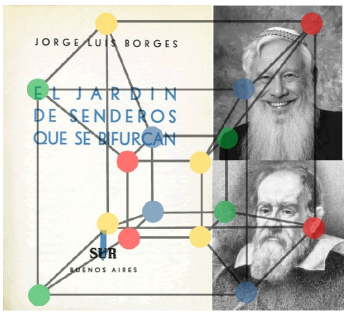
MAT^2
MATerials MATemàtics
Volum 2025, treball no. 1, 21 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/web/matmat

Comunicacions subtils: Yá Tsun, Aumann, l'hipercub, Galileu, el coneixement comú i el coneixement zero

Jaume Aguadé



Quan vaig començar a estudiar matemàtiques —fa molts i molts anys— llegíem *Cien años de soledad* i *Rayuela* però també, de forma recurrent i molt substancial, *Ficciones* i *El Aleph*, que contenen contes que encara ara recordo molt millor que gairebé qualsevol obra que hagi llegit d'ençà d'aleshores, contes que s'han convertit en tòpics culturals universals —*La biblioteca de Babel* o *Tlön, Uqbar, Orbis Tertius*, per exemple— i personatges inoblidables —*Pierre Menard, Funes, Almotásim* o *Juan de Panonia*, per exemple.

Un d'aquells contes que van deixar en mi una profunda empremta es titula *El jardín de senderos que se bifurcan* i ens servirà d'introducció al tema que vull tractar en aquest escrit. Recordem-ne breument l'argument:

> *Yá Tsun és un espia d'origen xinès que viu a Anglaterra en el temps de la Primera Guerra Mundial i treballa per als alemanys. L'han descobert i s'escapa en un tren i això li dóna quaranta minuts d'avantatge sobre el seu perseguidor. Dedica aquest temps a visitar el Dr. Stephen Albert, un famós sintoista. L'espia i el sintoista no es coneixen de res, però el Dr. Albert rep amablement Yá Tsun a casa seva i entre ells s'estableix una conversa filosòfica extraordinària (que deixarem de banda, malgrat ser la part fonamental del conte). Quan l'espia veu el seu perseguidor al jardí del Dr. Albert, sense cap motiu imaginable, mata d'un tret el doctor, just abans de ser capturat. L'endemà, els diaris es fan ressò de l'assassinat del Dr. Albert a mans d'un desconegut*

> *de nom Yá Tsun i aleshores, a les darreres línies del conte, entenem que l'espia havia aconseguit comunicar als seus superiors la situació del secret parc d'artilleria britànic al nord de França, a la Picardia, exactament al poble que es diu* ***Albert****.*

El títol *«comunicacions subtils»* fa referència a la capacitat de comunicar una informació en unes condicions aparentment impossibles, com ho fa en Yá Tsun. Veurem alguns exemple força curiosos i, evidentment, mirarem d'entendre, en cada cas, les matemàtiques que hi ha al darrere de les diverses *comunicacions subtils*.

Abans de començar, cal explicar que aquest és un article de divulgació —sense deixar de ser un article de matemàtiques— en el que intuirem, molt d'esquitllentes, indicis de teories matemàtiques importants, de camps d'estudi immensos, que no podrem visitar plenament. Gaudiu-ne com el que és i no n'espereu cap tractament a fons de les teories que, ací i allà, aniran traient el cap al llarg del text.

1 Per un grapat de dòlars

Es tracta d'un curiós repte per a un equip de dues persones que actuen solidàriament —diguem-ne Alícia i Bernat— als que es mostra una petita calaixera amb dos calaixos i se'ls explica que a la calaixera hi ha una quantitat de monedes —dòlars de plata, per exemple— igual a un d'aquests dos valors: r, $r+k$ amb $r, k > 0$. L'Alícia i en Bernat guanyaran aquestes monedes si aconsegueixen saber quantes monedes hi ha en total, amb aquestes regles del joc:

1. Es mostra a l'Alícia el contingut d'un calaix: hi ha a monedes. Es mostra a en Bernat el contingut de l'altre calaix: hi ha b monedes.

2. Es pregunta a l'Alícia si sap quantes monedes hi ha en total, i només hi ha dues respostes possibles: (a) *«No ho sé»* (és a dir, *passo*), (b) *«Hi ha x monedes»*.

3. Si l'Alícia ha passat, es fa la mateixa pregunta a en Bernat, amb les mateixes dues respostes possibles.

4. Si en Bernat ha passat, es torna al pas 2.

5. El joc s'acaba quan un dels dos jugadors no passa. Si encerta el nombre de monedes, els dos jugadors s'emporten el premi, si no l'encerta, els dos jugadors han perdut i marxen amb les mans buides.

Es tracta de trobar una estratègia que puguin pactar A i B abans de començar el joc i que els permeti, amb total seguretat, aconseguir el premi. Tenim, doncs, un repte de *comunicació subtil*: n'hi ha prou que A comuniqui

a B el valor de a o que B comuniqui a A el valor de b. El problema és que el *canal* de comunicació és molt *estret*: només admet la informació «passo».

Ara el lector pot deixar de llegir i buscar una estratègia guanyadora. Crec que no li costarà gaire arribar a alguna cosa similar (o millor) a aquesta estratègia recursiva:

1. Si $a > r$, A proclama que hi ha $r + k$ monedes i guanyen el joc.
2. Si $a \leq r$, A passa i imagina que guanya una moneda. És a dir, ara a ha augmentat en una unitat.
3. Si arribem en aquest punt, això vol dir que A ha passat i, per tant, B sap que $a \leq r$. Aleshores, si $b < k$, es compleix $a + b < a + k \leq r + k$ i B proclama que hi ha r monedes i guanyen el joc.
4. Si $b \geq k$, B passa i imagina que perd una moneda. És a dir, ara b ha disminuït en una unitat.
5. Observem que la quantitat total de monedes $a + b$ no ha canviat. Tornem al pas 1.

Com en moltes altres situacions, una manera d'assegurar-nos d'haver entès un algorisme és programar-lo. A més, programant-lo podem fer una comprovació experimental que l'algorisme funciona. Per exemple, un petit codi python com aquest ens pot servir.

Podeu trobar a internet moltes petites variants d'aquest mateix enigma, però totes les que jo he trobat difereixen del plantejament anterior en una **hipòtesi crucial**: no es permet que l'Alícia i el Bernat pactin una estratègia abans de començar a jugar, sinó que pretenen que els dos jugadors arribin a resoldre l'enigma **per pura lògica**.[1] Això ens fa entrar en un món completament diferent que discutirem a fons en l'apartat següent. Abans, però, deixeu-me dir que si bé el plantejament que hem fet nosaltres abans és obvi i no ha de suscitar cap dubte, les *solucions per pura lògica* que trobareu a internet són, com a mínim, molt discutibles —n'hi ha prou amb llegir els comentaris que generen entre els lectors, plens d'escepticismes, de solucions alternatives, de dubtes i de manifestacions d'incredulitat.

