Llibre blanc de la recerca matemàtica a Catalunya

DOI 10.2436/15.2000.07.7

Josep Fàbrega Canudas

Volem presentar en aquest article una visió general de la recerca que es fa a Catalunya en la disciplina coneguda per matemàtica discreta. La relació de temes que podem incloure en aquesta branca de les matemàtiques no està del tot ben precisada i sovint són temes a cavall de diverses matèries de la pròpia matemàtica —com l'àlgebra, la geometria, la teoria de nombres o la teoria de la probabilitat— i d'altres matèries més pròpies de la informàtica teòrica i, fins i tot, de les telecomunicacions. En tot cas, la feina que recollim aquí fa referència als grups de recerca de les universitats catalanes que treballen en combinatòria, teoria de grafs, geometria computacional, criptologia, teoria de codis, algorísmia i teoria de la complexitat. Pel que fa a la distribució per universitats, el gruix més important d'investigadors en l'àrea es concentra a la Universitat Politècnica de Catalunya (UPC), però també trobem grups potents i molt actius a les universitats Autònoma de Barcelona (UAB), Rovira i Virgili (URV), de Lleida (UdL), i també investigadors de la Universitat Pompeu Fabra (UPF). Cal tenir present que les relacions entre els científics de l'àrea són estretes i sovint grups que tenen el centre de gravetat en una determinada universitat compten, entre els seus membres, amb investigadors d'altres universitats.

Abans de començar aquest repàs, l'autor vol agrair als diferents grups de recerca l'ajuda rebuda a l'hora de preparar aquest treball, però tingui en compte el lector que la visió que es presenta està segurament esbiaixada pels coneixements i els interessos de qui escriu. Explicarem en primer lloc la recerca vinculada a la teoria de grafs, a la combinatòria i, en general, a l'estudi d'estructures discretes; després repassarem la feina feta en l'àmbit de la criptologia i la teoria de codis, i finalment, en l'àmbit de l'algorísmia i la complexitat.

La recerca en teoria de grafs i en combinatòria

Una de les àrees més actives desenvolupades a la UPC fa referència a l'estudi de problemes extremals i d'optimització de la teoria de grafs i de la combinatòria sorgits al voltant de les aplicacions a xarxes de comunicació i d'interconnexió. Aquesta línia de recerca, juntament amb l'estudi dels grafs anomenats *snarks*, va ser

encetada, ja l'any 1980, pels professors José Luis Andrés Yebra i Miquel Àngel Fiol, els quals ben segur podríem considerar els iniciadors dels treballs en matemàtica discreta a les universitats catalanes. El llistat de problemes investigats és llarg i, per motius històrics, voldríem citar en primer lloc el *Problema (Δ,D)* lligat a l'obtenció de grafs densos, és a dir, grafs amb un nombre de vèrtexs elevat amb relació a la distància màxima entre ells i el nombre màxim de branques incidents en cada vèrtex. Es coneix una cota superior, anomenada cota de Moore, pel nombre màxim de vèrtexs que pot tenir el graf però les construccions explícites són escasses. Juntament amb investigadors de la UdL, s'han fet aportacions significatives tant en l'obtenció de noves topologies per a grafs densos com en l'estudi teòric de grafs dirigits de Moore dèbilment distància-regulars i grafs dirigits de Moore en què es relaxen certes condicions referents a l'excentricitat dels seus vèrtexs. Des de Barcelona es manté per a la *World Combinatorial Exchange* una pàgina web amb la taula dels millors resultats coneguts en aquest problema.

