n'hi ha molts menys que de noms comuns, no inclourem el nombre de lletres de la solució.

En cas de dubte podeu trobar-ne les respostes al peu de pàgina.[6]

1. Personatge bíblic que fou assassinat per un enemic de la teoria de grups.
2. Savi que hauria pogut explicar els políedres regulars en *prime-time*.
3. Matemàtica que sofria quan impartia les seves classes.
4. Matemàtic que es quedà sense sexe per la seva dèria per les equacions de tercer grau.
5. Matemàtic extremista radical pel que fa a les funcions el·líptiques.
6. Matemàtic destre en espases i en integrals de línia i de superfície.
7. Matemàtic que refilava dins el paradís dels conjunts.
8. Matemàtica amiga dels anells però intolerant amb l'etoxietà.

Xavier Gràcia
Universitat Politècnica de Catalunya

Tesis i treballs de fi de màster

Tesis

- María Pilar Silvestre Albero va llegir la seva tesi, dirigida per Joan Cerdà i Joaquim Martín, titulada *Capacitary function spaces and applications*, el dia 8 de febrer de 2012. La tesi correspon a la Facultat de Matemàtiques de la Universitat de Barcelona.

Per començar, vull enviar la meua salutació més cordial a tots els lectors i interessats pel fascinant món de les matemàtiques, així com agrair a tots els que contribueixen, encara que siga de manera molt simbòlica, a fer possible l'estudi i la recerca en aquesta disciplina. També vull agrair aquesta invitació de la SCM.

L'any 2012 vaig llegir la tesi doctoral *Capacitary function spaces and applications* gràcies al suport i guia de dues grans persones, els doctors Joan Cerdà i Joaquim Martín. Aprofito per expressar el meu agraïment a tots dos. Fer la tesi doctoral en matemàtiques sempre havia sigut una de les meues il·lusions però mai m'hagués pensat que la faria realitat a Catalunya. Déu, el meu esforç i la guia dels meus directors ho van fer possible.

El concepte de capacitat entrà a l'anàlisi clàssica amb la teoria de singularitats evitables. Un exemple clàssic de capacitat el trobem a l'electrostàtica. Siga $K \subset \mathbb{R}^3$ un conductor. Considerem una distribució de càrrega en K i deixem que es moga fins a arribar a l'equilibri. Siga μ la distribució d'equilibri. El potencial newtonià de la mesura μ pren valor constant V en K, i la capacitat de Wiener de K és

$$\begin{aligned} C(K) &= \frac{\mu(K)}{V} \\ &= \left\{ \|\nabla f\|_2^2;\ 0 \le f \le 1,\ f = 1 \text{ en } K \right\}. \end{aligned}$$

Si pensem que la frontera de K i una esfera contenint a K són les plaques del condensador, aleshores fent el radi de l'esfera tendir a infinit obtenim un condensador ideal, i la capacitat de Wiener ha de ser entesa com la capacitat d'eixe condensador ideal.

En el passat més recent les capacitats han sigut utilitzades més com una ferramenta arran del desig d'integrar respecte a una capacitat. Aquesta qüestió va ser resolta pel cèlebre Choquet, qui proposà definir la integral d'una funció respecte a una capacitat (integral de Choquet) utilitzant la forma distribucional d'una integral de Lebesgue. Així defineix per una

[6] Resposes als matemots: 4. Cardano, 1. Abel, 7. Cantor, 3. Hipàtia, 6. Stokes, 2. Plató, 8. Noether, 5. Jacobi.

capacitat C i una funció f no-negativa

$$\int_E f dC := \int_0^\infty C\{x \in E; f(x) > t\} dt.$$

El concepte principal de la tesi és el de capacitat, que està fortament relacionat amb el d'espais de funcions. En aquest treball estudiem les propietats dels espais capacitaris —espais funcionals modelats sobre espais de capacitat en comptes d'estar definits sobre espais de mesura— en relació amb propietats d'immersió de Sobolev.

Al congrés Interpolation Theory and Applications: a Conference in Honor of Michael Cwikel (Miami 2006) es proposà com a problema obert l'estudi dels espais de Lorentz associats a una capacitat. Atès que un poc abans els meus directors havien estudiat els espais de Lorentz associats a una entropia, cas particular de capacitat, es decidiren per seguir amb aquest estudi i me'l proposaren com a començament per a la tesi.

Al treball anomenem capacitat a una funció de conjunt creixent C que satisfà la propietat de Fatou, $C(A_n) \to C(A)$ si $A_n \uparrow A$, i que és quasi-subadditiva, $C(A \cup B) \leq c(C(A) + C(B))$ $(c \geq 1)$. Una propietat molt útil d'algunes capacitats és la de concavitat,

$$C(A \cup B) + C(A \cap B) \leq C(A) + C(B),$$

baix la qual tenim propietats de normabilitat.

