M, aleshores tota matriu amb determinant p, primer, seria producte de matrius de M. Ara, però, en haver-hi infinits nombres primers, el conjunt M hauria de contenir infinites matrius, una per a cada p.

A68. (D'una olimpíada brasilera.) Trobeu totes les solucions enteres i positives de l'equació

$$(m+1)^n - 1 = m!$$

Solució: (Solució de Jordi-Lluís Figueras Romero, UB.) Es comprova amb pocs càlculs que, si $m < 10$, aleshores les úniques solucions són $m = n = 1$, $m = 2$ i $n = 1$, i $m = 4$ i $n = 2$. Vegem ara que no n'hi ha més.

Clarament, $n < m$. Aleshores, segons el *postulat de Bertrand*, hi ha p_1, primer, amb $\frac{m}{2} < p_1 < m$, que divideix $m!$ i no divideix m. Per tant, $(m+1)^n \equiv 1(\mathrm{mod} p_1)$ equival que $p_1 - 1 | n$ i, com que $n < m$, resulta $p_1 - 1 = n$.

Una nova aplicació del *postulat de Bertrand* mostra l'existència de p_2, també primer, amb $\frac{m!}{2} < p_2 < m!$, que divideix $m!$ i no divideix m. Ara, $(m+1)^n \equiv 1(\mathrm{mod}\ p_2)$ equival que $p_2 - 1 | n$, és a dir, $p_2 - 1 < p_1 - 1$, cosa que no pot ser, perquè $p_2 > \frac{m!}{2} > m > p_1$.

Carles Romero
IES Manuel Blancafort, la Garriga

Tesis

- Juan A. Mantecón Baena va llegir la seva tesi, dirigida per José Rodellar Benedé i Manuel Gómez Valentín, titulada *Sistemas de control predictivo en canales de riego: Formulación y simulación numérica* , el dia 5 d'abril de 2004. La tesi correspon al Departament de Matemàtica Aplicada III de la Universitat Politècnica de Catalunya.

L'objectiu d'aquesta tesi és l'aplicació de mètodes de control predictiu al problema de la gestió automàtica de canals de reg.

En els últims anys s'ha despertat un notable interès pels sistemes de control automàtic per a la gestió de canals de reg. Aquest interès té la seva base en la motivació per a l'estalvi dels recursos hídrics mitjançant la modernització de les xarxes de distribució utilitzant noves tecnologies i nous mètodes d'optimització i control. Aquesta tesi pretén contribuir en aquest context amb el desenvolupament de sistemes de control per a canals de reg utilitzant conceptes de control predictiu, de modelització hidràulica i de simulació numèrica.

Es considera un canal com una conducció dividida en N trams separats per comportes amb un embassament de nivell constant en l'extrem aigua amunt, i un abocador en l'extrem aigua avall. En cada tram es considera una petita zona d'emmagatzematge, just abans de la comporta aigua avall, on es consideren situades les sortides laterals així com els sensors de nivell, cabal lateral i cabal sota comporta de cada tram.

El problema de control que es planteja és el de mantenir els nivells d'aigua en cada tram del canal a un cert valor de consigna, independentment que es produeixin pertorbacions en el sistema en forma de variació dels cabals laterals (demandes dels suposats regants). L'acció de control en cada tram està constituïda pel moviment de la comporta situada aigua amunt.

El model utilitzat per al control predictiu resulta de la combinació de dos conceptes clàssics: el model de Muskingum del flux en un tram i l'equació de continuïtat en la zona d'emmagatzematge.

Des del punt de vista del disseny i implementació dels algorismes de control, el problema s'aborda sota dues estratègies diferents: considerant cada tram com un sistema de control individual amb un controlador accionant cada comporta (estratègia descentralitzada) o

considerant un únic controlador multivariable que accioni totes les comportes simultàniament (estratègia centralitzada).

En el cas de l'estratègia descentralitzada, el sistema de control consta d'un controlador predictiu i d'un controlador local per a cada tram, així com d'una lògica de supervisió del sistema en el seu conjunt. L'algorisme de control predictiu per a cada tram té en compte l'acoblament existent entre dos trams adjacents.

