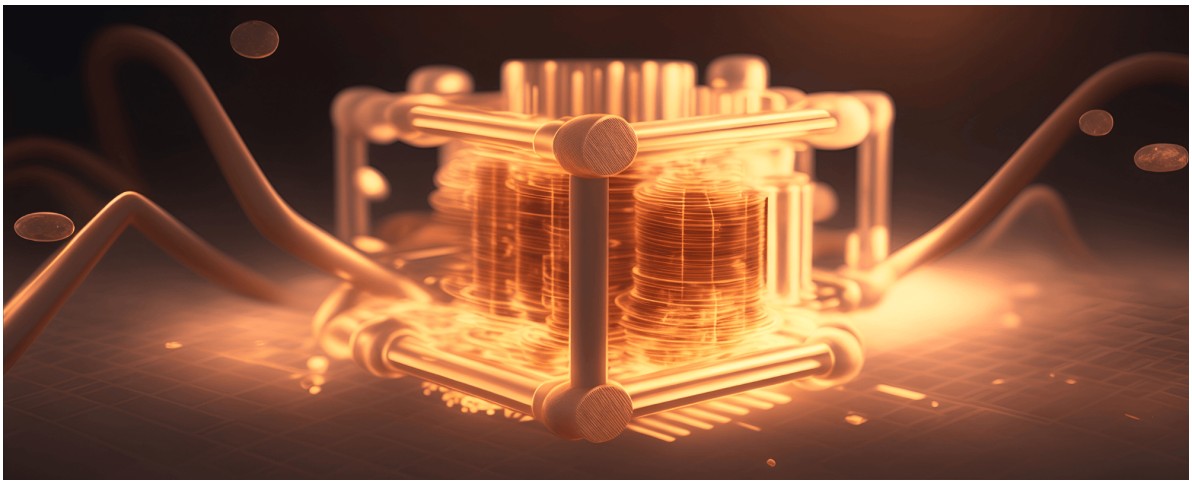
LA SEGONA REVOLUCIÓ QUÀNTICA

Física quàntica i informació: noves tecnologies per al segle XXI

Ignacio Cirac, Antonio Acín



Representació abstracta d'un ordinador quàntic amb partícules. Conceptualització: Luisa Quiroga

La informació és un concepte clau en la nostra societat, que té un impacte molt directe en el nostre dia a dia: des que ens llevem fins que ens fiquem al llit, s'intercanvien milers de missatges per internet o les xarxes de dades mòbils, i també s'executen milers d'operacions, de més o menys complexitat, en els diferents dispositius processadors d'informació, des de supercomputadors fins als nostres mòbils mateixos. La informació ha modificat de tal manera la forma en què vivim i convivim que sovint es coneix la nostra societat com la societat de la informació. La importància i l'impacte d'aquest concepte són fàcils d'entendre si es té en compte que multitud de llocs de treball, empreses, inversions i decisions polítiques giren entorn de la informació.

Totes les aplicacions d'informació operen en bits, que no són més que la seva unitat bàsica i que poden prendre dos valors: 0 o 1. La nostra connexió d'internet a casa o a la feina, la capacitat de memòria del nostre mòbil o la velocitat del processador del nostre portàtil: tot es mesura en bits. Un ordinador no és més que un dispositiu que pren informació codificada en bits, hi realitza operacions seguint els passos descrits en un algoritme i ens torna el resultat en bits. Quan enviem un correu electrònic a un amic a l'altra punta del planeta, la informació es transmet en bits codificats en llum, que s'envien a través d'una fibra òptica.

