

BUTLLETÍ

DE LA SOCIETAT CATALANA
DE MATEMÀTIQUES
Institut d'Estudis Catalans

í n d e x

- ☐ *Carles Barril, Sílvia Cuadrado i Jordi Ripoll*
Models matemàtics en dinàmica de poblacions 87
- ☐ *Agustí Reventós*
Gaspard Monge 111
- ☐ *Narcís Sayols i Sebastià Xambó*
Codis correctors d'errors i criptografia postquàntica 147
- ☐ English summaries 173



Volum 33 • Número 2 • Any 2018



Institut
d'Estudis
Catalans

BUTLLETÍ

DE LA SOCIETAT CATALANA
DE MATEMÀTIQUES
Institut d'Estudis Catalans

Volum 33 • Número 2 • Desembre 2018

BARCELONA
2018

© 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

CARLES BARRIL, SÍLVIA CUADRADO I JORDI RIPOLL Models matemàtics en dinàmica de poblacions.....	87
AGUSTÍ REVENTÓS Gaspard Monge.....	111
NARCÍS SAYOLS I SEBASTIÀ XAMBÓ Codis correctors d'errors i criptografia postquàntica	147
English summaries	173

Models matemàtics en dinàmica de poblacions

CARLES BARRIL, SÍLVIA CUADRADO I JORDI RIPOLL

Resum: La dinàmica de poblacions, com el seu nom indica, estudia l'evolució de la mida i la composició de les poblacions. En aquest article presentem un recull dels principals models matemàtics que descriuen la dinàmica de poblacions biològiques. Primerament, farem una introducció històrica a la matèria tot descrivint diferents problemes en ecologia, demografia i epidemiologia, així com les eines i tècniques matemàtiques emprades. Seguidament, descriurem una nova formulació en termes d'equacions amb retard que estableix un marc general rigorós per a la modelització matemàtica de la dinàmica de poblacions.

Paraules clau: biologia matemàtica, poblacions estructurades, equacions amb retard, equacions en derivades parcials.

Classificació MSC2010: 92D25, 35Q92, 47N20.

La biologia matemàtica és la disciplina que s'encarrega de proporcionar models i eines matemàtiques per a entendre processos biològics. En l'actualitat s'ocupa d'una gran varietat de temes, però les primeres interaccions entre biologia i matemàtiques van tenir lloc en el context de la *dinàmica de poblacions*, que és la branca de la biologia matemàtica que té per objecte l'estudi de l'evolució de la mida de les poblacions i la seva composició. Començarem fent-ne un breu repàs històric (vegeu, per a més informació, [3, 11, 9, 33, 45, 50]). Tot i que els models presentats en aquest treball són, en la nostra opinió, molt representatius de la història de la dinàmica de poblacions, degut al gran desenvolupament en els últims anys d'aquesta disciplina, una descripció exhaustiva de la matèria aniria més enllà de l'objectiu d'aquest article.

1 La dinàmica de poblacions anterior al segle xx

El que podríem considerar el primer problema en dinàmica de poblacions va ser el proposat per Leonardo de Pisa, més conegut com a Fibonacci, en el seu llibre *Liber abaci*, publicat el 1202:

Un home té una parella de conills en un lloc tancat. Es voldria saber quantes parelles més s'obtenen de la primera parella, en un any, si la natura d'aquests conills és tal que engendren una nova parella cada mes i comencen a ser fèrtils a partir del segon mes de vida.

Si anomenem u_n el nombre de parelles de conills joves i v_n el de parelles adultes, al començament del mes n , aleshores el problema anterior dona lloc a les relacions de recurrència

$$\begin{aligned}u_{n+1} &= v_n, \\v_{n+1} &= u_n + v_n.\end{aligned}$$

Això equival a l'equació de recurrència $v_{n+1} = u_n + v_n = v_{n-1} + v_n$, a partir de la qual Fibonacci va construir la famosa successió que porta el seu nom i que amb els anys s'ha observat que apareix de manera freqüent a la natura. Existeix fins i tot una revista científica, *The Fibonacci Quarterly*, que publica articles relacionats amb aquesta successió.

Tenim, doncs, que el primeríssim problema de dinàmica de poblacions ja considerava dues variables independents (discretes): temps i edat.

Després de Fibonacci, la història de la dinàmica de poblacions ha d'esperar cinc segles perquè es plantegi un nou problema, tot i que entremig es van fer grans aportacions a la matemàtica, com és el desenvolupament modern del càlcul diferencial.

Va ser Leonhard Euler qui el 1748 publicà el llibre *Introductio in analysin infinitorum* [22], on, al capítol sobre exponencials i logaritmes, inclou exemples de dinàmica de poblacions com el següent:

Si la població d'una certa regió augmenta anualment en una trentena part i inicialment hi havia 100 000 habitants, voldríem saber la població després de 100 anys.

Es tracta d'un exemple d'una població amb creixement geomètric i la resposta és $P_{100} = (1 + \frac{1}{30})^{100} 100\,000$.

L'any 1760 publicà als *proceedings* de l'Acadèmia de Ciències de Berlín el treball «Recherches générales sur la mortalité et la multiplication du genre humain», on es planteja el problema de trobar la distribució en edats d'una població sota certes hipòtesis [23, 24]:

Si anomenem P_n la població l'any n i B_n el nombre de naixements l'any n , Euler va suposar que la població creix geomètricament, és a dir,

$$P_{n+1} = \lambda P_n, \tag{1}$$

i que el quocient entre el nombre de naixements i la població és constant:

$$B_n = m P_n. \tag{2}$$

Notem que aquestes dues hipòtesis impliquen que el nombre de naixements creix geomètricament i amb la mateixa taxa:

$$B_{n+1} = \lambda B_n. \tag{3}$$

Denotant per l_k la proporció de nounats que encara són vius l'any k i suposant que ningú sobreviu més de 100 anys, Euler es planteja si, coneguts B_n , P_n i l_k , podem conèixer quants individus hi ha a cada grup d'edat. Tenim, fent servir reiteradament (1) i (3),

$$\begin{aligned}\lambda^{100}P_0 &= P_{100} = B_{100} + l_1B_{99} + l_2B_{98} + \cdots + l_{100}B_0 = \\ &= (\lambda^{100} + \lambda^{99}l_1 + \lambda^{98}l_2 + \cdots + l_{100})B_0.\end{aligned}$$

Dividint per $\lambda^{100}P_0$ obtenim l'anomenada *equació d'Euler*

$$1 = \left(1 + \frac{l_1}{\lambda} + \frac{l_2}{\lambda^2} + \cdots + \frac{l_{100}}{\lambda^{100}}\right) \frac{B_0}{P_0}. \quad (4)$$

Suposant coneguts els naixements i la població en un determinat any, B_n , P_n i, per tant, el paràmetre $m = B_n/P_n = \cdots = B_0/P_0$, i conegudes les probabilitats de supervivència l_k , $k \geq 1$, l'equació d'Euler ens permet trobar λ .

Tenint en compte que durant l'any n el nombre d'individus nascuts l'any $n - k$ que encara són vius és

$$l_k B_{n-k} = \frac{l_k}{\lambda^k} B_n,$$

la proporció d'individus d'edat k és

$$\frac{\frac{l_k}{\lambda^k} B_n}{P_n} = \frac{\frac{l_k}{\lambda^k} B_n}{B_n \left(1 + \frac{l_1}{\lambda} + \frac{l_2}{\lambda^2} + \cdots + \frac{l_{100}}{\lambda^{100}}\right)} = \frac{\frac{l_k}{\lambda^k}}{\left(1 + \frac{l_1}{\lambda} + \frac{l_2}{\lambda^2} + \cdots + \frac{l_{100}}{\lambda^{100}}\right)}.$$

Aquesta proporció és constant i, per tant, la piràmide d'edat no canvia amb el temps i es diu que la població és *estable*.

Tot i que l'equació (1) va ser proposada per Euler, es coneix com a *model de Malthus* en referència a Thomas Malthus, qui, l'any 1798, va publicar *An Essay on the Principle of Population* [42], que, tot i generar una gran controvèrsia en el moment de la seva publicació, va tenir una gran influència en les teories econòmiques del segle XIX, així com en el desenvolupament de la teoria de l'evolució. Efectivament, tant Charles Darwin com Alfred Russell Wallace van afirmar que el llibre de Malthus els havia inspirat per a formular la teoria de l'evolució per selecció natural, la qual, descoberta pels dos científics de manera independent, fou publicada de manera conjunta en un article presentat a la Linnean Society de Londres [12]. La tesi de Malthus al seu llibre és que la població creix de manera geomètrica (o exponencial), mentre que els recursos necessaris per a donar suport a la població creixen de manera aritmètica, cosa que dona lloc al que s'ha conegut com a *catàstrofe malthusiana*.

Malthus va considerar una població homogènia (tots els individus són idèntics) d'una sola espècie, aïllada o tancada (no hi ha migracions), gran (per tal de negligir factors estocàstics) i en un hàbitat invariant (la quantitat de recursos no canvia degut a factors externs ni a la mateixa població). Per formular el

model, denotem per $x(t)$ la mida de la població (nombre total d'individus) a temps t . Tot i que $x(t)$ és de fet discreta, com que s'està suposant una població molt gran, es considera $x(t)$ una funció real de la variable real t . Donat que no hi ha migració, la mida de la població canvia només degut a naixements i morts i, per tant, la taxa de canvi en la mida de la població serà la fertilitat (taxa *per capita* de naixements) menys la mortalitat (taxa *per capita* de morts). Atès que s'està suposant que l'hàbitat no canvia, aquestes dues taxes no dependran del temps ni de la població mateixa. Denotant per β la fertilitat i per μ la mortalitat tenim

$$x'(t) = (\beta - \mu)x(t), \quad x(0) = x_0. \quad (5)$$

El paràmetre $r := \beta - \mu$ és la taxa *per capita* de creixement (o decreixement) exponencial i rep el nom de paràmetre malthusià. En funció de la població inicial $x_0 \geq 0$, l'evolució de la població ve donada per

$$x(t) = e^{rt} x_0, \quad (6)$$

que és la solució del problema de valor inicial (5). La població s'extingirà, romandrà constant o creixerà il·limitadament depenent de si $r < 0$, $r = 0$ o $r > 0$, respectivament. Equivalentment, definint la quantitat $R_0 := \frac{\beta}{\mu}$, tenim el mateix resultat si $R_0 < 1$, $R_0 = 1$ o $R_0 > 1$, respectivament. R_0 , que és la taxa de fertilitat per l'esperança de vida $1/\mu$, dona el nombre esperat de descendents que té cada individu al llarg de la seva vida; vegeu [4].

Les hipòtesis considerades per Malthus sobre la població poden ser vàlides per a certes espècies en un període de temps suficientment curt, per a les quals s'observa efectivament un creixement exponencial. No obstant, la hipòtesi que la taxa de creixement d'una població és proporcional a la mida de la població (model lineal) és poc realista a escales de temps més grans.

Anys més tard, el 1838, Pierre-François Verhulst publica el treball «Notice sur la loi que la population suit dans son accroissement», on proposa, donant-li el nom de *equació logística*, el model

$$x'(t) = r \left(1 - \frac{x(t)}{K} \right) x(t), \quad x(0) = x_0, \quad (7)$$

on la taxa *per capita* de creixement de la població ja no és constant com en el model de Malthus, sinó que depèn de manera decreixent de la població: $r(x) := r(1 - \frac{x}{K})$ amb $r > 0$. En efecte, r és el valor màxim de la funció $r(x)$, que s'anul·la per a $x = K$ i es fa negativa quan $x > K$. Notem que si la població és petita aleshores la població té un creixement exponencial ($x' \approx rx$), mentre que quan la població té un valor proper a K , pràcticament no canvia ($x' \approx 0$).

La solució de (7) en funció de la població inicial és

$$x(t) = \frac{Kx_0}{x_0 + (K - x_0)e^{-rt}}, \quad (8)$$

d'on podem veure que per a una població inicial $x_0 > 0$, la població s'acosta a K quan el temps t tendeix a infinit. K equival a la capacitat de càrrega de

la població perquè representa la mida màxima sostenible de la població. Així doncs, el model logístic¹ prediu, si la població inicial és petita, creixement exponencial seguit d'un decreixement en la taxa de creixement quan el temps avança de manera que la població s'acosta al límit K .

2 La dinàmica de poblacions del segle xx

El treball de Verhulst va inspirar molts dels investigadors que desenvoluparien la dinàmica de poblacions de començaments del segle xx. Un d'ells va ser el matemàtic italià Vito Volterra, a qui el seu futur gendre i biòleg marí Umberto D'Ancona demanà si era possible estudiar matemàticament les variacions poblacionals observades en una població de peixos. D'Ancona (vegeu [10, 1]) tenia dades sobre el percentatge total de captures de condrictis (taurons, rajades...) sobre el total de peixos capturats durant un període al voltant de la Primera Guerra Mundial.

Percentatge de captures de condrictis al port del mar Adriàtic Fiume (Rijeka, Croàcia)									
1914	1915	1916	1917	1918	1919	1920	1921	1922	1923
11.9%	21.4%	22.1%	21.2%	36.4%	27.3%	16.0%	15.9%	14.8%	10.7%

D'Ancona va observar l'augment d'aquests depredadors, que en aquell moment no es consideraven comestibles, durant la guerra i creia que era degut a la disminució de la pesca en aquest període. El seu raonament era que, en pescar menys, hi havia més preses i per això el nombre de condrictis augmentava. Sorprenentment, però, semblava que el nombre de preses, en comptes d'augmentar, havia disminuït quan es pescava menys. Per tal d'entendre com aquesta disminució de la pesca podia afectar les poblacions de peixos va demanar ajut a Volterra. En resposta a D'Ancona, Volterra publicà l'any 1926 el treball «Variazioni e fluttuazioni del numero d'individui in specie animali conviventi» [54].

El mateix model proposat per Volterra va ser analitzat de manera independent (en un context diferent) per Alfred Lotka el 1920 a l'article [38] i el 1925 a la seva obra, publicada primer amb el títol *The Elements of Physical Biology* [39] i posteriorment amb el títol *Elements of Mathematical Biology* [41] i per això es coneix com a *model de Lotka i Volterra*. Passem ara a descriure'l.

Denotem per $x(t)$ i $y(t)$ el nombre de preses i depredadors a temps t , respectivament. Se suposa que, en absència de depredadors, les preses experimenten un creixement malthusià amb taxa de creixement $r > 0$, mentre que, en absència de preses, els depredadors s'extingeixen de manera exponencial amb taxa de mortalitat $\mu > 0$. També se suposa que la dinàmica d'aquestes poblacions vindrà donada només per les interaccions entre preses i depredadors, de manera que la supervivència dels depredadors depèn de la quantitat de preses i les preses a la vegada tenen només els depredadors com a factor de

¹ No és del tot clar, però sembla que el nom de *logística* té a veure amb els logaritmes (M. Iannelli, comunicació personal). Així, per exemple, de $x = 1/(1 + e^{-t})$ obtenim la relació inversa $t = \ln(x/(1 - x))$.

control. La taxa de predació s'obté del que s'anomena *lleï d'acció de masses*, que estableix que el nombre de trobades entre preses i depredadors és proporcional al producte de les poblacions respectives. Suposant que una fracció a de totes les trobades és efectiva (el depredador mata la presa), el nombre de preses consumides pels depredadors per unitat de temps és axy . Això s'anomena *resposta funcional de tipus I*. El nombre de nous depredadors per unitat de temps serà αxy , on α denota la taxa de conversió (habilitat dels depredadors de convertir les preses en taxa *per capita* de creixement per al predador). Amb tots aquests ingredients podem escriure ja el model de Lotka i Volterra

$$\begin{cases} x'(t) = rx(t) - ax(t)y(t), \\ y'(t) = -\mu y(t) + \alpha ax(t)y(t). \end{cases} \quad (9)$$

Aquest sistema té dos equilibris $(0, 0)$ i $(\frac{\mu}{\alpha a}, \frac{r}{a})$. Si $x \neq 0$, $y \neq 0$ es té

$$(\mu - \alpha ax) \frac{x'}{x} + (r - ay) \frac{y'}{y} = 0$$

o, equivalentment,

$$\frac{d}{dt} (\ln(x^\mu y^r) - \alpha ax - ay) = 0,$$

per la qual cosa es té

$$\frac{x^\mu y^r}{e^{\alpha ax} e^{ay}} = K$$

per a qualsevol constant positiva K . Tenim, doncs, que la funció $F(x, y) := \frac{x^\mu y^r}{e^{\alpha ax} e^{ay}}$ és una integral primera del sistema, és a dir, les òrbites de (9) estan contingudes als conjunts de nivell de F . Aquestes corbes de nivell són tancades al voltant de l'equilibri $(\frac{\mu}{\alpha a}, \frac{r}{a})$ [10, 1] i, per tant, les solucions de (9) són periòdiques.

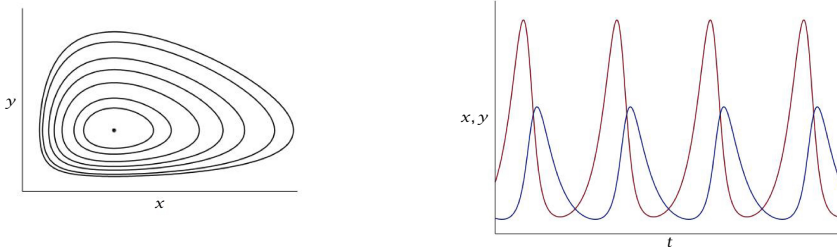


FIGURA 1: Simulacions numèriques del retrat de fase i de les solucions al llarg del temps en un sistema Lotka-Volterra.

Per tal de comparar les solucions del seu model amb les dades de D'Ancona, Volterra calcula $\hat{x}$ i $\hat{y}$, les mitjanes en un període T , de les poblacions de preses

i depredadors, respectivament, i demostra que

$$\hat{x} = \frac{1}{T} \int_0^T x(t) dt = \frac{\mu}{\alpha a}, \quad \hat{y} = \frac{1}{T} \int_0^T y(t) dt = \frac{r}{a}.$$

És a dir, les mitjanes del nombre de preses i del nombre de depredadors en un període són independents de les condicions inicials i iguals a les poblacions en equilibri.

Volterra considerarà els efectes de la pesca, afegint a les equacions (9) un terme per a modelitzar les captures, que suposà proporcionals a les poblacions respectives i amb la mateixa intensitat per a totes dues:

$$\begin{cases} x'(t) = rx(t) - ax(t)y(t) - \varepsilon x(t), \\ y'(t) = -\mu y(t) + \alpha ax(t)y(t) - \varepsilon y(t). \end{cases} \quad (10)$$

Per aquest sistema, les mitjanes són $\hat{x} = \frac{\mu + \varepsilon}{\alpha a}$, $\hat{y} = \frac{r - \varepsilon}{a}$, la qual cosa explica les dades de D'Ancona: un decreixement moderat de la pesca (reducció de ε) augmenta en mitjana el nombre de depredadors, mentre que disminueix el nombre de preses.

Com comentàvem anteriorment, Alfred Lotka va arribar a les mateixes conclusions que Volterra, pensant en reaccions químiques i en una població de plantes i herbívors. Però abans d'interessar-se per això, Lotka havia fet contribucions molt importants en altres aspectes de la dinàmica de poblacions, en particular en demografia. Els anys 1907 i 1911 publica els treballs [37] i [47] (el segon conjuntament amb F. R. Sharpe), on estudia la dinàmica de poblacions estructurades per l'edat. Desconeixedor dels treballs d'Euler sobre aquest tema, Lotka proposa el mateix model però considerant el temps i l'edat com a variables contínues (vegeu també [35, 32, 52]).

Considerant una població de femelles (de fet, al seu article, Sharpe i Lotka consideren una població de mascles), denotem per $B(t)$ la taxa de naixements a temps t , és a dir, el nombre total de naixements per unitat de temps, per $\mathcal{F}(a)$ la probabilitat de sobreviure fins a edat $a \geq 0$, i per $\beta(a)$ la taxa de fertilitat de les femelles d'edat a (nombre mitjà de filles per unitat de temps i per femella en l'interval infinitesimal $[a, a + da]$).

Aleshores, ja que les femelles d'edat a a temps t han nascut a temps $t - a$, tenim que el nombre de femelles nascudes entre el temps $t - a$ i $t - a + da$ que encara són vives a temps t és $B(t - a)\mathcal{F}(a)da$. Aquestes femelles tenen $\beta(a)B(t - a)\mathcal{F}(a)da$ filles per unitat de temps i obtenim l'equació de renovació (o de Volterra) següent:

$$B(t) = \int_0^t \beta(a)B(t - a)\mathcal{F}(a)da + F(t), \quad t \geq 0, \quad (11)$$

on el primer terme de la dreta ens dona el nombre de naixements de filles de femelles nascudes en l'interval de temps $[0, t]$ i el segon terme $F(t)$ són

els naixements deguts a les femelles ja presents a la població a temps $t = 0$. L'equació integral (11) és equivalent a

$$B(t) = \int_0^\infty \beta(a)B(t-a)\mathcal{F}(a) da, \quad t \geq 0, \quad (12)$$

si suposem una història de naixements coneguda $B(\theta) = \phi(\theta)$, $\theta \leq 0$. Noti's que l'edat màxima dels individus d'una població es pot suposar finita o potencialment infinita. Buscant una solució exponencial, $B(t) = be^{\lambda t}$, $b > 0$, d'aquesta equació integral, Lotka obté l'anomenada *equació característica de Lotka*

$$1 = \int_0^\infty \beta(a)e^{-\lambda a}\mathcal{F}(a) da, \quad (13)$$

que és la versió contínua de l'equació d'Euler (4).

Per a λ real, el costat dret de (13) és una funció decreixent de λ que tendeix a $+\infty$ quan $\lambda \rightarrow -\infty$ i a 0 quan $\lambda \rightarrow +\infty$. Per tant, hi ha un únic valor real λ^* que satisfà (13) que, a més, serà positiu si i només si

$$R_0 := \int_0^\infty \beta(a)\mathcal{F}(a) da > 1.$$

Aquesta quantitat és el famós número reproductiu bàsic (la notació va ser introduïda per Dublin i Lotka el 1925, [21]) i s'interpreta com el nombre esperat de filles que té cada individu de la població al llarg de la seva vida.

Sharpe i Lotka [47] van enunciar que el nombre de naixements per unitat de temps satisfà

$$B(t) \sim be^{\lambda^* t}$$

quan $t \rightarrow +\infty$ amb b una constant positiva.

Això va ser demostrat de manera rigorosa per W. Feller el 1941 [25] i es coneix com a *teorema fonamental de la demografia*.

Tenint en compte que la població total a temps t és

$$P(t) = \int_0^\infty B(t-a)\mathcal{F}(a) da,$$

tenim que l'estructura en edat de la població (distribució normalitzada d'edats) ve donada per

$$\frac{B(t-a)\mathcal{F}(a)}{P(t)}$$

que tendeix a

$$\frac{e^{-\lambda^* a}\mathcal{F}(a)}{\int_0^\infty e^{-\lambda^* a}\mathcal{F}(a) da}$$

que no depèn del temps (ni de la distribució inicial de la població) i, per tant, es té, com en el cas discret d'Euler, el que Lotka anomenà *població estable*: la piràmide d'edats manté la mateixa forma al llarg del temps, però la població total creix o decreix exponencialment.

Una manera alternativa de formular aquest model va ser proposada per A. G. McKendrick el 1926 [44] i més tard per H. von Foerster [55] i va donar lloc a l'anomenada *equació de McKendrick-von Foerster*, que va ser la primera equació en derivades parcials de la dinàmica de poblacions estructurades.

Denotant per $n(a, t)$ la densitat d'individus d'edat a a temps t i per $\mu(a)$ la taxa *per capita* de mortalitat a edat a tenim

$$n(a + \Delta t, t + \Delta t) - n(a, t) = -\mu(a)n(a, t)\Delta t, \quad (14)$$

és a dir, els individus d'edat a a temps t tindran edat $a + \Delta t$ quan ha passat un temps Δt i l'únic canvi en el nombre d'individus vindrà donat pels que han mort durant l'interval $(t, t + \Delta t)$. Dividint (14) per Δt i fent el límit $\Delta t \rightarrow 0$ suposant que n és diferenciable respecte a a i t obtenim

$$n_t(a, t) + n_a(a, t) = -\mu(a)n(a, t). \quad (15)$$

McKendrick va especificar que (per a $t > a$)

$$n(a, t) = n(0, t - a)e^{-\int_0^a \mu(s) ds},$$

però no va definir cap condició inicial ni cap condició de frontera. Per a descriure el model complet, denotant per $\beta(a)$ la taxa de fertilitat a edat a , tenim que els naixements venen donats per la condició de frontera (no local) a edat zero

$$B(t) = n(0, t) = \int_0^\infty \beta(a)n(a, t) da. \quad (16)$$

Si denotem per $n_0(a)$ la distribució inicial de la població, tenim que el model complet serà

$$\begin{cases} n_t(a, t) + n_a(a, t) = -\mu(a)n(a, t), \\ n(0, t) = \int_0^\infty \beta(a)n(a, t) da, \\ n(a, 0) = n_0(a). \end{cases} \quad (17)$$

Per veure l'equivalència entre els models de McKendrick-von Foerster i Sharpe-Lotka resolem (17) pel mètode de les característiques i obtenim

$$n(a, t) = \begin{cases} n(0, t - a)e^{-\int_0^a \mu(s) ds} & a < t, \\ n(a - t, 0)e^{-\int_{a-t}^a \mu(s) ds} & a \geq t. \end{cases}$$

Substituint aquesta expressió a la condició de frontera (16) escrivim

$$\begin{aligned} n(0, t) &= \int_0^\infty \beta(a)n(a, t) da = \\ &= \int_0^t \beta(a)n(0, t - a)e^{-\int_0^a \mu(s) ds} da + \\ &\quad + \int_t^\infty \beta(a)n(a - t, 0)e^{-\int_{a-t}^a \mu(s) ds} da. \end{aligned} \quad (18)$$

Definint $\mathcal{F}(a) := e^{-\int_0^a \mu(s) ds}$ i fent un canvi de variable al segon sumand, es pot escriure (18) com

$$n(0, t) = \int_0^t \beta(a) n(0, t-a) \mathcal{F}(a) da + \int_0^\infty \beta(a+t) n(a, 0) \frac{\mathcal{F}(a+t)}{\mathcal{F}(a)} da,$$

que és l'equació de renovació (11) amb $n(0, t) = B(t)$.

Des del punt de vista biològic, el model lineal (17) suposa que les taxes vitals β i μ són paràmetres intrínsecs del sistema i no tenen en compte la competència entre els individus pels recursos, que són limitats. Aquesta limitació va ser considerada per Gurtin i MacCamy el 1974 a [28], on van introduir taxes vitals dependents, a part de l'edat, de la mateixa població. Igual que en el cas de l'equació logística (7), això dona lloc a un model no lineal que permet que el creixement de la població sigui autoregulat per la mateixa població:

$$\begin{cases} n_t(a, t) + n_a(a, t) = -\mu(a, P(t))n(a, t), & P(t) = \int_0^\infty n(a, t) da, \\ n(0, t) = \int_0^\infty \beta(a, P(t))n(a, t) da, \\ n(a, 0) = n_0(a). \end{cases} \quad (19)$$

En aquest model, la influència de les *condicions ambientals* en els individus de la població es resumeix en una sola quantitat, que és la població total. Altres autors, com per exemple M. Iannelli el 1995 (vegeu [34]), han considerat aquest mateix model però per a edat màxima finita i suposant que la influència ambiental ve donada per una col·lecció finita de mides de la població amb un pes, és a dir, $S(t) = \int_0^\infty \gamma_i(a) n(a, t) da$, per $i = 1, \dots, m$.

Una gran varietat de models no lineals amb dependència en edat van aparèixer posteriorment. Podríem dir que la teoria de la dinàmica de poblacions estructurades per l'edat va quedar molt ben recollida per G. F. Webb a les referències [57, 56]. Webb estudia un model no lineal molt general per a la densitat respecte de l'edat a de m tipus o grups d'individus:

$$\begin{cases} D\vec{n}(a, t) = \mathcal{G}(\vec{n}(\cdot, t))(a), \\ \vec{n}(0, t) = \mathcal{B}(\vec{n}(\cdot, t)), \\ \vec{n}(a, 0) = \vec{n}_0(a), \end{cases} \quad (20)$$

on $D\phi(a, t) := \lim_{h \rightarrow 0^+} \frac{\phi(a+h, t+h) - \phi(a, t)}{h}$ és la «derivada direccional» en la direcció del vector $(1, 1)$ de la densitat vectorial de població a temps $t \geq 0$, $\vec{n}(\cdot, t)$ pertany a l'espai de Banach $X := L^1((0, \infty); \mathbb{R}^m)$ equipat amb la norma $\|\phi\| = \sum_{i=1}^m \int_0^\infty |\phi_i(a)| da$. En el sistema (20), per una banda hi tenim l'operador $\mathcal{G}: X \rightarrow X$, que s'anomena *funció d'envelliment* i pot incloure termes relacionats amb la mortalitat i amb les transicions entre tipus o grups d'individus, i per l'altra banda, hi tenim l'operador $\mathcal{B}: X \rightarrow \mathbb{R}^m$, que s'anomena *funció de naixements* i dona el nombre de nounats de cada tipus per unitat de temps.

