o bé} \quad \begin{cases} (\dots s_1 [+s_0] s_2 \dots) \\ (\dots s_3 s_0 s_4 \dots) \end{cases}$$

(el punt de tall s_0 és positiu), aleshores al voltant de s_0 hi tenim els dards ordenats cíclicament

$$(d_{s_1}^+, d_{s_4}^-, d_{s_2}^-, d_{s_3}^+),$$

on $d_{s_i}^\pm$ és el dard amb l'altre extrem de l'aresta a s_i i signat $\pm$. Vegeu la figura 2 o la part esquerra de la figura 14.

- Si ω^+ és

$$(\dots s_1 s_0 s_2 \dots s_3 + s_0 s_4 \dots) \quad \text{o bé} \quad \begin{cases} (\dots s_1 s_0 s_2 \dots) \\ (\dots s_3 + s_0 s_4 \dots) \end{cases}$$

(el tall s_0 és negatiu), aleshores al voltant de s_0 hi tenim els dards ordenats cíclicament

$$(d_{s_1}^+, d_{s_3}^+, d_{s_2}^-, d_{s_4}^-),$$

on $d_{s_i}^\pm$ és el dard amb l'altre extrem de l'aresta a s_i i signat $\pm$. Vegeu la figura 2 o la part esquerra de la figura 14.

EXEMPLE 6. El codi de Gauss signat de la figura 6 és

$$[+a] [-b] [-c] [+d] [+b] [-a] [-d] [+c]$$

i el mapa $\text{Gs}(\omega^+)$ ve donat pels vèrtexs $V = \{a, b, c, d\}$, les arestes

$$E = \{(a, b), (b, c), (c, d), (d, b), (b, a), (a, d), (d, c), (c, a)\},$$

on l'aresta (i, j) genera el dard $d_{i \rightarrow j}^-$ incident al vèrtex i i $d_{i \rightarrow j}^+$ incident al vèrtex j i el sistema de rotacions ve donat per les permutacions cícliques

$$\begin{cases} a \rightarrow (d_{b \rightarrow a}^+, d_{c \rightarrow a}^+, d_{a \rightarrow d}^-, d_{a \rightarrow b}^-), \\ b \rightarrow (d_{a \rightarrow b}^+, d_{d \rightarrow b}^+, d_{b \rightarrow c}^-, d_{b \rightarrow a}^-), \\ c \rightarrow (d_{b \rightarrow c}^+, d_{d \rightarrow c}^+, d_{c \rightarrow d}^-, d_{c \rightarrow a}^-), \\ d \rightarrow (d_{a \rightarrow d}^+, d_{c \rightarrow d}^+, d_{d \rightarrow c}^-, d_{d \rightarrow b}^-). \end{cases}$$

La signatura dels dards de la definició 5 és compatible amb l'orientació de les arestes del graf descrit a la definició 3. L'enriquiment ens indica quina de les quatre arestes incidents amb el vèrtex correspon a «seguir recte»; a la permutació dels quatre dards al voltant del vèrtex, seguir recte després del dard d correspon al dard que no és ni $\iota(d)$ ni $\tau^{-1}(\iota(d))$.

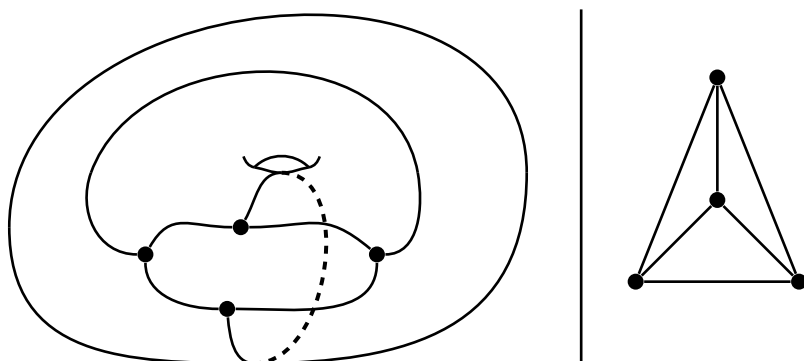


FIGURA 7: Graf complet en 4 vèrtexs al tor i al pla.

Donat un mapa, el conjunt de cares dona lloc a una partició del conjunt de dards i cada cara es pot trobar fàcilment com la seqüència $(d, \tau^{-1}(\iota(d)), [\tau^{-1}(\iota)]^2(d), \dots)$. Llavors, podem trobar, de manera senzilla, el nombre de cares en un nombre d'operacions lineal en el nombre d'arestes del mapa. Amb la fórmula d'Euler

$$\text{vèrtexs} - \text{arestes} + \text{cares} = 2 - 2 \text{ gènere}$$

podem determinar el gènere de la superfície on el codi de Gauss signat està immers. Així doncs, determinar si un codi de Gauss signat prové d'un nus és equivalent a comprovar que aquest gènere és zero, i això es pot determinar en temps lineal en el nombre de símbols de la paraula.⁸

2.4 Un mapa per un codi de Gauss sense signe

Com hem vist a la figura 3 i a l'equació (1), diferents signatures d'un codi de Gauss sense signe ens poden donar diferents superfícies. En particular, l'ordre cíclic de les arestes del graf introduït a la definició 3 no està determinat. Per això el problema de determinar si un codi de Gauss no signat prové d'un nus és, en principi, més complicat de resoldre. Per posar-ho en el context de la secció anterior, podem reformular la qüestió 1 de la manera següent:

⁸ Suposant que, donats un vèrtex u i una aresta adjacent $a = (u, v)$, podem accedir a la informació del vèrtex v en temps constant, i a les arestes següent i anterior a a en temps constant.

QÜESTIÓ 2 (PROBLEMA DE GAUSS, EQUIVALENT). *Donat un codi de Gauss (no signat) ω , hi ha alguna manera de signar-lo per tal que el mapa que indueix (el codi de Gauss signat) sigui pla?*

Donat que podem examinar les 2^n possibles maneres de signar la paraula en n símbols de manera exhaustiva, i que podem determinar si és un mapa pla o no en un nombre d'operacions lineal en n , podem resoldre la qüestió 2 i, per tant, la qüestió 1 usant força bruta en un nombre d'operacions de l'ordre de $n2^n$. La qüestió interessant algorítmicament és, doncs, la de donar una resposta positiva o negativa en substancialment menys operacions que $Cn2^n$, on C és una constant. Com veurem, podrem determinar si un codi de Gauss és realitzable al pla en temps lineal en n , que és el mateix ordre que determinar si un codi de Gauss signat és pla.

2.5 Diagrama de cordes d'un codi de Gauss i el seu graf d'intersecció

Denotem per $[2n]$ el conjunt $\{1, 2, \dots, 2n\}$ i per $\binom{[2n]}{2}$ el conjunt de parelles $\{a, b\}$ amb $a, b \in [2n]$ i $a \neq b$. Un *diagrama de cordes* en $2n$ punts $v_1, \dots, v_{2n}$ és un graf format pels vèrtexs $v_1, \dots, v_{2n}$ i pel conjunt d'arestes $\{(v_i, v_{i+1 \pmod{2n}}) : i \in [2n]\}$ anomenat *la vora del diagrama*, juntament amb un *aparellament perfecte* (un conjunt d'arestes $\{(v_i, v_j)\}_{(i,j) \in \binom{[2n]}{2}}$ tal que cada v_i apareix exactament un cop en alguna de les arestes de l'aparellament). Vegeu la figura 8.

Un codi de Gauss $\omega = l_1 \dots l_{2n}$ genera un diagrama de cordes de manera natural amb vèrtexs $\{l_1, \dots, l_{2n}\}$, vora $\{(l_i, l_{i+1 \pmod{2n}}) : i \in [2n]\}$, i on l'aparellament perfecte ve donat pel parell de lletres amb el mateix símbol.

La manera estàndard de dibuixar un diagrama de cordes és disposar els $2n$ punts al cercle pla, de tal manera que el cercle dibuixa les arestes de la vora i l'aparellament perfecte es dibuixa a l'interior. El *graf d'intersecció* I d'un diagrama de cordes C és el graf que té un vèrtex per a cada aresta de l'aparellament, i dos vèrtexs a I són adjacents si les respectives arestes es tallen a C . Vegeu la figura 8.

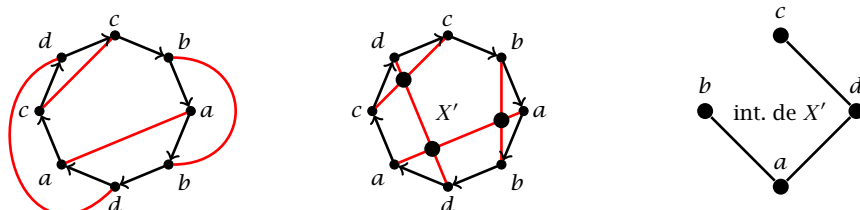


FIGURA 8: Exemple de diagrama de cordes, mateix diagrama de cordes amb les interseccions remarcades, i graf d'intersecció del diagrama de cordes anterior.

Passem a demostrar una relació entre un diagrama de cordes i el seu graf d'intersecció, que ens serà d'utilitat i que podem trobar a [21].

PROPOSICIÓ 7. *Sigui X un diagrama de cordes, aleshores*

X és planar $\iff$ el graf d'intersecció de X és un graf bipartit.

PROVA. En qualsevol immersió plana d'un diagrama de cordes planar, la vora del diagrama de cordes forma una corba tancada sense autointerseccions; les cordes de l'aparellament han de passar per l'exterior o l'interior d'aquesta. Donat que cap aresta es talla, les arestes de l'interior no es tallen dues a dues, ni les de l'exterior es tallen dues a dues.

Així doncs, al graf d'intersecció, els vèrtexs corresponents a les arestes interiors del diagrama de cordes formen un conjunt *independent* (sense arestes entre els vèrtexs, ja que les corresponents arestes no es tallen), i el mateix passa amb les arestes exteriors. Així doncs, totes les arestes del graf d'intersecció apareixen entre arestes de l'interior i de l'exterior en un mapa pla del diagrama de cordes.

Aquest argument és reversible: si dos conjunts de vèrtexs independents donen lloc a una partició dels vèrtexs del graf d'intersecció d'un diagrama de cordes, aleshores dibuixant unes arestes a l'interior i les altres a l'exterior de la vora del diagrama, obtenim un mapa al pla (sense punts de tall entre les arestes del diagrama de cordes). Notem que dibuixem la vora del diagrama de cordes com un polígon regular al pla. $\square$

3 Desfer el nus

Quan tenim un diagrama pla d'un nus i un punt de tall s , podem «desfer» o «resoldre» s de dues maneres diferents. Vegeu la figura 9. Aquestes formes de resoldre'l estan relacionades amb les maneres que tenim per sortir de l'encreuament que representa el punt de tall:

- (i) Seguir el camí que marca la corba. Prenem el camí que «surt» del punt de tall sense canviar la direcció. (Aquí no fem res i, per tant, no desfem el punt de tall.)
- (ii) Mantenir el sentit però canviant de direcció. Prenem l'altre camí que «surt» del punt de tall i que no és seguint la corba.
- (iii) Canviant la direcció i el sentit del camí. Prenent l'altre camí que «entra» al punt de tall, canviant el sentit del tram corresponent de corba (fins que tornem a trobar el mateix punt de tall).

Tant en el cas (ii) com en el (iii), si ens aturem just abans d'arribar al punt de tall i prenem una petita drecera cap a la branca que canvia de direcció, aleshores eliminem el punt de tall (vegeu com la figura central a la figura 9 es transforma en les figures laterals sense el punt de tall). Així, en aplicar (ii) o (iii) al punt de tall s , podem dir que les corbes «es toquen» a s sense tallar-se, o bé que es tallen tangencialment a s , o bé que hem desfet el punt de tall s .

Si tenim un codi de Gauss

$$\omega = Xs_1s_0s_2Ys_3s_0s_4Z,$$

on X , Y i Z són paraules, i considerem el punt de tall s_0 , aleshores l'efecte d'aplicar (i) deixa la paraula invariant. Si apliquem (ii), ω es transforma en el paràgraf

$$\begin{cases} Xs_1s_4Z \\ s_2Ys_3 \end{cases}$$

i s_0 ha desaparegut: l'hem «desfet» o «resolt».

