BUTLLETÍ

DE LA SOCIETAT CATALANA DE MATEMÀTIQUES
Institut d'Estudis Catalans

índex

Volum 31 • Número 1 • Any 2016

Institut d'Estudis Catalans

BUTLLETÍ

DE LA SOCIETAT CATALANA
DE MATEMÀTIQUES
Institut d'Estudis Catalans

Volum 31 • Número 1 • Juny 2016

BARCELONA
2016

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 Limpergraf, SL

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

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016

Índex

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 5–29. DOI: 10.2436/20.2002.01.64

L'obra matemàtica d'Evarist Giné

Vladimir Koltchinskii, Richard Nickl, Sara van de Geer i Jon A. Wellner

Resum: En aquest article es fa un repàs de les contribucions de l'Evarist Giné a la teoria moderna de la probabilitat i de l'estadística matemàtica en un context infinitodimensional. Les seccions corresponen a les àrees en les quals va tenir una participació més significativa: probabilitat en espais de Banach, processos empírics, el bootstrap, U-estadístics i U-processos, i estadística matemàtica. Es fa èmfasi a l'impuls que la seva obra ha donat a la teoria actual de la probabilitat, l'estadística matemàtica i també a l'aprenentatge automàtic (*machine learning*). A més conté un resum biogràfic i la llista completa de les seves publicacions. Ha esta escrit en ocasió de la seva mort.

Paraules clau: probabilitats en espais de Banach, teorema del límit central, processos empírics, bootstrap, U-estadístics, estimació de densitats.

Classificació MSC2010: 60B12, 60G15, 60E15, 62F40, 62G07.

1 Introducció

Evarist Giné, o bé Evarist Giné-Masdéu (1944–2015), va ser un contribuïdor influent, brillant i prolífic a la teoria moderna de la probabilitat i de l'estadística matemàtica, que es va centrar en els problemes que sorgeixen en un context infinitodimensional. La seva obra ha tingut un impacte important en la teoria moderna de la probabilitat, en l'estadística matemàtica i, recentment, també en l'aprenentatge automàtic. Aquest article és un intent de descriure les aportacions matemàtiques més rellevants d'Evarist Giné i l'hem dividit en diverses seccions cadascuna de les quals es dedica a una àrea de treball significativa: *probabilitat en espais de Banach*, *processos empírics*, *el bootstrap*, *U-estadístics i U-processos*, i *estadística matemàtica*. Al final de l'article es pot trobar un resum biogràfic i una llista de les publicacions d'Evarist Giné, incloent-hi els seus quatre llibres.

Un aspecte que dóna unitat a la major part de l'obra d'Evarist Giné és la combinació magistral de tècniques d'anàlisi real i d'anàlisi funcional amb idees

La traducció d'aquest article de l'original en anglès ha estat feta pels editors del *Butlletí* i revisada per Frederic Utzet.

fonamentals de la teoria de la probabilitat: Evarist Giné tenia un coneixement profund de les tècniques analítiques, les quals aplicava sovint amb una simplicitat molt enginyosa als problemes de probabilitat. Al mateix temps era un probabilista versàtil i de formació clàssica que dominava diverses àrees centrals, des de teoremes límit i desigualtats per a sumes de variables aleatòries independents fins a processos gaussians i l'argumentació amb martingales.

2 Els pilars bàsics de l'obra d'Evarist Giné

2.1 La tesi doctoral

Evarist Giné va escriure la seva tesi doctoral sota la direcció de Richard M. Dudley al Massachusetts Institute of Technology (MIT). De la tesi en van sortir cinc articles notables: dos dels quals [A1, A5] van ser publicats als *Annals of Probability* i eren el resultat de la feina feta com a estudiant de postgrau. L'article [A1] el va conduir cap a l'àrea que descrivim a la secció següent, i l'article [A5] en col·laboració amb R. Klein establia propietats en el límit de la variació quadràtica de processos amb increments gaussians, generalitzant resultats de Dudley [9] per al moviment brownià.

Però el tema principal de la tesi va ser la construcció de tests estadístics computables per a observacions que prenen valors en una varietat de Riemann compacta, que va aparèixer als *Annals of Statistics* l'any 1975 (vegeu [A4]). L'editor que es va encarregar d'aquest article fonamental va ser Lucien Le Cam, el qual va considerar que tenia un nivell matemàtic tan alt que l'únic revisor amb qui va poder pensar va ser Richard Dudley! Aquest article, de fet, va obrir l'àrea d'estudi dels tests de Sobolev, que ha estat important des d'aleshores en el camp de l'estadística direccional, i va requerir el desenvolupament d'alguns resultats matemàtics d'interès independent, com ara una prova del fet que una bola de Sobolev definida sobre qualsevol varietat de Riemann compacta satisfà el teorema del límit central empíric (*i. e.*, és una classe de P-Donsker —vegeu la subsecció 2.3 per a més informació—). En aquesta època la maquinària dels processos empírics generals no estava disponible encara, però Evarist Giné se'n va sortir amb una reducció intel·ligent del problema al teorema del límit central a $C(S)$ (l'espai de les funcions contínues sobre un espai mètric compacte S) fent servir la teoria de la dualitat per als espais de Sobolev. La tesi també requeria la prova d'algunes identitats en anàlisi geomètrica les quals van ser publicades en un article separat [A3] i van portar Evarist Giné a publicar un article genuïnament aplicat [A2], que va aparèixer al *Journal of Geology*. Es pot dir, sens dubte, que aquesta tesi va ser absolutament excepcional pel seu abast i per la seva profunditat.

2.2 Probabilitat en espais de Banach

Partint de l'article [A1] que era part de la seva tesi, Evarist Giné es va endinsar en un dels problemes candents de la teoria de la probabilitat dels anys setanta:

la formulació dels teoremes clàssics del límit per a sumes $\sum_{i=1}^n X_i$ de variables aleatòries centrades, independents i idènticament distribuïdes X_i que prenen valors en un espai de Banach B de dimensió infinita. Per exemple, el *teorema del límit central* (TLC): per a una variable aleatòria gaussiana adequada G que pren valors a B hom vol provar el teorema de límit distribucional

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} X_i \to^d G \quad \text{quan} \quad n \to \infty.$$

Mentre que per a espais de dimensió finita una condició necessària i suficient per a la validesa del TLC és que $E\|X_1\|^2$ sigui finita, en espais de dimensió infinita no és així i les propietats geomètriques de l'espai de Banach entren en joc d'una manera essencial. Les tècniques matemàtiques desenvolupades en aquesta àrea durant aquest període van ser fonamentals per a molts camps de les matemàtiques actuals, com ara l'anàlisi funcional geomètrica, la concentració de mesures, l'aprenentatge estadístic (*statistical learning*) o l'estadística matemàtica.

Les contribucions d'Evarist Giné en aquesta àrea van ser substancials; van donar lloc a uns vint articles i van culminar en el seu primer llibre, *The Central Limit Theorem for Real and Banach Valued Random Variables*, publicat el 1980. El seu treball en aquest camp, que el va dur a terme en col·laboració amb diversos coautors, entre els quals Alejandro de Acosta, Aloisio Araujo i Joel Zinn, inclou la fórmula de Lévy-Khintchine per a lleis infinitament divisibles en espais de Banach i caracteritzacions del domini d'atracció d'una llei normal en espais de Banach [A9, A12], així com teoremes de convergència de moments en el TLC en espais de Banach [A13] i el TLC per a alguns espais de funcions específics [A7, A15, A20, A27, A33].

Una aplicació elegant d'aquests mètodes a la teoria de *conjunts aleatoris* (vegeu [17, 25]) apareix a l'article [A31] escrit en col·laboració amb Marjorie Hahn i Joel Zinn: si B és un espai de Banach separable, podem considerar el conjunt $K(B)$ de tots els subconjunts de B compactes i no buits, el qual és un espai mètric complet respecte de la distància de Hausdorff δ. A més, la suma de Minkowski és una operació ben definida a $K(B)$ i podem fins i tot definir una norma posant $\|A\| = \sup\{\|a\|_B : a \in A\}$. Un *conjunt compacte aleatori* és qualsevol variable aleatòria boreliana X que pren valors a $K(B)$, i la seva esperança EX es pot definir en el sentit de Bochner. Fent servir una reducció molt intel·ligent al TLC per a $C(S)$ amb una elecció adequada de S, a l'article [A31] es prova el teorema del límit central per a conjunts aleatoris: per exemple, si $B = \mathbb{R}^d$, $E\|X\| < \infty$ i si els X_i són conjunts compactes aleatoris independents i idènticament distribuïts, llavors

$$\sqrt{n}\delta\left(\frac{1}{n}\sum_{i=1}^{n} X_i, EX\right)$$

convergeix en distribució cap a una determinada norma d'un procés gaussià. Així mateix es prova un resultat per al cas que B té dimensió infinita.

2.3 Processos empírics

Les tècniques per a l'estudi de la probabilitat en espais de Banach es van desenvolupar principalment per a espais separables, la qual cosa és molt raonable perquè les distribucions de probabilitat en espais mètrics complets per força tenen la seva massa concentrada essencialment en conjunts compactes (*i. e.* són mesures de Radon). Al mateix temps, un problema clau que era obert al final dels anys setanta era el teorema del límit central per a *processos empírics* indexats per classes abstractes $\mathcal{F}$ de funcions $f: S \to \mathbb{R}$, on S és un espai mostral arbitrari en el qual variables aleatòries independents i idènticament distribuïdes $X_1, \ldots, X_n$ amb llei P prenen els seus valors.

La *mesura empírica* $P_n := n^{-1} \sum_{j=1}^n \delta_{X_j}$ és un estimador natural de la llei desconeguda P i és important saber com de pròximes estan les mitjanes mostrals $P_n f = n^{-1} \sum_{j=1}^n f(X_j)$ de les mitjanes reals $Pf = Ef(X)$, uniformement sobre una classe gran $\mathcal{F}$ de funcions f. Al final dels anys seixanta i principi dels setanta, Vapnik i Chervonenkis, motivats per aplicacions a la teoria estadística del reconeixement de patrons (una part del que avui en dia es coneix per *teoria de l'aprenentatge estadístic*), van obtenir condicions necessàries i suficients, sorprenents per a la llei uniforme dels grans números per a mesures empíriques (el problema de Glivenko-Cantelli)

$$\sup_{f \in \mathcal{F}} |P_n f - Pf| \to 0 \quad \text{quan} \quad n \to \infty \ \text{ q.s.}$$

en el cas que $\mathcal{F} = \{I_C : C \in C\}$, on C és una classe de subconjunts mesurables de S. Més tard van estendre aquests resultats a classes de funcions uniformement acotades [36]. Tanmateix, l'extensió del famós «teorema de Donsker», és a dir, el teorema del límit central per a processos empírics clàssics sobre la recta, al mateix context general es mantenia oberta. En notació actual els processos empírics generals s'escriuen

$$f \mapsto \nu_n(f) = n^{1/2}(P_n f - Pf) = \frac{1}{\sqrt{n}} \sum_{i=1}^n (f(X_i) - Ef(X)), \quad f \in \mathcal{F},$$

i la qüestió és saber si ν_n convergeix cap a un procés gaussià $(G_P(f) : f \in \mathcal{F})$ uniformement en $f \in \mathcal{F}$. Tot i que a primera vista sembla que es tracta d'un problema molt abstracte, les tècniques que es necessiten per resoldre'l han tingut un impacte molt fort en la teoria actual de l'estadística i en la teoria de l'aprenentatge. En un article fonamental [10], Dudley va estudiar aquest tipus de teoremes límit, i va mostrar que fins i tot en el cas més senzill en el qual $\mathcal{F}$ està formada per indicadors d'una classe C de subconjunts de l'espai euclidià, es requereixen tècniques molt diferents de les que s'utilitzen en probabilitats en espais de Banach. Això és degut en part al fet que els processos empírics generalment *no* es concentren en algun espai de Banach de funcions *contínues* (per a alguna mètrica) sobre $\mathcal{F}$ —només cal pensar, per exemple, en la funció de distribució empírica $\mathcal{F} = \{1_{(-\infty,t]} : t \in \mathbb{R}^d\}$— i que, com a conseqüència, l'espai de Banach $\ell^\infty(\mathcal{F})$ de les funcions acotades sobre $\mathcal{F}$ en el

qual les ν_n prenen valors no és possible. Dudley [10] va estudiar el teorema del límit central per a processos empírics indexats per una classe de conjunts C i la va anomenar una classe de Donsker per a la llei P de $X_1, \ldots, X_n$ si el TLC era cert per a la classe. Va establir condicions suficients per a la propietat de Donsker en termes de l'entropia mètrica amb *bracketing* de C i va provar que les classes de conjunts de Vapnik-Chervonenkis (una noció que també va introduir Dudley) eren classes de Donsker per a qualsevol llei P que compleixi només unes condicions de mesurabilitat adequades.

Després de la contribució decisiva de Dudley, V. Koltchinskii [18] va donar un conjunt molt útil de condicions suficients per a la validesa del TLC per a processos empírics en termes d'entropies aleatòries de classes de funcions i D. Pollard [31] va fer el mateix en termes de les entropies uniformes. Le Cam [19] va obtenir condicions suficients per al TLC en classes de conjunts en termes d'entropies aleatòries.

Aquestes condicions eren d'un tipus semblant a les que van donar Vapnik i Chervonenkis per a les lleis dels grans números. Les proves d'aquests resultats es basaven en el que avui s'anomenen desigualtats de simetrització per a les probabilitats de les cues. Un argument de condicionament permetia reduir les cotes per a les normes del suprem dels processos empírics a cotes per a un procés subgaussià (condicionadament a $X_1, \ldots, X_n$) del tipus següent: $\mathcal{F} \ni f \mapsto n^{-1} \sum_{j=1}^{n} \varepsilon_j f(X_j)$, on les $\{\varepsilon_j\}$ són variables aleatòries de Rademacher independents i idènticament distribuïdes i independents de les $\{X_j\}$. Aquest procés subgaussià (que actualment s'anomena procés de Rademacher) estava controlat per les entropies de conjunts aleatoris $\{(f(X_1), \ldots, f(X_n)) : f \in \mathcal{F}\} \subset \mathbb{R}^n$.

L'entrada d'Evarist Giné a l'escenari dels processos empírics no podia haver estat més impressionant: va ser a través d'un article de setanta pàgines [A34] publicat per invitació dels *Annals of Probability* el 1984 i escrit conjuntament amb Joel Zinn. En aquest article no només van provar resultats molt definitius per al TLC per a processos empírics, sinó que també van introduir tècniques noves i potents en aquesta àrea i van desenvolupar fins a la perfecció les tècniques fetes servir anteriorment. En particular, el mètode de simetrització utilitzat per Koltchinskii [18], Pollard [31] i Le Cam [19] va aconseguir la seva versió definitiva gràcies a les dues magnífiques desigualtats de simetrització de Giné-Zinn que es fan servir des d'aleshores, i la reducció de l'acotació del procés empíric a l'acotació del procés de Rademacher va ser estudiada en tota la seva extensió. A més a més, aquesta tècnica la van combinar amb altres eines de la teoria de probabilitats en espais de Banach, com ara la desigualtat del multiplicador deguda a Pisier, i l'article va establir connexions entre la teoria emergent dels processos empírics i un cos extens de literatura sobre probabilitats en espais de Banach. La idea de la simetrització gaussiana o bé de Rademacher via la desigualtat del multiplicador de Pisier va tenir un paper important en el treball posterior de Giné, també en col·laboració amb Zinn, sobre el *bootstrap* per a processos empírics (vegeu la subsecció 2.4).

Resultats específics notables de l'article de Giné i Zinn del 1984 contenen les versions finals sobre les condicions d'entropia aleatòria per al teorema

del límit central per a processos empírics, la demostració de la necessitat d'aquestes condicions per a classes de conjunts (la necessitat de les condicions en termes dels números *shattering* de Vapnik-Chervonenkis va ser provada més tard per Talagrand) i l'extensió de la condició necessària i suficient de Vapnik-Chervonenkis per a la llei dels grans números (teorema de Glivenko-Cantelli) en el cas de classes de funcions no acotades.

Un altre resultat profund i bonic que Evarist Giné va obtenir en el camp dels processos empírics és la caracterització gaussiana de les classes de Donsker uniformes. Una altra vegada, en un article publicat amb Joel Zinn als *Annals of Probability* [A56], va posar la qüestió: quan és que el TLC per a un procés empíric val uniformement respecte de la distribució P de les X_i?, més precisament, si β és una mètrica per a la convergència feble a $\ell^\infty(\mathcal{F})$ i G el procés gaussià límit, quan és cert que

$$\sup_P \beta(\nu_n^P, G_P) \to 0 \quad \text{quan} \quad n \to \infty,$$

on el suprem es pren sobre totes les mesures de probabilitat a P? Un resultat d'aquest tipus té una importància clau per a la interpretació estadística del TLC, atès que en les aplicacions típiques es fa servir per a deduir propietats desconegudes de P i, per tant, no hauria de ser necessari cap coneixement *a priori* de P per a la seva validesa. Essencialment és una pregunta sobre l'estructura de la classe $\mathcal{F}$, i es diu que $\mathcal{F}$ és una classe de Donsker uniforme si el límit anterior es compleix. El resultat sorprenent de [A56] és que una condició necessària i suficient per a la propietat de Donsker uniforme és que el límit G_P sigui *pregaussià* uniforme en P (i això significa que la continuïtat mostral del procés gaussià G_P respecte del seu argument $f \in \mathcal{F}$ per a la mètrica de la covariància intrínseca sigui uniforme en P). En conseqüència, el fet que una classe $\mathcal{F}$ sigui una classe de Donsker uniforme és un problema que es pot decidir completament en termes de propietats de processos gaussians, en contrast notable amb el buit que d'altra banda hi ha entre la propietat de Donsker i les propietats de processos pregaussians. Si tal com sembla un dels objectius principals de la feina d'Evarist Giné en la teoria dels processos empírics era establir connexions importants entre els processos empírics i els (sub)gaussians, el resultat que hem comentat es pot considerar com un punt culminant del seu programa.

2.4 El *bootstrap*

Una idea fonamental en estadística, deguda a Efron [12], és el mètode de repetició del mostreig conegut per *bootstrap*. Es pot fer servir per a inferències i conjunts de confiança en situacions en les quals les distribucions límit existeixen però no són accessibles (perquè són complicades o bé depenen de paràmetres desconeguts). Això es pot il·lustrar en el cas que $X_1, \ldots, X_n$ són variables aleatòries independents i idènticament distribuïdes de llei P amb mitjana μ. Llavors podem fer una extracció a l'atzar dels valors mostrals

per tal de crear una mostra *bootstrap*: siguin X_{ni}^b, $i = 1, \ldots, n$, extraccions independents i idènticament distribuïdes de la variable aleatòria X_n^b amb llei $\mathbb{P}_n(X_n^b = X_i) = 1/n$ per a $i = 1, \ldots, n$. Si $\bar{X}_n = \frac{1}{n}\sum_{i=1}^n$ és la mitjana mostral i $\bar{X}_n^b = \frac{1}{n}\sum_{i=1}^n X_{ni}^b$ és la mitjana dels valors remostrejats, llavors la idea és que la distribució de $\bar{X}_n^b - \bar{X}_n$ (coneguda, donades les X_i) és independent de la distribució de $\bar{X}_n - \mu$ (desconeguda). Per tant, a l'hora de calcular quantils per a l'última distribució, podem recórrer a calcular (aproximadament) quantils per a la primera.

El fet que el que acabem de dir sigui correcte en moltes situacions està lligat bàsicament al teorema del límit central, i Evarist Giné (juntament amb Joel Zinn) va fer diverses contribucions substancials en aquest camp, entre les quals [A47], on es prova la necessitat de les condicions suficients trobades per Bickel i Freedman [3] i es dóna un TLC bootstrap general per a processos empírics, que de fet resol completament la qüestió de la «consistència» del bootstrap (no paramètric). El resultat principal publicat l'any 1990 als *Annals of Probability* [A52] diu que, per al procés empíric bootstrap ν_n^b,

$$\nu_n^b \to^d G_P \text{ (en probabilitat) si i només si } \nu_n \to^d G_P.$$

L'article de l'any 1990 és un cúmul de tècniques sobre la teoria de processos empírics i sobre la teoria de la probabilitat en espais de Banach en diversos aspectes, com ara: (a) proporcionar un altre ús de la desigualtat del multiplicador de Pisier, que tenia un paper important amb els multiplicadors gaussians en el seu article de l'any 1984, ara amb multiplicadors (simetritzats) de Poisson després d'aplicar poissonització i simetrització als pesos multinomials del bootstrap d'Efron; (b) connectar els resultats sorprenents de Ledoux i Talagrand [20, 21] sobre multiplicadors i multiplicadors condicionats del TLC en espais de Banach amb un conjunt important de qüestions estadístiques.

Evarist Giné, en col·laboració amb diversos coautors (especialment el seu alumne Miguel Arcones), també va considerar altres problemes en relació amb els mètodes de remostreig amb bootstrap. Arcones i Giné [A46] proven que el bootstrap de la mitjana mostral de variables aleatòries independents i idènticament distribuïdes amb variància finita «funciona» si tant la mida de la mostra bootstrap m_n com la mida de la mostra original tendeixen a infinit. A [A53] estudien diversos tests de bootstrap de simetria, i a [A57] mostren com es pot fer bootstrap de U- i V-estadístics. La qüestió important de fer bootstrap de M-estimadors i altres funcionals estadístics regulars va ser considerada a [A58]. Tot aquest conjunt de línies de recerca i de problemes va culminar a les notes del curs que Evarist Giné va impartir a St. Flour sobre teoria asimptòtica per al remostreig amb bootstrap. Aquestes notes continuen essent una referència important i una pedra angular per a la recerca actual [L2].

2.5 U-estadístics i U-processos

La noció de U-estadístic és una extensió natural d'un dels objectes més clàssics de la probabilitat, la suma de variables aleatòries independents. Donada una

successió de variables aleatòries independents i idènticament distribuïdes $X_1, \ldots, X_n, \ldots$ en un espai mesurable S i una funció mesurable $h\colon S \times \cdots \times S \mapsto \mathbb{R}$ (un nucli), el *U-estadístic d'ordre k* es defineix com

$$U_n(h) := \frac{(n-k)!}{n!} \sum_{i_1,\ldots,i_k} h(X_{i_1}, \ldots, X_{i_k})$$

amb la suma estesa a tots els $1 \le i_1, \ldots, i_k \le n$ tals que $i_l \neq i_{l'}$, $l \neq l'$.

Aquesta noció té el seu origen en el treballs de Halmos [13] sobre estimació no esbiaixada i de von Mises [35] sobre desenvolupaments de funcionals estadístics regulars a finals dels quaranta. Els U-estadístics van ser introduïts formalment i estudiats per Hoeffding l'any 1948. Evarist Giné es va interessar en la teoria asimptòtica dels U-estadístics a l'inici dels anys noranta, quan aquesta teoria ja estava relativament ben desenvolupada, tant en el cas de U-estadístics basats en observacions independents i idènticament distribuïdes com en casos més generals. A més, Nolan i Pollard [29, 30] van iniciar l'estudi dels *U-processos* (processos empírics amb estructura de U-estadístics indexats pel seus nuclis). Tanmateix, a l'inici dels noranta, molts d'aquests resultats no havien assolit el mateix progrés que els teoremes límit clàssics per a sumes de variables aleatòries independents i un nombre important de problemes estimulants i difícils estaven oberts. Molts d'aquests problemes van ser resolts al llarg dels anys noranta per Evarist Giné en una sèrie d'articles escrits amb diversos coautors, entre els quals Joel Zinn, Miguel Arcones, Stanislaw Kwapień i Rafal Latała. Els resultats obtinguts inclouen lleis del tipus de Marcinkiewicz dels grans números per a U-estadístics (Giné-Zinn [A60]) i la necessitat que el segon moment sigui finit i el nucli degenerat per a la validesa del TLC per a U-estadístics (Giné-Zinn [A66]). També van obtenir resultats notables sobre el teorema del límit central per a U-processos indexats per classes de funcions de Vapnik-Chervonenkis (Arcones-Giné [A65]) i aplicacions sorprenents d'aquests resultats a l'estudi asimptòtic dels M-estimadors basat en U-estadístics; en particular una demostració molt bonica de la normalitat asimptòtica de la mediana simplicial (Arcones, Chen i Giné [A64]).

Els treballs anteriors depenen d'eines tècniques noves i potents, com ara la desigualtat de Hoffmann-Jorgenssen per a U-processos (Giné-Zinn [A60]) i desigualtats de desacoblament (*decoupling*) degudes a de la Peña [5] i de la Peña i Montgomery-Smith [6, 7]. El mètode del desacoblament va ser especialment important i va donar nom al llibre *Decoupling*, escrit l'any 1999 per Giné i de la Peña, que continua essent la referència més important sobre la teoria moderna dels U-estadístics [L3]. Tot i així un dels resultats més espectaculars d'aquesta teoria es va obtenir després de la publicació d'aquest llibre. En diversos articles escrits a finals dels noranta, Evarist Giné i els seus col·laboradors van intentar trobar una condició necessària i suficient per a llei dels logaritmes iterats (LLI) per a U-estadístics degenerats, un problema que va resultar extremament difícil. El fet que la finitud del segon moment del nucli era suficient per a la LLI era conegut des de finals dels vuitanta [8]. Giné i Zhang [A71] van mostrar que hi

ha nuclis degenerats amb segon moment infinit per als quals val la LLI. Van donar condicions suficients sobre el nucli que no implicaven la finitud del segon moment, però aquestes condicions encara no eren necessàries. Aquest problema desafiador va ser resolt per a U-estadístics de segon ordre en un article notable de Giné, Kwapień, Latała i Zinn [A84] en el qual van provar el resultat següent. Suposem que X, Y, X_1, $X_2, \ldots$ són variables aleatòries independents i idènticament distribuïdes amb valors en un espai mesurable $(S, \mathcal{A})$ i sigui $h\colon S \times S \mapsto \mathbb{R}$ un nucli mesurable i simètric. Aleshores,

$$\limsup_n \frac{1}{n \log\log n} \left| \sum_{1 \le i \ne j \le n} h(X_i, X_j) \right| < \infty \text{ q.s.}$$

si i només si es compleixen les condicions següents per a alguna constant $C < \infty$:

(a) h és canònic (degenerat) per a la llei de X (és a dir, $Eh(X, y) = 0$ per a gairebé tot y);

(b) per a tota $u \ge 10$,

$$E(h^2(X, Y) \wedge u) \le C \log\log u;$$

(c) per a alguna $C > 0$,

$$\sup E\left\{h(X, Y) f(X) g(Y) : \max(Ef^2(X), Eg^2(X)) \le 1;\ f, g \in L^\infty\right\} \le C.$$

La prova d'aquest resultat completament inesperat fou una obra mestra de tècniques basades en diverses eines de la teoria dels U-estadístics (moltes d'elles desenvolupades pels mateixos autors, com ara les cotes exponencials per al caos de Rademacher degudes a Latała) i en arguments de truncament bastant sofisticats. Un resultat relacionat és una versió nova i definitiva d'una desigualtat de concentració tipus Bernstein per a U-estadístics (Giné, Latała i Zinn [A80]), que és una de les desigualtats més importants i útils en aquesta àrea de les probabilitats. Aquesta desigualtat la van provar per a U-estadístics d'ordre 2 i més endavant va ser estesa a ordres superiors per Adamczak [1]. Adamczak i Latała [2] van obtenir condicions necessàries i suficients per a la llei del logaritme iterat acotada per a U-estadístics d'ordre superior.

2.6 La distribució asimptòtica de l'estadístic *t*

L'estadístic t de Student amb una mostra

$$T_n = \frac{\sum_{i=1}^n X_i / n^{1/2}}{\left\{\sum_{i=1}^n (X_i - \overline{X}_n)^2/(n-1)\right\}^{1/2}} = \frac{S_n/V_n}{\sqrt{\frac{n-(S_n/V_n)^2}{n-1}}},$$

on $S_n = \sum_{i=1}^n X_i$, $V_n = \sum_{i=1}^n X_i^2$ i $X_1, \ldots, X_n$ són variables aleatòries independents i idènticament distribuïdes, juga un paper clau en l'estadística bàsica

aplicada. Mentre que la seva distribució exacta és ben coneguda des del punt de vista de la teoria del mostreig gaussià, és important conèixer les propietats de T_n sota hipòtesis no gaussianes (o d'altres tipus no estàndard). Efron [11] va revisar estudis previs sobre T_n sota condicions no estàndards (incloent-hi els de Hotelling [16], Hoeffding [14] i d'altres) i va considerar el comportament límit de T_n i de sumes autonormalitzades d'aquests estadístics. Logan, Mallows, Rice i Shepp [23] van provar que si X està en el domini d'atracció d'una llei alfa-estable, $0 < \alpha \leq 2$, centrada si $\alpha > 1$ i simètrica si $\alpha = 1$, aleshores $S_n/V_n \to_d Z_\alpha$, on Z_α és subgaussià. A més van conjecturar que «S_n/V_n és asimptòticament normal si [i potser només si] X està en el domini d'atracció de la llei normal i X està centrada». La implicació directa d'aquesta conjectura es prova amb relativa facilitat a partir de resultats estàndards; vegeu [24]. El recíproc, és a dir, el «només si», va ser provat l'any 1997 per Evarist Giné en col·laboració amb Friedrich Götze i David Mason [A74]. Aquest article brillant fa palès el domini absolut que Evarist Giné tenia de la desigualtat de Paley-Zygmund, la qual fa servir per veure que si $\{S_n/V_n\}$ està acotada estocàsticament, aleshores també ho està en L_1.

Giné va tornar a aquest tema almenys en dos articles més: a [A77] (amb David Mason) estudia lleis del logaritme iterat per a sumes autonormalitzades; a [A92] (amb Friedrich Götze) va establir la normalitat asimptòtica dels estadístics t multivariats sota condicions no estàndards.