En el cas de l'estratègia centralitzada, el sistema de control consta d'un únic controlador centralitzat que implementa l'algorisme de control predictiu per a tot el canal i d'un controlador local per a cada tram. El controlador predictiu ha de gestionar la política de mostreig del sistema que, en el cas de canals amb trams desiguals, ha de formular-se amb un esquema de múltiples períodes de mostreig. S'inclouen una sèrie d'exemples de simulació dels sistemes de control proposats i una descripció de l'eina de simulació utilitzada per a això, la qual ha estat desenvolupada en el context d'aquesta tesi.

- David Galindo Chacón va llegir la seva tesi, dirigida per Sebastià Martí Molleví, titulada *Design and analysis of semantically secure public key encryption schemes*, el dia 30 de juny de 2004. La tesi correspon al Departament de Matemàtica Aplicada IV de la Universitat Politècnica de Catalunya.

Un esquema de xifrat és un procediment que fa possible que dues entitats es puguin comunicar de forma segura mitjançant un canal públic, de tal manera que, si una entitat externa a la comunicació intercepta la comunicació, no pugui recuperar el missatge original. A la criptografia de clau pública, les claus necessàries per a xifrar i desxifrar són diferents; la clau de xifrat és pública, i per tant a disposició tant d'usuaris legítims com il·legítims. Malgrat que els esquemes de xifrat són objectes bàsics dins la criptografia de clau pública i han estat objecte d'estudi des dels orígens d'aquesta disciplina, les exigents nocions de seguretat actuals i els recents progressos en criptoanàlisi fan del disseny de nous esquemes de xifrat un camp de recerca actiu. En aquesta tesi s'estudien esquemes de xifrat amb «seguretat semàntica». Informalment, un xifrat té seguretat semàntica si la possessió del missatge xifrat no dóna més informació sobre el missatge original que la que es coneixia amb antelació a rebre el xifrat. Així, en aquest treball es proposen i analitzen nous esquemes amb seguretat semàntica, alhora que s'estudien i milloren esquemes previs d'especial rellevància.

- Sergi Elizalde Torrent va llegir la seva tesi, dirigida per Marc Noy Serrano, titulada *Motius consecutius i estadístics en permutacions restringides*, el dia 16 de juliol de 2004. La tesi correspon al Departament de Matemàtica Aplicada II de la Universitat Politècnica de Catalunya.

El tema d'aquesta tesi és l'enumeració de permutacions amb subseqüències prohibides respecte a certs estadístics, i l'enumeració de permutacions que eviten subseqüències generalitzades.

Després d'introduir algunes definicions sobre subseqüències i estadístics en permutacions i camins de Dyck, comencem estudiant la distribució dels estadístics *nombre de punts fixos* i *nombre d'excedències* en permutacions que eviten una subseqüència de longitud 3. Un dels resultats principals és que la distribució conjunta d'aquest parell de paràmetres és la mateixa en permutacions que eviten 321 que en permutacions que eviten 132. Això generalitza un teorema recent de Robertson, Saracino i Zeilberger. Demostrem aquest resultat donant una bijecció que preserva els dos estadístics en qüestió i un altre paràmetre. La idea clau consisteix a introduir una nova classe d'estadístics en camins de Dyck, basada en el que anomenem *túnel*.

A continuació considerem el mateix parell d'estadístics en permutacions que eviten simultàniament dues o més subseqüències de longi-

tud 3. Resolem tots els casos donant les funcions generadores corresponents. Alguns casos són generalitzats a subseqüències de longitud arbitrària. També descrivim la distribució d'aquests paràmetres en involucions que eviten qualsevol subconjunt de subseqüències de longitud 3. La tècnica principal consisteix a fer servir bijeccions entre permutacions amb subseqüències prohibides i certs tipus de camins de Dyck, de manera que els estadístics en permutacions que considerem corresponen a estadístics en camins de Dyck que són més fàcils d'enumerar.

