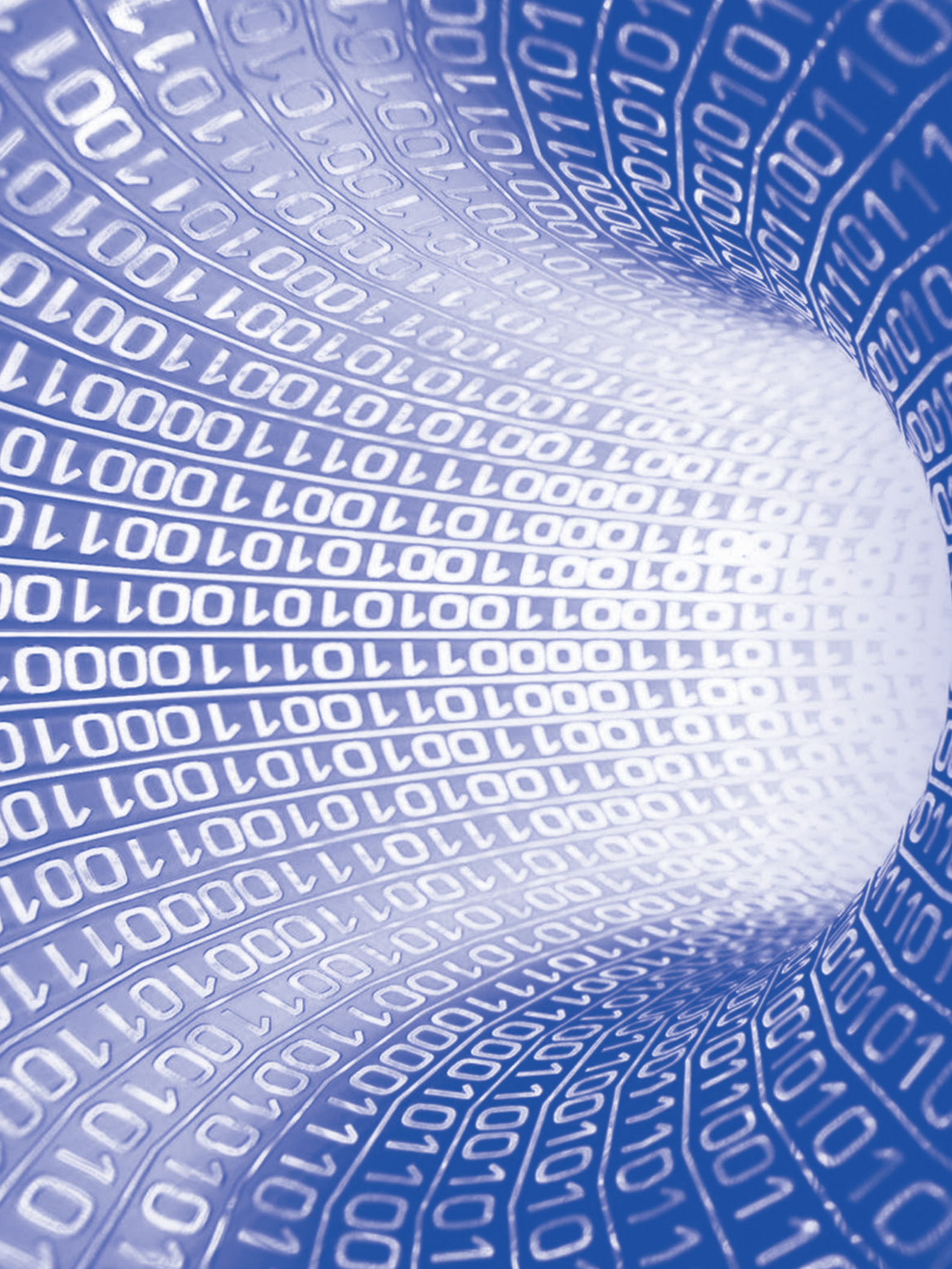

Computació i supremacia quàntica

Per què tothom parla d'això?

La computació quàntica segurament canviarà el món en què vivim i impulsarà enormement el coneixement científic, tal com ho va fer la computació clàssica.