Si fem el canvi (iii), obtenim la paraula

$$Xs_1s_3\bar{Y}s_2s_4Z,$$

on $\bar{Y}$ denota la paraula Y amb les lletres en ordre invertit: $\overline{abc\dots t} = t\dots cba$. En aquest cas, hem canviat el sentit dels trams de corba entre les lletres de Y .

En els casos (ii) i (iii), i degut al fet que ens interessarà de reconstruir o desfer aquestes operacions, usarem

$$\begin{cases} Xs_1s'_0s_4Z \\ s''_0s_2Ys_3 \end{cases} \quad \text{o bé} \quad Xs_1s'_0s_3\bar{Y}s_2s''_0s_4Z$$

per denotar que els nous codis de Gauss comparteixen el punt de tall s_0 i denotar la seva localització abans de desfer el tall. Considerem que s'_0 i s''_0 són dos punts de la corba (o les corbes) diferents del pla que ja no són punts de tall; alternativament, podem considerar que s'_0 i s''_0 és un punt d'intersecció on les corbes es tallen tangencialment i no es creuen (es besen).

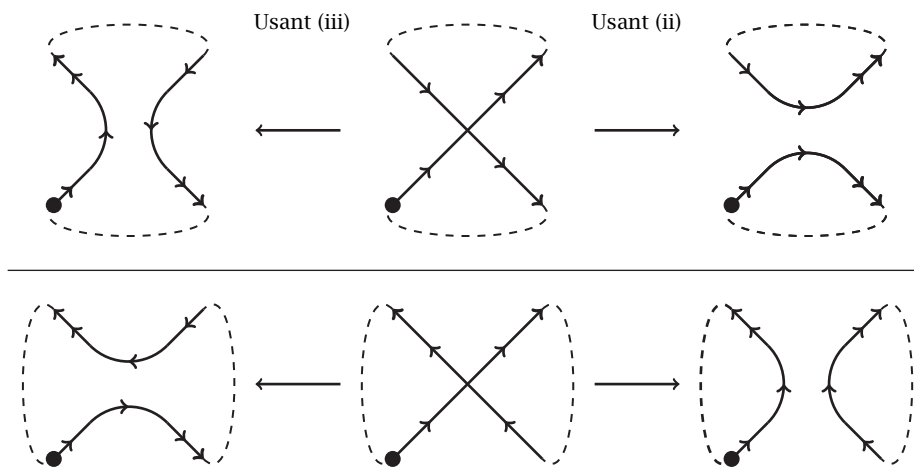


FIGURA 9: «Simplificació» del codi de Gauss: eliminem encreuaments i donem informació alternativa amb la qual recuperar-los.

3.1 Refer els punts de tall

Per tal d'invertir l'operació (ii) cal que la part de la corba que passa per s'_i i la que passa per s''_i tinguin sentits congruents. Per tal de desfer (iii) cal que la part de la corba que passa per s'_i i la que passa per s''_i tinguin sentits oposats. Vegeu la figura 9.

Com que l'operació (ii) no canvia el sentit de cap tram de corba, sempre podem invertir aquesta operació. Per altra banda, l'operació (iii) canvia el sentit d'un dels trams de corba entre els dos cops que passa pel punt de tall. Això fa que, si apliquem primer l'operació al punt de tall s_0 i després a s_1 , pot succeir que no puguem revertir l'operació a s_0 si no revertim abans l'operació a s_1 . Vegeu la figura 10. Aquest punt serà important a la secció 4.

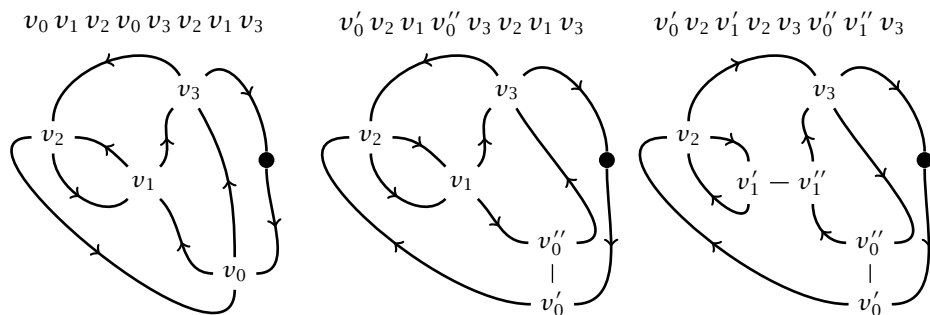


FIGURA 10: Si resoltem primer v_0 i després v_1 , aleshores no podem desfem la resolució de v_0 si no desfem abans la de v_1 .

3.2 Desfent els punts de tall

Un cop presentades les operacions (ii) i (iii) és natural preguntar-se què passa si desfem seqüencialment (seguint un ordre a l'atzar o el criteri preferit del lector) tots els punts de tall usant el mateix criteri ((ii) o (iii)).

Canviant el sentit i la direcció: aplicant (iii). Aplicant un cop (iii) a un codi de Gauss representat per γ obtenim una altra corba. És clar que el resultat final d'aplicar sempre el criteri (iii) serà una nova corba sense punts de tall γ' (vegeu la part esquerra de la figura 9 o la figura 10). Si γ és al pla, aleshores γ' també serà al pla, és a dir, γ' és una circumferència deformada al pla. Si en desfem els nusos deformem la corba el mínim possible i mantenim els nous punts s'_i i s''_i propers al punt de tall original s_i , aleshores podem connectar s'_i i s''_i amb una corda addicional sense obtenir nous punts de tall.

Així, si la corba original induïa un mapa pla, obtenim un diagrama de cordes que és un graf planar (les arestes de l'aparellament perfecte poden ser dibuixades per dins o per fora de la vora del diagrama de cordes).

Observem que l'ordre en què hem processat els vèrtexs és rellevant ja que determinarà l'ordre cíclic dels vèrtexs de la vora del diagrama de cordes. A més, si primer desfem s_0 i després s_1 , pot succeir que no puguem refer s_0

immediatament (vegeu la figura 10 amb $s_0 = v_0$ i $s_1 = v_1$). Al teorema 8 veurem que, partint del cercle pla amb tots els talls desfets i imposant la condició de Gauss, podrem refer els punts de tall en ordre invers a com els hem desfet, i així obtenim la caracterització.

Canviant la direcció però no el sentit: aplicant (ii). Si apliquem (ii) consistentment als diferents punts de tall a γ una corba al pla, aleshores el conjunt de corbes tancades resultants també és al pla i no es tallen (ni entre corbes diferents ni una corba amb si mateixa). Així, cada corba és un (homeomorf a un) cercle i determina dues cares del pla, la interior i l'exterior. Efectivament, a cada pas, reduïm el nombre de punts de tall totals en una unitat (sempre que s'_i i s''_i siguin propers a s_i no creem nous punts de tall en resoldre s_i).

Com que l'orientació de les arestes de la corba original no canvia, sempre podem recrear qualsevol punt de tall original s_i i mantenir el conjunt de corbes al pla. A més, els cercles resultants tenen una orientació congruent a s'_i i s''_i : els dos cercles giren en el mateix sentit i estan «engranats» com els engranatges d'un rellotge. Aquests cercles reben el nom de *cercles de Seifert* [35], que els va usar per construir una superfície on la vora coincideix amb un nus donat qualsevol. Els cercles de Seifert depenen només del codi de Gauss (la paraula) i no de la seva possible realització plana (vegeu la subsecció 5.1).

El fet que els cercles de Seifert poden ser al pla si el codi de Gauss és realitzable, juntament amb el fet que han d'estar engranats, permet la caracterització donada al teorema 16 i al teorema 17.

4 Girant la primera cantonada

En aquesta secció seguirem l'excel·lent presentació de Godsil i Royle [21] de la caracterització dels codis de Gauss representables de Dehn [5] i refinada per Read i Rosenstiehl [29, 30, 32].

TEOREMA 8 (CARACTERITZACIÓ DELS CODIS DE GAUSS). *Sigui ω un codi de Gauss i ω' el codi de Gauss obtingut de ω capgirant les lletres entre qualsevol parell de lletres del mateix símbol, seqüencialment, en qualsevol ordre (aplicant (iii)). Aleshores, el codi de Gauss ω és realitzable al pla si i només si:*

- (a) *entre cada parell de lletres del mateix símbol hi ha un nombre parell de lletres, i*
- (b) *el diagrama de cordes de ω' és planar.*

Equivalentment:

- (a') *tots els vèrtexs del graf d'intersecció del diagrama de cordes de ω tenen grau parell, i*
- (b') *el graf d'intersecció del diagrama de cordes de ω' és bipartit.*

PROVA. Denotem els símbols per $s_1, \dots, s_n$ i suposarem que els processem, usant (iii), seguint l'ordre creixent en el subíndex. Usarem $t_0, \dots, t_{n-1}$ per denotar símbols genèrics, no necessàriament en l'ordre $s_1, \dots, s_n$.

Si ω és realitzable al pla, aleshores (b) se satisfà. Si

$$\omega = \dots t_1 s_1 t_2 \dots t_3 s_1 t_4 \dots$$

és un codi de Gauss realitzable, i γ una corba que el realitza, aleshores si desfem el punt de tall s_1 usant (iii) generem dos punts nous s'_1, s''_1 i trams de corba $t_1 s'_1 t_3$ i $t_2 s_1 t_4$. Si s'_1 i s''_1 són propers a s_0 al pla, aleshores podem afegir una corda entre s'_1 i s''_1 sense crear cap punt de tall addicional. Repetint aquest procés seqüencialment obtenim la nova paraula ω' que té, per diagrama de cordes, el mapa obtingut mitjançant l'addició de les cordes entre s'_i i s''_i . Aquest diagrama és pla ja que hem desfet tots els punts de tall i no n'hem creat de nous en afegir les cordes.

Si ω és realitzable al pla, aleshores (a) se satisfà. Veure aquesta part és equivalent a veure la proposició 2. A γ les dues lletres amb el mateix símbol a generen una subcorba tancada.

Si entre les dues còpies de a no hi ha símbols repetits, aleshores el tram no té autointerseccions i podem aplicar el teorema de la corba tancada de Jordan. El tram tancat de corba divideix el pla en dues regions, la resta de la corba s'inicia i finalitza en la mateixa regió, de manera que cada cop que entrem a l'altra regió, n'hem de sortir. Com que cada cop que entrem a la regió o en sortim això correspon a un punt de tall del tram de corba, el nombre de talls (que correspon al nombre de lletres entre les dues còpies del símbol a) és parell.

Si entre dues còpies de a hi ha símbols repetits, usem inducció en el nombre de parelles repetides niades. Si

$$\omega = \dots t_0 X_0 t_1 X_2 \dots t_i X_i t_i Y_{i-1} t_{i-1} \dots t_1 Y_0 t_0 \dots,$$

on $t_0, t_1, \dots, t_i$ són els símbols niats, aleshores les subcorbes

$$t_0 X_0 t_1 Y_0 (t_0)$$

$$t_1 X_1 t_2 Y_1 (t_1)$$

$$\vdots$$

$$t_i X_i (t_i)$$

formen $i + 1$ corbes tancades que no s'autointersequen (tot i que dues a dues sí es poden interseçar). Aquestes corbes es troben aplicant l'operació (ii) de desfer nusos als punts de tall $t_0, \dots, t_i$. Si a cada cercle apliquem el resultat de la corba tancada de Jordan i tenim en compte que quan dos cercles s'intersequen ho han de fer un nombre parell de vegades, obtenim el resultat desitjat (en aquest cas entre les dues còpies de t_0).

La condició (a) i la condició (a') són equivalents. Amb aquesta demostració quedarà establerta l'equivalència entre les condicions (a) + (b) i (a') + (b') ja que l'equivalència entre les condicions (b) i (b') prové de la proposició 7. Cada parell

de lletres de ω del mateix símbol s_1 divideix la paraula en dues parts A_1 i A_2 . Llavors, dues còpies del símbol s_i estan a diferents parts si i només si s_1 i s_i són adjacents al graf d'intersecció de ω . (L'aresta s_j del diagrama de cordes no creua l'aresta s_1 quan els símbols estan niats; vegeu a la figura 8 arestes de a i de c .) Per tant, cada vèrtex del graf d'intersecció té grau parell si i només si el nombre de lletres entre cada parell de lletres del mateix símbol és parell.