Per acabar aquesta exposició històrica, volem destacar que no gaire lluny d'aquests models ecològics hi ha tota una classe de models en dinàmica de

poblacions que constitueixen el que s'anomena *epidemiologia matemàtica*. Els primers treballs que es coneixen en aquest camp són els de Daniel Bernoulli sobre la inoculació de la verola [7] (gairebé quaranta anys abans del descobriment de les vacunes, atribuït a Edward Jenner, 1798) i els de Ronald Ross sobre la malària [46]. Ross va ser un dels primers de formular un model compartimental, donat que considerava una població de mosquits i una d'humans, i també va ser un dels primers de parlar d'un llinar de l'epidèmia que més endavant s'anomenà *número reproductiu bàsic* (nombre esperat d'infeccions produïdes per un individu típic de la població a l'inici de l'epidèmia) i que és l'equivalent del número R_0 definit anteriorment en el context ecològic.

Hi ha una classe de models epidèmics que també consideren l'edat però en el sentit del temps transcorregut des del moment en què un individu contrau una malaltia infecciosa (*edat de la infecció*). L'article de W. O. Kermack i A. G. McKendrick del 1927 [36] ha esdevingut un clàssic de l'epidemiologia matemàtica que ha estat citat una infinitat de vegades. Per tal de fer justícia, cal destacar que aquest article es coneix principalment pel famós model SIR (sistema simplificat d'EDOs), però que, en realitat, estudia un model més general tenint en compte l'edat de la infecció.

El model clàssic de Kermack-McKendrick descriu l'evolució del brot epidèmic d'una malaltia infecciosa on els naixements i les morts per causes naturals són negligits i, per tant, la mida de la població es manté constant. La població es divideix en tres grups: individus *susceptibles* (d'adquirir la malaltia), densitat d'individus *infectats* respecte de l'edat d'infecció (poden transmetre la malaltia), i individus *recuperats* (els que han superat la malaltia i ara són immunes permanentment, per exemple) i evoluciona segons:

$$\begin{cases} S'(t) = - \int_0^{\tau^\dagger} \beta(\tau) i(\tau, t) d\tau \cdot S(t), \\ i_t(\tau, t) + i_\tau(\tau, t) + \gamma(\tau) i(\tau, t) = 0, \\ i(0, t) = \int_0^{\tau^\dagger} \beta(\tau) i(\tau, t) d\tau \cdot S(t), \\ R'(t) = \int_0^{\tau^\dagger} \gamma(\tau) i(\tau, t) d\tau, \end{cases} \quad (21)$$

amb condicions inicials $S(0) = S_0$, $i(\theta, 0) = i_0(\theta)$, $R(0) = R_0$, i on $\tau \in [0, \tau^\dagger]$ és l'edat de la infecció, $\beta(\tau)$ és la taxa de transmissió de la malaltia i $\gamma(\tau)$ és la taxa de recuperació, vegeu [36, 34]. En el cas que les taxes β , γ siguin constants, llavors, integrant respecte a l'edat de la infecció l'equació en derivades parcials a (21), obtenim el famós sistema d'equacions diferencials ordinàries SIR:

$$S'(t) = -\beta I(t)S(t), \quad I'(t) = \beta I(t)S(t) - \gamma I(t), \quad R'(t) = \gamma I(t),$$

amb $I(t) = \int_0^{\tau^\dagger} i(\tau, t) d\tau$ (nombre total d'infectats a temps t).

Fins aquí hem exposat el desenvolupament històric de la dinàmica de poblacions aprofundint especialment en les poblacions estructurades per l'edat, ja que podríem dir que tot model de dinàmica de poblacions considera implícitament l'edat dels individus, donat que l'edat no és res més que el temps

transcorregut des del moment del naixement dels individus. En resum, la cronologia de la teoria de les poblacions estructurades per l'edat comença essencialment amb Euler [23], passant per Lotka [37, 47, 40], Feller [25], McKendrick [44], von Foerster [55], Gurtin i MacCamy [28], i conclou substancialment amb Webb [56, 57].

Paradoxalment, l'edat és una variable massa senzilla per a descriure amb detall els processos fisiològics de les poblacions. Això fa que, depenent del tipus de problema biològic que vulguem analitzar pot ser convenient classificar els individus segons alguna mesura biomètrica, en comptes (o a més) de l'edat, per exemple estructurar la població per la mida en poblacions cel·lulars. Els primers que van considerar poblacions estructurades fisiològicament van ser Fredrickson *et al.* [51, 26, 27], Bell *et al.* [6, 5, 2] i Sinko i Streifer [48, 49]; vegeu [29] per a més detalls. El model més senzill d'una població estructurada per la mida dels individus va ser analitzat per Van Sickle a [53]. Aquest model, que és un cas particular dels models introduïts pels grups d'investigadors citats anteriorment, suposa que els nounats tenen tots una mida $\varepsilon > 0$ i que la densitat respecte de la mida $x \geq \varepsilon$ a temps t , $n(x, t)$ evoluciona segons (vegeu [43] per a la deducció del model):

$$\begin{cases} n_t(x, t) + (g(x) n(x, t))_x = -\mu(x) n(x, t), \\ g(\varepsilon) n(\varepsilon, t) = \rho \int_{\varepsilon}^{\infty} \beta(x) n(x, t) dx, \\ n(x, 0) = n_0(x), \end{cases} \quad (22)$$

on $g(x) > 0$ és la taxa *per capita* de creixement individual, és a dir, $x'(t) = g(x(t))$, $\mu(x)$ és la taxa *per capita* de mortalitat a mida x , $\beta(x)$ és la taxa *per capita* de fertilitat a mida x , i ρ és la probabilitat dels nounats de sobreviure durant el *nursery stage*. Vegeu Heijmans i Metz [31] per a una millora d'aquest model lineal.

En la propera secció es veurà com tots aquests models estructurats per l'edat o per una variable fisiològica més general, que fins ara han estat descrits en termes de taxes instantànies de canvi i, per tant, amb equacions diferencials, es poden descriure amb una nova formulació desenvolupada per O. Diekmann, M. Gyllenberg i J. Metz, i H. Thieme i altres col·laboradors (1986-actualitat), que estén i generalitza la ja famosa equació de Volterra (12) afegint-hi un recurs dinàmic que és consumit pels individus de la població. Aquesta teoria va ser iniciada amb el llibre [43] i desenvolupada posteriorment als treballs [17, 14, 15, 13] i [20, 19, 16], entre d'altres.

3 Formulació de la dinàmica de poblacions usant equacions amb retard

Per a estudiar la dinàmica d'una població des d'un punt de vista mecanicista cal considerar el comportament dels seus individus. Un individu particular actuarà d'una manera o altra en funció de les seves característiques i de l'ambient en el qual viu. És oportú, per tant, estructurar la població de forma que s'agrupin els

individus que són anàlegs. En aquest sentit, cada individu està dotat d'un *estat individual* (també anomenat *estat-i*) i es consideren equivalents els individus que comparteixen el mateix estat. L'*estat-i* és la variable d'estructura de la població i pot fer referència tant a variables internes de l'individu (com l'edat, la mida, el fenotip, l'estat d'alerta o el que sigui que ens interessi) com a variables externes (com la posició en un hàbitat donat). Al seu torn, es defineix l'*estat poblacional* (també anomenat *estat-p*) com la densitat poblacional respecte de l'*estat-i* dels seus individus.

Clàssicament la dinàmica de poblacions, com hem vist a les seccions anteriors, ha considerat l'*estat-p* com la variable dependent del problema. La formulació amb retard es diferencia en aquest punt perquè, en lloc de considerar l'*estat-p*, utilitza la *història dels naixements*. Aquesta variable descriu com han estat els naixements en el passat, i en concret es pot utilitzar per a saber quants individus d'*estat individual* x estaven naixent τ unitats de temps en el passat. En particular, si coneixem la *història de naixements* i com són les trajectòries de cada individu per l'espai d'*estats-i* des del moment en què neix fins al present, aleshores podem recuperar la densitat poblacional al present, és a dir, l'*estat-p*.

Com hem dit, per a saber com varia l'*estat-i* d'un individu en un instant no n'hi ha prou de conèixer l'*estat-i* de l'individu en aquell instant. A part d'aquesta variable també cal saber quina és la *condició ambiental* en aquell instant. Remarquem que n'hi ha prou amb la *condició ambiental* instantània i que no cal conèixer com era l'ambient en el passat. Això és així perquè l'efecte que ha tingut l'ambient del passat en l'individu està contingut implícitament en el seu *estat-i* actual. Notem també que la *condició ambiental* és una variable global en el sentit que és la mateixa per a tots els individus. És l'efecte que té l'ambient sobre els diferents subjectes el que pot variar. Per exemple, pot passar que certa font d'aliment només sigui accessible als individus petits o que els individus grans no siguin perseguits pels depredadors. L'ambient, però, és el que és.

Si es coneix la *condició ambiental* al llarg del temps, aleshores es pot escriure una equació de renovació o equació de Volterra per a la *història de naixements*. La població, però, té un impacte sobre l'ambient, ja sigui perquè consumeix recursos o perquè contamina, la qual cosa impedeix conèixer, *a priori*, com serà l'ambient. La *condició ambiental* és, de fet, una variable del sistema que depèn tant de la *condició ambiental* en el passat com de la *història de naixements*. Així s'arriba a un sistema de dues equacions amb retard acoblades. L'objectiu d'aquesta secció és donar una expressió explícita del sistema anterior en termes de quatre ingredients fenomenològics. El primer ingredient conté informació sobre com evoluciona l'*estat-i* d'un individu a través de l'espai d'*estats individuals*, i, per tant, té en compte processos com el desenvolupament, el creixement, el moviment o la supervivència. El segon ingredient inclou tot el que està relacionat amb la reproducció dels individus. El tercer ingredient descriu l'impacte que té un individu sobre l'ambient mentre que el quart descriu com varia el medi en absència de població. Tots quatre ingredients s'especificaran formalment quan sigui necessari.

Dels individus a la població

Comencem introduint Ω com el conjunt de tots els *estats individuals* admissibles. Els elements de Ω depenen tant del que s'està modelitzant com del nivell de detall del model. Per exemple, si estem interessats en la mida dels individus, podem optar per un model molt senzill, en què $\Omega = \{\text{petit}, \text{gran}\}$ o per un model una mica més ric en el qual es distingeixen els individus en funció de la seva massa corporal, de manera que $\Omega = \mathbb{R}_+$. Fins i tot es podrien classificar els individus en funció de diverses mesures biomètriques. Per exemple, si volguéssim estudiar una població d'aus, podria ser rellevant distingir els ocells en funció de la mida del bec i de la longitud de les ales. En aquest cas prendríem $\Omega = \mathbb{R}_+^2$.

De forma similar, considerem el conjunt de totes les *condicions ambientals* admissibles i el denotem amb el símbol $\mathcal{E}$. De forma més o menys general, es pot dir que la dinàmica d'una població està determinada per dos factors: els recursos de què disposa i les amenaces a les quals està exposada. En aquest sentit, el conjunt de *condicions ambientals* hauria de reflectir aquesta informació i obviar altres característiques ambientals supèrflues com, per exemple, la posició dels planetes al firmament (notem, però, que aquesta informació seria important si estudiéssim una població d'astrònoms i astrònomes, o fins i tot si consideréssim una població d'escarabats pilots, dels quals se sap que s'orienten amb les estrelles). En el cas que la població només depengui d'un tipus de recurs, $\mathcal{E}$ pot anar, en funció de la simplicitat del model, des d'un conjunt de dos elements com $\{\text{poc}, \text{molt}\}$ a un conjunt continu com $\mathbb{R}_+$ que reflecteixi la concentració del recurs en el medi. Si es tingués en compte la distribució espacial dels individus, aleshores els elements de $\mathcal{E}$ serien funcions que especificarien la concentració de recurs en cada posició.

3.1 Dinàmica poblacional donat el medi: teoria lineal

Per tal de plantejar el sistema dinàmic comencem suposant que la *condició ambiental* està donada per a tot temps. És a dir, considerem una funció $E: \mathbb{R} \rightarrow \mathcal{E}$ tal que $E(t)$ denota l'ambient del sistema a l'instant t .

Primer ingredient Sigui $u_E(t, s, \xi, \omega)$ la probabilitat que un individu amb *estat individual* $\xi \in \Omega$ en l'instant s tingui un *estat-i* contingut a $\omega \subset \Omega$ en l'instant posterior t sabent que la *condició ambiental* ve donada per E entre s i t .

Per definició es té que $u_E(s, s, \xi, \omega)$ és 1 si $\xi \in \omega$ i 0 en cas contrari, la qual cosa es pot escriure formalment utilitzant la delta de Dirac com $u_E(s, s, \xi, \omega) = \delta_\xi(\omega)$. Observi's també que la probabilitat que un individu amb *estat individual* ξ a l'instant s segueixi viu a l'instant posterior t és $u_E(t, s, \xi, \Omega) \leq 1$. A més a més, com que la dinàmica d'un individu només depèn del seu *estat-i* a l'instant s i de les *condicions ambientals* entre s i t , es conclou que les equacions de Chapman-Kolmogorov (vegeu [29]) se satisfan, és a dir, per a tot $\tau \in (s, t)$

$$u_E(t, s, \xi, \omega) = \int_{\Omega} u_E(t, \tau, \eta, \omega) u_E(\tau, s, \xi, d\eta). \quad (23)$$

Observem que E només cal que estigui definida entre τ i t al primer factor de la integral i entre s i τ en el segon. D'ara endavant utilitzarem, com a norma notacional, que el subíndex E en una funció que depèn de dues variables temporals indica que la funció només està afectada per la part de E definida entre aquestes dues variables.

Segon ingredient Sigui $\beta(\xi, \tilde{E}, \omega)$ el nombre esperat de descendents directes nascuts en $\omega \subset \Omega$ per unitat de temps que produeix un individu amb *estat individual* $\xi \in \Omega$ sabent que la *condició ambiental* instantània és $\tilde{E}$.

Combinant els ingredients β i u_E es pot definir

$$\beta_E^1(t, s, \xi, \omega) := \int_{\Omega} \beta(\eta, E(t), \omega) u_E(t, s, \xi, d\eta) \quad (24)$$

com el nombre esperat de nounats amb *estat-i* contingut a $\omega \subset \Omega$ que estan naixent per unitat de temps a l'instant t i que són descendents directes (fills i filles només) d'un individu amb *estat individual* $\xi \in \Omega$ a l'instant s , sabent que la *condició ambiental* entre s i t és la donada per E .

A partir del significat de la funció β_E^1 és possible construir un sistema dinàmic per a les *històries dels naixements*. El sistema pren la forma d'una equació de renovació, i s'obté observant que els nounats que estan naixent al present són necessàriament descendents directes d'individus nascuts al passat. Així, el nombre esperat de nounats amb *estat-i* contingut a $\omega \subset \Omega$ que estan naixent per unitat de temps a l'instant t , magnitud que denotem com a $B(t, \omega)$, s'obté «sumant» els descendents directes de les diferents cohorts d'edat nascudes al passat. La descripció anterior s'escriu formalment com

$$B(t, \omega) = \int_0^\infty \int_{\Omega} \beta_E^1(t, t-a, \xi, \omega) B(t-a, d\xi) da. \quad (25)$$

Observem que és possible recuperar la mesura poblacional en un instant t si es coneix la història de B fins a l'instant t . Només cal seguir la dinàmica dels individus des del moment en què neixen fins a l'instant t , la qual cosa és possible si es disposa del primer ingredient del model. En efecte, si denotem amb $m(t, \omega)$ la quantitat d'individus que hi ha d'*estat-i* contingut a $\omega \subset \Omega$ a l'instant t , tenim

$$m(t, \omega) = \int_0^\infty \int_{\Omega} u_E(t, t-a, \xi, \omega) B(t-a, d\xi) da. \quad (26)$$

3.2 Dinàmica poblacional i ambiental: teoria no lineal

Considerem ara que els individus de la població poden alterar la *condició ambiental*, de manera que aquesta deixa de ser independent de la població. L'efecte concret que tenen els individus sobre l'ambient és un altre ingredient del model.

Tercer ingredient Sigui $\gamma(\xi, \tilde{E})$ la taxa de canvi que experimenta el medi quan la *condició ambiental* és $\tilde{E}$ degut a les accions d'un individu d'*estat individual* ξ . Ens referim a la funció γ com l'alteració ambiental *per capita*.

«Sumant» l'alteració ambiental que provoca cada individu d'una població obtenim la taxa de canvi ambiental degut a la població en conjunt. Denotem aquesta taxa amb la lletra g i ens hi referim com l'alteració ambiental poblacional. Formalment, si m és la mesura poblacional i $\tilde{E}$ és la *condició ambiental*, l'alteració ambiental poblacional ve donada per

$$g(\tilde{E}, m) := \int_{\Omega} \gamma(\eta, \tilde{E}) m(d\eta). \quad (27)$$

Notem que implícitament estem suposant que cada individu afecta l'ambient de forma independent. Això, però, no és una restricció sinó una conseqüència del fet que la informació que determina el comportament d'un individu està continguda a la *condició ambiental*. En aquest sentit, si es produeixen interaccions directes entre individus diferents (depredació, cooperació, aparellament, etc.), aleshores la *condició ambiental* ha de recollir els detalls pertinents de la distribució poblacional per tal de reflectir aquestes interaccions. De fet, el que passa en aquestes situacions és que l'ambient efectiu d'un individu no només conté recursos aliens a la població sinó també elements de la mateixa població.

A més a més dels canvis ambientals provocats per la població, el medi també pot manifestar una dinàmica intrínseca. Aquest és el darrer ingredient del model.

Quart ingredient Sigui $g_0(\tilde{E})$ la taxa de canvi que experimenta el medi quan la *condició ambiental* és $\tilde{E}$ degut a causes alienes a la població.

Amb aquesta informació és possible donar una equació diferencial per a la *condició ambiental*. Si no hi ha cap individu en la població modelitzada, aleshores l'alteració ambiental poblacional és nul·la i l'equació diferencial és simplement

$$E'(t) = g_0(E(t)).$$

En general, si la mesura poblacional està descrita per una funció $m(t)$, es té

$$E'(t) = g_0(E(t)) + g(E(t), m(t)). \quad (28)$$

Com hem vist en l'apartat anterior, la mesura poblacional $m(t)$ es pot escriure en termes de la història de naixements fins a l'instant t utilitzant l'equació (26). Per tant, l'equació (28) relaciona la dinàmica dels naixements amb la dinàmica ambiental, la qual cosa acobla les equacions (25) i (28). D'aquesta manera s'obté un sistema no lineal amb retard que involucra una equació de renovació i una equació diferencial amb retard. Prenent $t > 0$ i $\theta \leq 0$, de manera que t es

pot pensar com un instant del futur (posterior a 0) i θ com un instant del passat (anterior a 0), el problema en qüestió s'escriu com

$$\begin{cases} B(t, \omega) = \int_{-\infty}^t \int_{\Omega} \beta_E^1(t, \tau, \xi, \omega) B(\tau, d\xi) d\tau, \\ E'(t) = g_0(E(t)) + \int_{\Omega} \gamma(\eta, E(t)) \int_0^{\infty} \int_{\Omega} u_E(t, t-a, \xi, d\eta) B(t-a, d\xi) da, \\ B(\theta, \omega) = \phi_1(\theta, \omega), \\ E(\theta) = \phi_2(\theta), \end{cases} \quad (29)$$

on ϕ_1 i ϕ_2 són les històries inicials de B i E . Observem que com a variables d'estat estem agafant històries tant de les taxes de naixement com de la *condició ambiental*. Observem també que l'equació de renovació per a la funció B pot fer que aquesta presenti discontinuïtats, mentre que l'equació diferencial amb retard suggereix que la funció E és contínua. Per aquests motius prenem com a espai de fase del sistema dinàmic definit per (29) l'espai

$$L^1((-\infty, 0); \mathcal{M}(\Omega)) \times C((-\infty, 0]; \mathcal{E}),$$

on $\mathcal{M}(\Omega)$ denota el conjunt de mesures definides sobre el conjunt Ω i recordem que la condició ambiental pren valors al conjunt $\mathcal{E}$. Com és habitual en equacions amb retard, una solució $(B(t, \cdot), E(t))$ de (29) defineix un punt d'aquest espai d'estats mitjançant $B_t(\theta) := B(t + \theta, \cdot)$, $E_t(\theta) := E(t + \theta)$.

Notem també que si la història de B fins a l'instant s és donada per ϕ , de manera que $B(\tau, \omega) := \phi(\tau, \omega)$ per a tot $\tau \leq s$, aleshores (25) es pot reescriure com

$$B(t, \omega) = \int_s^t \int_{\Omega} \beta_E^1(t, \sigma, \xi, \omega) B(\sigma, d\xi) d\sigma + F(t, \omega), \quad (30)$$

on $F(t, \omega)$ és la taxa de naixements de nounats amb *estat-i* contingut a $\omega \subset \Omega$ que són descendents directes d'individus que a l'instant s ja existien, *i. e.*,

$$\begin{aligned} F(t, \omega) &:= \int_{-\infty}^s \int_{\Omega} \beta_E^1(t, \sigma, \xi, \omega) \phi(\sigma, d\xi) d\sigma = \\ &= \int_{-\infty}^0 \int_{\Omega} \beta_E^1(t, s-a, \xi, \omega) \phi(s-a, d\xi) da. \end{aligned} \quad (31)$$

En resum, el sistema (29) es pot interpretar com una extensió de l'equació (25), que al seu torn és una generalització de l'equació de Volterra (12).

Finalment volem acabar aquesta teoria abstracta de poblacions amb un exemple il·lustratiu i, alhora, entenedor. Considerem una població estructurada per l'edat, de manera que $\Omega = [0, \infty)$. Suposem que la condició ambiental és un escalar que representa la concentració de nutrients, de manera que $\mathcal{E} = [0, \infty)$. Per determinar el primer ingredient fem la hipòtesi que la taxa de mortalitat

és una funció que depèn de l'edat i de la concentració de nutrients $\mu(a, E)$. En símbols tenim que

$$u_E(t, s, \xi, \omega) = e^{-\int_s^t \mu(\xi + \tau - s, E(\tau)) d\tau} \delta_{\xi + t - s}(\omega). \quad (32)$$

Per al segon ingredient, prenem $\beta(\eta, \tilde{E}, \omega) = \beta_0(\eta, \tilde{E}) \delta_0(\omega)$, la qual cosa significa que quan la condició ambiental és $\tilde{E}$, un individu d'edat η té una taxa de fertilitat $\beta_0(\eta, \tilde{E})$ i la δ de Dirac δ_0 apareix de manera natural ja que tots els individus neixen amb edat zero.

Per al tercer ingredient, suposem que el consum de nutrients per part d'un individu és proporcional a la concentració de nutrients i independent de la seva edat, de manera que $\gamma(\eta, \tilde{E}) = -c\tilde{E}$, $c > 0$.

Per al quart ingredient, suposem que els nutrients s'estan generant a una taxa constant $r > 0$ i que no es degraden de forma natural, de manera que $g_0(\tilde{E}) = r$. Tots aquests ingredients, usant (32), (24) i les formes especials de les funcions β i γ a (29), donen lloc al següent sistema no lineal amb retard

$$\begin{cases} B(t, \omega) = \int_{-\infty}^t \int_{[0, \infty)} \beta_0(\xi + t - \tau, E(t)) e^{-\int_{\tau}^t \mu(\sigma - \tau, E(\sigma)) d\sigma} B(\tau, d\xi) d\tau \delta_0(\omega), \\ E'(t) = r - cE(t) \int_{[0, \infty)} \int_0^{\infty} \int_{[0, \infty)} e^{-\int_{t-a}^t \mu(\sigma - t + a, E(\sigma)) d\sigma} \delta_{\xi+a}(d\eta) B(t-a, d\xi) da, \\ B(\theta, \omega) = \phi_1(\theta, \omega), \\ E(\theta) = \phi_2(\theta). \end{cases} \quad (33)$$

Observem que la primera equació és de la forma $B(t, \omega) = b(t) \delta_0(\omega)$. Considerant que això es dona per a qualsevol temps (cosa raonable ja que tots els individus neixen amb edat zero), les equacions dinàmiques del sistema anterior esdevenen:

$$\begin{cases} b(t) \delta_0(\omega) = \int_{-\infty}^t \beta_0(t - \tau, E(t)) e^{-\int_{\tau}^t \mu(\sigma - \tau, E(\sigma)) d\sigma} b(\tau) d\tau \delta_0(\omega), \\ E'(t) = r - cE(t) \int_0^{\infty} e^{-\int_{t-a}^t \mu(\sigma - t + a, E(\sigma)) d\sigma} b(t-a) da. \end{cases} \quad (34)$$

Si a més suposem que el recurs té una dinàmica ràpida i que està en un estat quasiestacionari (i.e. $E'(t) \approx 0$), llavors podem relacionar la població total, que recordem que ve donada per $P(t) = \int_0^{\infty} e^{-\int_{t-a}^t \mu(\sigma - t + a, E(\sigma)) d\sigma} b(t-a) da$, amb el mateix recurs:

$$E(t) = \frac{r}{cP(t)}$$

i aleshores (34) es redueix a una sola equació de renovació

$$b(t) = \int_{-\infty}^t \beta_0\left(t - \tau, \frac{r}{cP(t)}\right) e^{-\int_{\tau}^t \mu\left(\sigma - \tau, \frac{r}{cP(t)}\right) d\sigma} b(\tau) d\tau,$$

que és equivalent a l'equació de renovació del model no lineal de Gurtin i MacCamy (19) amb funcions β i μ adequades.

Certament, l'exemple anterior és prou senzill per a poder-lo tractar directament utilitzant la formulació amb equacions en derivades parcials. No obstant això, quan els estats dels individus són més complicats (vegeu, per exemple [30] i [18] on els individus estan estructurats per la mida i [8] on es té en compte la concentració intracel·lular d'una proteïna), llavors la formulació amb retard no només ens ajuda a plantejar el model en termes de propietats bàsiques dels individus, sinó que també ens permet fer una anàlisi més rigorosa sobre el comportament asimptòtic de les solucions entorn dels estats estacionaris.

Agraïments

Els autors han rebut parcialment el suport del Ministeri de Ciència i Innovació, referències MTM2017-84214-C2 i MTM2014-52402-C3, i de l'Agència de Gestió d'Ajuts Universitaris i de Recerca - Generalitat de Catalunya, referència 2017-SGR-1392.

Referències

- [1] ALLEN, L. J. S. *An Introduction to Mathematical Biology*. Upper Saddle River, NJ: Pearson Prentice Hall, 2007.
- [2] ANDERSON, E. C.; BELL, G. I.; PETERSEN, D. F.; TOBEY, R. A. «Cell growth and division IV. Determination of volume growth rate and division probability». *Biophys. J.*, 9 (1969), 246-263.
- [3] BACAËR, N. *A Short History of Mathematical Population Dynamics*. Londres: Springer-Verlag London, Ltd., 2011.
- [4] BARRIL, C.; CALSINA, À.; RIPOLL, J. «A practical approach to R_0 in continuous-time ecological models». *Math. Methods Appl. Sci.*, special issue paper (2017). DOI: 10.1002/mma.4673.
- [5] BELL, G. I. «Cell growth and division III. Conditions for balanced exponential growth in a mathematical model». *Biophys. J.*, 8 (4) (1968), 431-444.
- [6] BELL, G. I.; ANDERSON, E. C. «Cell growth and division I. A mathematical model with applications to cell volume distributions in mammalian suspension cultures». *Biophys. J.*, 7 (4) (1967), 329-351.
- [7] BERNOULLI, D. «Essai d'une nouvelle analyse de la mortalité causée par la petite vérole, et des avantages de l'inoculation pour la prévenir». *Mem. Math. Phys. Acad. R. Sci.* (1766), 1-45.
- [8] BORGES, R.; CALSINA, À.; CUADRADO, S.; DIEKMANN, O. «Delay equation formulation of a cyclin-structured cell population model». *J. Evol. Equ.*, 14 (4-5) (2014), 841-862.

- [9] BRAUER, F.; CASTILLO-CHÁVEZ, C. *Mathematical Models in Population Biology and Epidemiology*. Nova York: Springer-Verlag, 2001. (Texts in Applied Mathematics; 40)
- [10] BRAUN, M. *Differential Equations and Their Applications. An Introduction to Applied Mathematics*. Nova York: Springer-Verlag, 1975. (Applied Mathematical Sciences; 15)
- [11] BRITTON, N. F. *Essential Mathematical Biology*. Londres: Springer-Verlag London, Ltd., 2003. (Springer Undergraduate Mathematics Series)
- [12] DARWIN, C.; WALLACE, A. R. «On the tendency of species to form varieties; and on the perpetuation of varieties and species by natural means of selection». *Journal of the Proceedings of the Linnean Society. Zoology*, 3 (1858), 45-62.
- [13] DE ROOS, A. M.; DIEKMANN, O.; GETTO, P.; KIRKILIONIS, M. A. «Numerical equilibrium analysis for structured consumer resource models». *Bull. Math. Biol.*, 72 (2) (2010), 259-297.
- [14] DIEKMANN, O.; GETTO, P.; GYLLENBERG, M. «Stability and bifurcation analysis of Volterra functional equations in the light of suns and stars». *SIAM J. Math. Anal.*, 39 (4) (2007/08), 1023-1069.
- [15] DIEKMANN, O.; GYLLENBERG, M. «Abstract delay equations inspired by population dynamics». A: *Functional Analysis and Evolution Equations*. Basilea: Birkhäuser, 2008, 187-200.
- [16] DIEKMANN, O.; GYLLENBERG, M.; HUANG, H.; KIRKILIONIS, M.; METZ, J. A. J.; THIEME, H. R. «On the formulation and analysis of general deterministic structured population models. II. Nonlinear theory». *J. Math. Biol.*, 43 (2) (2001), 157-189.
- [17] DIEKMANN, O.; GYLLENBERG, M.; METZ, J. «Physiologically structured population models: towards a general mathematical theory». A: *Mathematics for Ecology and Environmental Sciences*. Berlín: Springer, 2007, 5-20. (Biol. Med. Phys. Biomed. Eng.)
- [18] DIEKMANN, O.; GYLLENBERG, M.; METZ, J. A. J.; NAKAOKA, S.; DE ROOS, A. M. «Daphnia revisited: local stability and bifurcation theory for physiologically structured population models explained by way of an example». *J. Math. Biol.*, 61 (2) (2010), 277-318.
- [19] DIEKMANN, O.; GYLLENBERG, M.; METZ, J. A. J.; THIEME, H. R. «On the formulation and analysis of general deterministic structured population models. I. Linear theory». *J. Math. Biol.*, 36 (4) (1998), 349-388.
- [20] DIEKMANN, O.; GYLLENBERG, M.; THIEME, H. R. «Semigroups and renewal equations on dual Banach spaces with applications to population dynamics». A: *Delay Differential Equations and Dynamical Systems*. Berlín: Springer, 1991, 116-129. (Lecture Notes in Math.; 1475)
- [21] DUBLIN, L. I.; LOTKA, A. J. «On the true rate of natural increase». *J. Amer. Statist. Assoc.*, 20 (151) (1925), 305-339.