2 El cas de les esposes infidels: no és el que sembla

Quan em van explicar el **principi d'inducció** —això era a començaments de la dècada dels setanta del segle passat— hi va haver un professor que, com a exemple curiós d'aquest principi matemàtic fonamental, ens va explicar

[1] Això és el que passa, per exemple, amb la comunicació subtil de Yá Tsun: que l'espia mataria una persona per comunicar el lloc que calia bombardejar no havia estat pactat d'antuvi, però quan els superiors de Yá Tsun van conèixer la notícia van deduir, *per pura lògica*, quin era el missatge que el seu espia els volia transmetre.

una història truculenta que involucrava un xeic tirànic, unes esposes infidels i unes decapitacions misterioses que, presumptament, eren conseqüència del principi d'inducció. Potser a algú de vosaltres, amables lectors, també us van explicar aquest *exemple* i encara el recordeu. Entre els meus companys d'aquells anys n'hi va haver alguns que es van mostrar molt escèptics amb la història mentre que un altre grup va dir que sí que l'entenia. Jo era d'aquest segon grup i van haver de passar cinquanta anys perquè m'adonés que estava equivocat: no l'havia entès gens ni mica.

Vaig tornar a pensar en aquella antiga història quan vaig començar a impartir un curs de *Fonaments de les Matemàtiques* a primer curs del Grau de Matemàtiques de la UAB[2] i això em va fer veure fins a quin punt és cert que *ensenyar* i *aprendre* són dos conceptes indestriables. Aquell curs de fonaments em va dur a entendre, més enllà d'aquella història de les dones infidels, tota una sèrie de conceptes que jo creia, equivocadament, que ja havia après feia molts anys. *Potser creure que saps allò que realment no saps és pitjor que ignorar.*

En aquest segon apartat de *Comunicacions subtils* discutirem la història de les esposes infidels. Com que el llenguatge original ja no és apropiat als temps actuals, utilitzaré una variant que, si bé no està exempta de sang i fetge, potser trobareu menys extemporània.

> *En una comunitat aïllada, algunes criatures neixen amb l'iris de color panotxa. Antigament, aquest fet es considerava de mal averany i la persona d'ulls panotxa era sacrificada. Això va canviar quan un savi de la comunitat va tenir la idea de respectar la tradició —tota persona que sàpiga amb seguretat que té els ulls panotxa ha de cometre suïcidi públic a l'alba de l'endemà de saber-ho— però —aquí rau la saviesa— també va decretar que parlar del color dels ulls era tabú. D'aquesta manera, com que ningú podia veure el color dels seus ulls i com que ningú podia parlar sobre el color dels ulls de ningú, els que tenien els ulls panotxa no van saber-ho mai i van viure en pau indefinidament...*
>
> *...fins que un foraster va visitar la comunitat i, just abans de marxar, desconeixedor del tabú que havia mantingut en pau aquella comunitat, va dir:* «m'ha sorprès trobar ulls de color panotxa»*. Quaranta dies després que el foraster digués això, a l'alba, tots els membres de la comunitat amb els ulls panotxa van cometre suïcidi públic. N'hi havia, exactament, quaranta.*[3]

Quina explicació té aquest comportament? A mi em van ensenyar que era

[2] Aquell curs va donar lloc al llibre *Matemàtiques: comenceu per aquí* que podeu trobar (en accés obert) a `https://ddd.uab.cat`.

[3] És clar que, per evitar solucions trivials, cal afegir hipòtesis com: no hi ha miralls, tothom es coneix, etc.

una conseqüència lògica el principi d'inducció. Si $k > 0$ designa el nombre d'individus amb els ulls panotxa, podríem raonar d'aquesta manera:

- Si $k = 1$, l'únic individu amb els ulls panotxa no veurà ningú amb els ull panotxa i, com que el foraster diu que hi ha algú amb els ulls panotxa, deduirà que és ell i cometrà suïcidi l'endemà.
- Suposem, per inducció, que el «teorema» és cert per $k-1$, és a dir, si hi ha exactament $k-1$ individus amb els ulls panotxa, tots ells cometran suïcidi després de $k-1$ dies. Aleshores, si hi ha k individus amb els ulls panotxa i després de $k-1$ dies ningú es suïcida, tots ells deduiran que n'hi ha, com a mínim, k. Com que cadascú d'ells en veu $k-1$, tots ells deduiran que ells mateixos tenen els ulls panotxa i se suïcidaran l'endemà, quan farà exactament k dies de l'observació del foraster.

Força convincent, oi? A mi aquest argument em va convèncer durant cinquanta anys, fins que em vaig plantejar aquestes preguntes:

- Si $k > 2$, el que diu el foraster ho sap tothom, perquè tothom veu algú amb els ulls panotxa. Aleshores, com és possible que donar una informació **que tothom coneix** posi en marxa una matança?
- Tothom veu, com a mínim, $k-1$ individus amb els ulls panotxa. Per tant, si el raonament anterior és correcte, tothom sap que no passarà res en els primers $k-2$ dies. Aleshores, quin sentit té esperar tots aquests dies, quan **tothom sap** que no passarà res?
- Finalment —i aquesta és la pregunta fonamental— per demostrar un teorema per inducció cal que tingui la forma

$$H \Longrightarrow \forall\, n\, P(n) \qquad\qquad (*)$$

  on H són les hipòtesis del teorema i $P(-)$ és un cert predicat sobre els nombres naturals. Quins són H i P, en aquest cas?

Quan, finalment, em vaig adonar que no era capaç de contestar les preguntes anteriors —principalment, l'última, que és la que ha de donar la clau de tot plegat— va ser quan vaig començar a aprendre coses noves i interessants, que són les que vull compartir amb vosaltres aquí.

No és matemàtiques: és lògica epistemològica

Quan intentem escriure el teorema $(*)$ en el llenguatge de la lògica proposicional ens adonem que cal utilitzar alguns predicats del tipus $K_a(x)$ amb el significat intuïtiu de *«a coneix x»*, i també $T(x) := \big(\forall a\, K_a(x)\big)$, que representarà *«tothom coneix x»*. Per poder prosseguir, veiem que cal postular alguns axiomes sobre aquests predicats: per exemple, podríem postular

$K_a(x) \Rightarrow x$ (que ens diu que estem axiomatitzant el coneixement veritable, no l'opinió) o $K_a(x) \Rightarrow K_a(K_a(x))$ (que descarta el cas de saber una cosa sense saber que la sabem). Observem que hi ha moltes axiomàtiques diverses per al *coneixement* i els teoremes que obtindrem en una axiomàtica o una altra seran diferents.

