Demostracions assistides per ordinadors

Un problema filosòfic per a les matemàtiques?

L'ús d'ordinadors per a demostracions matemàtiques va obrir, als anys vuitanta, un debat al voltant de la naturalesa mateixa d'aquesta ciència. Amb el desenvolupament de la computació quàntica i la intel·ligència artificial, l'horitzó de la problemàtica s'ha ampliat molt més.

Per **Elena Menta Oliva**

«L'ús d'ordinadors en matemàtiques pot fer que la naturalesa de les matemàtiques s'hagi de repensar.»

No és estrany l'ús d'ordinadors en matemàtiques. Ben al contrari, actualment s'utilitzen sovint per assistir tasques com ara l'execució de càlculs llargs —com buscar nombres primers cada cop més grans—, la verificació automatitzada de raonaments, la gestió i anàlisi de dades... Però durant la dècada dels vuitanta n'aparegué un nou ús que va despertar sospites entre alguns filòsofs de les matemàtiques.

L'any 1976 els matemàtics K. Appel i W. Haken publicaren la demostració del teorema dels quatre colors (T4C), que va ser la primera demostració matemàtica assistida per ordinadors. Si bé els matemàtics l'acceptaren sense recances, des de la filosofia es va obrir un petit debat sobre la possibilitat que aquest tipus de pràctica ataqués frontalment intuïcions sobre la naturalesa de les matemàtiques.

Línies generals del debat filosòfic sobre les demostracions assistides per ordinadors

A grans trets i sense entrar en els detalls del teorema, l'estructura de la demostració del T4C constava d'una primera part en què els matemàtics van descompondre el problema en un total de 1.936 configuracions mínimes i una segona part en què l'ordinador va demostrar que cap d'aquestes 1.936 configuracions no era un contraexemple del T4C. Aquesta darrera part, la demostració dels casos, va requerir més de 1.200 hores de computació.

Les especificitats de l'ús dels ordinadors en demostracions com aquesta, que marquen la diferència respecte a altres usos no problemàtics filosòficament, són: càlculs massius (d'una magnitud no equiparable amb la capacitat humana de reproduir-los), inevitabilitat de l'ús dels ordinadors i absència de demostració tradicional (que no recorri a ordinadors).

Imatge de fons: il·lustració sobre el procés cognitiu de la intel·ligència artificial.

Davant d'això, Thomas Tymoczko, filòsof de les matemàtiques, va obrir dues línies argumentals per defensar que l'ús d'ordinadors en matemàtiques pot fer que la naturalesa de les matemàtiques s'hagi de repensar.

El primer argument de Tymoczko consistí a invocar l'empiricitat dels ordinadors (i l'observació física dels resultats a la pantalla) per atacar la concepció de les matemàtiques com a ciència formal, com a ciència *a priori*, independent de l'experiència (Tymoczko, 1979: 58 i 62).

Aquest argument es va rebatre, en primer lloc, evidenciant que l'ús del terme «empíric» era massa ampli —el comprometria a acceptar com a experiment *a posteriori* l'ús de paper i llapis—. I, en segon lloc, desambiguant el significat d'aprioricitat: no esperem obtenir coneixement matemàtic sense recórrer a l'experiència (cognoscibilitat *a priori*); esperem que el coneixement obtingut sigui necessàriament vertader independentment de l'experiència, veritat en tot món possible (veritat *a priori*) (Swart, 1980: 699) (Bondecka-Krzykowska, 2004: 7-12).

El segon argument de Tymoczko invoca una altra característica definitòria de tota demostració matemàtica: la propietat de ser comprovable, és a dir, comprensible, revisable i verificable per éssers racionals a mà. A causa de la immensa extensió del càlcul, cap ésser humà ha comprovat ni podrà comprovar en una vida finita la demostració en la seva totalitat, i això serví a Tymoczko per no considerar com a tals demostracions com ara la del T4C (Tymoczko, 1979: 60 i 68).

Les rèpliques a aquest argument, de nou, foren dues. Per una banda, Krakowski en va discutir l'ús restringit del terme «verificable»: no ser verificable en una escala temporal humana no equival a ser no verificable. La finitud dels càlculs implica verificabilitat, ja que «res no evita que, quan la longevitat humana adquireixi proporcions astronòmiques, un humà pugui passar un mil·lenni revisant la demostració» (Krakowski, 1980: 93). Per altra banda, es va apuntar una llista de mètodes de comprova-

«El component creatiu i intuïtiu de la demostració (típicament humà) és prescindible o assumible per la pura computació?»

ció —alternatius a la força bruta de revisar-ho a mà— que verificarien la demostració: replicar el codi en diferents *hardwares*, trobar el mateix resultat amb algorismes equivalents o amb diferents llenguatges de programació, verificar el codi —no el resultat— amb un programa d'ordre superior, i fragmentar i repartir el càlcul en parts comprovables efectivament a mà per una comunitat d'investigadors (Swart, 1980: 703-704).

Possibles derives futures del debat sobre l'ús d'ordinadors en matemàtiques

El debat obert a partir del T4C es va tancar relativament ràpid i ha quedat com a anecdòtic. Des d'aleshores, la tecnologia ha anat desenvolupant-se incansablement i convertint-se en habitual en la pràctica matemàtica. I així com als anys vuitanta la tecnologia innovadora —com ho era la del T4C— va generar interrogants, tecnologies actuals com la computació quàntica i la intel·ligència artificial conviden a recuperar i actualitzar la mateixa reflexió filosòfica: introduir elements nous en la pràctica de les matemàtiques xoca amb la seva naturalesa?

