P vs. NP
(i el 10è problema de Hilbert)

Albert Atserias
atserias@lsi.upc.edu

22 de juny de 2005

1 Introducció

L'any 1900, David Hilbert proposà vint-i-tres problemes no resolts de les matemàtiques del moment com a grans reptes per al segle XX. A dia d'avui, alguns d'aquests problemes es consideren resolts satisfactòriament i d'altres es mantenen sense solució o, com se sol dir, "oberts". D'entre els problemes resolts, però, en trobem un amb una solució molt singular i sorprenent que volem destacar. La formulació original del problema és la següent [3]:

> *Determinar un procés mitjançant el qual es pugui establir, en un nombre finit d'operacions, si una equació diofàntica amb una quantitat arbitrària d'indeterminades i coeficients enters té solució en els enters.*

Aquest enunciat es coneix com el 10è problema de Hilbert. La solució final va ser trobada l'any 1970 per un jove matemàtic rus, de nom Matijasevich, culminant el treball dels seus predecessor americans Davis, Putnam i Robinson (vegeu [4]). En poques paraules, la solució al 10è problema de Hilbert és la següent:

No n'hi ha cap, de procés.

I això és una solució satisfactòria? El cert és que, amb els matisos necessaris per fer que tant la pregunta com la resposta siguin enunciats pròpiament matemàtics, ho és. A més, és probable que el propi Hilbert l'hagués considerada

satisfactòria. I no tant perquè Hilbert intuís per on anava la resposta, sinó més aviat al contrari, perquè ni el propi Hilbert podia imaginar-se que la solució requeriria el descobriment d'un fructífer nou camp de la matemàtica: la teoria de la computabilitat.

Però, què té a veure el 10è problema de Hilbert amb la qüestió P vs. NP i els problemes del mil·leni? Per esbrinar-ho, us convidem a llegir la transcripció d'una hipotètica conversa entre un metòdic matemàtic d'inicis del segle XX, de nom **V**, i una brillant matemàtica de finals del segle XX, de nom **P**. En **V** tot just acaba d'aterrar a l'any 1983 venint directament de l'any 1938, per alguna extranya drecera de l'espai-temps, i ha sentit dir que un tal Yuri Matijasevich va demostrar l'any 1970 que el 10è problema de Hilbert no té solució.

2 Primer contacte

V: Què vol dir que no n'hi ha cap, de procés? No ho entenc Dra. **P**. Això no sembla que es pugui establir matemàticament sense definir prèviament què vol dir el terme "procés" del propi enunciat del 10è problema de Hilbert.

P: Evidentment Dr. **V**; té tota la raó. Qualsevol pregunta matemàtica requereix que els conceptes involucrats estiguin definits amb el rigor propi de la nostra ciència. En el cas del 10è problema de Hilbert, un "procés" s'interpreta simplement com un procediment efectiu, o computable, en el sentit de Gödel, Turing o Church.

V: Conec molt bé el concepte de funció computable i no entenc com el problema de les equacions diofàntiques s'hi pot encabir. Les funcions computables són funcions de $\mathbf{N} \to \mathbf{N}$ i per tant prenen simples nombres naturals com arguments i retornen simples nombres naturals com a resposta.

P: Bé doncs també deu saber, per tant, que qualsevol seqüència de nombres naturals es pot representar unívocament per un únic nombre natural, oi? Per exemple, la seqüència de nombres naturals $4, 5, 4, 3$ es pot representar unívocament pel nombre natural $2^4 \cdot 3^5 \cdot 5^4 \cdot 7^3$ que s'obté d'elevar els 4 primers nombres primers 2, 3, 5 i 7 a les potències indicades per la seqüència.

V: Sí, és clar. Això es pot fer gràcies al Teorema Fonamental de l'Aritmètica segons el qual qualsevol nombre natural admet una única representació com a producte de nombres primers. Aquest truc ja el va fer servir Gödel. On vol anar a parar amb això?

P: Doncs fixi's bé: una equació diofàntica amb incògnites $X_1, \ldots, X_n$ i coeficients enters no és més que una expressió de la forma

$$\sum_{i=1}^{r} \alpha_{0,i} \prod_{k=1}^{n} X_k^{\alpha_{k,i}} = \sum_{i=r+1}^{s} \alpha_{0,i} \prod_{k=1}^{n} X_k^{\alpha_{k,i}}$$

on cada $\alpha_{k,i}$ és un nombre natural.

V: Això és pràcticament la definició.

P: Això mateix. Per tant, una equació diofàntica es pot representar mitjançant la seqüència de nombre naturals següent:

$$n, r, s, \alpha_{0,1}, \ldots, \alpha_{n,1}, \ldots, \alpha_{0,s}, \ldots, \alpha_{n,s}.$$

Per exemple, la famosa equació diofàntica $X^4 + Y^4 - Z^2 = 0$ es pot escriure de manera equivalent així

$$1 \cdot X^4 Y^0 Z^0 + 1 \cdot X^0 Y^4 Z^0 = 1 \cdot X^0 Y^0 X^2,$$

i per tant es pot representar mitjançant la seqüència

$$3, 2, 3, 1, 4, 0, 0, 1, 0, 4, 0, 1, 0, 0, 2,$$

que al seu torn es pot codificar com el nombre $2^3 \cdot 3^2 \cdot 5^3 \cdot 7^1 \cdot 11^4 \cdot 13^0 \cdot 17^0 \cdot 19^1 \cdot 23^0 \cdot 29^4 \cdot 31^0 \cdot 37^1 \cdot 41^0 \cdot 43^0 \cdot 47^2$.

V: Ja ho entenc. Així doncs, la questió del 10è problema de Hilbert consisteix en determinar la computabilitat de la funció $H_{10} : \mathbf{N} \to \mathbf{N}$ on: si x és un nombre natural tal que la seva factorització única en nombres primers representa una seqüència de nombres naturals que representa una equació diofàntica amb solucions en els enters, aleshores $H_{10}(x) = 1$ i altrament $H_{10}(x) = 0$. És això?

P: Sí, és això. I en Matijasevich, seguint la drecera marcada per Davis, Putnam i Robinson, va aconseguir demostrar que H_{10} de fet *no és* computable. Per tant, si entenem que el "procés" que demanava Hilbert es formalitza

mitjançant el concepte de funció computable que coneixem, la solució al 10è problema de Hilbert és precisament que no n'hi ha cap; com deiem abans.