2.7 Estadística no paramètrica

Al segle XXI, Evarist Giné va començar a treballar en problemes d'estadística no paramètrica, una àrea de l'estadística matemàtica amb una gran activitat des de mitjan anys noranta. L'interès de Giné va ser provocat per l'àmplia aplicabilitat de les eines dels processos empírics en aquesta àrea. Un punt de vista fonamental va ser observar que la profunda desigualtat de Talagrand [34] per als processos empírics es podia utilitzar amb efectes notables, particularment per a tractar problemes que tenen a veure amb cotes del risc en la norma del suprem en estimació de densitats; vegeu [A85, A107]. Per exemple, considerem un estimador de nucli de la forma

$$f_n(x) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{x - X_i}{h}\right), \quad X_i \sim \text{i.i.d.} \quad P,$$

amb K una funció nucli adequada. Si ignorem el «biaix» de l'estimació, el risc uniforme es pot entendre com el procés empíric

$$\|f_n - Ef_n\|_\infty = \frac{1}{h} \sup_{g \in \mathcal{G}} |(P_n - P)g|, \quad \mathcal{G} = \left\{ g = K\left(\frac{x - \cdot}{h}\right) : x \in \mathbb{R}^d \right\}.$$

Una primera idea clau que es troba a [A85] és que sota condicions simples per a K, per exemple que sigui de variació acotada, la classe $\mathcal{G}$ resulta que és una classe de tipus Vapnik-Chervonenkis i, per tant, fent servir un «chaining

argument» i si P té densitat acotada, resulta

$$E \sup_{g \in \mathcal{G}} |(P_n - P)g| \lesssim \sqrt{\frac{h \log(1/h)}{n}}$$

per a eleccions adequades de h. A més per la desigualtat de Talagrand la concentració de $\|f_n - Ef_n\|_\infty$ al voltant de la seva esperança és efectivament gaussiana (sempre per a eleccions adequades de h), i aquest fet es pot fer servir amb objectius diversos: inicialment Evarist Giné en va deduir la constant exacta que limita quasi segurament $\sqrt{nh/\log(1/h)}\|f_n - Ef_n\|_\infty$ quan $n \to \infty$ i $h \to 0$, tant per als estimadors de nucli [A85] com per als estimadors per a ondetes [A107], cas en el qual es requereix un escalat lleugerament diferent. En treballs posteriors [A106, A111] es va posar de manifest que aquestes desigualtats exponencials eren molt útils per a construir estimadors adaptatius de densitats que podien tractar també el biaix $\|Ef_n - f\|_\infty$ (aplicant el mètode de Lepskiĭ [22]). Tècniques relacionades van ser també utilitzades a l'article [A97] per tal de donar aproximacions empíriques (fent servir el graf laplacià) de l'operador de Laplace sobre una varietat de Riemann (un resultat que va ser útil en el camp de l'aprenentatge automàtic), i en l'article [A113] aquestes desigualtats de concentració es van fer servir en una nova manera d'obtenir taxes de contracció en l'estimació de la funció bayesiana no paramètrica; aquestes idees han estat utilitzades des d'aleshores en estadística bayesiana no paramètrica en els articles recents de Ray [32] i Nickl i Söhl [28], entre d'altres.

En un altre article de molta influència [A110] Evarist Giné va construir bandes de confiança adaptatives per a densitats desconegudes trobant amb exactitud la distribució límit de Gumbel de $\|f_n - f\|_\infty$, adequadament escalada i centrada, on f_n és un estimador totalment adaptatiu (una altra vegada basant-se en el mètode de Lepskiĭ [22]). Aquest va ser el primer resultat sobre el límit exacte d'una distribució per a qualsevol estimador adaptatiu, i va requerir una utilització subtil de les tècniques d'aproximació i de la teoria de límits per a processos gaussians no estacionaris. A més de resoldre reptes probabilístics va ser necessària també la introducció de noves hipòtesis qualitatives per a f, que ara es coneixen amb el nom d'*autosimilitud*, les quals van ser adequades també per al cas general d'espais de Hölder [A110]. Aquestes condicions d'autosimilitud resulta que són més o menys les condicions correctes per a l'existència de conjunts de confiança adaptatius no paramètrics, i han estat tractades més a fons en articles recents de Hoffmann i Nickl [15], Chernozhukov, Chetverikov i Kato [4] i en l'article panoràmic de Szabó, van der Vaart i van Zanten [33], tots ells en els *Annals of Statistics*.

Un altre resultat que es mereix ser esmentat, i que està relacionat amb algunes tècniques anteriors al famós article [A34] de Giné i Zinn de l'any 1984, és el de l'article [A103], que afirma l'existència de determinades classes pregaussianes de funcions $\mathcal{F}$ tals que: a) *no* són de P-Donsker per a alguna P però b) el *procés empíric regularitzat* $\sqrt{n}(P_n * K_h - P)$ corresponent a un estimador de nucli de la densitat *sí* que convergeix en distribució a $\ell_\infty(\mathcal{F})$ cap al pont

brownià generalitzat G_P —per tant, $P_n * K_h$ és estrictament millor que P_n en aquest cas. Aquests resultats han estat instruments molt útils en l'estudi recent de la inferència estadística per a la funció de distribució de mesures de Lévy i distribucions infinitament divisibles; vegeu els articles de Nickl i Reiß [26] i de Nickl, Reiß, Söhl i Trabs [27].

La importància de les tècniques probabilístiques en els fonaments de l'estadística no paramètrica van portar Evarist Giné a escriure la seva quarta monografia, amb el títol de *Mathematical Foundations of Infinite-Dimensional Statistical Models* [L4]. Aplega gran part del seu treball en aquesta àrea, i demostra una altra vegada la visió profunda que tenia dels fonaments matemàtics en què es basen la teoria moderna de la probabilitat i l'estadística. En particular, en els capítols d'aquest llibre dedicats als processos gaussians i als processos empírics, Giné ens ha deixat un monument intel·lectual que serà una referència per a les generacions futures.

3 Biografia[1]

Evarist Giné va morir el 13 de març del 2015 a Hartford, Connecticut. Ha estat un contribuïdor molt important i cocreador de diverses branques de la teoria moderna de la probabilitat les quals han tingut una gran influència, especialment en l'estadística i la teoria de l'aprenentatge (*statistical learning*). La seva feina abasta àrees com ara la probabilitat en espais de Banach, la teoria dels processos empírics, la teoria asimptòtica del bootstrap i dels U-estadístics i processos, així com l'estadística no paramètrica. Va publicar al voltant de cent articles en revistes de primer nivell: vint-i-dos articles als *Annals of Probability* com a autor únic, deu a *Probability Theory and Related Fields*, i vuit articles als *Annals of Statistics*. A més va escriure dos llibres amb una repercussió molt gran, un sobre el teorema del límit central en espais de Banach amb Aloisio Araujo, i l'altre amb Víctor de la Peña sobre desacoblament. Amb Richard Nickl va acabar el seu quart llibre, *Mathematical Foundations of Infinite-Dimensional Statistical Models*, poc abans de morir, publicat a Cambridge University Press.

Evarist Giné va ser elegit membre de l'Institute of Mathematical Statistics (IMS) l'any 1984 i de l'International Statistical Institute (ISI) l'any 1991, va ser membre corresponent de l'Institut d'Estudis Catalans a partir del 1996 i va fer una conferència Medaillon[2] al Congrés Mundial de la Societat Bernoulli l'any 2004 a Barcelona. El juny del 2014 va tenir lloc a Cambridge (Regne Unit) un congrés per celebrar les seves aportacions matemàtiques en ocasió del seu setantè aniversari. Una fotografia de l'Evarist presa per Lucien Birgé en aquest congrés, amb plena salut i el seu bon humor habitual, la reproduïm a la pàgina següent. Evarist Giné havia estat sempre extremament modest i una mostra del seu humor la dóna el correu electrònic que va escriure el juliol del 2014 dient que el congrés en honor seu era «totalment immerescut, però tot i així

1 Aquest apartat, escrit pels mateixos autors de l'article, va ser publicat en el *Institute of Mathematical Statistics Bulletin*.

2 Aquesta conferència comporta l'atorgament d'una medalla.

molt estimulant». De fet, el congrés va servir per posar de manifest les diverses àrees entre les matemàtiques i l'estadística en les quals Evarist Giné i els seus treballs havien tingut un impacte més notable. Un gran respecte per a les seves matemàtiques i la seva personalitat va ser compartit pel gran nombre d'amics i de col·legues que eren presents a Cambridge.

Evarist Giné va néixer el 31 de juliol del 1944 a Falset (Catalunya), en una família que s'ocupava de l'agricultura i de l'elaboració de vins. El seu talent matemàtic prodigiós es va manifestar molt aviat i un professor local va convèncer la seva família que l'Evarist havia de fer l'ensenyament secundari i entrar a la universitat. Va acabar els estudis de batxillerat amb èxit i va fer la carrera de matemàtiques a la Universitat de Barcelona, on va aconseguir el grau de llicenciat l'any 1966. Evarist es va casar amb Rosalind Eastaway aquell mateix any.

En part pel règim franquista i en part pel seu temperament aventurer, el matrimoni va deixar Catalunya, i després d'algun temps fent de professor de matemàtiques a Veneçuela, Evarist va ser acceptat al programa de doctorat en matemàtiques del Massachusetts Institute of Technology (MIT). Va acabar la tesi doctoral el 1973, sota la direcció de Richard M. Dudley, amb un treball sobre tests estadístics per a la uniformitat en varietats riemannianes, que va ser publicat als *Annals of Statistics*. Aquest primer treball, àmpliament citat a la literatura sobre estadística els anys següents, ja posa de manifest una de les característiques principals de la seva recerca: el seu gran interès per als problemes motivats per l'estadística matemàtica, en els quals es necessita desenvolupar eines potents i subtils. Les seves habilitats matemàtiques van produir dos articles més durant el seu període com a doctorand, tots dos publicats en els *Annals of Probability*, que van iniciar una de les seves línies

principals de recerca, l'estudi de teoremes de límit en espai de Banach de dimensió infinita.

Evarist Giné va passar el curs 1974–1975 a Berkeley com a lector, i allà va conèixer Le Cam i els altres grans personatges de l'època daurada de l'estadística a Berkeley. Després d'alguns anys passant per diverses institucions, va tornar a Veneçuela, on va ser el cap del departament de matemàtiques de l'Instituto Venezolano de Investigaciones Científicas, va ser professor de la Universitat Autònoma de Barcelona i finalment es va establir a la Universitat Texas A&M, on va ser professor a partir de l'any 1983. Una gran part de la seva feina més original i més influent la va fer en aquesta època en col·laboració amb Joel Zinn, un col·lega i amic de la Texas A&M. El seu treball conjunt va donar lloc al desenvolupament de les eines més importants de la teoria dels processos empírics, com ara les desigualtats de simetrització, cotes per a l'entropia i desigualtats per al multiplicador aleatori, que més tard van penetrar en moltes àrees de les matemàtiques, l'estadística i la informàtica (en particular, l'aprenentatge automàtic). Després de dos anys com a professor al CUNY (Nova York), Evarist Giné va obtenir una posició a la Universitat de Connecticut el 1990, on s'hi va estar fins a la seva mort, últimament com a cap del departament de matemàtiques. Evarist Giné va tenir vuit estudiants de doctorat, entre els quals destaca Miguel Arcones, i va tenir un impacte notable sobre tota una generació de probabilistes i teòrics de l'estadística, la que va rebre la seva formació entre els anys 1990 i 2010.

La pèrdua de l'Evarist provoca un buit enorme en la comunitat matemàtica. Per als que el van conèixer personalment i van treballar amb ell, sempre serà recordat com un gran amic amb qui es podia parlar sense fi de matemàtiques al seu despatx o bé en l'hospitalitat de casa seva. La pèrdua és encara més greu per a la seva família: la seva dona Rosalind, que el sobreviu; les seves dues filles, Núria i Roser, i els seus néts, Liam i Mireia. Però el seu gran entusiasme, l'originalitat i la profunditat de les seves idees perviuran per a moltes generacions futures, a través dels seus escrits matemàtics, en les nostres memòries i en la seva família.

4 Publicacions d'Evarist Giné

Llibres

[L1] Araujo, A.; Giné, E. *The Central Limit Theorem for Real and Banach Valued Random Variables*. Nova York; Chichester; Brisbane: John Wiley & Sons, 1980. (Wiley Series in Probability and Mathematical Statistics)

[L2] Giné, E.; Grimmett, G. R.; Saloff-Coste, L. *Lectures on Probability Theory and Statistics*. Lectures from the 26th Summer School on Probability Theory held in Saint-Flour, August 19–September 4, 1996. Edició a cura de P. Bernard. Berlín: Springer-Verlag, 1997. (Lecture Notes in Math.; 1665)

[L3] DE LA PEÑA, V. H.; GINÉ, E. *Decoupling. From Dependence to Independence. Randomly Stopped Processes. U-Statistics and Processes. Martingales and Beyond.* Nova York: Springer-Verlag, 1999. (Probability and its Applications (New York))

[L4] GINÉ, E.; NICKL, R. *Mathematical Foundations of Infinite-Dimensional Statistical Models.* Cambridge, Regne Unit: Cambridge University Press, 2015.

Articles i edicions de llibres

[A1] GINÉ M., E. «On the central limit theorem for sample continuous processes». *Ann. Probability*, 2 (1974), 629–641.

[A2] DUDLEY, R.; PERKINS, P. C.; GINÉ M., E. «Statistical tests for preferred orientation». *J. Geology*, 83 (1975), 685–705.

[A3] GINÉ M., E. «The addition formula for the eigenfunctions of the Laplacian». *Advances in Math.*, 18 (1) (1975), 102–107.

[A4] GINÉ M., E. «Invariant tests for uniformity on compact Riemannian manifolds based on Sobolev norms». *Ann. Statist.*, 3 (6) (1975), 1243–1266.

[A5] KLEIN, R.; GINÉ, E. «On quadratic variation of processes with Gaussian increments». *Ann. Probability*, 3 (4) (1975), 716–721.

[A6] GINÉ M., E. «Bounds for the speed of convergence in the central limit theorem in $C(S)$». *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 36 (4) (1976), 317–331.

[A7] GINÉ M., E. «Some remarks on the central limit theorem in $C(S)$». A: *Probability in Banach Spaces* (Proc. First Internat. Conf., Oberwolfach, 1975). Berlín: Springer, 1976, 101–106. (Lecture Notes in Math.; 526)

[A8] GARCÍA-PALOMARES, U.; GINÉ M., E. «On the linear programming approach to the optimality property of Prokhorov's distance». *J. Math. Anal. Appl.*, 60 (3) (1977), 596–600.

[A9] ARAUJO, A.; GINÉ M., E. «Type, cotype and Lévy measures in Banach spaces». *Ann. Probab.*, 6 (4) (1978), 637–643.

[A10] DE ACOSTA, A.; ARAUJO, A.; GINÉ, E. «On Poisson measures, Gaussian measures and the central limit theorem in Banach spaces». A: *Probability on Banach Spaces.* Nova York: Dekker, 1978, 1–68. (Adv. Probab. Related Topics; 4)

[A11] GINÉ, E. «A survey on the general central limit problem in Banach spaces». A: *Séminaire sur la Géométrie des Espaces de Banach (1977–1978).* Palaiseau: École Polytech., 1978, Exp. núm. 24, 17 p.

[A12] ARAUJO, A.; GINÉ, E. «On tails and domains of attraction of stable measures in Banach spaces». *Trans. Amer. Math. Soc.*, 248 (1) (1979), 105–119.

[A13] DE ACOSTA, A.; GINÉ, E. «Convergence of moments and related functionals in the general central limit theorem in Banach spaces». *Z. Wahrsch. Verw. Gebiete*, 48 (2) (1979), 213–231.

[A14] GINÉ, E. «Domains of attraction in Banach spaces». A: *Séminaire de Probabilités, XIII (Univ. Strasbourg, Strasbourg, 1977/78)*. Berlín: Springer, 1979, 22–40. (Lecture Notes in Math.; 721)

[A15] GINÉ, E.; MANDREKAR, V.; ZINN, J. «On sums of independent random variables with values in L_p $(2 \leq p < \infty)$». A: *Probability in Banach Spaces, II* (Proc. Second Internat. Conf., Oberwolfach, 1978). Berlín: Springer, 1979, 111–124. (Lecture Notes in Math.; 709)

[A16] GINÉ, E. «Corrections to: "Domains of attraction in Banach spaces"». [*Séminaire de Probabilités, XIII (Univ. Strasbourg, Strasbourg, 1977/78)*. Berlín: Springer, 1979, 22–40. (Lecture Notes in Math.; 721)]. A: *Seminar on Probability, XIV (Paris, 1978/1979) (French)*. Berlín: Springer, 1980, p. 17. (Lecture Notes in Math.; 784)

[A17] GINÉ, E. «Sums of independent random variables and sums of their squares». Proceedings of the seventh Spanish-Portuguese conference on mathematics, Part III (Sant Feliu de Guíxois, 1980). *Publ. Sec. Mat. Univ. Autònoma Barcelona*, 22 (1980), 127–132.

[A18] GINÉ, E. «Domains of partial attraction in several dimensions». *Ann. Inst. H. Poincaré Sect. B (N.S.)*, 16 (2) (1980), 87–100.

[A19] GINÉ, E. «The central limit problem: three less typical aspects». Proceedings of the seventh Spanish-Portuguese conference on mathematics, Part III (Sant Feliu de Guíxois, 1980). *Publ. Sec. Mat. Univ. Autònoma Barcelona*, 22 (1980), 133–138.

[A20] GINÉ, E.; LEÓN, J. R. «On the central limit theorem in Hilbert space». *Stochastica*, 4 (1) (1980), 43–71.

[A21] GINÉ M., E.; LEÓN, J. R. «On the central limit theorem in Hilbert space». A: *Proceedings of the First World Conference on Mathematics at the Service of Man* (Barcelona, 1977). Vol. I. Barcelona: Univ. Politec., 1980, 620–625.

[A22] ARAUJO, A.; GINÉ, E.; MANDREKAR, V.; ZINN, J. «On the accompanying laws theorem in Banach spaces». *Ann. Probab.*, 9 (2) (1981), 202–210.

[A23] GINÉ, E. «Correction to: "Domains of partial attraction in several dimensions"». *Ann. Inst. H. Poincaré Sect. B (N.S.)*, 17 (1) (1981), 143–145.

[A24] GINÉ, E. «Central limit theorems in Banach spaces: a survey». A: *Probability in Banach Spaces, III* (Medford, Mass., 1980). Berlín; Nova York: Springer, 1981, 138–152. (Lecture Notes in Math.; 860)

[A25] GINÉ, E.; MARCUS, M. B. «On the central limit theorem in $C(K)$». A: *Statistical and Physical Aspects of Gaussian Processes* (Saint-Flour, 1980). París: CNRS, 1981, 361–383. (Colloq. Internat. CNRS; 307)

[A26] GINÉ, A.; MARCUS, M. B. «Some results on the domain of attraction of stable measures on $C(K)$». *Probab. Math. Statist.*, 2 (2) (1982), 125–147 (1983).

[A27] GINÉ, E. «The Lévy-Lindeberg central limit theorem in L_p, $0 < p < 1$». *Proc. Amer. Math. Soc.*, 88 (1) (1983), 147–153.

[A28] GINÉ, E. «Large deviations in spaces of stable type». *Ann. Inst. H. Poincaré Sect. B (N.S.)*, 19 (3) (1983), 267–279.

[A29] GINÉ, E. «A counterexample on domains of partial attraction in Banach spaces». A: *Probability in Banach Spaces, IV* (Oberwolfach, 1982). Berlín; Nova York: Springer, 1983, 102–111. (Lecture Notes in Math.; 990)

[A30] GINÉ, E.; HAHN, M. G. «On stability of probability laws with univariate stable marginals». *Z. Wahrsch. Verw. Gebiete*, 64 (2) (1983), 157–165.

[A31] GINÉ, E.; HAHN, M. G.; ZINN, J. «Limit theorems for random sets: an application of probability in Banach space results». A: *Probability in Banach Spaces, IV* (Oberwolfach, 1982). Berlín: Springer, 1983, 112–135. (Lecture Notes in Math.; 990)

[A32] GINÉ, E.; MARCUS, M. B. «The central limit theorem for stochastic integrals with respect to Lévy processes». *Ann. Probab.*, 11 (1) (1983), 58–77.

[A33] GINÉ, E.; ZINN, J. «Central limit theorems and weak laws of large numbers in certain Banach spaces». *Z. Wahrsch. Verw. Gebiete*, 62 (3) (1983), 323–354.

[A34] GINÉ, E.; ZINN, J. «Some limit theorems for empirical processes. With discussion». *Ann. Probab.*, 12 (4) (1984), 929–998.

[A35] GINÉ, E.; HAHN, M. G. «Characterization and domains of attraction of p-stable random compact sets». *Ann. Probab.*, 13 (2) (1985), 447–468.

[A36] GINÉ, E.; HAHN, M. G. «The Lévy-Hinčin representation for random compact convex subsets which are infinitely divisible under Minkowski addition». *Z. Wahrsch. Verw. Gebiete*, 70 (2) (1985), 271–287.

[A37] GINÉ, E.; HAHN, M. G. «M-infinitely divisible random compact convex sets». A: *Probability in Banach Spaces, V* (Medford, Mass., 1984). Berlín: Springer, 1985, 226–248. (Lecture Notes in Math.; 1153)

[A38] GINÉ, E.; MARCUS, M. B.; ZINN, J. «A version of Chevet's theorem for stable processes». *J. Funct. Anal.*, 63 (1) (1985), 47–73.

[A39] GINÉ, E.; ZINN, J. «On the approximation of p-homogeneous functions in Banach spaces». A: *Homenatge a Francesc Sales*. Barcelona: Universitat de Barcelona, 1985, 78–87.

[A40] GINÉ, E.; ZINN, J. «Lectures on the central limit theorem for empirical processes». A: *Probability and Banach Spaces* (Zaragoza, 1985). Berlín: Springer, 1986, 50–113. (Lecture Notes in Math.; 1221)

[A41] GINÉ, E.; ZINN, J. «Empirical processes indexed by Lipschitz functions». *Ann. Probab.*, 14 (4) (1986), 1329–1338.

[A42] GINÉ, E.; ZINN, J. «A remark on the central limit theorem for random measures and processes». A: *Probability Theory and Mathematical Statistics, Vol. I* (Vilnius, 1985). Utrecht: VNU Sci. Press, 1987, 483–487.

[A43] GINÉ, E.; ZINN, J. «The law of large numbers for partial sum processes indexed by sets». *Ann. Probab.*, 15 (1) (1987), 154–163.

[A44] ANDERSEN, N. T.; GINÉ, E.; OSSIANDER, M.; ZINN, J. «The central limit theorem and the law of iterated logarithm for empirical processes under local conditions». *Probab. Theory Related Fields*, 77 (2) (1988), 271–305.

[A45] ANDERSEN, N. T.; GINÉ, E.; ZINN, J. «The central limit theorem for empirical processes under local conditions: the case of Radon infinitely divisible limits without Gaussian component». *Trans. Amer. Math. Soc.*, 308 (2) (1988), 603–635.

[A46] ARCONES, M. A.; GINÉ, E. «The bootstrap of the mean with arbitrary bootstrap sample size». *Ann. Inst. H. Poincaré Probab. Statist.*, 25 (4) (1989), 457–481.

[A47] GINÉ, E.; ZINN, J. «Necessary conditions for the bootstrap of the mean». *Ann. Statist.*, 17 (2) (1989), 684–691.

[A48] GINÉ, E.; ZINN, J. «Discussion of D. Pollard's paper». Asymptotics via empirical processes. *Statistical Science*, 4 (1989), 355–356.

[A49] GINÉ, E.; ZINN, J. «L_p multipliers in the central limit theorem with p-stable limit». A: *Probability Theory on Vector Spaces, IV* (Łańcut, 1987). Berlín: Springer, 1989, 74–81. (Lecture Notes in Math.; 1391)

[A50] GINÉ, E.; HAHN, M. G.; VATAN, P. «Max-infinitely divisible and max-stable sample continuous processes». *Probab. Theory Related Fields*, 87 (2) (1990), 139–165.

[A51] GINÉ, E.; MARCUS, M. B.; ZINN, J. «On random multipliers in the central limit theorem with p-stable limit, $0 < p < 2$». A: *Probability in Banach Spaces, 6* (Sandbjerg, 1986). Boston, Mass.: Birkhäuser Boston, 1990, 120–149. (Progr. Probab.; 20)

[A52] GINÉ, E.; ZINN, J. «Bootstrapping general empirical measures». *Ann. Probab.*, 18 (2) (1990), 851–869.

[A53] ARCONES, M. A.; GINÉ, E. «Some bootstrap tests of symmetry for univariate continuous distributions». *Ann. Statist.*, 19 (3) (1991), 1496–1511.

[A54] ARCONES, M. A.; GINÉ, E. «Additions and correction to: "The bootstrap of the mean with arbitrary bootstrap sample size"» [*Ann. Inst. H. Poincaré Probab. Statist.*, 25 (4) (1989), 457–481]. *Ann. Inst. H. Poincaré Probab. Statist.*, 27 (4) (1991), 583–595.

[A55] DUDLEY, R. M.; GINÉ, E.; ZINN, J. «Uniform and universal Glivenko-Cantelli classes». *J. Theoret. Probab.*, 4 (3) (1991), 485–510.

[A56] GINÉ, E.; ZINN, J. «Gaussian characterization of uniform Donsker classes of functions». *Ann. Probab.*, 19 (2) (1991), 758–782.

[A57] Arcones, M. A.; Giné, E. «On the bootstrap of U and V statistics». *Ann. Statist.*, 20 (2) (1992), 655–674.

[A58] Arcones, M. A.; Giné, E. «On the bootstrap of M-estimators and other statistical functionals». A: *Exploring the Limits of Bootstrap* (East Lansing, MI, 1990). Nova York: Wiley, 1992, 13–47. (Wiley Ser. Probab. Math. Statist. Probab. Math. Statist.)

[A59] Giné, E.; Zinn, J. «On Hoffmann-Jørgensen's inequality for U-processes». A: *Probability in Banach Spaces, 8* (Brunswick, ME, 1991). Boston, Mass.: Birkhäuser Boston, 1992, 80–91. (Progr. Probab.; 30)

[A60] Giné, E.; Zinn, J. «Marcinkiewicz type laws of large numbers and convergence of moments for U-statistics». A: *Probability in Banach Spaces, 8* (Brunswick, ME, 1991). Boston, Mass.: Birkhäuser Boston, 1992, 273–291. (Progr. Probab.; 30)

[A61] Alamayehu, D.; de la Peña, V.; Giné, E. «Bootstrap goodness of fit tests based on the empirical distribution function». A: Tarter, M. E.; Look, M. D. (ed.). *Computing Science and Statistics: Proceedings of the 25th Annual Symposium on the Interface*. Virginia: Interface Foundation of North America, Fairfax Station, 1993, 228–233.

[A62] Arcones, M. A.; Giné, E. «On decoupling, series expansions, and tail behavior of chaos processes». *J. Theoret. Probab.*, 6 (1) (1993), 101–122.

[A63] Arcones, M. A.; Giné, E. «Limit theorems for U-processes». *Ann. Probab.*, 21 (3) (1993), 1494–1542.

[A64] Arcones, M. A.; Chen, Z.; Giné, E. «Estimators related to U-processes with applications to multivariate medians: asymptotic normality». *Ann. Statist.*, 22 (3) (1994), 1460–1477.

[A65] Arcones, M. A.; Giné, E. «U-processes indexed by Vapnik-Červonenkis classes of functions with applications to asymptotics and bootstrap of U-statistics with estimated parameters». *Stochastic Process. Appl.*, 52 (1) (1994), 17–38.

[A66] Giné, E.; Zinn, J. «A remark on convergence in distribution of U-statistics». *Ann. Probab.*, 22 (1) (1994), 117–125.

[A67] Giné-Masdéu, E. «Processos empírics i aplicacions: visió general amb biaix». *Butlletí de la Societat Catalana de Matemàtiques*, 9 (1994), 7–34.

[A68] Arcones, M. A.; Giné, E. «On the law of the iterated logarithm for canonical U-statistics and processes». *Stochastic Process. Appl.*, 58 (2) (1995), 217–245.

[A69] Cuzick, J.; Giné, E.; Zinn, J. «Laws of large numbers for quadratic forms, maxima of products and truncated sums of i.i.d. random variables». *Ann. Probab.*, 23 (1) (1995), 292–333.

[A70] Giné, E. «Empirical processes and applications: an overview». With a discussion by Jon A. Wellner and a rejoinder by the author. *Bernoulli*, 2 (1) (1996), 1–38.

[A71] GINÉ, E.; ZHANG, C.-H. «On integrability in the LIL for degenerate U-statistics». *J. Theoret. Probab.*, 9 (2) (1996), 385–412.

[A72] GINÉ, E. «Lectures on some aspects of the bootstrap». A: *Lectures on Probability Theory and Statistics* (Saint-Flour, 1996). Berlín: Springer, 1997, 37–151. (Lecture Notes in Math.; 1665)

[A73] GINÉ, E. «Decoupling and limit theorems for U-statistics and U-processes». A: *Lectures on Probability Theory and Statistics* (Saint-Flour, 1996). Berlín: Springer, 1997, 1–35. (Lecture Notes in Math.; 1665)

[A74] GINÉ, E.; GÖTZE, F.; MASON, D. M. «When is the Student t-statistic asymptotically standard normal?». *Ann. Probab.*, 25 (3) (1997), 1514–1531.

[A75] GINÉ, E.; WELLNER, J. A. «Uniform convergence in some limit theorems for multiple particle systems». *Stochastic Process. Appl.*, 72 (1) (1997), 47–72.

[A76] GINÉ, E. «A consequence for random polynomials of a result of de la Peña and Montgomery-Smith». A: *High Dimensional Probability* (Oberwolfach, 1996). Basel: Birkhäuser, 1998, 103–110. (Progr. Probab.; 43)

[A77] GINÉ, E.; MASON, D. M. «On the LIL for self-normalized sums of IID random variables». *J. Theoret. Probab.*, 11 (2) (1998), 351–370.

[A78] DEL BARRIO, E.; GINÉ, E.; MATRÁN, C. «Central limit theorems for the Wasserstein distance between the empirical and the true distributions». *Ann. Probab.*, 27 (2) (1999), 1009–1071.

[A79] GINÉ, E.; GUILLOU, A. «Laws of the iterated logarithm for censored data». *Ann. Probab.*, 27 (4) (1999), 2042–2067.

[A80] GINÉ, E.; LATAŁA, R.; ZINN, J. «Exponential and moment inequalities for U-statistics». A: *High Dimensional Probability, II* (Seattle, WA, 1999). Boston, Mass.: Birkhäuser Boston, 2000, 13–38. (Progr. Probab.; 47)

[A81] GINÉ, E.; MASON, D.; WELLNER, J. A. (ED.). *High Dimensional Probability, II* (Seattle, WA, 1999). Boston, Mass.: Birhhäuser Boston, 2000. (Progr. Probab.; 47)

[A82] KOLTCHINSKII, V.; GINÉ, E. «Random matrix approximation of spectra of integral operators». *Bernoulli*, 6 (1) (2000), 113–167.

[A83] GINÉ, E.; GUILLOU, A. «On consistency of kernel density estimators for randomly censored data: rates holding uniformly over adaptive intervals». *Ann. Inst. H. Poincaré Probab. Statist.*, 37 (4) (2001), 503–522.

[A84] GINÉ, E.; KWAPIEŃ, S.; LATAŁA, R.; ZINN, J. «The LIL for canonical U-statistics of order 2». *Ann. Probab.*, 29 (1) (2001), 520–557.

[A85] GINÉ, E.; GUILLOU, A. «Rates of strong uniform consistency for multivariate kernel density estimators». *Ann. Inst. H. Poincaré Probab. Statist.*, 38 (6) (2002), 907–921. [En l'honor de J. Bretagnolle, D. Dacunha-Castelle, I. Ibragimov]

[A86] DEL BARRIO, E.; GINÉ, E.; MATRÁN, C. «Correction: "Central limit theorems for the Wasserstein distance between the empirical and the true distributions"» [*Ann. Probab.*, 27 (2) (1999), 1009–1071]. *Ann. Probab.*, 31 (2) (2003), 1142–1143.