La física quàntica va ser una altra de les revolucions que ens va oferir el segle XX. És el formalisme que explica tots els fenòmens microscòpics que ens envolten. En tenir a veure amb el món d'allò més petit, el seu impacte en la nostra societat no és tan evident a primera vista. Tanmateix, aquesta conclusió és incorrecta, perquè és superficial. D'una banda, i des d'un àmbit fonamental, les prediccions de la física quàntica van suposar un canvi radical en la comprensió de la naturalesa, ja que són, en molts aspectes, molt diferents de les prediccions de la fins aleshores imperant física newtoniana. D'altra banda, des d'un àmbit més aplicat, la física quàntica ha estat i és crucial per comprendre els materials, la química i l'estructura molecular i, per tant, gran part de la ciència i la tecnologia modernes. Aplicacions com el làser, que s'utilitza des de per llegir el codi de barres al supermercat fins per a complexes operacions quirúrgiques, o el transistor, que és fonamental per al funcionament de qualsevol ordinador, van ser només possibles gràcies a la comprensió del món microscòpic que va proporcionar la física quàntica.

Partícules quàntiques per processar i transmetre informació: canvi de paradigma

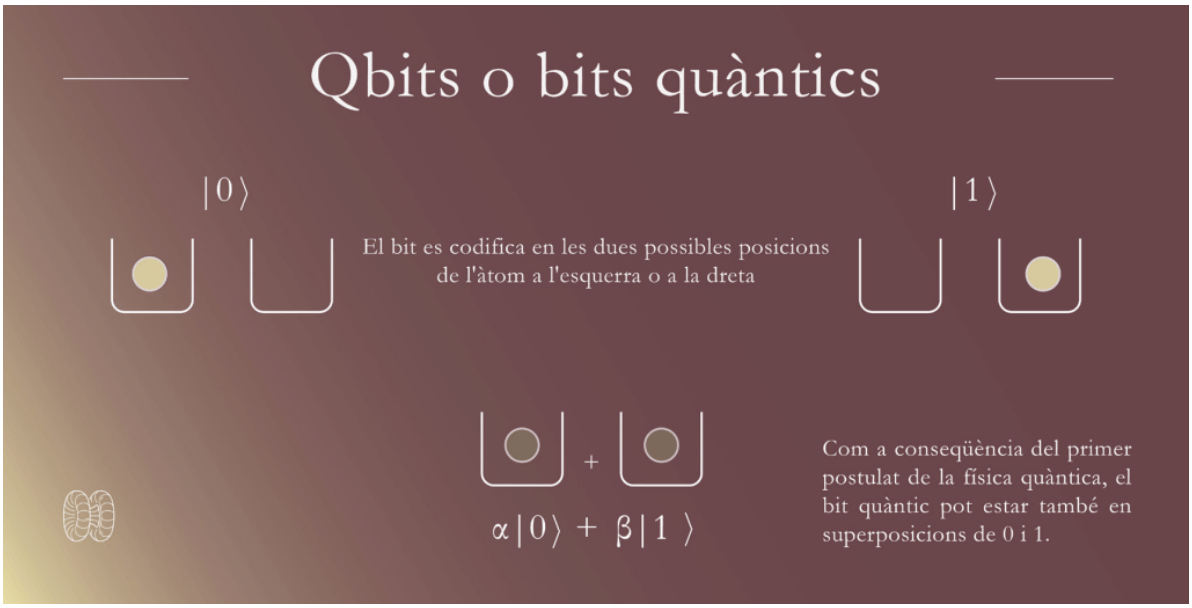
Ja fa unes quantes dècades, diversos investigadors van començar a plantejar-se què passaria si es combinessin la informació i la física quàntica. Després d'haver llegit els paràgrafs anteriors, la pregunta pot semblar fins i tot senzilla i natural: què passaria si utilitzéssim partícules quàntiques, com els àtoms o els fotons de llum, per transmetre i processar informació? Dit d'una altra manera: què passa si emmagatzemem els bits en partícules quàntiques? Però en aquell temps, i malgrat que era una pregunta molt estimulant des d'un punt de vista conceptual i teòric, era una possibilitat propera a la ciència-ficció, tenint en compte l'estat de les tecnologies. Tanmateix, les tecnologies de la informació han avançat de manera vertiginosa en les últimes dècades, i idees que semblaven més pròpies de la ciència-ficció s'han convertit en realitat. En particular, ja es té el coneixement i les tècniques per emmagatzemar bits en partícules quàntiques com els àtoms o fotons. Què podem esperar, llavors, de la combinació de la informació i la física quàntica? Aquesta és la pregunta principal que la nova disciplina de les ciències i tecnologies de la informació quàntica busca respondre.