La tesi s'estructura en tres capítols. El primer capítol conté un estudi ampli de les propietats analítiques i topològiques dels espais de funcions capacitaris. L'èmfasi està en l'estudi dels elements funcionals essencials que fan possible una teoria satisfactòria en el context dels espais quasi-Banach, en particular dels espais de Lorentz capacitaris $L^{p,q}(C)$ $(p, q > 0)$ definits per

$$\|f\|_{L^{p,q}(C)} := \begin{cases} \left(q \int_0^\infty t^{q-1} C\{|f| > t\}^{q/p} dt\right)^{1/q} < \infty, \\ \qquad\qquad q < \infty \\ \sup_{t>0} t C\{|f| > t\}^{1/p} < \infty, \\ \qquad\qquad q = \infty, \end{cases}$$

on $L^p(C) = L^{p,p}(C)$ és l'espai de Lebesgue capacitari. Els elements clau són les extensions dels resultats de Fatou, Hölder i Minkowski a capacitats. Com a aplicació veiem que els espais de Lorentz capacitaris són quasi-Banach ($\|\cdot\|_{L^{p,q}(C)}$ és una quasi-norma de Banach) i estudiem la normabilitat de $L^p(C)$, on recordem que un espai és normable si existeix una norma comparable a la seua quasi-norma. Primer provem que, si C és invariant i quasi-còncava respecte d'una mesura μ, és a dir, $C(A) = C(B)$ si $\mu(A) = \mu(B)$ i existeix $\gamma \geq 1$ tal que si $\mu(A) \leq \mu(B)$, aleshores

(a) $C(A) \leq \gamma\, C(B)$, i

(b) $\frac{C(B)}{\mu(B)} \leq \gamma \frac{C(A)}{\mu(A)}$,

tenim que

$$\widetilde{C}(A) := \sup\Big\{ \sum_{i=1}^n \lambda_i C(A_i);\ n \in \mathbb{N}, \\ \sum_{i=1}^n \lambda_i = 1,\ \lambda_i \geq 0,\ \sum_{i=1}^n \lambda_i \mu(A_i) \leq \mu(A) \Big\}$$

defineix una capacitat còncava equivalent a C. Amb això, veiem que si C és una capacitat quasi-còncava respecte de μ, $L^p(C)$ és normable per $1 \leq p \leq \infty$.

Com és ben sabut, la interpolació d'operadors té moltes aplicacions en diferents àrees de les matemàtiques. Per això, estudiem les propietats d'interpolació dels espais de Lorentz capacitaris. J. L. Lions i J. Peetre van construir l'anomenat mètode real d'interpolació amb la inspiració de la prova del teorema clàssic de Marcinkiewicz. Si $\bar{A} = (A_0, A_1)$ és un parell d'espais quasi-Banach, $0 < \theta < 1$ i $0 < q \leq \infty$, l'espai d'interpolació $\bar{A}_{\theta,q}$ és l'espai de quasi-Banach de totes les funcions f que satisfan

$$\|f\|_{\theta,q} := \Big(\int_0^\infty (t^{-\theta} K(t, f; \bar{A}))^q \frac{dt}{t} \Big)^{1/q} < \infty,$$

on $K(t, f; \bar{A})$ és el K-funcional definit per

$$K(t, f; \bar{A}) := \inf\Big\{ \|f_0\|_{A_0} + t\|f_1\|_{A_1};\ f = f_0 + f_1 \Big\}.$$

Al segon capítol estudiem propietats d'interpolació dels espais de Lorentz capacitaris. L'objectiu final és interpolar espais de Lorentz associats a diferents capacitats. Primerament obtenim una expressió integral de $K(t, f; L^p(C),\ L^\infty(C))$ si $0 < p < \infty$ i $t > 0$. Amb aquesta fórmula obtenim els resultats d'interpolació real de la manera clàssica. Seguidament, una extensió del mètode de Sparr

per triples d'espais de Banach a espais quasi-Banach ens permet obtenir una expressió del tipus

$$\Big(\big(L^{p_0,q_0}(C_0), L^{p_2,q_2}(C_2)\big)_{\alpha_0,\bar{q}_0}, \big(L^{p_1,q_1}(C_1), L^{p_2,q_2}(C_2)\big)_{\alpha_1,\bar{q}_1}\Big)_{\mu,q} = \big(L^{p_0,q_0}(C_0), L^{p_1,q_1}(C_1), L^{p_2,q_2}(C_2)\big)_{(\theta_1,\theta_2),q},$$

baix certes condicions. Com a aplicació obtenim el resultat principal, siguin C_0, C_1 un parell de capacitats, $0 < \eta < 1$, $\frac{1}{p} := \frac{1-\eta}{p_0} + \frac{\eta}{p_1}$ i $\frac{1}{q} := \frac{1-\eta}{q_0} + \frac{\eta}{q_1}$, aleshores per $C_{\theta,q}(A) := \|\chi_A\|_{(L(C_0),L(C_1))_{\theta,q}}$ $(0 < \theta < 1)$,

$$\big(L^{p_0,q_0}(C_0), L^{p_1,q_1}(C_1)\big)_{\eta,q} = L^{p,q}\Big(C_{\frac{\eta p}{p_1},q/p}\Big).$$

V. Maz'ya, de molt jove, descobrí que les desigualtats isoperimètriques i isocapacitàries són equivalents a certes desigualtats de Sobolev. D'ací ha resultat que les classes de dominis i mesures que apareixen a certs teoremes d'immersió i compacitat poden ser descrits completament en termes de longitud i àrea. V. Maz'ya considerà la capacitat de Wiener per a un compacte K d'un domini $\Omega \subset \mathbb{R}^n$,

$$\mathrm{cap}_p(K,\Omega) := \inf_{0\le f\le 1,\, f=1 \text{ on } K} \|\nabla f\|_p^p \qquad (f \in \mathrm{Lip}_0(\Omega))$$

on $\mathrm{Lip}_0(\Omega)$ és la classe de totes les funcions Lipschitz amb suport compacte a Ω i ∇f és el seu gradient, i demostrà la desigualtat de Sobolev

$$\int_0^\infty \mathrm{cap}_p(\overline{M}_{at}, M_t)d(t^p) \le c(a,p)\|\nabla f\|_p^p,$$

on $M_t := \{x \in \Omega; |f(x)| > t\}$ per $t > 0$. En el passat recent S. Costea i V. Maz'ya estenen aquesta desigualtat als espais de Lorentz clàssics, espais de Lorentz associats a una mesura, gràcies a certes propietats de convexitat dels espais de Lorentz. La seua tècnica s'aplica a un conjunt reduït d'espais.