[A87] GINÉ, E.; HOUDRÉ, C.; NUALART, D. (ED.). *Stochastic Inequalities and Applications*. Basel: Birkhauser, 2003. (Progr. Probab.; 56)

[A88] GINÉ, E.; KOLTCHINSKII, V.; SAKHANENKO, L. «Convergence in distribution of self-normalized sup-norms of kernel density estimators». A: *High Dimensional Probability, III* (Sandjberg, 2002). Basel: Birkhäuser, 2003, 241–253. (Progr. Probab.; 55)

[A89] GINÉ, E.; KOLTCHINSKII, V.; WELLNER, J. A. «Ratio limit theorems for empirical processes». A: *Stochastic Inequalities and Applications*. Basel: Birkhäuser, 2003, 249–278. (Progr. Probab.; 56)

[A90] GINÉ, E.; MASON, D. M.; ZAITSEV, A. YU. «The L_1-norm density estimator process». *Ann. Probab.*, 31 (2) (2003), 719–768.

[A91] CHEN, Z.; GINÉ, E. «Another approach to asymptotics and bootstrap of randomly trimmed means». *Ann. Inst. Statist. Math.*, 56 (4) (2004), 771–790.

[A92] GINÉ, E.; GÖTZE, F. «On standard normal convergence of the multivariate Student t-statistic for symmetric random vectors». *Electron. Comm. Probab.*, 9 (2004), 162–171 (electronic).

[A93] GINÉ, E.; KOLTCHINSKII, V.; SAKHANENKO, L. «Kernel density estimators: convergence in distribution for weighted sup-norms». *Probab. Theory Related Fields*, 130 (2) (2004), 167–198.

[A94] GINÉ, E.; KOLTCHINSKII, V.; ZINN, J. «Weighted uniform consistency of kernel density estimators». *Ann. Probab.*, 32 (3B) (2004), 2570–2605.

[A95] GINÉ, E.; MASON, D. M. «The law of the iterated logarithm for the integrated squared deviation of a kernel density estimator». *Bernoulli*, 10 (4) (2004), 721–752.

[A96] DEL BARRIO, E.; GINÉ, E.; UTZET, F. «Asymptotics for L_2 functionals of the empirical quantile process, with applications to tests of fit based on weighted Wasserstein distances». *Bernoulli*, 11 (1) (2005), 131–189.

[A97] GINÉ, E; KOLTCHINSKII, V. «Empirical graph Laplacian approximation of Laplace-Beltrami operators: large sample results». A: *High Dimensional Probability*. Beachwood, Ohio: Inst. Math. Statist., 2006, 238–259. (IMS Lecture Notes Monogr. Ser.; 51)

[A98] GINÉ, E.; KOLTCHINSKII, V. «Concentration inequalities and asymptotic results for ratio type empirical processes». *Ann. Probab.*, 34 (3) (2006), 1143–1216.

[A99] GINÉ, E.; KOLTCHINSKII, V.; LI, W.; ZINN, J. (ED.). *High Dimensional Probability*. Proceedings of the Fourth International Conference. Beachwood, Ohio: Inst. Math. Statist., 2006. (IMS Lecture Notes Monogr. Ser.; 51)

[A100] GINÉ, E.; MASON, D. M. «On local U-statistic processes and the estimation of densities of functions of several sample variables». *Ann. Statist.*, 35 (3) (2007), 1105–1145.

[A101] GINÉ, E.; MASON, D. M. «Laws of the iterated logarithm for the local U-statistic process». *J. Theoret. Probab.*, 20 (3) (2007), 457–485.

[A102] GINÉ, E.; MASON, D. M. «Uniform in bandwidth estimation of integral functionals of the density function». *Scand. J. Statist.*, 35 (4) (2008), 739–761.

[A103] GINÉ, E.; NICKL, R. «Uniform central limit theorems for kernel density estimators». *Probab. Theory Related Fields*, 141 (3–4) (2008), 333–387.

[A104] GINÉ, E.; NICKL, R. «A simple adaptive estimator of the integrated square of a density». *Bernoulli*, 14 (1) (2008), 47–61.

[A105] GINÉ, E.; NICKL, R. «Adaptation on the space of finite signed measures». *Math. Methods Statist.*, 17 (2) (2008), 113–122.

[A106] GINÉ, E.; NICKL, R. «An exponential inequality for the distribution function of the kernel density estimator, with applications to adaptive estimation». *Probab. Theory Related Fields*, 143 (3–4) (2009), 569–596.

[A107] GINÉ, E.; NICKL, R. «Uniform limit theorems for wavelet density estimators». *Ann. Probab.*, 37 (4) (2009), 1605–1646.

[A108] GINÉ, E.; KOLTCHINSKII, V.; NORVAIŠA, R. (ED.). *Selected Works of R. M. Dudley*. Nova York: Springer, 2010.

[A109] GINÉ, E.; NICKL, R. «Adaptive estimation of a distribution function and its density in sup-norm loss by wavelet and spline projections». *Bernoulli*, 16 (4) (2010), 1137–1163.

[A110] GINÉ, E.; NICKL, R. «Confidence bands in density estimation». *Ann. Statist.*, 38 (2) (2010), 1122–1170.

[A111] GINÉ, E.; SANG, H. «Uniform asymptotics for kernel density estimators with variable bandwidths». *J. Nonparametr. Stat.*, 22 (5–6) (2010), 773–795.

[A112] GINÉ, E.; GÜNTÜRK, C. S.; MADYCH, W. R. «On the periodized square of L^2 cardinal splines». *Exp. Math.*, 20 (2) (2011), 177–188.

[A113] GINÉ, E.; NICKL, R. «Rates of contraction for posterior distributions in L^r-metrics, $1 \leq r \leq \infty$». *Ann. Statist.*, 39 (6) (2011), 2883–2911.

[A114] GINÉ, E.; SANG, H. «On the estimation of smooth densities by strict probability densities at optimal rates in sup-norm». A: *From Probability to Statistics and Back: High-Dimensional Models and Processes*. Beachwood, Ohio: Inst. Math. Statist., 2013, 128–149. (Inst. Math. Stat. (IMS) Collect.; 9)

[A115] GINÉ, E.; MADYCH, W. R. «On wavelet projection kernels and the integrated squared error in density estimation». *Statist. Probab. Lett.*, 91 (2014), 32–40.

Referències

[1] Adamczak, R. «Moment inequalities for U-statistics». *Ann. Probab.*, 34 (6) (2006), 2288–2314.

[2] Adamczak, R.; Latała, R. «The LIL for canonical U-statistics». *Ann. Probab.*, 36 (3) (2008), 1023–1058.

[3] Bickel, P. J.; Freedman, D. A. «Some asymptotic theory for the bootstrap». *Ann. Statist.*, 9 (6) (1981), 1196–1217.

[4] Chernozhukov, V.; Chetverikov, D.; Kato, K. «Anti-concentration and honest, adaptive confidence bands». *Ann. Statist.*, 42 (5) (2014), 1787–1818.

[5] de la Peña, V. H. «Decoupling and Khintchine's inequalities for U-statistics». *Ann. Probab.*, 20 (4) (1991), 1877–1892.

[6] de la Peña, V. H.; Montgomery-Smith, S. J. «Bounds on the tail probability of U-statistics and quadratic forms». *Bull. Amer. Math. Soc. (N.S.)*, 31 (2) (1994), 223–227.

[7] de la Peña, V. H.; Montgomery-Smith, S. J.; Szulga, J. «Contraction and decoupling inequalities for multilinear forms and U-statistics». *Ann. Probab.*, 22 (4) (1994), 1745–1765.

[8] Dehling, H. «The functional law of the iterated logarithm for von Mises functionals and multiple Wiener integrals». *J. Multivariate Anal.*, 28 (2) (1989), 177–189.

[9] Dudley, R. M. «Sample functions of the Gaussian process». *Ann. Probability*, 1 (1) (1973), 66–103.

[10] Dudley, R. M. «Central limit theorems for empirical measures». *Ann. Probab.*, 6 (6) (1978), 899–929 (1979).

[11] Efron, B. «Student's t-test under symmetry conditions». *J. Amer. Statist. Assoc.*, 64 (1969), 1278–1302.

[12] Efron, B. «Bootstrap methods: another look at the jackknife». *Ann. Statist.*, 7 (1) (1979), 1–26.

[13] Halmos, P. R. «The theory of unbiased estimation». *Ann. Math. Statistics*, 17 (1946), 34–43.

[14] Hoeffding, W. «Probability inequalities for sums of bounded random variables». *J. Amer. Statist. Assoc.*, 58 (1963), 13–30.

[15] Hoffmann, M.; Nickl, R. «On adaptive inference and confidence bands». *Ann. Statist.*, 39 (5) (2011), 2383–2409.

[16] Hotelling, H. «The behavior of some standard statistical tests under nonstandard conditions». A: *Proc. 4th Berkeley Sympos. Math. Statist. and Prob.* Vol. I. Berkeley: Univ. California Press, 1961, 319–359.

[17] Kendall, D. G. «Foundations of a theory of random sets». A: *Stochastic Geometry (a tribute to the memory of Rollo Davidson)*. Londres: Wiley, 1974, 322–376.

[18] KOLTCHINS'KIĬ, V. I. «On the central limit theorem for empirical measures». *Teor. Veroyatnost. i Mat. Statist.*, 24 (1981), 63–75, 152. [Traducció a l'anglès: *Theory Probab. Math. Statist.*, 24 (1982), 71–82]

[19] LE CAM, L. «A remark on empirical measures». A: *A Festschrift for Erich L. Lehmann*. Belmont, Calif.: Wadsworth, 1983, 305–327. (Wadsworth Statist./Probab. Ser.)

[20] LEDOUX, M.; TALAGRAND, M. «Conditions d'intégrabilité pour les multiplicateurs dans le TLC banachique». *Ann. Probab.*, 14 (3) (1986), 916–921.

[21] LEDOUX, M.; TALAGRAND, M. «Un critère sur les petites boules dans le théorème limite central». *Probab. Theory Related Fields*, 77 (1) (1988), 29–47.

[22] LEPSKIĬ, O. V. «A problem of adaptive estimation in Gaussian white noise». *Teor. Veroyatnost. i Primenen.*, 35 (3) (1990), 459–470. [Traducció a l'anglès: *Theory Probab. Appl.*, 35 (3) (1990), 454–466 (1991)]

[23] LOGAN, B. F.; MALLOWS, C. L.; RICE, S. O.; SHEPP, L. A. «Limit distributions of self-normalized sums». *Ann. Probability*, 1 (1973), 788–809.

[24] MALLER, R. A. «A theorem on products of random variables, with application to regression». *Austral. J. Statist.*, 23 (2) (1981), 177–185.

[25] MATHERON, G. *Random sets and integral geometry*. Nova York; Londres; Sydney: John Wiley & Sons, 1975.

[26] NICKL, R.; REIß, M. «A Donsker theorem for Lévy measures». *J. Funct. Anal.*, 263 (10) (2012), 3306–3332.

[27] NICKL, R.; REIß, M.; SÖHL, J.; TRABS, M. «High frequency Donsker theorems for Lévy measures». *Probab. Theory Related Fields*, 164 (1–2) (2016), 61–108.

[28] NICKL, R.; SÖHL, J. «Nonparametric Bayesian posterior contraction rates for discretely observed scalar diffusions». Preprint (2015), disponible a `arXiv:1510.05526`.

[29] NOLAN, D.; POLLARD, D. «*U*-processes: rates of convergence». *Ann. Statist.*, 15 (2) (1987), 780–799.

[30] NOLAN, D.; POLLARD, D. «Functional limit theorems for *U*-processes». *Ann. Probab.*, 16 (3) (1988), 1291–1298.

[31] POLLARD, D. «A central limit theorem for empirical processes». *J. Austral. Math. Soc. Ser. A*, 33 (2) (1982), 235–248.

[32] RAY, K. «Bayesian inverse problems with non-conjugate priors». *Electron. J. Stat.*, 7 (2013), 2516–2549.

[33] SZABÓ, B.; VAN DER VAART, A. W.; VAN ZANTEN, J. H. «Frequentist coverage of adaptive nonparametric Bayesian credible sets (with discussion)». *Ann. Statist.*, 43 (4) (2015), 1391–1428.

[34] TALAGRAND, M. «New concentration inequalities in product spaces». *Invent. Math.*, 126 (3) (1996), 505–563.

[35] v. Mises, R. «On the asymptotic distribution of differentiable statistical functions». *Ann. Math. Statistics*, 18 (1947), 309–348.

[36] Vapnik, V. N.; Chervonenkis, A. Ya. «Necessary and sufficient conditions for the uniform convergence of empirical means to their true values». *Teor. Veroyatnost. i Primenen.*, 26 (3) (1981), 543–563. [Traducció a l'anglès: *Theory Probab. Appl.*, 26 (3) (1981), 532–553]

Vladimir Koltchinskii
School of Mathematics
Georgia Institute of Technology
Atlanta, GA 30332-0160
vlad@math.gatech.edu

Richard Nickl
Center for Mathematical Sciences
CB3 0WB Cambridge
United Kingdom
r.nickl@statslab.cam.ac.uk

Sara van de Geer
Seminar for Statistics
ETH Zurich
Ramistrasse 101
8092 Zürich
geer@stat.math.ethz.ch

Jon A. Wellner
Department of Statistics
B313 Padelford Hall
Northeast Stevens Way
University of Washington
Seattle, WA 98195
jaw@stat.washington.edu

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 31–50. DOI: 10.2436/20.2002.01.65

Les matemàtiques al darrere de les criptomonedes

Elitza Maneva

Resum: Mitjançant una presentació dels fonaments de les criptomonedes com ara Bitcoin, exposarem tres temes que pertanyen a la criptografia moderna: les *firmes digitals*, les *funcions de hash* i les *demostracions de coneixement nul*. Els problemes de caràcter purament matemàtic que hi sorgeixen poden servir d'exemples als professionals docents per motivar l'estudi de l'aritmètica modular, la probabilitat, la teoria de grafs o la complexitat computacional.

Paraules clau: criptografia, criptomonedes, RSA, corbes el·líptiques, funció de *hash*, probabilitat, grafs, complexitat computacional, aritmètica modular.

Classificació MSC2010: 68-02, 68Q15, 68Q17, 68Q05.

1 Introducció

Fa sis anys que la moneda electrònica bitcoin atreu l'interès d'economistes, de polítics i de la ciutadania en general. Abans de Bitcoin, poca gent s'havia preguntat si la manera com funcionen els diners avui dia és l'única o la millor possible. Tot i que ningú no dirà que Bitcoin dóna respostes definitives a aquestes preguntes, clarament és una idea que obre moltes portes.

A part del fet de ser de codi obert, la novetat principal de Bitcoin és que és una moneda distribuïda, és a dir, no depèn de cap banc o autoritat central: ni per crear monedes, ni per efectuar transaccions, ni per assegurar la integritat de les monedes en circulació. Podria Bitcoin ser una oportunitat per canviar les regles del joc financer i fer-les més justes? Probablement és massa aviat per avaluar aquesta possibilitat. El que de ben segur és cert és que el fenomen Bitcoin representa una oportunitat excel·lent per explicar com les matemàtiques fan possibles coses que *a priori* semblen impossibles, com són, per exemple, firmar

Aquest article es basa en la lliçó inaugural del curs acadèmic 2014–2015 de la Facultat de Matemàtiques de la Universitat de Barcelona, impartida per l'autora. Una primera versió d'aquest text va aparèixer a les Publicacions de la Universitat de Barcelona.

documents sense ser físicament present en un lloc, regular el funcionament de sistemes distribuïts sense cap autoritat central, o demostrar que saps alguna cosa sense donar-ne més informació que el fet que la saps.

La criptografia ha entrat en gairebé tots els àmbits de la societat moderna, ja que és la branca de les matemàtiques que fa possible l'ús de xarxes públiques per a assumptes privats. Mitjançant Internet, aquesta ciència ha canviat la manera com ens relacionem i gestionem el dia a dia. Donades les moltes ocasions en què la seguretat d'Internet falla, segurament ja intuïu que aquesta ciència està molt poc desenvolupada. De fet, en bona part es basa en conjectures matemàtiques.

Podem, doncs, considerar que les criptomonedes són una especulació amb peus de fang? Hi ha molts arguments en contra de la seva adopció, però la confiança en la certesa de les conjectures matemàtiques és un dels més febles perquè, en realitat, tots els serveis electrònics dels bancs i la seguretat de l'ús de paraules clau secretes es basa en aquestes mateixes conjectures. L'argument més fort en contra de les criptomonedes és que al seu darrere no hi ha cap govern que en reguli el valor. En aquesta exposició no entrarem en qüestions econòmiques ni en comparacions amb les monedes tradicionals, conegudes per *monedes fiduciàries* (*fiat money*). Per entendre millor el protocol i el potencial del sistema és millor deixar de banda les preconcepcions i pensar *outside the box*.

2 Bitcoin

L'octubre de 2008 Satoshi Nakamoto (pseudònim d'una o de més persones anònimes) va enviar un article titulat «Bitcoin: A peer-to-peer electronic cash system» a un grup de notícies de recerca en criptografia [7]. Dos mesos més tard en va publicar també la implementació de programari (o codi) obert. Es basava en altres idees de monedes electròniques que no es van arribar a realitzar, tècniques clàssiques de la criptografia i el desenvolupament de xarxes d'igual a igual (*peer-to-peer*). La idea va agradar a molts criptògrafs i programadors en general. Alguns van contribuir millorant el codi. Molts més van instal·lar-lo i van començar a efectuar transaccions i a generar més monedes virtuals segons el protocol que explicarem a continuació.

Al principi, les transaccions eren intercanvis més o menys simbòlics, com, per exemple, dotacions de premis o pagaments a canvi de programari, i, de mitjana, cada 10 minuts es generaven 50 bitcoins més. La primera compra de veritat que es va efectuar amb bitcoins va ser un any i tres mesos més tard. Va ser la compra d'una pizza a canvi de 10 000 bitcoins. Això representava el 0.4 % de tots els bitcoins que existien en aquell moment. La cotització de 10 000 bitcoins quatre anys més tard va arribar als quatre milions d'euros.

A mesura que més gent va descarregar-se el codi i va començar a efectuar transaccions, el valor dels bitcoins (BTC) va començar a pujar. Es van crear diversos mercats i negocis al voltant de Bitcoin. Avui en dia hi ha milers de negocis que accepten pagament en bitcoins.

2.1 Protocol

El protocol és bastant senzill i les eines que fa servir són eines clàssiques de la criptografia.

Els participants estan organitzats en una xarxa d'igual a igual (*peer-to-peer*): cada participant es pot comunicar amb un nombre relativament petit d'altres participants, però de tal manera que, si bona part dels usuaris reenvia la informació que rep a totes les seves connexions, aquesta informació arriba a tothom.

Absolutament totes les transaccions es guarden en un fitxer, anomenat *cadena de blocs* (*block chain*). Aquest fitxer està disponible públicament i a més es guarda i s'actualitza regularment als ordinadors de tots els usuaris.[1] Consisteix en una seqüència de blocs; cadascun conté una sèrie de transaccions de bitcoins. A més de les transaccions, cada bloc conté una quantitat de bitcoins nous en concepte de premi. Per exemple, un bloc podria contenir la informació següent:

- La Marta envia 2 BTC al Jordi.
- L'Elsa envia 1.567 5566 BTC al Gerard.
- El Jordi rep 50 BTC nous.

És important subratllar que no hi ha cap autoritat que s'ocupi de mantenir la cadena de blocs. Tots els usuaris —qualsevol persona que s'hagi baixat el programari— col·laboren en el manteniment de la informació i tothom la guarda localment al seu ordinador. Si algú intenta manipular la història, no podrà fer-ho sol perquè la informació està replicada als ordinadors de tots els usuaris.

Si hom vol enviar una quantitat de bitcoins, tot el que ha de fer és anunciar-ho a les connexions pertinents. Aquestes connexions comproven si la persona té els bitcoins que diu que vol gastar mirant, a la cadena de blocs, totes les transaccions en què ha participat en el passat, i, si és així, llavors reenvien la transacció a les seves pròpies connexions. En el fons, un bitcoin és la seva pròpia història des que es va crear, totes les transaccions que l'afecten, i la darrera indica qui n'és el propietari.

En cada moment, qualsevol participant té constància d'una sèrie de transaccions entre usuaris que encara no apareixen a la cadena de blocs. Fent servir una idea anomenada *proof of work* o *demostració de feina* (vegeu la subsecció 4.2), aquesta sèrie de transaccions es reinterpreta com un trencaclosques, la resolució del qual és, de fet, un bloc que es pot afegir al final de la cadena de blocs. El participant que aconsegueix resoldre el seu trencaclosques abans de rebre una solució d'un altre participant, envia el bloc a totes les seves connexions, que en comproven la validesa, l'afegeixen al final de la seva còpia de la cadena de blocs i el reenvien a les seves connexions.

1 Aquesta és una petita simplificació. Encara que va ser així al principi, com que la cadena s'ha fet gran (més de 20 GB el setembre de 2014) i com que hi ha usuaris que fan servir dispositius petits, com ara mòbils, avui en dia molts clients no guarden tota la informació i només contribueixen a la connectivitat de la xarxa. La seguretat del protocol depèn dels usuaris amb la versió completa.

Els trencaclosques estan dissenyats perquè, de mitjana, se'n resolgui un cada 10 minuts entre tots els participants de la xarxa. Naturalment, l'autor de la resolució pot destinar els bitcoins nous en concepte de premi (l'última transacció en el bloc, la que no té cap originari) a si mateix o a qui vulgui. En tot cas, la quantitat de bitcoins que hi ha a la xarxa creix, de mitjana, cada 10 minuts, quan es genera un bloc nou, però el valor del premi és cada cop més baix, perquè es redueix a la meitat cada 210 000 blocs. L'any 2140 el valor del premi serà menys que un *satoshi*, que és la unitat mínima de bitcoins i equival a 10^{-8} BTC. Arribat aquest punt, en comptes de guanyar monedes noves, el guanyador del premi cobrarà només unes taxes voluntàries que s'especifiquen a cada transacció. Cada participant pot fer servir el seu criteri per incloure una transacció en el bloc en què està treballant o no, segons la taxa voluntària que s'especifiqui en aquesta transacció.

Per garantir que realment és la Marta qui autoritza la transacció «La Marta envia 2 BTC al Jordi» s'aplica una tècnica estàndard de la criptografia anomenada *criptografia de clau pública*. Aquesta tècnica ens proporciona una manera de firmar contractes de manera digital. Només si la frase està firmada per la Marta, la resta d'usuaris acceptaran la transacció com a autèntica. A la secció següent veurem un mètode concret per implementar firmes digitals basat en la teoria de números.

Els trencaclosques estan basats en les funcions de *hash* (conegudes per *funcions resum)*, que també es fan servir en el context de l'autenticació d'usuaris amb paraules clau, entre moltes altres aplicacions. Explicarem aquesta tècnica a la secció 4.

2.2 Evolució

El primer mercat de bitcoins va ser un lloc web per intercanviar cromos anomenat Mt.Gox (una abreviació de Magic: The Gathering Online Exchange). Va fer fallida a principis de 2014 per problemes tecnològics, però en aquell moment ja s'havien creat moltes alternatives més fiables.

Després de Bitcoin s'han creat desenes d'altres varietats de criptomonedes inspirades en el programari de Bitcoin, o en alguns casos còpies gairebé idèntiques a Bitcoin. Un exemple és Luckycoin, que es diferencia de Bitcoin pel fet que la quantitat del premi en cada bloc és aleatòria. Un altre és Dogecoin, que va començar a finals de 2013 com una broma (*doge* es refereix a una moda d'Internet sobre fotos de gossos en diverses situacions, amb els pensaments del gos escrits en idioma de gos: «Wow. Much funny.») i en sis mesos va arribar a tenir un valor total de 24 milions d'euros (comparat amb el valor de 5 000 milions d'euros del mercat de Bitcoin). Dogecoin, a més, és notable perquè se sol fer servir per a projectes altruistes com, per exemple, una campanya per ajudar a finançar l'equip de bob de Jamaica per anar als Jocs Olímpics de Sotxi i un altre per construir un pou a Kenya.

Fins ara només hi ha hagut un problema de seguretat en el programari de Bitcoin, trobat l'any 2010, i es va arreglar ràpidament. El problema més

greu de Bitcoin que fa que els criptògrafs busquin alternatives és la falta d'anonimat en el protocol [10]. Encara que els usuaris facin servir pseudònims —en general fins i tot fan servir pseudònims diferents per rebre diners de fonts diferents—, és molt fàcil fer servir la informació que hi ha a la cadena de blocs per identificar diverses entitats i persones i el flux de diners entre elles. Una alternativa que s'està implementant per abordar aquest problema és el protocol Zerocash [1], que fa servir proves de coneixement nul (*zero-knowledge proofs*). Ho veurem a la secció 5.

3 Firmes digitals

En el món físic verifiquem la identitat de les persones amb imatges: comparem la cara de la persona amb la foto a la targeta d'identitat o les corbes d'una firma amb les de l'original. En canvi, en el món digital tractem amb números. La firma no és més que un número que envia la persona, tradicionalment anomenada Alice, junt amb el missatge que vol firmar. El receptor, tradicionalment anomenat Bob, hauria de poder comprovar que aquest número només el pot haver generat l'Alice. En principi això no sembla possible perquè qualsevol persona, tradicionalment anomenada Òscar, d'*oponent*, pot intentar endevinar números fins que n'hi surti un que passi el test que fa servir el Bob per comprovar que el missatge ve de l'Alice. En el món físic això correspon a una falsificació de la firma. Però, de fet, falsificar una firma digital és bastant més difícil que falsificar una firma física, perquè si el test del Bob és complicat, pot ser que l'Òscar hagi de provar essencialment tots els números de la mida adequada per trobar el correcte. Si el número té una longitud de 100 dígits, per exemple, i l'Òscar triga un nanosegon per comprovar que un número passa el test del Bob, en total l'Òscar trigarà $\frac{10^{100}}{10^9\times 60\times 60\times 24\times 356} > 10^{82}$ anys per provar tots els números (l'edat de l'Univers és del voltant de 10^{10} anys).

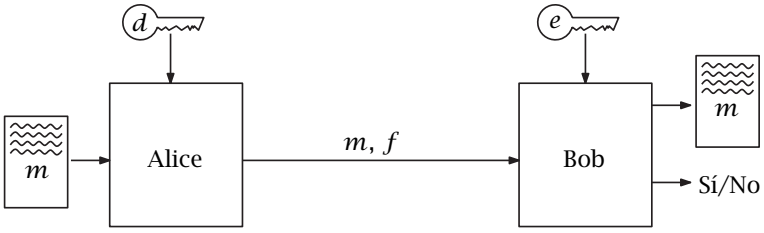


FIGURA 1: Protocol general de firmes digitals.

Una possibilitat que no es pot descartar és que, un cop coneguem els detalls del test que fa servir el Bob, se'ns faci molt més fàcil trobar un número que passi el test. Ben mirat, actualment les matemàtiques no disposen de tècniques prou fortes per demostrar que això sigui impossible per a algun d'aquests tests (o almenys no hem trobat cap test per al qual puguem demostrar-ho). Per

aquesta raó, la seguretat dels sistemes de firmes digitals encara es basa en conjectures sobre la dificultat d'alguns problemes computacionals. En aquest apartat en veurem dos exemples concrets.

Abans d'entrar en els detalls, és útil establir algunes notacions i introduir el concepte de *clau*. Hi ha dues claus que són dos números que fan servir l'Alice i el Bob durant el protocol. Una clau diem que és *privada*, perquè només la sap l'Alice, i la denotarem per d. L'altra és *pública*, perquè la pot saber qualsevol, i la denotarem per e. La clau privada es fa servir per crear el número que l'Alice envia junt amb el seu missatge m. D'aquest número se'n diu *firma* i el denotarem per f. La clau pública la genera l'Alice i l'envia al Bob (o a qualsevol altra persona) per poder comprovar que les firmes que rep de l'Alice són realment de l'Alice. Un esquema del protocol es pot veure a la figura 1.

3.1 Firmes i claus en el sistema Bitcoin

Per tenir bitcoins, l'usuari primer ha de crear una adreça (un número o una seqüència de caràcters, segons com vulgueu pensar-hi), en què es guardaran les monedes. Seria millor dir «a la qual s'associaran les monedes» perquè en realitat les monedes no tenen una realització física. Aquesta adreça, de fet, és la clau pública e del parell de claus (e, d) del protocol de firmes digitals. La clau privada d es guarda com un secret i es fa servir quan gastem els bitcoins per firmar transaccions. Cada transacció té una o més adreces d'origen i una o més adreces de destinació i s'ha de firmar amb les claus secretes de les adreces d'origen.

Per tant, si algú té la clau privada d'una adreça és com si tingués tots els bitcoins associats a aquesta adreça. Això és important perquè fa que els bitcoins siguin més aviat claus que no pas diners. Si un lladre fa una foto de la nostra clau és com si tingués la clau, però si fa una foto d'un bitllet que tenim és clar que no s'apropia d'aquest bitllet. Això ho van aprendre no fa gaire uns periodistes de la cadena de televisió Bloomberg dels Estats Units i van pagar la lliçó en bitcoins. Durant un reportatge sobre Bitcoin, van tenir l'ocurrència d'ensenyar l'imprès d'un regal de bitcoins que els havien donat. Amb la clau secreta al bell mig de la pantalla de la tele, en pocs segons aquests bitcoins van desaparèixer de la seva adreça.

3.2 Aritmètica modular

En la criptografia es fan servir números molt grans, per exemple, de centenars de dígits. Els protocols, com els de firmes digitals, demanen fer operacions amb aquests números, com ara, elevar un nombre de centenars de dígits a un altre d'una llargada comparable. El resultat és un número que no es podria guardar en un disc dur encara que estigués fet de tots els àtoms de l'Univers. Llavors, com fem aquests càlculs?

La idea és que, en comptes de fer servir l'aritmètica clàssica dels números enters, fem servir aritmètica modular. És a dir, en lloc de pensar en números

enters, pensem només en els residus que aquests números donen en dividir-los per un número especial N que escollim.

Recordeu que per denotar equivalències en l'aritmètica modular fem servir el símbol $\equiv$ en lloc del símbol $=$, i posem $(\mathrm{mod}\ N)$ al final de l'equació per denotar que les equivalències són *mòdul* N. És a dir, tots els números que donen el mateix residu de divisió per N els considerem equivalents.

Les operacions de suma, resta i multiplicació mòdul un número gran es poden implementar de manera eficient fàcilment. El càlcul de l'invers mòdul un número gran també es pot implementar de manera eficient fent servir l'algoritme d'Euclides.

Finalment, queda per implementar l'operació d'exponenciació de manera eficient. Per calcular $a^b \pmod N$ de la manera òbvia hauríem d'executar b multiplicacions, calculant el residu de divisió per N cada vegada, per evitar que els resultats es facin llargs. El truc per fer aquest procés més ràpidament s'anomena *quadratura iterada* (*repeated squaring*). En comptes de calcular $a^2, a^3, a^4, \ldots, a^b$ calculem només $a^2, a^4, a^8, a^{16}, \ldots, a^{2^{\lfloor \log_2 b \rfloor}}$. Cada membre d'aquesta sèrie és el quadrat de l'anterior. El nombre de multiplicacions per generar aquesta sèrie és, doncs, $t = \lfloor \log_2 b \rfloor$, que és comparable al nombre de dígits de b (de l'ordre dels centenars, que són poques multiplicacions per a un ordinador).