Tot seguit presentem una nova família de bijeccions del conjunt de camins de Dyck a si mateix, que envien estadístics que apareixen en l'estudi de permutacions amb subseqüències prohibides a estadístics clàssics en camins de Dyck, la distribució dels quals s'obté fàcilment. En particular, això ens dóna una prova bijectiva senzilla de l'equidistribució de punts fixos en les permutacions que eviten 321 i en les que eviten 132. A continuació donem noves interpretacions dels nombres de Catalan i dels nombres de Fine. Considerem una classe de permutacions definida en termes d'aparellaments de dos punts en una circumferència sense creuaments. N'estudiem l'estructura i algunes propietats, i donem la distribució de diversos estadístics en aquestes permutacions.

En la part següent de la tesi introduïm una noció diferent de subseqüències prohibides, amb el requeriment que els elements que formen la subseqüència han d'aparèixer en posicions consecutives a la permutació. De manera més general, estudiem la distribució del nombre d'ocurrències de subparaules (subseqüències consecutives) en permutacions. Resolem el problema en diversos casos segons la forma de la subparaula, i n'obtenim les funcions generadores exponencials bivariades corresponents com a solucions de certes equacions diferencials lineals. El mètode està basat en la representació de permutacions com a arbres binaris creixents i en mètodes simbòlics.

La part final tracta de subseqüències generalitzades, que estenen tant la noció de subseqüències clàssiques com la de subparaules. Per a algunes subseqüències obtenim nous resultats enumeratius. Finalment, estudiem el comportament asimptòtic del nombre de permutacions de mida n que eviten una subseqüència generalitzada fixa quan n tendeix a infinit. També donem fites inferiors i superiors en el nombre de permutacions que eviten certes subseqüències.

- Mónica Blanco Abellán va llegir la seva tesi, dirigida per Josep Pla i Carrera, titulada *Hermenèutica del càlcul diferencial a l'Europa del segle* XVIII*: de l'*Analyse des infiniment petits de L'Hôpital *(1696) al* Traité élémentaire de calcul différentiel et de calcul intégral de Lacroix *(1802)*, el dia 28 d'octubre de 2004. La tesi correspon al Departament de Matemàtiques de la Universitat Autònoma de Barcelona, dins del Programa Interuniversitari de Doctorat d'Història de les Ciències (UAB-UB), coordinat pel CEHIC.

L'objectiu d'aquesta tesi és analitzar el desenvolupament matemàtic del càlcul diferencial mitjançant l'estudi d'algunes obres aparegudes al segle XVIII a França, Alemanya, Itàlia i Gran Bretanya. Situant el treball dins el context del desenvolupament històric del càlcul i dins del context institucional de les matemàtiques, s'ha comparat com, a través dels textos tractats, els diferents països exposen els elements del càlcul. Les obres escollides per a elaborar aquesta tesi han estat:

- *Analyse démontrée* (1708), de Charles René Reyneau.
- *Cours de mathématiques à l'usage du corps de l'artillerie* (1799–1800), d'Étienne Bézout.
- *Leçons sur le calcul des fonctions* (1800), de Joseph Louis Lagrange.
- *Traité élémentaire de calcul différentiel et de calcul intégral* (1802), de Sylvestre François Lacroix.
- *Elementa analyseos* (1713–1715), de Christian Wolff.
- *Anfangsgründe der Analysis des Unendlichen* (1760), d'Abraham Gotthelf Kästner.
- *Anfangsgründe der Analysis des Unendlichen* (1770), de Georg Friedrich Tempelhoff.
- *Anfangsgründe der mathematischen Analysis und höhern Geometrie* (1786), de Wenceslau J. G. Karsten.

- *Instituzioni Analitiche* (1748), de Maria Gaetana Agnesi.
- *Principj di analisi sublime* (1759), de Giuseppe Luigi Lagrange.
- *Institutiones Analyticae* (1765–1767), de Vincenzo Riccati i Girolamo Saladini i *Compendio d'analisi* (1775), de Girolamo Saladini.
- *An Institution of Fluxions* (1706), de Humphry Ditton.
- *A Treatise of Fluxions* (1742), de Colin Maclaurin.
- *The Doctrine and Application of Fluxions* (1750), de Thomas Simpson.