Arribats en aquest punt ja no estem treballant a la lògica de primer ordre pura i simple sinó en una *extensió* d'aquesta lògica que inclou com a mínim un nou predicat primitiu que formalitza el concepte de *coneixement*. Recordem que fonamentem la matemàtica en una extensió de la lògica de primer ordre amb un nou predicat designat pel símbol $\in$ que compleix uns certs axiomes (ZFC) i modelitza la idea de *pertinença*: d'aquesta extensió en diem *teoria de conjunts*. Anàlogament, de l'extensió de la lògica de primer ordre que vol formalitzar el coneixement se'n diu **lògica epistemològica**. En principi, doncs, el problema dels ulls panotxa l'hauríem de formalitzar en la lògica epistemològica i, per fer-ho, hauríem de fixar quins són els axiomes que postulem per als predicats $K_a(x)$.

Quan comencem a treballar amb els predicats $K_a(x)$ i $T(x)$ de seguida ens adonem que, per composició, obtenim una infinitat de predicats *essencialment diferents*. Per exemple,

$$T(x),\ T(T(x)),\ T(T(T(x))),\ \ldots, T^n(x), \ldots$$

i encara un altre més:

$$T^\infty(x) := \big(\forall n T^n(x)\big).$$

La distinció entre $T(x)$ (*tothom coneix x*) i $T^\infty(x)$ (*tothom coneix x i tothom coneix que tothom coneix x i tothom coneix que tothom coneix que tothom coneix x i* ...) és essencial i va ser posada en valor pel premi Nobel Robert J. Aumann en un article del 1976 de només quatre pàgines que va tenir una gran influència: *Agreeing to Disagree*.

Precisament, la història dels ulls panotxa ens proporciona un exemple magnífic de la distinció entre $T(x)$ i $T^\infty(x)$. Imaginem, per exemple, que $k = 2$, és a dir, només hi ha dos individus amb els ulls panotxa. Designem per a l'afirmació del foraster:

$$a := \textit{«hi ha algú amb els ulls panotxa»}.$$

Aleshores, $T(a)$ és cert —com havíem dit abans— però $T^2(a)$ no ho és: cadascun dels individus amb els ulls panotxa no pot saber si l'altre individu amb els ulls panotxa sap que hi ha algú amb els ulls panotxa. Amb aquesta formalització hem resolt ja els dos primers dels tres dubtes que se m'havien plantejat i que he explicat més amunt. El foraster sí que fa una aportació substancial: abans que ell parlés, $T(a)$ era cert però $T^k(a)$ no ho era, després que ell parlés, $T^\infty(a)$ va passar a ser cert.

En la terminologia d'Aumann, $T^\infty(x)$ s'expressa «x **és coneixement comú**».

La diferència profunda que hi ha entre allò que tothom sap i allò que és coneixement comú té una immensa transcendència a les Ciències Socials i, de fet, a la història de la humanitat, i és una distinció que convindria que fos més coneguda perquè explica molts fenòmens socials: els paper dels mitjans de comunicació, l'espurna que posa en marxa la revolució, etc. Imaginem una comunitat (un grup ètnic, una nacionalitat, una classe social, etc.) en la que tots els seus membres saben, per exemple, que estan discriminats, o estarien disposats a la revolta. En aquestes circumstàncies, un líder o un fet puntual que produís el pas d'allò que tothom sap a un coneixement comú podria provocar la revolta que tots voldrien fer. Efectivament: dir en públic allò que tothom sap i convertir-ho en coneixement comú pot produir moviments socials d'una magnitud insospitada. Hi ha infinits exemples a la història.[4]

La lògica epistemològica —que hem tocat tangencialment en aquest apartat— és fonamental a la teoria de jocs, a la informàtica, a l'economia (Aumann va guanyar el Premi Nobel d'Economia) i, no cal dir-ho, a l'epistemologia.

Ho podríem resoldre dins de les matemàtiques?

Tornem al problema inicial, el de la comunitat amb k individus amb els ulls panotxa. Ara que ja hem vist que al seu darrere hi ha ni més ni menys que la lògica epistemològica, ara que ja hem *desaprès* la «solució» estàndard, ens podem preguntar si podem trobar una solució rigorosa del problema *dins de les matemàtiques*. Va ser el mateix Aumann qui va donar una interpretació matemàtica de la lògica del coneixement comú i, basant-me en les seves idees, us proposo aquesta manera —força geomètrica, perquè així és com m'agrada pensar les matemàtiques— d'enfocar el problema:

- Centrem-nos d'entrada en el coneixement comú. Tot això ho és: (a) a la comunitat hi ha n individus; (b) cada individu pot tenir els ulls panotxa o no tenir-los-hi; (c) cada individu pot veure els ulls de tots els altres, però no els seus. Per tant, si designem per 1 tenir els ulls panotxa i per 0 no tenir-los-hi, l'*espai mostral* Ω —abans de l'arribada del foraster— s'identifica als enters de n bits és a dir, als vèrtex d'un **hipercub** de dimensió n, Q_n.

- Quan el foraster diu que $k > 0$, això esdevé coneixement comú i l'espai mostral canvia a $\Omega_0 \subsetneq \Omega$: l'hipercub ha perdut el vèrtex $(0, \ldots, 0)$.

[4] No cal anar gaire lluny ni en el temps ni en l'espai: en tenim prou amb pensar en el primer d'octubre de 2017 a Catalunya. Abans del primer d'octubre, tots sabíem que els independentistes érem molts; després del primer d'octubre, aquest fet va passar a ser *coneixement comú*. Les conseqüències —com tothom sap i és també coneixement comú— van ser terribles.

- L'espai mostral canvia cada dia perquè cada matinada es produeix un fet que és del domini públic: el suïcidi o el no suïcidi d'algun membre de la comunitat. Tindrem, doncs, una cadena d'espais mostrals

$$\Omega \supsetneq \Omega_0 \supsetneq \Omega_1 \supsetneq \Omega_2 \supsetneq \Omega_3 \supsetneq \cdots$$

- Cada individu de la comunitat dóna lloc a una partició de l'espai mostral: dos elements de l'espai mostral són equivalents per a l'individu i si (és coneixement comú que) aquest individu no té cap informació que li permeti creure que un és més probable que l'altre. Observem que les arestes de l'hipercub uneixen dos vèrtex que difereixen en una única coordenada. Si aquesta coordenada és la i-èssima, els dos vèrtex d'aquesta aresta seran una classe d'equivalència per a l'individu i. Tot això és coneixement comú.

- En conclusió: l'espai mostral Ω és un cub de dimensió n i cada aresta té assignat un valor $i \in \{1, \ldots, n\}$ que indica que per a l'individu i, els vèrtex de l'aresta són indistingibles. En el cas $n = 4$, el dibuix seria el de la figura 1, en el que cada individu s'ha representat per un color diferent: verd, vermell, groc i blau.