V: Què curiós. No em puc imaginar de cap de les maneres com s'ho va fer en Matijasevich per aconseguir demostrar això.

P: Si ho vol, Dr. **V**, el convido a venir demà i l'hi explico una mica per sobre com ho va fer. A més, fer-ho em permetrà introduir-lo a un dels problemes oberts més interessants per al proper segle: P vs. NP.

V: Vindré encantat. Curiosament, aquest matí he sentit una conversa entre dos estudiants que parlaven d'un tal "problema P vs. NP". Diu que té relació amb el 10è de Hilbert? Demà m'ho explica.

3 Solució al 10è problema de Hilbert

P: Bon dia Dr. **V**. Va trobar el camí fins a la residència d'investigadors ahir a la nit?

V: No podríem dir que el vaig trobar de seguida. Però l'ambient que s'hi respira pels voltants és d'allò més interessant i no em va faltar distracció...

P: Si li sembla, tornem al 10è problema de Hilbert i li explico què té a veure amb el meu camp d'expertesa. Oi que em va dir que coneix el concepte de funció computable? Recordem-lo, de totes maneres.

La Dra. **P** *s'aixeca del seu seient, s'acosta a la pissarra del seu despatx, agafa un tros de guix, i es posa a dibuixar l'esquema de la Figura 1.*

Faré servir la definició de Turing, que al cap i a la fi és equivalent a les altres. En Turing es va inventar un model de màquina, avui dia anomenada màquina de Turing, i és precisament això que veu en aquest esquema: tenim un conjunt finit d'*estats* $Q = \{q_0, q_1, \cdots\}$, i un *estat actual*, en el dibuix q_3. Tenim una *cinta* dividida en infinites *cel·les*, on cada cel·la pot contenir 0, 1 o $\sqcup$ (espai en blanc). I tenim un *capçal* que permet modificar el contingut d'una cel·la, i que es pot desplaçar una posició a l'esquerra o a la dreta en funció de l'estat actual i del símbol que conté la cel·la del capçal. És així com coneix vostè el model de màquina que va proposar Turing?

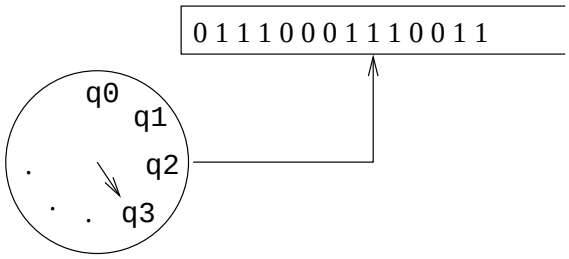

Figura 1: esquema d'una màquina de Turing.

V: Potser amb una nomenclatura diferent, però sí. Aquesta és la mateixa definició que conec jo. Jo tinc per costum especificar una màquina d'aquestes com una 5-tupla $M = (Q, q_0, q_+, q_-, \delta)$, on Q és el conjunt finit d'estats, q_0, q_+ i q_- són estats especials anomenats estat inicial, estat acceptador i estat rebutjador, respectivament, i δ és la funció de transició

$$\delta : Q \times \{0, 1, \sqcup\} \to Q \times \{0, 1, \sqcup\} \times \{-1, +1\},$$

on $\delta(q, a) = (q', a', m)$ indica que "si l'estat actual és q i el símbol del capçal és a, aleshores el següent estat és q', el símbol de sota el capçal es substitueix per a', i el capçal es mou a l'esquerra o a la dreta segons si $m = -1$ o $m = +1$ respectivament."

P: Perfecte. Així doncs tenim la mateixa definició en ment. Direm doncs que una funció $f : \mathbf{N} \to \mathbf{N}$ és *computable* si existeix una màquina de Turing M que, iniciada amb la representació binària d'un nombre natural x continguda a la cinta, i iniciada a l'estat inicial q_0, arriba a l'estat q_+, i quan ho fa, el contingut de la cinta és precisament la representació binària de $f(x)$.

V: Representació binària? Què vol dir amb això?

P: Sí home, representació binària vol dir representació en base 2. Per exemple el setè nombre primer en representació binària és 10001, i en representació decimal és 17.

V: I perquè es complica tant la vida? N'hi ha prou a iniciar el còmput amb x zeros consecutius continguts a la cinta i exigir que el còmput acabi amb $f(x)$ zeros consecutius continguts a la cinta. No és més senzill?

P: M'oblidava que vostè acaba d'arribar de l'any 1938. No li falta raó quan argumenta que x zeros consecutius són una representació tan vàlida

de x com la seva representació binària. De fet, si ho pensa un moment, veurà que x zeros consecutius són la representació *unària* de x. El problema és la longitud de la representació: fixi's bé que la representació unària de x requereix x símbols, mentre que la representació binària de x només en requereix $\lceil \log_2(x+1) \rceil$.

V: I quina importància té això? La representació decimal de x només en requereix $\lceil \log_{10}(x+1) \rceil$ que és un nombre encara més petit de símbols. Encara no veig quin és el problema amb la representació "unària", com diu vostè.

P: El problema és que la representació unària no és *eficient* tenint en compte que disposem de dos símbols 0 i 1. Evidentment, la representació decimal seria encara més eficient, però això requeriria tenir deu símbols per la cinta de la nostra màquina de Turing, i el resultat ve a ser el mateix.

V: Però, al cap i a la fi, disposar de dos símbols, en comptes d'un o deu, és només una decisió arbitrària que ha près vostè, no?

P: Entenc que vol dir. Potser hauria d'haver començat per aquí. Resulta que les realitzacions físiques de la màquina de Turing que s'han dissenyat fins al moment només són tecnològicament viables (o útils) si es disposa d'un nombre de símbols b petit però $b > 1$. Si el nombre de símbols fos massa gran, seria un maldecap tecnològic realitzar físicament la funció de transició; i si només hi hagués un símbol possible, la cinta necessària per representar nombres astronòmicament grans com ara 10^{50} hauria de ser tan gran que la realització física seria impossible. I posats que el nombre de símbols sigui petit, s'escull $b = 2$ perquè la diferència entre les longituds de les representacions en base 2 o qualsevol altre base fixada més gran que 1 és només d'una constant multiplicativa independent de x. Però també hi ha una raó més pràctica; dos símbols es poden representar mitjançant dos estats físics elementals: "on/off", o encès/apagat.