Les condicions (a') i (b') sobre ω impliquen que ω és realitzable al pla. Un cop hem vist l'equivalència entre els dos parells de condicions, resta veure la implicació que manca. La paraula $\omega' = \omega_n$ s'ha obtingut de $\omega = \omega_0$ capgirant successivament les lletres entre les ocurrences de $s_1, \dots, s_n$. En general, denotem per ω_i la paraula obtinguda de ω_0 capgirant les lletres (aplicant l'operació de desfer punts de tall (iii)) entre $s_1, \dots, s_i$. L'estratègia consisteix a, partint d'una immersió plana del diagrama de cordes de $\omega' = \omega_n$, que denotem per $X' = X_n$, refer els punts de tall corresponents a $s_n, \dots, s_1$ en ordre invers a com hem tractat els símbols a ω , fins a obtenir una corba al pla. Cal veure, doncs, que, per a cada $i = n, n-1, \dots, 1$, si hem refet els punts de tall $s_n, \dots, s_{i+1}$, aleshores podem refer el tall s_i .

Denotem per X_i el diagrama de cordes de ω_i . Denotem per M_i , $i = n, n-1, \dots, 1, 0$, el mapa obtingut de refer el tall s_{i+1} a M_{i+1} . En particular, M_n és el mapa associat al diagrama de cordes X_n . La taula 1 (parcialment il·lustrada a la figura 11) resumeix els diferents tipus de talls entre les cordes relacionades amb s_{i+1} i dues cordes genèriques s_t i s_j abans i després d'aplicar (iii): si s_j i s_{i+1} no es tallen, aleshores la relació de tall entre s_j i s_t no canvia en capgirar s_{i+1} ; si s_j i s_{i+1} es tallen, aleshores s_j i s_t canvien el seu estat de tall segons si s_t talla s_{j+1} o no. De la taula 1 en deduirem les afirmacions (2), (3), (4) descrites més avall.

Tall (s_j, s_{i+1}) a X_i i X_{i+1}	Tall (s_t, s_{i+1}) a X_i	Tall (s_t, s_j) a X_i	$\Rightarrow$	Tall (s_t, s_{i+1}) a X_{i+1}	Tall (s_t, s_j) a X_{i+1}
s_j talla s_{i+1}	i	s_t talla s_{i+1} i s_t no talla s_{i+1}	$\Rightarrow$	s_t talla s_{i+1} i s_t no talla s_{i+1}	s_t no talla s_j i s_t talla s_j
s_j no talla s_{i+1}	i	s_t talla s_j i s_t no talla s_j	$\Rightarrow$	s_t talla s_j i s_t no talla s_j	s_t no talla s_j i s_t talla s_j

TAULA 1: Taula resum de l'efecte de desfer el punt de tall s_{i+1} de X_i a X_{i+1} .

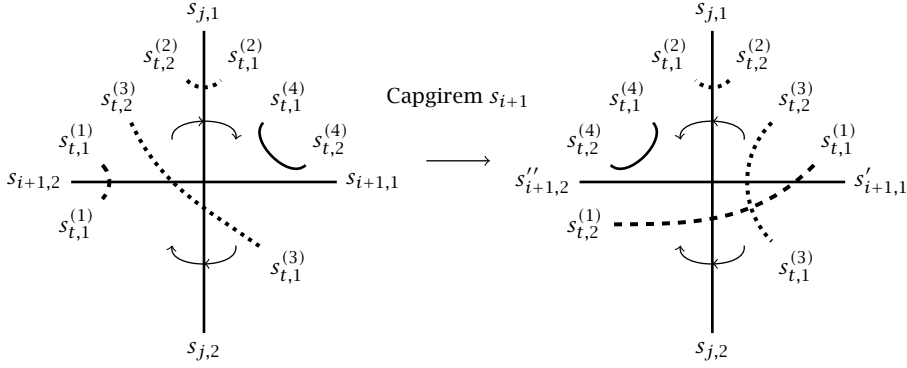


FIGURA 11: Il·lustració de la taula 1.

$$\left. \begin{array}{l} \text{A } X_i, \text{ l'aresta } s_{i+1} \text{ es talla amb} \\ \text{un nombre parell d'arestes d'entre } \{s_{i+2}, \dots, s_n\}. \end{array} \right\} \quad (2)$$

Veurem (2) mitjançant un argument inductiu en i més restrictiu: tot s_j amb $j \geq i+1$ talla un nombre parell d'arestes d'entre $\{s_{i+2}, \dots, s_n\}$ a X_i . El cas $i=0$ és cert per la condició de Gauss. Suposem, doncs, que s_j talla un nombre parell d'arestes a $\{s_{i+1}, \dots, s_n\}$ al diagrama de cordes X_i de ω_i i dividim l'argument en dos petits casos:

Si s_j no talla s_{i+1} , aleshores, usant la taula 1, s_j talla s_t amb $t \geq i+2$ a X_{i+1} si i només si s_j talla s_t a X_i . La hipòtesi d'inducció fa la resta.

Si s_j talla s_{i+1} , aleshores S denota el conjunt d'arestes d'entre $\{s_{i+2}, \dots, s_n\} \setminus \{s_j\}$ que talla s_{i+1} . De la hipòtesi d'inducció deduïm que un nombre parell d'arestes d'entre $\{s_{i+2}, \dots, s_n\}$ talla s_{i+1} . Per tant, $|S|$ és senar. Per la taula 1, la paritat del conjunt d'arestes d'entre S que talla a s_j a X_i i a X_{i+1} és diferent. Això darrer, afegit al fet que les arestes que talla s_j d'entre $\{s_{i+2}, \dots, s_n\} \setminus \{s_j\}$ és el mateix a X_i i a X_{i+1} , que s_j talla s_{i+1} , i que hi ha un nombre parell d'arestes que tallen s_j d'entre $\{s_{i+1}, \dots, s_n\}$ a X_i (per la hipòtesi d'inducció), fa que el nombre d'arestes que tallen s_j d'entre $\{s_{i+2}, \dots, s_n\}$ a X_{i+1} sigui també parell.

Resseguint l'argument de (2) veiem també (3) i (4).

$$\left. \begin{array}{l} \text{Si } s_j \text{ no talla } s_{i+1} \text{ al diagrama de cordes } X_i \text{ de } \omega_i, \\ \text{aleshores la paritat del nombre de talls de } s_j \text{ amb} \\ \text{les arestes } \{s_{i+1}, s_{i+2}, \dots, s_n\} \text{ a } X_i \text{ és el mateix que} \\ \text{la paritat del nombre de talls entre } s_j \text{ amb} \\ \text{les arestes } \{s_{i+2}, \dots, s_n\} \text{ a } X_{i+1}. \end{array} \right\} \quad (3)$$

$$\left. \begin{array}{l} \text{Si } s_j \text{ talla } s_{i+1} \text{ al diagrama de cordes } X_i \text{ de } \omega_i, \text{ i } j < i+1, \\ \text{aleshores la paritat del nombre de talls de } s_j \text{ amb} \\ \text{les arestes } \{s_{i+1}, s_{i+2}, \dots, s_n\} \text{ a } X_i \text{ és diferent de} \\ \text{la paritat del nombre de talls entre } s_j \text{ amb} \\ \text{les arestes } \{s_{i+2}, \dots, s_n\} \text{ a } X_{i+1}. \end{array} \right\} \quad (4)$$

Començant a refer els talls a X_n de $\omega_n = \omega'$ observem que, si podem refer i refem el tall s_j , i l'aresta de s_i talla la de s_j amb $i < j$ a X_j , aleshores el sentit relatiu entre les branques de la corba a s'_i i s''_i canvia. Alhora, la paritat del nombre d'arestes que s_i talla a X_{j-1} d'entre $\{s_j, \dots, s_n\}$ canvia respecte del nombre d'arestes d'entre $\{s_{j+1}, \dots, s_n\}$ que s_i talla a X_j . Com que comencem amb un nombre parell de talls, 0, els sentits són oposats per a tots els s_i (comencem amb una corba tancada sense talls al pla), i canviem de paritat un nombre parell de cops (el nombre de talls de s_i a X_i entre $\{s_{i+1}, \dots, s_n\}$ és parell), el nombre de canvis de sentit és parell i, per tant, com que hem començat amb orientacions oposades, quan volem refer el tall s_i aquest tindrà orientacions oposades. Per tant, podrem refer tots els talls i obtenim una representació de $\omega_0 = \omega$ al pla. Això conclou la demostració. $\square$

Si volem implementar un algoritme de reconeixement i/o construcció de la representació plana hem de:

- Veure si la condició de Gauss es compleix.
- Capgirar les lletres entre les parelles de símbols per obtenir ω' .
- Determinar si el diagrama de cordes de ω' és planar.

El primer punt es pot determinar en temps lineal recurrent ω un cop tot portant el compte del nombre d'elements entre cada parell de lletres. Trobar el diagrama de cordes de ω' es pot aconseguir en temps lineal en el nombre de símbols, així com determinar-ne la planaritat (podem usar el resultat general de Hopcroft i Tarjan [23]). Ara bé, capgirar les lletres entre totes les parelles de símbols pot tenir, en general, un cost quadràtic en el nombre de símbols. Tot i això, tal com s'explica a Rosenstiehl i Tarjan [33], es pot modificar lleugerament l'algoritme que es dedueix de la caracterització per tal d'obtenir la construcció de la representació plana en temps lineal en el nombre de símbols.⁹

5 Girant la segona cantonada

En aquesta secció veurem que també podem usar el resultat de processar tots els punts de tall usant (ii) per tal de caracteritzar els codis i paràgrafs de Gauss realitzables al pla.

5.1 Cercles de Seifert i propietats

DEFINICIÓ 9 (CERCLES DE SEIFERT). Sigui ω un codi o paràgraf de Gauss i Ω el seu graf enriquit. Aleshores la seqüència cíclica d'arestes dirigides $(e_1, \dots, e_t)$ és un *cercle de Seifert* de ω si

- $(e_1, \dots, e_t)$ forma un cicle dirigit i tancat a Ω . És a dir, $e_i = (v_i, v_{i+1 \pmod{t}})$, amb $i \in [t]$.

⁹ Rosenstiehl i Tarjan [33] també donen un algoritme específic per veure la planaritat d'un diagrama de cordes que resulta més senzill que el general de Hopcroft i Tarjan [23].

- Per a cada i , l'aresta

$$e_{i+1 \pmod t} = (v_i, v_{i+1 \pmod t})$$

és l'aresta que no segueix

$$e_i = (v_{i-1 \pmod t}, v_i)$$

en el camí induït per ω .

Alternativament,

- La seqüència de símbols de ω en ordre cíclic $(s_1, \dots, s_t)$ forma un cercle de Seifert C_i si s_i és el següent vèrtex després d'usar (ii) per resoldre el punt de tall s_{i-1} .

EXEMPLE 10. Els cercles de Seifert del codi de Gauss de la figura 12 són les seqüències d'arestes

$$\begin{cases} ((a, b), (b, a)), \\ ((b, c), (c, a), (a, d), (d, b)), \\ ((c, d), (d, c)), \end{cases}$$

o les seqüències de vèrtexs

$$\begin{cases} a b, \\ a d b c, \\ c d. \end{cases}$$

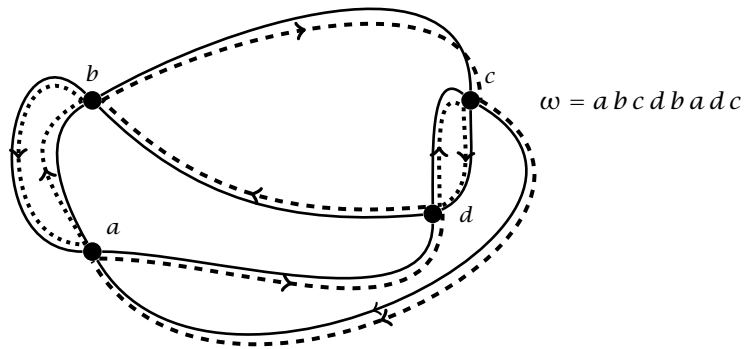


FIGURA 12: Corba representable al pla.