- [22] EULER, L. *Introductio in analysin infinitorum*. Tomus primus. Lausana: apud Marcum-Michaelem Bousquet & Socies, 1748.
- [23] EULER, L. «Recherches générales sur la mortalité et la multiplication du genre humain». *Mémoires de l'Académie des sciences de Berlin*, 16 (1760), 144-164.
- [24] EULER, L. «A general investigation into the mortality and multiplication of the human species». *Theoret. Population Biol.*, 1 (3) (1970), 307-314. [Traduït per Nathan i Beatrice Keyfitz]
- [25] FELLER, W. «On the integral equation of renewal theory.» *Ann. Math. Statistics*, 12 (1941), 243-267.
- [26] FREDRICKSON, A. G.; RAMKRISHNA, D.; TSUCHIYA, H. M. «Statistics and dynamics of procaryotic cell populations». *Math. Biosci.*, 1 (1967), 327-374.
- [27] FREDRICKSON, A. G.; TSUCHIYA, H. M. «Continuous propagation of micro-organisms». *AIChE J.*, 9 (4) (1963), 459-468.
- [28] GURTIN, M. E.; MACCAMY, R. C. «Non-linear age-dependent population dynamics». *Arch. Rational Mech. Anal.*, 54 (1974), 281-300.
- [29] GYLLENBERG, M. «Mathematical aspects of physiologically structured populations: the contributions of J. A. J. Metz». *J. Biol. Dyn.*, 1 (1) (2007), 3-44.
- [30] HEIJMANS, H. J. A. M. «The dynamical behaviour of the age-size-distribution of a cell population». A: *The Dynamics of Physiologically Structured Populations*. Berlín: Springer, 1986, 185-202. (Lecture Notes in Biomath.; 68)
- [31] HEIJMANS, H. J. A. M.; METZ, J. A. J. «Small parameters in structured population models and the Trotter-Kato theorem». *SIAM J. Math. Anal.*, 20 (4) (1989), 870-885.
- [32] IANNELLI, M.; MARTCHEVA, M.; MILNER, F. A. *Gender-Structured Population Modeling: Mathematical Methods, Numerics, and Simulations*. Filadèlfia, PA: Society for Industrial and Applied Mathematics (SIAM), 2005. (Frontiers in Applied Mathematics; 31)
- [33] IANNELLI, M.; MILNER, F. *An Introduction to Mathematical Population Dynamics. Along the trail of Volterra and Lotka*. Cham: Springer, 2014. (Unitext-La Matematica per il 3 + 2; 79)
- [34] IANNELLI, M.; MILNER, F. *The Basic Approach to Age-Structured Population Dynamics. Models, Methods and Numerics*. Dordrecht: Springer, 2017. (Lecture Notes on Mathematical Modelling in the Life Sciences)
- [35] INABA, H. *Age-Structured Population Dynamics in Demography and Epidemiology*. Singapur: Springer, 2017.
- [36] KERMACK, W. O.; MCKENDRICK, A. G. «A contribution to the mathematical theory of epidemics». *Proc. Roy. Soc. London Ser. A*, 115 (1927), 700-721.
- [37] LOTKA, A. J. «Relation between birth rates and death rates». *Science*, 26 (653) (1907), 21-22.

- [38] LOTKA, A. J. «Analytical note on certain rhythmic relations in organic systems». *Proc. Natl. Acad. Sci. USA*, 6 (7) (1920), 410–415.
- [39] LOTKA, A. J. *The Elements of Physical Biology*. Baltimore: Williams & Wilkins Co.; Londres: Baillière, Tindall & Cox, 1925.
- [40] LOTKA, A. J. «On an integral equation in population analysis». *Ann. Math. Statist.*, 10 (2) (1939), 144–161.
- [41] LOTKA, A. J. *Elements of Mathematical Biology*. Nova York: Dover Publications, Inc., 1956. [Republicació sense sobresortir de la primera edició publicada sota el títol: *The Elements of Physical Biology* [39]]
- [42] MALTHUS, T. *An Essay on the Principle of Population*. Londres: J. Johnson, 1798.
- [43] METZ, J. A. J.; DIEKMANN, O. (ed.). *The Dynamics of Physiologically Structured Populations*. Berlín: Springer, 1986. (Lecture Notes in Biomathematics; 68)
- [44] M'KENDRICK, A. G. «Applications of mathematics to medical problems». *Proc. Edinburgh Math. Soc.*, 40 (1926), 98–130.
- [45] MURRAY, J. D. *Mathematical Biology*. Berlín: Springer-Verlag, 1989. (Biomathematics; 19)
- [46] ROSS, R. *The Prevention of Malaria*. Londres: John Murray, 1911.
- [47] SHARPE, F. R.; LOTKA, A. J. «A problem in age-distribution». *Philos. Mag.* (6), 21 (124) (1911), 435–438.
- [48] SINKO, J. W.; STREIFER, W. «A new model for age-size structure of a population». *Ecology*, 48 (6) (1967), 910–918.
- [49] SINKO, J. W.; STREIFER, W. «Applying models incorporating age-size structure of a population to *Daphnia*». *Ecology*, 50 (4) (1969), 608–615.
- [50] THIEME, H. R. *Mathematics in Population Biology*. Princeton, NJ: Princeton University Press, 2003. (Princeton Series in Theoretical and Computational Biology)
- [51] TSUCHIYA, H. M.; FREDRICKSON, A. G.; ARIS, R. «Dynamics of microbial cell populations». A: *Advances in Chemical Engineering*. Vol. 6. Nova York; Londres: Academic Press, 1966, 125–206.
- [52] TULJAPURKAR, S. «Stable population theory». A: *The New Palgrave Dictionary of Economics*. Londres: Palgrave Macmillan UK, 2008, 1–7.
- [53] VANSICKLE, J. «Analysis of a distributed-parameter population model based on physiological age». *J. Theoret. Biol.*, 64 (3) (1977), 571–586.
- [54] VOLTERRA, V. «Variazioni e fluttuazioni del numero d'individui in specie animali conviventi». *Memorie della Reale Accademia Nazionale dei Lincei* (6), 2 (1926), 31–113.
- [55] VON FOERSTER, H. «Some remarks on changing populations». A: *The Kinetics of Cellular Proliferation*. Nova York: Grune & Stratton, 1959, 382–407.
- [56] WEBB, G. F. «Nonlinear semigroups and age-dependent population models». *Ann. Mat. Pura Appl.* (4), 129 (1981), 43–55 (1982).

- [57] WEBB, G. F. *Theory of Nonlinear Age-Dependent Population Dynamics*. Nova York: Marcel Dekker, Inc., 1985. (Monographs and Textbooks in Pure and Applied Mathematics; 89)

CARLES BARRIL, SÍLVIA CUADRADO
DEPARTAMENT DE MATEMÀTIQUES
UNIVERSITAT AUTÒNOMA DE BARCELONA
EDIFICI C, FACULTAT DE CIÈNCIES
08193, Cerdanyola del Vallès, Barcelona
{carlesbarril,silvia}@mat.uab.cat

JORDI RIPOLL
DEPARTAMENT D'INFORMÀTICA, MATEMÀTICA APLICADA I ESTADÍSTICA
UNIVERSITAT DE GIRONA
AV. LLUÍS SANTALÓ, S/N
17003, GIRONA
jripoll@imae.udg.edu

Gaspard Monge

AGUSTÍ REVENTÓS

Resum: Aquest article vol ser un tribut a l'obra de Monge en el camp de la geometria diferencial de corbes i superfícies en els dos-cents anys de la seva mort. Després d'un breu recordatori de la seva biografia, ens centrem en els seus treballs sobre evolutes de corbes a l'espai i sobretot en el naixement de les línies de curvatura en un article dedicat al transport de terres. Analitzem en detall el full xv de les seves famoses *Feuilles d'analyse* i fem un breu comentari de la resta dels seus treballs sobre geometria diferencial. Acabem amb una nota de Josep Lluís Solé sobre un dels amics i biògraf de Monge: François Arago.

Paraules clau: Monge, corbes, superfícies, evolutes, línies de curvatura.

Classificació MSC2010: 53A04, 53A05, 01A50.

1 Introducció

El 28 de juliol d'aquest any 2018 s'ha complert dos-cents anys de la mort del gran geòmetra Gaspard Monge (1746-1818). Intentaré donar una visió resumida de la seva vida i obra centrant-me, però, només en els treballs de geometria diferencial, ja que l'obra global de Monge és immensa i abraça des de la química, a la meteorologia, la mecànica, etc.



Gaspard Monge (1746-1818).

A Monge se'l pot considerar, juntament amb Euler i Gauss, com el fundador de la geometria diferencial de corbes i superfícies. També se'l considera creador de la teoria de derivades parcials de segon ordre, que ell sempre estudiava lligades a problemes geomètrics, però que han tingut posteriorment tanta importància en altres camps.

Els treballs sobre la vida i l'obra de Monge escrits per persones que el coneixien directament i que són molt complets són els dels seus deixebles Charles Dupin [T7], de 1819, i el de François Arago [T1], de 1846.

El treball de Dupin es titula *Essai historique sur les services et les travaux scientifiques de Gaspard Monge*. Després d'una primera part biogràfica conté els capítols següents: «Géométrie pure et descriptive», «Géométrie analytique», «Géométrie appliquée aux arts», «Géométrie appliquée à la mécanique», «Physique: Attraction moléculaire», «Optique», «Météorologie», «Technologie: Feutrage», «Chimie générale», «Arts chimiques: Métallurgie», «Économie domestique: Fabrication des fromages de Lodézan», «Ouvrages et Mémoires publiés par G. Monge», «Monument à eriger en honneur de Monge», «Liste de souscripteurs».

Com veieu, hi podeu trobar la llista exhaustiva de les publicacions de Monge i els seus diversos camps d'interès, inclosos els formatges!¹

Dupin també fa un retrat de Monge que ens pot ajudar a acostar-nos al personatge ([T7, p. 150]):

Il étai d'une haute stature, la force physique se montrait dans ses larges muscles, comme la force morale se peignait dans son regard vaste et profond. Sa figure était large et raccourcie comme la face du lion. [...] Dès qu'il parlait, on croyait voir un autre homme. . . , un feu nouveau brillait dans ses yeux.

[Era alt, la força física es veia en els seus llargs muscles, com la força moral es reflectia en la seva mirada vasta i profunda. La seva figura era ampla i escurçada com la cara d'un lleó. [...] Quan parlava, hom creia veure un altre home. . . , un foc nou brillava en els seus ulls.]

El treball d'Arago² fou llegit a l'Académie des sciences el 1846, consta de 157 pàgines, i s'hi veu en tot moment la gran estima que Arago sentia per Monge. Dona molta informació interessant, per la proximitat temporal, sobre la Revolució Francesa i la campanya d'Egipte.

¹ Dupin va dedicar el seu primer llibre, *Développements de géométrie* [A1], de 1813, a Monge posant com a subtítol *Pour faire suite à la Géométrie Descriptive et à la Géométrie Analytique de M. Monge*, i dient:

MON ILLUSTRE MAÎTRE, Je vous dédie mon premier Ouvrage dans un genre où je dois tout à vos leçons; vos encouragements m'ont engagé dans la carrière aplanie par vos travaux [...]

[IL·LUSTRE MESTRE, us dedico la meva primera Obra sobre un tema en el qual ho dec tot a les vostres lliçons; els vostres encoratjaments m'han compromès en la carrera aplanada pels vostres treballs [...]]

² Per saber més sobre Arago, vegeu la secció 8, escrita per Josep Lluís Solé Clivillés.

Així mateix hem consultat els elogis fúnebres de dos dels seus primers alumnes a l'École polytechnique, N. Guyon [T10] i B. Brisson [T3], del mateix 1818.

També són d'interès els elogis que el 1849 dedica a Monge el director de l'escola de Beaune, F. Ravailhe [T12]. Es tracta de l'escola on va estudiar Monge de petit. Aquests elogis estan dedicats a la filla de Monge, Émilie, en aquell moment Madame Marey Monge, ja que s'havia casat amb Nicolas-Joseph Marey el 1789. El motiu és que l'esposa de Monge havia llegat al col·legi de Beaune la quantitat de 3 000 francs per dotar d'una beca anual l'alumne més distingit en matemàtiques durant l'any. El premi l'entregaven els fills d'Émilie.

Una obra molt documentada és *Un grand français. Monge fondateur de l'École polytechnique* [T5], de Louis de Launay (1933). Aprofundeix molt en la relació entre Monge i Napoleó i les tasques de Monge com a president del Senat. Però l'autor que més ha estudiat Monge, uns anys més tard (1951), és sens dubte René Taton a *L'œuvre scientifique de Monge* [T16]. És l'obra definitiva sobre el tema.

Trobareu més detalls sobre la vida, obra, deixebles i continuadors de Monge a les notes biogràfiques de Struik [T15]. També a l'article que Sergescu va escriure el 1946 amb motiu del bicentenari del naixement de Monge [T14].

Altres referències són els articles de Bruno Belhoste «Gaspard Monge: Urgences révolutionnaires et utopie» [T2] (1989), de José J. Etayo «Las bases de la Geometría Diferencial» [T8] (1993), i de Rémi Langevin «Gaspard Monge, de la planche à dessin aux lignes de courbure» [T11] (2002). També hi ha una molt bona informació a la Viquipèdia.

Les llistes bibliogràfiques que tanquen aquest article, tant la que es refereix als treballs de Monge com la dels treballs sobre Monge, no són exhaustives i fan referència només a les obres que he consultat. He procurat, això sí, que a la llista de treballs de Monge apareguin tots els relacionats amb la geometria diferencial, però les fronteres matemàtiques són difuses.

2 Breu biografia

Gaspard Monge neix el 9 de maig del 1746 a Beaune. Va ser el primer dels tres fills de Jacques Monge, un comerciant que va portar una vida de privacions per poder portar els fills a l'escola, concretament al Collège d'Oratoriens de Beaune.

El 1762 Gaspard acaba els estudis de filosofia, física i matemàtiques a Beaune. Amb només setze anys és nomenat professor de física a Lió. Segons Ravailhe [T12], el seu pare el va acomiadar dient: «Fill meu, recorda que en tota circumstància deus respecte als teus superiors i exemple als teus inferiors».

El 1764 fa un plànol detallat de Beaune que ofereix a la municipalitat. El coronel de Vignan, segon comandant de l'École royale du génie de Mézières,³ sap apreciar el treball i proposa al seu autor d'anar a Mézières.

³ L'escola d'enginyers de Mézières va ser fundada el 1748 pel cavaller de Chastillon, per tal de formar enginyers militars experts en fortificacions. Va agafar de seguida gran reputació. Les matemàtiques i la física eren ensenyades pels prestigiosos professors i abats Bossut i Nollet.

Hi entra, però com a alumne de segona categoria, destinat a un taller annex. Sembla que aquí ja treballa amb dovelles de guix, cosa que potser l'influirà en els seus treballs posteriors sobre el tall de pedres.

Per tal de resoldre problemes pràctics de fortificacions inventa, quan tenia aproximadament uns dinou anys, la *geometria descriptiva*. Com que aquests coneixements podien caure en mans de l'enemic, se li ordena de «ne rien divulguer ni verbalement ni par écrit». ⁴ No va poder explicar aquestes coses fins al 1794, quan es va crear l'École normale. Això va ser poc després del 9 de termidor, ⁵ quan la Convenció Nacional (règim polític que va governar França del 1792 al 1795) va sentir la necessitat de reorganitzar la instrucció pública.

El 1768 passa de *répétiteur* ⁶ a professor a Mézières i el 1771 es fa càrrec dels ensenyaments de matemàtiques i física. Aquest any fa un primer viatge a París, on coneix Condorcet, d'Alembert i Vandermonde; aquest últim tindrà un paper important durant la Revolució i exercirà influència sobre Monge. Vegeu «Monge, géomètre et Jacobin», de J. Chapelon [T4]. El 1772 és nomenat *correspondant* a l'Académie des sciences per un tribunal format per d'Alembert, Bossut i Condorcet.

Es casa el 1777 amb Marie-Catherine Huart, vídua Horbon, amb qui té tres filles, Émilie, Louise i Adélaïde. ⁷

El 14 de gener del 1780 Monge és elegit geòmetra adjunt de l'Académie des sciences, en substitució de Vandermonde. Això li exigeix estar-se a París almenys cinc mesos per any. Durant aquests períodes ajudava l'abat Bossut en els seus cursos al Louvre. Es va dedicar a la física i la química, va treballar amb Lavoisier, publicant memòries sobre la síntesi de l'aigua, tema de moda a l'època.

El 1783 mor Étienne Bézout, que exercia d'examinador dels alumnes de marina, i Monge és nomenat per a aquest càrrec. Això el fa abandonar definitivament l'École royale du génie de Mézières, ja que havia de viatjar molt. Va rebre de l'École una pensió de 1 000 lliures per any.

Quan esclata la Revolució Francesa, Monge és un dels científics més coneguts, probablement més pels seus treballs de física i química que com a matemàtic. Ocupa diversos llocs de direcció al club dels jacobins, i forma part de la comissió de pesos i mesures per introduir el sistema mètric decimal. ⁸

⁴ Diversos autors posen en dubte aquesta afirmació d'Arago.

⁵ Dia de l'arrest de Robespierre, 27 de juliol del 1794.

⁶ S'estava amb els alumnes a les sales d'estudi ajudant-los amb els treballs gràfics. Repetia el que havia explicat el professor.

⁷ Napoleó, en el seu desterrament a Santa Helena, va dir que Monge havia ofert les seves filles en matrimoni als primers soldats ferits en defensa de França, però Arago, després d'una conversa amb l'esposa de Monge, ho desmenteix o almenys ho matisa.

⁸ Monge ja participà en la comissió que l'Académie creà el 1789 per estudiar un pla per a la uniformització dels pesos i mesures, la qual aconsellà la proposta de Talleyrand a l'Assemblée National el 1790, en la qual exposen els avantatges de triar la longitud del pèndol que bat un segon en el paral·lel 45 com a unitat de mesura. El 1791 la proposta ja ha canviat: es decideix que la nova unitat sigui una fracció del meridià, i que es faran noves mesures del meridià de París entre Dunkerque i Barcelona (l'Académie necessita fer-se necessària en els convulsos temps revolucionaris). Monge i Meusnier són encarregats de mesurar les bases de la triangulació, però

A finals del 1792⁹ és elegit, per l'Assemblea, ministre de la Marina, càrrec que exercirà només fins a l'abril del 1793. El setembre del 1793 és encarregat, juntament amb Vandermonde i Berthollet, d'organitzar la fabricació de l'acer, per tal d'accelerar la fabricació d'armes. Publica *Description de l'art de fabriquer les canons* com a manual per a les fàbriques.



École polytechnique, de 1805 a 1976.

L'11 de març del 1794¹⁰ el Comitè de Salut Pública crea una comissió formada per Jacques-Éli Lamblardie, Gaspard Monge i Lazare Carnot amb la missió d'organitzar una «école central de travaux publics». Finalment s'inaugura el 21 de desembre amb seu al Palais Bourbon. L'1 de setembre del 1795 l'escola canvia de nom, passa a dir-se École polytechnique i s'ubica a l'Hôtel de Lassay. Es considera Monge com el seu principal fundador i impulsor. La seva experiència de vint anys a l'École royale du génie de Mézières va ser fonamental.

Monge va ser l'ànima de l'École. En va ser director del 1796 al 1799. Vivia rodejat dels seus alumnes, a qui no dubtava d'ajudar en tot el que podia, inclús oposant-se a l'emperador. Avui dia és universalment reconegut com un gran professor. Taton [T16], a la pàgina 367, cita paraules de Jomard, un dels alumnes de Monge:

Quand il décrivait une surface il la dessinait de ses mains... et l'engendrait avec un geste éloquent de manière à la rendre palpable; [...] il avait l'art de rendre simples les choses les plus compliquées et claires les plus obscures.

no compliran aquesta tasca ja que Meusnier, general de l'exèrcit, mor el 1793 en el setge de Mainz, i Monge és nomenat ministre.

També el 1793, el govern revolucionari suprimeix per elitisme l'Académie, però constitueix una «Comission temporaire des poids et mesures» en la qual hi ha Monge. Sense esperar els resultats de les medicions de Delambre i Méchain, s'acorda el 1795 definir un metre provisional, basat en les mesures del meridià fetes per La Caille quaranta anys abans. Monge col·labora en els càlculs corresponents.

Finalment, el 1798, una nova comissió estudia les dades aportades per Delambre i Méchain i encara que Monge hi figura, tampoc pot participar-hi, ja que acompanya Napoleó a Egipte.

Una referència molt bona sobre aquesta història apassionant és: Antonio E. Ten (1996), *Medir el Metro*, Instituto de Estudios Documentales e Históricos sobre la Ciencia, Universitat de València. [Pou de pàgina escrit per Josep Lluís Solé.]

9 El 13 d'agost del 1792 Lluís XVI és detingut i substituït per un consell format per ministres elegits per l'Assemblea.

10 «21 ventôse, an II», amb la notació de l'època.

[Quan descrivia una superfície la dibuixava amb les seves mans... i l'engendrava amb un gest eloqüent per fer-la palpable; [...] tenia l'art de fer simples les coses més complicades i clares les més fosques.]

Entre els deixebles de Monge destaquem Charles de Tinseau d'Amondans (1748-1822) i Jean Baptiste Meusnier (1754-1793), que ja van ser alumnes seus a Mézières. Citem també Sylvestre Lacroix (1765-1843), Jean Baptiste Joseph Fourier (1768-1830), Michel Ange Lancret (1774-1807), Joseph Diez Gergonne (1771-1859), André-Marie Ampère (1775-1836), Sophie Germain (1776-1831) (amb nom fals), Pierre Charles François Dupin (1784-1873), Louis-Léger Vallée (1784-1864), Jean-Victor Poncelet (1788-1867), Michel Chasles (1793-1880), Théodore Olivier (1793-1853), Benjamin Olinde Rodrigues (1795-1851), Gabriel Lamé (1795-1870), Adhémar Barré de Saint-Venant (1797-1886), etc.

Monge va ser també un dels principals inspiradors del *Journal de l'École polytechnique*.¹¹ El primer article del primer volum del *Journal*, aparegut el 1794, és de Monge i es titula «Stéréotomie» [M8]. L'estereotomia és l'art de tallar i acoblar les peces de pedra o fusta, per tal de construir elements arquitectònics com ara arcs, mènsules, trams d'escalas, etc.

Les primeres tres línies diuen:

La géométrie descriptive est l'art de représenter sur des feuilles de dessins qui n'ont que deux dimensions, les objets qui en ont trois, et qui sont susceptibles d'une définition rigoureuse.

[La geometria descriptiva és l'art de representar sobre els fulls de dibuix que no tenen més que dues dimensions, els objectes que en tenen tres, i que poden ser definits rigorosament.]

Els apunts de classe de Monge apareixen en diverses notes posteriors del *Journal*, signades per Eisenman i amb el mateix títol genèric de «Stéréotomie» [A3].

En aquesta època Monge va començar a parlar als seus alumnes de *geometria analítica* per referir-se al que fins al moment s'anomenava simplement *àlgebra aplicada a la geometria*.¹²

El 1796 va a Itàlia com a membre d'una comissió que ha de recollir «les monuments d'art et de science que les traités de paix accordaient aux armées françaises victorieuses». Com diu Louis de Launay [T5], un saqueig organitzat.

¹¹ A <http://gallica.bnf.fr/ark:/12148/cb34378280v/date.r=journal+ecole> podeu trobar els volums entre els anys 1794 i 1938.

¹² Lacroix, en el seu *Traité élémentaire de calcul différentiel et de calcul intégral* [A8], de 1797, per referir-se als treballs de Monge on aquest utilitza derivades parcials per generar superfícies, com per exemple «Sur l'expression analytique de la génération des surfaces courbes» [M6], diu: «Voyez sa Géométrie Analytique». Per aquest motiu es considera aquest llibre de Lacroix com el primer lloc on apareix aquesta expressió de *geometria analítica* (pàgina 504 de la quarta edició de Bachelier de 1828).

A [T5] podeu trobar informació sobre els cinc combois amb obres d'art que es van organitzar. Torna a París el 1797 i és nomenat director de la «pauvre École polytechnique», com diu ell mateix, que estava en hores baixes. Encara farà un segon viatge a Roma motivat per l'assassinat del general Duphot, que el Directori li encarrega investigar. I per comminar el papa Pius VI a abandonar el poder temporal. El Papa abandona Roma el 20 de febrer del 1798. Aquesta estada coincideix amb els preparatius de la campanya de Napoleó a Egipte.

Segons Arago, Napoleó s'havia sentit molt ben tractat pel ministre de marina Monge quan ell era un jove oficial d'artilleria. Això va fer néixer una amistat entre Monge i Napoleó, qui insisteix fortament perquè l'acompanyi a la campanya d'Egipte. Una amistat en la qual Napoleó manava i Monge obeïa.

Es troba amb Napoleó a Malta el 9 de juny del 1798. L'illa és conquerida el 10 de juny i el 13 de juny ja s'hi creen tretze escoles primàries i una escola central per ensenyar matemàtiques, astronomia, etc.

Un cop a Egipte va amb Napoleó fins a Ramanieh, on se separen i Monge remunta el Nil amb Berthollet. Són atacats pels turcs i els mamelucs, però salvats finalment per les tropes franceses.¹³ És llavors, el 20 de juliol del 1798, que Napoleó diu davant la piràmide de Gizeh la cèlebre frase: «Soldats, du haut de ces monuments, quarante siècles vous contemplent!».

Posteriorment Napoleó crea l'Institut d'Egipte i en confia la presidència a Monge.¹⁴ Pren part també en l'expedició a Síria, però es posa malalt i torna a París amb Napoleó l'octubre del 1799. Fan el viatge de Fréjus a París en cotxe de sis cavalls Berthollet, Monge i Napoleó. Segons Arago, la gent s'es-tranyava de veure Napoleó en companyia de dues persones mal vestides (feia gairebé dos anys que eren fora de casa). El desembre del mateix any és nomenat senador.

El 1803 acompanya Napoleó per Bèlgica i el nord de França. Tornant, és nomenat per a la senadoria de Lieja. Sembla que no ho accepta de gaire bon grat, ja que en una carta a la seva dona per justificar la seva absència comenta que «Le Premier Consul a tant fait pour moi que je dois faire ce que je puis pour lui». Hi fa llargues estades entre 1803 i 1805, any en què Napoleó dona a l'École polytechnique un estatus militar i la situa a la muntanya de Santa Genoveva a París.

Del maig del 1806 al setembre del 1807 és president del Senat de l'emperador, i rep una donació que ell mateix havia sol·licitat en favor de Berthollet de cent mil francs, amb la qual compra el castell de Bierre, a la Borgonya.

Nomenat compte de Péluse, el 1808, rep en dotació diverses propietats a Westfàlia.

¹³ El butlletí oficial del combat fa menció de la bravura de Monge i Berthollet. Però aquest últim es va omplir les butxaques de pedres per anar al fons del riu i no ser capturat i mutilat pels ferotges mamelucs. Molts d'aquests mamelucs es van acabar posant posteriorment al costat de Napoleó.

¹⁴ Del procés verbal (Arago [T1]): *le citoyen Monge, président; le citoyen Bonaparte, vice-président, pour le premier trimestre; et le citoyen Fourier, secrétaire perpétuel*. Sobre la campanya d'Egipte vegeu *Gaspard Monge et l'expédition d'Égypte*, de Jean-Baptiste Sanson de Pongerville [T6].

El 1809, començant a sentir-se cansat, deixa amb recança l'École polytechnique; però no la relació científica que hi tenia, ja que entre 1810 i 1816 encara podem trobar a *Correspondance sur l'École impériale polytechnique* set notes molt breus de Monge, potser la més important de les quals és «Sur les équations différentielles des courbes du second degré» [M17].

El 1813 intenta organitzar la resistència contra els invasors (Àustria, Rússia i Prússia). El febrer del 1814, dos mesos abans que Napoleó fos desterrat a Elba, pel tractat de Fontainebleau, destrueix part dels seus documents de la Revolució, en particular la correspondència amb Napoleó, i, fugint de l'enemic, abandona París el 29 de març.

Quan torna a París el 1816, després d'haver estat amagat un temps, veu destruir la seva obra: l'École polytechnique és primer suprimida i després reorganitzada, és exclòs de l'Académie des sciences,¹⁵ etc. Mor el 28 de juliol del 1818. Els alumnes de l'École polytechnique no van tenir autorització per assistir als funerals de Monge, que no va rebre cap homenatge oficial, però van aprofitar el primer dia de sortida per anar-se a inclinar sobre la tomba del fundador de la seva escola.