V: Bé, bé; tant és. Al cap i a la fi només és una qüestió de convenció sobre com es representen els nombres naturals. Els humans fa molts anys que fem servir la base 10 i vostè em vol convèncer que al final del segle XX la tecnologia ens farà canviar a base 2. Tant és. Hi ha un noi al MIT que també està capficat amb la base binària. Acaba d'escriure la seva tesi de màster. Com es diu... Claude Shannon, crec.

P: Sí, és clar, en Shannon; conec la seva feina. Vull que entengui, però, que a part d'una convenció, la representació en base unària és *exponencialment* més llarga i per tant ineficient si es disposa al menys de dos símbols.

Aclarit aquest punt, tornem doncs a les funcions computables i el 10è problema de Hilbert. La clau de tot plegat va ser adonar-se que el conjunt de solucions d'una equació diofàntica permet codificar molta informació. Per exemple, l'equació diofàntica $X - Y^2 = 0$ té solució si i només si X és un quadrat perfecte. De la mateixa manera, l'equació diofàntica $X_1 \cdot Y_1 + X_2 \cdot Y_2 - 1 = 0$ té solució si i només si X_1 i X_2 són nombres relativament primers.

En general, Davis, Putnam i Robinson van demostrar, amb molt d'enginy i esforç, que si f és una funció computable qualsevol, aleshores existeix un polinomi exponencial $p_f(X_1, X_2, Y_1, \ldots, Y_m)$ amb coeficients enters tal que l'equació diofàntica exponencial $p_f(X_1, X_2, Y_1, \ldots, Y_m) = 0$ té solució si i només si $f(X_1) = X_2$.

V: M'imagino que un polinomi exponencial és com un polinomi normal on a més tenim dret a incloure factors del tipus 2^X o X^Y, on X i Y són incògnites. Però no estavem parlant d'equacions diofàntiques normals i corrents? A què vé això d'equacions diofàntiques exponencials?

P: Si té raó; ara hi tornem. Però fixi's que el resultat de Davis, Putnam i Robinson és suficient per concloure que un problema semblant al 10è de Hilbert no té solució.

V: Evidentment, podem concloure que no hi ha cap procés computable per determinar si una equació diofàntica exponencial té solució. Si n'hi hagués, llavors per cada funció computable f hi hauria un procés computable per determinar si $f(x) = 1$ per cada x donat. Però això sabem que no és possible com va demostrar el propi Turing amb la seva funció universal. Potser sí que és veritat que això s'acosta a una solució al 10è problema de Hilbert, però no crec que els grecs consideressin equacions diofàntiques exponencials... Li agraïria que tornéssim a les equacions diofàntiques *sense* exponencials.

P: D'acord, d'acord, una mica de paciència. Fixi's que si es pogués trobar un polinomi $p_{\exp}(X_1, X_2, X_3, Y_1, \ldots, Y_r)$ de coeficients enters tal que l'equació diofàntica $p_{\exp}(X_1, X_2, X_3, Y_1, \ldots, Y_r) = 0$ té solució si i només si $X_1^{X_2} = X_3$, aleshores podríem eliminar tots els exponencials de qualsevol equació diofàntica exponencial $q(Z_1, \ldots, Z_m) = 0$. Pensi-hi un moment.

V: Vejam... El que podem fer és substituir un factor de q que tingui la forma $Z_i^{Z_j}$ per una nova incògnita, digue'm-ne $Z_{i,j}$, i obtenir d'aquesta manera un polinomi exponencial $q'(Z_1, \ldots, Z_m, Z_{i,j})$ amb una exponencial menys. Llavors, l'equació $q(Z_1, \ldots, Z_m) = 0$ té solució si i només si l'equació

$$(q'(Z_1, \ldots, Z_m, Z_{i,j}))^2 + (p_{\exp}(Z_i, Z_j, Z_{i,j}, Y_1, \ldots, Y_r))^2 = 0$$

té solució. Interessant...

P: D'això se'n diu reduir el problema de les equacions diofàntiques exponencials al problema de les equacions diofàntiques normals. Doncs aquí és on apareix Matijasevich. Ell va ser qui va construïr el polinomi $p_{\exp}$ i en va demostrar la propietat necessària. La demostració va requerir força teoria de nombres.

V: Molt impressionant...

P: Demà m'agradaria explicar-li què és això del problema P vs. NP i què té a veure amb el 10è problema de Hilbert. Ara em veig obligada a deixar-lo per atendre qüestions administratives del departament.

4 El problema P vs. NP: explicació informal

P: Bon dia Dr. **V**. Permeti'm que comenci amb un petit joc. Suposem que el vull convèncer que l'equació diofàntica

$$3 \cdot X^2 \cdot Y \cdot Z^2 - 3 \cdot Z^2 \cdot Y^2 - X^4 - 20 = 0$$

té solució. Què hauria de fer?

V: Bé doncs... doni'm una solució per tal que la verifiqui i m'ho creuré.

P: Exacte. En aquest cas la meva prova que l'equació té solució és $X = 2$, $Y = 3$, $Z = 2$. Per la seva part, per comprovar-ho només haurà de fer unes quantes operacions aritmètiques. Ja ho ha comprovat? Suposem ara, però, que intento convèncer'l que l'equació diofàntica

$$Z^4 + Y^4 - Z^2 = 0$$

no té cap solució tret de la trivial $X = Y = Z = 0$. Com podria convèncer'l?

V: En aquest cas ho té fàcil. Només m'ha d'explicar la demostració que va donar Fermat. Però crec que ja sé on vol anar a parar. Demostrar que una equació diofàntica no té cap solució pot arribar a ser molt molt complicat. En canvi, demostrar que una equació té alguna solució sempre és molt senzill; una qüestió molt diferent és com trobar aquesta solució.

P: Sí senyor. Aquest és un problema etern de les matemàtiques: enunciats existencials vs. enunciats universals. De fet, se'n desprèn del Teorema d'Incompletesa de Gödel i de la solució al 10è problema de Hilbert, que existeixen equacions diofàntiques sense solució per a les quals no existeix cap demostració d'insatisfactibilitat amb les regles habituals de la lògica i els axiomes de Peano, per exemple. Oi que fa ràbia que passin aquestes coses?