Un altre tema d'interès per les seves aplicacions al disseny de xarxes d'interconnexió fiables, però també per la importància del paràmetre en problemes teòrics, és l'estudi de la connectivitat. A la UPC s'ha treballat en l'obtenció de nous paràmetres que mesurin de manera precisa el grau de disgregació d'un graf davant la supressió d'alguns dels seus vèrtexs o branques, així com en la determinació de condicions suficients que permetin assegurar un alt grau de connectivitat. Un problema, en certa manera dual al problema de Moore esmentat anteriorment, és el de minimitzar el nombre de vèrtexs, donats el nombre de branques incidents en cada vèrtex i la longitud dels cicles més curts. De nou, les construccions explícites són escasses i les propietats d'aquests grafs, anomenats *cages*, són relativament desconegudes. Se n'ha estudiat la connectivitat i s'han aportat nous resultats al voltant de la conjectura que estableix que les *cages* són grafs maximalment connectats. També s'han investigat problemes isoperimètrics en què es persegueix obtenir cotes mínimes òptimes per a la funció que dóna la mesura de la frontera d'un conjunt en termes de la seva cardinalitat i que poden ser vistos com un cas límit de les mesures de connectivitat.

La teoria espectral de grafs ha estat també una línia molt activa. Hem de mencionar els resultats aportats principalment des de la UPC, però també cal tenir en compte els treballs en col·laboració amb investigadors que actualment pertanyen a la UdL i a la URV. El coneixement dels autovalors i autovectors de les matrius d'adjacència o laplaciana és molt rellevant per a estudiar certes propietats estructurals del graf. Hi juguen un paper fonamental algunes famílies de polinomis, com els anomenats polinomis alternants i els sistemes de polinomis ortogonals. Les tècniques espectrals

són especialment útils en grafs amb elevada simetria i podem destacar les aportacions realitzades en la caracterització quasiespectral dels grafs distància-regulars, el teorema de l'excés espectral, els conceptes d'espectre local i pseudo-distància-regularitat local, i l'estudi de les relacions de grafs distància-regulars amb determinats codis.

Com s'ha dit abans, la llista de temes motivats per la modelització matemàtica de les xarxes és llarga i també hauríem de citar l'estudi de problemes de coloració de vèrtexs i branques, l'estudi de noves mesures i paràmetres per a la modelització de xarxes complexes (com la Xarxa Internet o, en general, les xarxes anomenades *petit món*), l'estudi de problemes d'etiquetatge i empaquetatge, de problemes extremals en grafs altament regulars, i l'estudi de grafs de Cayley i grafs circulants.

Cal esmentar també els resultats obtinguts en combinatòria enumerativa. Investigadors de la UPC han determinat amb precisió el nombre asimptòtic de grafs planars, un problema obert des del 1960, i han fet aportacions significatives en la determinació de les lleis límit que obeeixen alguns paràmetres dels grafs planars aleatoris. Les tècniques emprades es basen en una anàlisi detallada de les funcions generadores involucrades. Altres treballs en aquesta línia fan referència a la distribució de graus, a l'enumeració de grafs que no contenen menors prefixats i a l'enumeració i les lleis límit de famílies particulars, com els grafs anomenats *sèrie-paral·lel*. També s'ha fet una àmplia i important recerca en l'estudi i el càlcul del polinomi de Tutte de grafs i matroides i en l'enumeració de grafs ordenats amb configuracions prohibides. (El polinomi de Tutte d'un graf és un potent invariant amb la propietat que la seva avaluació en punts especials del pla proporciona diferents paràmetres del graf, com per exemple el nombre d'arbres generadors.)

En l'àmbit de la combinatòria i les estructures finites, altres línies actives a la UPC s'han dedicat a l'estudi de problemes extremals en combinatòria additiva i en geometries finites. Pel que fa a la combinatòria additiva, s'ha treballat en l'obtenció de caracteritzacions estructurals de conjunts de nombres, o en general d'elements d'un grup abelià, a partir del coneixement de la seva suma. Aquest tipus de caracteritzacions es pot obtenir només del coneixement del cardinal de la suma d'un conjunt amb si mateix quan aquest cardinal és petit. S'han desenvolupat tècniques de naturalesa combinatòria relacionades amb problemes isoperimètrics en grafs amb grups d'automorfismes transitius. Pel que fa a les geometries finites, s'ha treballat en l'aplicació de mètodes polinomials per a obtenir resultats d'existència (i en el seu cas construcció) de configuracions extremals com són els anomenats (k,n)-arcs o els *blocking sets*.