Donada aquesta sèrie, podem calcular a^b fent només t multiplicacions més. Representem b com la suma d'un subconjunt dels números $\{1, 2, 4, 8, 16, \ldots, 2^{\lfloor \log_2 b \rfloor}\}$, és a dir,

$$b = \sum_{i=0}^{t} b_i \times 2^i,$$

per a alguns $b_0, b_1, \ldots, b_t \in \{0, 1\}$ (la representació binària de b).

Les t multiplicacions finals són:

$$a^b = a^{\sum_{i=0}^{t} b_i \times 2^i} = \prod_{i=0}^{t} a^{b_i \times 2^i} = \prod_{i \in \{0,\ldots,t\} : b_i = 1} a^{2^i}.$$

Per explicar el primer protocol de firmes digitals, que és RSA, necessitarem també el teorema d'Euler: per a cada N hi ha un número anomenat $\phi(N)$, tal que per a qualsevol x que no té divisors comuns amb N es compleix que

$$x^{\phi(N)} \equiv 1 \pmod N.$$

La funció d'Euler $\phi(N)$ és la quantitat de números més petits que N que no tenen divisors comuns amb N. Si N és un número primer, és clar que $\phi(N) = N - 1$. Si N és el producte de dos números primers p i q, com és el cas que ens interessa per entendre RSA, podem comprovar que

$$\phi(N) = (pq - 1) - (p - 1) - (q - 1) = (p - 1)(q - 1),$$

perquè, de tots els $pq-1$ números més petits que N, n'hi ha $p-1$ que són divisibles per q, $q-1$ que són divisibles per p i la resta no tenen divisors comuns amb N.

Necessitarem el corol·lari del teorema d'Euler següent.

PROPOSICIÓ 1. *Si N és producte de dos primers diferents p i q i α és un enter qualsevol, aleshores per a tot enter m es compleix*

$$m^{\phi(N)\alpha+1} \equiv m \pmod{N}.$$

PROVA. Hi ha tres casos:

1. Si $\mathrm{mcd}(m,N) = 1$, el teorema d'Euler ens diu que $m^{\phi(N)} \equiv 1 \pmod{N}$. Tenim
$$m^{\phi(N)\alpha+1} = (m^{\phi(N)})^{\alpha} \times m \equiv 1^{\alpha} \times m \equiv m \pmod{N}.$$
2. Si $\mathrm{mcd}(m,N) = N$, l'equivalència és certa perquè les dues bandes són 0.
3. Queda el cas que $\mathrm{mcd}(m,p) = p$ i $\mathrm{mcd}(m,q) = 1$ (o viceversa). És suficient demostrar que $m^{\phi(N)\alpha+1} \equiv m \pmod{p}$ i $m^{\phi(N)\alpha+1} \equiv m \pmod{q}$. La primera congruència és obvia, i la segona és conseqüència del teorema d'Euler com en el cas anterior, tenint en compte que $\phi(q) = q-1$,
$$m^{\phi(N)\alpha+1} = (m^{q-1})^{(p-1)\alpha} \times m \equiv 1^{(p-1)\alpha} \times m \equiv m \pmod{q}.$$

Amb aquestes eines per fer càlculs amb números grans en aritmètica modular, ja podem explicar el primer algoritme de firmes digitals.

3.3 Firmes mitjançant RSA

Un dels primers sistemes de firmes digitals va ser el de Ronald Rivest, Adi Shamir i Len Adleman de 1978, conegut per RSA [9]. Per crear les claus, l'Alice escull dos números primers p i q de molts dígits (centenars), que són secrets, i en calcula el producte

$$N = p \times q.$$

El producte N és informació pública, però no els números p i q. Una de les conjectures en què es basa el mètode és que si només tenim N, trobar p i q (*i. e.* factoritzar N) és un problema computacionalment difícil.[2]

Llavors, l'Alice escull dos números d i e, el d serà secret, el e, públic, tals que per a qualsevol missatge m el valor de $(m^d)^e$ mòdul N (el qual es pot calcular amb $2\log(d) + 2\log(e)$ multiplicacions de números de la mateixa mida que N) és el mateix que m. És a dir,

$$(m^d)^e \equiv m \pmod{N}.$$

2 Si un dia es construïssin ordinadors quàntics, amb aquests sí que podríem factoritzar números grans fent servir l'algoritme de Shor [11].

En el cas de RSA, només l'Alice pot calcular $\phi(N) = (p-1)(q-1)$ perquè només ella coneix p i q. Havent calculat $\phi(N)$, pot escollir e i d tals que

$$ed \equiv 1 \pmod{\phi(N)}.$$

La manera de fer-ho és trobar e que no tingui divisors comuns amb $\phi(N)$ (escollir e aleatòriament entre 1 i $\phi(N)-1$ funciona) i, mitjançant l'algoritme d'Euclides, calcular el seu invers mòdul $\phi(N)$, que serà d.

Un cop l'Alice té un parell de números amb aquesta propietat, el protocol és el següent: fent servir la clau secreta d, l'Alice calcula la firma

$$f = m^d \pmod{N}$$

i l'envia junt amb el missatge m.[3] El Bob agafa la firma i l'eleva a e mòdul N (recordeu que N és públic). Si el resultat és m, accepta la firma com a autèntica; si no, la rebutja.

Per convèncer-nos que el protocol és correcte només queda comprovar que $m^{de} \equiv m \pmod{N}$, el qual és conseqüència directa de la proposició 1.

Si l'Òscar vol firmar un altre missatge m fent veure que és l'Alice, necessitarà la clau d. La seguretat del protocol RSA depèn de la conjectura que és computacionalment difícil trobar d si només coneixes e i N (es pot comprovar que si pots factoritzar N, llavors sí que pots trobar d).

Cal mencionar que la mateixa idea es fa servir per xifrar i desxifrar missatges. El Bob pot xifrar els missatges que envia a l'Alice elevant-los a la clau pública e. És a dir, el Bob envia el missatge $\hat{m} = m^e \pmod{N}$. Només l'Alice pot desxifrar el missatge perquè té la seva clau privada d i pot calcular $\hat{m}^d \equiv \left((m^e)^d\right) \equiv m \pmod{N}$. D'aquí vénen els noms de les claus e i d: d'*encriptació* i *desencriptació*.

3.4 Firmes mitjançant ECDSA

El protocol de firmes digitals que fa servir Bitcoin no és RSA perquè els creadors van decidir optar per un protocol més modern i menys habitual però que comporta alguns avantatges com ara càlculs més eficients i claus més petites (per aconseguir la mateixa seguretat). És l'ECDSA o *Eliptic Curve Digital Signature Algorithm*, que va ser dissenyat els anys vuitanta ([5] i [6]), i es va popularitzar a principis d'aquest segle. La conjectura matemàtica en la qual es basa aquest protocol pertany a l'aritmètica dels grups associats a corbes el·líptiques sobre cossos finits. Concretament, es basa en la complexitat computacional del problema del logaritme discret.

3.4.1 Corbes el·líptiques El conjunt dels punts (x, y) que satisfan una equació no singular $y^2 = x^3 + ax + b$, a més d'un punt especial O que ens podem imaginar com l'infinit, és una corba el·líptica amb paràmetres a i b. Vegeu [12]

3 En realitat per calcular la firma, en els protocols de RSA i d'ECDSA, no es fa servir el missatge m original, sinó un *hash* del missatge $H(m)$ que té una llargada fixa. Fem servir m per comoditat. A la secció següent explicarem què és un *hash*.

per a la definició general de corba el·líptica.[4] Denotem aquest conjunt per $\mathcal{E}$. En el context de la criptografia, x i y són enters i l'aritmètica és la d'un cos finit, per exemple, la dels enters mòdul p per a algun número primer p. Per tant, l'equació que els punts satisfan és $y^2 \equiv x^3 + ax + b \pmod{p}$. Així, si $p = 23$, $a = 1$, $b = 0$, els punts de la corba el·líptica són

$$\begin{aligned}\mathcal{E} = \{&(0,0),(1,5),(1,18),(9,5),(9,18),(11,10),\\ &(11,13),(13,5),(13,18),(15,3),(15,20),(16,8),\\ &(16,15),(17,10),(17,13),(18,10),(18,13),(19,1),\\ &(19,22),(20,4),(20,19),(21,6),(21,17),O\}.\end{aligned}$$

Es pot definir una operació «$\odot$» sobre dos punts de la corba el·líptica de manera que $\mathcal{E}$ equipat amb aquesta operació sigui un grup abelià. El punt O en seria l'element identitat. Aquesta operació admet una interpretació geomètrica, il·lustrada a la figura 2. Es considera la recta que passa per P i Q i el tercer punt R de tall amb la corba. Aleshores $P \odot Q = -R$ on $-R$ és el simètric de R respecte l'eix de les x, és a dir, $P \odot Q = (r_x, -r_y)$ amb $(r_x, r_y) = R$. El punt $-R$ és l'oposat de R amb l'operació $\odot$ i es pot pensar com la tercera intersecció de la recta que passa per R i O amb la corba (les rectes per O són les rectes verticals).

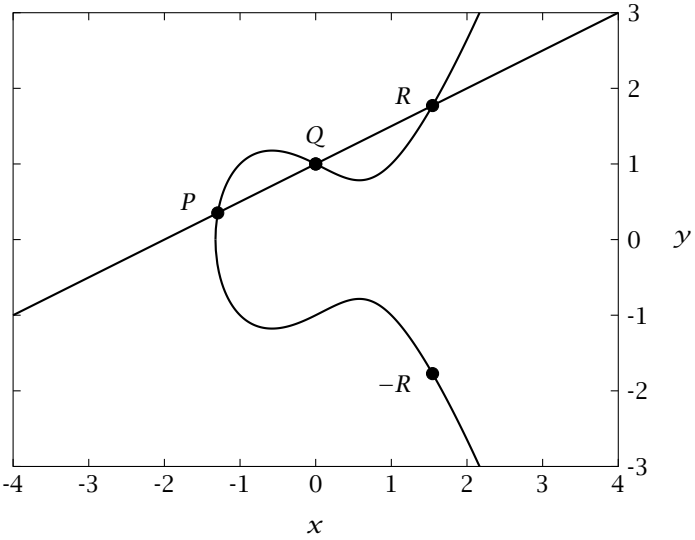


FIGURA 2: L'operació $\odot$ en una corba el·líptica amb equació $y^2 = x^3 - x + 1$.

En característica diferent de 2 i 3, es poden donar les coordenades de $P \odot Q$ de manera explícita. Suposem que $P = (p_x, p_y)$ i $Q = (q_x, q_y)$ són punts d'una corba el·líptica $\mathcal{E}$. Si $p_x = q_x$ i $p_y = -q_y$, llavors $P \odot Q = O$; en cas contrari,

4 Cal dir que en característica 2 o 3 no totes les corbes el·líptiques es poden reduir a l'expressió $y^2 = x^3 + ax + b$.

$P \odot Q = (r_x, r_y)$ on

$$\begin{aligned} r_x &:= s^2 - p_x - q_x, \\ r_y &:= (p_x - r_x)s - p_y \end{aligned}$$

per a

$$s := \begin{cases} (q_y - p_y)(q_x - p_x)^{-1}, & \text{si } P \neq Q, \\ (3p_x^2 + a)(2p_y)^{-1}, & \text{si } P = Q. \end{cases}$$

Farem servir la notació

$$S^t := \underbrace{S \odot S \odot S \odot \cdots \odot S}_{t}.$$

El problema del logaritme discret és: donats dos punts de la corba R i S, trobar un enter t tal que $S^t = R$. El t s'anomena *logaritme* en associació amb el logaritme continu i l'operació de multiplicació. El problema del logaritme discret, de fet, es pot plantejar a qualsevol grup. La seguretat de la criptografia de corbes el·líptiques es basa en la conjectura que trobar aquest t, donats R i S, és computacionalment difícil.

3.4.2 Protocol de firmes digitals El protocol té com a paràmetres (públics) la corba el·líptica definida per a, b i p, a més d'un element del grup amb ordre primer conegut. Diguem que aquest element és G i el seu ordre és n, és a dir, $G^n = O$.

La clau privada de l'Alice és un enter d escollit aleatòriament entre 0 i n. La seva clau pública és el punt $Q = G^d$. Per calcular-la l'Alice fa servir la quadratura iterada com quan elevem enters a una potència gran. El pas contrari, calcular d donat Q, és molt més difícil —concretament, és equivalent al problema del logaritme discret.

Donat un missatge m, l'Alice primer prepara un enter aleatori k secret que és nou per a cada nou missatge, s'assegura que k és coprimer amb n, i calcula $(p_x, p_y) = G^k$. Després fa servir la clau privada per calcular la firma, que en aquest cas té dues parts:

$$(f_1, f_2) := (p_x, (m + dp_x)k^{-1}) \pmod{n}.$$

Si f_1 o f_2 són zero, l'Alice tria un altre k.

El Bob rep el missatge m i la firma (f_1, f_2). Per verificar que la firma és autèntica el Bob calcula el punt

$$T = (t_x, t_y) := G^{mf_2^{-1}} \odot Q^{f_1 f_2^{-1}},$$

i comprova que $t_x = f_1$. Si la firma és vàlida el test surt correcte perquè $T = G^k$:

$$\begin{aligned} T &= G^{mf_2^{-1}} \odot Q^{f_1 f_2^{-1}} \\ &= G^{mf_2^{-1}} \odot G^{df_1 f_2^{-1}} \\ &= G^{(m+dp_x)f_2^{-1}} \\ &= G^k. \end{aligned}$$

4 Funcions de hash

L'altre ingredient principal en el disseny de Bitcoin és el concepte de *demostracions de feina* i, alhora, la creació de monedes noves. La tecnologia, en aquest cas, és molt senzilla i es basa en una idea ja força utilitzada: les funcions de hash.

Les funcions de *hash* tenen un munt d'aplicacions en el món digital. Una funció de hash pren d'entrada seqüències o fitxers de qualsevol mida i retorna seqüències de caràcters d'una mida fixa i petita, com ara 256 bits (o equivalentment 64 caràcters hexadecimals, 0–9 i a–f). Per il·lustrar-ho amb un exemple, imagineu-vos que dos amics que viuen lluny l'un de l'altre tenen fitxers que contenen la mateixa pel·lícula però no saben si els fitxers són idèntics. Per estar convençuts que ho són no cal que s'enviïn un dels fitxers sencer, que pot tenir una mida d'uns quants gigues. Els pot ser suficient aplicar una funció predeterminada, la funció de hash, que s'aplica al fitxer i dóna una línia de 256 bits, anomenada *el hash del fitxer*, que no té cap sentit o cap relació òbvia amb el contingut del fitxer. Tot i així, com que la funció és determinista, si els dos fitxers són idèntics, aquests 256 bits seran els mateixos. Les funcions de hash criptogràfiques normalment estan dissenyades de manera que si els dos fitxers es diferencien, encara que sigui només una mica, els dos hashos seran completament diferents en pràcticament tots el casos.[5] Per exemple, el hash de la frase de Douglas R. Hofstadter «If you think this sentence is confusing, then change one pig» és:

```
b0c840435c3ce497fc451f333ad18702443c1d822161150b8fa23bdb4ace97f9
```

i el hash de la mateixa frase amb punt final és:

```
380c4122fc5a3211bf801d8a02cc34928fecfc3732f1b4c6183d9ca608805b7d
```

De la mateixa manera, si els dos hashos són idèntics, podem estar pràcticament segurs que els dos fitxers són els mateixos fins a l'últim bit.

Encara que hi ha molts fitxers que tenen el mateix hash (perquè hi ha molts més fitxers possibles que seqüències de 256 bits), una bona funció de hash criptogràfica té la propietat que és molt difícil trobar dos fitxers amb el mateix hash. D'aquesta propietat se'n diu *resistència a col·lisions*. Una altra propietat d'aquestes funcions és que, si tenim el hash, és molt difícil recuperar el fitxer, o més ben dit, trobar algun fitxer que tingui aquest hash. Aquesta propietat s'anomena *resistència a inversions*.

Aquí ens trobem amb una altra conjectura. L'existència de funcions de hash que tenen aquestes dues propietats no està demostrada matemàticament. A la pràctica, al llarg dels anys s'han dissenyat diverses funcions de hash i algunes han estat «trencades» en el sentit que s'han trobat col·lisions o algoritmes

5 Hi ha funcions de hash per a altres aplicacions que tenen propietats diferents, per exemple, els locality-sensitive hashes, que funcionen exactament al revés: fitxers semblants tenen el mateix hash. En aquest article quan diem *hash* entendrem *hash criptogràfic*.

eficients per calcular-ne inversos. Actualment, la funció de hash més utilitzada es diu SHA-256 i és la que fa servir el protocol de Bitcoin.

Curiosament, les constants internes que fan servir les funcions de hash tenen explicacions senzilles, com per exemple els dígits del desenvolupament de π o els dígits de les arrels quadrades dels primers números primers. S'han escollit així per convèncer el públic que la funció no està dissenyada per cap agent maliciós, per exemple la NSA (National Security Agency), que tingui una clau secreta amb la qual pugui invertir la funció (cosa que igualment no es pot descartar del tot).

Els resultats d'aplicar una bona funció de hash a diferents fitxers són números que semblen generats a l'atzar. Si suposem que aquesta fos realment la distribució dels resultats, podem calcular la probabilitat de trobar-nos dos fitxers amb el mateix hash quan generem un gran nombre de hashos. Aquest experiment és conegut per *experiment dels aniversaris*. Imaginem-nos que els fitxers són persones i que els seus hashos són els seus aniversaris. A quantes persones necessitem preguntar-los l'aniversari per tenir una bona probabilitat de trobar-ne dues amb el mateix aniversari? Resulta que amb 23 persones ja tenim una probabilitat superior al 50 % d'èxit. D'aquest fet se'n diu *paradoxa dels aniversaris*.

Ens interessa el resultat del mateix experiment si l'any, en comptes de tenir 365 dies, en tingués molts més. Per posar un exemple, en el cas de la funció SHA-256, el hash del fitxer pot ser qualsevol número de 256 bits. D'aquests n'hi ha $2^{256} > 10^{76}$.

A continuació aproximem la probabilitat de col·lisió si tenim n dies diferents a l'any i m persones. Demostrarem que la probabilitat que dos aniversaris coincideixin passa de menys del 50 % a més del 50 % dins l'interval $m \in [\sqrt{n}, 2\sqrt{n}]$.

Denotem la probabilitat que hi hagi una col·lisió per $q(n,m)$ i la probabilitat que no n'hi hagi cap per $p(n,m) = 1 - q(n,m)$. Si les primeres k persones tenen aniversaris diferents, la probabilitat que l'aniversari de la persona següent a la qual ho preguntem coincideixi amb alguns dels k anteriors és k/n. Hi ha col·lisió si un d'aquests casos succeeix: la primera col·lisió es produeix o bé a l'hora de preguntar a la segona persona pel seu aniversari, o bé a l'hora de preguntar a la tercera, o bé a l'hora de preguntar a la quarta, etc. Per tant, la probabilitat que algun d'aquests casos es doni és la suma de probabilitats de tots els casos. D'altra banda, la probabilitat de tenir la primera coincidència en preguntar a la persona k-èsima és menor o igual que $(k-1)/n$. Per tant,

$$q(n,m) \leq \frac{1}{n} + \frac{2}{n} + \cdots + \frac{m-1}{n} = \frac{1}{n} \times \frac{(m-1)m}{2}.$$

Substituint m per $\sqrt{n}$ (suposant, per simplificar, que n és un quadrat perfecte), obtenim que:

$$q(n,\sqrt{n}) \leq \frac{(\sqrt{n}-1)\sqrt{n}}{2n} < \frac{1}{2}.$$

Per tant, si $m < \sqrt{n}$, la probabilitat de col·lisió encara està per sota del 50 %.

D'altra banda, podem fitar la probabilitat que no hi hagi cap col·lisió pensant en les últimes $m/2$ persones i exigint que els seus aniversaris siguin diferents dels de les primeres $m/2$ (suposant, per simplificar, que m és parell). Per tant,

$$p(n,m) \leq \left(\frac{n-m/2}{n}\right)^{m/2}.$$

Posem $m = 2\sqrt{n}$ i tenim

$$p(n,2\sqrt{n}) \leq \left(1-\frac{1}{\sqrt{n}}\right)^{\sqrt{n}} < e^{-1} < \frac{1}{2}.$$

Per tant, si $m \geq 2\sqrt{n}$ es compleix $p(n,m) < 1/2$ i $q(n,m) > 1/2$.

En el cas de SHA-256, $n > 10^{76}$, i per tant per tenir una probabilitat del 50% de veure dos fitxers amb el mateix hash hem de provar més de 10^{38} fitxers. Això fa que sigui pràcticament impossible trobar dos fitxers amb el mateix hash fent servir aquest mètode.

4.1 Paraules clau

Una de les aplicacions més importants de les funcions de hash és el seu ús per guardar paraules clau d'usuaris. La bona pràctica és evitar guardar les paraules clau tal com són, en un fitxer, perquè hi ha el perill que algú el pugui obrir. La manera de protegir-se d'aquest atac és la següent: en comptes de guardar les paraules clau, se'n poden guardar els hashos. Quan l'usuari envia la paraula clau c al servidor, aquest aplica la funció de hash H i compara el resultat $H(c)$ amb el hash que té guardat en el fitxer de hashos. D'aquesta manera encara que algú obtingués el fitxer, igualment no hi tindria accés perquè no podria recuperar les paraules que generen aquests hashos.

Si donem el disseny per fet, un atacant podria generar un diccionari de moltes de les possibles paraules clau (típicament combinacions d'uns vuit caràcters) junt amb els seus hashos i consultar aquest diccionari per recuperar les paraules clau, donats els seus hashos. Per evitar aquest atac, junt amb el hash es guarda un número aleatori s (relativament gran), anomenat *sal*, i el hash es calcula sobre la paraula clau concatenada amb la sal.

Finalment, per evitar que algú pugui fer moltes proves amb paraules clau de manera automàtica, la funció de hash s'aplica recursivament unes quantes vegades. En lloc de $H(c+s)$ es guarda $H(H(H\ldots H(c+s)\ldots))$, amb la funció de hash aplicada unes mil vegades o més per tal que la comprovació trigui un temps que no serà notable per a un usuari honest però que pot impedir un atacant automàtic.

4.2 Demostracions de feina en Bitcoin

El que fa Bitcoin especial és un mètode enginyós per aconseguir que la verificació de les transaccions sigui una tasca distribuïda, compartida entre tots els participants, que no s'hagin de refiar d'un banc central, i crear incentius

per col·laborar en aquesta tasca. La tècnica per aconseguir-ho es basa en les funcions de hash.

Com ja hem explicat a la introducció, el primer que fa un usuari quan rep una transacció és verificar-la. Tot i així, una transacció de bitcoins es converteix en oficial només quan la transacció s'afegeix a la cadena de blocs com a part d'un bloc. El procés de creació de blocs, el qual anomenem *trencaclosques*, és una tasca d'una gran complexitat computacional, que expliquem a continuació.

La tasca consisteix a trobar una seqüència de caràcters tal que, si adjuntem el contingut del bloc (la sèrie de transaccions) a aquesta seqüència i apliquem la funció de hash SHA-256, el resultat és un número més petit que un número donat: *l'objectiu* (*target*). La mida de l'objectiu determina la dificultat del problema i es regula cada dues setmanes per tal que algú a la xarxa trobi una solució, de mitjana, cada 10 minuts. L'objectiu és cada cop més petit perquè la tecnologia dels processadors d'ordinadors millora, i cada cop hi ha més usuaris i més recursos computacionals empleats a la tasca.

Com veieu, la tasca és molt semblant a la inversió de hashos. Per tant, el més probable és que ningú no tingui cap altra manera de resoldre'l que no sigui provant múltiples seqüències aleatòries de caràcters fins que una d'elles tingui un hash amb la propietat desitjada. El procés per resoldre aquests trencaclosques computacionals es coneix per *mineria* (*mining*), perquè amb cada bloc es creen bitcoins nous (el premi) i recorda la tasca de buscar or en una mina (una tasca bastant feixuga i inútil per si sola).

Per què cal que la tasca de crear blocs nous sigui computacionalment difícil? La idea és que d'aquesta manera s'evita que un participant domini el procés de verificació i manipuli la cadena de blocs, per exemple incloent-hi dues transaccions diferents que fan servir els mateixos bitcoins (un atac conegut per *doublespending*). La idea no és totalment nova i es coneix per *demostració de feina* (*proof of work*). Originalment es va inventar per combatre el correu brossa (*spam*) [2]. En aquest context, per enviar un correu, primer es demana al servidor que l'envia que resolgui un problema computacional que normalment requereix uns segons; així s'evita que algú pugui enviar un gran nombre de correus en molt poc temps.

Sovint passa que dos blocs, tots dos vàlids, es creen aproximadament al mateix temps. Llavors hi ha una bifurcació en la cadena de blocs i alguns participants treballen per continuar una cadena mentre que d'altres treballen per continuar-ne l'altra. El protocol exigeix que es continuï la que sigui més llarga. Normalment, en pocs minuts (suficients per crear tres o quatre blocs nous) una de les dues branques guanya l'altra en longitud i ja es pot considerar que és la cadena oficial perquè la segona mai no arribarà a atrapar la primera.

5 Tecnologies criptogràfiques més avançades

Com ja hem destacat a la introducció, és important pensar en Bitcoin com el primer pas important (o almenys el primer pas d'impacte real) cap al desenvolupament de protocols distribuïts de caràcter econòmic o financer. Aquest és

un tema de recerca actiu i no pas una qüestió tancada. En aquesta secció farem una introducció breu a una tecnologia criptogràfica encara més sofisticada que té el potencial d'acabar eliminant alguns dels defectes actuals de Bitcoin.

En la seva encarnació actual, Bitcoin proporciona molt poca anonimitat als usuaris. Tota la informació de les transaccions està disponible públicament. Però, com veurem, això no és un tret necessari, perquè es pot resoldre fent servir la tecnologia de *proves de coneixement nul* (*zero-knowledge proofs*).

5.1 Proves de coneixement nul

De vegades volem demostrar a algú que sabem una cosa sense donar-ne més informació que el fet que la sabem. Un exemple del món físic (per distingir-lo del món dels ordinadors) pot ser la tasca de demostrar a un nen que sabem on és en Wally sense revelar-ne la localització en el pòster. Com ho farem? Si disposéssim d'una fotocopiadora, podríem fer una còpia del pòster, tallar la figura del Wally, destruir la resta de la còpia, i només ensenyar la figura al nen [8]. Perquè sigui un bon protocol, caldria que no donés cap informació sobre la ubicació del Wally al nen, i també convèncer-lo que no hem fet trampa. En el món físic no és fàcil fer-ho de manera precisa. Per exemple, hem de posar condicions sobre el que pot i no pot haver-hi dins l'habitació de la fotocopiadora perquè el nen estigui segur que, posem per cas, no hem retallat la figura del Wally d'un altre pòster.

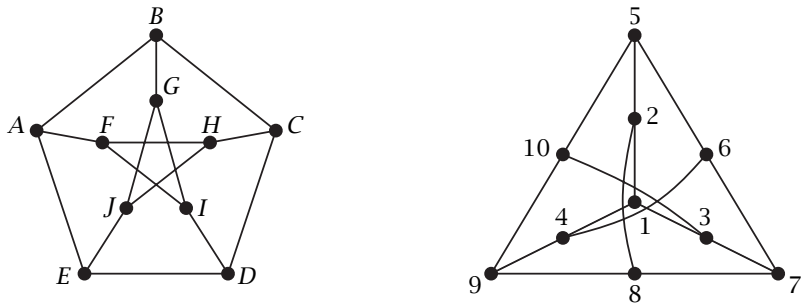


FIGURA 3: Dos grafs que són isomorfs.

El Premi Turing de l'any 2012 (considerat l'equivalent del Premi Nobel en la informàtica) es va atorgar als inventors de la definició matemàtica del concepte de *proves de coneixement nul*. En un article de l'any 1985, Goldwasser, Micali i Rackoff [4] van donar el primer exemple d'aquest tipus de demostració per a dos problemes computacionals de la teoria de números: el problema del residu quadràtic i el problema del no-residu quadràtic. Donat un número a i una base N, es vol demostrar que existeix (pel problema del residu quadràtic) o que no existeix (pel problema del no-residu quadràtic) un número b tal que $b^2 \equiv a \pmod{N}$.

La definició de *prova de coneixement nul* fa servir el concepte de *sistema de demostracions interactives de la complexitat computacional*. Per no haver d'entrar en aquests temes, aquí en farem una descripció informal mitjançant un exemple. L'any 1986 Goldreich, Micali i Wigderson [3] van presentar les primeres proves de coneixement nul per a problemes que no venien de la teoria de números. En concret, ho van fer per als problemes d'isomorfisme i no-isomorfisme de grafs.[6]

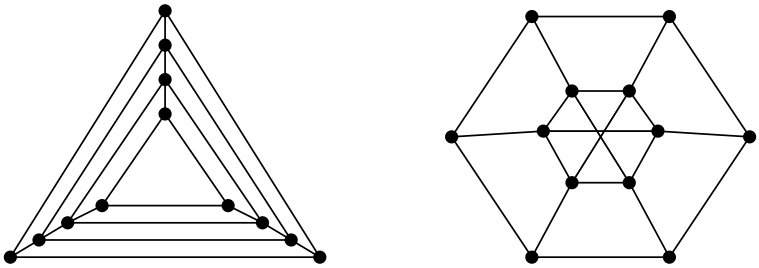


FIGURA 4: Dos grafs que no són isomorfs.

Diem que dos grafs són isomorfs si existeix una correspondència (bijecció) entre els vèrtexs dels dos grafs tal que cada parell de vèrtexs connectats en un dels grafs correspon a un parell de vèrtexs connectats en l'altre i cada parell de vèrtexs no connectats en l'un correspon a un parell de vèrtexs no connectats en l'altre. D'aquest tipus de correspondència se'n diu *isomorfisme*. També podem pensar que els dos grafs realment són representacions diferents del mateix graf, amb diferents etiquetes als vèrtexs. Per exemple, a la figura 3, una correspondència entre els dos grafs que és un isomorfisme és: A amb 1, B amb 2, C amb 5, D amb 6, E amb 4, F amb 3, G amb 8, H amb 10, I amb 7, J amb 9. D'altra banda, els dos grafs de la figura 4 no són isomorfs. Una manera de convèncer-nos d'aquest fet és notar que un dels grafs conté triangles i l'altre no.

Per a grafs petits, sempre podem comprovar si dos grafs són isomorfs o no mirant totes les possibles correspondències entre els vèrtexs. Per a dos grafs de n vèrtexs hi ha $n!$ possibles correspondències i, per tant, aquesta estratègia no és pràctica per a n gran. Hi ha estratègies que funcionen per a molts parells de grafs, però no es coneix cap algoritme eficient (que trigui temps polinòmic en la mida dels grafs) que pugui detectar tots els parells de grafs isomorfs.

Suposem que tenim dos jugadors: la demostradora (*prover*) Peggy i el verificador (*verifier*) Vic. La Peggy coneix un isomorfisme entre els dos grafs G_1 i G_2 i vol demostrar al Vic que els grafs són isomorfs sense donar-li cap informació d'aquest isomorfisme, tret del fet que existeix. El protocol és el següent.