3 Memòria sobre les evolutes

Comentem a continuació el que es considera com el primer article de Monge [M7]. El 22 de gener del 1769 Monge va escriure a l'abat Charles Bossut per a explicar-li que estava treballant en «développées» de corbes de doble curvatura.¹⁶

En réfléchissant dernièrement sur ce qui arrive à plusieurs surfaces courbes que l'on fait mouvoir les unes sur les autres pour engendrer des épicycloïdes sur toutes sortes de surfaces, je suis parvenu à trouver les développées des courbes à double courbure. [Taton [T16, p. 166]]

[Reflexionant darrerament sobre el que passa a diverses superfícies corbes que es fan moure les unes sobre les altres per engendrar epicicloides sobre tot tipus de superfícies, he arribat a trobar les evolutes de les corbes de doble curvatura.]

Recordem que la *développée* o *evoluta* d'una corba plana és la corba que s'obté com a envoltent de les seves normals. Equivalentment, és la corba que té la propietat que un cordill embolicat sobre ella, en desembolicar-se, genera la corba donada. Monge generalitza aquesta construcció a l'espai exigint que en desenvolupar el cordill es vagi mantenint sempre sobre la superfície formada per les tangents a la corba (la *desenvolupable tangencial*).

¹⁵ Tothom va veure la greu injustícia que es feia amb Monge, i Cauchy va ser durament criticat pel fet d'acceptar el lloc vacant.

¹⁶ Amb l'expressió *corbes de doble curvatura* es refereix a corbes guerxes (no planars) de l'espai. Les dues curvatures serien en llenguatge actual la curvatura i la torsió.

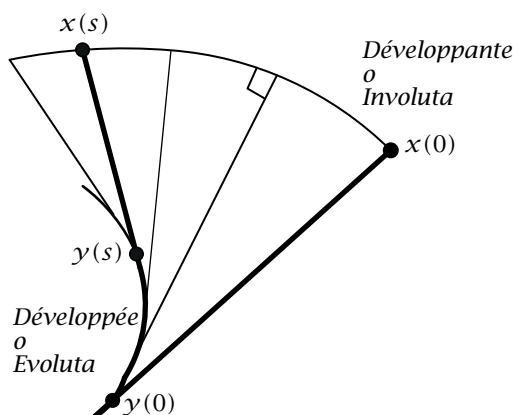


FIGURA 1: Evolutes i involutes.

Concretament, l'*evoluta* d'una corba $x(s)$ de l'espai és una altra corba $y(s)$ (la *développante* o *involuta*) tal que $x(s)$ està continguda a la desenvolupable tangencial de $y(s)$ i la tangent a $y(s)$ pertany al pla normal a $x(s)$ en el punt corresponent. Desenrotllant un cordill prèviament embolicat a $y(s)$, mantenint-lo en la superfície de les tangents, obtenim $x(s)$.

El juny del 1769 va aparèixer un sumari dels seus resultats al *Journal encyclopédique*, editat a Bouillon per Pierre Rousseau, que es considera com la primera publicació de Monge.¹⁷ El treball complet es va sotmetre a l'Académie des sciences de París l'octubre del 1770 i es va llegir davant l'Académie l'agost del 1771, però no es va publicar fins al 1785 amb el títol «Mémoire sur les développées, les rayons de courbure, et les différents genres d'inflexions des courbes à double courbure»; vegeu [M7] i les pàgines 392–420 de [M18].

Aquest article comença així:

Tout ce que l'on a fait jusqu'à présent sur les Développées des courbes en general se réduit à avoir trouvé celles des courbes planes [...] Je me propose de démontrer dans ce Mémoire qu'une courbe, plane ou à double courbure a une infinité de développées, toutes à double courbure, à l'exception d'une seule pour chaque courbe plane, et de donner la manière de trouver les équations de telle de ces courbes qu'on voudra, étant données les équations de la développante.

[Tot el que s'ha fet fins ara sobre les evolutes de corbes en general es redueix a haver trobat les de les corbes planes [...] Em proposo demostrar en aquesta Memòria que una corba, plana o de doble curvatura, té una infinitat d'evolutes, totes de doble curvatura, amb l'excepció d'una sola per a cada corba plana, i donar la manera de trobar les equacions d'aquestes corbes, donades les equacions de la involuta.]

¹⁷ Vegeu l'article de René Taton «La première note mathématique de Gaspard Monge» [T17], on es reproduïx aquest escrit.

La figura 2 mostra una corba plana i algunes de les seves evolutes, que, com ja va observar Monge, estan sobre la superfície polar, és a dir, la superfície reglada formada per rectes que passen pels centres de curvatura i tenen la direcció de la binormal corresponent.

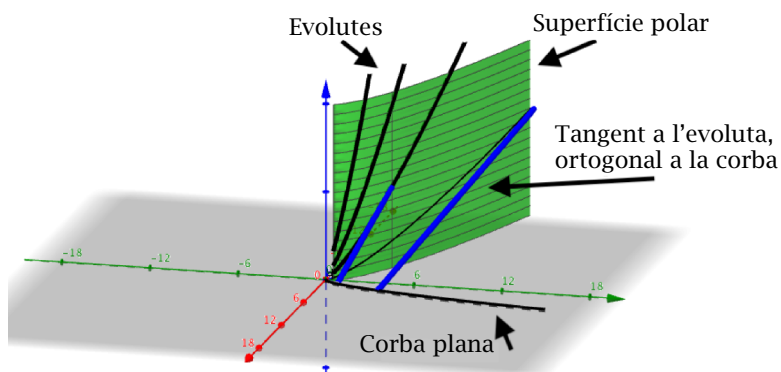


FIGURA 2: Evolutes i superfície polar.

Veiem com introdueix Monge l'eix polar. Comença observant que les normals en un punt no singular d'una corba a l'espai estan en un pla. En aquest pla es troba una recta que ell anomena «eix», que és el límit de la intersecció d'aquest pla amb el pla corresponent a un altre punt de la corba, infinitament pròxim. És a dir, cada punt P de la corba té el seu «eix». Si hom traça una perpendicular des de P a l'eix corresponent a P i anomenem Q el peu d'aquesta perpendicular, Q serà el centre de curvatura, PQ el radi de curvatura, i la inversa de la longitud PQ , la curvatura.

Com diu Girbau [A6], d'aquesta manera s'estableix clarament per primer cop la noció de *curvatura* d'una corba a l'espai.

La *torsió* hi apareix implícitament.¹⁸ Amb notació actual l'eix polar corresponent al punt de paràmetre s de la corba $\gamma(s)$ és la recta

$$r(u) : \gamma(s) + \rho(s)N(s) + uB(s),$$

on $\rho(s)$ és el radi de curvatura i $N(s)$, $B(s)$ els vectors normal principal i binormal, respectivament.

La unió de totes aquestes rectes és la superfície reglada

$$\varphi(s, u) = \gamma(s) + \rho(s)N(s) + uB(s),$$

anomenada *superfície polar* associada a la corba $\gamma(s)$. Monge la calcula a la secció XX de l'article i troba que és la superfície envoltant de la família de plans

¹⁸ El concepte de torsió va ser definitivament establert més tard per Lancet a «Mémoire sur les courbes a double courbure» [A9], però havia estat usat ja per Lacroix a [A8]. L'anomenaven *segona flexió* o *segona curvatura*. El nom de *torsió* prové de Louis L. Vallée.

normals. És a dir, veu que el pla tangent a aquesta superfície en qualsevol dels seus punts coincideix amb un dels plans de la família de plans normals.

Demuestra també que aquesta superfície és *desenvolupable*,¹⁹ veient que les seves generatrius, els eixos polars, són tangents a la corba formada pels centres de les esferes osculatius.

Aquesta corba dels centres és anomenada per Monge *arête de rebroussement*, nom que podríem traduir per *aresta de retrocés* o *eix de regressió*, de la superfície polar, i ve donada per

$$\gamma(s) + \rho(s)N(s) + \frac{\rho'(s)}{\tau(s)}B(s),$$

on $\tau(s)$ és la torsió de $\gamma(s)$ (suposada no nul·la). Monge la calcula a la secció XXII de l'article.

Els punts d'aquesta aresta no formen part de la superfície (són punts singulars), que queda, doncs, dividida en dues parts.

Tot això ho fa Monge amb arguments geomètrics com ara tallar un pla amb el «següent», etc., ja que aquesta superfície és, com hem dit, l'envolvent dels plans normals.

L'esfera osculatriu²⁰ la introdueix així a la secció XXIV:

[...] dans toute courbe à double courbure trois éléments consécutifs sont toujours à égales distances d'un certain point, et peuvent, par conséquent, être regardés comme placés sur la surface d'une même sphère dont ce point est le centre.

[...] en tota corba de doble curvatura tres elements consecutius estan sempre a la mateixa distància d'un cert punt, i poden, per consegüent, ser vistos com situats sobre la superfície d'una mateixa esfera que té aquest punt com a centre.]

Dels càlculs anteriors es dedueix que el radi de l'esfera osculatriu és

$$R(s) = \sqrt{\rho(s)^2 + \left(\frac{\rho'(s)}{\tau(s)}\right)^2}.$$

També es veu que la corba formada pels centres de curvatura d'una corba (projecció d'aquesta corba sobre l'eix polar) no pot ser una evoluta de la

¹⁹ Una superfície reglada es diu *desenvolupable* si les rectes que la formen són tangents a una corba (eix de regressió). Equivalentment, són les superfícies reglades amb curvatura de Gauss zero o encara una altra equivalència: són les superfícies reglades tals que el pla tangent és constant al llarg de les generatrius.

²⁰ Théodore Olivier (1793-1853), alumne de l'École polytechnique, estudia les esferes osculatius i l'ordre de contacte d'aquestes amb les hèlixs, vegeu «De la courbure et la flexion d'une courbe à double courbure» [A12]. És conegut pels seus models de superfícies que es tallen, superfícies formades per cordes i metall, que en moure's permeten estudiar la corba intersecció. Vegeu *Theodore Olivier Three-Dimensional Geometry String Models*, un àlbum editat pel Canada Science and Technology Museum.

corba donada a menys que aquesta sigui plana. En aquest cas tenim la clàssica evoluta, una corba les tangents de la qual són normals a la corba donada.

Donada una corba $x(s)$ Monge es proposa, a la secció xxv, trobar totes les corbes $y(s)$ (*les evolutes de $x(s)$*) tals que les tangents a $y(s)$ pertanyen al pla normal de $x(s)$. És a dir, vol trobar les corbes que si es desenvolupen pel mètode del cordill donen $x(s)$.

Amb notació actual s'obté

$$y(s) = x(s) + \rho(s)(N(s) + \cot \alpha(s)B(s)),$$

on $\rho(s)$ és el radi de curvatura, $N(s)$, $B(s)$ la normal principal i la binormal de $x(s)$, i

$$\alpha(s) = \int_0^s \tau(t) dt + c,$$

amb $\tau(s)$ la torsió.

Cada valor de c correspon a una de les infinites evolutes de la corba $x(s)$. Si $\tau = 0$, una de les evolutes és plana i les altres són hèlixs sobre el cilindre ortogonal al pla de la corba.

Quan parla dels *diferents gèneres d'inflexió*, a la secció xxx, es refereix al fet que la curvatura i la torsió es poden anul·lar. Ho diu així:

[...] il peut arriver ou que trois éléments consécutifs d'une même courbe à double courbure se trouvent dans un même plan, ou que deux de ces éléments soient en ligne droite. Il suit de là que les courbes à double courbure peuvent avoir deux espèces d'inflexions: la première a lieu lorsque la courbe devient plane, et nous l'appellerons *simple inflexion*; la seconde, que nous appellerons *double inflexion*, a lieu lorsque la courbe devient droite dans un de ses points.

[...] pot passar que tres elements consecutius d'una mateixa corba de doble curvatura es trobin en un mateix pla, o que dos d'aquests elements estiguin alineats. Se segueix d'això que les corbes de doble curvatura poden tenir dos tipus d'inflexions: la primera es dona quan la corba esdevé plana, i nosaltres l'anomenarem *inflexió simple*; la segona, que anomenarem *inflexió doble*, té lloc quan la corba esdevé recta en un dels seus punts.²¹

Cap al final de l'article, a la secció xxxiii, troba l'expressió explícita del radi de curvatura de la corba (amb la seva notació $y = \varphi x$, $z = \psi x$)

$$\frac{[1 + (\varphi'x')^2 + (\psi'x')^2]^{3/2}}{\sqrt{(\varphi''x')^2 + (\psi''x')^2 + (\psi'x'\varphi''x' - \varphi'x'\psi''x')^2}}$$

que, posant $\sigma(s) = (s, \varphi(s), \psi(s))$, no és més que

$$\rho(s) = \frac{\|\sigma'(s)\|^3}{\|\sigma'(s) \wedge \sigma''(s)\|}.$$

²¹ Com és ben sabut, si la curvatura és zero en un interval, la corba és recta en aquest interval, i si la torsió és zero en un interval, la corba és plana en aquest interval. Però la curvatura i la torsió es poden anul·lar només en un sol punt (punt d'inflexió) i llavors la corba no és recta ni plana al voltant d'aquest punt.

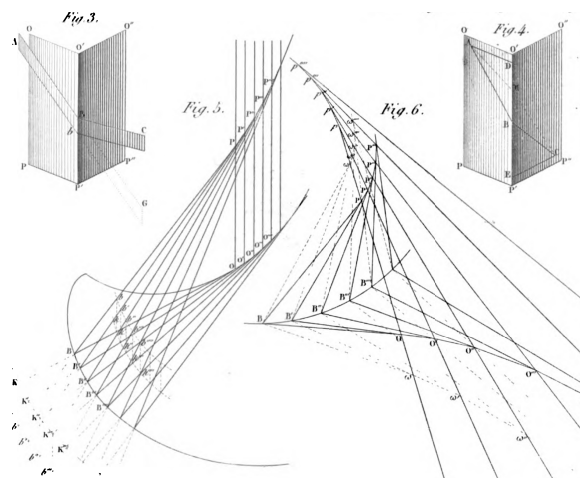


FIGURA 3: Detall de la planxa que tanca aquest article de Monge.

4 Ombres i penombres

L'11 de gener del 1775 Monge presenta a l'Académie el treball «Mémoire sur les propriétés de plusieurs genres de surfaces courbes, particulièrement sur celles des surfaces développables, avec une application à la théorie des ombres et des pénombres» [M1], que no es publica fins al 1780.

En aquesta memòria dona l'avui ben coneguda equació del pla tangent en funció de determinades derivades parcials, que denota per p i q , notació que ha perdurat fins a l'actualitat. I també l'equació diferencial de les superfícies desenvolupables, $rt - s^2 = 0$, on ara r , s , t són les derivades segones. Observeu que aquesta expressió només diu que la curvatura de Gauss és zero ja que és el determinant de la segona forma fonamental. El problema I d'aquest l'article està dedicat a trobar l'equació general de les superfícies desenvolupables. En dona tres solucions i alguns corollaris.

El problema II consisteix a trobar les superfícies tals que la relació entre l'àrea d'una part qualsevol d'elles i la seva projecció [sobre un pla] és constant. Òbviament, amb la mateixa notació que anteriorment, ha de passar que $\sqrt{1 + p^2 + q^2}$ sigui constant i, per tant, que p sigui funció de q .

A continuació introdueix la *théorie générale des ombres et des pénombres*. Dona una definició precisa d'ombra i penombra suposant primer que hi ha un punt de llum i un cos opac que la tapa i suposant després que la llum prové d'una superfície. Demostra que en aquest cas l'ombra «pura» està delimitada per una superfície desenvolupable circumscrita a la vegada a les superfícies del cos lluminós i del cos opac. Dona una definició intuïtiva de penombra i demostra que està determinada per una altra superfície desenvolupable parcialment circumscrita també a les superfícies dels cossos opac i lluminós.

La diferència entre aquesta superfície i la primera és que l'aresta de retrocés (*arête de rebroussement*) es troba entre els dos cossos i en el primer cas els dos cossos són al mateix costat d'aquesta arista. Aquestes demostracions les presenta sense fer cap càlcul.

Posa com a exemple el cas de dos cossos esfèrics, com els de la figura 4.

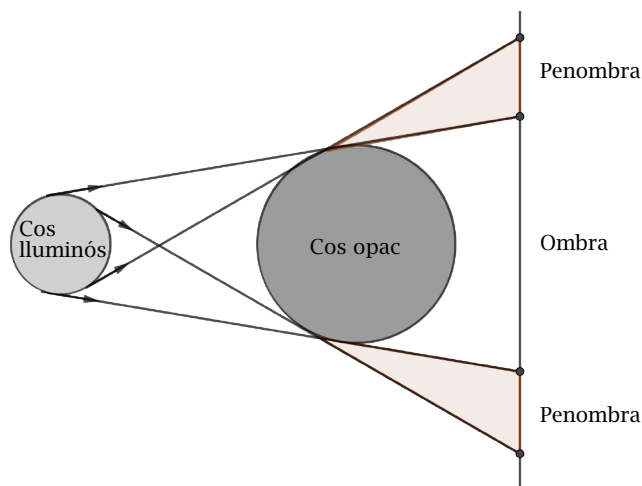


FIGURA 4: Ombres i penombres.

El problema III d'aquest article consisteix a trobar, per a una superfície donada, l'equació de la corba intersecció d'aquesta superfície amb un con circumscrit a la mateixa, de vèrtex un punt donat. Està estudiant, doncs, ombres i penombres en el cas particular en què el cos lluminós es redueix a un punt. Actualment es diu que aquesta corba és la corba generadora del contorn o corba generatriu. Està caracteritzada per la condició de ser el vector normal a la superfície sobre aquesta corba perpendicular en cada punt a la recta determinada per aquest punt i el punt de llum. Monge, a l'article que comentarem a continuació, [M2], en diu *corba de contorn aparent*.

L'article [M1] acaba amb un parell de problemes sobre el mateix tema. El problema IV s'ocupa de trobar la superfície cònica amb vèrtex donat que passa per una corba donada, i en el problema V estableix les equacions de les superfícies que envolten l'ombra i la penombra d'un cos opac il·luminat per un cos lluminós.

5 Teoria del transport

En aquesta secció estudiem un dels articles més importants de Monge, «Mémoire sur la théorie des déblais et des remblais» [M2], de 1781.²²

²² Aquest article està molt ben estudiat per Étienne Ghys a [T9]. Comenta Ghys que, com en altres treballs de Monge, es barreja aquí la teoria i la pràctica. Monge parteix d'un problema pràctic,

Aquest article comença parlant del transport de terres.

Lorsqu'on doit transporter des terres d'un lieu dans un autre, on a coutume de donner le nom de *Déblai* au volume des terres que l'on doit transporter, et le nom de *Remblai* à l'espace qu'elles doivent occuper après le transport.

[Quan s'han de transportar terres d'un lloc a un altre, es té el costum d'anomenar *déblai* el volum de terres que s'ha de transportar, i anomenar *remblai* l'espai que han d'ocupar després del transport.]

I continua comentant que, com que el preu del transport d'una molècula és proporcional al seu pes i a l'espai que recorre, el preu total del transport ha de ser proporcional a la suma dels productes de les molècules (els seus pesos) multiplicada cadascuna per l'espai recorregut, i també que donat el *déblai* i el *remblai* en figura i posició, no és indiferent que una molècula del *déblai* sigui transportada a un lloc o altre del *remblai*. S'ha d'aconseguir que la suma d'aquests productes sigui la mínima possible per tal de minimitzar el preu del transport.

Pl. 1.

Mém. de l'Ac. R. des Sc. An. 1781. Page. 704. Pl. XVIII.

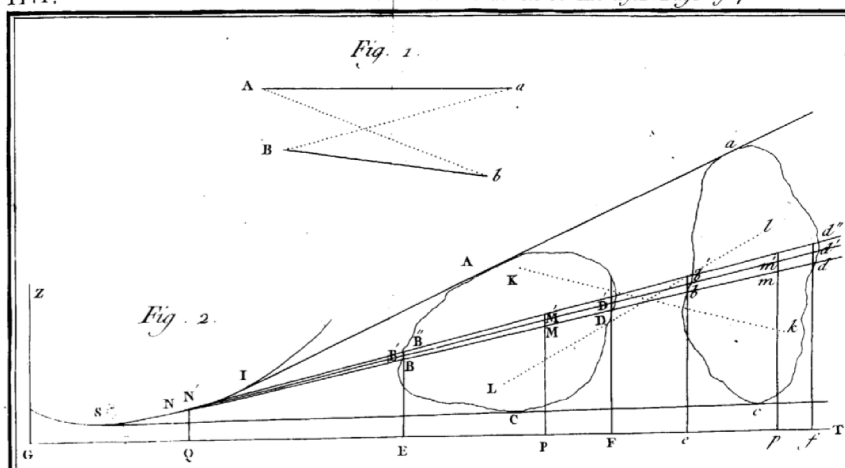


FIGURA 5: Dibuix de Monge del *déblai* i el *remblai*. Les rectes determinen una àrea igual sobre cada figura, $ABD = abd$. Són tangents a una corba. BD ha d'anar a bd .

Aquest problema ha donat lloc a la *teoria del transport*, molt usada també en economia. En llenguatge actual es tracta de minimitzar una integral del tipus

$$\int_D \|F(x, y) - (x, y)\| dx dy,$$

on D és el *déblai* i F la transformació entre *déblai* i *remblai*.

que en realitat no acaba de resoldre, però que li serveix de motivació i que dona lloc a importants desenvolupaments teòrics.

Feta aquesta introducció, Monge divideix la memòria en dues parts: el cas del pla i el cas de l'espai.

Dimensió 2

Després d'observar que les trajectòries seguides per les molècules no es poden tallar, ja que la suma de distàncies $Ab + Ba$ és major que $Aa + Bb$, torna a repetir l'enunciat pel pla:

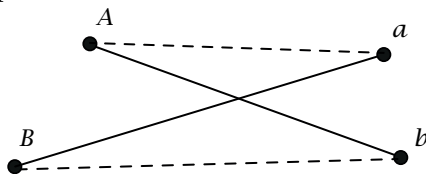


FIGURA 6: Transport en el pla.

Donades dues àrees iguals, trobar el camí que ha de seguir cada molècula de la primera i el punt on ha d'arribar de la segona per tal que, quan s'han transportat tots els punts, la suma dels productes de cada molècula (el seu pes) per l'espai que ella ha recorregut sigui mínim. Suposa per simplificar que la densitat és uniforme.²³

Primer argumenta que si una recta talla el *déblai* i el *remblai* deixant a un mateix costat àrees iguals, les molècules de la primera regió han d'anar a parar a les de la segona.²⁴ En el dibuix de Monge (figura 5), la regió ABD ha d'anar a la regió abd (sempre utilitza majúscules per al *déblai* i minúscules per al *remblai*). I conclou que, dividint el *déblai* i el *remblai* en una infinitat de petits rombes, cadascun dels rombes del *déblai* ha de ser transportat sobre el corresponent rombe del *remblai*. I que és indiferent en quin ordre les molècules del primer es distribueixen sobre el segon.

Introdueix coordenades i dona una fórmula per a la direcció de cada molècula. La tècnica consisteix a transformar la família biparamètrica de rectes $y = ax + b$ en una família uniparamètrica en imposar que aquestes rectes tallin, del mateix costat, *déblai* i *remblai* en regions d'àrea igual.

Si l'envolvent d'aquesta família uniparamètrica de rectes està a l'esquerra del *déblai*, les seves tangents tallen el *déblai* i el *remblai* en segments BD i bd , respectivament. En aquest cas el que s'ha de fer és transportar el segment BD sobre el segment bd .

S'adona, però, que, com que trajectòries de punts pròxims es poden tallar, i això no donaria un mínim, cal que la càustica²⁵ que es forma com a envolvent dels camins es trobi més enllà del *déblai* respecte del *remblai* o més enllà del *remblai* respecte del *déblai*.

²³ Com remarca Étienne Ghys a [T9], Monge no es preocupa per l'existència de solucions del problema d'extremals que es proposa resoldre. Tampoc s'ocupa de si, donades dues regions diferents del pla de la mateixa àrea, hi ha una transformació que porta l'una sobre l'altra.

²⁴ Aquesta afirmació no és certa en general, el mateix Monge ho reconeix més endavant, quan diu «la solution précédente est illusoire».

²⁵ Monge utilitza la paraula *càustica*, paraula que ara es reserva a l'envolvent de rajos de llum.

Un cop coneix la direcció d'una molècula qualsevol (les tangents a l'envoltant), ja és fàcil trobar el preu del transport.

A la secció XIV tracta el cas en què les rutes de les molècules estan subjectes a passar per punts determinats, com per exemple ponts sobre rius o portes en els murs. Quants ponts hi hauria d'haver? Però si en el problema de minimitzar el transport hi entra el preu dels ponts, el tema es complica! Així acaba la primera part de l'article.

Dimensió 3

La segona part, dedicada al problema del transport en dimensió 3, comença donant els principis de geometria sobre els quals es fonamentaran les idees posteriors.

La primera observació és fonamental²⁶ i fa referència a famílies biparamètriques de rectes: *si per cada punt d'un pla hi passa una recta de l'espai determinada per una certa llei i prenem una d'aquestes rectes, llavors entre les rectes infinitament pròximes a aquesta només n'hi ha dues, genèricament, que la tallen.*²⁷

I posa l'exemple següent. Prenem una recta exterior al pla donat i per cada punt del pla hi tracem la perpendicular a aquesta recta.

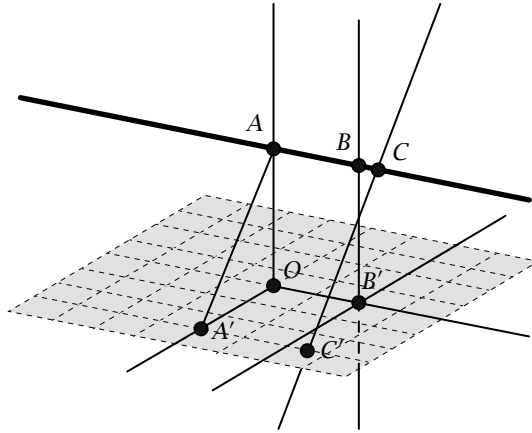


FIGURA 7: Les rectes AA' i BB' determinen, cadascuna d'elles, un pla amb OA ; en canvi, CC' no.

Només hi ha dues direccions que fan que rectes infinitament pròximes a una de donada es tallin (en particular estiguin en un pla): les determinades

²⁶ Lamentablement és falsa. O certa només sota determinades condicions. Étienne Ghys remarca a [T9] que la fibració de Hopf n'és un contraexemple. La família de rectes de R^3 que tallen el pla $z = z_0$ amb vector tangent en (x, y, z_0) donat per $(xz_0 + y, yz_0 - x, z_0^2 + 1)$ no té cap parella de rectes coplanàries, ni a nivell infinitesimal. No poden ser, per tant, les normals a una superfície. Vegeu la nota de la pàgina 132.

²⁷ En lloc de família biparamètrica de rectes també es parla de *congruència de rectes*.

pel pla format per la recta donada i la recta exterior (es tallen a l'infinit) i les determinades pel pla perpendicular a la recta.

A continuació en dona una demostració que pretén ser general però aquesta demostració falla, ja que suposa que una equació de segon grau té sempre arrels reals. És curiós que Monge no faci cap comentari sobre això, tret que la paraula «généralement» quan diu «cette équation du second degré ne donne généralement que deux valeurs» es pugui interpretar en sentit ampli.

I a la secció xx s'hi troba ja en germen el teorema de Monge:

Il suit de-là que dans le système de droites dont il s'agit on peut toujours passer de deux manières différentes d'une quelconque de ces droites à une autre infiniment proche, qui soit avec elle dans un même plane: cela posé, de l'une quelconque de ces droites, passons en effet à l'une de celles qui la coupe, ensuite et dans le même sens, à celle qui coupe la second, de-là à celle qui dans le même sens coupe la troisième; il est évident qu'en continuant ainsi de suite nous parcourrons une surface développable.

[D'això es dedueix que en el sistema de rectes en qüestió sempre es pot passar de dues maneres diferents d'una qualsevol d'aquestes rectes a una altra d'infinítament propera, que estigui amb ella en un mateix pla: dit això, d'una qualsevol d'aquestes rectes, passem efectivament a una d'aquestes que la tallen, a continuació i en el mateix sentit a la que talla la segona, d'aquí a la que en el mateix sentit talla la tercera; és evident que si continuem d'aquesta manera recorrerem una superfície desenvolupable.]

Quan generalitzem aquest resultat a la família biparamètrica de rectes formada per les normals a una superfície obtenim una part del teorema de Monge. Això és el que fa a la secció XXI: *les normals a una superfície són les interseccions de dues successions de superfícies desenvolupables tals que cada superfície de la primera successió talla totes les de la segona en línies rectes i en angles rectes i recíprocament*.

I ara, a la secció XXII, que reproduïxo íntegrament, és quan ens fa notar que aquí estan apareixent, encara que no ho sembli, les línies de curvatura! El resultat d'aquesta observació és el famós teorema de Monge: *les normals a una superfície sobre les línies de curvatura formen una superfície desenvolupable*.

Quoique cette proposition ne semble avoir qu'un rapport éloigné avec la belle théorie des rayons de courbure des surfaces courbes qu'a donnée M. Euler, dans les Mémoires de l'Académie de Berlin, année 1760;²⁸ cependant, si j'ose parler ainsi, elle complète le travail de cet illustre Géomètre sur cette matière: car les deux points où chaque normale est coupée par les deux normales voisines sont précisément les extrémités des deux rayons de plus grande et de moindre courbure, en sorte que les intersections de la surface courbe avec les surfaces développables qui composent la première suite sont, les lignes de moindre courbure de la surface et que les intersections avec les surfaces développables qui composent l'autre suite sont les lignes de plus grande courbure.