A cavall de la matemàtica discreta, la geometria i la informàtica, una altra línia de recerca molt activa a la UPC se centra en la geometria discreta, combinatòria i computacional. En aquest tercer vessant s'estudien problemes geomètrics des del punt de vista de la computació, la qual cosa és inseparable de l'estudi dels fonaments corresponents en el camp discret i combinatori. Les àrees principals d'aplicació són la informàtica gràfica, el disseny i la fabricació assistits per ordinador, el reconeixement de formes, la morfologia computacional, el disseny de circuits integrats a molt gran escala, la visió artificial, els sistemes d'informació geogràfica i la robòtica. L'objectiu principal és el disseny i l'anàlisi d'algorismes per a la solució eficient de problemes geomètrics, l'anàlisi de la complexitat combinatòria d'estructures geomètriques, l'estudi d'estructures de dades geomètriques, la representació i manipulació d'objectes geomètrics i de les relacions entre ells, i, més en general, el desenvolupament de la fonamentació geomètrica apropiada. Entre els principals temes de treball en què s'han fet aportacions d'especial repercussió internacional, podem destacar els resultats obtinguts en la transformació progressiva d'estructures per successions de petits canvis (*flips*), les variants cromàtiques del teorema d'Erdös-Szekeres, les afitacions del nombre de grafs geomètrics —en sentit estricte, punts com nodes i segments com arestes— de famílies significades, l'obtenció de propietats dels grafs de proximitat geomètrica, el disseny d'algorismes d'optimització geomètrica, particularment en problemes d'ubicació òptima per a mètriques temporals, els resultats en teoria geomètrica de la convexitat en grafs combinatoris i, ja en el vessant més algebraic de les bases de Gröbner, el disseny d'algorismes eficients per a la discussió de sistemes d'equacions polinòmiques amb paràmetres.

L'expertesa dels grups de la UPC que fan recerca en matemàtica discreta els ha permès forjar-se un prestigi internacional; han coordinat xarxes d'àmbit europeu i formen part de *DIMATIA* (*Discrete Mathematics and Theoretical Computer Science*), consorci que agrupa una vintena de prestigiosos equips d'investigació a Europa i als Estats Units.

També des de la UPC es desenvolupen tècniques d'aproximació per a problemes de contorn i estats d'equilibri tant en el context de grafs localment finits com en el dels medis continus. Pel que fa a l'anàlisi en grafs, s'ha treballat en la determinació d'una estructura intrínseca que permeti establir els fonaments del càlcul vectorial, així com el tractament de problemes de contorn, la caracterització de les funcions de Green, l'estimació d'autovalors, el problema invers d'identificació i l'avaluació de les propietats estructurals de les xarxes. La principal aportació ha estat la introducció de l'espai tangent a un vèrtex i el tractament de problemes de contorn,

que s'ha desenvolupat de manera molt innovadora. També s'ha contribuït de manera destacable a l'estudi del problema de l'estimació dels punts de Fekete d'un compacte, en què s'han analitzat detalladament els casos corresponents a l'energia potencial electrostàtica —a causa del seu interès en Enginyeria Elèctrica— i a d'altres funcionals d'energia potencial propis de la Química i la Biologia.

La recerca en criptologia i en teoria de codis

En criptologia, trobem també a la UPC línies de treball molt actives dedicades a investigar qüestions referides a criptografia de clau pública, a criptografia distribuïda (que tracta amb criptosistemes que proveeixen seguretat en les comunicacions en situacions que involucren un gran nombre d'usuaris) i a la compartició de secrets. Pel que fa a la criptografia de clau pública i a la criptografia distribuïda, cal esmentar la recerca adreçada al disseny de nous sistemes de xifrat de clau pública basats en certificats i nous protocols criptogràfics distribuïts en què les aplicacions bilineals (*pairings*) sobre corbes el·líptiques juguen un paper fonamental. S'ha investigat també la construcció de nous sistemes de xifrat basats en grups no commutatius que compleixin els màxims requeriments de seguretat.