V: Doncs sí, la veritat. Però coneixent el Teorema d'Incompletesa de Gödel, no em sorprèn. A mi m'atabalaria encara més que existissin enunciats simples i demostrables per als quals la demostració més curta sigui tan gran que un humà fos incapaç de llegir-la, o pitjor encara, que hi hagi demostracions curtes però ningú sigui capaç de trobar-les.

P: Caram Dr. **V**, quina intuició que té! El problema P vs. NP tracta precisament d'això. Abans de donar la definició, però, necessitaré alguns exemples més. Consideri els grafs següents:

La Dra. **P** *torna a aixecar-se i s'acosta a la pissarra per dibuixar els grafs de la Figura 2.*

Suposem que el vull convèncer que els dos grafs són el mateix, és a dir, isomorfs. Oi que n'hi ha prou que li proporcioni la bijecció entre nodes que ho fa evident?

0	$\mapsto$	0	1	$\mapsto$	4
2	$\mapsto$	3	3	$\mapsto$	2
4	$\mapsto$	1	5	$\mapsto$	5
6	$\mapsto$	8	7	$\mapsto$	6
8	$\mapsto$	9	9	$\mapsto$	7

Vostè ho pot verificar en un tres i no res. En canvi, trobar la bijecció sembla una tasca molt més difícil; en general, no sembla que hi hagi millors maneres que recórrer les $10! = 3628800$ possibilitats.

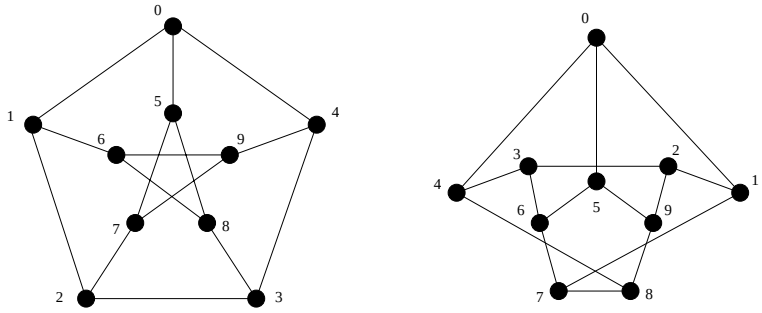

Figura 2: grafs dibuixats a la pissarra.

Un altre exemple. Suposem que el vull convèncer que el següent sistema d'equacions quadràtiques sobre els enters mòdul dos té solució en els enters mòdul dos:

$$
\begin{aligned}
&x_0 + x_1 + x_2x_3 + x_4 \equiv 0\\
&x_1(x_2 + x_4 + x_6 + x_8 + x_{10}) + x_0 \equiv 0\\
&x_2(x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13}) + x_4 + x_6 \equiv 1\\
&(1 + x_8)(1 + x_{10}) + x_{12} + x_8(x_7 + x_9) \equiv 0\\
&x_2 + x_3(1 + x_4) + x_5x_7 \equiv 1\\
&x_8 + x_{11} + x_{12} + x_{13} \equiv 1\\
&x_{13}x_1 + x_{12}x_2 + x_{11}x_3 + x_{10}x_4 \equiv 1
\end{aligned}
$$

N'hi ha prou que li proporcioni la solució

$$
\begin{array}{llll}
x_0 = 0 & & x_1 = 1\\
x_2 = 1 & & x_3 = 1\\
x_4 = 0 & & x_5 = 1\\
x_6 = 1 & & x_7 = 1\\
x_8 = 0 & & x_9 = 1\\
x_{10} = 0 & & x_{11} = 1\\
x_{12} = 1 & & x_{13} = 1
\end{array}
$$

Una vegada més, la solució es pot verificar molt ràpidament. En canvi, si vol trobar la solució vostè mateix, probablement li calgui recórrer de manera més o menys sistemàtica les $2^{14} = 16384$ possibilitats i verificar-les.

V: En aquests dos exemples que m'ha donat, una solució sempre és més o menys curta en relació al nombre de graus de llibertat del problema en

qüestió. La dificultat està en què hi ha moltíssimes possibles solucions, de fet una quantitat exponencial respecte del nombre de graus de llibertat, i no tenim manera de descartar-ne gaires. És això?

P: Sí, és això. Òbviament els meus exemples són petits. Però imagini's què passaria si els grafs tinguessin 200 nodes cadascun, o el sistema d'equacions tingués 150 variables i 300 equacions com sol passar en problemes d'enginyeria real.

Fixi's però, que no sempre ens cal recórrer una quantitat exponencial de possibles solucions. Per exemple, en un sistema d'equacions lineals podem trobar una solució per eliminació gaussiana. En aquest cas, l'àlgebra lineal ens ajuda a trobar la solució molt més ràpidament. Malauradament no tenim una teoria de l'àlgebra "quadràtica" que ens permeti fer el mateix amb sistemes d'equacions quadràtiques.

V: L'entenc. I llavors, el problema P vs. NP quin és?

P: En poques paraules, el problema P vs. NP consisteix a determinar si costa el mateix trobar solucions que verificar-les encara i quan el conjunt de solucions pot ser exponencialment gran respecte del nombre de variables del problema.

V: Què vol dir que costi el mateix?

P: Doncs que hi hagi un mètode tan eficient per trobar solucions com per verificar-les. Després de dinar li ensenyo les definicions.

5 Sobre l'eficiència

P: Permeti'm que introdueixi una mica de notació. Per un nombre natural x, faré servir $|x|$ per denotar la longitud de la seva representació en binari. Per tant, $|x| = \lceil \log_2(x+1) \rceil$.

V: Insisteix amb la notació binària. Confio que sigui important.

P: Recordi la definició de computabilitat d'una funció $f : \mathbf{N} \to \mathbf{N}$: diem que f és computable si existeix una màquina de Turing M que, quan rep un nombre natural x escrit en binari, produeix $f(x)$ també en binari, en un nombre finit de passos. Considerem ara el nombre de passos $t_M(x)$ que

fa la màquina M quan rep x com entrada. Si la màquina fa massa passos per produir la sortida, com per exemple 2^{2^x} passos, serà bastant inútil, no troba? A la pràctica, hi ha raons per creure que la tecnologia mai serà capaç d'implementar les màquines de Turing de manera que executin més de $|x|^4$ passos en un temps físicament raonable, quan x és molt gran.