Observem que la següent aresta a cada cercle de Seifert està definida de manera única si el graf prové d'un codi o paràgraf de Gauss no signat. Per tant, els cercles de Seifert descomponen les arestes del graf de ω en cicles dirigits tancats $C_1, \dots, C_r$. Denotem per C el conjunt de cercles de Seifert.

DEFINICIÓ 11 (GRAF I MAPA DE SEIFERT D'UN PARÀGRAF DE GAUSS). Sigui Ω el graf enriquit d'un codi (o paràgraf) de Gauss ω , aleshores $\text{Sf}(\Omega) = \text{Sf}(\omega)$ és el *mapa de Seifert* $M = (V, D)$ amb:

- $V(M)$ és el conjunt de cercles de Seifert, $\{C_1, \dots, C_r\}$.
- Hi ha un dard d per cada lletra de ω . És a dir, $|D| = 2n$. Dos dards formen una aresta si les respectives lletres comparteixen símbol.
- Si el cercle C_i està format per l'ordre cíclic de lletres $(l_1, \dots, l_t)$, aleshores el dard d_{l_j} associat a la lletra l_j , $j \in \{1, \dots, t\}$, és incident al vèrtex C_i i l'ordre cíclic dels dards al voltant de C_i és $(d_{l_1}, \dots, d_{l_t})$.

Una signatura ω^+ de

$$\omega = \dots l_1 l_0 l_2 \dots l_3 l'_0 l_4 \dots,$$

on l_0 i l'_0 tenen el mateix símbol s_0 , orienta les arestes de $\text{Sf}(\omega)$ de la manera següent (vegeu la figura 14 per al cercle de Seifert i la figura 2 per al signe/orientació del punt de tall):

- Si ω^+ signa s_0 positivament (+), aleshores l'aresta de s_0 va de C_1 a C_2 .
- Si ω^+ signa s_0 negativament (−), aleshores l'aresta de s_0 va de C_2 a C_1 .

Vegeu la figura 13 com un exemple d'un mapa de Seifert d'un codi de Gauss.

$$C(\omega) = \{\{a, b\}, \{a, d, b, c\}, \{c, d\}\}$$

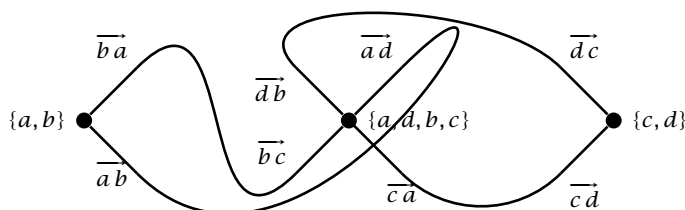


FIGURA 13: Mapa de Seifert de $\omega = a b c d b a d c$.

DEFINICIÓ 12 (MAPA VÈRTEX MEDIAL). Si M és un mapa orientat per σ , aleshores $\text{Mv}(M, \sigma)$, o el *mapa vèrtex medial* és un mapa orientat 4-regular amb:

- Els vèrtexs de $\text{Mv}(M, \sigma)$ són les arestes de M .
- Les arestes de Mv són les cordes entre els dards de M seguint la rotació τ . Això és:

Per cada dard d de M , $\text{Mv}(M, \sigma)$ té dos dards: d^- i d^+ , el de sortida de d i el d'entrada a d .

Els dards de sortida estan orientats amb $-$ i els d'entrada amb $+$ a $\text{Mv}(M, \sigma)$.

El dard d^- està aparellat amb el d'entrada a $\tau(d)$: $\iota_{\text{Mv}(M, \sigma)}(d^-) = \tau_M(d)^+$.

- Si $\{d_1, \iota(d_1) = d_2\}$ és una aresta de M amb $\sigma(d_1) = -1$ i $\sigma(d_2) = +1$ (orientada de d_1 a d_2), aleshores el vèrtex associat a $\{d_1, d_2\}$ a Mv té la rotació

$$([\tau^{-1}(d_2)]^+, [\tau^{-1}(d_1)]^+, [\tau(d_1)]^-, [\tau(d_2)]^-),$$

i si $\sigma(d_1) = +1$ i $\sigma(d_2) = -1$, aleshores Mv té la rotació

$$([\tau^{-1}(d_1)]^+, [\tau^{-1}(d_2)]^+, [\tau(d_2)]^-, [\tau(d_1)]^-).$$

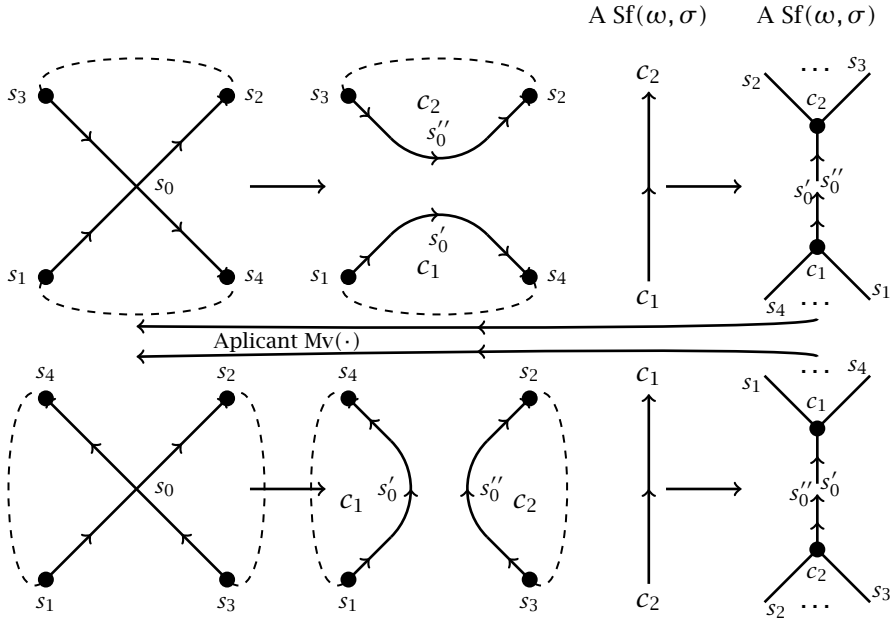


FIGURA 14: Construcció del graf vèrtex medial i mapa de Seifert.

OBSERVACIÓ 13. Sigui ω un paràgraf de Gauss. A la figura 14 podem observar com l'operació vèrtex medial és la inversa de l'obtenció d'un mapa de Seifert orientat a partir d'una signatura de ω .

Així, donar una orientació a les arestes del mapa de Seifert de ω és equivalent a donar una signatura de ω i tenim la següent reformulació de la qüestió 1:

QÜESTIÓ 3. Si ω és un paràgraf de Gauss, existeix una orientació de les arestes del mapa de Seifert de ω tal que indueixi una signatura a ω que el converteixi en un mapa pla?

Vegem algunes propietats dels cercles de Seifert.

PROPOSICIÓ 14. *Sigui ω un paràgraf de Gauss realitzable al pla, i sigui Ω un mapa orientat pla que realitza ω . Suposem que el pla està orientat. Aleshores:*

- (a) *Qualsevol cercle de Seifert c de Ω és una corba tancada al pla sense autointerseccions. L'orientació de les arestes de Ω els dona una orientació. En particular, c té l'orientació horària o antihorària (respecte de l'orientació del pla).*
- (b) *Dos cercles de Seifert s'intersequen, sense travessar-se (tangencialment, besant-se), als vèrtexs de Ω /punts de tall de ω .*
- (c) *A cada vèrtex de Ω /punt de tall de ω hi conflueixen dos cercles de Seifert, i són diferents.*
- (d) *Siguin c_1, c_2 els dos cercles de Seifert de Ω que es toquen a v . Siguin c_1^+ i c_2^+ els dards de Ω que van cap a v de c_1 i c_2 respectivament. Denotem per c_1^- and c_2^- els dards que deixen v de c_1 i c_2 respectivament. Aleshores tenim les següents situacions relatives entre la contenció de c_1, c_2 i les seves orientacions:*

Interior/Exterior	$\Rightarrow$ Orientació de c_1	$\Rightarrow$ Orientació de c_2	$\Rightarrow$ Rotació de v a Ω	$\Rightarrow$ Orientació de l'aresta v a $Sf(\Omega)$
c_1 a l'interior de c_2	antihorària	antihorària	$(c_1^+, c_2^+, c_2^-, c_1^-)$	de c_2 a c_1
c_1 a l'interior de c_2	horària	horària	$(c_2^+, c_1^+, c_1^-, c_2^-)$	de c_1 a c_2
c_1 a l'exterior de c_2	antihorària	horària	$(c_1^+, c_2^+, c_2^-, c_1^-)$	de c_2 a c_1
c_1 a l'exterior de c_2	horària	antihorària	$(c_2^+, c_1^+, c_1^-, c_2^-)$	de c_1 a c_2

TAULA 2

- (e) *Cada cercle de Seifert que no és vèrtex de tall al mapa de Seifert de ω és una cara (possiblement la cara exterior) del mapa Ω .*

DEMOSTRACIÓ DE LA PROPOSICIÓ 14. Per la definició dels cercles de Seifert i del mapa Ω (en tot mapa, dues arestes mai es tallen sobre la superfície que el mapa defineix, en aquest cas el pla), la intersecció entre dos cercles de Seifert només es pot donar als punts de tall de ω .

Cada cercle de Seifert s'obté de prendre la següent aresta del cicle com la que, sortint del punt de tall, no és la que segueix la direcció «tot recte». Per tant, el cercle de Seifert aparella les quatre arestes concurrents a un punt de tall de tal manera que les direccions concurrents no s'intersequen; els camins dels cercles es toquen al punt de tall sense tallar-se. Podem dir que els cercles es repelleixen en trobar-se en un punt de tall. En particular, dos cercles de Seifert no es tallen entre ells. Això demostra (b) i la primera part de (c).

Adicionalment, un cercle de Seifert no es talla amb si mateix. Efectivament, si un cercle de Seifert s'autointersequés, aleshores per l'argument precedent hi hauria una corba més curta continguda a c que separaria el cercle c en dues parts (ja que el nombre total de punts de tall de ω és finit). Això contradiu el fet que dos trams de cercles de Seifert, al pla, reboten per localment allunyar-se en arribar als punts d'intersecció. Això demostra (a) i la segona meitat de (c).

Com que cada cercle de Seifert de Ω és una corba tancada que no s'autointersecta al pla, aquest defineix una cara exterior i una cara interior (pel teorema de la corba tancada de Jordan). Com que dos cercles de Seifert no es travessen, podem determinar el seu conteniment relatiu (si c_1 té un punt a la cara interior de c_2 , aleshores diem que c_1 és a l'interior de c_2 , altrament c_1 és a l'exterior de c_2).

Si c_1 i c_2 comparteixen un punt de tall de ω , aleshores la relació *estar a l'interior/exterior*, juntament amb l'orientació horària/antihorària d'un d'ells, determina l'orientació de l'altre. El motiu és que les direccions són concurrents en el punt de contacte com dos engranatges. Les relacions estan donades a la taula de l'apartat (d) de la proposició. Vegeu també la figura 17 per a un exemple o la figura 15.