²⁸ Es refereix a [A4].

[Encara que aquesta proposició no sembla tenir gaire a veure amb la bella teoria dels radis de curvatura de les superfícies corbes que va donar el senyor Euler, a les Memòries de l'Acadèmia de Berlín, l'any 1760; no obstant això, si se'm permet dir-ho, completa l'obra d'aquest il·lustre geòmetra d'aquesta manera: com que els dos punts on cada normal és tallada per les dues normals pròximes són precisament els extrems dels dos radis de major i menor curvatura, de manera que les interseccions de la superfície corba amb les superfícies desenvolupables que componen la primera seqüència són les línies de menor curvatura de la superfície i que les interseccions amb les superfícies desenvolupables que componen l'altra successió són les línies de major curvatura.]

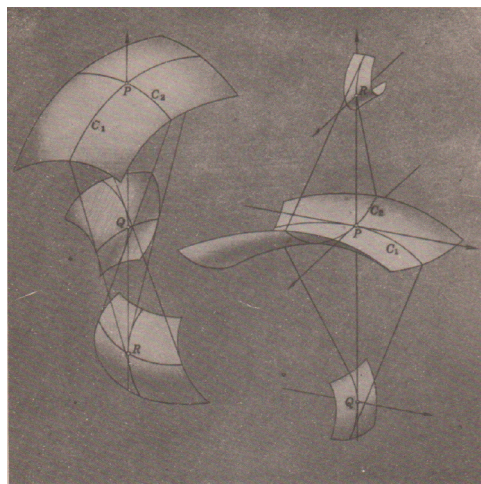


FIGURA 8: Dibuix de Struik [T15, p. 108].²⁹

A la secció xxv dona l'expressió dels radis de curvatura a partir de les consideracions que ha fet i veu que coincideix amb la donada per Euler. A la secció xxvi dona les equacions de les línies de curvatura. I això ja no ho va fer Euler. A la secció xxvii troba les evolutes de la superfície donada: llocs geomètrics dels centres de major i menor curvatura de la superfície. A la secció xxix estudia breument les *línies del contorn aparent* en relació amb aquestes superfícies.

A la secció xxxi dona l'element d'àrea en coordenades principals. En el seu llenguatge troba l'àrea del «quadrat» format per dues corbes «consecutives» de major curvatura amb dues corbes «consecutives» de menor curvatura. Troba també, a la secció següent, el volum del sòlid format per aquest quadrat i les normals a la superfície en els seus punts.

²⁹ La figura de l'esquerra representa una superfície en la que els dos radis de curvatura principal tenen el mateix signe; les evolutes estan en el mateix costat respecte de la superfície. La figura de la dreta representa una superfície en la que els dos radis de curvatura principal tenen signes oposats; les evolutes estan en costats oposats respecte de la superfície. En els dos casos, seguint la normal fins a ρ_1 o ρ_2 (radis de curvatura principal) trobem dues evolutes de la superfície. Les normals a la superfície són tangents a les evolutes.

Fins a la secció xxxiv no retorna al problema de *déblai* i *remblai*. Aplicant tots els resultats anteriors arriba a la conclusió que les rutes de les molècules, que seran com en el cas pla línies rectes, han de ser les interseccions de dues successions de superfícies desenvolupables tals que cada superfície de la primera successió talli totes les de la segona en angles rectes; i aquesta situació es correspon amb el que succeeix amb les normals a una superfície, com ha vist a la secció xxi, de manera que pot dir que *les trajectòries que han de seguir les molècules del primer volum per arribar a omplir el segon han de ser les normals a una mateixa superfície corba*.

I dona l'equació diferencial d'aquesta superfície. Com fa notar Étienne Ghys, és en aquestes equacions on apareix per primer cop la famosa equació de Monge-Ampère, una equació en derivades parcials de segon ordre que no és ni lineal ni quasi lineal però que és lineal en el hessià i les derivades segones. Si la superfície és $z = z(x, y)$ es compleix

$$F \cdot [\text{hessià}] + G \cdot \left(\left[1 + \left(\frac{dz}{dy} \right)^2 \right] \frac{d^2 z}{dx^2} - 2 \frac{dz}{dx} \frac{dz}{dy} \frac{d^2 z}{dx dy} + \left[1 + \left(\frac{dz}{dx} \right)^2 \right] \frac{d^2 z}{dy^2} \right) + H \cdot \left[1 + \left(\frac{dz}{dx} \right)^2 + \left(\frac{dz}{dy} \right)^2 \right] = 0$$

per a determinades funcions F, G, H .

I acaba reconeixent que la solució d'aquest problema està molt lluny de poder ser aplicada a la pràctica, ja que hi intervenen moltes més variables, les molècules no es poden transportar en línia recta, etc.³⁰

6 Fulls d'anàlisi, full xv

En aquesta secció estudiarem les línies de curvatura tal com ho va fer Monge al full xv de les seves *Feuilles d'analyse* [M11], titulat *Des deux courbures d'une surface courbe*. Però totes les idees estan a l'article sobre *déblai* i *remblai* [M2].

La idea de Monge és tan simple com intentar copiar per a superfícies la construcció de l'envolvent de les normals considerada per a corbes planes: l'evoluta d'una corba es pot considerar com la corba que s'obté en tallar normals a la corba donada en punts *infinítament pròxims*. Quan els clàssics parlen de punts infinitament pròxims, com ara en el cas de les normals que estem comentant, volen dir tallar la normal a la corba $\alpha(s)$ en el punt $\alpha(0)$ amb la normal a la corba en el punt $\alpha(\Delta s)$, i a continuació passar al límit quan Δs tendeix a zero.

³⁰ Dupin va tractar aquest tema del *déblai* i el *remblai* el 1813 a [A1] i el 1822 a [A2] (tota la tercera part de l'obra, unes seixanta pàgines, està dedicada a aquest tema; es titula *Sur le tracé des routes dans les déblais et les remblais*) tractant d'aclarir, ampliar i justificar punts dèbils de l'article de Monge. Considera casos en què el terreny no és pla i obté solucions ens les quals les trajectòries de les molècules no són rectes.

El problema és que si considerem dues normals a una superfície en punts infinitament pròxims pot passar que aquestes dues normals no es tallin, ja que dues rectes a l'espai normalment no es tallen.

També la idea d'infinítament pròxim s'ha de retocar en el sentit que ara tenim moltes maneres diferents d'acostar-nos a un punt donat. És el mateix problema que hi ha quan passem de l'estudi de derivades de funcions d'una variable a funcions de dues variables.

Tot això es resol de la manera següent. Suposem una superfície donada per la gràfica d'una funció $z = z(x, y)$ que passa per l'origen $O = (0, 0, 0)$ amb pla tangent $z = 0$. Prenem una corba $\gamma(x) = (x, y(x), z(x, y(x)))$ sobre la superfície que passi per O quan $x = 0$.

Voldríem tallar la recta normal a la superfície en el punt $\gamma(x)$ amb la recta normal a la superfície en el punt $O = \gamma(0)$, que és la recta $x = y = 0$. Aquestes rectes potser no es tallen i, per tant, el que farem serà tallar la normal a la superfície en $\gamma(x)$ amb els plans $x = 0$ i $y = 0$.

Obtenim com a punts de tall

$$\left(0, *, z + \frac{x}{p}\right), \quad \left(*, 0, z + \frac{y}{q}\right),$$

on p, q són les derivades primeres de z en el punt corresponent. Els asterics són quantitats que tendeixen a zero amb x i no ens calen.

Si volem que en el límit les rectes es tallin, les terceres components d'aquests punts han de coincidir (han de coincidir els punts, però amb les terceres components ja n'hi ha prou). Aplicant la regla de L'Hôpital i recordant que $p(0) = q(0) = 0$, tenim

$$\lim_{x \rightarrow 0} \frac{x}{p(x)} = \frac{1}{r + sy'}, \quad \lim_{x \rightarrow 0} \frac{y(x)}{q(x)} = \frac{y'}{s + ty'},$$

on r, s, t són les derivades segones de z en el punt $x = 0$. Per tant, ha de ser

$$\frac{1}{r + sy'} = \frac{y'}{s + ty'},$$

és a dir,

$$sy'^2 + (r - t)y' - s = 0.$$

Aquesta és l'equació de les direccions principals: *les direccions sobre les quals t'has d'aproximar a un punt per tal que les normals es tallin*.

Com que el producte de les arrels d'aquesta equació de segon grau és -1 , aquestes direccions són ortogonals. Observem que el discriminant d'aquesta equació és positiu.

Si repetim l'argument que hem usat per calcular les direccions principals a l'origen, però ara treballant sobre un punt arbitrari P , obtenim l'equació general de les línies de curvatura.

TEOREMA. *L'equació diferencial de les línies de curvatura d'una superfície donada com a gràfica de $z = z(x, y)$ és*

$$\begin{vmatrix} y'^2 & -y' & 1 \\ 1+p^2 & pq & 1+q^2 \\ r & s & t \end{vmatrix} = 0.$$

Observem que la segona i tercera files són els coeficients de la primera i segona formes fonamentals.

NOTA. Donem un contraexemple a l'afirmació de Monge de la pàgina 127, on afirma que, donada una recta d'una família biparamètrica de rectes, n'hi ha dues d'infinítament pròximes que la tallen. Per a això repetim els càlculs d'aquesta secció per a la família biparamètrica de rectes formada per aquelles rectes que tallen el pla $z = 1$ amb vector director $(x + y, y - x, 2)$, és a dir, les rectes

$$(x, y, 1) + \langle (x + y, y - x, 2) \rangle.$$

Aquesta família s'obté a partir de la fibració de Hopf, com indica É. Ghys a [T9].

Considerem una corba $(t, y(t), 1)$, definida per a valors petits de t , amb $y(0) = 0$. Les rectes de la família inicial que passen per aquesta corba tallen el pla $x = 0$ en un punt que té per tercera component

$$1 - \frac{2t}{t + y(t)},$$

i tallen el pla $y = 0$ en un punt que té per tercera component

$$1 - \frac{2y(t)}{y(t) - t}.$$

Si volem que en el límit la recta de la família talli l'eix z , que és també una recta de la família (i, per tant, que sigui coplanària amb ella com deia Monge), s'ha de complir

$$\lim_{t \rightarrow 0} \frac{t}{t + y(t)} = \lim_{t \rightarrow 0} \frac{y(t)}{y(t) - t}.$$

Obtenim, per L'Hôpital,

$$\frac{1}{1 + y'} = \frac{y'}{y' - 1},$$

equació que no té solució sobre els reals.

És a dir, tal com hem comentat a la nota 26 (pàgina 127), la família de rectes donada no té cap parella de rectes coplanàries, ni a nivell infinitesimal. No són les rectes normals a una superfície.

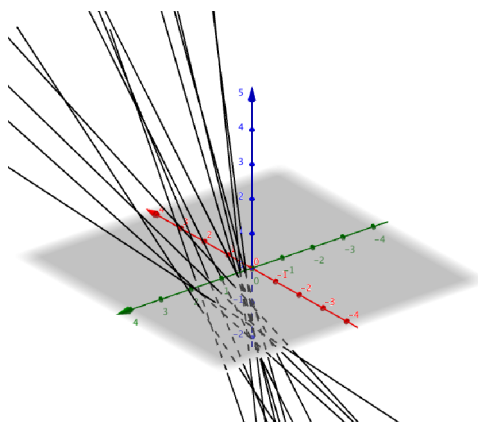


FIGURA 9: La foliació donada pels plans ortogonals a aquestes rectes no és integrable.

7 Altres treballs

Comentem breument alguns treballs més de Monge sobre geometria diferencial.

El 1783 publica «Sur une méthode d'intégrer les équations aux différences ordinaires» [M3], on es limita a donar a la primera pàgina un mètode per resoldre equacions diferencials i aplicar-lo a diverses situacions, com ara resoldre la típica equació de les superfícies minimals³¹

$$(1 + q^2)r - 2pqs + (1 + p^2)t = 0,$$

que atribueix a M. le Chevalier de Borda, a trobar línies de curvatura, etc.

Del 1784 és «Sur le calcul intégral des équations aux différences partielles» [M5]. Es tracta d'un treball molt extens on torna a integrar l'equació diferencial de les superfícies minimals, recordant novament M. le Chevalier de Borda. El mètode d'integració de Monge és millorat més tard per Legendre a «Mémoire sur l'intégration de quelques équations aux différences partielles» [A10], on també corregeix alguns errors comesos per Monge.

El mateix any 1784 estudia la generació de superfícies i publica essencialment la mateixa memòria «Sur l'expression analytique de la génération des surfaces courbes» a Torí [M6] i a París [M4].

A la memòria de Torí resol tres problemes que consisteixen a expressar que una superfície corba està generada per: 1) Un cercle que es mou de manera que el seu pla sigui sempre perpendicular a la corba recorreguda pels centres. 2) Un cercle que es mou d'una manera qualsevol. 3) Una corba qualsevol constant de forma que es mou d'una manera qualsevol a l'espai.

A la de París, més detallada i extensa, resol exactament aquests tres mateixos problemes més el següent: *expressar que una superfície corba està generada per una corba plana que es mou de manera que el pla que la conté es manté*

³¹ Superfícies d'àrea mínima amb vora donada. Estan caracteritzades pel fet de tenir curvatura mitjana zero.

perpendicular a les corbes recorregudes per tots els seus punts. De seguida diu que aquestes superfícies es poden definir com les superfícies generades per una corba plana quan el seu pla gira sense lliscar sobre una superfície desenvolupable. Aquestes superfícies reben avui el nom de *superfícies de Monge* i estan caracteritzades perquè les línies de curvatura (les màximes o mínimes) són geodèsiques.³² Monge demostra que sobre una línia de curvatura l'altra curvatura és constant.

El 1795 publica «Sur les lignes de courbure de la surface de l'Ellipsoïde» [M9], utilitzant les equacions generals de les línies de curvatura, que havia estudiat a «Mémoire sur la théorie des déblais et des remblais» [M2]. Obté

$$Axyy'^2 + y'(x^2 - Ay^2 - B) - xy = 0,$$

amb

$$A = \frac{a^2(b^2 - c^2)}{b^2(a^2 - c^2)}, \quad B = \frac{a^2(a^2 - b^2)}{a^2 - c^2},$$

on a, b, c són els semieixos de l'el·lipsoide. I de seguida integra l'equació i veu que es tracta d'una secció cònica del tipus $y^2 = \beta x^2 + \gamma$, per certes constants β, γ que s'han d'ajustar. Per tant, es tracta d'una cònica concèntrica amb l'el·lipsoide que serà una el·lipse o una hipèrbola segons el signe de β . Observem que aquesta cònica és la projecció sobre el pla $z = 0$ de les línies de curvatura.

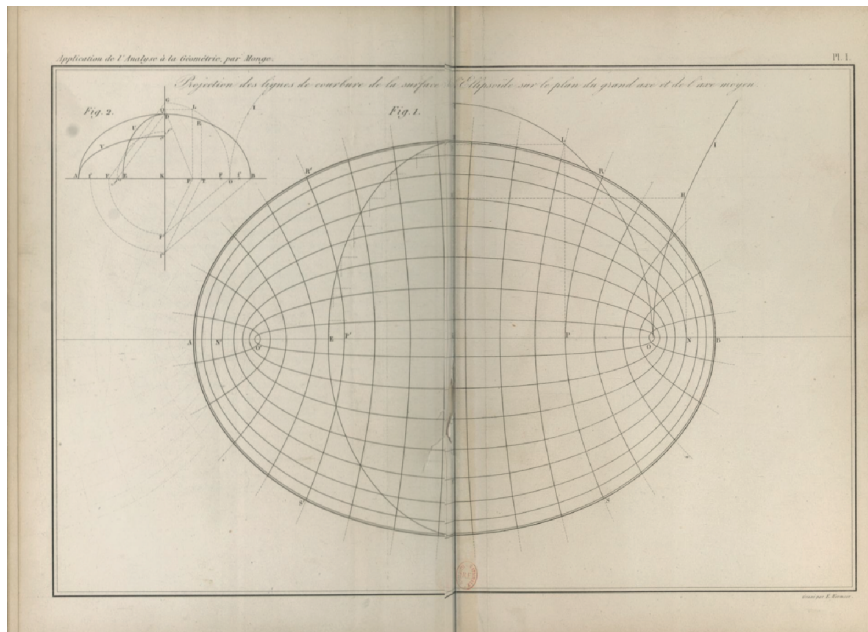


FIGURA 10: Línies de curvatura de l'el·lipsoide [M18].

³² Recordem que les línies de curvatura tenen torsió geodèsica zero i que sobre les geodèsiques la torsió i la torsió geodèsica coincideixen. Per tant, una geodèsica i línia de curvatura és plana. A partir d'aquí es pot recuperar el resultat de Monge amb relativa facilitat.

Posteriorment reproduceix aquests treballs a la secció XVI d'*Application de l'analyse à la géométrie* [M18].

La idea és intentar fer un arc de pedra, com ara una porta, però de manera que la corba suport no sigui un arc de circumferència sinó un arc, per exemple, d'el·lipse. El picapedrer ha de tallar les pedres que van a sobre d'aquest arc de manera que s'acoblin bé entre elles, i els picapedrers piquen en línies rectes, de manera que ja es veu que la pedra ha d'estar tallada com una superfície reglada, però el que no és tan evident és que hagi de ser també desenvolupable.

Monge ho diu així:

S'il étoit question de voûter un space circonscrit en projection horizontale par une ellipse, on ne pourroit pas donner à la voûte une surface plus convenable que celle de la moitié d'une ellipsoïde [...] et en supposant que cette voûte dût être exécuté en pierres de taille, il faudroit que la division en voussoirs fût opérée au moyen des lignes de courbure [...] et que les joints fussent les surfaces développables normales à la voûte.

[Si es tractés de fer una volta sobre un espai circumscriu en projecció horitzontal per una el·lipse, no es podria donar a la volta una superfície més adequada que la de la meitat d'un el·lipsoide [...] i suposant que aquesta volta s'executés en pedres tallades, seria necessari que la divisió en dovelles es fes per mitjà de les línies de curvatura [...] i que les juntes fossin les superfícies desenvolupables normals a la volta.]

Comenta que en aquell moment s'estan construint les sales per als consells de la legislatura i que la millor forma que se'ls pot donar és l'el·líptica i que estigui coberta per un el·lipsoide. Llavors es posaria la tribuna d'oradors just sota un dels punts umbilicals de la volta. I es podria decorar l'espai posant columnes seguint les línies de curvatura. I s'imagina també dos llums d'aranya penjant dels umbilicals!

A l'article de J. Sakarovitch «Gaspard Monge founder of "Constructive Geometry"» [T13], es reproduceix la figura següent (figura 11), que atribueix a Leroy, 1844.³³ Es veu la volta el·lipsoïdal amb les pedres superiors o dovelles acoblades entre elles perpendicularment a la superfície que les aguanta.

El 1801 es publiquen les *Feuilles d'analyse appliquée à la géométrie à l'usage de l'École polytechnique* [M11], però les primeres notes amb aquest nom per als estudiants de l'École polytechnique són del 1795. Els alumnes anomenaven aquest llibre «Le gros Monge».

En una nota del 1799, «Des courbes à double courbure» [M19], es complementen qüestions sobre les corbes de doble curvatura que falten a les *Feuilles*. Aquest article acaba amb una nota a peu de pàgina d'Hachette,³⁴ que diu:

³³ El llibre IV del *Traité de stéréotomie* de Leroy (1780-1854) [A11] es diu «Coupe des Pierres», i té una secció que es titula «Voûte en ellipsoïde à trois axes inégaux. Emploi des lignes de courbure». El dibuix que reproduceix Sakarovitch és la planxa 44 de [A11].

³⁴ Jean Nicolas Pierre Hachette va ser un dels més importants impulsors del *Journal de l'École polytechnique*. Va col·laborar estretament amb Monge sobretot en l'estudi i les aplicacions de la geometria descriptiva. Va estudiar els radis de curvatura de les superfícies a «De quelques propriétés des rayons de courbure d'une surface» [A7].

dear colleague, what you have just exposed was very elegant; I wish I had done it". Monge admitted having never received a compliment that touched him so deeply". Ellipsoid vaults therefore provide an excellent example of application of his theory. All the more so since in this particular case, the criticisms mentioned earlier do not apply and the "lines of greatest contraction" and the lines of smallest surface curvature coincide. Twice in his writings, Monge comes back to the question of ellipsoid vault stone assembly. No doubt in reference to the project for the National Assembly Hall, which was being discussed at the time, he even describes an ideal amphitheatre that might respect the surface geometry (Monge 1795b, Folio n° 20) and (Monge 1796, pp. 162-163). One really feels in this text, fully quoted by Hachette (Hachette 1822, p. 293) and later Leroy (Leroy 1844, pp. 366-367) in their courses on stereotomy, the way Monge's theory of the vault assembly revive mortarless architecture (cf. Sakarovich 1998, p. 311). One must however observe that this did not happen. We have not been able to find any examples or any mortarless architectural works involving new surfaces or vaults involving intradoses with complex surfaces assembled according to the lines of curvature.

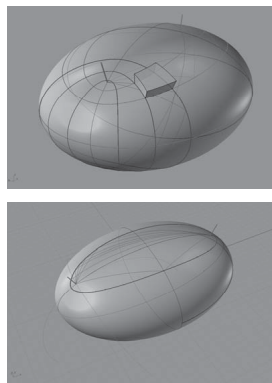


Figure 4: The lines of curvature as generalized ellipses

"The families of the lines of curvature can be regarded as generalized ellipses: choosing a pair of umbilical points not diametrically opposite, we attach the ends of a thread of sufficient length to them and pull it toward a point P of the ellipsoid. The various positions that P can assume on the ellipsoid trace out a line of curvature"; (Hilbert 1952, p. 188).

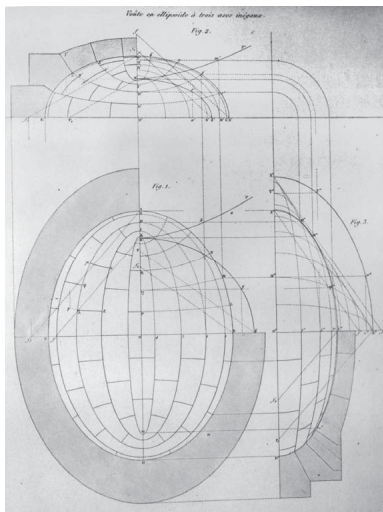


Figure 5 : ellipsoid vault using lines of curvature (in Leroy 1844)

FIGURA 11: Dovelles sobre el·lipsoide.

Cet écrit pourra suppléer à ce qui manque sur les Courbes à double courbure dans les feuilles d'analyse appliquée à la géométrie, que le C.^{en} Monge a fait imprimer pour les élèves de l'École polytechnique.

[Aquest escrit podrà suplir el que manca sobre les corbes de doble curvatura a les *Feuilles d'analyse appliquée à la géométrie*, que el ciutadà Monge ha fet imprimir per als alumnes de l'École polytechnique.]

Edicions posteriors de les *Feuilles*, fetes a partir del 1807, portaven per títol *Application de l'analyse a la géométrie*. Liouville va tenir cura de la cinquena edició, de 675 pàgines, que va corregir i comentar, vegeu [M18]. A la secció 6 hem estudiat el full xv.

Aquesta edició de Liouville està composta de vint-i-set seccions, dedicades totes al que podríem anomenar de manera genèrica *generació de superfícies*. Per exemple: «x. De la superfície engendrada pel moviment d'una línia recta paral·lela a un pla fixat», «xii. Superfícies desenvolupables», «xvii. De la generació de la superfície corba en la qual totes les línies d'una de les curvatures estan en plans paral·lels a un pla donat», «xx. De la superfície corba en la qual els dos radis de curvatura són sempre iguals i de signes contraris», «xxii. De la superfície corba que envolta una successió d'esferes de radi variable i centres sobre una corba qualsevol», «xxiii. Article [M12]», «xxiv. Article [M13]», «xxv. Article [M14]», «xxvi. Article [M15]», «xxvii. Article [M7]».

A continuació Liouville reproduïx la memòria immortal de C. F. Gauss traduïda al francès amb el títol «Recherches sur la théorie général des surfaces courbes» [A5]. I acaba amb unes famoses set notes: «I. Sobre les corbes de doble curvatura», «II. Expressions diverses de la distància de dos punts infinitament

pròxims i de la curvatura geodèsica de les línies sobre una superfície», «III. Teorema sobre la integració de les línies geodèsiques», «IV. Sobre el teorema de Gauss sobre el producte dels dos radis de curvatura principals en cada punt d'una superfície», «V. Del traçat geogràfic de superfícies, les unes sobre les altres», «VI. Extensió al cas de tres dimensions de la qüestió del traçat geogràfic», «VII. Sobre l'equació de les cordes vibrants».

El 1802 Monge publica «Mémoire sur la surface courbe dont toutes les normales sont tangentes à la surface d'une même sphère» [M12], on introdueix el nom de corba *caractéristica* dient:

C'est à cette courbe, dont toutes les surfaces soumises à la même génération sont pour ainsi dire composées,³⁵ qu'on aurait dû consacrer le nom de *génératrice*; mais ce mot est déjà employé dans un sens qui n'est pas toujours le même que celui-ci: j'ai donc cru nécessaire de me servir d'un mot nouveau, et j'ai nommé cette courbe *caractéristique*.

[És a aquesta corba, de la qual totes les superfícies sotmeses a la mateixa generació estan per així dir compostes, que se li hauria d'haver assignat el nom de *generatriu*; però aquest nom ja s'utilitza en un sentit que no és el mateix que aquest d'aquí: he cregut, doncs, necessari servir-me d'una nova paraula, i he anomenat aquesta corba *caractéristica*.]

Veu, entre altres coses, que una superfície que satisfà les hipòtesis del títol és tal que l'esfera és el lloc geomètric dels centres d'una de les seves curvatures. Amplia aquest tipus de resultats canviant l'esfera per una superfície cònica arbitrària a «Sur la surface courbe dont toutes les normales sont tangentes à une même surface conique à base arbitraire» [M13], publicat just a continuació de l'anterior.

El 1805, apareix el llibre de Monge i Hachette, *Application de l'algèbre a la géométrie* [M21], que recull diversos treballs de Monge. De fet, ja el 1802 havien publicat un article amb el mateix nom al *Journal de l'École polytechnique* [M20], base del llibre posterior. Abans de començar diu (observeu les dates segons el nou calendari imposat per la Revolució Francesa):

AVERTISSEMENT

Lés Éléves de l'École polytechnique ont trouvé jusqu'à présent le précis des leçons sur l'application de l'Algèbre à la Géométrie, dans les Feuilles d'analyse de *Monge*, et le Mémoire sur les surfaces du second degré, imprimé en l'an 10 dans le Journal de l'École. Tous les exemplaires de ce Mémoire, tirés à part lors de la publication du Journal, ayant été distribués, MM. MONGE et HACHETTE ont proposé de le remplacer par un ouvrage ayant pour titre: «Surfaces du premier et second degré», le Conseil d'instruction, dans sa séance du 19 pluviôse an 13, a arrêté que cet Ouvrage seroit imprimé pour l'École.

[Els alumnes de l'École polytechnique han trobat fins ara els apunts de les lliçons sobre l'aplicació de l'àlgebra a la geometria, a les *Feuilles d'analyse de Monge*, i a la Memòria sobre les superfícies de segon grau, impresa l'any 10

³⁵ Abans ha posat, com a exemple d'aquesta corba, els meridians de les superfícies de revolució.

a la revista de l'Escola. Havent estat distribuïts tots els exemplars d'aquesta Memòria, impresos per separat quan es va publicar el *Journal*, els senyors MONGE i HACHETTE han proposat reemplaçar-la per una obra que té per títol: «Surfaces du premier et second degré», el Conseil d'Instruction, en la seva sessió del 19 pluviós any 13, ha donat permís perquè aquesta obra sigui impresa per l'Escola.]

El llibre està compost de les vuit seccions següents: «I. Equacions d'un punt», «II. Equacions de la línia recta», «III. Equacions del pla», «IV. Problemes relatius a rectes i plans», «V. Canvis de coordenades», «VI. Del centre i dels plans diametral d'una superfície», «VII. Superfícies de segon grau», «VIII. Superfícies de segon grau quan les coordenades del centre són a l'infinit».

El 1806 publica dos articles llargs consecutius al *Journal de l'École polytechnique*. Els títols són explícits del seu contingut, el primer es titula «Sur la surface courbe dont toutes les normales sont tangentes à une même surface développable quelconque» [M14], i toca el mateix tema que en els anteriors [M12] i [M13], i el segon «De la surface courbe qui enveloppe l'espace parcouru par une sphère variable de rayon, et dont le centre parcourt une courbe à double courbure quelconque» [M15]. Estudia, doncs, tubs.

El 1807 envia a l'École polytechnique una breu solució del problema de trobar una superfície desenvolupable que tingui com a aresta de retrocés una corba donada, que Hachette recull a *Correspondance sur l'École impériale polytechnique* [M16]. També d'aquest any és la nota conjunta amb Hachette «Sur la théorie des ombres et de la perspective; sur les points brillants des surfaces courbes» [M22]. Defineixen *punt brillant* com el punt de la superfície que reflecteix un raig lluminós cap a l'ull de l'espectador. No hi ha cap fórmula, només consideracions geomètriques.

El 1810 envia una nota a l'École titulada «Sur les équations différentielles des courbes du second degré» [M17]. Diu que plantejar-se aquest problema per a corbes de grau arbitrari li sembla «une entreprise inutile». Però que, per la seva importància, val la pena fer-ho per a les corbes de segon grau. Com que les seves equacions són

$$Ay^2 + 2Bxy + Cx^2 + 2Dy + 2Ex + 1 = 0,$$

posant

$$\frac{dy}{dx} = p, \quad \frac{dp}{dx} = q, \quad \frac{dq}{dx} = r, \quad \frac{dr}{dx} = s, \quad \frac{ds}{dx} = t,$$

s'obté

$$9q^2t - 45qrs + 40r^3 = 0$$

com a equació diferencial de totes les corbes de segon grau.