V: Em semblen molt pocs $|x|^4$ passos. El mínim nombre de passos exigible és $|x|$ perquè l'entrada ella mateixa ja té aquesta quantitat de símbols. Per tant $|x|^4$ passos sembla que sigui només una mica més del que és imperativament necessari.

P: A veure si això el convenç. Fixi's bé. Suposem que un pas elemental d'una màquina de Turing triga 10^{-6} segons a executar-se. Estem d'acord que això és un temps fantàsticament petit per un procés físic complex com el d'una transició d'una màquina de Turing?

V: Sí.

P: Considerem ara dues màquines, una que fa $|x|^2$ passos amb entrada x, i una que en fa $2^{|x|}$.

La Dra. **P** *s'aixeca una vegada més i escriu la següent taula a la pissarra:*

x	$\|x\|^2$	$2^{\|x\|}$
2^{20}	0.4 ms	1.0 segon
2^{30}	0.9 ms	17.9 minuts
2^{40}	1.6 ms	12.7 dies
2^{50}	2.5 ms	35.7 anys
2^{60}	3.6 ms	36.6 segles

Fixi's que el creixement del temps de la primera màquina és molt més suau. Es diu que és *escalable*. En canvi, el segon *explota*, com es diu col.loquialment. Per cert, recordi que entrades de l'ordre de 2^{60} no són excessivament grans. Al cap i a la fi només són 60 símbols en binari que fem servir per codificar un objecte finit qualsevol, com ara una equació diofàntica, un graf, o un sistema d'equacions.

V: Aquesta taula és del tot elemental, Dra. **P**. Però he de reconèixer que és molt convincent.

P: Doncs bé; siguem una mica generosos i postulem que una funció f és eficientment computable si existeix una màquina de Turing M que la computa de manera que

$$t_M(x) \leq |x|^c$$

per alguna constant $c > 0$ independent de x. En aquest cas es diu que M computa f en temps polinòmic perquè el nombre de passos està afitat per un polinomi en el nombre de símbols de l'entrada. La gràcia principal de considerar polinomis de grau arbitrari es que llavors les funcions computables en temps polinòmic estan tancades per composició. Això fa que la definició sigui robusta i fàcil de treballar.

V: Molt bé. Això formalitza el concepte de funció eficientment computable. En particular, això permet formular preguntes del tipus: existeix una funció eficientment computable que, donat un sistema d'equacions sobre els enters mòdul dos, trobi una solució o indiqui que no n'hi ha cap? A priori no és gens obvi que un algorisme d'aquest tipus pugui existir perquè el conjunt de possibles solucions és exponencialment gran respecte del nombre de variables del sistema. Espero, però, que el mètode de l'eliminació gaussiana proporcioni un algorisme eficient en el cas lineal.

P: Efectivament. La seva intuició no deixa de sorprendre'm. De fet, l'eliminació gaussiana ho aconsegueix en uns n^3 passos elementals, on n és el nombre de variables del sistema lineal. Per tant, l'algorisme és polinòmic respecte del nombre de símbols per representar l'entrada que serà, certament, com a mínim n.

V: Entenc. Com sempre, m'imagino que haurem fixat alguna codificació raonable dels sistemes d'equacions com un nombre natural en binari. De fet, ara començo a entendre perquè és tant important l'eficiència de les codificacions. Si la codificació fos més llarga del que és estrictament necessari, com en el cas de la representació unària dels nombres naturals, aleshores podríem disposar de molt més temps de càlcul per una deficiència artificial de la codificació i no intrínsica del problema.

P: M'alleuja que hi reflexioni. Posats a fer, fixi's que la representació de l'altre dia per seqüències finites de nombres naturals $a_1, a_2, \ldots, a_m$ com a productes de potències de primers $p_1^{a_1} \cdot p_2^{a_2} \cdots p_m^{a_m}$ no és eficient perquè és molt semblant a la unària. Més valdria representar els nombres en binari

amb un nombre de bits fixat però prou llarg per representar el més gran de tots, i concatenar-los afegint-hi un 1^m0 al principi per saber quants en tenim. Per exemple, la codificació de $4, 5, 4, 3$ seria la concatenació de 11110, 100, 101, 100, i 011.

V: Tot i que em sembla entendre-ho, m'avorreix aquesta obsessió que teniu al final del segle XX per fer servir les representacions més eficients possibles. M'esperaria que una teoria robusta no hagués de fixar-se en aquests detalls.

P: De fet, la teoria és robusta sempre i quan es permetin un mínim de dos símbols. De fet, els detalls de codificació no són pràcticament mai un problema. És qüestió de pràctica i sentit comú.

Tornem ara a les definicions. Plantegem-nos aquests problemes de cerca de solucions en abstracte. Sigui

$$R \subseteq \mathbf{N} \times \mathbf{N}$$

una relació binària tal que si $(x, y) \in R$, aleshores $|y| \leq |x|^d$ per alguna constant $d > 0$ independent de x. Per raons òbvies, es diu que R és una relació *equilibrada* polinòmicament. Haurem de pensar que R relaciona les entrades d'un problema amb les seves solucions. En l'exemple anterior, R relacionaria els sistemes d'equacions mòdul dos amb les seves solucions. Per tant, és exigible que es pugui determinar de manera eficient, és a dir, en temps polinòmic respecte de la longitud de l'entrada, si un parell donat (x, y) pertany a R. En altres paraules, suposem que verificar solucions de R és computacionalment fàcil. En aquest cas direm que R és *decidible en temps polinòmic*.

Ara podem plantejar-nos el *problema d'existència* associat a una relació binària R que sigui equilibrada i decidible en temps polinòmic: donada una entrada x, determinar si existeix un $y \leq 2^{|x|^d}$ tal que $(x, y) \in R$. El conjunt de possibles y pot ser $2^{|x|^d}$, que és exponencial respecte de la longitud $|x|$ de l'entrada x. Per tant, un algorisme de cerca exhaustiva sobre tots els possibles y no és eficient. El problema P vs. NP és doncs el següent:

> *Determinar si existeixen relacions $R \subseteq \mathbf{N} \times \mathbf{N}$, equilibrades i decidibles en temps polinòmic, per a les quals el problema d'existència associat a R no és computable en temps polinòmic.*

És clar que si R és una d'aquestes relacions en què el problema d'existència associat no és eficientment computable, aleshores, amb més raó, el problema de cerca de solucions de R no serà eficientment computable.