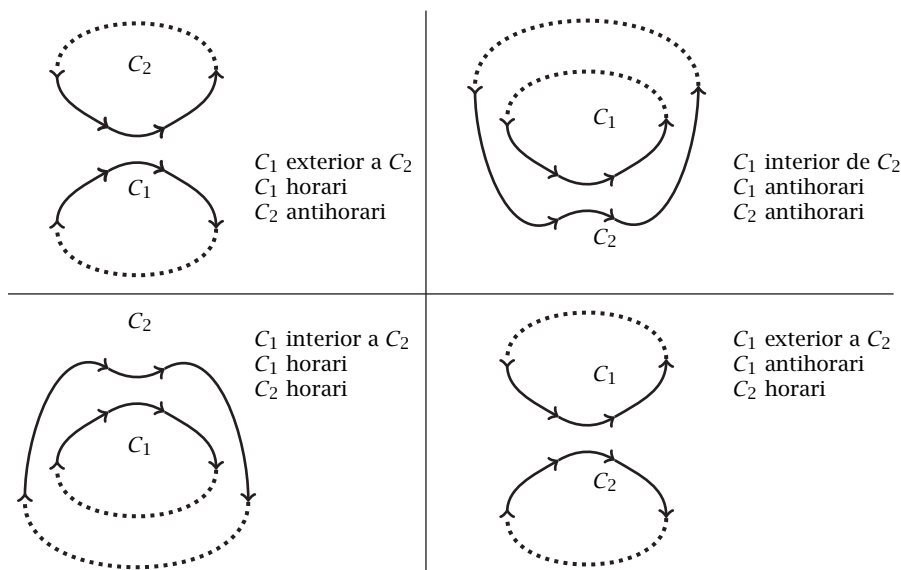


FIGURA 15: Cicles de Seifert: conteniment relatiu i orientació.

Com ja hem dit, cada cercle de Seifert de Ω indueix una regió interior i una d'exterior del pla. Si no hi ha cap altre punt de Ω (vèrtex o aresta) en alguna d'aquestes regions, aleshores la regió en qüestió és una cara de Ω . Si suposem que c_1 no defineix una cara (en alguna de les dues regions en què divideix el pla), aleshores hi ha una aresta de Ω en cadascuna d'aquestes regions. En particular, cadascuna d'aquestes arestes pertanyerà a un cercle de Seifert. Denotem per c_2 el cercle de Seifert a l'interior de c_1 i c_3 el cercle de Seifert de la regió exterior de c_1 . Qualsevol camí per punts de Ω entre un punt de Ω a l'interior de c_1 i un punt de Ω a l'exterior de c_1 involucra una aresta de c_1 a Ω . Efectivament, c_1 forma una corba tancada sense autointerseccions; si volem anar de l'interior a l'exterior l'hem d'intersecar. En un mapa, dues arestes només s'intersequen als vèrtexs. Així, per anar d'un punt de l'interior de c_1 a l'exterior de c_1 a Ω cal passar per un vèrtex de c_1 . Cada vèrtex de c_1 és

una intersecció de dos cercles de Seifert, un és c_1 i l'altre és o bé a l'interior o bé a l'exterior de c_1 . Així, si el camí comença a l'interior i arriba a c_1 , o bé pren una aresta de c_2 o bé continua a l'interior de c_1 . Cada camí a Ω indueix un camí a $Sf(\omega)$ i viceversa. Si usem una aresta a Ω , aleshores usem el vèrtex corresponent al seu cercle de Seifert a $Sf(\omega)$. Si canviem de cercle de Seifert a Ω ho hem de fer en un vèrtex on convergeixen els dos, de manera que podem usar una aresta entre els dos cercles de Seifert a $Sf(\omega)$. Així, qualsevol camí a Ω entre dos punts a l'interior de les arestes que usa arestes dels cercles de Seifert $\{c_4, \dots, c_t\}$ es tradueix en un camí a $Sf(\omega)$ que passa pels vèrtexs $\{c_4, \dots, c_t\}$. A més, qualsevol camí a $Sf(\omega)$ que passa pels vèrtexs $Sf(\omega)$ indueix un camí a Ω que usa arestes dels cercles de Seifert $\{c_4, \dots, c_t\}$. Per tant, com que qualsevol camí entre c_2 i c_3 a Ω usa una aresta de c_1 , qualsevol camí entre el vèrtex c_2 i el vèrtex c_3 a $Sf(\omega)$ passa per c_1 . A més, qualsevol camí entre c_2 i c_3 a $Sf(\omega)$ es tradueix en un camí, a Ω , entre un punt a l'interior d'una aresta de c_2 i un punt a l'interior d'una aresta de c_3 i aquest ha de passar per una aresta de c_1 . Així, c_1 és un vèrtex de tall a $Sf(\omega)$. Això demostra (e) i finalitza la prova. $\square$

5.2 Procediment per orientar les arestes d'un mapa

En aquesta secció donem un procediment, denotat per $\text{Alg}(\cdot)$, que assigna orientacions a les arestes d'un mapa. La intenció és aplicar l'algoritme al mapa de Seifert d'un paràgraf de Gauss. Així, volem usar les relacions de la proposició 14, part (d) per tal de determinar el tipus de punt de tall usant els cercles de Seifert. Més concretament, $\text{Alg}(\cdot)$ dona una orientació de les arestes mitjançant una bicoloració dels vèrtexs del mapa amb $\{0, 1\}$. Com queda reflectit a la taula 3, hom pot pensar que el color 1 assigna al cercle de Seifert l'orientació antihorària al pla.

Algoritme $\text{Alg}(M)$ per assignar orientacions a les arestes d'un mapa M .

1. Sigui $M = (D; \tau, \iota)$ un mapa, on τ denota la permutació que dona el sistema de rotacions i ι és la involució entre els dards.

Si M no és connex, l'algoritme s'aplica a cada component connexa de manera separada.

Assignem un ordre total, arbitrari, als vèrtexs de M i als dards de M .

Si M no és bipartit, aleshores M no és el mapa de Seifert d'un paràgraf de Gauss.

2. Seleccionem v_0 , un vèrtex que no sigui de tall al mapa. (En eliminar-lo no desconnectem el graf.)

Arrelem el mapa a v_0 i acolorim v_0 amb el color 1.

3. Considerem l'arbre de blocs 2-connexos de M (més concretament, del graf subjacent a M) [6, proposició 3.1.2]. Els punts d'articulació de l'arbre són els punts de tall de M .

Arrelem el bloc de v_0 a v_0 .

L'arrel d'un bloc 2-connex B és el vèrtex de B que desconnecta la resta de B respecte a v_0 , l'arrel del mapa M .

L'arrel d'una unió connexa de blocs 2-connexos $\{B_1, \dots, B_s\}$ ve donada per l'arrel més propera a v_0 ; això és, si v_i és el vèrtex arrel de B_i , aleshores l'arrel de $\{B_1, \dots, B_s\}$ és el vèrtex v_i tal que $d(v_i, v_0) = \min_{j \in [s]} d(v_j, v_0)$.

4. Sigui v un vèrtex de M i siguin $B'_0, B'_1, \dots, B'_k$ les components connexes a $M \setminus \{v\}$, i $L_1, \dots, L_r$ els llaços de v .¹⁰ Per a tot $i \in [0, k]$, denotem per B_i el graf induït per $V(B'_i) \cup \{v\}$, sense els llaços de v . B_0 conté el vèrtex v_0 . Siguin $d_1, \dots, d_t$ els dards ordenats cíclicament de M incidents a v . Sigui S_v el graf que té $\{d_1, \dots, d_t, B_0, B_1, \dots, B_k, L_1, \dots, L_r\}$ com a conjunt de vèrtexs. Com a arestes: B_i és adjacent a d_j si i només si l'aresta $\{d_j, \iota(d_j)\}$ de M pertany a B_i . També connectem d_i amb d_{i+1} , índexs mòdul t , de tal manera que $d_1, \dots, d_t$ forma un cicle. L_i és adjacent als vèrtexs $d_j, d_{j'}$ si i només si L_i és el llaç $\{d_j, d_{j'}\}$ a M .

Per a tot vèrtex v , que sigui de tall o que contingui llaços (és a dir, tot v tal que $k \geq 1$ o bé $r \geq 1$), o bé si $v = v_0$, decidirem si $B \in \{B_0, B_1, \dots, B_k, L_1, \dots, L_r\}$ és *dins* de v o bé *fora* de v de la manera següent:

- (a) Si S_v és planar, sigui M_v una immersió plana de S_v . El cicle $(d_1, \dots, d_t)$ a M_v determina dues cares al pla, la cara *exterior* i la cara *interior*. Un vèrtex de $\{B_0, \dots, B_k, L_1, \dots, L_r\}$ és a *dins* de v si es troba a la cara interior, i és *fora* si es troba a la cara exterior.

Si $v \neq v_0$, aleshores B_0 és a la cara exterior de M_v .

Si $v = v_0$, aleshores B_0 és a la cara interior de M_{v_0} .

- (b) Si S_v no és planar, aleshores M no és un mapa de Seifert d'un paràgraf de Gauss realitzable al pla.

En aquest cas, denotem per D_v un dibuix pla de S_v amb el nombre mínim d'encreuaments entre les arestes de S_v amb la condició que les arestes del cicle $d_1, \dots, d_t$ no es tallen dues a dues.¹¹

De les dues cares induïdes per v a D_v (pel cicle $d_1, \dots, d_t$), declarem que la cara que conté B_0 és la cara exterior i que l'altra cara és la interior (llevat del cas que $v = v_0$, llavors B_0 és a la cara interior).

5. Donat un bloc 2-connex B amb arrel v , ordenem els vèrtexs de B d'acord amb les distàncies a v . Sigui $l(v)$ el color de v :

- (a) Si B és dins de v , aleshores acolorem els vèrtexs a distància i de v amb color $l(v) + i + 1 \pmod{2}$ (de tal manera que els veïns de v tenen el mateix color que v).
- (b) Si B és fora de v , aleshores els vèrtexs a distància i de v reben el color $l(v) + i \pmod{2}$.
- (c) El pare del vèrtex u a B és el mínim veí de v (en l'ordenació total que hem donat als vèrtexs) que és estrictament més proper a v_0 que u .

¹⁰ Els casos interessants són $v = v_0$ o v un punt de tall, o que contingui llaços.

¹¹ Si només volem detectar si ω és realitzable, prendrem qualsevol immersió que tingui la propietat respecte del cicle, però no cal un nombre mínim de punts d'encreuaments. Així mantindrem el cost lineal.

6. Orientem les arestes del vèrtex colorat 0 cap al vèrtex colorat 1 si els colors dels vèrtexs difereixen. (Si M és bipartit, aquesta orientació és independent del pare que haguem triat.)

Si l'aresta connecta dos vèrtexs amb la mateixa coloració, i els dos vèrtexs tenen la mateixa distància a v_0 , aleshores el graf no és bipartit i orientem l'aresta del vèrtex més gran al més petit. Si un vèrtex és més proper a v_0 que l'altre, aleshores són pare i fill i l'orientació de l'aresta ve donada pel color del fill: l'aresta va del fill al pare si el fill té el color 0 i del pare cap al fill si el fill té el color 1.

Orientem els llaços del dard menor al dard més gran, segons l'ordre total sobre els dards imposat al principi.

7. Retornem el mapa amb l'orientació sobre les arestes trobada.

5.3 Propietats de l'algoritme i caracterització

En aquesta secció veurem unes quantes propietats de l'algoritme juntament amb el resultat de caracterització usant els cercles de Seifert.

PROPOSICIÓ 15 (PROPIETATS DE $\text{Alg}(\cdot)$). *Sigui M un mapa connex. Aleshores*

- (a) $\text{Alg}(M)$ dona una orientació a les arestes de M .
- (b) *Siguin $\{M_1, \dots, M_q\}$, tots els possibles mapes orientats que $\text{Alg}(M)$ dona com a sortida (per exemple, segons les diferents tries de mapa pla per a S_v al pas 4(a)). Suposem que el mapa obtingut usant la definició 12 a M_1 és pla. Aleshores, usant la definició 12 a M_i obtenim un mapa pla per a tot $i \in [q]$.*
- (c) *L'algoritme té un cost d'operacions lineal en $|E(M)| + |V(M)|$.*

Si ω és un paràgraf de Gauss realitzable al pla i $M = \text{Sf}(\omega)$. Aleshores

- (d) M és bipartit.
- (e) *Per a tot vèrtex de tall v de M , S_v (definit al pas 4) és un graf planar.*

Les propietats de l'algoritme, proposició 15, les veurem a la subsecció 5.5. Primer enunciem i demostrarem el teorema de caracterització, més algorítmic, següent.