També s'analitza l'obra *Institutiones calculi differentialis* (1755), de Leonhard Euler, donada la influència d'aquest autor en el desenvolupament del càlcul, així com la seva internacionalitat.

La tesi comença amb una anàlisi comparativa de l'*Analyse des infiniment petits de L'Hôpital* (1696), primer tractat sistemàtic de càlcul diferencial, i de les *Lectiones de calculo differentialium*, de Johann Bernoulli, basades en les lliçons que aquest oferí a L'Hôpital entre 1691 i 1692. Aquesta anàlisi porta a establir les principals línies que s'han seguit a l'hora d'analitzar i comparar les obres escollides:

a) la manera com presenten els fonaments del càlcul i el corpus teòric que inclouen;
b) si el llenguatge que utilitzen és geomètric o algèbric;
c) els criteris per a escollir les coordenades en relació amb la manera com tracten les corbes (algèbriques i transcendents);
d) els problemes i aplicacions que tracten, així com el seu plantejament;
e) aspectes metodològics, com l'estructura, la intenció didàctica i la notació (aplicant tècniques d'estadística multivariant per a caracteritzar les obres mitjançant les freqüències d'alguns mots).

S'inclou una revisió dels factors que impulsaren la seva lectura com, per exemple, el públic al qual anaven dirigides. També s'avalua la influència de l'*Analyse de L'Hôpital* sobre aquestes obres.

Tenint en compte la influència de Leibniz i Euler en les obres de càlcul diferencial analitzades, i a partir dels resultats d'aquesta anàlisi comparativa detallada dels textos, es detecten tres grups: 1) les obres de L'Hôpital, Reyneau, Wolff, Agnesi, Saladini i Bézout; 2) l'obra italiana de Lagrange i les obres de Kästner i Tempelhoff; 3) les obres de Karsten i Lacroix.

D'altra banda, l'estudi de les obres britàniques fa palès el desenvolupament no homogeni del càlcul fluxional. Així mateix, a partir de les obres d'àmbit militar es veu com varia la importància donada a l'exposició dels fonaments i a la presència d'aplicacions. Finalment, s'estableix el desenvolupament cronològic dels problemes i aplicacions inclosos en les obres analitzades, així com de les corbes tractades, en relació amb l'elecció de les coordenades.

- Jordi Ripoll i Missé va llegir la seva tesi, dirigida per Àngel Calsina i Ballesta, titulada *Evolution of Sex-Ratio in Structured Population Dynamics*, el dia 5 d'octubre de 2005. La tesi correspon al Departament de Matemàtica Aplicada i Anàlisi de la Universitat de Barcelona.

En aquesta tesi abordem l'estudi d'algunes equacions d'evolució no lineals (*e. g.* EDP) que modelitzen la dinàmica de poblacions estructurades amb reproducció sexual, donant una èmfasi especial en l'*evolució biològica* conduïda per la selecció natural. Això últim s'incorpora en els models mitjançant la dinàmica adaptativa, que és una manera de descriure com evolucionen les característiques hereditàries de la població. La *sex-ratio*, definida com la proporció entre el número de femelles i mascles, és analitzada des del punt de vista evolutiu.

La memòria consta de dues parts més una breu introducció a la dinàmica de poblacions estructurades per l'edat (capítol 1).

La primera part (capítol 2) està dedicada a un model per a la dinàmica d'una espècie hermafrodita seqüencial, *i. e.*, una població on cada individu comença la vida essent d'un sexe (concretament com a femella) i després canvia a l'altre per la resta de la seva vida, i el canvi de sexe es produeix en una edat específica la qual és considerada com una variable aleatòria no negativa. Aquest fenomen ha estat observat en

diversos animals incloent-hi espècies de peixos com l'orada (*sparus aurata*), el peix anèmona, el peix lloro i el làbrid de cap blau (*thalassoma bifasciatum*). Primer de tot introduïm les hipòtesis bàsiques i els paràmetres del model: la llei de probabilitat de l'edat del canvi, el funcional no lineal (a causa de la reproducció sexual) que dóna el número de naixements per unitat de temps (*funció de naixença*), i la taxa de mortalitat per càpita, que depèn de la densitat de població. El sistema complet (que exhibeix els processos de naixement, transició i mort), per les densitats en edat de femelles i mascles, és formulat i deduït en la forma d'equacions integrals no lineals, així com també la versió regular en la forma d'equacions en derivades parcials hiperbòliques de primer ordre no lineals no locals amb condicions de frontera, a edat zero, i inicials. Prenem la primera formulació donada la falta de regularitat en general, i en la segona, la derivada de la llei de probabilitat apareix en el terme de transició de femella a mascle.