V: Ja ho entenc. M'imagino que els exemples dels grafs isomorfs i els sistemes d'equacions quadràtiques mòdul dos són bons candidats de problemes difícils. El problema és demostrar que *qualsevol* algorisme que els resolgui requereix fer un nombre de passos que no està afitat per cap polinomi en la longitud de l'entrada.

P: Sí. El proper dia li explico d'on venen els noms P i NP, i al següent alguna cosa més sobre aquests candidats.

6 Origen de P vs. NP i definició formal

V: Vam dir que avui m'explicaria d'on venen els noms P i NP.

P: Això mateix. És molt senzill: P vé de "Polynomial time" en anglès. De fet, P és una classe de conjunts. Per una màquina de Turing M, direm que M accepta l'entrada x si la màquina arriba a l'estat q_+ quan s'inicia amb x escrit en binari a la cinta. Sigui $L(M)$ el conjunt de les entrades acceptades per M. Definim P com la classe dels conjunts A per als quals existeix una màquina de Turing M tal que $L(M) = A$ i $t_M(x) \leq |x|^c$ per alguna constant $c > 0$ independent de x. Això defineix P. Per altra banda, les sigles NP provenen de "Non-deterministic Polynomial time", també en anglès.

La Dra. **P** *fa una pausa per veure la cara que fa el Dr.* **V**.

V: Expliqui'm això de l'indeterminisme. Què fem, filosofia, ara?

P: Anem a pams. El model de màquina de Turing és perfectament determinista: a cada configuració no terminal de la cinta i l'estat actual, la següent configuració està unívocament determinada. De fet, no podia ser d'una altra manera. De què serviria una màquina amb un comportament imprevisible?

V: De res.

P: Bé doncs, donem-li un significat a una màquina que a cada configuració no terminal té una o més opcions per on continuar. Imaginem-nos que la

màquina té més d'una funció de transició, i cada cop que la màquina es troba davant d'una alternativa, es *multiplica* en còpies paral.leles, una per cada opció. Sembla una bajanada, oi?

V: Doncs sí. Sembla el discurs d'un defensor de la mecànica quàntica...

P: No va molt desencaminat Dr. **V**; però no subestimi els seus col.legues físics, faci'm cas. Suposarem, però, a diferència de l'indeterminisme quàntic, que les còpies paral.leles no poden interferir entre si. Direm que la màquina accepta l'entrada x si alguna de les còpies arriba a l'estat acceptador q_+. Com amb les màquines deterministes, sigui $L(M)$ el conjunt de les entrades acceptades per la màquina indeterminista M. Definirem el nombre de passos $t_M(x)$ de M com el màxim dels nombres de passos de les còpies produïdes quan s'inicia el còmput amb l'entrada x. Finalment, definim NP com la classe dels conjunts A per als quals existeix una màquina de Turing indeterminista tal que $L(M) = A$ i $t_M(x) \leq |x|^c$ per alguna constant $c > 0$ independent de x.

V: M'imagino que el problema P vs. NP consisteix a determinar si P = NP o P $\neq$ NP. És això?

P: Correcte. Fixi's que P $\subseteq$ NP, perquè qualsevol màquina determinista és un cas particular d'una d'indeterminista.

V: Sí, sí, és clar. Però escolti una cosa, Dra. **P**. Aquesta formulació de P vs. NP no s'assembla de res a l'anterior! M'està dient que son el mateix problema?

P: Evidentment. Deixi'm que ho raoni. Suposem primer que per qualsevol relació R, equilibrada i decidible en temps polinòmic, podem resoldre el problema d'existència associat a R en temps polinòmic. Veurem que sota aquesta hipòtesi, NP $\subseteq$ P i per tant P = NP. Per qualsevol màquina indeterminista M tal que $t_M(x) \leq |x|^d$, podem definir una relació R així: $(x, y) \in R$ si y codifica el còmput d'una còpia de M que acaba a l'estat q_+ quan s'inicia amb l'entrada x. No és difícil veure que R és equilibrada i decidible en temps polinòmic. Per hipòtesi, doncs, el seu problema d'existència associat es pot resoldre en temps polinòmic. Però el problema d'existència de R és precisament el problema de determinar si la màquina indeterminista M accepta o no. Per tant NP $\subseteq$ P.

Per veure l'altra implicació, suposem que NP $\subseteq$ P i sigui R una relació qualsevol, equilibrada i decidible en temps polinòmic. És prou evident que el problema existencial associat a R es pot resoldre amb una màquina indeterminista així: durant els $|x|^d$ primers passos, fem que la màquina es multipliqui en dues còpies a cada pas, generant un total $2^{|x|^d}$ còpies, una per cada candidat a solució y. A continuació, només cal fer que cada còpia verifiqui el seu candidat a solució, de manera determinista, en temps polinòmic, i fer acceptar les còpies que realment corresponen a una solució. Per tant, el problema d'existència associat a R pertany a NP i, per hipòtesi, a P. Per tant el podem resoldre en temps polinòmic.

V: Si ho he entès bé, aquest segon argument aprofita l'indeterminisme per "provar" totes les possibles solucions en paral.lel. És evident que això no es pot dur a terme a la pràctica.

P: Precisament la qüestió P vs. NP està plantejant si hi ha alguna manera d'evitar simular totes les còpies paral.leles. No deixa de ser curiós que en l'exemple del sistema d'equacions lineals siguem capaços de fer-ho gràcies a l'eliminació gaussiana, un mètode inventat al segle XIX.

V: Sí que és curiós...

7 Teorema de Cook: NP-completesa

P: Avui m'agradaria tornar sobre els exemples de l'altre dia. Recordem-los. El primer consistia a determinar si dos grafs són isomorfs: donats dos grafs G i H, determinar si existeix una bijecció h del conjunt de vèrtexs de G al conjunt de vèrtexs de H, de manera que $\{u, v\}$ és una aresta de G si i només si $\{h(u), h(v)\}$ és una aresta de H. Per qualsevol esquema de codificació raonable, és clar que aquest problema pertany a NP. El segon exemple consistia en determinar si un sistema d'equacions quadràtiques mòdul dos té solució. També pertany a NP. Permeti'm una pregunta. Aprecia alguna relació entre els dos problemes?

V: A part del fet que ambdós problemes pertanyen a NP, a simple vista no en veig cap de relació.