A la tesi veiem que una extensió és possible per tot espai quasi-Banach X que satistà una *lower p-estimate*, que és una condició de convexitat. Donat (K,G) un conductor, on K és un compacte i G és un obert a $\Omega \subset \mathbb{R}^n$ contenint a K, es defineix la seua capacitat per

$$\mathrm{Cap}_X(K,G) := \inf\{\|\nabla u\|_X;\, u \in W(K,G)\},$$

on $W(K,G) := \{u \in \mathrm{Lip}_0(G); u = 1$ a un entorn de $K, 0 \le u \le 1\}$. Amb un argument nou, utilitzant propietats fines de la teoria de submesures, demostrem el resultat principal d'aquest capítol: si X és un espai de funcions quasi-Banach que satisfà una *lower $p-$estimate* $(0 < p < \infty)$, tenim per $a > 1$ que

$$\int_0^\infty t^p \mathrm{Cap}_X(\overline{\{|f|>at\}}, \{f>t\})^p \frac{dt}{t} \le c_1 \|\nabla f\|_X^p,$$

per tota funció Lipschitz amb suport compacte en Ω, on c_1 depèn de a, p, de les constants de convexitat i quasi-subadditivitat de X. Tenim així, baix certes condicions, una desigualtat integral que connecta la norma del gradient d'una funció en un espai de funcions amb la integral de la corresponent capacitat del conductor entre dues superfícies de nivell de la funció. La desigualtat permet una caracterització de les desigualtats de tipus Sobolev per dues mesures, condicions necessàries i suficients per desigualtats isocapacitàries de tipus Sobolev, i la millora de l'autointegrabilitat de les funcions de Lipschitz. Veiem així que per a millores de la integrabilitat de funcions Lipschitz són necessaris no només mètodes de truncació sinó que també calen condicions de convexitat de l'espai.

Els resultats de la tesi han estat publicats als següents articles:

Referències

[1] J. Cerdà, J. Martín, and P. Silvestre, «Capacitary function spaces», *Collectanea Math.* 62 (2011), no.1, 95-118.

[2] J. Cerdà, J. Martín, and P. Silvestre, «Interpolation of quasicontinuous functions», *Józef Marcinkiewicz Centenary Volume*, Banach Center Publ. 95 (2011), 281-286.

[3] J. Cerdà, J. Martín, and P. Silvestre, «Conductor Sobolev type and isocapacitary inequalities», *Indiana Univ. Math. J.* 61 (2012), no.5, 1925-1947.

[4] P. Silvestre, «Capacitary Orlicz spaces, Calderón couples and interpolation», to appear in *Proceedings of the conference Function Spaces X. Banach Center of Publications.*

- Víctor Ortiz va llegir la seva tesi, dirigida per Marta Sanz, titulada *Principi de grans desviacions per a l'equació en derivades parcials estocàstica d'ones en dimensió espacial 3*, el dia 13 de març de 2012. La tesi correspon al Departament de Probabilitat, Lògica i Estadística de la Universitat de Barcelona.

Sigui E un espai polonès (això és, un espai mètric separable complet) i $\mathcal{E}$ la σ-àlgebra de conjunts d'E generada per les funcions contínues definides en E. Siguin $\{\mu_\varepsilon\}_\varepsilon$ una família de mesures de probabilitat sobre $\mathcal{E}$ tals que $\mu_\varepsilon \overset{\varepsilon\to 0}{\longrightarrow} \delta_p$ feblement, on $p \in E$ i δ_p és una delta de Dirac centrada en p. Aleshores, a causa del teorema de Portmanteau, es té que, per cada $U \in \mathcal{E}$ tal que $p \in U$, $\mu_\varepsilon(U^c) \to 0$ quan $\varepsilon \to 0$.

Situats en aquest context, és natural preguntar-se, donat $V \in \mathcal{E}$ tal que $p \notin \overline{V}$, per la velocitat amb què $\mu_\varepsilon(V)$ tendirà a 0. Dit d'una altra manera, podem preguntar-nos amb quina velocitat V es desvia dels esdeveniments que $\lim_{\varepsilon\to 0} \mu_\varepsilon$ considera normals (això és, aquells $U \in \mathcal{E}$ tals que $p \in U$). Intuïtivament, i de manera no rigorosa, direm que la família $\{\mu_\varepsilon\}_{\varepsilon>0}$ satisfà un principi de grans desviacions (en endavant, PGD) sobre $\mathcal{E}$ si aquesta velocitat és exponencial.