En la secció 2.3 provem l'existència i unicitat de solucions globals que són no negatives i amb sentit biològic per al present model. Introduïm hipòtesis addicionals, a saber, condicions de Lipschitz adequades sobre la funció de naixença i la taxa de mortalitat. En la secció 2.4 provem que el sistema es pot reduir al *subespai de la sex-ratio intrínseca*, on la dinàmica ve descrita per una sola equació integral no lineal per la densitat en edat d'individus d'ambdós sexes. Una forma explícita de la funció de naixença, en termes de les taxes de fertilitat, és deduïda per a implementacions numèriques posteriors. Aquesta forma es correspon a una resposta funcional de Holling de tipus II i es basa en el fet que les femelles reparteixen el seu temps entre buscar parella i produir nous descendents. El temps esperat de cerca és $\propto$ (número de mascles)$^{-1}$, mentre que el temps esperat de producció de descendència és una constant. La secció 2.5 estudia el comportament asimptòtic de les solucions quan el temps tendeix a infinit. Hem determinat una condició suficient per a poder tenir trajectòries acotades i la possibilitat de dinàmica no trivial. D'altra banda, hem vist també que l'*equilibri d'extinció* és sempre localment asimptòticament estable, mostrant l'efecte Allee, el qual és una característica típica en poblacions amb reproducció sexual.

En la secció 2.6 abordem el problema estacionari, *i. e.*, busquem solucions independents del temps en L^1_+. Els estats d'equilibri no trivials vénen determinats per una equació escalar no lineal per a la població total en equilibri com a variable independent. Tanquem la secció il·lustrant dos casos. El primer és el cas (no lineal) sense competència pels recursos, obtenint com a molt que hi ha un equilibri no trivial, el qual és sempre inestable. S'arriba a una expressió explícita per l'equilibri, i la inestabilitat s'obté per mitjà d'un procés de linealització. El segon cas, el qual és bastant general, inclou un cert tipus de competència i hem trobat que hi ha dos equilibris no trivials per a cada valor de l'edat esperada del canvi en un interval obert acotat. Ambdós casos són representats en un diagrama de bifurcació, per a dos tipus de llei de probabilitat (Heaviside/exponencial).

La teoria dels *operadors acretius*, *i. e.*, aquells que el seu operador resolvent és una aplicació no expansiva, és necessària per a estudiar l'estabilitat local dels equilibris del cas general. En l'apèndix A es demostra la validesa del principi d'estabilitat lineal per al sistema reduït. La demostració es basa en un principi per a equacions d'evolució no lineals governades per operadors acretius, on l'estabilitat ve determinada per l'acretivitat d'un operador lineal associat. En la secció 2.7 reescrivim el sistema reduït com una equació d'evolució i introduïm hipòtesis addicionals, essencialment, condicions adequades sobre la regularitat de la funció de naixença i la taxa de mortalitat. Finalment obtenim una condició suficient per l'estabilitat local sense calcular l'espectre de la part lineal.

La secció 2.8 estudia la dinàmica evolutiva de l'edat del canvi considerant evolució fenotípica en models de poblacions diploides. Prenem com a variable evolutiva de dimensió infinita la llei de probabilitat. Suposem una població resident en equilibri estable i considerem una població invasora/mutant petita formada per *heterozigots* i *homozigots* (≈ 0). Hem usat anàlisi convexa per a provar que una estratègia invencible o estratègia evolutivament estable (ESS) és una funció de Heaviside: tots els individus de la població canvien de sexe a la mateixa edat. Més concretament, el càlcul d'una estratègia tal es basa en optimització lineal/afí sobre conjunts compactes i convexos. El nostre resultat generalitza l'obtingut per Char-

nov. Finalment, la secció 2.9 tracta del valor adaptatiu de la *sex-ratio* de la població en equilibri, el qual és en general diferent d'u. No obstant això, si les fertilitats no depenen de l'edat dels individus llavors la *sex-ratio* és igual a u. A més, suposant també una mortalitat independent de l'edat hem trobat que la transició de femella a mascle es produeix en el $69,3$ % de l'esperança de vida de la població.