Per **Carlos Bravo Prieto, Diego García Martín i Adrián Pérez Salinas, del grup QUANTIC (UB-IFAE-BSC)**

La computació quàntica és un dels grans reptes tecnològics i intel·lectuals de l'actualitat. Durant molt de temps, des que Richard Feynman ho va proposar ja fa quasi quaranta anys, va ser una branca més de la física quàntica, però recentment ha experimentat un creixement sense precedents que transcendeix els límits de l'àmbit purament acadèmic. Les grans empreses tecnològiques de la informació, com ara Google, IBM, Microsoft o Intel, competeixen per liderar la cursa fins a l'ordinador quàntic. Els governs de les grans potències mundials també mouen fitxa. Ja existeixen, de fet, els primers ordinadors quàntics, encara que estan en una fase molt primitiva. La gran promesa de la computació quàntica és que, en un futur no gaire llunyà, tindrem ordinadors capaços de resoldre problemes que avui dia no sabem com atacar eficaçment. Entre les futuribles aplicacions de la computació quàntica hi ha la intel·ligència artificial, el disseny de fàrmacs o l'optimització, tot omnipresent avui dia.

Tots els ordinadors clàssics són, en essència, el mateix tipus de màquina. Funcionen amb bits, que són objectes amb estats 0 o 1 ben diferenciats, sobre els quals s'executen milions d'operacions per segon. Altrament, els ordinadors quàntics funcionen amb bits quàntics o qbits, que posseeixen una propietat intrínsecament quàntica anomenada *superposició*. Una superposició és un estat quàntic amb part de 0 i part d'1. Quan s'observa el qbit, quan *s'efectua una mesura*, aquest es mostra com a 0 o com a 1 aleatòriament, amb certa probabilitat, i perd la superposició. Una conseqüència immediata d'aquest fet és que, al contrari que en els ordinadors clàssics, per als quàntics no és possible conèixer el que està succeint en el seu interior sense destruir el càlcul. L'estat dels qbits no es revela fins al final de la computació.

Una altra propietat purament quàntica és l'*entrellaçament*. Quan dos o més qbits estan entrellaçats, no és possible assignar un estat a cada qbit per separat: només és possible descriure l'estat de tots els qbits en el seu conjunt. Aquesta propietat recorda, per tant, allò que «el tot és més que la suma de les parts». En els ordinadors clàssics, en afegir un bit, la quantitat d'informació que pot emmagatzemar-se augmenta en (+1). Al contrari, en afegir un qbit en un ordinador quàntic, la capacitat es duplica (× 2), és a dir, creix *exponencialment* amb el nombre de qbits, si bé és cert que no tota la informació és directament accessible per a l'usuari.

La superposició i l'entrellaçament fan que el processament de la informació en els ordinadors clàssics i quàntics sigui completament diferent. Llavors, hem de plantejar-nos com podem programar un ordinador quàntic de manera que permeti resoldre problemes millor inclús que els superordinadors més potents. Aquesta possibilitat es coneix com a *avantatge quàntic*. Trobar les receptes, els *algorismes*, per a l'avantatge quàntic no és senzill, però ja se'n coneixen alguns que utilitzen les propietats de la mecànica quàntica a favor seu. Un dels més famosos és l'algorisme de factorització de *Shor*, que permet trencar la seguretat de la majoria dels sistemes informàtics del món. Això és així perquè la criptografia depèn d'alguns problemes matemàtics molt difícils per als ordinadors actuals (amb un temps de resolució de milers d'anys), però senzills per als quàntics (minuts). Malgrat això, no cal entrar en pànic, els investigadors ja han ideat mètodes d'encriptació resistents a la quàntica.

Encara que les diferències en el processament d'informació són importants, ja que es tradueixen en l'avantatge quàntic, la computació quàntica pot significar, a més, un estalvi considerable en el consum energètic. El MareNostrum 4, el superordinador de Barcelona, consumeix aproximadament un milió i mig d'euros anuals, uns tres mil euros diaris, tenint en compte l'alimentació de l'ordinador i la refrigeració. En canvi, l'alimentació d'un ordinador quàntic no requereix pràcticament energia, ja que es controla per mitjà de polsos de llum molt febles i la despesa en refrigeració és molt petita.