L'objectiu d'aquesta tesi és establir un PGD per a la família d'equacions d'ones estocàstiques $\{u^\varepsilon,\ \varepsilon \in (0,1]\}$, amb

$$\begin{cases} \left(\frac{\partial^2}{\partial t^2} - \Delta\right) u^\varepsilon(t,x) = \sqrt{\varepsilon}\sigma(u^\varepsilon(t,x))\dot{F}(t,x) \\ \qquad\qquad\qquad\qquad + b(u^\varepsilon(t,x)),\ t \in [0,T], \\ u(0,x) = v_0(x), \\ \frac{\partial}{\partial t} u(0,x) = \tilde{v}_0(x),\ x \in \mathbb{R}^3, \end{cases} \tag{1}$$

on Δ denota el laplacià en $\mathbb{R}^3$, b i σ són funcions contínues Lipschitz i el proces $\dot{F}$ és la derivada formal d'un camp aleatori gaussià, blanc en temps i correlacionat en espai. L'objecte que prendrem com a solució de (1) serà un camp aleatori, $\{u^\varepsilon(t,x), t \in [0,T], x \in \mathbb{R}^3\}$, i el PGD enunciat es satisfarà en un espai de funcions Hölder contínues.

F. Chenal i A. Millet ja demostraren un PGD per a les lleis de l'equació d'ones en dimensió espacial $d \in \{1,2\}$. Aquest resultat s'obtingué emprant el que anomenem *mètode d'afitació d'Azencott*.

En precisar càlculs sobre el nucli de Green de l'equació en derivades parcials estocàstica considerada, i en ésser aquest una distribució en el cas de l'equació d'ones en dimensió $d = 3$, aplicar el mètode d'afitació d'Azencott en el cas que ens ocupa resulta complicat: hauria de fer-se a partir d'aproximacions exponencials de les lleis originals de la família d'equacions, construïdes a partir de regularitzar el nucli de Green amb funcions test. No és gens clar, a més, que aquesta estratègia donés fruits.

El mètode que emprem per tal d'obtenir el PGD cercat és el que anomenem tècnica de Budhiraja-Dupuis. Més recent que l'afitació d'Azencott, aquest mètode permet tractar el cas estudiat de manera més simplificada. A més, els arguments realitzats per provar els resultats de convergència necessaris per poder establir el PGD cercat són, en general, també aplicables als casos $d \in \{1,2\}$. Així doncs, seguint els passos detallats en aquesta tesi, seria possible presentar de manera unificada un PGD per a les famílies de l'equació estocàstica d'ones en dimensions espacials 1, 2, i 3, emprant aquesta tècnica.

- Eulàlia Tramuns Figueres va llegir la seva tesi, dirigida per Jordi Guàrdia, titulada *Una formalització de les construccions geomètriques*, el dia 18 de juliol de 2012. La tesi correspon al Departament de Matemàtica Aplicada IV de la Universitat Politècnica de Catalunya.

Aquesta tesi s'emmarca dins el context de les construccions geomètriques i la teoria de nombres.

A partir d'una anàlisi global d'instruments geomètrics i dels resultats principals que es coneixen sobre ells, hem introduït un llenguatge formal que ens permet un tractament unificat dels instruments, les seves construccions i els teoremes relacionats. Dins d'aquest llenguatge definim tres conceptes principals, que són els d'axioma, eina i mapa.

D'una banda, definim les eines com a formalització dels instruments geomètrics. Cada eina té associats uns axiomes, que són els processos bàsics que permet fer l'instrument. De l'altra, definim formalment les construccions com a successions d'axiomes, que inclouen tota la informació necessària per descriure el procés que es du a terme.

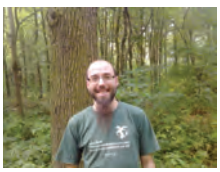
Una vegada definits els conceptes d'eina i de construcció, proposem una classificació de les eines segons dues relacions d'equivalència: l'equivalència geomètrica i l'equivalència virtual. Aquestes classificacions permeten reformular resultats coneguts, com ara el teorema de Mohr-Mascheroni, i provar noves relacions entre eines.

Finalment, definim un mapa com un objecte geomètric i aritmètic que està format per una eina i un conjunt inicial de punts i de corbes. Els mapes tenen associades capes, compostes i generades iterativament per punts i corbes. A causa de la complexitat dels mapes i de les seves capes la informació que se'n pot donar és sovint escassa. Atès que el seu estudi té una relació estreta amb certs problemes de geometria computacional, es poden deduir, però, fites del nombre d'objectes generats per certs axiomes. Per a alguns mapes determinats donem el creixement asimptòtic del cardinal del nombre de punts i de corbes de cada capa. En el cas del mapa del compàs fix caracteritzem exactament els conjunts de punts i de corbes de cada capa del mapa. Introduïm també una classificació dels mapes, que agrupa aquells que tenen el mateix conjunt de punts construïbles i reformulem el teorema de Poncelet-Steiner en el llenguatge dels mapes. A partir de la classificació dels mapes, introduïm una tercera classificació de les eines, aquesta vegada aritmètica, i donem nous resultats d'equivalència aritmètica, utilitzant els conceptes algebraics de grau d'un axioma i signatura d'una eina.

En una altra direcció, estudiem l'estructura de les construccions, a les quals associem dos tipus de mesures, que permeten donar criteris de minimalitat i optimalitat d'una construcció. El primer tipus de mesures, extrínseques a la construcció, són el nivell i el nivell virtual, que fan ús de les capes de mapes associats a la construcció. El segon tipus de mesures, intrínseques a la construcció, són la llargada, l'amplada, l'ordre i el rang. Calculem aquestes mesures per a les construccions aritmètiques i algebraiques bàsiques i deduïm relacions entre diferents capes dels mapes del regle i el compàs, l'*origami* i les còniques.