On les tècniques combinatòries han jugat un paper fonamental, però, ha estat en els resultats obtinguts sobre els esquemes per a compartir secrets, que són un dels components importants dels protocols usats per a construir criptosistemes distribuïts. Els esquemes per a compartir secrets són mètodes per a distribuir fragments d'un valor secret entre un conjunt de participants de manera que només els subconjunts de participants autoritzats (l'especificació dels quals s'anomena *estructura d'accés*) poden recobrar el secret, però en canvi els subconjunts de participants no autoritzats són incapaços d'obtenir-ne qualsevol informació. L'objectiu general és l'optimització dels esquemes per a estructures d'accés generals. Podríem dir que els temes tractats en aquesta línia de treball pels investigadors de la UPC exploren les relacions entre codis, matroides i famílies particulars d'esquemes per a compartir secrets. Així, destaca l'aplicació de matroides i polimatroides a la caracterització de les estructures d'accés que admeten esquemes ideals, en els quals s'assoleix la situació òptima en què els fragments tenen la mateixa llargada que el secret, i en el cas general, a la determinació de les taxes d'informació òptimes. S'ha resolt el problema obert sobre els valors que pot prendre la taxa d'informació òptima i s'ha mostrat, al mateix temps, el primer exemple d'una estructura d'accés de matroide amb taxa d'informació estrictament menor que 1. També s'han caracteritzat les estructures d'accés tripartides que són ideals; s'ha estudiat l'apli-

cació dels esquemes per a compartir secrets lineals i multiplicatius a la computació multipart segura; s'han investigat esquemes basats en codis algebraico-geomètrics, i s'ha treballat en el problema de la detecció de tramposos.

La privadesa i la seguretat de les dades també s'ha treballat intensament a la URV. La recerca feta es troba de nou a cavall de diverses disciplines, com l'estadística, la matemàtica discreta, la criptografia, la informàtica i les telecomunicacions. A més de fer contribucions importants en les temàtiques del secret estadístic i del modelatge econòmic de la privadesa i de la seguretat, també s'ha treballat en el disseny de protocols criptogràfics combinatoris *peer-to-peer* que proporcionin privadesa i seguretat en la recuperació privada d'informació (per exemple, consultar Google o qualsevol base de dades sense que puguin crear cap perfil de l'usuari). En aquesta línia s'han explotat resultats coneguts i se n'han obtingut de nous en configuracions combinatòries, plans projectius, grafs de Ramanujan i mesures de centralitat en grafs. Una altra temàtica investigada fa referència a la seguretat i la privadesa en xarxes vehiculars (fer que els vehicles emetin informació sobre les condicions del trànsit sense revelar qui són, però amb la garantia que els missatges emesos són fiables). Aquí s'han emprat coneixements sobre criptosistemes el·líptics, criptografia basada en la identitat, criptografia sense certificats i criptografia asimètrica de grups.

També a la UdL s'ha fet recerca en l'estudi de problemes computacionals amb corbes el·líptiques i hiperel·líptiques sobre cossos finits, i en el disseny de protocols criptogràfics en entorns restringits computacionalment, com els sistemes RFID (*Radio Frequency Identification*) i les targetes intel·ligents.