TEOREMA 16 (CARACTERITZACIÓ ALGORÍTMICA DELS CODIS DE GAUSS AMB CERCLES DE SEIFERT). *Sigui ω un paràgraf de Gauss. Si ω és realitzable al pla, aleshores:*

- (a) *L'algoritme $\text{Alg}(\text{Sf}(\omega))$ dona una orientació de les arestes, σ , tal que $\text{Mv}(\text{Sf}(\omega), \sigma)$ és un mapa pla.*
- (b) *Si recorrem les arestes del graf dirigit 4-regular $\text{Mv}(\text{Sf}(\omega), \sigma)$ seguint l'aresta sortint que està «just davant» i registrem els vèrtexs pels quals passem, aleshores recuperem ω . És a dir, el mapa $\text{Mv}(\text{Sf}(\omega), \sigma)$ representa ω .*

Si ω no és realitzable, aleshores el mapa $\text{Mv}(\text{Sf}(\omega), \sigma)$ no és pla.

Hi ha un algoritme que, en temps lineal en el nombre símbols de ω , respon si ω és realitzable al pla o no. A més, dona una representació plana en cas afirmatiu.

DEMOSTRACIÓ DEL TEOREMA 16. Per tal de veure (a) i (b) quan ω és realitzable al pla, és suficient de veure (a). Efectivament, si tenim (a), aleshores $Mv(Sf(\omega), \sigma)$ és una realització plana de ω degut a la definició 12 i l'observació 13. Així doncs, vegem ara que, si ω és realitzable al pla, aleshores (a) se satisfà.

Sigui Ω el mapa induït per una representació plana de ω . Com ja hem vist a l'observació 13, podem construir Ω usant una orientació σ de les arestes de $Sf(\omega)$. Si veiem que l'orientació σ induïda per Ω pot ser replicada per l'algoritme, la proposició 15, part (b) completa l'argument.

Per la darrera propietat de la proposició 14, qualsevol immersió plana que realitza ω és tal que qualsevol vèrtex que no sigui de tall a $Sf(\omega)$ és una cara. En particular, podem escollir una immersió plana que realitza ω , denotada per Ω , de tal manera que el vèrtex que no és de tall v_0 triat per l'algoritme és una cara exterior de Ω i està orientat antihoràriament (seguint l'orientació de les arestes de Ω).

La planaritat de Ω induïx una orientació horària/antihorària als cercles de Seifert (segons l'orientació de les arestes induïda per ω i l'orientació positiva del pla), i una relació d'interior/exterior entre dos cercles de Seifert, pel fet de ser corbes tancades al pla que no es tallen entre elles. Usant la part (e) de la proposició 14, S_v és un graf planar per a tot vèrtex de tall v de $Sf(\omega)$. Encara més; per la segona part de l'afirmació 1, juntament amb l'argument just posterior a la prova de l'afirmació 1, podem concloure que Ω induïx un mapa pla per a tots els S_v , on v és un vèrtex de tall de $Sf(\omega)$ o $v = v_0$. Llavors, tenim les següents relacions entre Ω , $Sf(\omega)$ i els mapes plans induïts per Ω a S_v :

1. Si c és un cercle de Seifert que comparteix un punt de tall amb v a ω (v i c són adjacents a $Sf(\omega)$), i c és a l'interior/exterior de v a Ω , aleshores c és a l'interior/exterior de v a la immersió plana de S_v induïda per Ω . Aquest fet es pot veure a través dels arguments de l'afirmació 1.

Això també succeeix amb la unió de blocs 2-connexos que conté c , B_c , a $Sf(\omega) \setminus v$: tots els cercles de $B_c \setminus v$ són a l'interior/exterior de v a Ω si i només si són a l'interior/exterior de v a S_v .

2. Tots els cercles són a l'interior de v_0 . Això passa a tot S_v i també a Ω ja que v_0 defineix la cara exterior de Ω .
3. Si dos cercles de Seifert adjacents a $Sf(\omega)$ pertanyen al mateix bloc 2-connex de $Sf(\omega)$, i cap d'ells és el cercle més proper a v_0 del bloc 2-connex, aleshores cadascun és a l'exterior de l'altre a Ω .

Altrament, podem usar un argument similar al de l'última part de la proposició 14 afegint el fet que v_0 és a l'exterior de tots els cercles de Seifert.

Amb aquests fets veiem que la relació interior/exterior a Ω de dos cercles de Seifert adjacents queda ben reflectida als mapes plans dels S_v de $Sf(\omega)$ que Ω induïx: o bé en sabem informació directa pel fet de ser veï d'un punt de tall, o bé en propaguem la informació a través del bloc 2-connex sabent que són exteriors dos a dos.

Amb aquests fets, vegem inductivament que la coloració induïda per l'algorisme és tal que

c té l'orientació horària/antihorària a Ω
si i només si l'algorisme acoloreix c amb el color 0/1.

Aquesta condició és certa per a v_0 . Suposem que v té aquesta propietat i vegem què podem dir de S_v . Si c és veí de v , aleshores usem les parts 1 i 2 anteriors per obtenir la taula 3; a la cinquena columna veiem que l'algorisme $\text{Alg}(\text{Sf}(\omega))$ produeix l'ordenació de les arestes al mapa dirigit $\text{Sf}(\omega)$ coincident amb la que indueix Ω via definició 11.

Or. v a Ω /Color. de v per $\text{Alg}()$	c int./ext. a v a Ω/S_v	$\Rightarrow$ Or. de c a Ω	Coloració de c per $\text{Alg}()$	$\Rightarrow$ Or. $\{c, v\}$ a $\text{Sf}(\omega)$
antihorària /1	c a l'interior de v	c antihorària	1	de v a c
antihorària /1	c a l'exterior de v	c horària	0	de c a v
horària /0	c a l'interior de v	c horària	0	de c a v
horària /0	c a l'exterior de v	c antihorària	1	de v a c

TAULA 3: La primera columna i la segona impliquen la tercera i la quarta. La primera i la quarta, juntament amb el fet que v és el pare de c , impliquen la cinquena.

Si usem la part 3 concloem que la coloració a la resta de blocs 2-connexos també és la correcta ja que la coloració es propaga, canviant el color, segons la distància creixent a v sabent que el vèrtex sempre és exterior a un de ja acolorit que no és v . Observem que en aquests casos els colors són diferents entre les arestes i, per tant, no cal usar el desempat pare/fill a l'hora de decidir la direcció de l'aresta.

En aquest punt notem que això demostra la proposició 15, part (d). Efectivament, la coloració alternada segons la distància dins de la component 2-connexa, deixant de banda v , està ben definida degut al fet que dos cercles, llevat de v , han de ser mútuament exteriors; aquest fet implica que l'orientació dels cicles s'alterna segons la paritat de la distància amb v . A aquest fet hem d'afegir que tots els veïns de v del mateix bloc 2-connex són a la mateixa banda i, per tant, tots tenen la mateixa orientació, cosa que fa que el bloc sigui bipartit. Si tots els blocs 2-connexos són bipartits, aleshores el graf també ho és.

Així doncs, l'argument inductiu esbossat al paràgraf anterior ens mostra que hi ha una orientació σ de les arestes de $\text{Sf}(\omega)$ que l'algorisme pot donar com a resposta, i que és tal que $\Omega = \text{Mv}(\text{Sf}(\omega), \sigma)$. Això finalitza l'argument de la implicació d'esquerra a dreta.

$\text{Alg}(\omega)$ dona una orientació de les arestes de $\text{Sf}(\omega)$ per la proposició 15. L'observació 13 ens permet concloure que per a tota orientació σ de les arestes de $\text{Sf}(\omega)$, $\text{Mv}(\text{Sf}(\omega), \sigma)$ dona una representació de ω en alguna superfície. Si Ω no és representable, aleshores cap σ farà que $\text{Mv}(\text{Sf}(\omega), \sigma)$ sigui pla. Això conclou la segona part del teorema.

El cost d'obtenir $Sf(\omega)$ a partir de ω és lineal en el nombre de símbols de ω . Usant la proposició 15, part (c), si ω és realitzable al pla, l'algoritme aplicat a $Sf(\omega)$ dona una orientació de les arestes σ en temps lineal en el nombre d'arestes. Això és el nombre de símbols de ω . El mapa $Mv(Sf(\omega), \sigma)$ es pot trobar en temps lineal al nombre d'arestes, que és lineal en $|\omega|$. Calcular el nombre de cares de $Mv(Sf(\omega), \sigma)$ també és lineal en el nombre d'arestes i, per tant, podem donar una resposta afirmativa i donar una representació plana en temps lineal si ω és representable.¹² L'algoritme es pot modificar lleugerament per donar, en cas que el graf S_v no sigui planar, un dibuix pla on el cicle v no té cap tall, i fer-ho en temps lineal en el nombre d'arestes de S_v . Així, usem la fórmula d'Euler per veure que el mapa $Mv(Sf(\omega), \sigma)$ no és pla. Tot això ho podem fer en temps lineal en $|\omega|$. $\square$

5.4 Un altre resultat de caracterització

Si N és un mapa bipartit amb A i B com a conjunts de vèrtexs estables amb $V(N) = A \sqcup B$, aleshores diem que N' és el mapa *mig girat de N* si:

- La permutació cíclica dels dards al voltant dels vèrtexs v de B és τ_v (la mateixa que a N).
- La permutació dels dards al voltant dels vèrtexs v de A és τ_v^{-1} (la inversa de la de N).

Amb aquesta definició podem usar els resultats i arguments anteriors per obtenir la caracterització següent:

TEOREMA 17 (CARACTERITZACIÓ DELS CODIS DE GAUSS USANT CERCLES DE SEIFERT). *Sigui ω un paràgraf de Gauss i $M = Sf(\omega)$ el seu mapa de Seifert. Aleshores,*

ω és un paràgraf de Gauss representable al pla

si i només si:

- Per a tot v , S_v definit al pas 4 de $Alg(\cdot)$ és un graf planar.*
- El graf subjacent a M és bipartit.*
- Per a tot bloc 2-connex N de M , el mapa N' , obtingut després de mig girar el submapa N , és pla.*

DEMOSTRACIÓ DEL TEOREMA 17. D'esquerra a dreta. Les parts (b) i (a) corresponen, respectivament, a les parts (d) i (e) de la proposició 15.

Per veure la part (c), usem $Alg(\omega)$ per obtenir una representació plana de ω . Denotem per Ω aquesta representació. Observant la part 3 a la demostració del teorema 16, juntament amb la part (d) de la proposició 14 i la interpretació de la coloració $\{0, 1\}$ de l'algoritme als cercles de Seifert (que coincideix amb l'orientació horària/antihorària usant la taula 3), tenim que els cercles de

¹² Hem suposat que, des del caràcter d'un paràgraf, podem accedir a totes les còpies del caràcter en temps constant, així com als seus veïnatsges de mida 4. Això també passa als mapes ι i τ d'un mapa a l'hora de calcular les cares o $Mv(Sf(\omega), \sigma)$.

Seifert a Ω segueixen l'orientació horària/antihorària segons la coloració $\{0, 1\}$ atorgada per $\text{Alg}(\omega)$. Denotem per Ω_N el submapa de Ω on hem eliminat els punts de tall de ω no continguts en algun cercle de Seifert de N i totes les arestes de Ω incidents a aquests vèrtexs. A Ω_N , cada cercle de Seifert de N defineix una cara on no hi ha altres punts de tall de Ω_N (aquí usem la part 3 de la demostració del teorema 16). Llavors, si posem un vèrtex a cada cara de Ω_N definida per un cercle de Seifert de N i l'unim amb els punts de tall del corresponent cercle de Seifert sense crear punts de tall (per tal que el resultat sigui un altre mapa pla), obtenim un mapa pla Ω'_N on els punts de tall originals tenen grau sis. Si a Ω'_N eliminem les arestes de Ω_N , aleshores obtenim un mapa pla Ω''_N on els punts de tall de ω tenen grau dos. Si a Ω''_N convertim els camins que contenen els punts de tall de ω (ara tenen ordre dos) en arestes, obtenim precisament el mapa mig girat de N , que és, doncs, pla.