Al llarg del treball, il·lustrem la nostra formalització amb diversos catàlegs: un catàleg d'axiomes, un catàleg d'eines, i un catàleg de mapes. Finalment, presentem un catàleg de construccions, que consta d'una setantena de construccions, descrites amb el nou llenguatge que hem introduït, les seves mesures i la demostració de la seva validesa. La versió digital de la tesi incorpora enllaços a animacions interactives on es poden reproduir els passos de les construccions.

- Victor Gonzàlez va llegir la seva tesi, dirigida per Miguel Ángel Barja Yáñez i Juan Carlos Naranjo del Val, titulada *Hode numbers of irregular varieties and fibrations*, el dia 8 de juliol de 2013. La tesi correspon al Departament de Matemàtica Aplicada I de la Universitat Politècnica de Catalunya.



El tema central d'aquesta tesi és la geografia de varietats projectives complexes irregulars, parant especial atenció a les de fibracions. La tesi està dividida en dues parts, diferenciades tant pel tipus de resultats obtinguts com per les tècniques utilitzades.

A la primera part s'ha relacionat l'existència d'un tipus particular de fibracions en una varietat irregular (els anomenats *higher irrational pencils*) amb desigualtats satisfetes pels nombres de Hodge de la varietat. L'exemple paradigmàtic és la desigualtat de Castelnuovo-

di Franchis, provada fa més de cent anys per superfícies. Aquesta desigualtat admet diverses generalitzacions a dimensió superior, com les que es dedueixen de treballs de Ran i Catanese per una banda, o les demostrades més recentment per Pareschi-Popa i Lazarsfeld-Popa. El principi general d'aquests resultats és que si la varietat té «poques» formes diferencials holomorfes d'un cert rang, aleshores l'àlgebra de formes diferencials té alguna propietat especial que permet construir una fibració.

En aquest context, la tesi conté diversos resultats nous. D'una banda, truncant el complex BGG de la varietat (l'eina utilitzada per Lazarsfeld-Popa en el seu treball, desenvolupada a partir del complex derivat de Green-Lazarsfeld) s'obtenen fites inferiors per les característiques d'Euler parcials. Per tal de millorar aquests primers resultats, s'han introduït els complexos derivats de rang superior, estudiant-ne l'exactitud mitjançant complexos d'Eagon-Northcott, i obtenint noves desigualtats entre els nombres de Hodge de varietats que admeten certs subespais de 1-formes diferencials (anomenats *no degenerats*). En el cas de subvarietats de varietats abelianes, l'existència de subespais no degenerats de qualsevol dimensió permet millorar les desigualtats obtingudes en el cas general.

En el cas concret del nombre de Hodge $h^(2,0)$, un mètode diferent proporciona un resultat molt millor, tant perquè la fita és més acurada, com perquè només cal que la varietat no tingui *higher irrational pencils*, que és una hipòtesi més relaxada que l'existència de subespais no degenerats.

A la segona part s'ha considerat un cas complementari a l'anterior: es parteix d'una superfície fibrada sobre una corba, intentant obtenir fites superiors per la irregularitat de la superfície en termes del gènere de la corba base i propietats de la fibra genèrica. El prototipus de resultat és una desigualtat obtinguda per Xiao en el cas que la base és una corba racional. En aquest cas, la irregularitat de la superfície és com a molt el gènere de les fibres genèriques, i Xiao va demostrar que si aquestes no són totes isomorfes, aleshores la fita superior es pot rebaixar a l'ordre de la meitat del gènere.

Quan la base no és una corba racional, Xiao va conjecturar que s'hauria de complir la mateixa desigualtat, però poc temps després Pirola va trobar un contraexemple, proposant una correcció a la conjectura. El resultat obtingut en aquesta tesi és una fita dependent del gènere i l'índex de Clifford de la fibra genèrica. A més, en el cas que l'índex de Clifford és el màxim possible, la fita coincideix amb la correcció proposada per Pirola.

Les tècniques utilitzades per obtenir aquesta fita són bastant variades. D'una banda, s'utilitzen de forma crucial les «imatges adjuntes» subespais de formes diferencials, introduïdes per Collino i Pirola per estudiar deformacions infinitesimals de corbes, i generalitzades posteriorment per Pirola i Zucconi per a varietats de dimensió arbitrària. L'aportació d'aquesta tesi és la construcció de l'«aplicació adjunta global», que permet trobar subespais amb imatge adjunta zero assumint que almenys la meitat de les formes diferencials de la corba es poden estendre a la deformació. D'altra banda, s'han estès a famílies arbitràries (unidimensionals) de corbes alguns conceptes ben establerts per a deformacions infinitesimals, relacionants amb la immersió bicanònica de la corba. Totes aquestes construccions admeten generalitzacions a famílies de varietats irregulars de dimensió qualsevol.

Tots aquests resultats previs permeten trobar un resultat sobre l'estructura de fibracions suportades a un divisor relativament rígid, que és un dels dos casos que apareixen a la prova de la conjectura de Xiao. Per a l'altre cas s'utilitza una fita inferior del rang d'una deformació infinitesimal en termes d'un divisor que la suporti (el seu grau i la dimensió de la sèrie lineal associada).

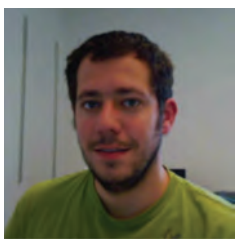
- Alexandre Ruiz Rodríguez va llegir la seva tesi, dirigida per Javier Herranz Sotoca i Germán Sáez i Moreno, titulada *Contributions to secret sharing and other distributed cryptosystems*, el dia 22 de juliol de 2013. La tesi correspon al Departament de Matemàtica Aplicada IV de la Universitat Politècnica de Catalunya.