P: D'acord. M'agradaria argumentar que de fet hi ha una relació bastant directa. El que veurem és que el primer es pot transformar en el segon. Fixi's

bé. El que volem fer és tranformar un parell de grafs G i H en un sistema d'equacions quadràtiques $S(G,H)$ de manera que G i H siguin isomorfs si i només si $S(G,H)$ té solució. Vol veure-ho?

V: Sí.

P: Per cada vèrtex u de G i cada vèrtex v de H, sigui $x_{u,v}$ una variable que pren valors a $\mathbf{Z}/2\mathbf{Z}$, els enters mòdul dos. El significat intuitiu de $x_{u,v} = 1$ és que la possible bijecció entre G i H, si n'hi ha, envia u a v. Em segueix?

V: Sí.

P: Ara ens caldrà imposar equacions que forcin que un mateix vèrtex u no s'envii a dos vèrtexs diferents v i v' simultàniament. Per tant, volem que

$$x_{u,v}x_{u,v'} \equiv 0 \tag{1}$$

per cada vèrtex u de G i cada parell de vèrtexs v i v' de H amb $v \neq v'$. També necessitarem imposar que si $\{u,u'\}$ és una aresta de G però $\{v,v'\}$ no és una aresta de H, aleshores o bé u no s'envia a v, o bé u' no s'envia a v'. Per tant, volem que

$$x_{u,v}x_{u',v'} \equiv 0 \tag{2}$$

per cada aresta $\{u,u'\}$ de G i cada parell $\{v,v'\}$ que no és una aresta de H. Òbviament, també imposarem aquesta equació per cada parell $\{u,u'\}$ que no és una aresta de G i cada aresta $\{v,v'\}$ de H. Finalment, ens caldrà especificar que cada u s'envia com a mínim a un v i que cada v rep algun u. De moment ens contentarem de fer-ho amb equacions no quadràtiques: per cada vèrtex u de G imposarem l'equació

$$\prod_v (1 - x_{u,v}) \equiv 0, \tag{3}$$

i per cada vèrtex v de H imposarem l'equació

$$\prod_u (1 - x_{u,v}) \equiv 0. \tag{4}$$

Vol comprovar que és correcte?

V: Anem a veure... si volem que el producte $\prod_v (1 - x_{u,v})$ sigui congruent amb 0, necessàriament algun $x_{u,v}$ haurà de prendre el valor 1, i per tant no

tots seran 0. Per tant, tot u s'envia a algun v, i el mateix per l'altre equació, tot v rep algun u. D'acord, això fa el que volem. Però això no és quadràtic, com vostè diu.

P: Ara ho fem quadràtic. Sigui $\{v_1, \ldots, v_n\}$ una enumeració dels vèrtexs de H. Per cada cada vèrtex u de G i cada $i \in \{0, \ldots, n\}$ introduïm una nova variable $z_{u,i}$. Ara imposem l'equació quadràtica

$$z_{u,i} \equiv z_{u,i-1}(1 - x_{u,v_i}). \tag{5}$$

Per $i = 0$ imposarem l'equació $z_{u,0} \equiv 1$. Amb aquestes restriccions, és clar que

$$\prod_v (1 - x_{u,v}) \equiv z_{u,n}.$$

Per tant, podem substituïr l'equació (3) per les equacions quadràtiques (5) i l'equació

$$z_{u,n} \equiv 0. \tag{6}$$

Si fem el mateix per l'equació (4), haurem aconseguit un sistema quadràtic d'equacions mòdul dos que té solució si i només si G i H són isomorfs. Fixi's que la transformació és eficient, és a dir, es pot trobar en temps polinòmic.

V: Ara entenc què volia dir quan em preguntava si apreciava alguna relació entre els problemes. Amb aquesta transformació, si sabéssim resoldre sistemes d'equacions quadràtiques mòdul dos en temps polinòmic també sabriem resoldre el problema de l'isomorfisme de grafs en temps polinòmic.

P: Exacte. D'això se'n diu fer una reducció d'un problema a l'altre, de la mateixa manera que en Matijasevich va reduir el 10è problema de Hilbert per equacions diofàntiques exponencials al 10è problema de Hilbert per equacions diofàntiques normals. Se'n recorda?

V: Sí que ho recordo. Però deixi'm dir-li una cosa. No em sorprèn gens que hàgim estat capaços d'expressar problemes de grafs de manera algebraica. Descartes ja va expressar problemes de geometria en termes algebraics.

P: És veritat. El que potser és una mica més sorprenent és el que es coneix com el Teorema de Cook segons el qual *qualsevol* problema que pertanyi a NP es pot transformar, de manera eficient, al problema de resoldre

sistemes d'equacions quadràtiques mòdul dos. De fet, Cook no va considerar sistemes d'equacions directament, sino fórmules booleanes en forma normal conjuntiva, però vé a ser el mateix en una àlgebra diferent.

V: Qualsevol problema que pertanyi a NP s'hi pot reduir? Això és més interessant perquè vol dir que el conjunt de solucions d'un sistema quadràtic en els enters mòdul dos pot codificar còmputs eficients d'una màquina de Turing. És anàleg al fet que el conjunt de solucions d'una equació diofàntica també pot codificar còmputs, eficients o no, d'una màquina de Turing.

P: Aquesta és l'analogia exacta. Més tard hi tornarem. Ara, però, deixi'm que enuncïi el Teorema de Cook amb precisió:

> **Teorema (de Cook 1971 [1], versió sistemes quadràtics)** *Per tot A que pertanyi a NP, existeix una funció f computable en temps polinòmic, i tal que per a tota entrada x tenim $x \in A$ si i només si $f(x)$ codifica un sistema d'equacions quadràtiques en els enters mòdul dos que té solució.*

Una conseqüència immediata del Teorema de Cook és que per demostrar P = NP *n'hi ha prou* a trobar un algorisme eficient per resoldre sistemes quadràtics mòdul dos. De la mateixa manera, per demostrar P $\neq$ NP és suficient i necessari demostrar que no es poden resoldre sistemes quadràtics mòdul dos en temps polinòmic.

V: En certa manera ens podem oblidar de la classe NP. Tota la seva dificultat es troba en un sol problema!

P: En certa manera sí, i això el fa interessant. El Teorema de Cook, a més, suggereix una definició. Direm que un conjunt B és NP-complet si B pertany a NP i per qualsevol altre problema A que pertanyi a NP existeix una reducció de A a B com en el Teorema de Cook; és a dir, existeix una funció f computable en temps polinòmic tal que $x \in A$ si i només si $f(x) \in B$. El Teorema diu que el problema de les equacions quadràtiques en els enters mòdul dos és NP-complet.