A continuació demostrarem que (a) + (b) + (c) implica que ω és realitzable al pla. Triem v_0 un cercle de Seifert que no sigui un vèrtex de tall a M , el definim com a cara exterior, i donem mapes plans per tot S_v (els S_v són planars per (a) seguint les directrius de $\text{Alg}(\cdot)$; això és, el vèrtex de S_v que conté v_0 és a l'exterior de v). Construïm el mapa que realitza ω «enganxant» els mapes plans associats als mapes mig girats dels blocs 2-connexos; els enganxem seguint l'ordre proporcionat per la distància (a l'arbre de components 2-connexes de M) entre el bloc en qüestió i el que conté v_0 .

Assignem colors $\{0, 1\}$ als vèrtexs seguint $\text{Alg}(M)$. Per (b) podem definir el mapa mig girat de cada bloc 2-connex N . Per (c) els mig girem i hi trobem el mapa pla N' . Denotem per N'' el mapa creat a partir de N' subdividint les arestes de N' , afegint arestes dirigides segons l'orientació cíclica de les arestes al voltant dels vèrtexs de N entre els nous vèrtexs (cada vèrtex de N genera un cicle dirigit, el que serà el cercle de Seifert corresponent), i eliminant les arestes i els vèrtexs de N ; aquesta operació crea un nou mapa pla on cada cicle afegit defineix una cara on hi ha un únic vèrtex original de N .

A N'' podem dibuixar el cicles de tal manera que segueixin l'orientació indicada per la coloració $\{0, 1\}$ de $\text{Alg}(\cdot)$. Efectivament, tots els cicles que no són v o bé tenen tots la mateixa orientació antihorària/horària a N'' i la 1/0 de $\text{Alg}(\cdot)$, o bé tots les tenen diferents (degut a (b), a l'operació de capgirar N cap a N' , i a la manera en què hem creat N'' a partir de N'). En cas que la tinguin diferent, podem «veure el pla des de sota» i això inverteix l'orientació horària/antihorària dels cercles. Finalment, si v té una orientació diferent a N'' que l'assignada per l'algoritme, aleshores $\text{Alg}(\omega)$ el colora igual que els seus veïns, i N és a l'interior de v . Així doncs, determinem que la cara associada a v és la cara exterior i modifiquem el dibuix de N'' de manera que només canviï l'orientació horària/antihorària del cicle associat a v (ja que l'anterior cara exterior no estava associada a cap cercle de Seifert, usem v per «embolcallar» o encerclar la resta de N''). Usem, doncs, v per «enganxar» N a la resta del mapa trobat anteriorment. Donat que S_v és planar, això no crea cap nou tall, i el mapa on el bloc 2-connex N s'ha afegit continua essent pla.

Així doncs, obtenim una representació plana de ω . □

5.5 Demostració de la proposició 15

Part (d). L'hem vist a la demostració del teorema 16.

Part (a). L'algoritme assigna un vèrtex com a arrel del graf i un pare independentment de si M és bipartit o S_v és planar, per a tot v . L'orientació de cada aresta queda determinada per com hem triat l'arrel, pel color dels vèrtexs, i el color del pare.

Part (e). Usem l'afirmació següent:

AFIRMACIÓ 1. *Sigui σ una orientació de les arestes de M , v un vèrtex de M i S_v el graf definit al pas 4. Si $Mv(M, \sigma)$ és un mapa en una superfície orientable de gènere k , aleshores el graf S_v té gènere orientable $\leq k$.¹³*

Adicionalment, si $Mv(M, \sigma)$ és pla, aleshores $Mv(M, \sigma)$ defineix un mapa pla per a qualsevol S_v .

DEMOSTRACIÓ DE L'AFIRMACIÓ 1. Denotem per G_0 el graf 4-regular subjacent al mapa orientat $Mv(M, \sigma)$, i denotem per $(d_1, \dots, d_t)$ la rotació de dards associada a v a M . A G_0 aquesta rotació associada a v induïx un circuit tancat format pel conjunt de vèrtexs ordenats $(\{d_1, \iota(d_1)\}, \{d_2, \iota(d_2)\}, \dots, \{d_t, \iota(d_t)\})$ (són els vèrtexs corresponents als símbols d'un cercle de Seifert de ω , i aquests són independents de la signatura de ω per l'observació 13). Si v no té cap llaç, aleshores el circuit és un cicle en t vèrtexs.

Denotem per G_1 el graf obtingut de G_0 subdividint un cop l'aresta del circuit tancat induït per v a G_0 : per a cada $i \in [1, t]$, índexs mòdul t , l'aresta de $\{d_i, \iota(d_i)\}$ a $\{d_{i+1}, \iota(d_{i+1})\}$ és substituïda per un camí de 3 vèrtexs $(\{d_i, \iota(d_i)\}, u_i, \{d_{i+1}, \iota(d_{i+1})\})$, on u_i és un nou vèrtex. Del mapa $Mv(M, \sigma)$ obtenim $Mv(M, \sigma)'$, una immersió de G_1 a la mateixa superfície que $Mv(M, \sigma)$, ja que podem considerar que el vèrtex u_i és un punt a l'aresta de $\{d_i, \iota(d_i)\}$ a $\{d_{i+1}, \iota(d_{i+1})\}$.

Sigui G_2 el graf derivat de G_1 afegint l'aresta e_i entre u_i i u_{i+1} per a cada $i \in [1, t]$, índexs mòdul t . A $Mv(M, \sigma)$, l'aresta de $\{d_i, \iota(d_i)\}$ a $\{d_{i+1}, \iota(d_{i+1})\}$, i l'aresta de $\{d_{i+1}, \iota(d_{i+1})\}$ a $\{d_{i+2}, \iota(d_{i+2})\}$ són consecutives a l'orientació cíclica al voltant del vèrtex $\{d_{i+1}, \iota(d_{i+1})\}$ (vegeu la definició 12). Així doncs, són arestes consecutives en una cara de $Mv(M, \sigma)$. Això implica que podem afegir l'aresta e_i al mapa $Mv(M, \sigma)'$ per tal de crear un mapa $Mv(M, \sigma)''$ que és la immersió de G_2 a la mateixa superfície que $Mv(M, \sigma)$. Consegüentment, el gènere de G_2 és com a màxim el gènere de $Mv(M, \sigma)$.

Denotem per G_3 el graf obtingut d'eliminar, per a cada $i \in [1, t]$, l'aresta de u_i a $\{d_{i+1}, \iota(d_{i+1})\}$ a G_2 . Denotem per G_4 el graf obtingut de G_3 després de contraure totes les arestes no incidents als vèrtexs $\{u_i\}_{i \in [1, t]}$. Llavors tenim que $S_v = G_4$, i, per tant, podem immersir S_v a la mateixa superfície que $Mv(M, \sigma)$

¹³ El gènere d'un graf Γ és el mínim gènere d'una superfície orientable on Γ es pot immersir (per tant, sense talls entre les arestes) o, equivalentment, el mínim gènere entre la col·lecció de mapes que tenen Γ com a graf subjacent.

o alguna de gènere menor (ja que G_4 és un menor de G_2).¹⁴ Això implica les dues parts de l'afirmació. $\square$

Donat que les operacions Mv i Sf són invertibles per l'observació 13, el mapa pla Ω del paràgraf de Gauss ω indueix una orientació σ a les arestes de $Sf(\omega)$ per la qual $Mv(Sf(\omega), \sigma)$ és un mapa dirigit pla. Per tant, l'afirmació 1 demostra que tot S_v és un graf planar.

Part (b). És una prova bastant tècnica. Es pot trobar completa a [38, lema 3.3]. Podem resumir-la dient que podem, ordenadament, fer petits canvis a les immersions planes, que ens porten d'una immersió plana a l'altra. Els canvis venen indicats per les diferents immersions planes de S_v . Vegeu la figura 16 per observar la naturalesa dels canvis que fem i les conseqüències que tenen a $Mv(Sf(\omega, \sigma))$.

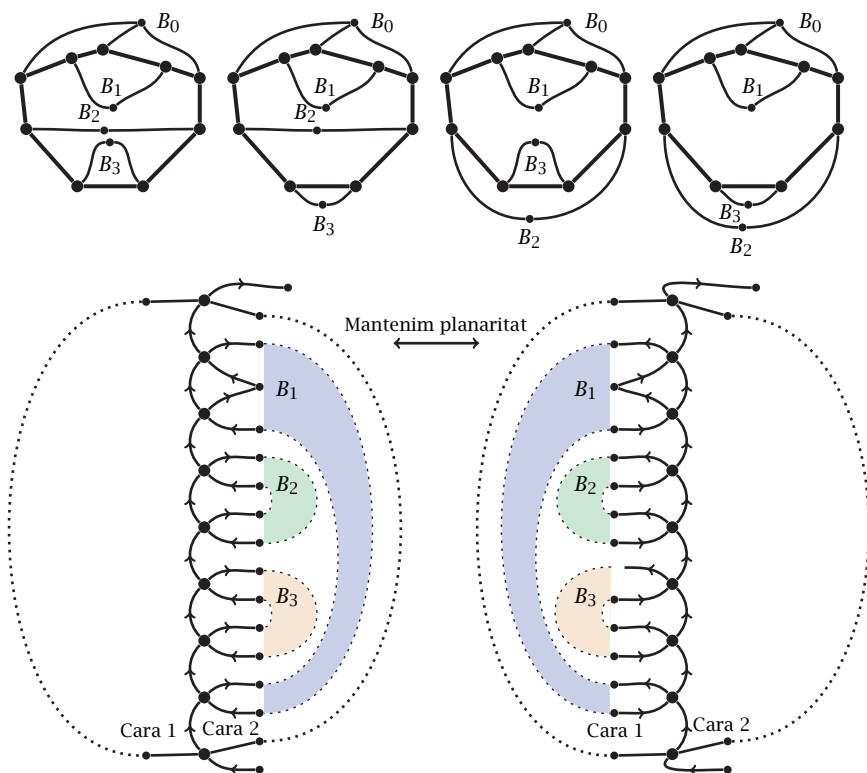


FIGURA 16: Dalt: diferents possibles immersions planes de S_v i com es transformen l'una en l'altra. Baix esquerra/dreta: representació amb B_1 , B_2 i B_3 dins/fora de v a S_v .

¹⁴ El graf G és un menor del graf H si podem obtenir G mitjançant una seqüència d'operacions d'eliminació d'arestes i de vèrtexs o de contracció d'arestes, les quals es poden dur a terme en un graf immers en una superfície sense augmentar-ne el gènere (vegeu [37, p. 463]).

Part (c). Assumim que podem construir una estructura de dades en la qual podem visitar un veí concret d'un vèrtex de M en temps constant. El nombre de components connexes de M es pot obtenir en temps lineal en el nombre de $|V(M)| + |E(M)|$ usant una cerca en profunditat (vegeu, per exemple, el treball de Hopcroft i Tarjan [22, figura 1]). Donar un ordre total arbitrari a les arestes i vèrtexs de M ho podem fer en un nombre lineal d'operacions en $|E(M)| + |V(M)|$. Comprovar que el graf és bipartit també té un cost lineal ja que el nombre d'arestes és lineal. El càlcul de la descomposició en blocs 2-connexos de M , així com el conjunt de punts de tall, es pot realitzar en temps lineal en el nombre de $|V(M)| + |E(M)|$ (vegeu Hopcroft i Tarjan [22, figura 2]).

Sigui $W = \sqcup_v$ de tall a M o $v_0 V(S_v)$ el conjunt de tots els vèrtexs de S_v . Cada aresta de M genera, com a molt, dos vèrtexs a W . Usem [23] per determinar si cada S_v és planar i trobar-ne una immersió en temps lineal en $|W|$. Si algun S_v no és planar, usem (e) per determinar que ω no és representable al pla i l'algoritme acaba en temps lineal. Si tot S_v és pla, en tenim immersions planes en temps lineal en $|E(M)|$, això assigna un pare a cada vèrtex de M i l'orientació de les arestes de M en temps lineal; amb aquesta orientació σ trobem el mapa orientat $Mv(M, \sigma)$ (que representa ω) i en determinem la seva planaritat en temps lineal. Usant (b), (c) i la primera part del teorema 16, si ω és representable al pla, $Mv(M, \sigma)$ és pla i l'algoritme dona una representació plana de ω en temps lineal en $|E(M)| + |V(M)|$.