La recerca en teoria de codis també és molt activa a la UAB. S'ha treballat en diversos problemes referents a codis que són òptims en algun sentit, com els codis perfectes en l'espai de Hamming, els codis uniformement empilats, els codis perfectes definits en grafs distància regulars, entre altres. Basant-se en la combinatòria i, a vegades en l'àlgebra, s'han estudiat variants no lineals de codis coneguts com els de Reed-Muller, Preparata, Kerdock i Hadamard. S'han estudiat estructures no lineals, però que tenen un substrat donat per un grup. Quan aquest grup és commutatiu, s'arriba al que s'anomenen *codis Z4-lineals*, o més en general, *codis Z2Z4-lineals* (aquests últims introduïts en la literatura pels investigadors de la UAB). Per a totes les variants de codis no lineals és important calcular el rang (dimensió del mínim espai vectorial que el conté) i el *kernel* (dimensió del major espai vectorial dins del grup de manera que aquest es pugui construir com una reunió de classes laterals d'aquell). Així mateix, s'ha construït una variant *Z2Z4*-lineal dels codis de Reed-Muller i s'han dedicat esforços a considerar la mida i

l'estructura algebraica resultant de fer interseccions de codis de la mateixa longitud i de les mateixes característiques (per exemple, codis de Hadamard, o perfectes, etc.). També s'han investigat de manera intensiva els codis completament regulars (CR). La completa classificació d'aquests codis és lluny de ser una realitat, i s'ha tractat de construir nous exemplars amb noves tècniques més algebraiques que les clàssiques basades en la teoria de dissenys i esquemes d'associació. Ara mateix, la principal conjectura en aquest camp de recerca és la no existència de codis CR amb una capacitat correctora més gran de tres. El investigadors de la UAB han demostrat la conjectura per a codis CR completament transitius.

La recerca en algorísmia i complexitat

En l'àrea de l'algorísmia i complexitat hem de mencionar el treball del potent grup d'investigadors de la UPC. Es tracta d'un grup gran que ha fet contribucions importants en una llarga llista de temàtiques relacionades amb la informàtica teòrica. Entre altres, podríem citar l'estudi de la relació entre la complexitat de funcions booleanes i mètodes de desaleatorització d'algorismes probabilístics, la recerca en complexitat parametritzada, l'estudi d'algorismes exactes i parametritzats per a problemes *hard*, així com algorismes i estructures de dades per a problemes fonamentals de les ciències de la computació. Aquí només farem esment d'algunes de les línies i resultats més lligats a la teoria de grafs i de la combinatòria. Així, podríem citar l'estudi de la complexitat de problemes de *graph layout* i de problemes isoperimètrics, en què s'ha treballat de manera especial el disseny i l'avaluació analítica i empírica d'algorismes i mètodes heurístics. Les tècniques desenvolupades tenen aplicació pràctica al disseny de circuits integrats a molt gran escala. Un altre tema de treball ha estat la modelització de xarxes dinàmiques; se n'han investigat la formulació i l'evolució amb el propòsit de fer-ne un estudi aprofundit del rendiment en les aplicacions. A més de tècniques de simulació, es fan servir en aquest estudi mètodes probabilístics i de la teoria de jocs. Mencionarem també la recerca en l'anàlisi de problemes combinatoris intractables, fent èmfasi en les seves propietats estructurals, així com la recerca en el disseny i anàlisi d'algorismes aproximats per a problemes d'optimització combinatòria. Aquestes investigacions, motivades per l'estudi de problemes fonamentals de les ciències de la computació, han donat com a fruit aportacions concretes en problemes interessants de la teoria de grafs. Per exemple, s'han estudiat problemes de coloració de diferents models de grafs adequats al disseny de xarxes de transmissió sense fils (com ara xarxes de sensors), com són els grafs geomètrics aleatoris i els grafs de proximitat aleatoris. Per mitjà de tècniques probabilístiques, s'han estudiat altres

propietats estructurals dels grafs geomètrics aleatoris com són l'existència de cicles hamiltonians, la robustesa de la seva connectivitat o l'estudi de conjunts separadors de branques que parteixen el graf de manera equilibrada.

Acabem aquest repàs citant també el destacable treball dut a terme per alguns investigadors de la UPF en els àmbit de la teoria de la informació, l'estudi d'estructures combinatòries aleatòries, el reconeixement de patrons, i l'estudi de la complexitat computacional de problemes de satisfacció de restriccions i, en general, de problemes combinatoris.