Avui dia les persones estan implicades cada cop més en diferents activitats digitals tant en la vida professional com en el temps privat. Molts articles de paper, com diners i tiquets, s'estan reemplaçant més i més per objectes digitals. La criptografia té un paper crucial en aquesta transformació, perquè proporciona seguretat en la comunicació entre diferents participants que utilitzen un canal digital. Depenent de la situació específica, alguns requisits de seguretat en la comunicació poden incloure privacitat (o confidencialitat), autenticitat, integritat o no-repudi. La criptografia distribuïda juga una funció important dins de la criptografia. Quan l'operació secreta s'estén entre un grup de participants això fa el procés més segur i fiable que quan la informació secreta és centralitzada en un únic participant.

La tesi aquí presentada tracta de primitives criptogràfiques relacionades amb aquest camp. Primer, estudiem des d'un punt de vista teòric esquemes *signcryption*, en què l'operació distribuïda recau en el protocol *unsigncryption*, i també posem un marc de seguretat per a ells. Llavors, es presenten dos esquemes *signcryption* amb una estructura llindar en l'operació d'*unsigncryption* per diferents models de seguretat. A més, utilitzem la seva propietat d'autenticitat per construir signatures digitals amb verificació distribuïda. La nostra recerca ens dirigeix també a esquemes de compartició de secrets. Després d'estudiar algunes limitacions en els esquemes de compartició *multisecret* en un escenari incondicional, presentem diversos esquemes de compartició *multisecret* computacionalment segurs. Finalment, treballem en altres sistemes distribuïts, on utilitzem la recerca feta en els esquemes de compartició multisecret per generalitzar-ho a un marc *multiusuari*, i presentar un esquema *multi-policy* de dexifrat distribuït i un esquema *multi-policy* de signatura distribuïda. A més, donem indicacions de com es poden aplicar els esquemes de compartició multisecret als esquemes *signcryption* proposats al llarg d'aquesta tesi.

Tots els esquemes que s'han proposat al llarg d'aquesta tesi, segueixen la mateixa estructura. Després de definir els protocols primitius i el seu model de seguretat, proposem l'esquema nou i provem formalment la seva seguretat computacional.

- Guillem Perarnau Llobet va llegir la seva tesi, dirigida per Oriol Serra, titulada *Random combinatorial structures with low dependencies: existence and enumeration (Estructures combinatòries aleatòries amb dependències febles: existència i enumeració)*, el dia 1 d'octubre de 2013. La tesi correspon al Departament de Matemàtica Aplicada IV de la Universitat Politècnica de Catalunya.



En aquesta tesi s'han estudiat diferents problemes en el camp de la combinatòria i la teoria de grafs, utilitzant el mètode probabilístic. Aquesta tècnica, introduïda per Erdös als anys cinquanta, ha esdevingut una eina molt útil per donar proves existencials a certs problemes en diferents camps de les matemàtiques en què altres mètodes no ho han aconseguit. Un dels seus principals objectius és l'estudi del comportament de les variables aleatòries. En l'estudi de problemes combinatoris, el cas en què aquestes variables compten el nombre d'esdeveniments dolents que tenen lloc en una estructura combinatòria és de particular interès. El paradigma de Poisson diu que quan les dependències entre aquests esdeveniments són febles o poc nombroses, la probabilitat que tots aquests esdeveniments dolents no succeeixin és

similar a la probabilitat que un obté quan els esdeveniments són mutualment independents. El lema local de Lovász o la desigualtat de Suen són exemples concrets d'aquest paradigma. L'objectiu de la tesi ha estat estudiar aquestes tècniques i donar-ne noves aplicacions en diferents àmbits de la combinatòria.

La primera part d'aquesta tesi estudia una conjectura de Ryser [1] sobre l'existència de transversals llatins en quadrats llatins. Això equival a estudiar l'existència d'aparellaments multicolor en aresta-coloracions de grafs complets bipartits. Erdös i Spencer [2] van provar que qualsevol aresta-coloració en què cap color apareix massa vegades admet un aparallement en què tots els colors són diferents. Sota les mateixes hipòtesis, en aquesta tesi es donen resultats sobre el nombre d'aquests aparellaments.

En la segona part d'aquesta tesi s'estudien els codis identificadors. Donat un graf, un codi identificador d'aquest és un conjunt de vèrtexs tal que per qualsevol vèrtex del graf, la intersecció del seu veïnatge amb el codi es única. En aquesta tesi s'estableixen fites en la mida d'un codi identificador mínim en funció dels graus del graf i es resol parcialment una conjectura de Foucaud *et al.* [3]. També es mostra que qualsevol graf suficientment dens conté un gran subgraf que admet un codi identificador òptim.

Les tècniques abans esmentades no tan sols permeten donar resultats existencials sinó també resultats enumeratius. L'estudi de patrons en permutacions n'és un bon exemple. A la tercera part de la tesi es desenvolupa una nova tècnica per tal d'estimar el nombre de permutacions d'una certa llargada que eviten còpies consecutives d'un patró donat. Una de les conseqüències és la prova de la conjectura CMP enunciada per Elizalde i Noy [4], així com nous resultats en el comportament de la majoria dels patrons.