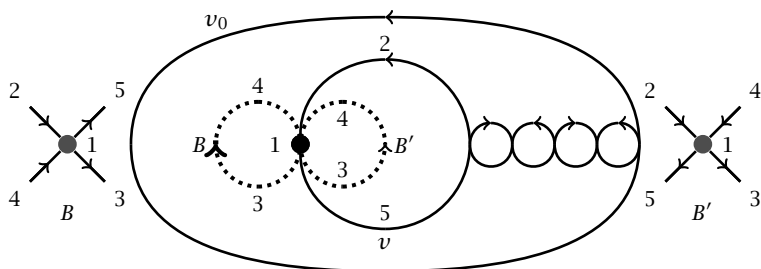


FIGURA 17: Correspondència entre l'orientació cíclica de les arestes cap a 2, 3, 4, 5 al voltant del punt de tall 1 en la representació de ω i les immersions planes de S_v .

6 Girant la tercera cantonada

Hem vist que, tant si desfem el nus girant sempre cap a l'altra aresta en el mateix sentit com si girem sempre cap a l'aresta en sentit contrari, podem obtenir una caracterització dels codis de Gauss representables al pla.

Com a curiositat, fem notar que la figura 18 ja apareix en els treballs complets de Gauss, concretament a la pàgina 274 de [16], vuit pàgines abans

de la nota on es presenta el problema en detall i dues pàgines després de la primera menció que se'n fa. En aquesta figura apareixen els cercles de Seifert d'un nus; com hem vist, una estructura fonamental en teoria de nusos i que ens porta a la segona caracterització.

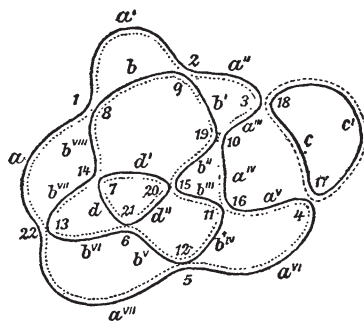


FIGURA 18: Cicles de Seifert en els treballs complets de Gauss. (Reprduït a [16].)

En particular, els cercles de Seifert representats a la figura 18 són els cercles de Seifert del codi de Gauss

$$\begin{aligned} &\{1, 8\}, \{2, 9\}, \{10, 19\}, \{11, 16\}, \{5, 12\}, \{13, 22\}, \{7, 14\}, \{13, 20\}, \\ &\{11, 16\}, \{4, 17\}, \{3, 18\}, \{10, 19\}, \{13, 20\}, \{6, 21\}, \{13, 21\}, \\ &\{1, 8\}, \{2, 9\}, \{3, 18\}, \{4, 17\}, \{5, 12\}, \{6, 21\}, \{7, 14\}. \end{aligned}$$

Així doncs, podem dir que la caracterització també es pot descobrir girant les pàgines de llibre de les obres completes de Gauss; en altres paraules, la resposta es trobava, materialment, en girar la cantonada!

Referències

- [1] CAIRNS, G.; ELTON, D. M. «The planarity problem for signed Gauss words». *J. Knot Theory Ramifications*, 2 (4) (1993), 359-367.
- [2] CAIRNS, G.; ELTON, D. M. «The planarity problem. II». *J. Knot Theory Ramifications*, 5 (2) (1996), 137-144.
- [3] DE FRAYSSEIX, H. «Sur la représentation d'une suite à triples et à doubles occurrences par la suite des points d'intersection d'une courbe fermée du plan». A: *Problèmes combinatoires et théorie des graphes* (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976). París: CNRS, 1978, 161-165. (Colloq. Internat. CNRS; 260)
- [4] DE FRAYSSEIX, H.; OSSONA DE MENDEZ, P. «On a characterization of Gauss codes». *Discrete Comput. Geom.*, 22 (2) (1999), 287-295.

- [5] DEHN, M. «Über kombinatorische Topologie». *Acta Math.*, 67 (1) (1936), 123–168.
- [6] DIESTEL, R. *Graph Theory*. 3a ed. Berlín: Springer-Verlag, 2005. (Graduate Texts in Mathematics; 173)
- [7] DUNNINGTON, G. W. «The Gauss Archive and the Complete Edition of His Collected Works, 1860–1933». *Math. News Lett.*, 8 (5) (1934), 103–107.
- [8] EDMONDS, J. R. «A combinatorial representation for polyhedral surfaces». *Notices Amer. Math. Soc.*, 7 (1960), art. A646.
- [9] GAUSS, C. F. *Werke. Band I*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1863.
- [10] GAUSS, C. F. *Werke. Band II*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1863.
- [11] GAUSS, C. F. *Werke. Band III*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1866.
- [12] GAUSS, C. F. *Werke. Band IV*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1873.
- [13] GAUSS, C. F. *Werke. Band V*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1867.
- [14] GAUSS, C. F. *Werke. Band VI*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1874.
- [15] GAUSS, C. F. *Werke. Band VII*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1906.
- [16] GAUSS, C. F. *Werke. Band VIII*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1900.
- [17] GAUSS, C. F. *Werke. Band IX*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1903.
- [18] GAUSS, C. F. *Werke. Band X. Abt. I, II*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió dels originals de 1917 i de 1922–1933.
- [19] GAUSS, C. F. *Werke. Band XI. Abt. I, II*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió dels originals de 1927 i de 1924–1929.
- [20] GAUSS, C. F. *Werke. Band XII*. Hildesheim: Georg Olms Verlag, 1973. Reimpressió de l'original de 1929.
- [21] GODSIL, C.; ROYLE, G. *Algebraic Graph Theory*. Nova York: Springer-Verlag, 2001. (Graduate Texts in Mathematics; 207)
- [22] HOPCROFT, J.; TARJAN, R. «Algorithm 447: efficient algorithms for graph manipulation». *Comm. ACM*, 16 (6) (1973), 372–378.
- [23] HOPCROFT, J.; TARJAN, R. «Efficient planarity testing». *J. Assoc. Comput. Mach.*, 21 (1974), 549–568.
- [24] LINS, S.; OLIVEIRA-LIMA, E.; SILVA, V. «A homological solution for the Gauss code problem in arbitrary surfaces». *J. Combin. Theory Ser. B*, 98 (3) (2008), 506–515.

- [25] LINS, S.; RICHTER, B.; SHANK, H. «The Gauss code problem off the plane». *Aequationes Math.*, 33 (1) (1987), 81–95.
- [26] LOVÁSZ, L.; MARX, M. L. «A forbidden substructure characterization of Gauss codes». *Acta Sci. Math. (Szeged)*, 38 (1–2) (1976), 115–119.
- [27] MARX, M. L. «The Gauss realizability problem». *Proc. Amer. Math. Soc.*, 22 (1969), 610–613.
- [28] NAGY, J. «Über ein topologisches Problem von Gauß». *Math. Z.*, 26 (1) (1927), 579–592.
- [29] READ, R. C.; ROSENSTIEHL, P. «On the Gauss crossing problem». A: *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976)*. Vol. II, Amsterdam; Nova York: North-Holland, 1978, 843–876. (Colloq. Math. Soc. János Bolyai; 18)
- [30] ROSENSTIEHL, P. «Les graphes d'entrelacement d'un graphe». A: *Problèmes combinatoires et théorie des graphes: Orsay 9–13 Juillet 1976*. Éditions du Centre national de la recherche scientifique, 1978, 359–362. (Colloq. Int. CNRS; 260)
- [31] ROSENSTIEHL, P. «A new proof of the Gauss interlace conjecture». *Adv. in Appl. Math.*, 23 (1) (1999), 3–13.
- [32] ROSENSTIEHL, P.; READ, R. C. «On the principal edge tripartition of a graph». A: *Advances in Graph Theory*. Amsterdam, Nova York, Oxford: North-Holland, 1978, 195–226. (Ann. Discrete Math.; 3)
- [33] ROSENSTIEHL, P.; TARJAN, R. E. «Gauss codes, planar Hamiltonian graphs, and stack-sortable permutations». *J. Algorithms*, 5 (3) (1984), 375–390.
- [34] SEIFERT, H. «Über das Geschlecht von Knoten». *Math. Ann.*, 110 (1) (1935), 571–592.
- [35] SEIFERT, H.; THRELFAH, W. *Lehrbuch der Topologie*. Leipzig: Teubner, 1934.
- [36] TREYBIG, L. B. «A characterization of the double point structure of the projection of a polygonal knot in regular position». *Trans. Amer. Math. Soc.*, 130 (1968), 223–247.
- [37] VAN LINT, J. H.; WILSON, R. M. *A Course in Combinatorics*. 2a ed. Cambridge: Cambridge University Press, 2001.
- [38] VENA, LL. «A topological characterization of Gauss codes». Preprint, 2018. <https://arxiv.org/abs/1808.04630>.

English summaries

Esther Barrabés and Mercè Ollé

Space manifold dynamics: the highways of the universe

In this article we seek to illustrate how the understanding of the dynamics of some models of Celestial Mechanics allows both to explain some astronomical phenomena and to design realistic space missions. The paradigmatic model used is the restricted three-body problem in which the invariant manifolds of the so-called libration orbits, that is, periodic and quasi-periodic orbits around the collinear equilibrium points of the model, play a key role. We will describe some of these phenomena and mention a number of specific missions. Lastly, we will comment on other useful (and more sophisticated) models in Astrodynamics and we will conclude with a remark on how the tools of Dynamical Systems can be transferred from the macroscopic (celestial) world to microscopic ones, such as classic atomic physics.

Keywords: restricted problem, invariant manifolds, equilibrium points, periodic and quasi-periodic orbits, space missions, homoclinic and heteroclinic connections.

MSC2010 Subject Classification: 70F07, 70F10, 70F15, 70H12, 70H33, 70K44.

Ramsès Fernández-València

Isogenies, codes and lattices in post-quantum cryptography

In this paper we give a brief introduction to some of the concepts and mathematical techniques that are being explored in post-quantum cryptography. We introduce lattice theory together with code theory and the theory of isogenies of supersingular elliptic curves.

Keywords: lattice, code, isogeny, supersingular elliptic curve.

MSC2010 Subject Classification: 11T71, 14G50, 94A60.

Jordi Marzo*Minimal energy points and sphere packing*

In this article we deal with two very interesting problems and a way to relate them. The first problem is the study of the asymptotic development of the minimum energy of a set of points confined to a sphere and interacting through a Riesz potential. The limiting case of one of the constants that appear in this development will lead us to our second problem, that of determining the best sphere packing in the Euclidean space, a problem in which important advances have recently come out.

Keywords: Riesz energy, well-distributed points, sphere packing, linear programming.

MSC2010 Subject Classification: 31C20, 52C07, 11K36.

Lluís Vena*On two characterizations of Gauss codes*

In this paper we give some historical background, the motivation and some solutions to the *Gauss codes* problem.

A closed curve on the plane with n self-intersection points that are non-tangential, and where the curve goes through all points of the plane twice at the most, generates a double occurrence word on n symbols as follows. Label the intersection points with $\{1, \dots, n\}$, choose an initial point on the curve, a direction of travel through the curve, and record the sequence of self-intersection points found. Such word is said to be a *Gauss code* representable on the plane.

The Gauss codes problem seeks to characterize those double occurrence words that are representable by plane curves. We explain two different characterizations that involve 'turning the corner' to undo the crossing points in the two most natural ways. The first one leads to the characterization known on account of Dehn, and Read and Rosenstiehl. We present an alternative characterization that uses the other way of 'undoing' the crossing points and involves the Seifert cycles of the word. We also give some historical insight.

Keywords: Gauss codes, Gauss paragraph, alternative characterization, Seifert cycles.

MSC2010 Subject Classification: Primary: 05C10; Secondary: 57M15, 57M25.

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



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

Bartomeu Coll

Dep. de Matemàtiques i Informàtica

Universitat de les Illes Balears

Núria Fagella

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Armengol Gasull

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Gábor Lugosi

ICREA i Departament d'Economia

Universitat Pompeu Fabra

Marc Noy

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Francesc Planas

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Joan Saldaña

Dep. d'Informàtica, Mat. Aplicada i Estadística

Universitat de Girona

Marta Sanz-Solé

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

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>