6 A més, van provar que aquestes demostracions existeixen per a tots els llenguatges NP, començant pel problema de coloració de grafs.

La Peggy envia al Vic un graf H que és isomorf a G_1 i a G_2. Perquè no doni cap informació al Vic sobre l'isomorfisme entre G_1 i G_2, la Peggy pot generar-lo etiquetant de manera aleatòria els vèrtexs de G_1. Com que ella sap com ha generat H, ella té un isomorfisme entre els vèrtexs de G_1 i de H. Com que també coneix un isomorfisme entre els vèrtexs de G_1 i G_2, també pot trobar un isomorfisme entre els vèrtexs de H i G_2.

En el segon pas, el Vic demana a la Peggy que li ensenyi l'isomorfisme entre H i G_1 o entre H i G_2. Ell escull quin dels dos li demana.

En cap cas la Peggy li envia tots dos isomorfismes perquè, amb tots dos, el Vic podria recuperar l'isomorfisme entre G_1 i G_2. Però el que és clar és que, si els dos grafs són realment isomorfs, la Peggy sempre pot enviar l'isomorfisme que li hagin demanat.

Si la Peggy intenta convèncer el Vic que dos grafs són isomorfs quan realment no ho són, el Vic l'enxamparà almenys en el 50 % dels casos independentment del que faci la Peggy. Per estar encara més segur que la Peggy no menteix, el Vic pot repetir els dos passos tantes vegades com vulgui. Si en k repeticions amb diferents H la Peggy sempre aconsegueix enviar-li un isomorfisme, el Vic estarà $100 \times \left(1 - \frac{1}{2^k}\right)$ % segur que la Peggy no menteix (perquè la probabilitat que ella endevini totes les preguntes del Vic és 1 entre 2^k). Per exemple, amb $k = 10$ repeticions, el Vic té una probabilitat del 99,9 % d'enxampar la Peggy.

Aquest protocol té les propietats següents que fan que sigui una prova de coneixement nul:

- Si G_1 i G_2 són isomorfs, el Vic sempre estarà convençut d'aquest fet al final.
- Si G_1 i G_2 no són isomorfs, el Vic estarà convençut que ho són només amb una probabilitat mínima (tan petita com vulgui).
- La comunicació del protocol tal com la veuria un tercer la pot generar el Vic tot sol i, per tant, el Vic no obté cap informació que no tingui ja.

La propietat de coneixement nul és l'última en aquesta llista i és la més difícil de demostrar en la majoria dels casos. S'ha de demostrar que hi ha una simulació eficient de la comunicació. És a dir, es pot generar una seqüència d'intercanvis amb la mateixa distribució de probabilitat que la del protocol real, i a més això es pot fer tenint no més informació que la que té el Vic. En el cas especial de l'isomorfisme de grafs això resulta fàcil. El Vic pot simular tota la comunicació generant primer les seves preguntes i després els grafs H isomorfs al graf que correspon a cada pregunta, junt amb l'isomorfisme entre H i aquest graf.

5.2 Proves de coneixement nul per a l'anonimitat de les criptomonedes

Una de les criptomonedes més sofisticades, la Zerocash, es va presentar la primavera de 2014 i la seva descripció està disponible a [1]. La idea al darrere de Zerocash és fer servir proves de coneixement nul per demostrar que es té

una moneda sense revelar quina és. D'aquesta manera les transaccions no es poden associar les unes amb les altres i no es poden seguir els traços de les monedes. S'aconsegueix l'anonimitat que li falta al protocol de Bitcoin. Les proves de coneixement nul són bastant més complicades que les que hem vist aquí, per diverses raons. Primer, no són interactives. Segon, estan dissenyades per ser molt més curtes perquè s'han de guardar en la cadena de blocs. I tercer, les afirmacions que s'han de demostrar són bastant més complicades perquè comporten demostrar que un programa s'ha executat correctament.

El Zerocash és un exemple de moneda que encara no s'ha implementat, però demostra les possibilitats de sofisticació que es poden arribar a incorporar a la idea original de Bitcoin si explotem tot el nostre coneixement matemàtic modern.

6 Rellevància

Bitcoin és un dels molts canvis econòmics i socials que es produeixen gràcies a les noves tecnologies. Al segle XXI veiem les llavors d'una societat més comunicativa i més funcional. Alguns exemples són: les inversions de la ciutadania en projectes d'interès comú mitjançant el micromecenatge (*crowdfunding*) en plataformes com Kickstarter; el periodisme obert mitjançant blogs i Twitter; les estructures d'organització de la informació basades en reputació (*reputation systems*) en plataformes com Stack Overflow i Quora. Una altra és la comunitat econòmica que s'està formant al voltant de Bitcoin.

Les possibilitats de canvi que ens garanteix la connectivitat immediata proporcionada per Internet són infinites, però és un terreny desconegut que, a més d'oportunitats, comporta perills. Un d'aquests perills és que no tothom pugui participar en la formulació de les estructures noves i que sigui només una elit tecnològica o financera la que faci servir aquestes oportunitats per crear un món paral·lel amb una democràcia selectiva. És un repte per als joves i per als educadors garantir que la població pugui entendre i actuar envers aquests canvis, que, a més, es produeixen a un ritme cada cop més vertiginós.

Referències

[1] BEN-SASSON. E.; CHIESA, A.; GARMAN, C.; GREEN, M.; MIERS, I.; TROMER, E.; VIRZA, M. «Zerocash: Decentralized Anonymous Payments from Bitcoin». A: *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. Washington, DC: IEEE Computer Society, 2014, 459–474.

[2] DWORK, C.; NAOR, M. «Pricing via Processing or Combatting Junk Mail». A: BRICKELL, E. F. (ed.). *Advances in Cryptology - CRYPTO' 92* (12th Annual International Cryptology Conference Santa Barbara, California, USA, August 16–20, 1992 Proceedings). Berlín: Springer, 1983, 139–147. (Lecture Notes in Comput. Sci.; 740)

[3] Goldreich, O.; Micali, S.; Wigderson, A. «Proofs that yield nothing but their validity and a methodology of cryptographic protocol design». A: *Proceedings of the 27th annual Symposium on Foundations of Computer Science (FOCS)*. Washington, DC: IEEE Computer Society, 1986, 174–187.

[4] Goldwasser, S.; Micali, S.; Rackoff, C. «The knowledge complexity of interactive proof systems». A: *Proceedings of the 17th annual ACM symposium on Theory of Computing* (Conference STOC'85, Providence, RI, USA, May 06–08, 1985). Nova York: ACM, 1985, 291–304.

[5] Koblitz, N. «Elliptic curve cryptosystems». *Math. Comp.*, 48 (177) (1987), 203–209.

[6] Miller, V. S. «Use of elliptic curves in cryptography». A: *Advances in Cryptology - CRYPTO' 85 Proceedings*. Berlín: Springer, 1986, 417–426. (Lecture Notes in Comput. Sci.; 218)

[7] Nakamoto, S. «Bitcoin: A peer-to-peer electronic cash system». Report, `bitcoin.org` (2008).

[8] Naor, M.; Naor, Y.; Reingold, O. «Applied kid cryptography or how to convince your children you are not cheating». *Journal of Craptology*, 0 (1) (1999).

[9] Rivest, R. L.; Shamir, A.; Adleman, L. «A method for obtaining digital signatures and public-key cryptosystems». *Comm. ACM*, 21 (2) (1978), 120–126.

[10] Ron, D.; Shamir, A. «Quantitative Analysis of the Full Bitcoin Transaction Graph». A: Sadeghi, A.-R. (ed.). *Financial Cryptography and Data Security* (17th International Conference, FC 2013, Okinawa, Japan, April 1–5, 2013, Revised Selected Papers). Berlín: Springer, 2013, 6–24. (Lecture Notes in Comput. Sci.; 7859)

[11] Shor, P. W. «Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer». *SIAM J. Comput.*, 26 (5) (1997), 1484–1509.

[12] Silverman, J. H. *The arithmetic of elliptic curves*. 2a ed. Dordrecht: Springer, 2009. (Graduate Texts in Mathematics; 106)

Departament de Matemàtica Aplicada i Anàlisi
Universitat de Barcelona
Gran Via de Les Corts Catalanes, 585
`elitza.maneva@gmail.com`

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 51–71. DOI: 10.2436/20.2002.01.66

Nous resultats i procediments en les matemàtiques del segle XVII: càlcul de màxims a Pietro Mengoli (1626/1627–1686)

M. Rosa Massa-Esteve

Resum: La publicació, l'any 1591, de l'obra *In artem analyticen isagoge* de François Viète (1540–1603) va constituir un pas endavant important en el desenvolupament del llenguatge simbòlic. A començaments del segle XVII la difusió de l'obra de Viète va provocar que altres autors, com ara Pietro Mengoli (1626/1627–1686), també consideressin la utilitat dels procediments algebraics per resoldre tot tipus de problemes. Mengoli va seguir el camí de Viète tot construint una geometria d'espècies, *Geometriae speciosae elementa* (1659), que li va permetre emprar conjuntament l'àlgebra i la geometria per resoldre problemes de quadratura. Mengoli, com Viète, va considerar la seva àlgebra una tècnica en la qual els símbols eren utilitzats no únicament per representar nombres sinó també valors de qualsevulla magnitud. Va tractar amb espècies, formes, taules triangulars, quasi raons i raons logarítmiques. Tanmateix, l'aspecte més innovador del seu treball va ser l'ús de les lletres per tractar directament les figures geomètriques mitjançant les seves expressions algebraiques. En aquest article, analitzo la construcció algebraica d'aquestes figures geomètriques, l'ús de les taules triangulars i la demostració molt original que va fer Mengoli per trobar el màxim d'aquestes figures geomètriques abans del desenvolupament del càlcul de Newton i Leibniz. Aquestes anàlisis il·lustren les idees matemàtiques de Mengoli sobre la funció específica del llenguatge simbòlic com a mitjà d'expressió i com a eina analítica.

Paraules clau: figures geomètriques, taules triangulars, Pietro Mengoli, matemàtiques del segle XVII, màxim d'una figura, logaritmes, expressió algebraica.

Classificació MSC2010: 01A45, 3303, 2603.

Introducció

El desenvolupament de les matemàtiques al segle XVII pot ser entès *grosso modo* per l'impuls de la conjunció de tres forces: a) l'herència de la matemàtica

Part d'aquesta investigació va ser presentada prèviament al congrés internacional de Manchester ICHSTM 2013 dins del simposi «The history and philosophy of mathematical optimization».

clàssica exemplificada per les traduccions llatines del Renaixement de les obres d'Euclides i Arquímedes; b) l'emergència de l'àlgebra i la seva utilització en la geometria conduents a una algebrització de la matemàtica, i c) l'extensió del domini propi de les matemàtiques a l'ús d'algoritmes infinits i a l'estudi d'objectes geomètrics de dimensió infinita. En una època en la qual s'havia recuperat el pensament clàssic a través de les traduccions dels textos grecs, s'introduïren a la vegada en el pensament matemàtic unes tècniques algebraiques molt fèrtils amb un significat que, a vegades, s'oposava a la comprensió de les tècniques clàssiques [16, 17].

Una de les transformacions essencials de les matemàtiques del segle XVII va ser l'establiment d'un nou llenguatge simbòlic com a eina matemàtica. El nou llenguatge de símbols, que no era només una nova manera d'escriure sinó que aportava nous objectes i nous procediments, es va començar a emprar també a les operacions i construccions geomètriques per obtenir nous resultats. De fet, dues de les novetats a les matemàtiques del segle XVII, la creació de la geometria analítica i els primers desenvolupaments del càlcul infinitesimal, van ser impulsats per les connexions entre les expressions algebraiques i les corbes que descriuen les figures geomètriques, en utilitzar procediments algebraics per a resoldre problemes geomètrics.

Un dels punts d'inflexió per al desenvolupament d'aquest llenguatge simbòlic el va constituir la publicació, l'any 1591, de l'obra *In artem analyticen isagoge* de François Viète (1540–1603). En aquesta obra es va fer evident l'avantatge d'utilitzar símbols dins la matemàtica, no únicament per representar les incògnites, sinó també per representar les quantitats conegudes, la qual cosa permetia tractar les equacions de manera general [32, 12] i [25]. A més Viète va introduir una àlgebra «nova», emprant la que va anomenar «logistica especiosa», és a dir, càlculs amb «espècies», enfront de la «logistica numerosa», és a dir, càlculs amb números que ja es desenvolupaven a les àlgebres renaixentistes anteriors. El sistema de Viète era un mètode de càlcul d'espècies, tipus o classes d'elements més que de càlculs directes amb cada element. Les espècies de l'àlgebra de Viète eren tot tipus de magnituds, numèriques —com ara els números naturals i racionals—, però també geomètriques —com ara les longituds, les àrees, els volums o els angles.

L'obra de Viète va tenir una gran difusió[1] i, a principis del segle XVII, un bon nombre de matemàtics va començar a adonar-se que els procediments algebraics eren una eina molt útil per resoldre problemes geomètrics. Entre aquests podem citar Pierre de Fermat (1601–1665),[2] tot i que la figura més influent en la recerca sobre les relacions entre l'àlgebra i la geometria va ser

1 L'àlgebra de Viète va ser la guia per a resoldre equacions a l'aritmètica, a la geometria i a la trigonometria. Un exemple és l'obra enciclopèdica de Pierre Hérigone (1580–1643), *Cursus mathematicus*, París (1634, 1637, 1642), que consta de sis volums, entre els quals un d'àlgebra. Sobre l'obra d'Hérigone vegeu una anàlisi comparativa entre l'àlgebra de Viète i la d'Hérigone a [23], el tractament dels *Elements* d'Euclides a l'obra d'Hérigone a [24] i la influència de l'obra de Viète en l'obra d'Hérigone i la d'aquest en la de Mengoli a [25].

2 Fermat no va publicar mentre vivia i els seus treballs circulaven en forma de cartes i manuscrits. Sobre Fermat vegeu [10, p. 65–71 i 286–292] i [15, p. 229–232].

René Descartes (1596–1650), autor de la coneguda obra *La géométrie*, que figurava com un apèndix en el seu *Discours de la méthode* (Leiden, 1637). Aquest treball de Descartes va suposar un punt de partida per contemplar la geometria des d'una altra perspectiva [11, 8, 3]. A partir de la seva obra, i durant un segle aproximadament, es va dur a terme el procés d'algebrització de les matemàtiques [17, 22], un període en el qual es va passar d'una manera de pensar les matemàtiques gairebé exclusivament geomètrica a un pensament matemàtic més algebraic. Aquesta evolució va ser lenta i desigual. Alguns autors van adoptar les tècniques algebraiques en la seva obra i, a la vegada, van intentar justificar-les o transformar-les d'acord amb la matemàtica clàssica. D'altres, malgrat conèixer l'existència d'aquests procediments, els consideraven aliens al pensament matemàtic i, fins i tot, els refusaven. Finalment, alguns acceptaven aquesta nova manera de pensar com un complement més per al desenvolupament de les seves tècniques matemàtiques [22].

Situat en aquest últim grup, Pietro Mengoli (1626/1627–1686), matemàtic bolonyès deixeble de Cavalieri, seguint les idees algebraiques de Viète, va construir una àlgebra d'«espècies» a la geometria, que li va permetre emprar complementàriament l'àlgebra i la geometria [19, 21]. El nom de Mengoli apareix en el registre de la Universitat de Bolonya en el període 1648–1686, on va succeir el seu mestre Cavalieri a la càtedra de matemàtiques. Es va graduar en filosofia l'any 1650 i tres anys més tard, en lleis civils i canòniques. En un primer període va escriure tres obres de matemàtica pura: *Novae quadraturae arithmeticae seu de additione fractionum* (Bolonya, 1650), *Via regia ad mathematicas per arithmeticam, algebram speciosam et planimetriam ornata maiestati serenisimae D. christinae reginae suecorum* (Bolonya, 1655) i *Geometriae speciosae elementa* (Bolonya, 1659), i més tard, el *Circolo* (Bolonya, 1672). L'any 1660 va ser ordenat sacerdot i, des d'aquest moment i fins a la seva mort, va ser prior de l'església de Santa Maria Magdalena de Bolonya [29].

A les seves obres, Mengoli va establir les propietats de les figures geomètriques definides mitjançant expressions algebraiques que en notació actual s'escriuen $y = Kx^m(1-x)^n$, i va trobar-ne a més les quadratures. Així va demostrar que les àrees entre 0 i 1 d'aquestes figures, amb els coeficients pertinents, valen 1 quan m i n són naturals. En notació actual [19, 21]:

$$(m+n+1)\binom{m+n}{n}\int_0^1 x^m(1-x)^n\,dx = 1.$$

Per a racionals de denominador 2, va demostrar [19, 26]:

$$\int_0^1 \sqrt{x^n(1-x)^{(m-n)}}\,dx = \frac{1}{(m/2+1)\binom{m/2}{n/2}}.$$

Mengoli va classificar les figures geomètriques descrites per les corbes $y = Kx^m(1-x)^n$ segons el grau i el tipus d'expressió algebraica, i en va descriure

la seva representació situant-les en unes taules triangulars. Va establir també un procediment per a trobar el seu màxim en un interval donat, sense les eines del càlcul infinitesimal que es desenvoluparien pocs anys més tard.

L'objectiu d'aquest article és analitzar la construcció algebraica d'aquestes figures geomètriques, l'ús de les taules triangulars i la singular demostració emprada per Mengoli per a trobar el màxim d'aquestes figures geomètriques, en el context de les matemàtiques del segle XVII. Mostrarem que l'ús del llenguatge simbòlic i de les taules triangulars són factors determinants en la demostració de Mengoli, en la justificació de la seva exactitud, de la validesa del procediment i de la generalitat del resultat.

1 Les expressions algebraiques de les figures geomètriques de Mengoli

A les matemàtiques del segle XVII, la relació entre les ordenades i les abscisses d'una figura geomètrica o de la corba que la descriu, tal com s'entén actualment, encara no estava establerta. El que feien els diferents autors eren intents d'introduir l'àlgebra en la geometria per construir les corbes emprant el nou llenguatge algebraic [2, 3]. Alguns autors definien i feien servir les corbes a través de les seves propietats, d'altres definien les figures geomètriques o les corbes que les determinaven a través de la descripció de la seva construcció punt a punt o bé del seu moviment però encara no definien expressions algebraiques que s'identifiquessin amb les figures geomètriques mitjançant un sistema de coordenades i encara menys prescindien del seu dibuix a l'hora de treballar-hi. Com es mostrarà, Mengoli presentava un procediment original i innovador per a l'època, emprant l'àlgebra en la geometria d'una manera singular.

La *Geometriae speciosae elementa* (1659) de Mengoli, d'ara en endavant *Geometria*, obra de 472 pàgines de matemàtica pura, està composta per sis capítols, que anomena *elements*, i una introducció titulada «Lectori elementario».[3] Ja en el títol, «Elements de geometria d'espècies», indica el singular ús del llenguatge simbòlic en aquesta obra i, en particular, en la geometria. Mengoli,

3 En el primer capítol d'aquesta obra, titulat «De potestatibus, à radice binomia et residua», Mengoli donava les 10 primeres potències d'un binomi, expressades en lletres, tant pel que fa a la suma com pel que fa a la diferència, i explicitava que era possible estendre aquest resultat a potències més grans. El segon, titulat «De innumerabilibus numerosis progressionibus», conté càlculs de nombroses sumes de potències i productes de potències amb una notació pròpia, així com demostracions d'algunes identitats. En el tercer, que té com a títol «De quasi proportionibus», a partir de la definició dels conceptes «raó quasi nul·la», «raó quasi infinita», «raó quasi la igualtat» i «raó quasi un número», desenvolupava una teoria de quasi proporcions, basant-se en la teoria de proporcions del Llibre V d'Euclides. En el quart capítol, titulat «De rationibus logarithmicis», basant-se també en el Llibre V d'Euclides, elaborava una teoria completa de proporcions logarítmiques. En el cinquè, titulat «De proprijs rationum logarithmis», construïa el logaritme d'una raó amb la teoria anterior i demostrava les seves propietats. Finalment, en el sisè, titulat «De innumerabilibus quadraturis», calculava les quadratures de figures mixtilínies desenvolupant l'àlgebra de Viète a través d'unes taules triangulars i la teoria de quasi proporcions.

encara que no intencionadament, va crear un nou camp dins de la matemàtica, una «geometria especiosa» modelada per l'àlgebra especiosa de Viète, ja que tractà la geometria amb el llenguatge especiós, on els símbols representaven no únicament números sinó també els valors de qualsevol magnitud, ja sigui longitud, àrea o volum.

En aquest apartat es mostra a continuació com, a la seva *Geometria*, Mengoli identifica i construeix les figures geomètriques descrites per les corbes, d'equació $y = Kx^m(1-x)^n$, emprant unes expressions algebraiques pròpies, i de quina manera fa servir aquesta identificació. També s'analitza com l'ús d'unes taules triangulars per classificar aquestes figures en grups permet tractar-ne les propietats.

1.1 Sistema de coordenades

Mengoli va començar l'element sisè, titulat «De innumerabilibus quadraturis», explicant el seu sistema de coordenades, definint l'abscissa i descrivint individualment les ordenades de les figures geomètriques a través de les seves abscisses. Mengoli proposà un segment de qualsevol longitud, amb el nom de *Rationalis*, i el va posar en una línia recta que va anomenar *Tota* i que representà amb la lletra t (de vegades amb la lletra u, si valia 1). Va definir una base com un segment de línia recta de mida t o 1 i utilitzà la paraula *abscissa* com la x que s'empra actualment, encara que dins d'aquesta base.[4] Sempre treballava dins d'una base finita on l'abscissa es representava per la lletra a i el residu per la lletra r, igual a $t-a$ o bé a $1-a$ segons fos la base un valor donat t o bé la unitat 1. Mengoli ho definia així [27, p. 367]:

> 3. I sigui donada una posició, a la qual se l'anomenarà Base $[AR]$.[5]
> 4. I un dels punts $[A]$ de l'extrem [de la base] se l'anomenarà fi de les abscisses [origen de la base].
> 5. I a l'altre punt $[R]$ se l'anomenarà fi dels residus [final de la base].
> 6. I a la quantitat que [va] des de qualsevol punt de la base fins a la fi de les abscisses $[AB]$, en la mida en què és estesa la mateixa base, se l'anomenarà abscissa $[a]$.[6]

En concret, Mengoli considerava la base AR, on A és la fi de les abscisses, R és la fi dels residus, AB és l'abscissa i BR és el residu (figura 1).

4 Encara que la paraula *abscissa* havia estat emprada per altres contemporanis, sembla que no havia estat utilitzada abans com ho fem actualment. La paraula *abscissa* ja havia aparegut en algun text de Fermat el 1644 [10, p. 195], de Torricelli el 1646 [31, p. 366], de Cavalieri el 1647 [4, p. 858–859] i de degli Angeli el 1659 [1, p. 175–179].

5 Els nombres que apareixen al començament són els nombres d'ordre de les definicions de Mengoli.

6 «3. Sitque data positione; quae dicetur, Basis. 4. Eiusque alterum extremorum punctorum, dicetur, Finis abscissarum. 5. Alterum, Finis residuarum. 6. Et ab unoquoque puncto in basi sumpto, usque ad finem abscissarum, quatenus ipsa basis extenditur, quantitas dicetur Abscissa.». Totes les traduccions del llatí al català són de l'autora.

FIGURA 1: Definició d'*abscissa*.

Pel que fa a l'ordenada, Mengoli utilitzava aquest terme en lloc d'«applicata», que s'emprava en aquella època.[7] Definia les ordenades per cada valor de l'abscissa de la base, començant per les ordenades de les figures conegudes, com és ara el quadrat (o el rectangle) i el triangle, a partir de la seva construcció sobre cada punt de la base.[8] Així explicava Mengoli com traçar les ordenades d'un quadrat [27, p. 368]:

> 10. Sobre una base és descrit un quadrat, i suposo que des d'un qualsevol dels punts de la base és traçada una recta fins al costat oposat, mantenint-la sempre paral·lela als costats del quadrat; la qual serà anomenada «ordenada dins del quadrat».[9]

En el cas de les figures mixtilínies (figures determinades per una part recta i per l'altra part corba), Mengoli no va definir les ordenades mitjançant la seva construcció, sinó que va explicar que eren iguals a les abscisses o a les potències de les abscisses; així per a les ordenades de la paràbola deia: «una ordenada qualsevol és abscissa al quadrat», en notació actual, $y = x^2$. Més endavant, quan feia les demostracions de les propietats de les figures, la igualtat entre les ordenades i les abscisses o les potències de les abscisses era també expressada mitjançant la proporció següent, essent 1 la mida de l'interval i y l'ordenada corresponent a l'abscissa x:

$$(1 : y) = (1 : x)^m.$$

L'ús de les proporcions i de la teoria de proporcions euclidiana és una constant en la matemàtica de Mengoli, ja sigui per establir la teoria de quasi proporcions i els logaritmes, com per descriure les operacions aritmètiques entre espècies [20].

1.2 Les expressions algebraiques de les figures geomètriques de Mengoli

Mengoli definia les figures geomètriques que volia quadrar com «esteses per les seves ordenades», les va anomenar «formes» i les va representar mitjançant

7 Descartes defineix les ordenades com «celles qui s'appliquen par ordre»; vegeu [8, p. 67], on hi ha una nota que diu: «L'equivalent de «ordination aplication» era utilitzat en el segle XV traduint Apolonius». La nota també cita que el *Diccionari matemàtic* d'Hutton (1796) dóna *aplicada* com la paraula corresponent a l'*ordenada* i diu que també s'utilitza «ordenada aplicada». De fet, Fermat i Cavalieri utilitzaven «applicata». Mengoli en el *Circolo* les anomenà «ordinatamente applicate».

8 Sembla que Fermat donava un sistema de coordenades similar per definir les corbes però la seva ordenada no era sempre perpendicular i, en aquests casos, donava l'angle que formava amb l'eix d'abscisses; vegeu [10, p. 91–131].

9 «10. Super basi describatur quadratum: & ab uno quolibet puncto in basi sumpto, recta ducatur, usque ad oppositum latus, reliquis lateribus quadrati parallela: quae dicetur, Ordinata in quadrato.».

una expressió algebraica FO. $a^m r^n$, on FO. denota la forma, a l'abscissa x i r el residu $(1-x)$. Mai no va mencionar la paraula *corba*, sinó que va parlar de *figura* o *forma*, paraula que s'utilitzava en els segles anteriors i que s'identificava amb la mesura de la qualitat d'una quantitat, com ara a l'obra de Nicolas Oresme (1323–1382) que du per títol *Tractatus de latitudinibus formarum* (1346) [6, 7].

Primer descrivia les figures conegudes com ara el quadrat i el triangle, i finalment les «formes» esteses per qualsevol ordenada del tipus $y = x^m(1 - x)^n$. Mengoli expressava algebraicament el quadrat [27, p. 368]:

> 12. I el quadrat estès per les seves «ordenades» serà anomenat «Forma de tots els racionals» i «Forma de totes les *totes*», i és representat amb els caràcters FO. u i FO. t.[10]

Definia el triangle com la «Forma de totes les abscisses» (estès per l'ordenada $y = x$) i el representà algebraicament amb el caràcter FO. a. Les paràboles són la «Forma de totes les abscisses al quadrat», la «Forma de totes les abscisses pels residus (uniprimes)», i la «Forma de tots els residus al quadrat»; els representà amb els caràcters FO. a^2, FO. ar, FO. r^2 [esteses per $y = x^2$, $y = x(1 - x)$, $y = (1 - x)^2$, respectivament]. I, en general Mengoli definia la figura estesa per qualsevol ordenada emprant l'expressió «tales» [27, p. 369]:

> 23. I, generalitzant, si sobre la base es forma una figura, estesa no solament per ordenades dins d'un quadrat, en la qual una ordenada qualsevol és considerada com algun element dels de la taula proporcional [$x^m(1 - x)^n$ essent x l'abscissa], [aquesta figura] serà anomenada «Forma de tots tals proporcionals» i serà representada amb els caràcters pertinents; per exemple «Forma de totes les abscisses al cub (*tertiae*)», FO. a^3 [estesa per $y = x^3$], «Forma de tots els productes de les abscisses al quadrat pel residu (*biprimae*)», FO. a^2r [estesa per $y = x^2(1 - x)$], «Forma de tots els productes de l'abscissa pels residus al quadrat (*unisecundae*)», FO. ar^2 [estesa per $y = x(1 - x)^2$], «Forma de tots els residus al cub (*tertiae*)», FO. r^3 [estesa per $y = (1 - x)^3$], i així indefinidament.[11]

Tanmateix, Mengoli volia assegurar-se que cadascuna d'aquestes expressions algebraiques definides per descriure les figures geomètriques, que eren objectes algebraics nous, podia ser identificada amb la figura corresponent a través d'una construcció. Així a la tercera proposició de l'element sisè demostrava que, proposada una expressió algebraica associada a una forma o figura geomètrica i donada una abscissa, sempre es podia construir una ordenada corresponent a aquesta abscissa dins d'aquesta figura geomètrica. Mengoli ho plantejava amb

10 «12. Et quadratum, per suas ordinatas extensum, dicetur, Forma omnes rationales, & Forma omnes totae. & significabitur characteribus FO. u & FO. t.».

11 «23. Et generaliter, si super basi concipiatur figura, extensa non nisi per ordinatas in quadrato: & in qua, unaquaelibet ordinata, est assumpta quaedam in tabula proportionalium: dicetur, Forma omnes tales proportionales. aptoque significabitur charactere. vt Forma omnes abscissae tertiae, FO. a^3: Forma omnes biprimae, FO. a^2r: Forma omnes unisecundae, FO. ar^2: Forma omnes residuae tertiae, FO. r^3 & sic deinceps.».

la paraula *problema*, ja que es tractava d'una construcció i no d'un teorema, i el resolia per a una forma concreta, FO. $10a^2r^3$. El que calia era traçar una recta y, perpendicular a la base, que per una abscissa donada x verifiqués la proporció: $(1 : y) = (1 : x)^2(1 : (1 - x))^3(1 : 10)$. Fent la composició de raons, com que eren iguals els numeradors havien de ser iguals els denominadors, i així trobava el valor de l'ordenada $y = 10x^2(1-x)^3$. Mengoli aquí dibuixava un eix horitzontal AR i una línia perpendicular (no en el punt mitjà) amb la lletra B sobre la base i la lletra C al final de la línia perpendicular (figura 2). Mengoli descrivia la construcció i la demostració d'aquesta manera [27, p. 377–378]:

Problema 1. Proposició 3.

Trobeu l'ordenada d'una forma [figura geomètrica] proposada, per un punt donat i en una base donada.[12]

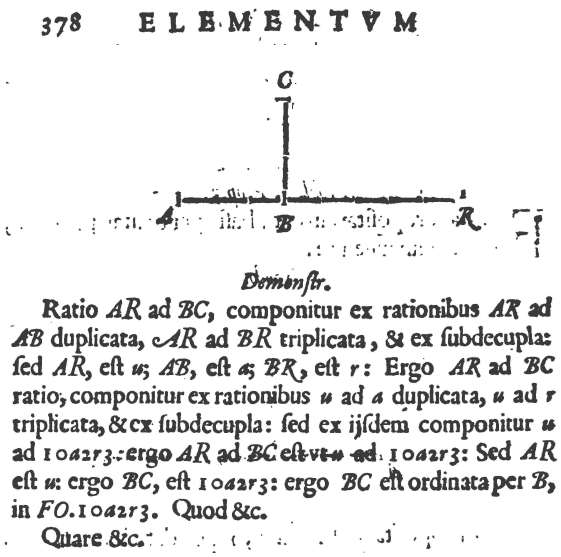


FIGURA 2: Proposició 3 [27, p. 378].