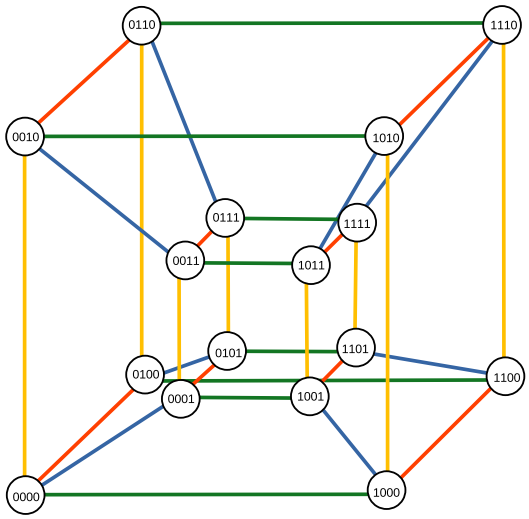


Figura 1: L'espai mostral inicial Ω per $n = 4$.

- Cal ara conèixer quins són els successius espais mostrals Ω_i. Si definim el *pes* d'un vèrtex com la suma de les seves coordenades i si k és el nombre d'individus amb ulls panotxa (és clar que k no és coneixement comú), es compleix

$$\Omega_r = \begin{cases} \{\text{tots els vèrtex de pes} > r\} \subseteq \Omega, & r < k \\ \{\text{un únic vèrtex de pes } k\} \subseteq \Omega, & r \geq k \end{cases}$$

Si això és cert, ja hem justificat els fets que es produeixen a la comunitat a rel del comentari del foraster. Per veure que la descripció dels espais mostrals Ω_i és correcta, observem que de les arestes que tenen l'etiqueta i n'hi ha exactament una que uneix els dos únics vèrtex compatibles amb el que l'individu i veu. D'aquesta aresta en direm l'*aresta fonamental* de i i, clarament, només la coneix l'individu i. En el moment que l'aresta fonamental perd un dels seus vèrtex —que serà el de pes mínim— l'individu i ja té la certesa que té els ulls panotxa i se suïcida l'endemà i, per tant, si no ho fa, és coneixement comú que l'aresta fonamental per a i encara conserva els seus dos vèrtex. Com que la situació és simètrica respecte de les permutacions dels individus amb ulls panotxa, si això passa per a un individu i, també passarà per a tots.

Els successius espais mostrals per $n = 4$, $k = 3$ estan representats en la figura 2, en la que hem suposat que els individus amb ulls panotxa són els k primers, és a dir, la situació real és la descrita pel vèrtex $(1110) \in \Omega$. Les quatre arestes fonamentals estan dibuixades amb traç més gruixut.

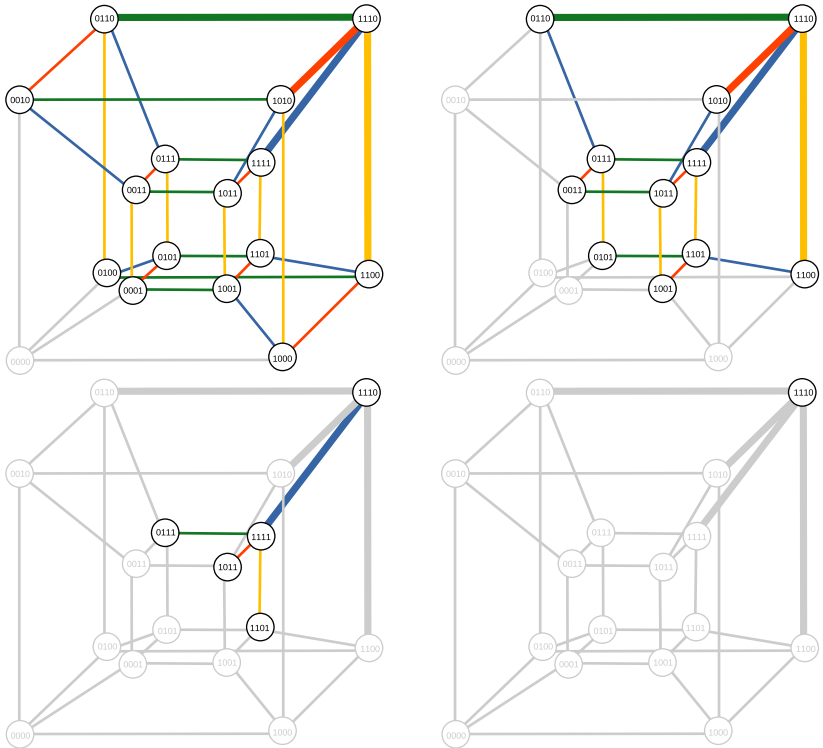


Figura 2: Ω_i per $i = 0, 1, 2, 3$, $n = 4$, $k = 3$.

3 En condicions aparentment impossibles

En aquest apartat estudiarem un curiós enigma —evidentment, també té a veure amb les *comunicacions subtils*— que es planteja com un repte on dos presoners han de trobar la clau per sortir de la presó, seguint unes estranyes regles. L'interès d'aquest enigma rau en aquests dos factors: d'una banda, és evident que la solució ha d'involucrar conceptes matemàtics, i de l'altra, l'existència d'una solució sembla impossible, talment com un truc de màgia. L'enigma és aquest:

> *Dos presoners (Alícia i Bernat) han de trobar la clau per escapar i coneixen les condicions del repte, de manera que poden haver preparat una estratègia. La clau estarà oculta en una casella d'un tauler d'escacs. En una primera fase, el carceller mostra —només a l'Alícia— el tauler i la casella on hi ha la clau. A continuació, sempre en presència només de l'Alícia, el carceller col·loca sobre cada casella del tauler una moneda que, de manera aleatòria o impredictible, mostra «cara» o «creu». Aleshores, l'Alícia ha de capgirar una* ***única*** *moneda, la que vulgui, i ha d'abandonar la sala. Entra en Bernat, veu el tauler amb les monedes i ha de dir on és la clau. Quina estratègia tenen els dos presoners per trobar la clau de manera infal·lible?*

Com és possible?

Aquest enigma sembla ben bé impossible i, per tant, el primer pas per a trobar la solució és modelitzar matemàticament el problema i adonar-se que *potser sí* que hi ha una solució.

En primer lloc, el tauler d'escacs no és cap peça fonamental del joc: podem imaginar simplement n caselles —en la formulació anterior $n = 64$— cadascuna amb una etiqueta *cara* o *creu*. És evident que l'única informació que l'Alícia pot transmetre a en Bernat és l'estat cara/creu de les n monedes sobre el tauler. Si prefixem un ordre de les caselles i denotem cara/creu per 0, 1, és clar que la informació que rep en Bernat és un nombre de n bits, és a dir, un enter K entre 0 i $2^n - 1$. A partir de K en Bernat ha de determinar a quina de les n caselles hi ha la clau. La solució és, doncs un nombre enter S entre 0 i $n - 1$ (denotem 0 la primera casella). Per tant, per resoldre l'enigma, els presoners s'han d'haver posat d'acord en una funció

$$F : \{0,1\}^n = (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow \{0, 1, \ldots, n-1\}$$

tal que $F(K) = S$.

El problema és que l'Alícia té un control molt limitat sobre el valor K que pot transmetre al seu company: l'Alícia només pot controlar un únic bit de K. La pregunta, doncs, és si una funció F d'aquestes característiques existeix.