La Dra. **P** *agafa un llibre de tapes toves, negres i molt gastades de la llibreria. El llibre porta per títol: "Computers and Intractability. A Guide to the Theory of NP-Completeness" i els autors són M. R. Garey i D. S. Johnson [2].*

Miri's aquest llibre. Aquí té una col.lecció de més d'un centenar de problemes NP-complets de molt diverses àrees de les matemàtiques i l'enginyeria: des de determinar el número cromàtic d'un graf, passant per problemes de lògica proposicional, fins a problemes de planificació en enginyeria.

V: Tots ells són, doncs, equivalents?

P: Sí. Demostri que un de sol és computable en temps polinòmic i haurà demostrat que tots ho són. Demostri que un de sol no és computable en temps polinòmic i haurà demostrat que cap no ho és. Hi ha qui creu que el fet que hi hagi tantíssims problemes NP-complets de tantes àrees diferents és l'evidència més flagrant que P $\neq$ NP. Però això és discutible...

V: Li estic molt agraït per les seves explicacions Dra. **P**. Malauradament, demà serà el meu últim dia a la ciutat i abans de marxar m'agradaria que parléssim de l'analogia amb el 10è problema de Hilbert que abans hem aparcat. Podríem parlar-ne demà?

P: I tant. Fins demà, doncs.

8 Analogia, estètica, i comiat

V: La nostra conversa es va iniciar pel meu interès en la resolució del 10è problema de Hilbert i hem acabat parlant del Teorema de Cook. Durant la conversa ens vam adonar d'una analogia entre les dues coses. Faci'm cinc cèntims de la relació exacta.

P: A vista d'ocell i amb la perspectiva històrica, la solució al 10è problema de Hilbert es pot resumir de la següent manera. 1) Turing identifica un problema no computable, i 2) Davis, Putnam, Robinson i Matijasevich demostren que el problema no computable de Turing es pot reduir al problema de determinar si una equació diofàntica té solució. La conclusió és que el problema de les equacions diofàntiques no és computable.

Però de fet, el problema que Turing va identificar és molt més que un problema no computable; Turing va identificar un problema *complet per als problemes d'existència* en general. M'explicaré. Sigui

$$R \subseteq \mathbf{N} \times \mathbf{N}$$

una relació binària. Aquest cop no exigirem que R sigui equilibrada. Suposem que es pugui determinar mitjançant una funció computable si un parell donat (x, y) pertany a R. En aquest cas direm que R és decidible. Com en el cas de les relacions equilibrades, ens podem plantejar el problema d'existència associat a R, però sense exigir que la solució y estigui afitada. El problema d'existència associat a R és, doncs, aquest: donada una entrada x, determinar si existeix un y tal que $(x, y) \in R$. Fins aquí tot és anàleg, oi? El que Turing va identificar és una relació binària i decidible tal que el seu problema d'existència associat no és computable.

V: I quina és aquesta relació binària?

P: Doncs la de la funció universal de Turing: la relació binària que relaciona màquines de Turing M i les entrades x amb els còmputs acceptadors. Però el més interessant del cas és que la relació binària de Turing és com un problema *complet*, és a dir, qualsevol problema d'existència associat a una relació decidible s'hi pot reduir.

V: Per tant, Turing va demostrar l'anàleg al Teorema de Cook per relacions decidibles generals.

P: Més aviat al contrari, amic meu. En Cook va demostrar l'anàleg al resultat de Turing per relacions binàries equilibrades i decidibles en temps polinòmic.

V: Sí és clar, perdoni. Viatjar en el temps provoca aquests lapsus.

P: Però seguim amb el 10è problema de Hilbert. Donat que Davis, Putnam, Robinson i Matijasevich van demostrar que el problema de Turing es redueix al problema de les equacions diofàntiques, en deduïm que qualsevol problema d'existència associat a una relació decidible es redueix al problema de les equacions diofàntiques.

V: Interessant. De fet, el propi problema de determinar si una equació diofàntica té solució és un problema d'existència associat a una relació decidible. Per tant, l'analogia és molt clara: el problema de les equacions diofàntiques és *complet per als problemes d'existència* generals. Però l'analogia hagués estat més estètica si el problema NP-complet de Cook fos més semblant al de les equacions diofàntiques.

P: Cert. Fixi's, però, que el problema de les equacions diofàntiques es pot reduir al problema de determinar si un sistema d'equacions diofàntiques quadràtiques té solució. Només hem d'aplicar el truc de les variables auxiliars per reduir el grau dels monomis.

V: ... molt astut. Tot i així, hagués estat més bonic mantenir intacte el problema clàssic dels grecs i canviar el de Cook.

P: Això mateix devien pensar l'Adleman i el Manders l'any 1978. Se'n recorda que el vaig avisar que hi havia problemes NP-complets per donar i vendre? Obri siusplau el llibre de Garey and Johnson per la pàgina 250. Quin problema hi veu a final de pàgina?

V: A veure... 248, pàgina 250. Equacions diofàntiques quadràtiques: donada una equació diofàntica de la forma $aX^2 + bY = c$ amb incògnites X i Y, determinar si té solució. Suposo que el fet que l'equació sigui quadràtica deu garantir que, si hi ha solucions, alguna estigui afitada polinòmicament... Aquesta analogia sí que és estèticament satisfactòria: el problema de les equacions diofàntiques generals és complet per als problemes d'existència generals, i el problema de les equacions diofàntiques quadràtiques és NP-complet, és a dir, complet per als problemes d'existència amb solucions petites i verificadors eficients. Només falta un petit detall per acabar de lligar-ho tot: demostrar que P $\neq$ NP.

Referències

[1] S. Cook. The complexity of theorem proving procedures. In *3rd Annual ACM Symposium on the Theory of Computing*, pages 151–158, 1971.

[2] M. R. Garey and D. S. Johnson. *Computers and Intractability.* W. H. Freeman and Company, 1979.

[3] D. Hilbert. Mathematical problems. *Bulletin of the American Mathematical Society*, 8:437–479, 1901–1902.

[4] Yu. V. Matijasevich. *Hilbert's Tenth Problem.* MIT Press, 1993.