En l'última part de la tesi s'estudia la conjectura del corredor solitari, enunciada independentment per Wills [5] i Cusick [6], i que té múltiples aplicacions en diferents camps de les matemàtiques com ara en aproximació diofàntica o en acoloriment circular de grafs. Aquesta coneguda conjectura diu que per qualsevol conjunt de corredors que corren al llarg d'un cercle unitari, hi ha un moment en què tots els corredors estan suficientment lluny de l'origen. En aquesta tesi s'ha millorat un resultat de Chen [7] ampliant la distància de tots els corredors a l'origen. També s'ha estès el teorema del corredor invisible de Czerwinski i Grytczuk [8].

Referències

[1] H. J. Ryser, «Neuere probleme der kombinatorik», *Vorträgeüber Kombinatorik*, Oberwolfach (1967).

[2] P. Erdös i J. H. Spencer, Lopsided Lovász local lemma and Latin transversals», *Discrete Appl. Math.* 30 (1991), no. 2-3, 151-154.

[3] F. Foucaud, R. Klasing, A. Kosowski, and A. Raspaud, «On the size of identifying codes in triangle-free graphs», *Discrete Appl. Math.* 160 (2012), no. 10-11, 1532-1546.

[4] S. Elizalde i M. Noy, «Consecutive patterns in permutations», *Adv. in Appl. Math.* 30 (2003), 110-125.

[5] J. M. Wills, «Zwei Sätze über inhomogene diophantische Approximation von Irrationalzahlen» , *Monatsh. Math.* 71 (1967), 263-269.

[6] T. W. Cusick, «View-obstruction problems II», *Proc. Amer. Math. Soc.* 84 (1982), no. 1, 25-28.

[7] Y. G. Chen, «View-obstruction problems in n-dimensional Euclidean space and a generalization of them», *Acta Math. Sinica* 37 (1994), no. 4, 551-562.

[8] S. Czerwnnd i J. Grytczuk, «Invisible runners in finite fields», *Inform. Process. Lett.* 108 (2008), no. 2, 64-67.

- Daniel Ramos Guallar va llegir la seva tesi, dirigida per Joan Porti Piqué, titulada *Ricci flow on cone surfaces and a three-dimensional expanding soliton*, el dia 28 de gener de 2014. La tesi correspon al Departament de Matemàtiques de la Universitat Autònoma de Barcelona.

Aquesta tesi estudia l'evolució mitjançant el flux de Ricci de superfícies amb singularitats de tipus cònic; i també l'estructura de famílies de solitons del flux de Ricci en dimensió 2 i 3.

El flux de Ricci és una equació d'evolució per a varietats Riemannianes, introduïda per R. Hamilton el 1982. És des dels avenços assolits per G. Perelman amb aquesta tècnica el 2002 que el flux de Ricci s'ha establert com una disciplina pròpia, aixecant un gran interès per la comunitat.

Un dels usos del flux de Ricci aplicat a superfícies llises és la reconstrucció del resultat clàssic d'uniformització de superfícies (tota superfície llisa tancada admet una mètrica de curvatura constant, del mateix signe que la seva característica d'Euler). Això ja va ser provat amb el flux per Hamilton, Chow, Chen, Lu i Tian, demostrant que una mètrica arbitrària convergeix sota el flux de Ricci, llevat de rescalaments, a una mètrica de curvatura constant. Els avenços de Perelman, d'altra banda, s'enfoquen a estudiar varietats de dimensió 3 però també s'apliquen a superfícies. Un resultat preliminar de la tesi és una revisió de les tècniques de Hamilton i Perelman combinades per a donar una demostració diferent del teorema d'uniformització de superfícies.

A continuació, plantegem el problema de l'evolució del flux en superfícies no llises, amb singularitats de tipus cònic. El punt de vista combinat de Hamilton amb Perelman ens permet generalitzar l'evolució del flux de Ricci a aquest cas no llis i demostrar la seva convergència. En el cas llis, Hamilton demostra que algunes mètriques convergeixen als anomenats solitons del flux de Ricci, és a dir, solucions especials a l'equació d'evolució del flux que només evolucionen per difeomorfismes i homotècies. En el cas llis i compacte, però, aquests solitons tenen sempre curvatura constant. Hamilton descobrí alguns exemples de solitons no llisos que existeixen en *orbifolds*.

El primer resultat principal de la nostra tesi és una enumeració exhaustiva de tots els solitons llisos i cònics en superfícies. Aquí trobem els exemples de Hamilton més altres exemples en el cas no compacte. Això ens requereix tècniques de sistemes dinàmics i retrats de fase, juntament amb les propietats geomètriques de les mètriques de solitó.

El segon resultat principal és una uniformització de les superfícies còniques mitjançant el flux de Ricci. Aquest resultat, que utilitza la classificació anterior dels solitons, estén la teoria de Hamilton al cas singular i prova que el flux convergeix, llevat rescalaments, a una superfície de curvatura constant o bé a una mètrica de solitó. Aquest resultat requereix adaptar els resultats de no-colapse de Perelman i també la teoria de convergència de successions de varietats en el cas de superfícies còniques.

A continuació ens detenim i ens plantegem la definició que hem fet servir del flux de Ricci en superfícies còniques. Des del punt de vista d'EDP, un punt cònic és la vora (puntual) del domini de definició de les funcions, i les condicions de frontera podrien variar. Des del punt de vista de la geometria, l'estructura d'espai mètric prop del punt cònic podria no mantenir-se. El resultat d'uniformització que hem obtingut assumeix un flux que preserva l'estructura cònica dels punts singulars, però això podria no ser així. El tercer resultat principal de la tesi és precisament la construcció d'un flux de Ricci que elimina les singularitats còniques, de manera que l'estructura cònica canvia abruptament. Això exposa clarament la no-unicitat de solucions al flux.