Els ordinadors quàntics que existeixen avui dia es troben encara en un estat molt experimental, són cars i incapaços de resoldre problemes complexos. Molts factors fan que la construcció d'un ordinador quàntic sigui un repte enorme. Actualment no se sap quin serà el suport físic definitiu

«No podem esperar que els ordinadors quàntics siguin tan potents com els superordinadors clàssics, però sí que s'han produït grans avenços.»

d'aquestes màquines. Diferents empreses i grups d'investigació exploren tecnologies diverses, com ara els circuits superconductors (Google o IBM), els ions atrapats (IonQ o Honeywell) o els fotons (Xanadu), entre d'altres. Per si no n'hi hagués prou, un ordinador quàntic totalment funcional també haurà d'incorporar esquemes de correcció d'errors. Ordinadors amb aquestes característiques són els anomenats *fault-tolerant*, resistents a errors.

A Barcelona s'està construint un ordinador quàntic a l'Institut de Física d'Altes Energies (UAB). El grup d'investigació QUANTIC (UB-IFAE-BSC)[1] impulsa aquest projecte, amb tecnologia de qbits superconductors. El xip quàntic és molt petit, milionèsimes de metre, i ha de funcionar a temperatures molt baixes, 10 mK o, el que és el mateix, 273, 14°C, molt a prop del zero absolut, la temperatura més baixa permesa per les lleis de la física. Per aconseguir aquesta temperatura, cal un refrigerador de la mida d'una persona, aproximadament. Sense entrar en detalls, és evident que fabricar un ordinador amb aquestes característiques és tremendament complicat.

A curt termini, no podem esperar que els ordinadors quàntics siguin tan potents com els superordinadors clàssics, però sí que s'han produït grans avenços en aquest sentit els últims mesos. El més rellevant va venir dels laboratoris de Google, a Santa Bàrbara (Califòrnia), on van proclamar l'obtenció de la *supremacia quàntica*, és a dir, van resoldre un problema irresoluble inclús per a un superordinador. Encara que aquest problema no té utilitat pràctica, demostra una millora dels prototips de processadors quàntics. D'altra banda, IBM té a disposició de tots els usuaris via Internet una xarxa de petits ordinadors quàntics. Es poden utilitzar gratuïtament des de la seva pàgina web.[2]

Actualment, la computació quàntica s'endinsa en l'anomenada fase NISQ, sigla en anglès de *noisy intermediate-scale quantum*. Aquesta fase es caracteritza per tenir ordinadors quàntics de petita escala, no més de centenars de qbits, i sense correcció d'errors. Aquests ordinadors NISQ no serveixen encara per completar càlculs útils d'una manera purament quàntica, però podran complementar-se amb ordinadors clàssics per dur a terme certes operacions d'una manera híbrida. Aquesta computació híbrida és una resposta enginyosa a l'expectació creada al voltant del món quàntic.

Els algorismes híbrids permetran avançar la data d'aplicabilitat de la computació quàntica a l'era NISQ i, d'aquesta manera, aproparan en el temps les primeres aplicacions pràctiques dels ordinadors quàntics. En el grup teòric de QUANTIC es desenvolupen algorismes en aquest camp.

La computació quàntica segurament canviarà el món en el qual vivim i impulsarà enormement el coneixement científic, tal com ja ho va fer la computació clàssica. La diferència fonamental respecte al temps en el qual es va desenvolupar aquesta última és que al segle XXI sí que se sap el que els ordinadors són capaços de fer, i estem tots impacients per veure-ho. Si la computació quàntica prospera, i res sembla indicar el contrari, la societat possiblement experimentarà una transformació disruptiva, anàloga a la revolució de la informàtica. L'era quàntica s'apropa. ●

Notes

1 Universitat de Barcelona, Institut de Física d'Altes Energies, Barcelona Supercomputing Center.
2 https://quantum-computing.ibm.com/.