La segona part (capítol 3) està dedicada a un model per a la fase sexual d'una espècie haplodiploide (*rotífers monogononts*) que exhibeix l'anomenada *partenogènesi cíclica* (ambdues formes de reproducció: asexual i sexual). Els rotífers monogononts són petits animals microinvertebrats que viuen en medis aquàtics amb variacions estacionals. El sistema original, el qual va ser introduït per Aparici, Carmona i Serra del Departament d'Ecologia de la Universitat de València, és formulat en la forma d'equacions en derivades parcials hiperbòliques de primer ordre no lineals no locals. Les variables d'estat són les densitats en edat de femelles míctiques verges (productores de mascles), femelles míctiques fecundades (productores d'ous de resistència) i mascles haploides, mentre que els paràmetres, independents del temps, del model són les taxes de mortalitat per càpita, la taxa d'encontres mascle-femella, la taxa d'entrada (reclutament) de femelles míctiques, la fertilitat de les femelles míctiques productores de mascles, l'edat de maduració de les femelles i el llindar per l'edat de fecundació (el qual és més petit o igual que l'edat de maduració). La transició de verge a fecundada ve donada en termes de la funció característica de l'interval de fecundació i de la població total de mascles haploides. L'equació per a les femelles fecundades resulta estar desacoblada de les altres; per tant, ens centrem en les altres dues. Fent un canvi d'unitats en edat, temps i població hem reduït el nombre de paràmetres a tan sols quatre: les noves taxes de mortalitat, el nou llindar per l'edat de fecundació i la nova taxa d'encontres. Com a resultat, obtenim el sistema reduït i adimensional.

La secció 3.3 aborda el problema estacionari, *i. e.*, busquem solucions independents del temps en $W^{1,1}$. Hem trobat que hi ha un únic estat d'equilibri continu el qual es pot escriure en funció de la població total de mascles en equilibri. Això últim s'obté com a única solució d'una equació escalar no lineal.

La secció 3.4 estudia l'estabilitat local de l'equilibri per mitjà d'un procés de linealització. Per una banda, analitzem la corresponent equació característica i obtenim solucions complexes que creuen l'eix imaginari, i, per altra banda, provem la validesa del principi d'estabilitat lineal, el qual està basat en una formulació semilineal a L^1, i en el fet que la cota de creixement essencial és negativa (com és habitual en aquest tipus d'equacions). L'anàlisi de l'estabilitat lineal revela que l'equilibri és estable per, valors dels paràmetres en una àmplia regió que conté els valors empírics. No obstant això, pot ser inestable per a valors no massa llunyans.

En la secció 3.5 apliquem un teorema de bifurcació de Hopf en un context de dimensió infinita. Comprovem que hi ha un parell de valors propis conjugats sobre l'eix imaginari que creuen amb velocitat positiva. Reescrivint el sistema com una equació d'evolució no lineal i calculant l'operador adjunt i l'operador resolvent (aquest últim resolent una EDO lineal amb coeficients constants a trossos), podem determinar si la bifurcació és *subcrítica* o *supercrítica*. Com a resultat, hem demostrat l'aparició d'un cicle límit estable (òrbita periòdica isolada).

La secció 3.6 està dedicada a la solució numèrica del problema. Hem dissenyat un esquema numèric explícit basat en integració analítica i numèrica al llarg de les corbes característiques. Diversos experiments numèrics són portats a terme. Les simulacions numèriques corroboren i amplien els resultats analítics obtinguts.

Fe d'errades

El títol de la tesi de Glòria Mateu és *Models de distribució sobre el símplex* i no el que va sortir publicat en la *SCM/Notícies* 21. El resum i la resta de dades estaven correctes.