Hipòtesi.

Això és, proposada FO. $10a^2r^3$ [expressió algebraica], sobre una base donada AR, en la qual un punt B és donat, és necessari trobar l'ordenada per B.[13]

12 «Probl. 1. Prop. 3. Formae propositae, in data basi, per datum punctum, ordinatam invenire.».

13 «*Hypoth.* Esto proposita FO. $10a^2r^3$, super data basi AR, in qua datum punctum B. Oportet per B ordinatam invenire.». Es transcriuen tots els apartats de la demostració.

Construcció.

Donat AR, i donats AB, BR, es trobarà la recta BC, a la qual AR té una raó composta de les raons donades AR a AB al quadrat, AR a BR al cub, i de la raó un dècim. I serà traçada BC perpendicular a AR. Afirmo, doncs, que BC és l'ordenada per B, dins de [la figura] FO. $10a^2r^3$.[14]

Demostració.

La raó AR a BC serà composta de les raons AR a AB al quadrat, AR a BR al cub, i d'un dècim; però AR és u [1]; AB és a; BR és r [$1-a$]. Llavors la raó AR a BC serà composta de les raons u a a, al quadrat, u a r, al cub, i d'un dècim. Però u a $10a^2r^3$ serà composta d'aquestes. Llavors AR a BC és tal com u a $10a^2r^3$. Però AR és u, d'aquí BC és $10a^2r^3$; en conseqüència, BC és l'ordenada per B, dins de FO. $10a^2r^3$.[15]

De fet, a cada abscissa x li correspon el valor $10x^2(1-x)^3$, que és el que mesura la recta perpendicular que va de B a C, essent C un punt de la línia que descriu la figura, nosaltres diríem la corba, i l'anomena ordenada de l'abscissa B dins de la figura FO. $10a^2r^3$. Mengoli no dóna valors particulars d'aquesta correspondència. Fa la demostració per a una figura qualsevol, però considera que és certa per a totes les altres figures fent les raons corresponents.

Cal remarcar que Mengoli en aquesta demostració no només treballava amb proporcions de segments sinó que també identificava els segments amb les lletres de l'expressió algebraica i igualava el producte de segments amb la composició de raons, emprant la teoria euclidiana de proporcions. Tanmateix, Mengoli no va definir una àlgebra de segments com va fer Descartes a la seva *Géométrie*, és a dir, no va donar una interpretació geomètrica de cadascuna de les operacions algebraiques que definia sinó que va demostrar, per a una mesura donada de l'interval, com construir l'ordenada per un punt donat emprant la composició de raons i la seva definició d'ordenades iguals a les abscisses de les seves figures geomètriques. La seva introducció de l'àlgebra dins la geometria té més similituds amb els procediments de Viète. Aquest també emprava la teoria de proporcions com un lligam, però feia diagrames sense utilitzar sistemes de coordenades i verificava les construccions de les solucions de les equacions de segon grau sense assumir cap connexió entre les ordenades i les abscisses. Quan es menciona la relació entre les ordenades i les abscisses en una corba, hom pensa immediatament en Fermat i en la seva obra *Ad locos planos et solidos isagoge* de 1636. Tot i que Mengoli podria haver pres la inspiració en l'obra de Fermat, només va establir la relació per a algunes

14 «*Constr.* Data AR, datisque AB, BR, inveniatur recta BC, ad quàm AR, rationem habet compositam ex datis rationibus, AR ad AB duplicata, AR ad BR triplicata, & ex ratione subdecupla:& collocetur BC perpendiculariter ad AR. Dico BC, esse ordinatam per B, in FO. $10a^2r^3$.».

15 «*Demonstr.* Ratio AR ad BC, componitur ex rationibus AR ad AB duplicata, AR ad BR triplicata, & ex subdecupla: sed AR, est u; AB est a; BR est r: Ergo AR ad BC ratio, componitur ex rationibus u ad a duplicata, u ad r triplicata, & ex subdecupla: sed ex ijsdem componitur u ad $10a^2r^3$: ergo AR ad BC est ut u ad $10a^2r^3$: sed AR est u: ergo BC est $10a^2r^3$: ergo BC est ordinata per B, in FO. $10a^2r^3$. Quod&c. Quare &c.».

figures geomètriques, com ara les determinades per $y = Kx^m(1-x)^n$ i no va mencionar haver trobat un principi general com va afirmar Fermat en la seva *Isagoge* [10, p. 91]. Mengoli no va tractar ni problemes sòlids, ni llocs geomètrics, com va fer Fermat; a més, el mètode d'identificació algebraica de Mengoli no pot ser aplicat per a resoldre aquests altres problemes geomètrics.

Tanmateix, la recerca de Mengoli és profundament original ja que, en construir l'ordenada dins d'una figura per una abscissa donada, va establir una identificació entre els nous objectes algebraics i les figures geomètriques que li permetia tractar les figures geomètriques mitjançant les seves expressions algebraiques, sense necessitat de dibuixar-les. De fet, Mengoli va fer tres dibuixos en tota la *Geometria*, i més tard en el *Circolo* (1672), on calculà la quadratura del cercle, no en va fer cap [26].

1.3 Les taules triangulars de les figures geomètriques

Després de definir les figures geomètriques anteriors i assignar-les-hi les expressions algebraiques corresponents, Mengoli procedeix a treballar amb aquests nous objectes algebraics, ordenant-los en unes taules triangulars, inspirades pel triangle combinatori (també conegut per *triangle de Pascal*).[16] Aquestes taules eren una eina molt utilitzada per Mengoli dins la *Geometria* ja que li permetien classificar els elements de la taula en tipus o grups, segons els exponents i el lloc que ocupaven, i d'aquesta manera podia estudiar les propietats de molts elements simultàniament.[17]

Mengoli ordenà les expressions algebraiques que representaven les figures geomètriques en una taula triangular infinita que anomenà *Tabula Formosa* («taula de les formes»). Vegeu la taula de les formes com l'escrivia Mengoli a la figura 3 i, a la figura 4, la nostra interpretació gràfica. L'expressió del vèrtex, FO. u, representa un quadrat de costat 1. Les dues expressions algebraiques de la primera fila representen dos triangles. El primer triangle, FO. a, està determinat per la bisectriu del primer quadrant $y = x$, l'eix d'abscisses i la línia recta $x = 1$ i el segon triangle, FO. r, està determinat per la línia recta $y = 1 - x$ traçada des de l'extrem $(1, 0)$ al $(0, 1)$ i l'eix d'abscisses. Les tres expressions algebraiques de la segona fila estan determinades per les ordenades d'una paràbola, l'eix d'abscisses i la línia recta $x = 1$. La primera, FO. a^2, determinada per les ordenades $y = x^2$; la segona, FO. ar, per les ordenades $y = x(1-x)$, i la tercera, FO. r^2, per les ordenades $y = (1-x)^2$ i de la mateixa manera descriuríem les altres files.

16 El triangle combinatori ha passat a la història com a *triangle de Pascal* ja que Blaise Pascal (1623–1662) va explicar i va demostrar les seves propietats en un estil molt clar [30, 9]. Mengoli probablement no coneixia el tractat de Pascal ja que havia estat publicat el 1665 però el podia haver conegut a través de la seva font, l'obra d'Hérigone, *Cursus mathematicus* (1634) [13].

17 En l'«Elementum primum» els elements de la taula eren nombres, representats per lletres, que, multiplicant-los pels nombres combinatoris, li permetien calcular els sumands $(a^m r^n)$ que formen el desenvolupament d'una potència natural d'un binomi qualsevol. En l'«Elementum secundum» els elements de la taula eren sumatoris de potències i de productes de potències $(Oa^m r^n)$.

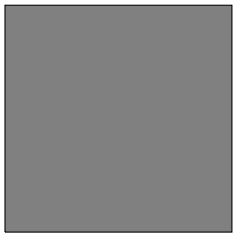
FO. u

FO. a FO. r

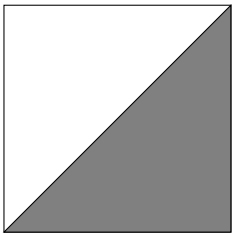
FO. a^2 FO. ar FO. r^2

FO. a^3 FO. a^2r FO. ar^2 FO. r^3

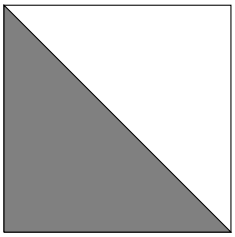
FIGURA 3: *Tabula Formosa.*



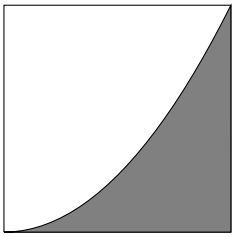
FO.u



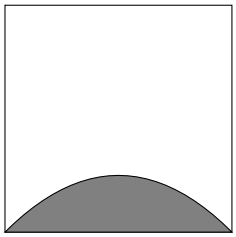
FO.a



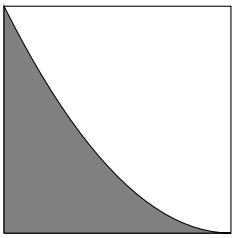
FO.r



FO.a^2



FO.ar



FO.r^2

FIGURA 4: Interpretació actual de les figures geomètriques.

Aquestes expressions algebraiques de la taula de les formes representaven unes figures geomètriques que ell no dibuixava, tot i que coneixia perfectament el traç de la corba que les determinava. Una evidència d'aquest coneixement es troba al final del capítol sisè, on Mengoli enuncia tot un seguit de resultats sobre aquestes figures geomètriques, sense cap demostració.[18] Mengoli explicava la classificació d'aquestes figures geomètriques segons la posició a la taula, descrivint els angles mixtilinis que formava la línia corba que les determinava, en tallar la base. A més especificava el valor dels angles, i donava noms a les figures: *binangula*, *unicornes*, *bicornes*, *unicornes* i *unangulae*. Així la figura de la segona fila (ell en deia segona base), que és la segona i penúltima, és a dir, FO. $x(1-x)$, era *binangula* i formava dos angles amb la base que valien $45°$. Mengoli no detallava a quins angles es referia però es pot deduir que eren els que forma la línia corba en els punts de tall dels extrems de la base. A partir de la tercera fila en endavant, les figures dels extrems de la taula, les primeres i les últimes, FO. x^m i FO. $(1-x)^n$, i les segones i les penúltimes, FO. $x^{m-1}(1-x)$ i FO. $x(1-x)^{n-1}$, eren anomenades *unicornes* i *unangulae*. Les primeres formaven un angle que té una raó entre el seu sinus i el seu cosinus (actualment la seva tangent) proporcional al número d'ordre de la fila. Pel que fa al segon grup, no especificava l'angle però, en ser *unangulae*, es pot deduir que la corba formava un angle de $45°$ amb un extrem de la base. Les figures restants, FO. $x^m(1-x)^n$, amb m i n diferents de 0 i 1, Mengoli les anomenava *bicornes*. Encara que no explicava el significat d'aquest nom, es pot deduir que *unicornes* i *bicornes* es refereix al fet que la corba forma un angle o dos de $0°$, respectivament, en els punts de tall dels extrems de la base, és a dir, es tracta d'un mínim o d'un punt d'inflexió.

Com es pot apreciar, Mengoli utilitzà la posició de les figures geomètriques a les taules triangulars per classificar-les d'acord amb els angles de tall de la corba que descriu la figura amb la base, agrupant-les segons el seu grau i segons la seva posició, mostrant així que coneixia el seu dibuix exactament, ja que donava també el valor quantitatiu dels angles de tall amb la base.

Com s'explica a l'apartat següent, Mengoli classificava també les figures geomètriques de la taula triangular en grups segons el seu màxim. Feia les demostracions per a un sol element del grup i considerava que el resultat era cert per a la resta. Mengoli feia aquesta generalització basant-se en la simetria de la taula triangular i la regularitat de les seves files, afirmació que explicità uns anys més tard en la seva obra *Circolo* (1672) [28, p. 24–25]. Es pot concloure, doncs, que la funció de les taules triangulars en l'obra de Mengoli, per classificar i establir la generalitat dels resultats, esdevé essencial.

2 Màxims de les figures geomètriques de Mengoli

Mengoli, a la *Geometria*, estudià també les figures geomètriques que hem definit en l'apartat anterior, pel que fa a la monotonia i al punt màxim de la corba.

18 Mengoli promet que les donarà més endavant amb l'ajuda de Déu, però sembla que no ho fa [27, p. 390].

Per a trobar el màxim d'aquestes figures geomètriques, Mengoli va considerar tres grups a la taula triangular: el primer, corresponent a les figures que es troben en diagonal al primer costat de la taula *Formosa*, FO. a^m; el segon, en la diagonal oposada de la taula, FO. r^n, i el tercer, en el mig de la taula, FO. $a^m r^n$. En les demostracions mengolianes del màxim de la figura geomètrica, una per a cada grup de la taula triangular, es pot comprovar de nou que Mengoli tenia molt clar el seu dibuix, encara que no l'inclogués.

Pel que fa al primer grup, en el primer teorema demostrà que en les figures geomètriques del primer costat de la taula (en diagonal), FO. a^m, determinades per $y = x^m$, en un interval donat, la unitat, les ordenades eren sempre creixents i que l'ordenada màxima es trobava a l'extrem de la base i valia el mateix que la base, la unitat. La demostració es basava en la mateixa definició de les ordenades, prenia $n = 2$ i emprava la proporció, $1 : y = (1 : x)^2$. Tot seguit, en la prova, partia de la desigualtat de les abscisses i obtenia la desigualtat de les ordenades, a través d'aquesta proporció. També va demostrar, pel que fa al segon grup, que en les figures geomètriques de l'últim costat, FO. r^n, determinades per $y = (1 - x)^n$, les ordenades eren sempre decreixents i que l'ordenada màxima es trobava a l'origen de la base i també valia el mateix que la base, la unitat.

Cal remarcar que Mengoli no comparava únicament potències de números racionals, sinó que aquestes potències, quan expressaven un segment, en aquest cas les ordenades d'una figura, també podien ser comparades i permetien estudiar la monotonia de la corba. Així, encara que les potències tinguin graus més grans que 3, representen segments lineals que mesuren aquestes quantitats, ja que hem definit la base com a unitat.

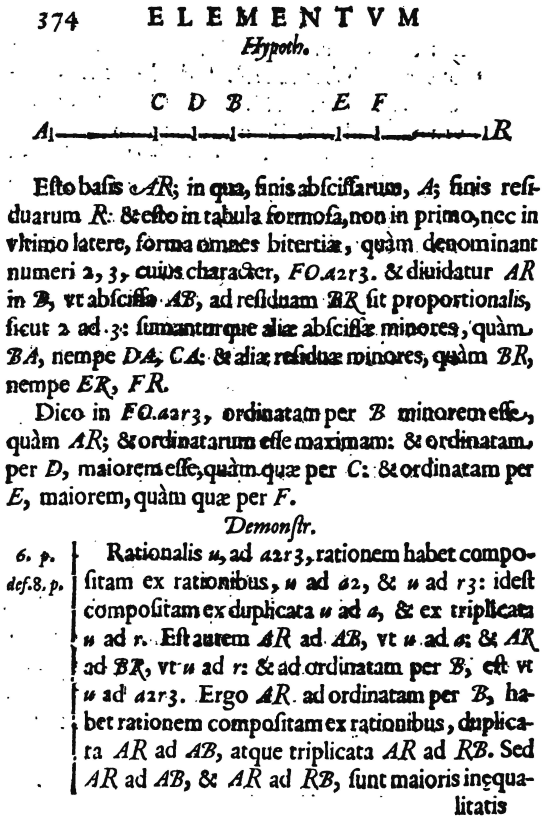
Pel que fa al tercer grup, en el segon teorema, va demostrar que en les figures geomètriques del mig de la taula, FO. $a^m r^n$, determinades per $y = x^m(1-x)^n$, les ordenades eren primer creixents i després decreixents i prenien el seu valor màxim en una abscissa que divideix la base en la raó dels exponents $x : (1 - x) = m : n$. De fet, si es resol l'equació, s'obté $x_{\max} = m/(m + n)$. Mengoli ho plantejava així al segon teorema [27, p. 373]:

> *Theor. 2. Prop. 2.* A la taula *Formosa*, les figures [formes] que no estan en el primer ni en l'últim costat tindran una ordenada màxima que és més petita que la base [tota], i que la seva abscissa és proporcional al residu com els nombres que determinen aquesta forma [els exponents], i l'ordenada dels residus d'una part [i de les abscisses de l'altra] és més gran com més s'acosten aquests [i aquestes] a l'abscissa del màxim.[19]

L'única representació gràfica en la demostració és un segment amb les lletres A, C, D, B, E, F, R, essent AR la base; A l'origen de les abscisses (ell l'anomena la fi); R és el final de la base (que ell anomena la fi dels residus), C, D, E, F són

19 «Theor. 2. Prop. 2. In singulis formosae tabule, non primi, nec ultimi lateris formis, ordinatarum maxima, minor est, quam tota. &facit abscissam, & residuam, proporcionales, ut numeri, à quibus ipsa forma denominatur: reliquarum verò ex utralibet parte, propior maxime remotiore maior est.».

divisions de la base AR i cadascuna representa una abscissa, i B representa l'abscissa que correspon al màxim (figura 5).


374 ELEMENTVM

Hypoth.

C D B E F

A R

Esto basis AR; in qua, finis abscissarum, A; finis residuarum R. & esto in tabula formosa, non in primo, nec in vltimo latere, forma omnes bitertiæ, quàm denominant numeri 2, 3, cuius character, FO.a2r3. & diuidatur AR in B, vt abscissa AB, ad residuam BR sit proportionalis, sicut 2 ad 3: sumanturque aliæ abscissæ minores, quàm BA, nempe DA, CA: & aliæ residuæ minores, quàm BR, nempe ER, FR.

Dico in FO.a2r3, ordinatam per B minorem esse, quàm AR; & ordinatarum esse maximam: & ordinatam per D, maiorem esse, quàm quæ per C: & ordinatam per E, maiorem, quàm quæ per F.

Demonstr.

6. p. def. 8. p. Rationalis u, ad a2r3, rationem habet compositam ex rationibus, u ad a2, & u ad r3: idest compositam ex duplicata u ad a, & ex triplicata u ad r. Est autem AR ad AB, vt u ad a: & AR ad BR, vt u ad r: & ad ordinatam per B, est vt u ad a2r3. Ergo AR ad ordinatam per B, habet rationem compositam ex rationibus, duplicata AR ad AB, atque triplicata AR ad RB. Sed AR ad AB, & AR ad RB, sunt maioris inequalitatis

FIGURA 5: Representació de la demostració del màxim de Mengoli.

Mengoli presentava la demostració amb una figura concreta, FO. a^2r^3, on l'abscissa B que prenia l'ordenada màxima verificava $AB : BR = 2 : 3$. De fet, resolent l'equació $x_{\max} = 2/5$.

Mengoli primer demostrava que l'ordenada de l'abscissa B és més petita que la base AR, és a dir, que la unitat. Resumim la demostració: sabent que l'abscissa $AB = x$ és menor que 1 i que el residu $r = 1 - x$ és menor que 1, i denotant l'ordenada de l'abscissa B per $\mathrm{Ord}\, B = y$ i la base per $AR = 1$, Mengoli provava que la base AR és més gran que l'ordenada de l'abscissa B, és a dir, que $AR > \mathrm{Ord}\, B$; $1 > y$.

Començava la demostració recordant la igualtat següent, fent referència al primer llibre de la *Geometria*, on tractava les potències i el seu producte:[20]

$$1 : x^2(1-x)^3 = (1 : x^2)(1 : (1-x)^3) = (1 : x)^2(1 : (1-x))^3. \qquad (1)$$

20 Com en altres parts de l'obra Mengoli empra la teoria de proporcions per definir els seus productes de potències.

D'altra banda, amb les notacions proposades establia les proporcions següents:

$$AR : AB = 1 : x; \quad AR : BR = 1 : (1 - x);$$
$$AR : \operatorname{Ord} B = 1 : x^2(1 - x)^3.$$

Llavors per la igualtat anterior (1) i aplicant la propietat transitiva euclidiana,

$$AR : \operatorname{Ord} B = (1 : x)^2(1 : (1 - x))^3.$$

Mengoli concloïa que es verificava la desigualtat entre AR i $\operatorname{Ord} B$, explicant que el producte de les dues raons $(1 : x)^2$ i $(1 : (1 - x))^3$, que són més grans que la unitat, dóna una raó més gran que la unitat, així: $AR : \operatorname{Ord} B > 1$ i en conseqüència, $AR > \operatorname{Ord} B$.

Després per demostrar que l'ordenada de l'abscissa B, que verifica la proporció amb els exponents, és la màxima, provava que l'ordenada de qualsevol altra abscissa C o D, o bé E o F és més petita. Com a exemple d'aquest segon tipus de demostracions provarem que l'ordenada de l'abscissa D és més petita que l'ordenada de l'abscissa B, que és l'abscissa que pren el màxim, és a dir, Mengoli demostrava que $\operatorname{Ord} D < \operatorname{Ord} B$.

Prenent l'abscissa $x = AB$ i $x_1 = AD$ una divisió qualsevol de la base més petita que la divisió AB, llavors per la definició mengoliana de les figures geomètriques, s'estableixen les proporcions següents:

$$\operatorname{Ord} D : AR = \operatorname{Ord} D : 1 = (x_1 : 1)^2((1 - x_1) : 1)^3,$$
$$AR : \operatorname{Ord} B = 1 : \operatorname{Ord} B = (1 : x)^2(1 : (1 - x))^3.$$

Operant i component les dues proporcions resulta,

$$\operatorname{Ord} D : \operatorname{Ord} B = x_1^2(1 - x_1)^3 : x^2(1 - x)^3.$$

Ara es tracta de veure que l'antecedent de la raó, $\operatorname{Ord} D = (x_1)^2(1 - x_1)^3$, és més petit que el conseqüent, $\operatorname{Ord} B = (x)^2(1 - x)^3$, per a qualsevol abscissa D, i així queda vist que l'ordenada per B és màxima.

Per veure que l'antecedent és més petit que el conseqüent Mengoli va emprar un teorema demostrat amb els seus logaritmes que establia la desigualtat següent:

$$(x_1 : x)^2 < ((1 - x) : (1 - x_1))^3. \tag{2}$$

Llavors, de la desigualtat, en resulta: $x_1^2(1 - x_1)^3 < x^2(1 - x)^3$ i, aplicant la propietat transitiva, $\operatorname{Ord} D < \operatorname{Ord} B$.

Finalment, Mengoli demostrava també que l'ordenada per C és més petita que l'ordenada per D (és a dir, que les ordenades són creixents) i que l'ordenada per F és més petita que l'ordenada per E (és a dir, que les ordenades després de l'ordenada màxima són decreixents). Mengoli només ho demostrava per a dos valors qualssevol però afirmava que era cert per a tots els altres valors de l'abscissa. Mengoli va fer totes aquestes demostracions amb procediments

similars i emprant resultats obtinguts amb els logaritmes. Cal remarcar que és essencial la relació d'ordre dins l'interval i que la continuïtat de la corba es donava per suposada; Mengoli mai no ho va mencionar ni va suggerir que tingués cap dubte o que li presentés cap problema.[21]

2.1 Els logaritmes a la demostració del màxim

Per tal d'entendre la demostració de la desigualtat (2) presentarem un esbós de la idea mengoliana de logaritme i de les propietats que utilitza en la prova del màxim.

Mengoli exposa la seva teoria de logaritmes en l'*element cinquè*, titulat «De proprijs rationum logarithmis», que comprèn 145 pàgines, amb 34 definicions i 107 proposicions. Mengoli definia el logaritme com el límit de les sumes de termes de la sèrie harmònica. El tractament és complex ja que Mengoli vol demostrar les propietats dels logaritmes en general, utilitzant el llenguatge simbòlic. Treballa amb el llenguatge de les proporcions i defineix el logaritme dels números a través de les raons de termes de la sèrie harmònica que mesuren l'allunyament de la unitat.

Vegem-ne un exemple: per trobar el logaritme de 2 utilitza la raó $(1/5 : 1/10)$ i defineix dues nocions noves, l'hiperlogaritme de 2 i l'hipologaritme de 2. L'hiperlogaritme de $2 = (1/5 : 1/10)$ és $1/5+1/6+1/7+1/8+1/9$. L'hipologaritme de $2 = (1/5 : 1/10)$ és $1/6 + 1/7 + 1/8 + 1/9 + 1/10$. Mengoli afirmava que el logaritme serà el límit d'aquestes dues sumes.[22] Així ho explicava en el «Lectori elementario» [27, p. 69–70].

> Per tant l'hiperlogaritme i l'hipologaritme són quasi iguals. I el logaritme és aquella quantitat a què tendeixen els hiperlogaritmes quan van disminuint i a què tendeixen i els hipologaritmes quan van augmentant, el més petit de tots els hiperlogaritmes i el més gran de tots els hipologaritmes.[23]

I ja en les definicions Mengoli afirmava [27, p. 206],

> Def. 24. Una quantitat més petita que tots els hiperlogaritmes d'una raó i més gran que tots els hipologaritmes s'anomenarà logaritme d'aquella raó.[24]

Vegem tot seguit el teorema dels logaritmes que Mengoli va emprar en la prova del màxim per demostrar la desigualtat (2) $(x_1 : x)^2 < ((1-x) : (1-x_1))^3$. Es tracta d'un teorema de l'*element cinquè* de la *Geometria* que s'aplica a

21 Knobloch quan analitza les quadratures de Leibniz remarca també que la condició de continuïtat de la corba és indispensable [14, p. 63].

22 La idea de *quasi proporció* (*quasi igual*, *quasi infinit*, etc.), que esdevé essencial per trobar les quadratures, és també determinant a la definició de límit [18].

23 «Unde hyperlogarithmus, & hypologarithmus quasi sunt aequales. Porrò logarithmus illa est quantitats, ad quam tenduat hyperlogarithmi, cum sempre deinceps minuuntur, & ad quam tendunt hypologarithmi, cum sempre deinceps augentur; omni minor hyprlogarithmo, & omni maior hypologarithmo.».

24 «Def. 24. Quantitas omni minor hyperlogarithmo earumdem rationum, & omni maior hypologarithmo, earumdem Logarithmus dicetur.».

quatre quantitats que tenen les mateixes diferències dues a dues, que anomenà disposades aritmèticament. Així les nostres quantitats, AD, AB, BR, RD dins del segment $AR = 1$ són d'aquest tipus, ja que prenent $AD = x_1$; $AB = x$; $BR = 1 - x$ i $DR = 1 - x_1$, les diferències són iguals a BD, en aquest cas: $AB - AD = x - x_1 = RD - BR = (1 - x_1) - (1 - x) = BD$.

A més dues d'aquestes quantitats estan en una raó determinada i verifiquen, com en l'enunciat del teorema 2 de la pàgina 63, que $AB : BR = x : (1 - x) = 2 : 3$.

Per tant, amb aquestes hipòtesis, Mengoli demostrà en la proposició 105, que donem a continuació, que es verificava la desigualtat següent (2):

$$(AD : AB)^2 = (x_1 : x)^2 < ((1 - x) : (1 - x_1))^3 = (BR : RD)^3.$$

Mengoli enuncià la proposició en llenguatge retòric, encara que a la demostració utilitzà com a exponents les lletres b i c [27, p. 338]:

> Prop. 105. Donades quatre quantitats [en aquest cas x_1, x, $1 - x$, $1 - x_1$], disposades aritmèticament [$x - x_1 = (1 - x_1) - (1 - x)$], si es verifica que $x : (1 - x) = b : c$ [en aquest cas $2 : 3$], llavors la raó de la primera quantitat a la segona elevada al número homòleg a la segona quantitat serà més petita que la raó de la tercera a la quarta elevada al número homòleg a la tercera [$(x_1 : x)^2 < ((1 - x) : (1 - x_1))^3$].[25]

Vegem un resum de la demostració:

Siguin x_1, x, $1 - x$, $1 - x_1$ quantitats disposades aritmèticament, llavors $x - x_1 = (1 - x_1) - (1 - x)$. Mengoli va treballar amb les seves inverses que són termes que estan en sèrie harmònica: $1/x_1$, $1/x$, $1/(1 - x)$, $1/(1 - x_1)$. Ja havia basat la seva definició de logaritme en el fet que sempre existeix i que es pot definir el logaritme de les raons de termes de la sèrie harmònica, així:

$$\log(1/x : 1/x_1) = \log(x_1 : x) = e;$$
$$\log(1/(1 - x_1) : 1/(1 - x)) = \log((1 - x) : (1 - x_1)) = f.$$

Però a més, com que $x : (1 - x) = b : c$, llavors $e : f > c : b$ (relació entre logaritmes de les raons i les raons que s'ha demostrat anteriorment). De la proporció es dedueix $eb > fc$, és a dir, $b \log(x_1 : x) > c \log((1 - x) : (1 - x_1))$.

Mengoli va demostrar també la coneguda igualtat del logaritme d'un producte i la suma de logaritmes dels factors, i també la relació corresponent per al logaritme d'una potència, a la proposició 80. Per tant:

$$\log(x_1 : x)^b > \log((1 - x) : (1 - x_1))^c.$$

25 «Prop. 105. Quatuor arithmeticè dispositarum quantitatum, si primam ad ultimam, fuerit ut numerus ad numerum erit primae ad secundam totuplicata ratio, quotus est homologus primae, maior, quàm tertiae ad quartam. totuplicata ratio, quotus est homologus quartae, quod si secunda ad tertiam fuerit ut numerus ad numerum: erit primae ad secundam totuplicata ratio, quotus est homologus secundae, minor, quàm tertiae ad quartam totuplicata, quotus est homologus tertiae.».

Com que el logaritme de les potències de les raons és més gran, la potència de la raó $(x_1 : x)^b$, estarà, doncs, més allunyada de la unitat que $((1-x) : (1-x_1))^c$, vegeu [20]. Però com que per definició $x_1 < x$ i $1-x < 1-x_1$, llavors $x_1 : x$ i $(1-x) : (1-x_1)$ són raons més petites que la unitat, $x_1 : x < 1$ i $(1-x) : (1-x_1) < 1$. Així també les potències d'aquestes raons seran raons més petites que la unitat i les raons més petites que la unitat, com més lluny de la unitat estan, més petites són: $(x_1 : x)^b < ((1-x) : (1-x_1))^c$. En el cas de la demostració de la pàgina anterior, $b = 2$ i $c = 3$, llavors s'obté la desigualtat (2): $(x_1 : x)^2 < ((1-x) : (1-x_1))^3$ i operant: $x_1^2(1-x_1)^3 < x^2(1-x)^3$, per tant: $\operatorname{Ord} D < \operatorname{Ord} B$.