L'exemple minimal

Observem que en l'exemple proposat n és una potència (parella) de 2. Potser aquesta condició jugarà —o no— algun paper en la resolució del problema? De tota manera, crec que la condició necessària —i gairebé suficient— per resoldre l'enigma, és a dir, trobar la funció F, és ser capaç de resoldre el mateix problema en un tauler 2×2, és a dir, quan $n = 4$.

Es tracta ara d'associar a cada nombre binari de 4 bits un nombre binari de 2 bits i aquí entra en escena un objecte geomètric que ja ens ha ajudat anteriorment: l'**hipercub** Q_4, que té per vèrtex precisament els 16 nombres binaris de 4 dígits. Ja sabem que dos vèrtex de Q_4 estan units per una aresta si i només si els nombres binaris que representen els dos vèrtex difereixen només en un únic bit.

Imaginem ara que som capaços de *pintar* cada vèrtex de Q_4 amb un color —vermell, blau, verd, groc— de manera que els 4 vèrtex contigus de cada vèrtex tinguin colors diferents. Si podem fer això, ja podem escapar de la presó. Vegem com. El carceller ha col·locat una moneda (que mostra cara o creu) sobre cadascuna de les 4 caselles. Aquestes monedes determinen unívocament un vèrtex de l'hipercub. Els dos presoners s'han posat d'acord en quina casella és vermell, quina és blau, quina és verd i quina és groc. Aleshores, l'Alícia capgira la moneda que fa que el vèrtex creat pel carceller es converteixi en un vèrtex del color de la casella que conté la clau. En Bernat mira quin color té el vèrtex que apareix al tauler i troba la clau.

Pintar els vèrtex de Q_4 de la manera requerida es pot fer amb relativa facilitat per *assaig-error*. Per exemple, com a la figura 3.

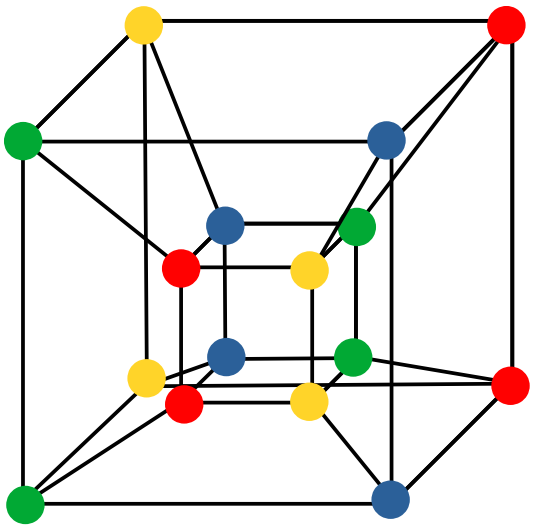


Figura 3: L'hipercub amb els vèrtex de colors que resol l'enigma sobre un tauler 2×2. Observem que cada vèrtex està unit amb vèrtex de tots els quatre colors.

Com que voldrem generalitzar les idees anteriors a un valor qualsevol de

n ens caldria tenir aquesta solució expressada d'una manera analítica. Els vèrtex de l'hipercub són

$$0000,\ 0001,\ 0010,\ \ldots,\ 1101,\ 1110,\ 1111$$

i els colors (les caselles del tauler) són

$$00, 01, 10, 11.$$

Aleshores, no costa gaire adonar-se que aquesta funció *lineal* ens resol el problema en el cas 2×2:

$$F : (\mathbb{Z}/2\mathbb{Z})^4 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2$$

$$(x_1, x_2, x_3, x_4) \mapsto (x_1 + x_4, x_2 + x_4)$$

En efecte. Suposem que el carceller ens ha deixat el tauler en la posició (x_1, x_2, x_3, x_4) que té el «color» $(x_1 + x_4, x_2 + x_4)$ i suposem que la clau es troba a la casella (y_1, y_2). Si $(x_1 + x_4, x_2 + x_4) = (y_1, y_2)$, capgirem la moneda de x_3; si $(x_1 + x_4, x_2 + x_4)$ i (y_1, y_2) difereixen només en el primer bit, capgirem la moneda de x_1; si només difereixen en el segon bit, capgirem la moneda de x_2 i si difereixen en tots dos bits, capgirem la moneda de x_4.

La solució general

A partir de les idees anteriors, podem resoldre el problema **quan n és una potència de 2**, $n = 2^k$, amb la funció:

$$F : (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow (\mathbb{Z}/2\mathbb{Z})^k$$

que definim de la manera següent.

- Considerem tots els subconjunts de $\{1, \ldots, k\}$ i els ordenem (de qualsevol manera), començant pel conjunt buit. N'hi ha $2^k = n$

  $$\varnothing = U_1, U_2, \ldots, U_n.$$

- Per cada $i = 1, \ldots, k$, considerem la funció lineal

  $$F_i := \sum_{i \in U_j} x_j.$$

  Observem que la variable x_1 no apareix a cap funció F_i.

- Definim la funció F com $F := (F_1, \ldots, F_k)$.

Aquesta funció que hem definit té la propietat essencial d'exhaustivitat que volem: per tot $(x_1, \ldots, x_n)$ i per tot $(\lambda_1, \ldots, \lambda_k)$, existeix r tal que

$$F(x_1, \ldots, x_r + 1, \ldots, x_n) = (\lambda_1, \ldots, \lambda_k).$$

És a dir, per cada nombre de n bits que ens proporcioni el carceller, alterant un únic bit podem obtenir qualsevol dels n «colors». Demostrem-ho: suposem que $F(x_1, \ldots, x_n) = (\mu_1, \ldots, \mu_k)$ i volem obtenir un cert color $(\lambda_1, \ldots, \lambda_k)$. Considerem el conjunt $\{j : \lambda_j \neq \mu_j\}$. Aquest conjunt coincidirà amb un cert U_r i l'índex r compleix el que volíem.

Ara que tenim la solució teòrica, què han de fer l'Alícia i en Bernat?

Pel que hem vist, encara que els dos presoners hagin sabut desenvolupar la teoria anterior, per dur-la a la pràctica han de fer uns càlculs que semblen força laboriosos. Anem a repassar-los.

1. Estem en el cas $n = 2^6$. Per tant, la funció F té sis components que cal calcular. Cada component F_i és una funció de 64 variables.

2. Un pas previ és numerar els 64 subconjunts de $\{1, \ldots, 6\}$ per poder determinar les funcions F_i.

3. L'Alícia ha de calcular el valor de F en la configuració i ha de determinar quina moneda cal capgirar perquè el valor de F passi a indicar el color (entre els 64 possibles) on es troba la clau.

4. En Bernat ha de calcular el valor de F sobre la configuració de monedes que veu i deduir en quina casella es troba la clau.