El 1811 es publica la seva famosa *Géométrie descriptive* [M10], on hi ha un capítol titulat «Des plans tangents et des normales aux surfaces courbes», en el qual es parla de canons, de l'enemic, etc. És molt curiós l'esperit patriòtic que destil·la la introducció.

Pour tirer la nation française de la dépendance où elle a été jusqu'à présent de l'industrie étrangère, il faut premièrement diriger l'éducation nationale vers la connaissance des objets qui exigent de l'exactitud [...] et, à cet égard, il aut l'avouer, nous avons beaucoup à puiser chez les nations étrangères.

C'est d'abord en familiarisant avec l'usage de la Géométrie descriptive tous les jeunes gens qui ont de l'intelligence, tant ceux qui ont une fortune acquise, afin qu'un jour ils soient en état de faire de leurs capitaux un emploi plus utile et pour eux et pour l'État, que ceux mêmes qui n'ont d'autre fortune que leur éducation, afin qu'ils puissent un jour grand prix à leur travail.

[Per treure la nació francesa de la dependència que ha tingut fins ara de la indústria estrangera, cal dirigir primer l'educació nacional cap al coneixement d'objectes que requereixen exactitud [...] i, en aquest sentit, ho hem de confessar, tenim molt a aprofitar de les nacions estrangeres.

En primer lloc familiaritzant tots els joves amb intel·ligència en l'ús de la geometria descriptiva, tant els que tenen fortuna adquirida, perquè un dia estiguin en condicions de fer dels seus capitals un ús més útil per a ells i per a l'Estat, com aquells que no tenen més fortuna que la seva educació, de manera que un dia puguin donar més valor al seu treball.]

Espero que aquest treball apropi els futurs alumnes de geometria diferencial de les nostres universitats a la figura de Monge i al context en què es va iniciar l'estudi de corbes i superfícies.

8 François Arago per Josep Lluís Solé

Per conèixer la vida de F. Arago³⁶ (1786-1853) us recomanem amb entusiasme l'autobiografia titulada *Història de la meva joventut* (col·lecció Popular Barcino, núm. 155), publicada per Editorial Barcino (1937), reimprès per Artífex Cultural, Palma (2000), que redactà quan, com diu ell mateix, ja era vell i estava malalt. Es llegeix com una magnífica novel·la d'aventures.

En el llibre ens parla de la seva infantesa al poble d'Estagell, al Rosselló, i la seva adolescència a Perpinyà. També de la preparació de l'examen d'ingrés a l'École polytechnique, estudiant en solitari obres de Legendre, Lacroix i Garnier... examen que feu a Tolosa, davant d'un tribunal presidit per Monge, que primer el rebé amb desconfiança. L'examen durà dues hores i acabà amb l'abraçada de Monge, impressionat pels coneixements del jove Arago.

Ens hi explica l'ambient de l'École polytechnique, lligada als moments polítics difícils de la França de la primera dècada del segle XIX. Allí conegué i feu amistat amb Laplace. Junt amb altres estudiants es negà a signar el document d'adhesió a la proclamació de Napoleó com a emperador, i per això el general Lacuée, director de l'École, proposà la seva expulsió. Napoleó demanà a Lacuée

³⁶ En aquesta secció s'ha respectat la grafia del cognom amb accent emprada per Josep Lluís Solé.

quin lloc de la promoció ocupava Aragó, i en veure a la llista que era el primer digué: «Ah, si haguessin estat a la cua!... Senyor Lacuée, deixeu-ho córrer...».

El 1804 fou nomenat secretari de l'Observatori de París recomanat per Poisson, professor del jove Aragó a la polytechnique. Demanà a Laplace, director de l'Observatori, reprendre les mesures del meridià de París a Espanya, interrompudes per la mort de Méchain.

Encara que trossos d'aquest meridià havien estat objecte de distintes campanyes de mesura anteriors (Picard, Cassini I, Cassini II, La Hire, Maraldi...), quan l'Assemblea Nacional decidí (1791) establir un patró de mesura que pogués ser acceptat per totes les nacions, l'Acadèmia proposà tornar a mesurar el meridià de París, però aquesta vegada no només en territori de França, sinó arribar fins a Barcelona (el meridià de París entra al Mediterrani a la platja d'Ocata, al Maresme). Delambre fou l'encarregat de mesurar la part nord, de Dunquerque a Rodés, i Méchain, la part sud, de Rodés a Barcelona. Les mesures començaren el dia abans de la presa de la Bastilla, i la història d'aquesta campanya científica, feta en moments convulsos, mereix una explicació a part.

El 1801, Méchain, director de l'Observatori de París, demanà prolongar les mesures del meridià de Barcelona a les Balears (el meridià de París talla sa Dragonera, i deixa l'illa de Mallorca totalment a llevant seu). Per fer-ho, proposà triangular la costa de Castelló i València per poder fer el salt a Eivissa i Formentera, i d'allí a la serra de Tramuntana de Mallorca. El 1803 Méchain començà els treballs, però morí el setembre del 1804 sense poder acabar el seu encàrrec.

F. Aragó i J.-B. Biot foren, doncs, comissionats per acabar les mesures de Méchain, i són les anècdotes d'aquesta expedició, iniciada a principis del 1806, les que ocupen la gran part del llibret que hem esmentat al principi. Ens hi explica la seva estada al cim del desert de València durant sis mesos intentant visualitzar el turó des Camp Vell, a Eivissa, a 150 km de distància. Les trobades i amistat amb els bandolers de prop de Cullera, al sud de València; la persecució d'un amant gelós a Sagunt; l'estada a la Mola de Formentera, en una casa que encara avui existeix, i la construcció d'una cabana de pedra al cim de la Mola de s'Esclop, sobre Andratx, últim vèrtex del darrer triangle, hi són descrits amb molta amenitat.

A la Mola de s'Esclop el sorprengué l'aixecament contra Napoleó (1808). Avisat que, com que el poble creia que era un espia, el pujaven a matar, fugí vestit de pastor i es refugià a Palma. Allí fou tancat al castell de Bellver, d'on escapà, i pujà a un vaixell que el portà a Alger. Embarcà cap a França, però un corsari de Roses capturà el vaixell, i Aragó, sense donar-se a conèixer i fent-se passar per català, fou tancat a la ciutadella de Roses i a Palamós. Alliberat, un vaixell l'havia de portar a Marsella, però una tempesta desvià el vaixell a Bugia, a les costes algerianes, on, després d'un viatge arriscat, pogué arribar al consolat francès d'Alger. Allí s'embarcà en un vaixell de bandera algeriana, i arribà finalment a Marsella el juny del 1809, evitant el bloqueig de la flota anglesa. Tot això amb la llibreta d'observacions amagada a la seva roba!

Un any després (1809) fou elegit membre de l'Acadèmia, per a una vacant a la qual també aspirava D. Poisson, que hagué d'esperar tres anys a poder-hi accedir. En el darrer capítol de *Memòries de la meua joventut* ens explica la seva activitat com a acadèmic, fins al seu nomenament com a secretari perpetu el 1830, i la seva renúncia la plaça de professor de l'École polytechnique a favor de Fourier.

No descriurem en aquestes notes de caràcter biogràfic l'obra científica d'Aragó, però sí que volem assenyalar que no abandonà el seu compromís polític. Fou membre del govern provisional de la Segona República, sorgida després de la Revolució del 1848, el qual establí el sufragi universal i l'abolició de l'esclavitud a França. Com a ministre de la guerra i de marina va suprimir els càstigs corporals a l'armada i millorà el tracte als mariners (vegeu el capítol 6 del llibre de P. Murdin *Full Meridian of Glory*, Nova York, Springer Bussiness Media, 2000).

Quan Napoleó III restablí l'imperi el 1851, Aragó es retirà de la vida política, però li permeteren continuar sent director de l'Observatori fins que es retirà a Estagell el 1853.

Agraïments

Agraeixo a Josep Lluís Solé Clivillés que ens hagi cedit el text sobre François Arago, així com la redacció del peu de pàgina 8. I a David Marín que em va ajudar en els càlculs sobre la fibració de Hopf.

Treballs de Monge

- [M1] MONGE, G. «Mémoire sur les propriétés de plusieurs genres de surfaces courbes, particulièrement sur celles des surfaces développables, avec une application à la théorie des ombres et des pénombres». *Mémoires de Mathématique et de Physique [Mémoires des Savants Étrangers]*, 9 (1780), 382-440.
- [M2] MONGE, G. «Mémoire sur la théorie des déblais et des remblais». *Histoire de l'Académie royale des sciences* [París] (1781), 666-704.
- [M3] MONGE, G. «Sur une méthode d'intégrer les équations aux différences ordinaires, lorsqu'elles sont élevées, et dans les cas où leurs intégrales complètes sont algébriques». *Mémoires de l'Académie des sciences de Paris* (1783), 719-724.
- [M4] MONGE, G. «Mémoire sur l'expression analytique de la génération des surfaces courbes». *Histoire de l'Académie royale des sciences. Mémoires de Mathématique et de Physique* [París] (1784), 85-117.
- [M5] MONGE, G. «Sur le calcul intégral des équations aux différences partielles». *Mémoires de Mathématique et de Physique [Mémoires des Savants Étrangers]* (1784), 118-192.

- [M6] MONGE, G. «Sur l'expression analytique de la génération des surfaces courbes». *Mémoires de l'Académie royale des sciences de Turin* (1784), 19-33.
- [M7] MONGE, G. «Mémoire sur les développées, les rayons de courbure, et les differens genres d'inflexions des courbes à double courbure». *Mémoires présentés par divers savants à l'Académie des sciences de l'Institut de France*, x (1785), 511-550. [Vegeu també [M18, 392-420]]
- [M8] MONGE, G. «Stéréotomie». *Journal polytechnique ou Bulletin du travail*, 1er cahier (1794), 1-15.
- [M9] MONGE, G. «Sur les lignes de courbure de la surface de l'ellipsoïde». *Journal de l'École polytechnique ou Bulletin du travail*, 2e cahier (1795), 145-165. [Reproduït a la secció XVI, p. 139, de [M18]]
- [M10] MONGE, G. *Géométrie descriptive. Leçons données aux écoles normales, l'an 3 de la République*. París: Baudouin, 1799. [N'hi ha moltes edicions, per exemple una de Klostermann de 1811 i una de Jacques Gabay de 1989]
- [M11] MONGE, G. *Feuilles d'analyse appliquée à la géométrie à l'usage de l'École polytechnique*. París: Baudouin, 1801. [Éditions Jacques Gabay en fa una reimpressió el 2008]
- [M12] MONGE, G. «Mémoire sur la surface courbe dont toutes les normales sont tangentes à la surface d'une même sphère». *Journal de l'École polytechnique*, 11e cahier, IV (1802), 28-58.
- [M13] MONGE, G. «Sur la surface courbe dont toutes les normales sont tangentes à une même surface conique à base arbitraire». *Journal de l'École polytechnique*, 11e cahier, IV (1802), 59-86.
- [M14] MONGE, G. «Sur la surface courbe dont toutes les normales sont tangentes à une même surface développable quelconque». *Journal de l'École polytechnique*, 13e cahier, VI (1806), 1-40.
- [M15] MONGE, G. «De la surface courbe qui enveloppe l'espace parcouru par une sphère variable de rayon, et dont le centre parcourt une courbe à double courbure quelconque». *Journal de l'École polytechnique*, 13e cahier, VI (1806), 41-59.
- [M16] MONGE, G. «Trouver l'équation de la surface développable, qui a pour arête de rebroussement une courbe à double courbure, dont on connaît l'équation unique aux différences ordinaires?». A: HACHETTE, J. N. P. (ed.). *Correspondance sur l'École impériale polytechnique* (Avril 1804-Mars 1808). Vol. I. París: Klostermann, 1807, 209-211.
- [M17] MONGE, G. «Sur les équations différentielles des courbes du second degré». A: HACHETTE, J. N. P. (ed.). *Correspondance sur l'École impériale polytechnique* (Janvier 1809-Mars 1813). Vol. II. París: Klostermann, 1810, 51-54.
- [M18] MONGE, G. *Application de l'analyse à la géométrie*. 5a ed., revisada, corregida i anotada per J. Liouville. París: Bachelier, 1850. [1a ed., 1807]

- [M19] MONGE, G.; HACHETTE, J. N. P., «Des courbes à double courbure. (Extrait des Ouvrages du C.^{en} Gaspard Monge.)» *Journal de l'École polytechnique* ou *Bulletin du travail*, 6e cahier, II (1799), 345-363.
- [M20] MONGE, G.; HACHETTE, J. N. P. «Application d'algèbre à la géométrie». *Journal de l'École polytechnique*, 11e cahier, IV (1802), 143-170.
- [M21] MONGE, G.; HACHETTE, J. N. P. *Application de l'algèbre à la géométrie. Des surfaces du premier et second degré, à l'usage de l'École polytechnique*. Paris: Bernard, 1805.
- [M22] MONGE, G.; HACHETTE, J. N. P. «Sur la théorie des ombres et de la perspective; sur les points brillants des surfaces courbes». A: HACHETTE, J. N. P. (ed.). *Correspondance sur l'École impériale polytechnique* (Avril 1804-Mars 1808). Vol. I. Paris: Klostermann, 1807, 295-305.

Treballs sobre Monge

- [T1] ARAGO, F. «Biographie de Gaspard Monge». *Mémoires de l'Académie des sciences de l'Institut de France*, XXIV (1854), I-CLVII. [Llegit a la sessió pública de l'11 de maig de 1846]
- [T2] BELHOSTE, B. «Gaspard Monge: Urgences révolutionnaires et utopie». *Cahiers du Mouvement universel de la responsabilité scientifique (MURS)*, 17 (1989), 55-75.
- [T3] BRISSON, B. *Notice historique sur Gaspard Monge*. Paris: Plancher, Éditeur du Manuel des Braves, 1818.
- [T4] CHAPELON, J. «Monge, géomètre et Jacobin». *La Pensée, Nouvelle Série*, 13 (1947).
- [T5] DE LAUNAY, L. *Un grand français. Monge fondateur de l'École polytechnique*. Paris: Éditions Pierre Roger, 1933.
- [T6] DE PONGERVILLE, J.-B. S. *Gaspard Monge et l'expédition d'Égypte*. Paris: Challamel Ainé, éditeur, 1860.
- [T7] DUPIN, CH. *Essai historique sur les services et les travaux scientifiques de Gaspard Monge*. Paris: Bachelier, 1819.
- [T8] ETAYO, J. J. «Las bases de la Geometría Diferencial». *Historia de la Matemática en el siglo XIX (2ª parte)*. Curs de conferències durant els mesos de febrer a abril del 1993. Real Academia de Ciencias Exactas, Físicas y Naturales, 1993, 171-190.
- [T9] GHYS, É. «Gaspard Monge. Le mémoire sur les déblais et les remblais». A: *Images des Mathématiques* (2012), 1-24. [Article adjunt a l'obra «Gaspard Monge, le beau, l'utile et le vrai», disponible a <http://images.math.cnrs.fr/Gaspard-Monge>]
- [T10] GUYON, N. *Éloge funèbre de M. Monge, compte de Peluze*. Paris: Plancher, Éditeur du Manuel des Braves, 1818.

- [T11] LANGEVIN, R. «Gaspard Monge, de la planche à dessin aux lignes de courbure». A: *De la méthode*. Besançon: Press. Univ. Franc-Comtoises, 2002, 127-154. (Colloq. Sémin.)
- [T12] RAVAILHE, F. *Éloge de Gaspard Monge*. Beaune: Imprimerie de Blondeau-Dejussieu, 1849.
- [T13] SAKAROVITCH, J. «Gaspard Monge founder of “Constructive Geometry”». A: *Proceedings of the Third International Congress on Construction History*. Cottbus: Brandenburg University of Technology, 2009, 1293-1300.
- [T14] SERGESCU, P. «Le bicentenaire de Gaspard Monge». *Rev. Histoire Sci. Appl.*, 1 (2) (1947), 162-170.
- [T15] STRUIK, D. J. *Geometría Diferencial Clásica*. Madrid: Aguilar, 1970. [Traducció de *Lectures on Classical Differential Geometry*. Cambridge, Mass.: Addison-Wesley Press, Inc., 1950]
- [T16] TATON, R. *L'œuvre scientifique de Monge*. París: Presses Universitaires de France, 1951.
- [T17] TATON, R. «La première note mathématique de Gaspard Monge (juin 1769)». *Rev. Histoire Sci. Appl.*, 19 (2) (1966), 143-149.

Altres

- [A1] DUPIN, CH. *Développements de géométrie, Avec des Applications à la stabilité des Vaisseaux, aux Déblais et Remblais, au Défilement, à l'Optique, etc.; ouvrage approuvé par l'Institut de France, pour faire suite a la Géométrie Descriptive et a la Géométrie Analytique de M. Monge*. París: M. V. Courcier, Imprimeur-Libraire pour les Mathématiques, 1813.
- [A2] DUPIN, CH. *Applications de géométrie et de mécanique a la marine, aux ponts et chaussées, etc., pour faire suite aux «Développements de géométrie»*. París: Bachelier, successeur de M. V. Courcier, 1822.
- [A3] EISENMAN. «Stérotomie». *Journal polytechnique ou Bulletin du travail*, 2e cahier (1795), 100-106; 3e cahier (1795), 440-442; 4e cahier (1796), 619-622.
- [A4] EULER, L. «Recherches sur la courbure des surfaces». *Mémoires de l'Académie des sciences de Berlin*, 16 (1767), 119-143. [Publicat també a *Opera Omnia*, Serie 1, 28 (1955), 1-22]
- [A5] GAUSS, C. F. «Disquisitiones generales circa superficies curvas». *Commentationes Societatis Regiae Scientiarum Gottingensis Recentiores Classis Mathematicae*, VI (1828), 99-146. [Presentat el 8 d'octubre del 1827]
- [A6] GIRBAU, J. *Memoria sobre el concepto, método y fuentes de la geometría diferencial*. Barcelona: 1973. [Apunts]
- [A7] HACHETTE, J. N. P. «De quelques propriétés des rayons de courbure d'une surface». A: HACHETTE, J. N. P. (ed.). *Correspondance sur l'École impériale*

- polytechnique* (Avril 1804–Mars 1808). Vol. I. Paris: Klostermann, 1807, 213–218.
- [A8] LACROIX, S. F. *Traité élémentaire de calcul différentiel et de calcul intégral*. 3 vol. Paris: Duprat, 1797–1800. [N'hi ha diverses edicions posteriors, editades per Bachelier, París. La que citem en el text de 1810 és editada per Chez Courcier, i porta el subtítol «Seconde édition, revue et augmentée»]
 - [A9] LANCRET, M. A. «Mémoire sur les courbes a double courbure». A: *Mémoires présentés par divers savants à l'Académie des sciences de l'Institut de France*, I (1802), 416–454. [Llegit el 6 de floreal de l'any 10]
 - [A10] LEGENDRE, A.-M. «Mémoire sur l'integration de quelques équations aux différences partielles». *Histoire de l'Académie royale des sciences*, Paris (1789), 309–351. [Llegit l'1 de setembre de 1787]
 - [A11] LEROY, C. F. A. *Traité de stéréotomie, comprenant les applications de la géométrie descriptive à la théorie des ombres, la perspective linéaire, la gnomonique, la coupe des pierres et la charpente*. Paris: Bachelier, 1844.
 - [A12] OLIVIER, T. «Mémoire de géométrie. De la courbure et la flexion d'une courbe a double courbure». *Journal de l'École royale polytechnique*, 24e cahier, 15 (1835), 61–92.

Codis correctors d'errors i criptografia postquàntica

NARCÍS SAYOLS I SEBASTIÀ XAMBÓ

Resum: Revisitem el sistema criptogràfic de clau pública de McEliece, introduït fa quaranta anys, amb l'ajuda de recursos desenvolupats recentment: una millora del descodificador de Peterson-Gorenstein-Zierler per als codis correctors d'errors alternants; un sistema de computació simbòlica i un paquet d'utilitats funcionals per als càlculs emprats en la definició, codificació i descodificació de codis correctors d'errors, tot programat en Python, i una pàgina web que dona accés lliure als materials generats pel projecte. L'interès principal del sistema de McEliece rau en el fet que és un candidat seriós per a un estàndard de criptografia postquàntica.

Paraules clau: criptografia postquàntica, codis alternants, computació simbòlica, programari lliure.

Classificació MSC2010: 11T71, 68-04, 68W30, 94A60.

Pròleg

Com que els autors d'aquest article no som experts en criptografia, abans de res ens sembla convenient comentar què ens ha portat a escriure'l.

El context ha estat el treball, iniciat la tardor del 2015, per dissenyar i programar PyECC, un entorn que permeti la construcció, codificació i descodificació de codis correctors d'errors i posar-lo a la lliure disposició del públic, tot pensant bàsicament en estudiants, docents i investigadors. El nucli d'aquest entorn és un paquet de classes i funcions de Python¹ que anomenem CC (vegeu [46]).

Inicialment la idea fou igualar la funcionalitat del paquet WIRIS/CC descrit a [56], un entorn desenvolupat a fi de poder realitzar les tasques computacionals esmentades per als codis correctors tractats en aquell text. Però aviat ens van convèncer que podíem anar més enllà en diverses direccions. Una d'elles, que ha resultat ser un bon test per a PyECC, fou la implementació d'un prototip rudimentari del sistema criptogràfic de clau pública descrit a [32].

¹ <https://ca.wikipedia.org/wiki/Python>.

Aquest estudi del sistema de McEliece ens portà a interessar-nos per la seva evolució des que es va publicar fa quaranta anys fins a l'actualitat. El resultat és que segueix sent, com veurem, una de les línies més prometedores en un horitzó de *criptografia postquàntica*, locució introduïda el 2003 per D. J. Bernstein (vegeu [41]) per designar paradigmes criptogràfics que garanteixin protecció contra qualsevol giny de computació, actual o futur, incloent-hi els sistemes de computació quàntica (per a una introducció general a la computació quàntica, vegeu, per exemple, [45]; per a una avaluació recent de la possible evolució de l'enginyeria de sistemes de computació quàntica i dels sistemes de *criptografia quàntica*, vegeu [17, 16] i la nota al final de la secció 5). Aquest fet ens sembla que té una gran importància, ja que els estàndards criptogràfics usats en l'actualitat no ofereixen aquestes garanties. Per exemple, els sistemes basats en la dificultat de factoritzar números enters, com ara el sistema RSA,² resulten extremament vulnerables a la computació quàntica a causa de la (baixa) complexitat polinòmica del q -algorisme de Shor per factoritzar números enters (vegeu [45, § 8]).

En gran mesura, el contingut d'aquest treball es correspon amb el de la conferència [47] programada en la Jornada de Teoria de Nombres celebrada el 7 d'octubre del 2017 al Departament de Matemàtica de la Universitat de Lleida.³ Tanmateix, el desig d'augmentar-ne l'asequibilitat ens ha impulsat a incorporar força més detalls dels que es poden comunicar en una presentació oral, i a introduir variacions en l'ordre expositiu per aconseguir que el pendent de la lectura sigui tan suau com sigui possible.

A la primera secció es descriuen breument els ingredients d'un sistema criptogràfic de clau pública i amb més detall, a la segona secció, els que concorren en un sistema de McEliece. Tot seguit s'exposen, a la tercera secció, les generalitats que necessitem sobre codis correctors d'errors, incloent-hi els detalls específics sobre els codis d'un sistema de McEliece (codis de Goppa clàssics binaris). A les seccions quarta i cinquena es tracten, respectivament, l'evolució dels sistemes de McEliece i el grau de seguretat criptogràfica que ofereixen. L'apèndix A conté una breu notícia sobre PyECC, i en particular sobre el seu ús i instal·lació, i a l'apèndix B es donen els detalls més rellevants sobre la implementació usant PyECC d'un sistema de McEliece.

1 Criptografia de clau pública

En un *sistema criptogràfic*, un missatge M és *encriptat* en un *criptograma* C amb una funció E_k que depèn d'un paràmetre k anomenat *clau d'encriptació*:

$$C = E_k(M).$$

² Vegeu <https://ca.wikipedia.org/wiki/RSA>.

³ Seminari «Cargols 2017», organitzat pel Grup de Recerca en Criptografia i Grafs, <http://www.cig.udl.cat/>.

La *descodificació* $D_{k'}(C)$ corresponent es realitza mitjançant una funció $D_{k'}$, també dependent d'un paràmetre k' (*clau de descriptació*), i el primer requisit fonamental és que s'ha de complir la relació

$$D_{k'}(C) = D_{k'}(E_k(M)) = M. \quad (1)$$

A més, les funcions E i D s'han de poder calcular eficientment.

Per tal que es pugui verificar l'equació (1), k i k' han d'estar relacionades i, per tant, un usuari emissor i un usuari receptor han de compartir informació adient sobre k i k' . L'intercanvi d'aquesta informació de manera que altres usuaris no hi puguin accedir és l'anomenat *problema de distribució de claus*. Un pas cabdal en la solució d'aquest problema fou l'esquema de Diffie i Hellman [22] publicat el 1976. Segons afirmen en el resum els seus autors: «les necessitats de telecomunicació han donat lloc a la necessitat de nous tipus de sistemes criptogràfics que minimitzin la necessitat de disposar de canals de distribució de claus segures i que proporcionin l'equivalent a una signatura per escrit. Aquest article suggereix maneres de resoldre aquests problemes actualment oberts». Una de les maneres que proposen és la dels *sistemes criptogràfics de clau pública*, «que permeten la transmissió d'informació per canals insegurs sense comprometre la seguretat del sistema».

En un sistema criptogràfic de *clau pública*, com ara el de McEliece, cada usuari té una clau d'encryptació *pública* i una clau de descriptació *privada* (o secreta). Abans d'entrar en més detalls, il·lustrem breument el funcionament en el cas del familiar sistema RSA. Publicat el 1978 per Rivest, Shamir i Adleman [44], en descrivim el funcionament a continuació (com a referència general, vegeu [20]).

Tot usuari disposa de la seva clau en una part privada i una part pública. La part privada està formada per dos números primers p i q , i la clau pública, pel producte $n = pq$ i per un número natural k primer amb $(p-1)(q-1)$. L'encryptació que fa un altre usuari del missatge M (que podem suposar que és un número enter no negatiu inferior a n) s'obté per la fórmula

$$C = M^k \bmod n, \quad (2)$$

i la descodificació amb

$$C^{k'} \bmod n, \quad (3)$$

on k' és l'invers de k mòdul $(p-1)(q-1)$. La relació (1) en aquest cas significa que

$$M^{kk'} = M \bmod n, \quad (4)$$

la qual és una conseqüència directa de resultats elementals d'aritmètica modular i per als quals el lector pot consultar [20, § 3.3.1]. Adonem-nos que un sistema RSA és segur sempre que la factorització de números enters grans sigui un problema difícil.

2 Ingredients d'un criptosistema de McEliece

Els ingredients *generals* d'aquest protocol d'encryptació són els següents:

- $F = F_q$, un cos finit de cardinal q (aquí el cas més important serà $F = \mathbb{Z}_2$).
- k , un número enter positiu. Dels elements de l'espai F^k en direm *missatges*.
- $n > k$, un número enter. Dels elements de l'espai F^n en direm *missatges de transmissió* o també *missatges de canal*. Si $\mathbf{x} \in F^n$, posarem $|\mathbf{x}|$ per denotar el nombre de components no nul·les de $\mathbf{x}$ i direm que és el *pes* de $\mathbf{x}$.

Aquests ingredients són públics i hom suposa que qualsevol usuari del protocol pot generar missatges i missatges de transmissió, i que pot enviar qualsevol missatge de transmissió a qualsevol altre usuari.

Cada usuari també ha de disposar de mitjans per generar els objectes i efectuar els càlculs adients al seu paper d'emissor o receptor. Tot seguit descrivim aquests objectes i operacions segons que es tracti de generar claus (clau privada i clau pública) per tal d'esdevenir un usuari receptor, d'encryptar i enviar un missatge en el cas d'un usuari emissor, o de descryptar un missatge rebut en el cas d'un receptor.

Generació de claus. Una *clau privada*, que denotarem $\{G, S, P\}$, està formada per tres matrius d'elements de F :

- G , matriu $k \times n$ de rang k .
- S , matriu $k \times k$ invertible seleccionada aleatòriament segons la distribució uniforme.
- P , matriu $n \times n$ de permutació seleccionada aleatòriament, també segons la distribució uniforme.

La propietat més decisiva de la matriu G per a un usuari receptor és que ha d'existir una funció

$$D: X \rightarrow F^n, \text{ on } X \subseteq F^n,$$

que gaudeixi de la propietat següent, on t és un número enter positiu prefixat:

(*) Per a tot $\mathbf{u} \in F^k$ i tot $\mathbf{e} \in F^n$ amb $|\mathbf{e}| \leq t$, es compleix

$$\mathbf{x} = \mathbf{u}G + \mathbf{e} \in X \quad \text{i} \quad D(\mathbf{x}) = \mathbf{u}G.$$

D'aquesta funció D en direm *descodificador*, i ens referirem a la propietat anterior dient que D *pot corregir fins a t errors*. Dels elements de X es diu que són vectors *descodificables*.

En principi, cada usuari pot tenir el seu propi descodificador, en el sentit que l'algorisme emprat per calcular D , i la seva implementació, poden ser privats per als usuaris que ho desitgin. Tanmateix, cal dir que un sistema complet ha d'incorporar un descodificador que serveixi per a tothom (descodificador *per*

defecte), i que en principi és raonable pensar que tots els usuaris poden ser emissors i receptors.