És previsible que en un futur proper es faci actual l'interès filosòfic de repensar les nostres intuïcions sobre la naturalesa de les matemàtiques en conjunció amb aquest progrés tecnològic.

Computació quàntica

La computació quàntica (CQ) és un nou paradigma de computació que explota propietats i estats quàntics. Sense entrar en detalls tècnics, el que principalment la diferencia de la computació clàssica (CC) és que la unitat mínima d'informació no és el bit, sinó el qbit (o bit quàntic). El bit pot estar en dos estats —1 o 0—; el qbit pot estar en dos estats base —$|1\rangle$ o $|0\rangle$— i també pot estar en un estat de superposició quàntica, en què és simultàniament $|1\rangle$ i $|0\rangle$. Ara bé, així com en qualsevol moment es pot observar un bit i saber en quin estat està, això no és possible amb els qbits. A conseqüència del problema de la mesura, la interacció que comporta l'observació del qbit l'altera i fa que l'estat de superposició col·lapsi en un estat base. Quan això succeeix, passa a operar com un bit.

La possibilitat de definir noves portes lògiques per operar amb qbits en estat de superposició fa que una mateixa tasca pugui tenir diferent complexitat en CC i en CQ. De fet, la CQ permet tractar problemes d'una complexitat exponencialment major que amb CC no es poden resoldre o requeririen quantitats ingents de temps per fer-ho.

Aquesta brevíssima imatge donada de la CQ ja permet intuir que un dels problemes analitzats en el debat filosòfic dels anys vuitanta es pot tornar més complex: el problema de la verificabilitat.

Només la diferència exponencial de capacitat i velocitat de computació multiplica l'extensió de la part executada per l'ordinador (ja fora de l'abast humà en CC). Però les dificultats significatives afecten els mètodes de verificació. D'entre els enumerats abans, el mètode de replicar el càlcul en diversos *hardwares* seria extremament costós, i actualment es dubta de la possibilitat de construir ordinadors quàntics físics prou grans. I la dificultat més rellevant: no es pot partir la demostració en parts, comprovar-les per separat i comprovar-ne les unions. Això és físicament impossible, a causa del problema de la mesura, en observar un qbit per conèixer-ne l'estat, ja que aquest col·lapsa irreversiblement i s'altera tot el càlcul posterior. Aquest desconeixement del procés fins al moment de la mesura final fa de la verificació en CQ un problema quantitativament més complex. Tot i poder afegir en el codi elements de correcció d'errors, sembla que sempre queda una pèrdua de transparència respecte a la CC.

Intel·ligència artificial

Així com la CQ encara està en procés de desenvolupament, la intel·ligència artificial (IA) ja és una realitat que s'ha anotat èxits significatius en l'àmbit de les matemàtiques. En aquest cas, les contribucions de la computació van més enllà de la simple execució de càlculs programats per matemàtics, van més enllà de «seguir ordres» d'un algorisme donat. La IA pot ser capaç d'intuir i decidir l'estratègia per demostrar conjectures i executar les ordres que autònomament s'hauria donat, duent a terme

«A qui s'ha d'atribuir l'autoria de les demostracions fetes per intel·ligència artificial?»

la part mecànica (el càlcul) i la part creativa (l'estructura i relació d'idees) de la demostració.

El marge de la IA per fer aportacions conceptualment significatives i audaces de manera autònoma fa que ja no es tracti d'una dificultat afegida als problemes vistos anteriorment, sinó que es planteja una dificultat qualitativament diferent. Es desafien un nou grup d'intuïcions sobre la naturalesa de les matemàtiques, aquest cop relatives a la noció d'agència del raonament matemàtic.

Les matemàtiques són una empresa únicament humana? El component creatiu i intuïtiu de la demostració (típicament humà) és prescindible o assumible per la pura computació? Així com en l'execució de càlculs els ordinadors superen els humans, podran també arribar a vèncer en intel·ligència matemàtica? Poden produir noves matemàtiques? A qui s'ha d'atribuir l'autoria de les demostracions fetes per IA?

Podem comprendre els resultats que generen? En aquest cas, ja no només l'execució dels càlculs podria escapar a la nostra capacitat de verificar-los, sinó que també el raonament que porta a combinar idees i regles lògiques seria independent de la figura del matemàtic. Obtenir de la IA un resultat (que podem entendre) sense tenir-ne la gènesi o un procés modular amb què arribar-hi, podria fer perdre de vista el perquè del raonament i diluir-ne la comprensió. ●

Bibliografia

Appel, Kenneth i Wolfgang Haken (1976). «Every planar map is four colorable». *Bulletin of the American Mathematical Society*, vol. 82, núm. 5: 711-712.

Bondecka-Krzykowska, Izabela (2004). «The Four-Color Theorem and its consequences for the philosophy of mathematics». *Annales UMCS Informatica*, vol. 2, núm. 1: 5-14.

Krakowski, Israel (1980). «The Four-Color Problem reconsidered». *Philosophical Studies*, vol. 38, núm. 1: 91-96.

Swart, Edward R. (1980). «The philosophical implications of the Four-Color Problem». *The American Mathematical Monthly*, vol. 87, núm. 9: 697-707.

Tymoczko, Thomas (1979). «The Four-Color Problem and its philosophical significance». *The Journal of Philosophy*, vol. 76, núm. 2: 57-83.