Tot això sembla massa complicat i ens podem preguntar si hi pot haver una estratègia més simple. Observem que l'elecció de l'ordenació dels subconjunts de $\{1, \ldots, k\}$ és arbitrària i, per tant, podem triar una ordenació que doni lloc a unes fórmules que siguin senzilles de recordar. La disposició de les caselles en forma de taulell d'escacs ara sí que ens pot ser útil. Per exemple, en el cas $n = 64$, que és el dels presoners, podem procedir d'aquesta manera:

- Numerem de 0 a 7 les files i columnes del tauler d'escacs començant per la cantonada superior esquerra i expressem el número assignat a cada casella com un nombre binari de 6 bits $n_5n_4n_3n_2n_1n_0$ on les tres primeres xifres indiquen la fila i les tres últimes indiquen la columna. Aquests 6 bits són senzills de calcular.
- Considerem ara aquesta matriu:

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

Observem:

- Mirant les 64 columnes de la matriu anterior veurem que hi apareixen efectivament tots els subconjunts de $\{1,2,3,4,5,6\}$. Per tant, aquesta matriu ens dóna una funció F com la que necessitem per resoldre el problema.
- La matriu anterior i la funció F que defineix són relativament senzilles de recordar i d'aplicar: F_1 és la suma (a $\mathbb{Z}/2\mathbb{Z}$) de les files 0, 2, 4, 6; F_2 és la suma de les files 1, 2, 5, 6; F_3 és la suma de les files 4, 5, 6, 7; F_4 és la suma de les columnes 0, 2, 4, 6; F_5 és la suma de les columnes 1, 2, 5, 6 i F_6 és la suma de les columnes 4, 5, 6, 7.

- Estudiem ara què ha de fer l'Alícia.
  - Ha d'aplicar la funció F a la configuració que ha creat el carceller i obtenir un nombre de 6 bits $n_5n_4n_3n_2n_1n_0$.
  - Mirant la fila i la columna de la casella on hi ha la clau, obté un altre nombre de 6 bits $m_5m_4m_3m_2m_1m_0$ que és el que ha de comunicar a en Bernat.
  - Ha de trobar l'únic canvi de moneda que converteix

    $$n_5n_4n_3n_2n_1n_0 \text{ en } m_5m_4m_3m_2m_1m_0.$$

    Aquest pas és més senzill del que sembla. Suposem, per exemple, que hem de passar de 101110 a 111011. Quina moneda hem de capgirar? Recordem que 101 vol dir que a les files 0, 2, 4, 6 hi ha un nombre senar de cares, a les files 1, 2, 5, 6 hi ha un nombre parell de cares i a les files 4, 5, 6, 7 hi ha un nombre senar de cares. Com que volem passar a 111, és clar que hem de capgirar una moneda de la fila 1. Pel mateix raonament, hem de capgirar una moneda de la columna 4. En conclusió, la moneda que cal capgirar és la de la fila 1, columna 4. Observem també que la casella de la fila 3, columna 3 és la que cal capgirar si no volem canviar el resultat.

- Finalment, en Bernat té una feina més senzilla: ha d'aplicar la funció F a la configuració que s'ha trobat i llegir el nombre de 6 bits

  $$m_5m_4m_3m_2m_1m_0$$

  que indica la fila i la columna on hi ha la clau per sortir de la presó.

Podem ajudar els presoners amb un programa en `sage` com aquest.

Zugzwang: què passa si n no és una potència de 2

Observeu que el fet que n sigui una potència de 2 juga un paper crucial en la solució que hem trobat, perquè ens permet utilitzar l'àlgebra lineal sobre el cos de dos elements $\mathbb{F}_2$. Això no és casual: si n no és una potència de 2, **el problema no té solució**, i això ho podem veure amb el raonament següent.

Una solució de l'enigma per un cert valor de n implica una coloració del cub de dimensió n amb n colors de manera que els n vèrtex que estan units a cada vèrtex tenen colors diferents. Suposem, doncs, que tenim aquesta coloració i comptem quants vèrtex hi ha de color, diguem, blau. Cada vèrtex té exactament un veí de color blau. Com que hi ha 2^n vèrtex, obtenim 2^n vèrtex de color blau. Però, evidentment, comptant-los així hem comptat cada vèrtex més d'una vegada. Quantes vegades? Cada vèrtex blau és veí de n vèrtex i, per tant, cada vèrtex blau l'hem comptat n vegades. En conclusió, el nombre de vèrtex blaus és $2^n/n$ que, per tant, ha de ser un nombre enter. Deduïm que n divideix 2^n i, per tant, n és una potència de 2.

D'altra banda, hi ha un detall en l'enunciat que, segons com s'interpreti, pot fer canviar la seva modelització matemàtica. Es tracta de l'**obligatorietat** que l'Alícia capgiri una moneda. Ens podem preguntar què succeeix si en l'enunciat inicial canviem la frase *«l'Alícia **ha** de capgirar una única moneda»* per *«l'Alícia **pot** capgirar una única moneda»*.

Evidentment, la solució que hem donat segueix sent vàlida si el presoner pot no tocar cap moneda. Però la demostració que l'enigma no té solució si n no és una potència de 2 deixa de ser vàlida en aquesta situació més laxa en la que no hi ha *Zugzwang*, és a dir, obligació de jugar, i això obre una nova pregunta: sense Zugzwang, podem resoldre l'enigma per a qualsevol valor de n? No tinc resposta per aquesta pregunta.

4 El coneixement zero

Galileu, Kepler i *mater amorum*

L'onze de desembre de 1610, Galileu va escriure una carta[5] a l'ambaixador toscà a Praga explicant-li que havia fet una descoberta que podia ser decisiva per a la confirmació de la teoria copernicana. Efectivament, Galileu havia començat a observar les fases de Venus —incompatibles amb la teoria geocèntrica— i sabia molt bé que, amb la proliferació de nous i millors telescopis, qualsevol que apuntés a Venus un d'aquests instruments veuria el mateix que estava veient ell. D'una banda, es volia assegurar la primacia del descobriment i, d'una altra, volia esperar uns dies per estar segur de poder afirmar que Venus tenia fases, com la lluna. La manera d'aconseguir aquests

[5] Vegeu S. Drake, *Galileo, Kepler, and Phases of Venus*, J. Hist. Astr. 15(3), 1984, 198–208.

dos objectius va consistir en fer que arribés a Kepler —a través de l'ambaixador a Praga— una frase xifrada que contingués el descobriment, però que fos pràcticament impossible de llegir. Aleshores, la carta de Galileu comença amb aquest anagrama

Haec immatura a me iam frustra leguntur o y

que, si descartem les dues lletres finals *«o y»*, ve a dir alguna cosa com ara *aquestes, de manera prematura per a mi, ara han estat llegides en va.* Però el que signifiqui aquesta frase no té cap importància —més enllà d'intentar despistar Kepler, com realment va aconseguir de fer— perquè el descobriment secret de Galileu s'ha d'escriure amb les mateixes lletres de la frase anterior, convenientment reordenades. Kepler no va saber resoldre l'enigma i el 9 de gener de 1611 va enviar a Galileu vuit possibles solucions, cap de les quals feia referència a Venus, però el cap d'any de 1611 Galileu ja havia fet pública la solució:

Cynthiae figuras aemulatur mater amorum

que, si identifiquem, com és lògic, *mater amorum* amb el planeta Venus, i *Cynthia* amb la Lluna —perquè, de vegades, la deessa Selene també s'anomenava Cynthia— veurem que Galileu afirma que *Venus emula les figures de la Lluna*, és a dir, Galileu havia descobert que Venus també té fases i, en conseqüència, la teoria ptolemaica ha de ser falsa.