La teoria fonamental que usarem per a la construcció de descodificadors apropiats és la teoria de codis correctors d'errors.

La *clau pública* corresponent a la clau privada $\{G, S, P\}$ és un parell $\{G', t\}$ definit com segueix:

- $G' = SGP$, que és una matriu $k \times n$.
- Un número enter positiu t que satisfà $(*)$.

Protocol d'encryptació. El protocol que ha de seguir un usuari que vol encryptar i enviar un missatge $\mathbf{u}$ a l'usuari amb clau pública $\{G', t\}$ consta de dos passos:

- Generació aleatòria d'un vector de transmissió $\mathbf{e}$ de pes t .
- Tramesa del vector $\mathbf{x} = \mathbf{u}G' + \mathbf{e} = \mathbf{u}SGP + \mathbf{e}$.

Protocol de desencryptació. Consta de quatre passos que només usen informació privada del receptor i el vector $\mathbf{x}$ enviat per l'emissor:

- Càlcul de $\mathbf{y} = \mathbf{x}P^{-1}$, de manera que $\mathbf{y} = (\mathbf{u}S)G + \mathbf{e}P^{-1}$.
- Càlcul de $\mathbf{x}' = D(\mathbf{y})$. Com que P és una matriu de permutació,

$$|\mathbf{e}P^{-1}| = |\mathbf{e}| = t$$

i, per tant, aquesta operació està ben definida, ja que D corregeix fins a t errors. El resultat és $\mathbf{x}' = (\mathbf{u}S)G$. És a dir, $\mathbf{x}'$ és una combinació lineal de les files de G amb coeficients $\mathbf{u}' = \mathbf{u}S$.

- Com que G té rang k , $\mathbf{u}'$ queda unívocament determinat per $\mathbf{x}'$ i es pot obtenir resolent el sistema d'equacions lineals $\mathbf{x}' = \mathbf{u}'G$, on la incògnita és el vector $\mathbf{u}'$.
- Càlcul de $\mathbf{u} = \mathbf{u}'S^{-1}$. Missatge rebut correctament!

Per als aspectes computacionals d'aquests ingredients, vegeu: A.2 «Aritmètica modular», A.3 «Polinomis irreductibles», A.4 «Construcció de cossos finits», A.5 «Vectors i matrius», i A.6 «Utilitats per al sistema McEliece».

3 Codis de Goppa clàssics

En el que segueix, posem $F(k, n)$ per denotar les matrius d'ordre $k \times n$ formades amb elements d'un cos F .

Codis lineals: conceptes bàsics i notacions Un codi (lineal) de tipus $[n, k]$ sobre F_q és un subespai vectorial C de dimensió k de F_q^n . En particular s'ha de complir $k \leq n$. Diem que n i k són la *longitud* i la *dimensió* de C , respectivament, i escrivim $C \sim [n, k]$. La *taxa de transmissió* de C és el quocient $R = k/n$.

Una matriu G de tipus $k \times n$ es diu que és una *matriu generadora* de C si les seves files formen una base de C . Donada una matriu G de tipus $k \times n$, posem $\langle G \rangle$ per denotar el subespai vectorial generat per les files de G . És un codi de tipus $[k', n]$, on k' és el rang de G . En el cas que G sigui una matriu generadora de C , llavors $\langle G \rangle = C$.

Si G és una matriu generadora del codi $C \sim [n, k]$, l'aplicació lineal $f: F_q^k \rightarrow F_q^n$, $\mathbf{u} \mapsto \mathbf{u}G$, és injectiva i la seva imatge és C . De l'aplicació f es diu que és un *codificador* de C , i si $\mathbf{u} \in F_q^k$, $\mathbf{x} = f(\mathbf{u})$ és la *codificació* de $\mathbf{u}$.

EXEMPLE (EL CODI DE HAMMING BINARI $[7, 4]$). $\mathbf{x} = \mathbf{u}G$, on

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

Els codis lineals també es poden descriure mitjançant el que podem anomenar *construcció dual*. Sigui H una matriu de tipus $r \times n$ i suposem que el seu rang és r . Llavors

$$C_H = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x}H^T = 0\} = \ker H^T$$

és un codi lineal $[n, n - r]$. De la matriu H es diu que és una *matriu de control* de C_H . És clar que podem formar una matriu generadora de C_H escollint una base de $\ker H^T$.

EXEMPLE. La matriu

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

és una matriu de control del codi de Hamming $[7, 4]$. En efecte, si posem R per denotar la submatriu formada per les tres darreres columnes de G , llavors $G = (I_4 | R)$, $H = (R^T | I_3)$, i

$$GH^T = (I_4 | R) \begin{pmatrix} R \\ I_3 \end{pmatrix} = R + R = 0.$$

Per tant, $C = \langle G \rangle \subseteq \ker H^T$, que de fet és una igualtat perquè els dos termes de la inclusió tenen dimensió 4.

REMARCA. Una matriu generadora de la forma $G = (I_k | R)$ es diu que és *sistemàtica* respecte de les components $1, \dots, k$, ja que $\mathbf{x} = \mathbf{u}G = (\mathbf{u} | \mathbf{u}R)$ i això permet recuperar $\mathbf{u}$ com les primeres k components de $\mathbf{x}$. En aquest cas, un argument similar al de l'exemple anterior ens permet concloure que $H = (-R^T | I_{n-k})$ és una matriu de control de $\langle G \rangle$. Remarquem que $H = (R^T | I_{n-k})$ en el cas binari.

La construcció dual admet la generalització que descrivim a continuació i que usarem per construir els codis de Goppa clàssics. Sigui $F = F_q$ i $\bar{F} = F_{q^m}$, on m és un número enter positiu. Sigui $\bar{H}$ una matriu de tipus $r \times n$ amb

components de $\bar{F}$ i suposem que el seu rang és r . Llavors podem definir el codi lineal/ F

$$C_{\bar{H},F} = C_{\bar{H}} \cap F^n = \{\mathbf{x} \in F^n : \mathbf{x}\bar{H}^T = 0\}.$$

Per trobar una matriu de control H (sobre F) d'aquest codi, podem procedir de la manera següent. Sigui H' la matriu sobre F obtinguda substituint cada element β de $\bar{H}$ per la columna de les m components de β relativament a una base de $\bar{F}$ sobre F , de manera que $H' \in F(rm, n)$. Finalment, sigui H el resultat de suprimir les files de H' que són combinació lineal de les anteriors, $H \in F(r', n)$. De la construcció es desprèn que

$$C_{\bar{H},F} = C_{H'} = C_H$$

i, per tant, $\dim C_H = n - r'$. Atès que $r' \leq mr$, resulta que $k \geq n - r'$. També es compleix que $r' \geq r$ o $k \leq n - r$ (vegeu, per exemple, [56, prop. 4.1]). Per a un exemple concret de càlcul de H' , H , r' i k , vegeu A.7.

Un *descodificador* d'un codi C és una aplicació exhaustiva $g: F^n \rightarrow C \sqcup \mathcal{E}$ (unió disjunta), on $\mathcal{E}$ és un conjunt de «missatges d'error», que compleix $g(\mathbf{x}) = \mathbf{x}$ per a tot $\mathbf{x} \in C$.

El conjunt $g^{-1}(C) \subseteq F^n$ és el dels *vectors descodificables*, mentre que el conjunt $F^n - g^{-1}(C) = g^{-1}\mathcal{E}$ és el conjunt dels *vectors erroris*. Un descodificador és *complet* si $g^{-1}(C) = F^n$ (cas en el qual $\mathcal{E} = \emptyset$).

Diem que el descodificador g té *capacitat correctora* t si $g(\mathbf{y}) = \mathbf{x}$ per a tot vector $\mathbf{y} \in F^n$ tal que $|\mathbf{y} - \mathbf{x}| \leq t$.

Si posem $B(\mathbf{x}, t) = \{\mathbf{y} \in \mathbb{F}^n : |\mathbf{y} - \mathbf{x}| \leq t\}$ (d'aquest conjunt es diu que és la *bola de Hamming* de centre $\mathbf{x}$ i radi t), aleshores tenim que $\cup_{\mathbf{x} \in C} B(\mathbf{x}, t) \subseteq g^{-1}(C)$ i $g(B(\mathbf{x}, t)) = \{\mathbf{x}\}$.

Codis de Goppa binaris Per completar la construcció d'un sistema de McEliece, l'ingredient més important que ens falta és una matriu generadora binària G que compleixi la condició (*) de la pàgina 150. Dediquem el que resta d'aquesta secció a descriure com es resol aquest problema. Per a la construcció efectiva de les matrius S i P , vegeu A.6.

Si bé és cert que el sistema inicial de McEliece és binari, la descripció dels codis de Goppa clàssics la farem sobre un cos finit F qualsevol. Preparem així el terreny per poder considerar variacions del sistema original introduïdes posteriorment sense que, de fet, representi cap dificultat teòrica addicional.

Sigui, doncs, $F = F_q$ un cos finit ($F = \mathbb{Z}_2$ en el cas binari). Escollim un número enter positiu m i posem $\bar{F} = F_{q^m}$. Escollim elements distints $\alpha = \alpha_1, \dots, \alpha_n \in \bar{F}$, cosa que implica $n \leq q^m$, i un polinomi $p \in \bar{F}[T]$ de grau $r \geq 1$ tal que $p(\alpha_j) \neq 0$ ($j = 1, \dots, n$). Finalment posem $h_j = 1/p(\alpha_j)$ ($j = 1, \dots, n$) i $\Gamma = \Gamma(p, \alpha) := C_{\bar{H},F}$, on

$$\bar{H} = \begin{pmatrix} h_1 & \dots & h_n \\ h_1\alpha_1 & \dots & h_n\alpha_n \\ \vdots & & \vdots \\ h_1\alpha_1^{r-1} & \dots & h_n\alpha_n^{r-1} \end{pmatrix}.$$

Diem que Γ és el *codi de Goppa clàssic* associat a p i α . Com que el nombre de files de $\bar{H}$ és r , i $\bar{F}$ té grau m sobre F , $k = \dim \Gamma(p, \alpha)$ compleix, pel que ja hem dit, que $n - r \geq k \geq n - rm$. A més, resulta que Γ corregeix t o menys errors, on t és la part entera de $r/2$ [56, p. 191]. En el cas binari, Γ corregeix r o menys errors si p no té arrels múltiples [56, exercici P.4.7, p. 194]. De fet, en aquest cas es compleix que $\Gamma(p, \alpha) = \Gamma(p^2, \alpha)$ i, per tant, aquest codi corregeix t errors si $t \leq r$. Per a un exemple detallat, vegeu A.8.

Descodificadors Els codis de Goppa clàssics són un cas especial dels anomenats *codis alternants*. L'interès d'aquests codis no rau només en el fet que els constructors de codis de Goppa clàssics són especialitzacions dels constructors de codis alternants, sinó que els codis alternants admeten descodificadors generals eficients que proporcionen bons descodificadors per als codis de Goppa clàssics i, en particular, per als codis de Goppa clàssics binaris.

El paquet PYECC inclou implementacions dels dos descodificadors principals per a codis alternants: el de Berlekamp-Massey-Sugiyama (BMS) i el de Petterson-Gorenstein-Zierler (PGZ). Vegeu l'exemple A.9.

4 Evolució dels sistemes de McEliece

El context en què McEliece va proposar el seu sistema va ser el creat pels treballs de Diffie i Hellman [22], en què van introduir la noció de sistema criptogràfic de clau pública; de Merkle i Hellman [33], en què van proposar el sistema basat en la dificultat de l'anomenat *problema de la motxilla*,⁴ i sobretot de Rivest, Shamir i Adleman [44], en què van proposar el celebrat sistema RSA basat en la dificultat de factoritzar números enters (vegeu § 1). El sistema de McEliece fou el primer sistema de clau pública basat en la teoria dels codis algebraics que havia introduït Goppa el 1970 [28], i que aquí en diem *codis de Goppa clàssics* (en el marc dels codis de Goppa generals, es corresponen amb els codis de gènere 0).⁵ Esmentem també que els paràmetres escollits per McEliece per il·lustrar diversos aspectes del seu sistema van ser $[n, k] = [1024, 524]$ i $t = 50$, que garantien una seguretat de més de 60 bits, considerable fa quaranta anys, però no, com veurem a la secció següent, en les circumstàncies actuals.

Una modificació del sistema de McEliece va ser proposada per Niederreiter el 1986 [37]. La clau privada d'aquest sistema és una terna $\{H, S, P\}$ de matrius binàries de tipus $n \times (n - k)$, $(n - k) \times (n - k)$ i $n \times n$, respectivament. Aquestes matrius han de satisfer les condicions següents: H és una matriu de control d'un codi de Goppa clàssic binari $\Gamma \sim [n, k]$ (és a dir, $y \in \Gamma$ si i només si $yH^T = 0$) que corregeix t errors, S és una matriu no singular escollida aleatòriament segons la distribució uniforme, i P és una matriu de permutació,

⁴ Vegeu https://ca.wikipedia.org/wiki/Problema_de_la_motxilla, on també es documenta la ruptura d'aquest sistema el 1982 per Shamir.

⁵ McEliece no cita l'article de Goppa i, en canvi, remet a les pàgines 179-180 i 193-194 de [31].

també escollida aleatòriament segons la distribució uniforme. La clau pública corresponent és el parell $\{H', t\}$, on $H' = PHS$. Els missatges $\mathbf{u}$ són vectors binaris de longitud n i pes t . El missatge encriptat és $\mathbf{x} = \mathbf{u}H' = \mathbf{u}PHS$. El receptor recupera $\mathbf{u}$ de la manera següent: (1) calcula $\mathbf{s} = \mathbf{x}S^{-1} = \mathbf{u}PH$; (2) com que coneix H , pot trobar $\mathbf{u}' = \mathbf{u}P = D(\mathbf{s}, \mathbf{x})$ amb un descodificador D apropiat (algorisme de Patterson [39], que avui convé veure com una variant dels descodificadors estàndard BMS o PGZ), i (3) com que coneix P , pot trobar $\mathbf{u} = \mathbf{u}'P^{-1}$, que és el missatge enviat. Els valors dels paràmetres en la il·lustració inicial eren $[n, k] = [1024, 644]$, $t = 38$. Per a la generació eficient de missatges de pes t i longitud n , vegeu [48].

En l'estudi dels sistemes de McEliece i Niederreiter presentat a la memòria d'habilitació de Sendrier de 2002 [49], s'afirma: «Després de vint anys d'esforços [i cita una dotzena llarga de treballs], cap criptoanàlisi ha pogut rompre aquests sistemes». Com veurem, aquesta apreciació segueix essent vàlida.

El problema de modificar els sistemes de McEliece i Niederreiter per poder funcionar amb claus públiques substancialment menors és considerat per Gaborit a [26]. Serveixin, com a il·lustració del resultat, les dades següents: per a longituds 2047 i 4095, són suficients claus públiques de 12 KB i 20 KB, respectivament. Per a més detalls de com estaven les coses fa una dècada, és recomanable l'article [24]. Per als autors, «la criptografia basada en teoria de codis és una alternativa interessant a la criptografia basada en teoria de nombres», ja que «moltes de les funcions criptogràfiques bàsiques [...] es poden realitzar amb conceptes de teoria de codis».

També cal esmentar l'article [12], que entre d'altres qüestions proposa nous paràmetres per als sistemes de McEliece i Niederreiter que assoleixen bons nivells de seguretat contra tots els atacs coneguts i amb longituds de les claus considerablement menors. A més, s'afirma que «els computadors quàntics no aporten millores significatives a la potència dels atacs més enllà de possibles millores genèriques derivades de l'algorisme de Grover i, per tant, l'esquema criptogràfic de McEliece és un dels candidats interessants per a la criptografia postquàntica» (per a l'algorisme de Grover, podeu consultar per exemple [45, § 5]).

Si bé la noció de criptografia postquàntica va ser introduïda, com ja s'ha dit, el 2003, al nostre entendre l'inici més visible es produeix quan a la publicació del magnífic manual de criptografia convencional [29] va seguir, un any més tard, la del volum [10]. En aquest volum, el primer d'aquest nou enfocament de la criptografia, és important l'article introductori de D. J. Bernstein [7], que en particular presenta els quatre paradigmes considerats més prometedors. A més de la criptografia basada en codis (article d'Overbeck i Sendrier [38]), es consideren també sistemes basats en polinomis de diverses variables, en reticles de $\mathbb{R}^n$ (vegeu [53] per a un article recent sobre la qüestió), i en funcions *hash*. En l'article de Bernstein tot just esmentat, trobem el que podria ser el *leitmotiv* de la criptografia postquàntica: «No hi ha justificació per saltar de l'afirmació “els computadors quàntics destrueixen RSA, DSA i ECDSA” a l'afirmació “els computadors quàntics destrueixen la criptografia”. Hi ha moltes

classes importants de sistemes criptogràfics més enllà de RSA, DSA i ECDSA». De fet, en l'article d'Overbeck i Sendrier llegim: «Passades tres dècades, s'han hagut d'ajustar una mica els paràmetres, però no es coneix cap atac que representi una amenaça seriosa [als sistemes de McEliece], ni tan sols els d'un computador quàntic».

Aquestes apreciacions s'han repetit, i fins i tot reforçat, en els darrers anys. Esmentem una mostra de treballs en què s'aprofundeix en diverses direccions: [15], [13] (aquest article proposa nous paràmetres per aconseguir un bon nivell de seguretat davant de tots els atacs coneguts), [3], [34], [36] (tesi doctoral), [40] (una altra tesi doctoral, en la qual es revitalitzen els codis de Srivastava generalitzats, i amb implementacions efectives), [43], [54] i [21].

En tota aquesta dècada postquàntica, un pioner a tenir en compte és D. J. Bernstein, que ja hem citat i del qual en recomanem la pàgina web: [6]. També val la pena consultar la pàgina que publica amb T. Lange, [41], i seguir la conferència PQC 2018, enfocada a aconseguir una estandardització dels protocols criptogràfics postquàntics i de la qual podeu trobar informació a [19].

5 Seguretat criptogràfica d'un sistema de McEliece

El mateix McEliece a [32] considerarà la qüestió de la seguretat que podia oferir el seu sistema. En un planteig general, hom suposa que un espia, diguem-ne E , ha aconseguit el vector encriptat $\mathbf{x}$ enviat per un usuari i que coneix la clau pública del destinatari, és a dir, $G' = SGP$ i t . Quines possibilitats té d'obtenir el missatge inicial $\mathbf{u}$?

Intentar descodificar $\mathbf{x} = \mathbf{u}G' + \mathbf{e}$ usant la matriu coneguda G' no es pot considerar prometedor, si k és suficientment gran, ja que el problema de descodificar codis lineals $[n, k]$ és NP-complet (cf. [5]).

L'altre atac que va considerar McEliece al seu sistema és més sorprenent. L'espia pot seleccionar k coordenades de $\mathbf{x}$ aleatòriament. Si té sort, cap d'aquestes coordenades serà errònia i podrà determinar $\mathbf{u}$ resolent el sistema d'equacions lineals $\tilde{\mathbf{x}} = \mathbf{u}\tilde{G}'$, on $\tilde{\mathbf{x}}$ és el vector format amb les coordenades de $\mathbf{x}$ seleccionades i $\tilde{G}'$ és la submatriu de G' formada amb les columnes corresponents als índexs de $\tilde{\mathbf{x}}$. Si no té sort, alguna de les entrades seleccionades serà errònia i el sistema no tindrà solució. Aquest atac és més seriós del que podria semblar a primera vista. En efecte, decidir si el sistema $\tilde{\mathbf{x}} = \mathbf{u}\tilde{G}'$ és compatible, i trobar la solució si en té, comporta un nombre d'operacions de l'ordre de k^3 , mentre que la probabilitat d'escollir k coordenades no errònies és

$$\binom{n-t}{k} / \binom{n}{k} = \left(1 - \frac{t}{n}\right) \left(1 - \frac{t}{n-1}\right) \cdots \left(1 - \frac{t}{n-(k-1)}\right) < (1 - t/n)^k,$$

de manera que el nombre d'operacions que l'espia ha d'esperar fer per tenir èxit és superior a $k^3/(1 - t/n)^k$. Amb els paràmetres de la il·lustració de McEliece, això comporta un esforç no inferior a 2^{64} operacions, un fet que podem expressar dient que assoleix una seguretat de 64 bits (relativament a l'atac en qüestió).

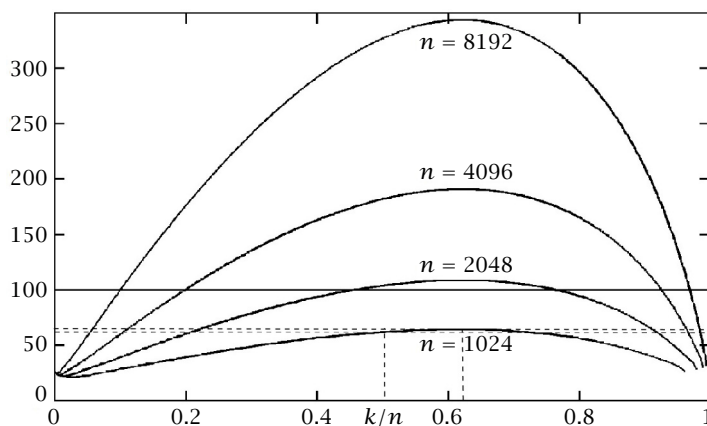


FIGURA 1: Grau de seguretat en bits del sistema de McEliece en funció de la taxa de transmissió $R = k/n$ i per a longituds $n = 2^l$ ($l = 10, \dots, 13$) del codi. Com a grau de seguretat es pren el logaritme en base 2 del nombre d'unitats de computació (factor de treball) de l'atac més fort conegut.

La figura 1, adaptada de la figura 6.2 de [49], resumeix el grau de seguretat del sistema de McEliece a principis d'aquest segle. Hi hem afegit les línies de punts per tal de poder-lo comparar amb el grau de seguretat que acabem de comentar. Veiem que, tenint en compte tots els atacs, els paràmetres originals garanteixen 63 bits de seguretat, i que amb una taxa una mica superior (0.625 en lloc de $524/1024 = 0.512$) es té, per la mateixa longitud, una seguretat de 64 bits, en remarcable coincidència amb l'anàlisi inicial.

Sendrier també remarca que, si bé els dos sistemes tenen avantatges pel que fa a la facilitat d'implementació, la seva clau pública és relativament gran. També anuncia un resultat que cal considerar important, ja que fins aleshores no s'havia aconseguit trobar: un esquema de signatura digital basat en McEliece.

Les referències que segueixen posen de manifest que aquests resultats de Sendrier sobre el grau de seguretat continuen essencialment vigents, sovint amb variacions pel que fa als codis emprats: [50, 52, 23, 2, 27, 11, 1].

En l'article [2] es consignen les recomanacions inicials del projecte PQCRYPTO, ja esmentat, pel que fa a la confiança en la seguretat dels sistemes, més que no pas en l'eficiència. Per exemple, per als sistemes de McEliece basats en codis de Goppa clàssics binaris, els paràmetres que es proposen són $n = 6960$, $k = 5413$ i $t = 119$ per assolir 128 bits de seguretat. La seguretat de 128 bits és inferior als 172 bits que dona el recompte de McEliece que hem comentat abans, la qual cosa s'explica pel fet que en les estimacions es tenen en compte tots els atacs coneguts que s'havien imaginat fins a aquell moment. Per a més detalls sobre el sistema de McEliece proposat per Bernstein *et al.*, i també sobre una variant del McEliece-Niederreiter, vegeu [18].

Acabem la secció amb unes referències sobre progressos en computació quàntica que poden ajudar a entendre per què aquest recurs, fins i tot amb tota la potència imaginable en el futur, potser no pot arribar a ser tan poderós com s'ha estimat en moments passats i que molt probablement mai serà suficient per trencar alguns dels sistemes que com el de McEliece tenen tot el potencial de ser realment postquàntics: [17, 9, 8, 14].

Tanmateix, cal esmentar que el treball pioner de Shor [51] va contribuir a promoure el camp de la criptografia quàntica, l'objectiu de la qual és usar les propietats quàntiques dels sistemes per dissenyar sistemes criptogràfics. Per a una descripció elemental d'aquests sistemes, vegeu [16] i la bibliografia corresponent. Per a una visió general, que inclou la relació amb la criptografia postquàntica, vegeu [55, 18] i els ja citats [10, 8, 11].

A Introducció a PyECC

L'arquitectura de PyECC es basa en una jerarquia de classes de Python gestionada mitjançant un paquet de funcions que li serveix d'interfície. Per als detalls sobre aquesta arquitectura, així com sobre la instal·lació i ús, vegeu [46]. En la resta d'aquest apèndix s'exposen unes consideracions generals destinades a il·lustrar-ne el funcionament.

A.1 Valors i noms

Tot objecte creat amb PyECC té un nom per defecte. Per exemple, $\text{Zn}(6)$ crea l'anell $\mathbb{Z}_6$ i el seu nom és Z6 . Podem optar per donar-li un nom, posem $'A'$, amb la sintaxi $\text{Zn}(6, 'A')$. La llista següent mostra la seva flexibilitat (emprem els símbols $\rightarrow$ per indicar que el valor que els segueix és el de l'expressió anterior):

```
Zn(6)
--> Z6 :: Ring
A = Zn(6)
A
--> Z6 :: Ring
Z6 = Zn(6, 'A')
Z6
--> A :: Ring
A = Zn(6, 'A')
A
--> A :: Ring
```

Un altre exemple és que l'anell de polinomis $A[X]$ sobre l'anell anomenat A es pot crear amb `polynomial_ring(A)`, i es pot optar per donar altres noms a la indeterminada i al mateix anell de polinomis:

```
A = Zn(6)
polynomial_ring(A)
--> [Z6[X] :: Ring, X :: Z6[X]]
```



```

A = Zn(6,'A')
polynomial_ring(A)
--> [A[X] :: Ring, X :: A[X]]
polynomial_ring(A,'t')
--> [A[t] :: Ring, t :: A[t]]
polynomial_ring(A,'t','P')
--> [P :: Ring, t :: P]
polynomial_ring(A,name='P')
--> [P :: Ring, X :: P]

```

Convencions similars són vàlides per a la creació d'extensions de cossos o d'anells, com es veurà en els exemples que segueixen.

A.2 Aritmètica modular

En general, $Zn(n)$ crea l'anell $\mathbb{Z}_n = \mathbb{Z}/(n)$, i en particular el cos de n elements quan n és primer. Si A i B són anells construïts i existeix un homomorfisme «canònic» de A a B , la imatge de $a \in A$ a B per aquest homomorfisme es denota $a \gg B$.

```

A = Zn(17)
# Projecció de 3 a A
a = 3>>A
--> 3 :: Z17
# Ordre de l'element a
order(a)
--> 16
# Ordre de 3 mòdul 17
order(3,17)
--> 16
# Potències de a, vistes com enters
[lift(a**j) for j in range(17)]
--> [1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]
# Potències de 3 mòdul 17
[3**j % 17 for j in range(17)]
--> [1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]
# Potències de a
vector([a**j for j in range(17)])
--> [1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,1] :: Vector[Z17]

```

A.3 Polinomis irreductibles

Per a la construcció de la matriu G d'una clau privada de McEliece és necessària l'elecció d'un polinomi mònic irreductible p de grau t sobre $F = F_q$ (t és el segon element de la clau pública). A tal fi tenim la funció

```
p = get_irreducible_polynomial(F,t)
```

Com que aquesta funció itera la selecció aleatòria d'un polinomi p mònic de grau t mentre p no sigui irreductible, és important conèixer la probabilitat que p sigui irreductible. El resultat és que aquesta probabilitat és $\sim 1/t$ com a

conseqüència de la *fórmula de Gauss* que dona el nombre $I_q(t)$ de polinomis mòncics irreductibles de grau t sobre $\mathbb{F}_q$:

$$I_q(t) = \frac{1}{t} \sum_{d|t} \mu(t/d) q^d = \frac{q^t}{t} + \dots$$

De fet, la probabilitat esmentada és $I_q(t)/q^t = \frac{1}{t} + \dots$, ja que q^t és el nombre de polinomis mòncics de grau t . Vegeu la figura 2 en la qual es mostra la primera cella d'un *notebook* de Jupyter (Nb) que conté codi PyECC per calcular $I_q(t)$ i tabular-ne uns quants valors.

A.4 Construcció de cossos finits

La creació de cossos (i anells) finits es pot fer com en l'exemple següent.

```
# Creació del cos binari
K = Zn(2)
# Creació del cos F = F8 com a K[X]/(f=X^3+X+1), amb a = X mod f
[F,a] = extension(K, [1,0,1,1], 'a', 'F')
```

Si A és un anell ja construït i $C = [1, a_1, \dots, a_r]$ és una llista d'elements de A amb primer element 1, PyECC crea l'anell

$$B = A[X]/(f = X^r + a_1 X^{r-1} + \dots + a_{r-1} X + a_r),$$

i ensems fa l'assignació $x = X \bmod f$, amb l'expressió

```
[B,x] = extension(A,C, 'x', 'B')
```

Com ja s'ha dit abans, l'anell de polinomis $P = A[X]$ es pot crear amb l'expressió

```
[P,X] = polynomial_ring(A, 'X')
```

Un cop creat P , si $f = X^r + a_1 X^{r-1} + \dots + a_{r-1} X + a_r \in P$, l'expressió

```
[B,x] = extension(A,f, 'x', 'B')
```

té el mateix valor que l'expressió $[B,x] = \text{extension}(A,C, 'x', 'B')$ d'abans.