Si fem una primera comparació del mètode de Mengoli per trobar el màxim amb el mètode de màxims i mínims de Fermat que va tenir molta difusió a Europa i que va ser molt emprat a l'època, podem assenyalar que aquest no utilitza el mètode de Fermat, que quasi segur que coneixia a través de l'obra d'Hérigone. El mètode de Fermat per trobar màxims i mínims data de 1636, i va ser publicat més tard, el 1642, al *Cursus mathematicus* d'Hérigone [5, 13]. S'il·lustrava resolent un problema, la solució del qual era ja coneguda i que tractava de trobar com dividir una línia en dues parts de manera que el producte de les parts fos un màxim. El mètode de Fermat requeria ésser fet de bell nou per a cada potència per conèixer el resultat, mentre la demostració de Mengoli funcionava per a totes les potències de les figures geomètriques a la vegada i només calia conèixer els exponents de l'expressió algebraica. De fet, si es vol calcular el màxim de l'expressió algebraica concreta de Mengoli emprant el mètode de Fermat, cal fer uns càlculs numèrics molt més llargs, començant amb els primers exponents i augmentant el grau, seguint una mena d'inducció. Un altre tret diferenciador dels dos procediments és que l'ús de la idea de derivada es pot interpretar que està implícita en el mètode de Fermat, en canvi en la demostració de Mengoli és absent. A més, Fermat volia explícitament trobar un mètode (com figura al títol *Mehtodus as disquirendam màxima & minimam*), que també va aplicar per a trobar tangents i en òptica. En canvi, Mengoli no pretenia trobar un mètode, només volia mostrar que coneixia la representació de la figura expressada algebraicament.

3 Algunes conclusions

Mengoli va emprar el llenguatge simbòlic com a mitjà d'expressió i com a eina analítica. Va treballar amb espècies, formes, taules triangulars (triangle harmònic) i quasi proporcions emprant el seu llenguatge especiós.

Tanmateix, un dels aspectes més innovadors de la seva investigació rau en la utilització de les lletres i els símbols per formar expressions algebraiques i identificar-les amb les figures geomètriques. Així va poder estudiar-les a través de les seves expressions algebraiques sense necessitat de fer cap construcció geomètrica. En l'obra de Mengoli la representació gràfica de la figura geomètrica no és el traç, que no fa, sinó una acurada descripció de la corba que determina la figura amb informació suficient per poder dibuixar el seu traç sense necessitat de donar valors concrets.

Cal remarcar l'ús de les taules triangulars com a eina de generalització de resultats. Així les descripcions i les propietats de les corbes que determinen les figures geomètriques només depenien dels grups obtinguts en classificar els elements de la taula triangular, d'acord amb els exponents de les expressions algebraiques i amb la seva posició en aquesta taula.

Pel que fa a la demostració del màxim, afirmem que l'ús del llenguatge simbòlic és un factor determinant ja que Mengoli tracta amb la mida d'un segment i considera la raó de dues parts del segment igual a la raó de dos números (els exponents) expressats amb les lletres *b* i *c*, tot fent la prova clau de l'*element cinquè* per a qualsevol exponent. Realment el procediment per trobar el màxim és independent de la representació gràfica de la figura geomètrica i la regla pot ser emprada per a totes les potències del mateix tipus.

Mengoli assegura l'exactitud de la demostració utilitzant la seva teoria de logaritmes de raons (nova) que ha fonamentat en la teoria de proporcions dels *Elements* d'Euclides, el seu llibre de matemàtiques per excel·lència. Una vegada més, la teoria de proporcions es presenta com un aval dels seus desenvolupaments i li permet operar amb els segments i establir relacions entre les raons i els logaritmes de les raons.

La demostració de Mengoli és vàlida per a totes les figures geomètriques del mateix grup a la taula triangular, ja que no depèn del valor concret de l'exponent de l'expressió algebraica sinó de la seva identificació emprant raons i relacions entre aquestes i els seus logaritmes.

Mengoli pren també per garantia la taula triangular en la generalització del raonament demostratiu, ja que si un resultat és cert per a una figura d'un grup, llavors ho serà per a totes les altres del grup; d'acord amb la simetria de la taula i la regularitat de les seves files, no cal fer cas per cas. Aquesta validesa de la demostració per a moltes figures a la vegada ens permet assenyalar una altra característica rellevant en les matemàtiques de Mengoli, la generalitat del seu resultat.

Probablement a causa de la notació original i del camí diferent que va emprendre Mengoli, la seva demostració no va tenir un impacte decisiu a les matemàtiques del segle XVII. Tanmateix, les seves contribucions són d'un gran interès ja que conjuntava els principis de la geometria euclidiana amb l'àlgebra nova de Viète, que va desenvolupar d'una manera singular. Aquesta original conjunció de l'àlgebra i la geometria per trobar de manera general nous resultats o per donar fonaments nous a resultats ja coneguts, va ser una de les grans contribucions de l'obra matemàtica de Mengoli.

Agraïments

L'autora agraeix a Craig Fraser la seva invitació a participar en el congrés ICHSTM 2013 i el seu interès en la demostració del màxim de Mengoli que presento. La investigació està inclosa en el projecte del Ministerio de Economía y Competitividad, Subdirección general de Proyectos de Investigación: HAR2013-44643-R.

Referències

[1] ANGELI, S. DEGLI *Miscellaneum hyperbolicum, et parabolicum*. Venècia: La Noù, 1659.

[2] BOS, H. J. M. «On the representation of curves in Descartes' *Géométrie*». *Arch. Hist. Exact Sci.*, 24 (4) (1981), 295–338.

[3] BOS, H. J. M. *Redefining geometrical exactness. Descartes' transformation of the early modern concept of construction*. Nova York: Springer-Verlag, 2001. (Sources and Studies in the History of Mathematics and Physical Sciences)

[4] CAVALIERI, B. *Exercitationes geometricae sex*. Bolonya: 1647.

[5] CIFOLETTI, G. C. *La méthode de Fermat: son statut et sa diffusion. Algèbre et comparaison de figures dans l'histoire de la méthode de Fermat*. París: Société Française d'Histoire des Sciences et des Techniques, 1990. (Cahiers d'Histoire et de Philosophie des Sciences. Nouvelle Série; 33)

[6] CLAGETT, M. (ED.). *Nicole Oresme and the medieval geometry of qualities and motion*. Wisconsin: University of Wisconsin Press, 1968.

[7] CROMBIE, A. C. *Historia de la Ciencia: de San Agustín a Galileo. Vol. 2: Siglos XIII–XVII*. 3a ed. Madrid: Alianza Universidad, 1980.

[8] DESCARTES, R. *The geometry of René Descartes*. Nova York: Dover, 1954. [Traduït per D. E. Smith i M. L. Latham]

[9] EDWARDS, A. W. F. *Pascal's arithmetical triangle. The story of a mathematical idea*. Baltimore, Md: Johns Hopkins University Press, 2002. [Reimpressió revisada de l'original de 1987]

[10] FERMAT, P. *Œuvres de Fermat*. TANNERY, P.; HENRY, C. (ed.). París: Gauthier-Villars, 1891–1922. 4 v. i supp.

[11] GIUSTI, E. «La «Géométrie» di Descartes tra numeri e grandezze». *Giornale critico della filosofia italiana*, 66 (68) (1987), 409–432.

[12] GIUSTI, E. «Algebra and geometry in Bombelli and Viète». *Boll. Storia Sci. Mat.*, 12 (2) (1992), 303–328.

[13] HÉRIGONE, P. *Cursus Mathematicus nova, brevi et clara methodo demonstratus. Per notas reales & universales, citra usum cuiuscumque idiomatis, intellectu, faciles/ Cours Mathematique demonstré d'une nouvelle briefve et Claire methode. Par notes reelles & universelles, qui peuvent estre entendues sans l'usage d'aucune langue*. 5 v. (1634, 1637) i suplement (1642). [Autor i Henry Le Gras, París]

[14] KNOBLOCH, E. «Leibniz's rigorous foundation of infinitesimal geometry by means of Riemannian sums». *Synthese*, 133 (2002), 59–73.

[15] MAHONEY, M. S. *The mathematical career of Pierre de Fermat*. Princeton, N. J.: Princeton University Press, 1973.

[16] MAHONEY, M. S. «The beginnings of algebraic thought in the seventeenth century». A: GAUKROGER, S. (ed.). *Descartes' philosophy, mathematics and phisics*. Brighton: Totowa, Barnes and Noble: Harvester, 1980, 141–156.

[17] MANCOSU, P. *Philosophy of mathematics and mathematical practice in the seventeenth century*. Nova York: The Clarendon Press: Oxford University Press, 1996.

[18] MASSA, M. R. «Mengoli on "quasi proportions"». *Historia Math.*, 24 (3) (1997), 257–280.

[19] MASSA-ESTEVE, M. R. *Estudis matemàtics de Pietro Mengoli (1625–1686): Taules triangulars i quasi proporcions com a desenvolupament de l'àlgebra de Viète*. Tesi doctoral. Universitat Autònoma de Barcelona, 1998, disponible a `http://hdl.handle.net/10803/3103`.

[20] MASSA-ESTEVE, M. R. «La théorie euclidienne des proportions dans les *Geometriæ Speciosae Elementa* (1659) de Pietro Mengoli». *Revue d'Histoire des Sciences*, 56 (2) (2003), 457–474.

[21] MASSA-ESTEVE, M. R. «Algebra and geometry in Pietro Mengoli (1625–1686)». *Historia Mathematica*, 33 (1) (2006), 82–112.

[22] MASSA-ESTEVE, M. R. *L'algebrització de les matemàtiques: Pietro Mengoli*. Barcelona: Institut d'Estudis Catalans, 2006.

[23] MASSA-ESTEVE, M. R. «Symbolic language in early modern mathematics: The *Algebra* of Pierre Hérigone (1580–1643)». *Historia Mathematica*, 35 (4) (2008), 285–301.

[24] MASSA-ESTEVE, M. R. «The symbolic treatment of Euclid's *Elements* in Hérigone's *Cursus mathematicus* (1634, 1637, 1642)». A: HEEFFER, A.; M. VAN DYCK, M. (ed.). *Philosophical aspects of symbolic reasoning in early modern mathematics*. Londres: College Publications, 2010, 165–191. (Studies in Logic; 26)

[25] MASSA-ESTEVE, M. R. «The role of symbolic language in the transformation of mathematics». *Philosophica*, 87 (2012), 153–193.

[26] MASSA-ESTEVE, M. R.; DESHALMS, A. «Euler's beta integral in Pietro Mengoli's works». *Arch. Hist. Exact Sci.*, 63 (3) (2009), 325–356.

[27] MENGOLI, P. *Geometriae speciosae elementa*. Bolonya: 1659.

[28] MENGOLI, P. *Circolo*. Bolonya: 1672.

[29] NATUCCI, A. «Mengoli». A: GILLISPIE, C. C. (ed.). *Dictionary of scientific biography*. Vol. 9. Nova York: Scribner's, 1981, 303–304.

[30] PASCAL, B. *Œuvres complètes*. París: Gallimard, 1954.

[31] TORRICELLI, E. *Opere*. 3 v. LORIA, G. ET AL. (ed.). Faenza: 1919.

[32] VIÈTE, F. *The analytic art*. Nine studies in algebra, geometry and trigonometry from the *Opus restitutae mathematicae analyseos, seu Algebrâ Novâ*. Traducció del llatí i introducció de T. Richard Witmer. Kent, Ohio: Kent State University Press, 1983.

CENTRE DE RECERCA D'HISTÒRIA DE LA CIÈNCIA I DE LA TÈCNICA
DEPARTAMENT DE MATEMÀTIQUES
UNIVERSITAT POLITÈCNICA DE CATALUNYA

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 73–89. DOI: 10.2436/20.2002.01.67

Matar mosques a canonades

Günter M. Ziegler

Resum: La història que expliquem aquí comença amb un petit problema geomètric inofensiu, plantejat el setembre de 2006 en una entrada de blog de R. Nandakumar, un enginyer de Calcuta, a l'Índia. Aquest petit problema és una «mosca»: és temptador, no tan fàcil de resoldre com hom potser podria esperar, i pertany a l'àmbit de les matemàtiques recreatives, sense cap ús pràctic.

Veurem, no obstant això, com aquest petit problema connecta amb matemàtiques molt serioses: per a la modelització d'aquest problema utilitzarem coneixements d'una àrea clau de les matemàtiques aplicades, la teoria del transport optimal. Aquest serà l'escenari per a l'aplicació d'una eina principal de les matemàtiques ben pures, coneguda com a *teoria equivariant d'obstruccions*. Això és un «canó», amb el qual passarem una estona divertida disparant a la mosca.

Per trobar una solució, les propietats combinatòries d'un objecte geomètric molt clàssic, el permutaedre, resulten essencials. Aquestes, al final de la història, ens portaran un altre cop a l'Índia, amb algun viatge en el temps que ens farà retrocedir cent anys cap al passat: per al darrer pas en la nostra solució (parcial) del problema de la mosca necessitem una propietat senzilla dels números del triangle de Pascal, que va ser observada per primer cop per Balak Ram, a Madràs, l'any 1909.

Però, fins i tot si el problema d'existència s'ha resolt, el petit problema geomètric encara no: si existeix solució, com podem trobar-ne una? Aquest problema es deixarà al lector. En canvi, parlarem de la relació tibant entre canons i mosques, i acabarem citant un poema de Hans Magnus Enzensberger.

Paraules clau: particions d'un polígon, espais de configuracions, teoria d'obstruccions, coeficients binomials, matemàtica pura i aplicada.

Classificació MSC2010: 00A08, 52A38, 55P91, 55R80.

Aquest treball va aparèixer en anglès amb el títol «Cannons at Sparrows» a *Eur. Math. Soc. Newsl.*, 95 (2015), 25–31. Agraïm als editors d'aquesta revista el permís per publicar-ne la traducció al català, revisada per Arnau Padrol.

Una mosca

El dijous 28 de setembre de 2006, ben d'hora al matí, a les 6.57, l'enginyer R. Nandakumar, que s'autoqualifica de «programador informàtic, estudiant de matemàtiques i espècie d'escriptor», va penjar al seu blog «Tech Musings» (`nandacumar.blogspot.de`) la conjectura següent sobre geometria del pla, la qual havia formulat conjuntament amb el seu amic R. Ramana Rao:

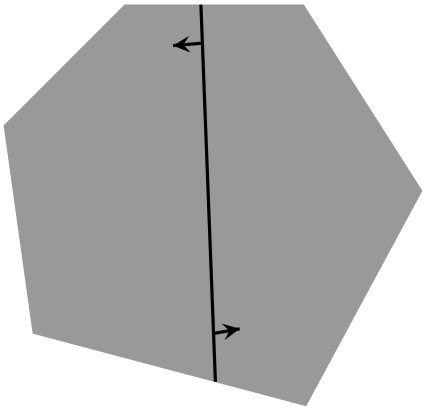
> Donada una regió convexa i un número natural n, existeix com a mínim una manera de trobar una partició de la regió en n trossos convexos de tal manera que tots els trossos tinguin la mateixa àrea i el mateix perímetre.

Aquest problema sembla completament inofensiu. Podria ser un problema de geometria de secundària? O potser sembla un problema d'Olimpíada Matemàtica? Penseu-hi vosaltres mateixos! Per exemple, podeu prendre un triangle i $n = 3$ o $n = 6$. De fet, com el mateix Nandakumar fa notar, no és evident ni tan sols com es pot dividir un triangle equilàter en $n = 5$ trossos convexos de la mateixa àrea i el mateix perímetre. Alguna idea? Proveu-ho!

El problema va captar l'atenció de la comunitat de geometria computacional després que Nandakumar el posés a la web «Open Problem Garden» (`openproblemgarden.org`) el desembre de 2007. Després, l'11 de desembre de 2008, Nandakumar i Ramana Rao van anunciar el seu primer progrés a arXiv (`arXiv:0812.2241`):

> Presentem una demostració senzilla del fet que la resposta al problema és «Sí» per a $n = 2$ (dues peces) i donem alguns arguments que indiquen amb força seguretat que la resposta també és «Sí» per a $n = 3$.

Fem-ho per a $n = 2$. Tota divisió d'un polígon convex en dues parts convexes prové d'un tall fet amb una recta. Observem que hi ha una (única!) recta vertical que divideix el polígon en dues parts convexes de la mateixa àrea. En general no tindrem sort i el perímetre del tros que quedi a la dreta de la recta, per exemple, serà més gran que el perímetre del tros que quedi a l'esquerra.



Ara fem girar la recta que biseccIona el polígon. És fàcil comprovar (!) que si girem de manera que sempre dividim l'àrea en dues parts iguals, llavors els perímetres de les parts que queden a la dreta i a l'esquerra de la recta varien *de manera contínua*. Per tant, també la quantitat «perímetre a la dreta menys perímetre a l'esquerra» varia de manera contínua. Un cop hàgim fet mitja volta, de 180 graus, el valor d'aquesta quantitat haurà canviat de signe. Si inicialment era positiva, serà negativa després de la mitja volta i, per continuïtat, haurà d'haver «tocat el zero» en algun moment entremig. Així doncs, una partició «justa» en $n = 2$ trossos existeix segons el *teorema del valor intermedi*.

Així que el problema està resolt, però com l'hem resolt? Ens hem adonat que l'espai de configuracions de totes les divisions en dos trossos convexos és un cercle (parametritzat per l'angle de la recta de divisió). I hem fet servir la continuïtat i hem aplicat un teorema topològic, el teorema del valor intermedi. Des del punt de vista de la topologia, això és el cas $d = 1$ del fet que no hi ha cap aplicació contínua entre les esferes $S^d \to S^{d-1}$ que apliqui punts oposats de S^d en punts oposats de S^{d-1}, el *teorema de Borsuk-Ulam* [13].

El problema semblava inofensiu però la topologia hi ha entrat, fins i tot en el cas $n = 2$. Nandakumar i Ramana Rao no van trobar una prova per al cas $n = 3$. Però uns quants dies després de publicar el seu *preprint*, el 16 de desembre de 2008, Imre Bárány, Pavle Blagojević i András Szűcs van enviar un article amb la solució per a $n = 3$ a l'*Advances in Mathematics*. Va ser publicat digitalment el setembre de 2009 i en versió impresa el 2010 com un article d'*Advances* de 15 pàgines, [2]. Potser això demostra que el petit i inofensiu problema «mosca» és més difícil del que semblava a primera vista.

Les canonades, I

Ens podem preguntar: quin és l'aspecte de l'espai de totes les particions d'un polígon en tres trossos convexos? Blagojević i d'altres a [2] el van descriure com una part d'una varietat de Stiefel. I pel que fa a l'espai de les particions en n trossos de la mateixa àrea? D'això no se'n sap res! (León a [12] en donarà alguna orientació). En aquesta qüestió un *ansatz* de la teoria del transport optimal hi intervé de manera essencial —el primer a observar-ho va ser Roman Karasev de Moscou.

El transport optimal és un tema antic iniciat per l'enginyer francès Gaspard Monge l'any 1781. El resultat clau que ara necessitem va ser obtingut per Leonid Kantoròvitx a finals dels anys trenta. (Per la seva obra Kantoròvitx va obtenir el Premi Stalin l'any 1949 i el Premi Nobel d'economia el 1975.) Aquesta àrea és ben viva, com ho han posat de manifest dos llibres recents, cabdals, publicats per Cédric Villani (Medalla Fields del 2010).

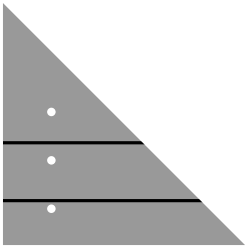
El nostre problema es resol amb la construcció de «diagrames de Voronoi amb pesos»: donada qualsevol massa (l'àrea d'un polígon convex) i un conjunt de llocs amb pesos (és a dir, n punts diferents i números reals associats a aquests de suma total nul·la), assignem a cada lloc tots els punts del polígon per als quals «la distància al lloc al quadrat menys el pes de la ubicació» és mínima. Això dóna una partició del polígon convex en trossos convexos!

El resultat que necessitem és el següent:

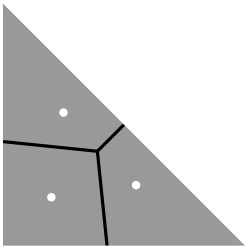
TEOREMA 1 (KANTORÒVITX [1938] ET AL.). *Donat un conjunt de $n \geq 2$ punts diferents del pla, i un polígon qualsevol, existeix una assignació* única *de pesos de manera que el diagrama de Voronoi amb pesos per a aquests punts i aquests pesos subdivideix el polígon en n trossos convexos de la mateixa àrea.*

Dit d'una altra manera, l'espai de configuracions $F(\mathbb{R}^2, n)$ de totes les ènuples de punts diferents en el pla parametritza les particions de Voronoi amb pesos en n trossos convexos de la mateixa àrea. Per què ens ajuda aquest resultat? Perquè entenem molt bé l'espai $F(\mathbb{R}^2, n)$!

Suposem, per exemple, que el polígon sigui un triangle i $n = 3$. Si els tres punts es troben sobre una recta vertical, llavors la partició en trossos de la mateixa àrea tindria aquest aspecte:



Ara bé, si tenim la sort de triar els tres punts de manera adequada, llavors podem aconseguir una partició en trossos de la mateixa àrea i el mateix perímetre:

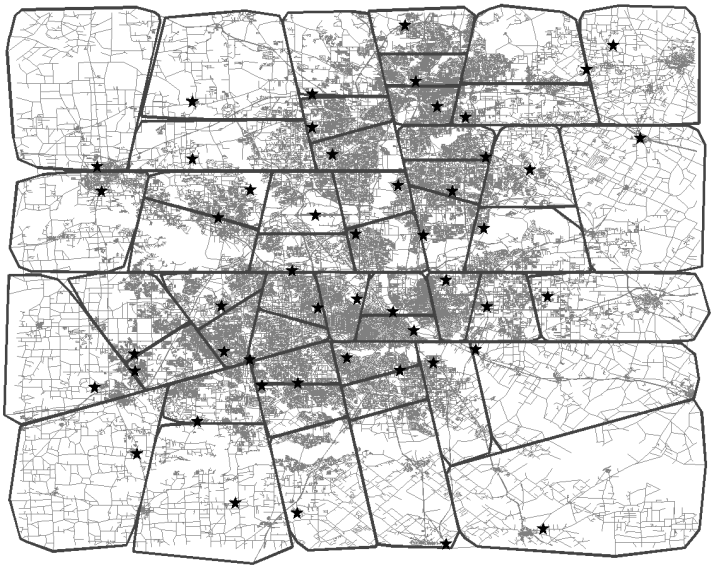


És, però, sempre possible fer una «elecció afortunada» per als n punts?

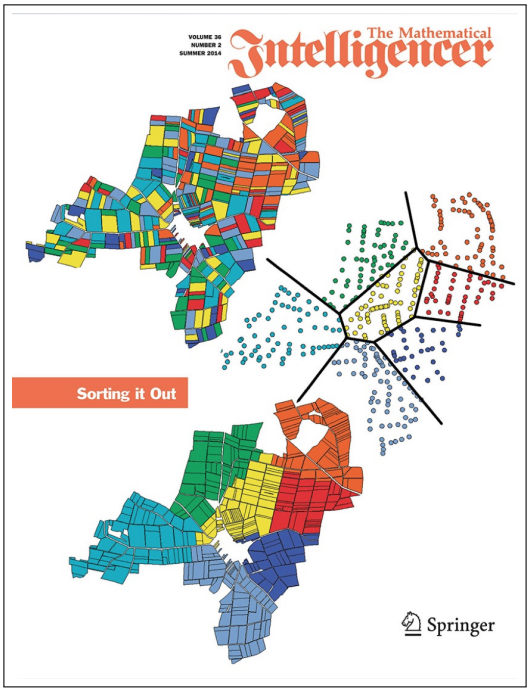
Un comentari

El transport optimal té un vessant pràctic que el fa molt útil en investigació operativa. Això està exemplificat de manera gràfica, entre d'altres, pels treballs de John Gunnar Carlsson, del departament d'enginyeria industrial i de sistemes, de la Universitat de Califòrnia del Sud:[1]

1 La figura mostra el mapa d'una ciutat, en el qual cada zona conté la mateixa longitud total de carrers. Això és útil per a les empreses que proporcionen màquines llevaneus o serveis de neteja, o que reparteixen correu i que han de recórrer els carrers de cada zona d'una manera eficient: establint aquestes zones tots els vehicles de l'empresa tindran la mateixa feina.



o els de Peter Gritzmann, del departament de matemàtiques, de la Universitat Politècnica de Munic, que utilitza el transport optimal per a la reassignació de terrenys de conreu a les àrees rurals de Baviera:



The Mathematical Intelligencer, 36 (2), 2014.
Amb l'amable permís de Springer Science+Business Media.

D'altra banda, el transport optimal és important en física (i també en matemàtiques molt dures, si s'hi dedica Villani). On l'hem de col·locar, doncs?

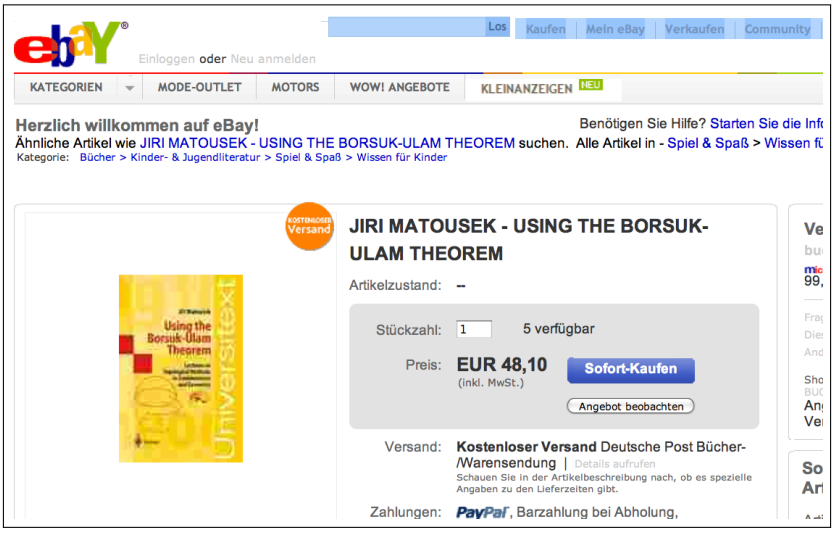
La resposta és que les categories tradicionals simplement ja no serveixen i les hauríem de descartar. El que s'ha vist fins ara és un problema de «matemàtica recreativa» que, per ser modelitzat i resolt, necessita mètodes de «matemàtica aplicada» (com el transport optimal) i de «matemàtica pura» (topologia algebraica). Les matemàtiques pures, les aplicades i les recreatives no es poden separar i no s'haurien de separar. Hi ha també altres parts de la ciència que pertanyen a les matemàtiques *sense fronteres*, com ara la informàtica (teòrica) i la investigació operativa (matemàtica). Si és ciència de qualitat, diguem-ne, senzillament, «matemàtiques».

A Berlín, en el context del centre de recerca MATHEON, Mathematics for Key Technologies, intentem evitar totes aquestes categories —al final, l'única distinció que podríem fer seria entre «matemàtiques» i «aplicacions de les matemàtiques».

La qüestió, en aquest article, és però una altra: a les matemàtiques hi ha «grans teories» i «petits problemes». De vegades podem necessitar grans teories per resoldre problemes (aparentment) petits i ara en discutim un exemple. De totes maneres, alhora, això funciona també en sentit contrari: fem servir problemes petits per posar a prova les grans teories, per veure què podem fer amb un problema concret. Hi ha grans teories en els prestatges de les biblioteques universitàries per a les quals mai no hi ha hagut cap càlcul concret o exemple resolt...

Les canonades, II

El segon tipus de canonades que farem servir prové de la topologia algebraica. Concretament, hi ha un procediment de modelització ben conegut, anomenat esquema d'espai de configuracions/aplicació de prova (CS/TM), desenvolupat per Sarkaria, Živaljević i d'altres, que converteix problemes de geometria discreta en qüestions de topologia algebraica equivariant. Dit d'una manera resumida, es prova que si el problema té un contraexemple, llavors hi ha espais topològics X i Y, on X és un *espai de configuracions* per al problema i Y és un espai de valors (sovint una esfera), i un grup finit de simetries G tals que hi ha una aplicació contínua $X \to_G Y$ que conserva les simetries. En conseqüència, si no existeix cap aplicació equivariant $X \to_G Y$ llavors no hi ha contraexemples i el problema està resolt. El teorema de Borsuk-Ulam, que diu que no hi ha cap aplicació $S^d \to_{\mathbb{Z}/2} S^{d-1}$, és el primer exemple important d'un teorema d'aquest tipus. Tot això està meravellosament explicat en el llibre *Using the Borsuk-Ulam theorem*, de Jiří Matoušek [13]. De fet, tothom l'hauria de conèixer ja que és un «material per a nens» —tal com podeu comprovar si busqueu el llibre a *ebay*, on el vaig trobar catalogat a la llista de «divertiments i jocs per a nens»!



Bé, si aquest joc de nens no ens és suficient, farem servir instruments més seriosos per a tractar el petit problema de la partició d'un polígon; concretament, la teoria equivariant d'obstruccions. Es tracta d'un mètode per a decidir sistemàticament si existeixen aplicacions equivariants $X \to_G Y$. Es pot trobar exposat d'una manera extraordinàriament clara i precisa (tot i que sense dibuixos ni exemples) a la secció II.3 del llibre *Transformation groups*, de Tammo tom Dieck [8]. Per tal de veure que hi ha una elecció afortunada per a les configuracions de punts que garanteix particions del nostre polígon amb la mateixa àrea i el mateix perímetre —per a algun n—, hem d'interpretar i avaluar els termes que apareixen en el resultat següent, en el cas del nostre problema:

Obstruction theory 115

(3.15)). If X_1 is path-connected, then so is X_k for $k \geqq 1$. Then the first main result of obstruction theory is

(3.10) Theorem. *For each integer $n \geq 1$ there exists an exact obstruction sequence*

$$[X_{n+1}, Y]_G \to \mathrm{Im}([X_n, Y]_G \to [X_{n-1}, Y]_G) \xrightarrow{c^{n+1}} \mathfrak{H}_G^{n+1}(X, A; \pi_n Y)$$

which is natural in (X, A) and Y.

The exactness of this sequence means that each homotopy class $X_{n-1} \to Y$ which is extendable over X_n has an associated obstruction element in the cohomology group $\mathfrak{H}_G^{n+1}(X, A; \pi_n Y)$ (as defined in (3.3)); this obstruction element is zero if and only if the homotopy class $X_{n-1} \to Y$ is extendable over X_{n+1}.

Alguns detalls

L'esquema CS/TM per al nostre problema ens porta d'una manera natural al plantejament següent:

$$\mathcal{F}(2,n) \underset{\mathfrak{S}_n}{\longrightarrow} F(\mathbb{R}^2,n) \underset{\mathfrak{S}_n}{\longrightarrow} \mathrm{EAP}(P,n) \underset{\mathfrak{S}_n}{\longrightarrow} S^{n-2}.$$

Es tracta d'una cadena d'objectes molt concrets (que són espais topològics) i d'aplicacions equivariants desconegudes (que són aplicacions contínues que respecten la simetria en relació amb el grup $\mathfrak{S}_n$ de permutacions):

- $\mathrm{EAP}(P,n)$ és l'espai de configuracions de totes les particions de P en n trossos convexos de la mateixa àrea, el qual és un espai de configuracions *no* gaire ben entès (vegeu León [12]).
- S^{n-2} representa una $(n-2)$-esfera particular, definida per

$$\{y \in \mathbb{R}^n : \quad y_1 + \cdots + y_n = 0, \\ y_1^2 + \cdots + y_n^2 = 1\}.$$

  Sobre aquesta esfera, el grup $\mathfrak{S}_n$ hi actua simplement per permutació de les coordenades.