Aquesta història, que quan la vaig llegir fa molts anys em va semblar curiosa però intranscendent, pròpia de temps remots i ja superats, ens duu a pensar en un tema d'una rellevància actual ben gran: com podem demostrar que posseïm una informació sense revelar aquesta informació? El corpus teòric que hi ha al voltant d'aquesta pregunta es coneix com la *teoria del coneixement zero* i, com el cas dels ulls panotxa que hem discutit abans, forma part de l'*epistemologia matemàtica*, una branca importantíssima de la ciència de la computació. Aquesta teoria (o tecnologia) del coneixement zero és crucial a la criptografia, a la tecnologia *blockchain*, a la teoria de jocs i a altres branques de plena vigència, però també interessa als filòsofs. En aquest darrer apartat parlarem —de manera força superficial, com escau al to general de l'article— del *coneixement zero*.

La Paula, en Vicenç, l'Helena i la TCZ

Imaginem tres agents que ara —a diferència de les situacions anteriors quan els protagonistes eren l'Alícia i en Bernat— anomenarem *Paula, Vicenç* i *Helena*. La Paula posseeix una informació que només coneix ella i ha de **p**rovar a en Vicenç que la posseeix, sense revelar-la-hi. En Vicenç ha de **v**alidar que la Paula posseeix la informació, sense obtenir, en el procés, cap altre coneixement. També ens hem d'assegurar que per a l'Helena sigui impossible ***h**ackejar* el procés i suplantar la Paula.

Amb un exemple d'una situació concreta habitual quedarà més clar quin és l'objectiu central de la teoria del coneixement zero (TCZ). Quan volem accedir a un cert servei en línia ens hem d'identificar amb una contrasenya. Aleshores, el servei al qual accedim ha de validar aquesta contrasenya comparant-la amb la contrasenya nostra que té desada al seu servidor. En aquest procés —sense TCZ— hi ha un problema evident: el servei ha de conèixer la nostra contrasenya i, voluntària o involuntàriament, la contrasenya podria arribar a mans d'un hacker. La TCZ vol evitar aquest problema i aconseguir que ens puguem identificar en un servei sense que el servei conegui la nostra contrasenya.

Hi ha, encara, un altre requeriment subtil per a una bona TCZ. Hem dit que en Vicenç no ha de guanyar cap mena d'informació —cap!— en el procés. Expliquem-ho amb aquest exemple. La Paula és una gran alquimista i ha trobat la pedra filosofal, és a dir, pot convertir l'or en plom i el plom en or. En Vicenç és un altre alquimista, envejós de la Paula. La Paula vol demostrar a en Vicenç que pot transmutar els metalls però, evidentment, no vol revelar el secret. Però la Paula tampoc es refia del tot d'en Vicenç perquè tem que quan sàpiga que la Paula té la pedra filosofal la pugui denunciar per bruixeria a la Inquisició. Un mètode amb TCZ ha de fer que tots aquests requeriments siguin possibles: la Paula ha de poder demostrar a en Vicenç que pot transmutar els metalls, en Vicenç no ha de saber com s'ho fa la Paula i si en Vicenç denuncia la Paula, ho haurà de fer només per la seva paraula, sense poder aportar cap prova irrefutable.[6]

Dos exemples de TCZ

Hi ha força exemples de TCZ aliens a les matemàtiques —si és que hi ha res que pugui ser aliè a les matemàtiques. El més elemental és el que s'anomena *On és Wally?* i és tan simple com això: la Paula vol mostrar a en Vicenç que ha trobat en Wally, però no vol revelar on és; aleshores, la Paula amaga el llibre al darrere d'un gran full de paper amb un únic petit forat pel qual es veu en Wally. Oi que és enginyós? Un altre exemple molt bo —perquè recull totes les subtileses de la TCZ que hem esmentat abans— és el que es coneix com *La cova d'Alí Babà* i està molt ben explicat a la Wikipedia. En aquest apartat discutiré dos exemples que sí que tenen un component matemàtic interessant i poden tractar-se en un curs de fonaments de les matemàtiques.

En el **primer exemple**, la informació secreta que posseeix la Paula és una **permutació** de n elements, és a dir, un element σ del *grup simètric* Σ_n, i del que es tracta és que la Paula pugui convèncer en Vicenç que realment coneix σ sense donar cap informació sobre σ i sense que l'Helena pugui ferho. Sembla impossible però veurem que hi ha una interessant TCZ que fa que sigui possible.

[6] És clar que aquest exemple és pura fantasia: tots sabem que no calia pas aportar cap prova per condemnar una dona per bruixeria.

En primer lloc, la Paula tria un **graf** G_0 qualsevol i calcula el graf $G_1 := \sigma G_0$, és a dir, el graf que s'obté a partir del graf inicial permutant els seus vèrtex segons σ. A continuació, la Paula fa públics els dos grafs G_0 i G_1 que, per exemple, podem imaginar que són els dos grafs de la figura 4.[7]

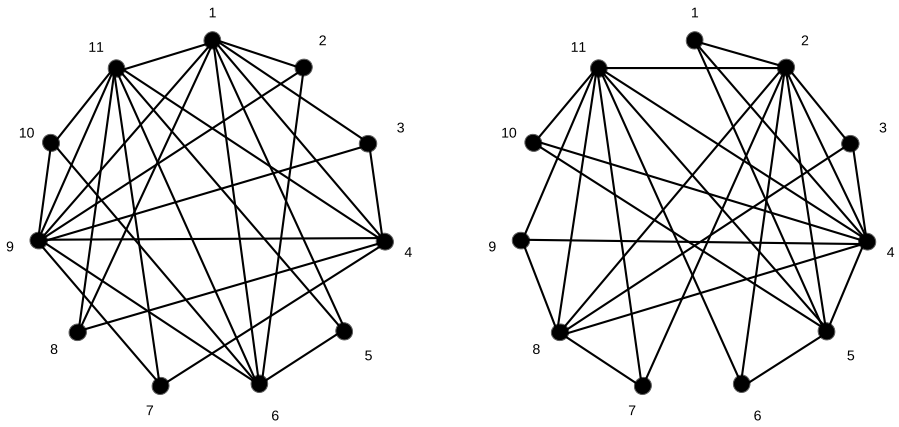


Figura 4: Dos grafs isomorfs G_0 i G_1.