A.5 Vectors i matrius

Sigui A un anell i n un número enter positiu. La funció $v = \text{vector}(A,n)$ crea el vector nul de longitud n amb coeficients de l'anell A . Si $a \in A$ i $0 \leq j < n$, l'expressió $v[j] = a$ assigna a a la component j -èsima de v , i si a és una llista d'elements de A , $\text{vector}(a)$ la transforma en un vector. Anàlogament, l'expressió $M = \text{matrix}(A,k,n)$ crea la matriu nul·la de k files i n columnes, i es pot assignar l'element $a \in A$ a la casella (i,j) amb l'expressió $M[i,j] = a$. Si $a_1, \dots, a_k$ són llistes de longitud n d'elements de A , l'expressió $\text{matrix}([a_1, \dots, a_k])$ les transforma en la corresponent matriu $k \times n$.

A.6 Utilitats per al sistema McEliece

Dels ingredients que entren en un sistema de McEliece, hem vist com es pot construir G a la secció 3. A continuació es mostra com podem construir les matrius P i S .

La funció `permutation_matrix(n)` crea una matriu de permutació d'ordre n escollida uniformement. En la implementació s'usen les funcions `ZZ()`, que crea l'anell dels números enters, i `permutation(n)`, que subministra una permutació aleatòria, uniformement distribuïda, del conjunt $N = [0, 1, \dots, n - 1]$.

```
def permutation_matrix(n):
    N = list(range(n))
    p = permutation(n)
    P = matrix(ZZ(), n, n)
    for j in range(n):
        P[j, p[j]] = 1
    return P
```

Adonem-nos que l'expressió `P[j, p[j]] = 1` posa un 1 a la fila j , columna $p[j]$.

La funció `rd_GL(n, F)` crea una matriu de $F(n)$ invertible escollida uniformement. Està definida de la manera següent:

```
def rd_GL(n, F=Zn(2)):
    a = rd_nonzero(F)
    A = matrix([a])
    for _ in range(2, n+1):
        A = rd_extend(A)
    return A
```

La part central és la funció `rd_extend(A)`, que crea, donada una matriu invertible $A \in F(k)$, una matriu invertible $B \in F(k + 1)$ que segueix la distribució uniforme si A té la mateixa propietat. Com que el valor inicial de A és clarament una selecció uniforme d'una matriu invertible de $F(1)$, la *iteració* produeix una matriu invertible de $F(n)$ distribuïda uniformement.

La definició de `rd_extend(A)` està inspirada en el senzill algorisme *recursiu* de D. Randall publicat a [42]. Primer se selecciona un vector no nul de longitud $k + 1$ i es posa r per indicar l'índex de la seva primera component no nul·la. La línia `rd_insert(A, r)` crea primer una matriu de $F(k, k + 1)$ inserint una columna aleatòria d'elements de F entre les columnes d'índexs $r - 1$ i r de A , després en fa una matriu invertible de $F(k + 1)$ afegint una primera fila de 0 amb un 1 en la posició d'índex r , i finalment multiplica el resultat per la matriu obtinguda de la matriu identitat I_{k+1} per substitució de la seva r -èsima fila pel vector v . Tot comptat, a la fi resulta la definició següent:

```
def rd_extend(A):
    k = ncols(A); F = K_(A)
    v = rd_nonzero_vector(F, k+1)
    r = 0
    for j in range(k+1):
        if v[j] != 0:
            r = j; break
    A = rd_insert(A, r)
    x = v[r]
```

```

for j in range(r+1,k+1):
    A[:,j] = A[:,j]+ A[:,r]*v[j]
A[:,r] = x*A[:,r]
return A

```

En lloc de donar aquí una explicació més detallada, que podeu trobar a [46], ens sembla més adient il·lustrar la construcció en el cas de matrius invertibles de $F(2)$. Inicialment tenim un element aleatori no nul $a \in F$ i v pot tenir una de les dues formes següents: $v = [b, y]$ o $v = [0, b]$ ($b, y \in F$, $b \neq 0$). En el primer cas, l'explicació que hem donat es concreta (posant $x \in F$) en l'expressió

$$\begin{pmatrix} 1 & 0 \\ x & a \end{pmatrix} \begin{pmatrix} b & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & y \\ xb & xy + a \end{pmatrix}.$$

En el segon cas, resulta l'expressió (posant $x \in F$)

$$\begin{pmatrix} 0 & 1 \\ a & x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & b \\ a & xb \end{pmatrix}.$$

La primera expressió dona totes les matrius invertibles de $F(2)$, la primera fila de les quals té un element no nul en la primera posició. El nombre de matrius així obtingudes és $m_0 = q^2(q-1)^2$. La segona expressió dona les matrius invertibles de $F(2)$, la primera fila de les quals comença amb 0. El nombre d'aquestes matrius és $m_1 = q(q-1)^2$, i és immediat comprovar que $m_0 + m_1 = (q^2 - 1)(q^2 - q)$, que és el cardinal del grup lineal $GL(2, F)$. Això prova que els elements d'aquest grup apareixen uniformement quan es generen pel procediment explicat.

A.7 Càlcul de matrius generadores

La funció `blow( $\tilde{H}$ ,  $F$ )` calcula H' i la funció `prune( $H'$ )` elimina les files que són combinació lineal de les anteriors, de manera que al final del procés tenim una matriu de control H .

```

n = 7; r = 2
K = Zn(2)
[F,a] = extension(K,[1,0,1,1], 'a', 'F')
R1 = [1,1,1,1,1,1,1]
R2 = [1,a,a**2,a**3,a**4,a**5,a**6]
HH = matrix(F,[R1,R2])
prune(blow(HH,F))
-->
[[1 1 1 1 1 1 1]
 [0 0 1 0 1 1 1]
 [0 1 0 1 1 1 0]
 [1 0 0 1 0 1 1]]

```

Això mostra que la dimensió del codi és $7 - 4 = 3$. Adonem-nos que les components de $1 \in F$ respecte de la base $\{1, a, a^2\}$ de F sobre K són $[1, 0, 0]$, de manera que la matriu $\text{blow}(\text{HH}, F)$, que és de tipus 6×7 , té dues files de zeros i per tant l'efecte de $\text{prune}(\text{blow}(\text{HH}, F))$ és simplement eliminar aquestes dues files.

A.8 Exemple de codi de Goppa

```
# Un codi de Goppa [19,12] sobre F5
F5 = Zn(5)
# Creació del cos F25, amb generador x tal que x**2-2=0
[F25,x] = extension(F5,[1,0,-2],'x','F25')
# Creació de l'aneïl de polinomis F25[T]
[A,T] = polynomial_ring(F25,'T')
# Conjunt dels elements no nuls del cos F25
# [1:] exclou l'element d'índex 0, que és 0>>F25
a = Set(F25)[1:]
# Creació d'un polinomi p
p = T**6 + T**3 + T + 1
# Llista d'elements de a que no són arrels de p
a = [t for t in a if evaluate(p,t)!=0]
n = len(a)
--> 19
# Creació del codi C de Goppa associat a p i a
C = Goppa(p,a)
# La matriu de control de C s'obté amb l'expressió H_(C)
H = blow(H_(C),F5)
n - rank(H)
--> 12
```

En l'exemple anterior, p té sis arrels $(2, 2, 3, 4, a + 2, 4a + 2)$ i, per tant, la longitud del codi és $25 - 1 - 5 = 19$. El rang de H resulta ser 7 i, per tant, $k = 12$.

A.9 Descodificació

L'exemple que segueix és una continuació de l'exemple anterior i il·lustra una descodificació amb PGZ.

```
# Generació d'un vector d'error aleatori de pes 3
e = rd_error_vector(Z5,n,3)
--> e = [0,1,0,0,0,3,0,4,0,0,0,0,0,0,0,0,0]
# Descodificació de e amb PGZ
PGZ(e,C)
--> PGZ: Error positions [1,5,7], error values [1,3,4]
      [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0] :: Vector[Z5]
```

A.10 Entorns Jupyter

Acabem aquesta secció veient un exemple del funcionament de Jupyter.⁶

⁶ <http://jupyter.org/>.

Referint-nos a la figura 2, la primera línia és un comentari que conté el títol del *notebook*. Amb la comanda de la segona línia, `from PyECC import *`, es carrega el paquet PyECC. En la definició de la funció `irr(q,m)`, `divisors` i `mu_moebius` són funcions de PyECC que calculen la llista ordenada de divisors de m i el valor $\mu(m//d)$ de la funció de Möbius per al quocient enter de m per d , quocient que en Python s'expressa $m//d$ (cal remarcar que el valor de l'expressió m/d és un número decimal). El resultat de `show(M)` és equivalent a la taula següent.

```
# Irr_q(t)
from PyECC import *

def irr(q,t):
    N = 0
    D = divisors(t)
    for d in D:
        N += mu_moebius(d)*q**(t//d)
    return N//t

M=[[irr(q,t) for t in range(1,8)] for q in [2,3,4,5,7,8,9]]

show(M)
```

FIGURA 2: Imatge de la primera cella d'un *notebook* de Jupyter que mostra la funció `irr(q,t)` de PyECC que calcula el nombre de polinomis irreductibles mònicos de grau t sobre F_q , així com les expressions per obtenir els valors de la taula 1.

1	2	3	4	5	6	7
2	1	2	3	6	9	18
3	3	8	18	48	116	312
4	6	20	60	204	670	2340
5	10	40	150	624	2580	11160
7	21	112	588	3360	19544	117648
8	28	168	1008	6552	43596	299592
9	36	240	1620	11808	88440	683280

TAULA 1: Valors de `irr(q,t)` per a $1 \leq t \leq 7$ i $q \leq 9$.

B Implementació d'un prototip de sistema de McEliece

Seguirem pas a pas un exemple molt senzill que hauria de ser suficient per il·lustrar els diversos passos del procediment.

```
# 0. Inici. Importem PyECC i definim Z2 amb nom 'K'
from PyECC import *
K = Zn(2, 'K')
```

```

# 1. Construïm F32 amb generador a
[F,a] = extension(K,get_irreducible_polynomial(K,5),'a','F')

# 2. Generem aleatòriament un polinomi mònic irreductible
#     de grau 3 de F[T]
p = get_irreducible_polynomial(F,3,'T')
show(p) -->
T**3+(a**4+a**3+a**2+a)*T**2+(a**4+a**3)*T+a**2+a :: F[T]

# 3. Creem el codi de Goppa de polinomi p**2 sobre
#     els elements no nuls de F (expressió X[1:])
#     Corregeix deg(p) = 3 errors
X = Set(F)
C = Goppa(p**2,X[1:])

# 4. Matrius de control/F i /K
HH = H_(C)
H1 = blow(HH,F)
show(shape(HH))
--> (6, 31)
show(shape(H1))
--> (30, 31)
show(rank(H1))
--> 15

# 5. Matriu generadora/K, G. Veiem que k = 16
G = transpose(kernel(H1))
show(shape(G))
--> (16, 31)

# 6. Matriu S de la clau privada; K_(G) és K, ja que C/K.
#     S és una matriu binària 16x16.
S=rd_GL(K_(G),nrows(G))
show(det(S))
--> 1

# 7. Matriu P (entera) de la clau privada. det(P) pot ser 1 o -1
P = permutation_matrix(ncols(G))
show(det(P))
--> 1

# 8. Clau pública (G1,t)
G1 = S*G*P
show(shape(G1))
--> (16, 31)
t = nrows(H_(C))/2
--> 3

```

```

# 9. Encriptació d'un vector aleatori u
u = rd_vector(F,nrows(G1))
--> [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1]
x = u*G1 -->
[0,0,0,0,1,1,1,1,1,0,0,0,0,1,0,0,1,0,0,0,0,1,1,0,1,0,0,1,0,1]
e = rd_error_vector(F,len(x),t) -->
[0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0]
x1 = x+e -->
[0,0,0,0,1,1,1,1,1,0,1,0,0,1,1,0,1,0,0,0,0,0,1,1,0,1,0,0,0,1]

# 10. Desencriptació. La inversa de P és la seva transposada
y = x1*transpose(P) -->
[0,0,1,1,1,0,1,1,0,0,0,1,0,0,1,1,0,0,1,0,1,1,1,1,0,0,0,0,1,0,0]
x2 = PGZ(y,C) --> # uSG
[0,0,0,1,1,0,1,1,0,0,0,1,0,0,1,1,0,0,1,0,0,1,1,1,0,1,0,0,1,0,0]
u1 = solve_linear_system(transpose(G),transpose(x2))
u1 = transpose(u1)
--> [1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0]
u1/S
--> [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1]
u
--> [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1]

```

Sigles

AKE	Authenticated Key Exchange ⁷
BMS	Berlekamp-Massey-Sugiyama decoding algorithm
CAKE	Code-based Algorithm for Key Encapsulation
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
HQC	Hamming Quasi-Cyclic Codes
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IND-CCA	Indistinguishability under Chosen Ciphertext Attack
IND-CPA	Indistinguishability under Chosen Plaintext Attack
INRIA	Institut National de Recherche en Informatique et en Automatique
ISIT	International Symposium on Information Theory
KEM	Key Encapsulation Mechanism
LDPC	Low-density Parity-check Codes
MDPC	Moderate-density Parity-Check Codes
NIST	National Institute of Standards and Technology
PGZ	Peterson-Gorenstein-Zierler decoding algorithm
RLCE	Random Linear Code Encryption
WCC	Workshop on Codes and Cryptography

⁷ Vegeu [30] per a molts altres acrònims relacionats.

Agraïments

La Jornada de Teoria de Nombres esmentada més amunt fou un important estímul per als autors, els quals es complauen a agrair la invitació dels organitzadors (Ana Río, Josep M. Miret i Jordi Guàrdia) i la benvolença dels participants a escoltar la seva conferència. Gràcies a Rafel Farré i Santiago Molina, coautors dels articles [25] i [35], respectivament, ja que la programació dels algorismes que s'hi tracten va representar un pas important en el desenvolupament de PyECC. El nostre agraïment també al revisor de l'article pels seus suggeriments, que han comportat una millora de la versió original.

Referències

- [1] ARAGON, N.; GABORIT, P.; HAUTEVILLE, A.; TILlich, J.-P. «Improvement of generic attacks on the rank syndrome decoding problem». 2017. <https://hal.archi-ves-ouvertes.fr/hal-01618464>.
- [2] AUGOT, D.; BATINA, L.; BERNSTEIN, D. J.; BOS, J.; BUCHMANN, J.; CASTRYCK, W.; DUNKELMAN, O.; GÜNEYSU, T.; GUERON, S.; HÜLSING, A.; LANGE, T.; MOHAMED, M. S. E.; RECHBERGER, C.; SCHWABE, P.; SENDRIER, N.; VERCAUTEREN, F.; YANG, B. Y. «Initial recommendations of long-term secure post-quantum systems». PQCRYPTO ICT-645622 - Horizon 2020, 2015. <https://pqcrypto.eu.org/docs/initial-recommendations.pdf>.
- [3] BARBIER, M.; BARRETO, P. S. L. M. «Key reduction of McEliece's cryptosystem using list decoding». A: KULESHOV, A.; BLINOVSKY, V. M.; EPHREMIDES, A. (ed.). *International Symposium of Information Theory (ISIT)*. Sant Petersburg: IEEE, 2011, 2657-2661.
- [4] BARRETO, P. S. L. M.; GUERON, S.; GÜNEYSU, T.; MISOCZKI, R.; PERSICHETTI, E.; SENDRIER, N.; TILlich, J.-P. «CAKE: Code-based algorithm for key encapsulation». A: *Cryptography and Coding*. Cham: Springer, 2017, 207-226. (Lecture Notes in Comput. Sci.; 10655)
- [5] 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.
- [6] BERNSTEIN, D. J. «Index of formal scientific papers». <https://cr.yp.to/papers.html>.
- [7] BERNSTEIN, D. J. «Introduction to post-quantum cryptography». A: *Post-Quantum Cryptography*. Berlín: Springer, 2009, 1-14.
- [8] BERNSTEIN, D. J. «Is the security of quantum cryptography guaranteed by the laws of physics?». 2017. <https://sidechannels.cr.yp.to/qkd/holographic-20160326.pdf>.
- [9] BERNSTEIN, D. J.; BIASSE, J.-F.; MOSCA, M. «A low-resource quantum factoring algorithm». A: *Post-Quantum Cryptography*. Cham: Springer, 2017, 330-346. (Lecture Notes in Comput. Sci.; 10346)

- [10] BERNSTEIN, D. J.; BUCHMANN, J.; DAHMEN, E. (ed). *Post-Quantum Cryptography*. Berlin: Springer, 2009.
- [11] BERNSTEIN, D. J.; LANGE, T. «Post-quantum cryptography». *Nature*, 549 (2017), 188–194.
- [12] BERNSTEIN, D. J.; LANGE, T.; PETERS, C. «Attacking and defending the McEliece cryptosystem». A: *Post-Quantum Cryptography*. Berlin: Springer, 2008, 31–46. (Lecture Notes in Comput. Sci.; 5299)
- [13] BERNSTEIN, D. J.; LANGE, T.; PETERS, C. «Wild McEliece incognito». A: *Post-Quantum Cryptography*. Heidelberg: Springer, 2011, 244–254. (Lecture Notes in Comput. Sci.; 7071)
- [14] BERNSTEIN, D. J.; YANG, B. Y. «Asymptotically faster quantum algorithms to solve multivariate quadratic equations». 2017. <https://cr.yp.to/papers/groverx1-20171215.pdf>.
- [15] BISWAS, B. «Implementational aspects of code-based cryptography». Tesi doctoral. École Polytechnique i INRIA, 2010.
- [16] CAMERON, P. J. «Notes on cryptography». <http://www.maths.qmul.ac.uk/~pjc/notes/crypt.pdf>.
- [17] CAMPBELL, E. T.; TERHAL, B. M.; VUILLOT, C. «The steep road towards robust and universal quantum computation». Preprint, 2016. <https://arxiv.org/abs/1612.07330>.
- [18] CHEN, L. [et al.] «Report on Post-Quantum Cryptography». NISTIR 8105. National Institute of Standards and Technology, U.S. Department of Commerce, 2016. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>.
- [19] CSRC (COMPUTER SECURITY RESOURCE CENTER). «Post-Quantum Cryptography 2018». <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>. [Primera conferència de normalització del PQC organitzada pel Centre de Recursos per a la Seguretat Informàtica - NIST]
- [20] DELFS, H.; KNEBL, H. *Introduction to Cryptography. Principles and Applications*. 2a ed. Berlin: Springer, 2007. (Information Security and Cryptography)
- [21] DENEUVILLE, J.-C.; GABORIT, P.; ZÉMOR, G. «Ouroboros: a simple, secure and efficient key exchange protocol based on coding theory». A: *Post-Quantum Cryptography*. Cham: Springer, 2017, 18–34. (Lecture Notes in Comput. Sci.; 10346)
- [22] DIFFIE, W.; HELLMAN, M. E. «New directions in cryptography». *IEEE Trans. Information Theory*, IT-22 (6) (1976), 644–654.
- [23] DINH, H.; MOORE, C.; RUSSELL, A. «McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks». A: *Advances in Cryptology—CRYPTO 2011*. Heidelberg: Springer, 2011, 761–779. (Lecture Notes in Comput. Sci.; 6841)
- [24] ENGELBERT, D.; OVERBECK, R.; SCHMIDT, A. «A summary of McEliece-type cryptosystems and their security». *J. Math. Cryptol.*, 1 (2) (2007), 151–199.

- [25] FARRÉ, R.; SAYOLS, N.; XAMBÓ-DESCAMPS, S. «On PGZ decoding of alternant codes». Preprint, 2017. <https://arxiv.org/abs/1704.05259>.
- [26] GABORIT, P. «Shorter keys for code-based cryptography». A: *Proceedings of Workshop on Codes and Cryptography*. França: WCC 2005, 2005, 81–90.
- [27] GABORIT, P.; RUATTA, O.; SCHREK, J. «On the complexity of the rank syndrome decoding problem». *IEEE Trans. Inform. Theory*, 62 (2) (2016), 1006–1019.
- [28] GOPPA, V. D. «A new class of linear correcting codes». *Problemy Peredači Informacii*, 6 (3) (1970), 24–30. [En rus]
- [29] KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. Boca Raton, FL: Chapman & Hall/CRC, 2008. (Chapman & Hall/CRC Cryptography and Network Security)
- [30] LEE, J.; PARK, C. S. «An efficient authenticated key exchange protocol with a tight security reduction». 2008. <https://eprint.iacr.org/2008/345.pdf>.
- [31] McELIECE, R. J. *The Theory of Information and Coding: A Mathematical Framework for Communication*. Mass.; Londres; Amsterdam: Addison-Wesley Publishing Co., Reading, 1977. (Encyclopedia of Mathematics and its Applications; 3)
- [32] McELIECE, R. J. «A public-key cryptosystem based on algebraic coding theory». *The Deep Space Network Progress Report* [Jet Propulsion Laboratory]. 42–44 (1978), NASA Code 310.10.67-11, 114–116.
- [33] MERKLE, R. C.; HELLMAN, M. E. «Hiding information and signatures in trapdoor knapsacks». *IEEE Trans. Information Theory*, IT-24 (5) (1978), 525–530.
- [34] MISOCZKI, R.; TILICH, J.-P.; SENDRIER, N.; BARRETO, P. S. L. M. «MDPC-McEliece: New McEliece variants from moderate density parity-check codes». 2012. <https://eprint.iacr.org/2012/409.pdf>.
- [35] MOLINA, S.; SAYOLS, N.; XAMBÓ-DESCAMPS, S. «A bootstrap for the number of $\mathbb{F}_{q^r}$ -rational points on a curve over $\mathbb{F}_q$ ». Preprint, 2017. <https://arxiv.org/abs/1704.04661>.
- [36] NIEBUHR, R. «Attacking and defending code-based cryptosystems». Tesi doctoral, Fachbereich Informatik der Technischen Universität Darmstadt, 2012.
- [37] NIEDERREITER, H. «Knapsack-type cryptosystems and algebraic coding theory». *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, 15 (2) (1986), 159–166.
- [38] OVERBECK, R.; SENDRIER, N. «Code-based cryptography». A: *Post-Quantum Cryptography*. Berlín: Springer, 2009, 95–145.
- [39] PATTERSON, N. J. «The algebraic decoding of Goppa codes». *IEEE Trans. Information Theory*, IT-21 (1975), 203–207.

- [40] PERSICHETTI, E. «Improving the efficiency of code-based cryptography». Tesi doctoral. Nova Zelanda: University of Auckland, Department of Mathematics, 2012.
- [41] *Post-quantum cryptography*. <https://pqcrypto.org/>.
- [42] RANDALL, D. «Efficient generation of random nonsingular matrices». Informe tècnic núm. UCB/CSD-91-658. Berkeley (EUA): University of California at Berkeley, 1991.
- [43] REPKA, M.; ZAJAC, P. «Overview of the McEliece cryptosystem and its security». *Tatra Mt. Math. Publ.*, 60 (2014), 57–83.
- [44] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. «A method for obtaining digital signatures and public-key cryptosystems». *Comm. ACM*, 21 (2) (1978), 120–126.
- [45] RUÉ, J.; XAMBÓ, S. «Introducció matemàtica a la computació quàntica». *Butlletí de la Societat Catalana de Matemàtiques*, 28 (2) (2013), 183–231.
- [46] SAYOLS, N.; XAMBÓ-DESCAMPS, S. «PyECC: A Python package for the construction, coding and decoding of error-correcting codes». 2015–2018. <https://mat-web.upc.edu/people/sebastia.xambo/PyECC.html>.
- [47] SAYOLS, N.; XAMBÓ-DESCAMPS, S. «Alternant codes and the McEliece cryptosystem». Conferència pronunciada a la Jornada de Teoria de Nombres (Universitat de Lleida, 2017). <https://mat-web.upc.edu/people/sebastia.xambo/PyECC/s-CryptoLleida-7-10-2017.pdf>.
- [48] SENDRIER, N. «Efficient generation of binary words of given weight». A: *Proceedings of the 5th IMA Conference on Cryptography and Coding*. Londres: Springer-Verlag, 1995, 184–187.
- [49] SENDRIER, N. «Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs». Mémoire d'habilitation à diriger des recherches. París: Université Pierre et Marie Curie, Paris 6; Rocquencourt: Institut National de Recherche en Informatique et Automatique, 2002.
- [50] SENDRIER, N. «On the use of structured codes in code based cryptography». A: *Coding Theory and Cryptography III. Contactforum*. Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten, 2009, 59–68.
- [51] SHOR, P. W. «Algorithms for quantum computation: discrete logarithms and factoring». A: *35th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, 124–134. [Per obtenir una versió revisada i ampliada d'aquest article, vegeu: «Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer». *SIAM J. Comput.*, 26 (5) (1997), 1484–1509]
- [52] TILICH, J.-P. «The decoding failure probability of MDPC codes». Preprint, 2018. <https://arxiv.org/abs/1801.04668>.
- [53] WANG, J. «Quantum resistant random linear code based public key encryption scheme RLCE». A: *Proceedings 2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2016, 2519–2523.

- [54] WANG, J. «Decoding generalized Reed-Solomon codes and its application to RLCE encryption schemes». Preprint, 2017. <https://arxiv.org/abs/1702.07737>.
- [55] «Quantum cryptography». A: Wikipedia. https://en.wikipedia.org/wiki/Quantum_cryptography.
- [56] XAMBÓ-DESCAMPS, S. *Block Error-correcting Codes. A Computational Primer*. Berlín: Springer-Verlag, 2003. (Universitext)

NARCÍS SAYOLS
DEPARTAMENT ESAII
UPC, EDIFICI K2M
C. JORDI GIRONA, 1-3
08034 BARCELONA, SPAIN
narcis.sayols@upc.edu

SEBASTIÀ XAMBÓ
DEPARTAMENT DE MATEMÀTIQUES
UPC, EDIFICI OMEGA
C. JORDI GIRONA, 1-3
08034 BARCELONA, SPAIN
sebastia.xambo@upc.edu

English summaries

Carles Barril, Sílvia Cuadrado and Jordi Ripoll

Mathematical models in population dynamics

Population dynamics studies the evolution of size and composition of populations. In this article we present a compilation of the main mathematical models describing the dynamics of biological populations. We start with a historical introduction to the subject showing different problems in ecology, demography and epidemiology, as well as the tools and mathematical techniques used. Then we describe a new formulation in terms of delay equations that establishes a thorough general framework for the mathematical modeling of population dynamics.

Keywords: mathematical biology, structured populations, delay equations, partial differential equations.

MSC2010 Subject Classification: 92D25, 35Q92, 47N20.

Agustí Reventós

Gaspard Monge

This article seeks to pay tribute, 200 years after his death, to Monge's work in the field of differential geometry of curves and surfaces. After a brief reminder of his biography, we focus on his work on evolutes of curves in space and especially on the origin of the lines of curvature, in an article dedicated to transport of land. The Feuille xv of his famous *Feuilles d'analyse* is analyzed in detail and a brief comment is made on the rest of his works in differential geometry. We attach a note, by Josep Lluís Solé, about one of Monge's friends and his biographer: François Arago.

Keywords: Monge, curves, surfaces, evolutes, lines of curvature.

MSC2010 Subject Classification: 53A04, 53A05, 01A50.

Narcís Sayols and Sebastià Xambó

Error-correcting codes and post-quantum cryptography

The forty-year old McEliece public-key crypto-system is revisited with the help of recently developed resources: an improved Peterson-Gorenstein-Zierler decoder for alternant error-correcting codes; a symbolic computation system and a package of functional utilities for the computations involved in defining, coding and decoding error-correcting codes, fully programmed in Python; and a web page with free-access to the materials generated by the project. The main interest of the McEliece system stems from it being a serious candidate for a post-quantum cryptography standard.

Keywords: post-quantum cryptography, alternant codes, symbolic computation, free software.

MSC2010 Subject Classification: 11T71, 68-04, 68W30, 94A60.

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

Julia Cufí (editor en cap)
Departament de Matemàtiques
Universitat Autònoma de Barcelona
jcufi@mat.uab.cat

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

Antoni Guillamon
Departament de Matemàtiques
Universitat Politècnica de Catalunya
antoni.guillamon@upc.edu

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

Agustí Reventós
Departament de Matemàtiques
Universitat Autònoma de Barcelona
agusti@mat.uab.cat

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



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:

PRESIDENT: Xavier Jarque i Ribera

VICEPRESIDENT: Enric Ventura i Capell

ADJUNTA DE LA VICEPRESIDÈNCIA: Iolanda Guevara i Casanova

SECRETARI: Albert Ruiz i Cirera

TRESORERA: Natàlia Castellana i Vila

VOCALS: Albert Avinyó i Andrés, Marta Berini i López-Lara, Abraham de la Fuente Pérez, Núria Fagella i Rabionet, Josep Grané i Manlleu, Carles Romero i Chesa, Manel Udina i Abelló

DELEGAT 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 _____

Julia Cufí

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Editora adjunta _____

Rosa Camps

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Comitè editorial _____

Bartomeu Coll

Dep. de Matemàtiques i Informàtica

Universitat de les Illes Balears

Marc Noy

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Núria Fagella

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Francesc Planas

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Armengol Gasull

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Agustí Reventós

Departament de Matemàtiques

Universitat Autònoma de Barcelona

Antoni Guillamon

Departament de Matemàtiques

Universitat Politècnica de Catalunya

Joan Saldaña

Dep. d'Informàtica, Mat. Aplicada i Estadística

Universitat de Girona

Gábor Lugosi

ICREA i Departament d'Economia

Universitat Pompeu Fabra

Marta Sanz-Solé

Dep. de Matemàtiques i Informàtica

Universitat de Barcelona

Societat Catalana de Matemàtiques

Carrer del Carme, 47 - 08001 Barcelona

tel. 933 248 583 - fax 932 701 180

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