- $\mathrm{EAP}(P,n) \to S^{n-2}$ envia cada partició en n trossos de la mateixa àrea $(P_1,\ldots,P_n)$ a «perímetres menys la mitjana, normalitzats» per tal d'obtenir un punt de l'esfera —sota la hipòtesi que no hi ha cap partició per a la qual tots els perímetres siguin iguals. Aquesta aplicació és $\mathfrak{S}_n$-equivariant: una permutació dels trossos P_i correspon a una permutació dels perímetres normalitzats i, per tant, de les coordenades de l'esfera.

- $F(\mathbb{R}^2,n)$ és l'espai de configuracions de n punts diferents, etiquetats, en el pla

$$\{(x_1,\ldots,x_n) \in \mathbb{R}^{2\times n} : x_i \neq x_j \text{ for } i<j\}.$$

  En contrast amb $\mathrm{EAP}(P,n)$, aquest espai està *força* ben entès. És el complementari d'un arranjament d'hiperplans complexos i això explica bona part de la seva geometria i la seva topologia; la literatura rellevant comença amb un article clàssic de l'any 1962 de Fox i Neuwirth [9].

- $F(\mathbb{R}^2,n) \to \mathrm{EAP}(P,n)$ és l'aplicació de transport optimal, quan fa correspondre a $(x_1,\ldots,x_n)$ el seu diagrama de Voronoi amb pesos amb totes les cel·les de la mateixa àrea. Es tracta d'una aplicació ben definida, contínua i equivariant, l'existència de la qual és deguda a Kantoròvitx (1938); una referència recent interessant és Geiß, Klein, Penninger i Rote [10].

- $\mathcal{F}(2,n)$ és un complex cel·lular finit i regular que modela $F(\mathbb{R}^2,n)$ —de fet, és un retracte de deformació equivariant. És de dimensió $n-1$, té $n!$ vèrtexs, indexats per permutacions (que corresponen a configuracions

de punts en el pla en les quals els punts estan ordenats d'esquerra a dreta d'acord amb una determinada permutació), i té $n!$ cel·les maximals, també indexades per permutacions (que corresponen a configuracions de punts en el pla en les quals els punts estan sobre una recta vertical, ordenats d'acord amb una determinada permutació). Aquestes cel·les maximals tenen l'estructura combinatòria d'uns politops *ben* clàssics: els permutaedres!

Aquest model de complex cel·lular sembla que va ser descrit explícitament per primera vegada a [7], tot i que un altre cop ens podem remuntar fins a Fox i Neuwirth [9].

- $\mathcal{F}(2,n) \to F(\mathbb{R}^2,n)$ és també una aplicació explícita, una inclusió equivariant.

Aquests són els (molts) elements que entren en joc. El resultat és que si suposem que per a algun n i per a algun P no hi ha cap partició en n trossos de la mateixa àrea i el mateix perímetre, llavors existeix una aplicació equivariant:

$$\mathcal{F}(2,n) \underset{\mathfrak{S}_n}{\longrightarrow} S^{n-2}.$$

Existeix una aplicació com aquesta? Aquest és el tipus de preguntes que es poden respondre amb la teoria equivariant d'obstruccions (EOT).

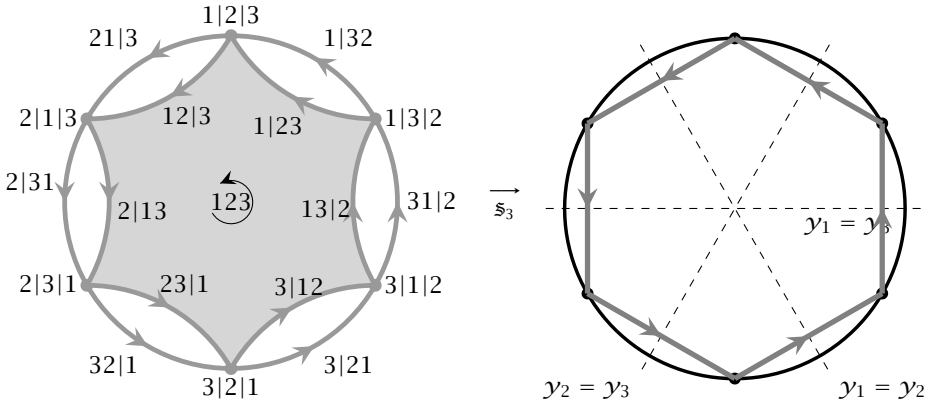
Què fa la EOT? Construeix l'aplicació de manera progressiva, pujant per les dimensions de l'esquelet del complex cel·lular $(n-1)$-dimensional $\mathcal{F}(2,n)$. Com que apliquem un espai amb una acció lliure d'un grup en una esfera de dimensió $n-2$, no hi ha cap problema, tret potser del darrer cas, on l'aplicació ja està fixada a les fronteres ∂c_σ de les $(n-1)$-cel·les c_σ, que són homeomorfes a $(n-2)$-esferes.

L'extensió és possible sense cap problema si totes les aplicacions $f\colon \partial c_\sigma \to S^{n-2}$ tenen grau 0. I, efectivament, totes les aplicacions tenen el mateix grau, ja que busquem aplicacions equivariants. Tanmateix, aquest grau no serà 0 en general, ja que potser hem fet errors en cel·les de dimensió inferior en el camí cap al cim. EOT ens diu ara que l'aplicació es pot *modificar en l'esquelet* $(n-2)$*-dimensional* de tal manera que es pugui estendre a tot el complex *si i només si* alguna classe de cohomologia equivariant amb coeficients no constants en el grup d'homologia $(n-2)$-dimensional d'una $(n-2)$-esfera, la «classe d'obstrucció», s'anul·la. Ho fa?

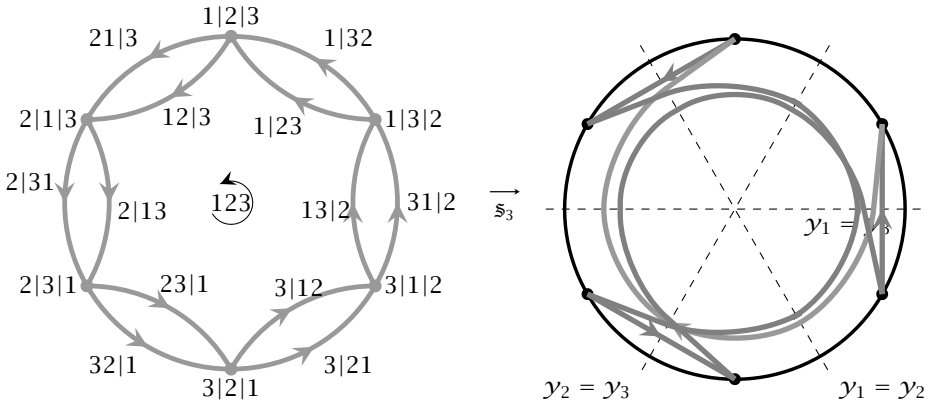
Un passi d'imatges

Per a $n=3$, hem d'esbrinar si existeix una aplicació $\mathfrak{S}_3$-equivariant $\mathcal{F}(2,3) \longrightarrow S^1$. L'espai $\mathcal{F}(2,3)$ és un complex cel·lular amb 6 vèrtexs, 12 arestes i 6 2-cares hexagonals. A la nostra figura només es mostra un dels hexàgons; però un hexàgon és tan bo com tots junts, atès que una aplicació equivariant queda especificada per la seva imatge en qualsevol dels hexàgons.

Hem d'aplicar l'1-esquelet (graf) del complex cel·lular, en particular la frontera de l'hexàgon, de manera que l'aplicació es pugui estendre a l'interior, com una aplicació al cercle S^1, que *no* té interior. L'aplicació equivariant «òbvia» porta la frontera de l'hexàgon al cercle, girant una volta, tal com indiquen les sis arestes orientades. Això es pot interpretar com una aplicació entre 1-esferes de grau 1, i per tant no s'estén a l'hexàgon.



Podríem intentar modificar l'aplicació canviant-la en una de les sis arestes de l'hexàgon. Tanmateix, com que hem de mantenir l'aplicació *equivariant*, l'aplicació s'hauria de canviar simultàniament a tota l'òrbita, és a dir, a totes les imatges de la nostra aresta per l'acció del grup de permutacions. Ara bé, es pot comprovar que qualsevol canvi de l'aplicació en una aresta afecta dues arestes més de l'hexàgon, tal com s'indica en aquesta figura:



Podem aconseguir una aplicació de grau 0, i per tant una aplicació que es pugui estendre a l'interior de l'hexàgon, fent canvis equivariants com els que hem indicat (sobre ternes d'arestes)? No és difícil veure que això equival al fet

següent. Una aplicació equivariant

$$\mathcal{F}(2,3) \underset{\mathfrak{S}_3}{\longrightarrow} S^1$$

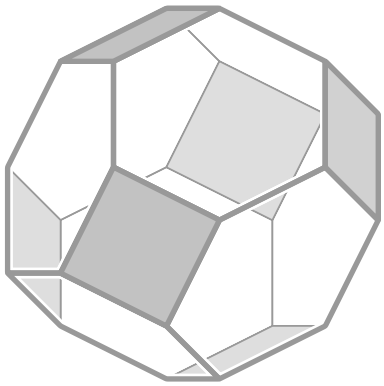
existeix si i només si hi ha una solució de l'equació

$$1 + 3x_1 + 3x_2 = 0$$

amb valors de x_1, x_2 enters, afirmació que és evidentment falsa. En conseqüència, atès que l'aplicació *no* existeix, el contraexemple a la conjectura de Nandakumar i Ramana Rao per a $n = 3$ no existeix. I, per tant, hem establert el cas $n = 3$ (!).

Què passa per a $n = 4$? Resulta que és un problema bastant semblant al cas anterior, però ara a l'esquerra tenim un complex cel·lular de dimensió 3, amb $4! = 24$ vèrtexs i 24 cel·les maximals, que tenen la combinatòria d'un permutaedre. (Els permutaedres estan explicats, per exemple, a [16], que a *ebay* es pot trobar classificat a la categoria d'«esoterisme»...)

Aquí teniu la imatge de la situació:



$\underset{\mathfrak{S}_4}{\longrightarrow} S^2$

Es pot veure fàcilment que les 14 cares del permutaedre es divideixen en tres classes d'equivalència separades (òrbites) per l'acció del grup simètric $\mathfrak{S}_4$: són l'òrbita dels 6 quadrats i 2 òrbites de 4 hexàgons cadascuna. Trobem així que una aplicació equivariant

$$\mathcal{F}(2,4) \underset{\mathfrak{S}_4}{\longrightarrow} S^2$$

existeix si i només si hi ha una solució de l'equació

$$1 + 4x_1 + 6x_2 + 4x_3 = 0$$

amb valors enters x_1, x_2, x_3, la qual cosa és, evidentment, impossible.

Veieu el patró, doncs? Per a n qualsevol, hi ha una aplicació equivariant

$$\mathcal{F}(2,n) \underset{\mathfrak{S}_n}{\longrightarrow} S^{n-2}$$

si i només si l'equació

$$1 + \binom{n}{1} x_1 + \cdots + \binom{n}{n-1} x_{n-1} = 0$$

té una solució amb valors enters, és a dir, si la fila enèsima del triangle de Pascal, un cop tret l'1 del final, no té cap factor comú.

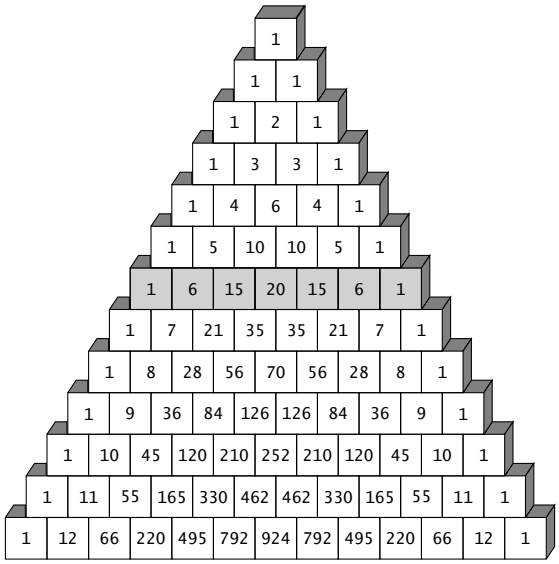
La reina

Hem començat amb un problema senzill de geometria discreta penjat a un blog a l'Índia el 2006 i el trajecte que hem fet fins aquí ens ha portat a fer servir el transport optimal, a idear una estratègia amb aplicacions contínues equivariants, és a dir, topologia, i a calcular la classe d'obstrucció en la cohomologia equivariant. Aquesta classe d'obstrucció no s'anul·la, és a dir, no existeix una aplicació equivariant, si una determinada equació diofàntica no té solució. Hem arribat a la teoria de números.

> Les matemàtiques són —en paraules de Gauss— la reina de les ciències i la teoria de números és la reina de les matemàtiques.
> Sovint condescendeix a servir l'astronomia i altres ciències naturals però en totes les seves relacions ocupa el primer lloc.

Coneixem aquestes paraules a través de Wolfgang Sartorius von Waltershausen, un amic de Gauss que va pronunciar el panegíric a la seva tomba i va escriure la seva primera biografia. Sartorius von Waltershausen era un geòleg i Gauss havia treballat dur en geografia («mesurant el món») i també en astronomia (la redescoberta de Ceres el va fer famós l'any 1801 i no pas les *Disquisitiones Arithmeticae*, que ningú no va entendre aleshores). Per tant, l'afirmació de Gauss sobre la teoria de números com la reina de les matemàtiques i de les matemàtiques com la reina de les ciències és autèntica i té el seu pes.

I tal com passa sovint, per al nostre problema, l'última paraula també pertany a la teoria de números. Podeu manipular fàcilment el triangle de Pascal; és un joc de nens. Probablement us encallareu a la sisena línia —com a la figura següent (extreta del llibre per a nens *El dimoni dels nombres* de l'escriptor alemany Hans Magnus Enzensberger).



Gràfic adaptat de la il·lustració de Rotraut Susanne Berner, del llibre
Der Zahlenteufel (*El dimoni dels nombres*), de Hans Magnus Enzensberger

En efecte, per a $n = 6$, tenim l'equació

$$1 + 6x_1 + 15x_2 + 20x_3 + 15x_4 + 6x_5 = 0$$

que *té* una solució entera (serveix $x_1 = x_2 = -1$, $x_3 = 1$ i $x_4 = x_5 = 0$) i, en conseqüència, l'aplicació *existeix*...

I què té el 6 d'especial? I què passa per a n qualsevol? Aquesta pregunta ens porta a l'Índia una altra vegada, però uns cent anys enrere. Al començament del primer volum del *Journal of the Mathematics Club* de Madràs (aquest és el lloc i l'època d'on procedeix Ramanujan!), Balak Ram va publicar el resultat següent:

TEOREMA 2 (BALAK RAM [15]). *L'equació*

$$1 + x_1\binom{n}{1} + \cdots + x_{n-1}\binom{n}{n-1} = 0$$

no té cap solució amb $x_1, \ldots, x_{n-1}$ *enters, és a dir, l'interior de la fila* n *del triangle de Pascal té un factor comú, si i només si* n *és potència d'un primer.*

Així doncs, el problema de Nandakumar i Ramana Rao queda resolt quan n és potència d'un primer però continua obert en el cas general, ara com ara.

TEOREMA 3 (BLAGOJEVIĆ I ZIEGLER [7]). *Si* n *és potència d'un primer, llavors tot polígon admet una partició «justa» en* n *trossos.*

En tots els altres casos, per a $n = 6, 10, 12, \ldots$, el problema queda obert —tot i que a [7] provem un teorema molt més general que justament es compleix si i només si n és potència d'un primer. També aquí el resultat se segueix del nostre càlcul EOT: *existeix una aplicació contínua equivariant*

$$F(\mathbb{R}^2, n) \underset{\mathfrak{S}_n}{\longrightarrow} S^{n-2}$$

si i només si n no és potència de primer.

Tres observacions (sobre les demostracions) abans d'acabar

Primera observació (sobre les demostracions en públic)

Segons Victor Klee (1925-2007):

> Les demostracions s'haurien de comunicar només entre adults que ho consentin i en privat.

El que hem presentat aquí, evidentment, no és una demostració sinó només un esbós. Hi falta omplir els detalls. Els detalls són importants.

Segona observació (sobre les demostracions senzilles/boniques)

Potser coneixeu la història de Paul Erdős sobre EL LLIBRE, que Déu manté i que conté les demostracions boniques, les demostracions perfectes, les demostracions perfectament senzilles, les *demostracions del LLIBRE* de teoremes matemàtics. Com al mateix Erdős li agradava dir, un matemàtic no cal que cregui en Déu però hauria de creure en EL LLIBRE. (De passada cal dir que aquesta citació d'Erdős no apareix a la traducció al farsi de [1] del 2001.)

D'altra banda, no tothom està d'acord amb la primera part, tampoc. A Solomon Lefschetz (1884–1972), el semidéu de les matemàtiques de Princeton, se li atribueix haver dit:

> No em vingueu amb les vostres demostracions boniques. No ens preocupem per aquests infantilismes per aquí.

... en particular, quan els seus estudiants es presentaven amb demostracions més senzilles o més completes dels seus resultats.

Tercera observació (sobre les demostracions correctes)

Sobre Solomon Lefschetz, es va dir:

> No va escriure mai una demostració correcta ni va enunciar un teorema incorrecte.

Aparentment, hi havia una part important de veritat en aquesta afirmació i, en part, era inevitable. Lefschetz va ser un pioner en la utilització de mètodes topològics en geometria algebraica. Ell mateix ho va descriure així més endavant:

> Tal com ho veig, temps enrere em va tocar clavar l'arpó de la topologia algebraica dins del cos de la balena de la geometria algebraica.

De totes maneres, ho va fer en un moment en el qual els fonaments matemàtics sòlids de la topologia algebraica encara no s'havien establert i, per tant, hi havia risc i emoció en el fet d'utilitzar mètodes topològics aleshores. Crec que avui hi ha menys risc però no menys emoció.

Quarta observació (sobre les demostracions correctes, II)

Fent matemàtiques, ens guiem per la intuïció i sovint «creiem» més coses de les que podem provar rigorosament. Això porta a enunciats del tipus següent:

> Provem que la resposta és afirmativa per a $n = 4$ i també discutim potències de 2 més altes.

Això està tret de la versió final en *preprint* (la sisena) a `arXiv:0812.2241v6` de l'article de Nandakumar i Ramana Rao [14]. A la versió publicada diu:

> Donem una prova elemental del fet que la resposta és afirmativa per a $n = 4$ i ho generalitzem a potències de 2 més altes.

Efectivament, a [14] s'exposen idees boniques però les proves que es donen per a $n = 4$ i les que s'indiquen per a potències de 2 superiors s'han d'elaborar més.[2] Per una altra banda, Karasev, Hubard i Aronov donen una prova diferent per al cas de potència d'un primer en el problema de Nandakumar i Ramana Rao, publicada a *Geometriae Dedicata* el 2014 [11]. Sembla que no hi ha cap manera de fer rigorós i complet el seu enfocament, un fet que comportaria establir una relació entre la classe d'Euler i les classes d'homologia induïdes per seccions transversals generals.[3] Karasev ho resumeix a la seva pàgina web de la manera següent:

> En aquesta versió donem uns enunciats més clars i una mica més generals dels teoremes principals i ens esforcem a explicar la prova del lema topològic. El nostre mètode amb vista a provar el lema topològic és el mateix que van fer servir D. B. Fuks i V. A. Vasiliev en els casos particulars que van tractar. Una altra aproximació, més tècnica i més rigorosa, al lema topològic es pot trobar a l'article `arXiv:1202.5504` de P. Blagojević i G. Ziegler.

2 Per exemple, el lema 4 de [14] no és cert tal com està enunciat, com es pot comprovar en el cas especial d'un quadrat per al qual una bisecció per una recta vertical dóna lloc a dos rectangles que tenen particions justes en dues parts convexes amb un rang de perímetres que varia contínuament, però per a una bisecció pròxima a la vertical els quadrilàters que s'obtenen només tenen un nombre finit de particions justes.

3 Karasev i d'altres també van considerar el problema de la no existència de l'aplicació equivariant $F(\mathbb{R}^d, n) \to S^{n-2}$ en el cas que n sigui potència d'un primer. Amb aquesta finalitat, van intentar provar que la classe d'Euler amb coeficients girats d'un fibrat vectorial natural sobre la varietat oberta $F(\mathbb{R}^d, n)/\mathfrak{S}_n$ no és nul·la. Tanmateix, la relació entre una secció transversal genèrica i la classe d'Euler del fibrat via la dualitat de Poincaré falla per a varietats obertes. Per a una discussió més detallada, vegeu [7, p. 51].

Cinquena observació (sobre comptar)

Havíem promès de fer tres observacions. Però tots sabem que hi ha tres classes de matemàtics: els que saben comptar i els que no en saben.

Un poema abans d'acabar

Aquest article pretén demostrar com un «problema petit com una mosca» serveix com a banc de proves per a alguns «canons de les grans teories». De problemes petits com una mosca n'hi ha molts més, com ara un problema d'incidència múltiple conegut com el problema de Tverberg amb colors (vegeu, per exemple, [17] i [4]) o el problema de l'existència d'aplicacions altament regulars de $\mathbb{R}^d \to \mathbb{R}^N$, contínues i que transformin k punts diferents en vectors linealment independents [6]. Els progressos en aquests problemes no només fan servir teories topològiques complicades sinó que depenen també del progrés en la comprensió i en el càlcul d'informació subtil de topologia algebraica sobre els espais de configuracions i del desenvolupament de teoria avançada. Així doncs, hom fa també progressos dins de la topologia algebraica, els quals ens han permès de resoldre problemes tècnics plantejats fa temps, com ara la conjectura generalitzada de Vassiliev [3].

En resum, la relació entre les mosques i les canonades és força més complicada del que es podria pensar a primera vista. Nosaltres *disparem* canonades a les mosques però, de vegades, les mosques s'hi tornen. Deixem parlar el poeta:

Dos errors

Reconec que, en el seu moment,
vaig disparar mosques contra canons.

No en vaig encertar cap de ple,
ho admeto.

[. . .]

Disparar canonades a les mosques, però,
hagués estat caure en l'error oposat.

Hans Magnus Enzensberger

Agraïments

Gràcies a Pavle Blagojević, que ha estat un company meravellós durant molts anys i en molts viatges, i a Arnau Padrol per la revisió de la traducció de l'article i la traducció del poema.

Referències

[1] Aigner, M.; Ziegler, G. M. *Proofs from The Book*. 5a ed. Berlín: Springer-Verlag, 2014.

[2] Bárány, I.; Blagojević, P.; Szűcs, A. «Equipartitioning by a convex 3-fan». *Adv. Math.*, 223 (2) (2010), 579–593.

[3] Blagojević, P. V. M.; Cohen, F. R.; Lück, W.; Ziegler, G. M. «On complex highly regular embeddings and the extended Vassiliev conjecture». *Int. Math. Research Notes (IMRN)* (2015), 49 p.

[4] Blagojević, P. V. M.; Frick, F.; Ziegler, G. M. «Tverberg plus constraints». *Bull. Lond. Math. Soc.*, 46 (5) (2014), 953–967.

[5] Blagojević, P. V. M.; Lück, W.; Ziegler, G. M. «Equivariant topology of configuration spaces». *J. Topol.*, 8 (2) (2015), 414–456.

[6] Blagojević, P. V. M.; Lück, W.; Ziegler, G. M. «On highly regular embeddings». *Trans. Amer. Math. Soc.* Publicat en línia (maig 2015), disponible a arXiv:1305.7483.

[7] Blagojević, P. V. M.; Ziegler, G. M. «Convex equipartitions via equivariant obstruction theory». *Israel J. Math.*, 200 (1) (2014), 49–77.

[8] tom Dieck, T. *Transformation groups*. Berlín: Walter de Gruyter & Co., 1987. (de Gruyter Studies in Mathematics; 8)

[9] Fox, R.; Neuwirth, L. «The braid groups». *Math. Scand.*, 10 (1962), 119–126.

[10] Geiß, D.; Klein, R.; Penninger, R.; Rote, G. «Optimally solving a transportation problem using Voronoi diagrams». *Comput. Geom.*, 46 (8) (2013), 1009–1016.

[11] Karasev, R.; Hubard, A.; Aronov, B. «Convex equipartitions: the spicy chicken theorem». *Geom. Dedicata*, 170 (2014), 263–279.

[12] León, E. *Spaces of convex n-partitions*. Tesi doctoral, FU Berlín, 2015.

[13] Matoušek, J. *Using the Borsuk-Ulam theorem*. Lectures on topological methods in combinatorics and geometry. Berlín: Springer-Verlag, 2003. (Universitext)

[14] Nandakumar, R.; Ramana Rao, N. «Fair partitions of polygons: an elementary introduction». *Proc. Indian Acad. Sci. Math. Sci.*, 122 (3) (2012), 459–467.

[15] Ram, B. «Common factors of $\frac{n!}{m!(n-m)!}$, $(m = 1, 2, \ldots, n-1)$». *J. Indian Math. Club (Madras)*, 1 (1909), 39–43.

[16] Ziegler, G. M. *Lectures on polytopes*. Nova York: Springer-Verlag, 1995. (Graduate Texts in Mathematics; 152)

[17] Ziegler, G. M. «3N colored points in a plane». *Notices Amer. Math. Soc.*, 58 (4) (2011), 550–557.

Inst. Mathematik
FU Berlin
Arnimallee 2
14195 Berlin, Germany
ziegler@math.fu-berlin.de

Butlletí de la Societat Catalana de Matemàtiques
Vol. 31, núm. 1, 2016. Pàg. 91–93

English summaries

Vladimir Koltchinskii, Richard Nickl, Sara van de Geer and Jon A. Wellner

The mathematical work of Evarist Giné

In this article we give an overview of Evarist Giné's contributions to the modern probability theory and mathematical statistics in an infinite-dimensional setting. The sections correspond to the areas in which he had the most relevant participation: probability in Banach spaces, empirical processes, the bootstrap, U-statistics and U-processes, and mathematical statistics. Emphasis is put on the profound impact his work has had on the present probability theory, mathematical statistics and more recently machine learning. It also contains a short biography and a list of his publications. It has been written on the occasion of his death.

Keywords: probability in Banach spaces, central limit theorem, empirical processes, bootstrap, U-statistics, density estimation.

MSC2010 Subject Classification: 60B12, 60G15, 60E15, 62F40, 62G07.

Elitza Maneva

The mathematics behind cryptocurrencies

In the context of a presentation on the basics of cryptocurrencies like Bitcoin, we introduce three topics central to modern cryptography: digital signatures, hash functions and zero-knowledge proofs. The mathematical problems that arise here can be used as examples by teachers and professors to encourage the study of modular arithmetic, probability theory, graph theory and computational complexity.

Keywords: cryptography, cryptocurrencies, RSA, elliptic curves, hash, probability, graphs, computational complexity, modular arithmetic.

MSC2010 Subject Classification: 68-02, 68Q15, 68Q17, 68Q05.

M. Rosa Massa-Esteve

New results and procedures in the mathematics of the 17th century: maxima's calculations in Pietro Mengoli (1626/1627–1686)

The publication in 1591 of *In artem analyticen isagoge* by François Viète (1540–1603) constituted an important step forward in the development of a symbolic language. As Viète's work came to prominence at the beginning of the 17th century, other authors, like Pietro Mengoli (1626/1627–1686), also began to consider the benefit of algebraic procedures for solving all kind of problems. Mengoli followed the algebraic research of Viète in order to construct geometry of species, *Geometriae Speciosae Elementa* (1659), which allowed him to use algebra in geometry in complementary ways to solve quadrature problems. Mengoli, like Viète, considered his algebra as a technique in which symbols are used to represent not just numbers but also values of any abstract magnitudes. He dealt with species, forms, triangular tables, quasi ratios and logarithmic ratios. However, the most innovative aspect of his work was his use of letters to directly study geometric figures via their algebraic expressions. In this article, I analyze the algebraic construction of these geometric figures, the use of triangular tables and the singular proof developed by Mengoli for finding the maxima of these geometric figures before the development of Newton's and Leibniz's calculus. This analysis illustrates Mengoli's mathematical ideas on the specific role of symbolic language as a means of expression and as an analytic tool.

Keywords: geometric figures, triangular tables, Pietro Mengoli, mathematics of the 17th century, maxima, logarithms, algebraic expression.

MSC2010 Subject Classification: 01A45, 3303, 2603.

Günter M. Ziegler

Cannons at Sparrows

The story told here starts with an innocuous little geometry problem, posed in a September 2006 blog entry by R. Nandakumar, an engineer from Calcutta, India: This little problem is a «sparrow», tantalizing, not as easy as one could perhaps expect, and Recreational Mathematics: of no practical use.

I will sketch, however, how this little problem connects to very serious mathematics: For the modelling of this problem we employ insights from a key area of Applied Mathematics, the Theory of Optimal Transportation. This will set up the stage for application of a major tool from Very Pure Mathematics, known as Equivariant Obstruction Theory. This is a «cannon», and we'll have some fun firing it at the sparrow.

On the way to a solution, combinatorial properties of a very classical geometric object, the permutahedron, turn out to be essential. These will, at the end of the story, lead us back to India, with some time travel that takes us one hundred years into the past: For the last step in our (partial) solution of the sparrows problem we need a simple property of the numbers in Pascal's triangle, which was first observed by Balak Ram, in Madras 1909.

But even if the existence problem is solved, the little geometry problem is not: If the solution exists, how do you find one? This problem will be left to you. Instead, I will comment on the strained relationship between cannons and sparrows, and to this avail quote a poem by Hans Magnus Enzensberger.

Keywords: partitions of a polygon, configuration spaces, obstruction theory, binomial coefficients, pure and applied mathematics.

MSC2010 Subject Classification: 00A08, 52A38, 55P91, 55R80.

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 TEX, preferentment en l'estil 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 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.

Els autors dels articles publicats al BUTLLETÍ en retenen el dret de còpia (*copyright*) i autoritzen l'IEC a difondre'ls, tant a través de la publicació impresa com mitjançant els portals digitals propis o d'altres amb què s'estableixin els convenis oportuns a aquest efecte. És responsabilitat dels autors assegurar que es disposa dels drets de reproducció dels gràfics i de les figures que hi apareguin. 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.

Comitè editorial

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: Núria Fagella i Rabionet, Josep Grané i Manlleu, Agustí Reventós i Tarrida, Carles Romero i Chesa, Oriol Serra i Albó, Esther Silberstein, Manel Udina i Abelló

DELEGAT DE L'IEC: Joan Girbau i Badó

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.

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*