Podríem pensar que si la Paula fa públics els dos grafs ja està desvelant el seu secret σ i, de fet, amb grafs tan senzills com els de la figura 4, és trivial trobar una permutació σ que transformi el primer graf en el segon.[8] A la pràctica, és cert que disposem d'algorismes molt eficients per trobar, donats dos grafs equivalents, una permutació que transformi un en l'altre però, de fet, el problema general sembla que no es pot resoldre en temps polinòmic i suposarem, doncs, que la Paula ha triat un graf molt gran i molt complex per al qual el que es coneix com el *problema de l'isomorfisme per a grafs* és pràcticament irresoluble. En conclusió, en Vicenç —i l'Helena!— coneixen els grafs G_0 i G_1, però això no els dóna cap informació sobre qui és σ.

En aquesta situació, un mètode de coneixement zero podria ser aquest:

1. La Paula tria un element qualsevol $\sigma_1 \in \Sigma_n$ i tria a l'atzar un dels dos grafs G_i amb $i \in \{0, 1\}$. Tot això ho fa en secret. Suposem que tria el graf G_0. Aleshores, envia a en Vicenç el graf $G_2 := \sigma_1 G_0$.

2. Quan en Vicenç rep el graf G_2, llança una moneda i:

   - si surt cara, demana a la Paula una permutació σ_2 tal que $\sigma_2 G_2 = G_0$;

[7] Els grafs de la figura 4 són el graf de Goldner–Harary (el seu grup d'automorfismes és el dièdric D_6) però això ara no té cap importància per al que estem explicant.

[8] La permutació σ no és única perquè la podem multiplicar per la dreta per un automorfisme del graf G_0. Per tant, si volem ser estrictes, el *secret* de la Paula no és una permutació, sinó una classe lateral de permutacions mòdul els automorfismes de G_0.

- si surt creu, demana a la Paula una permutació σ_3 tal que $\sigma_3 G_2 = G_1$.

3. La Paula respon a la demanda d'en Vicenç. Com que la Paula coneix els valors de i, σ i σ_1, és molt fàcil comprovar que la Paula pot calcular immediatament σ_2 i σ_3.

Si l'Helena intentés suplantar la Paula, què passaria? Ara, l'Helena coneix G_1, i, σ_1 i G_2.

- Si la moneda d'en Vicenç mostra cara, l'Helena pot contestar correctament $\sigma_2 = \sigma_1^{-1}$.

- Si la moneda d'en Vicenç mostra creu, l'Helena no pot contestar i queda en evidència.

Observem, doncs, que la Paula *passa el test* amb probabilitat 1 mentre que l'Helena el pot passar només amb probabilitat $1/2$. És clar que no tenim un test concloent però també és clar que si fem el test un cert nombre de vegades K, la probabilitat que l'Helena aconsegueixi suplantar la Paula és $2^{-K} \to 0$.

Manca encara un últim detall: podria en Vicenç demostrar que la Paula posseeix el valor de σ? La resposta és no perquè l'Helena també passaria el test pactant amb en Vicenç el resultat cara/creu. És a dir, el test és trivialment falsificable i només té capacitat probatòria per a en Vicenç, perquè només ell pot estar segur que cada vegada ha llançat realment una moneda.

Acabem amb un **segon exemple** en el que veurem com els mateixos fonaments de la **criptografia RSA**[9] —la funció φ d'Euler, el petit teorema de Fermat i l'algorisme d'Euclides— ens permeten validar una contrasenya amb *coneixement zero*. Veurem que l'esquema del procés és el mateix de l'exemple anterior, canviant *isomorfisme entre grafs* per *exponencial modular*. Suposem, doncs, que la Paula es vol registrar a un servidor que anomenarem *Ferrissa* (i farà el paper d'en Vicenç). Procedeixen d'aquesta manera:

- Quan la Paula es registra per primera vegada a Ferrissa:
  - La Paula envia a Ferrissa un nombre primer molt gran p i un element $g \neq 0$ del cos finit de p elements $\mathbb{F}_p$ d'ordre molt gran.
  - La Paula tria una contrasenya x (un nombre natural molt gran) i la manté en secret.
  - La Paula envia a Ferrissa el valor $y := g^x \in \mathbb{F}_p$.

[9] Penso que el funcionament bàsic de la criptografia RSA hauria de formar part de l'ensenyament de les matemàtiques generalistes. Aquesta creença la vaig dur a la pràctica en el llibre *Matemàtiques: comenceu per aquí* que he esmentat abans i en les meves classes a primer curs del grau de matemàtiques.

- Cada vegada que la Paula es vol registrar a Ferrissa:
  - La Paula tria un $r \in [0, p-2]$ a l'atzar, calcula $c := g^r \mod p$ i envia c a Ferrissa.
  - Ferrissa decideix aleatòriament entre aquestes dues accions:
    1. Demanar a la Paula el valor de r i comprovar que $c = g^r \mod p$.
    2. Demanar a la Paula el valor $u := x + r \mod (p-1)$ i comprovar que $cy = g^u \mod p$.
  - Es repeteix el procés anterior un cert nombre de vegades, i si la Paula sempre respon correctament, Ferrissa considera que, amb una probabilitat ≈ 1, la Paula posseeix realment la paraula de pas x.

L'explicació de la validesa del test anterior és senzilla. En primer lloc observem que el test és correcte perquè $cy = g^r g^x = g^u \mod p$. Observem també que ja sabem que si p és un primer prou gran, a partir de g^x no podem, a la pràctica, calcular x. També és clar que la Paula, com que coneix x, passa el test sempre, mentre que una persona que no conegui x només pot passar el test amb probabilitat $1/2$ i, per tant, passar el test n vegades sense conèixer x té una probabilitat $2^{-n} \approx 0$. El més interessant és comprovar la tercera condició de TCZ: Ferrissa no pot donar evidència que la Paula té realment la paraula de pas associada als valors y i g perquè Ferrissa podria presentar tota una transcripció d'un suposat test fet a la Paula que fos falsa. Com? Igual que passava en l'exemple del graf, si Ferrissa comparteix amb l'Helena les tries 1 o 2 que farà en cada moment, l'Helena passarà el test cada vegada, sense necessitat de conèixer la contrasenya x: si Ferrissa pensa demanar r, l'Helena envia a Ferrissa el valor de r i passa el test; si Ferrissa pensa demanar $x+r$, l'Helena calcula $c' := g^r y^{-1}$, envia c' (com si es tractés de c) i envia r, amb la qual cosa també passa el test.

* * * *

Ho deixem aquí. Hem vist diverses situacions curioses en les que que hem pogut comunicar una informació en condicions aparentment impossibles i hem vist com, en cada cas, hi havia, al darrere dels algorismes concrets, estructures matemàtiques importants. D'això es tractava.

Catedràtic de Topologia jubilat a la
Universitat Autònoma de Barcelona.
Jaume.Aguade@uab.cat

Publicat el 21 de gener de 2025