Finalment, el quart i últim resultat principal és la construcció d'un nou solitó gradient expansiu en dimensió 3. Aquí fixem una topologia específica (concretament el producte cartesià d'un tor amb una recta) i assumim una cota inferior de la curvatura. Amb tècniques de retrats de fase similars a les utilitzades per als solitons de dimensió 2, donem una construcció explícita d'aquest nou solitó amb una mètrica de *warped product*. Demostrem també que és l'únic solitó amb la seva topologia i la seva cota inferior de la curvatura, i que és un cas crític entre tots els solitons expansius en dimensió

3 amb curvatura acotada inferiorment. Aquest exemple és una mostra dels fenòmens que poden sorgir en el flux de Ricci en varietats obertes en dimensió 3, un problema que va més enllà dels resultats de Perelman i que encara no ha estat completament resolt.

- Alberto Gavira Romero va llegir la seva tesi, dirigida per Natàlia Castellana Vila, titulada *Aproximacions cel·lulars d'espais de llaços infinits i d'espais*, el dia 10 de febrer de 2014. La tesi correspon al Departament de Matemàtiques de la Universitat Autònoma de Barcelona

Un argument clàssic en topologia algebraica és l'estudi de propietats topològiques mitjançant functors $F\colon \mathbf{hoTop}_* \to \mathbf{C}$, on $\mathbf{hoTop}_*$ és la categoria homotòpica d'espais topològics puntejats i $\mathbf{C}$ és una categoria d'objectes algebraics (categoria de grups, grups abelians, anells, etc.). Com exemple tenim els grups d'homotopia. E. Dror-Farjoun introdueix en 1995 per a un espai topològic puntejat A, la noció d'A-homotopia, on A i les seves suspensions juguen el mateix paper que les esferes en homotopia clàssica. Es defineixen els grups d'A-homotopia d'un espai puntejat X com les classes d'homotopia d'aplicacions definides des de les suspensions d'A a X. A més a més, existeix una construcció anàloga a l'aproximació cel·lular: l'aproximació A-cel·lular, és a dir, un espai A-cel·lular $CW_A(X)$ (i.e., un espai construït mitjançant colímits homotòpics puntejats d'A de manera iterada) junt amb una aplicació natural $CW_A(X) \to X$ que indueix una equivalència entre els espais d'aplicacions puntejades $\mathrm{map}_*(A, CW_A(X))$ i $\mathrm{map}_*(A, X)$, i aleshores un isomorfisme en grups d'A-homotopia.

Sigui p un nombre primer. En aquest treball estudiem l'A-cel·lularització, on A és un espai classificador del tipus $B\mathbb{Z}/p^m$, $B\mathbb{Z}/p^\infty$ o un producte d'aquests, de dues famílies d'espais: els espais $\Sigma B\mathbb{Z}/p$-acíclics llevat p-completació i els espais classificadors de grups p-locals compactes.

Primer demostrem que la $B\mathbb{Z}/p^m$-cel·lularització d'un espai $\Sigma B\mathbb{Z}/p$-acíclic llevat p-completació 1-connex X és equivalent a la fibra homotòpica de la racionalització $\psi Xp \to (\psi Xp)_{\mathbb{Q}}$. Com exemples estan els espais de llaços infinits i les torres de Postnikov 1-connexos amb segon grup d'homotopia de torsió. Aquest resultat ens permet calcular la $B\mathbb{Z}/p$-cel·lularització dels espais BO, BU, BSp i dels seus recobridors connexos, completant això l'estudi de la $K(\mathbb{Z}/p, n)$-cel·lularització d'aquests espais que van realitzar N. Castellana, J. A. Crespo i J. Scherer pel cas $n > 1$.

En el segon cas, donat un grup p-local compacte $(S, \Phi, \mathcal{L})$, per l'estudi de la cel·lularització de $\psi|\mathcal{L}|p$ estenem la definició del nucli d'una aplicació $f\colon \psi|\mathcal{L}|p \to \psi Yp$, donada pel cas de grup de Lie compacte pel D. Notbohm, com el subgrup de S format pels elements x tals que en restringir f a $B\langle x\rangle$ és homotòpicament trivial. Demostrem que, sota certes hipòtesis sobre $\psi|\mathcal{L}|p$, si el nucli de certa aplicació determinant en el càlcul de la cel·lularització és tot el p-grup S, llavors l'A-cel·lularització de $\psi|\mathcal{L}|p$ és equivalent a la fibra homotòpica de la racionalització $\psi|\mathcal{L}|p \to (\psi|\mathcal{L}|p)_{\mathbb{Q}}$. En el cas finit som més precisos, demostrant que $\psi|\mathcal{L}|p$ és $B\mathbb{Z}/p^m$-cel·lular si i només si aquest nucli és el mínim subgrup de S fortament tancat que conté tota la p-torsió per $i \leq m$ (aquest resultat generalitza resultats previs sobre cel·lularització d'espais classificadors de grups finits realitzats per R. J. Flores, F. Foote i J. Scherer). En el cas d'un grup de Lie compacte simple 1-connex G provem, gràcies a l'estudi dels subgrups fortament tancats realitzat pel D. Notbohm, que en gairebé tot els casos, si $p \mid |G|$ i $m > 0$, $CW_{B\mathbb{Z}/p^m}(\psi BGp)$ és equivalent a la fibra homotòpica de la racionalització $\psi BGp \to (\psi BGp)_{\mathbb{Q}}$.