Es va comprendre relativament aviat que utilitzar bits codificats en partícules quàntiques obria noves oportunitats per processar i transmetre informació. El mer fet de col·locar un bit en una partícula quàntica ja donava com a resultat una cosa diferent de la que coneixíem. Considerem, per exemple, una possible realització d'un bit a través d'un àtom que pot estar en dues posicions, tal com es pot veure a la imatge: quan és a l'esquerra, el valor del bit és 0, i quan és a la dreta, el valor és 1. Ara obrim qualsevol llibre de text de física quàntica. No ens hem d'espantar, ni fa falta llegir gaire: n'hi ha prou amb arribar al primer postulat de la teoria, que acostuma a aparèixer a les primeres pàgines. Recordem que els postulats d'una teoria no es discuteixen, sinó que s'accepten.

> Les tecnologies de la informació han avançat de manera vertiginosa

> en les últimes dècades, i idees que semblaven més pròpies de la ciència-ficció s'han convertit en realitat. Actualment ja tenim el coneixement i les tècniques per emmagatzemar bits en partícules quàntiques com els àtoms o els fotons

Doncs bé, el primer postulat de la física quàntica ens diu que si una partícula quàntica pot estar en dos estats, també pot trobar-se en un estat que és la superposició dels dos estats. El concepte de superposició és difícil d'assimilar, ja que les superposicions tenen lloc en el món microscòpic, dels àtoms i les molècules, que no veiem amb els ulls, ni sentim, ni podem tocar; en el món en el qual vivim, que sí que percebem, desapareixen. No existeix, per tant, una analogia que puguem utilitzar per explicar la superposició: és una cosa molt especial d'aquest món d'allò més petit. Tanmateix, el fet que un concepte sigui difícil d'assimilar no significa que no sigui el correcte per descriure la naturalesa. I, de fet, el concepte de superposició quàntica és un dels ingredients que s'utilitzen per explicar els experiments a escala microscòpica. Tornem ara al nostre bit codificat en la partícula quàntica: quines implicacions té el postulat de les superposicions? De la seva aplicació s'entén que el bit quàntic, també conegut com a qbit, és diferent del bit utilitzat fins ara, el bit clàssic, ja que pot estar en els dos valors habituals de 0 i 1, però també en qualsevol superposició d'aquests valors. La unitat bàsica d'informació quàntica, el qbit, és, per tant, més ric que el seu anàleg clàssic.



Representació gràfica dels qbits o bits quàntics.

Els ordinadors quàntics

A partir d'aquesta observació, val la pena revisitar tots els usos que fem de la informació i veure com es modifiquen sota els fenòmens de la física quàntica, com per exemple les

superposicions esmentades. Com podem calcular i resoldre problemes quan els codifiquem en bits quàntics? Aquesta pregunta porta de manera immediata a la idea de l'ordinador quàntic. Què és un ordinador quàntic? Per respondre a aquesta pregunta, és útil recordar de nou què és un ordinador clàssic: una màquina que agafa informació codificada en bits, sobre els quals fa un seguit de transformacions per resoldre un problema, la solució dels quals ens torna de nou en bits. Encara que pugui semblar obvi, un ordinador quàntic no és res més que la translació d'aquesta idea a un entorn quàntic: una màquina que és capaç de processar informació en bits quàntics per resoldre problemes. La diferència, tanmateix, rau en el fet que aquest processament es porta a terme utilitzant els fenòmens de la física quàntica, que no tenen anàleg al nostre món macroscòpic clàssic i que, per tant, són inaccessibles als nostres ordinadors clàssics actuals. És a dir, l'ordinador quàntic pot utilitzar més operacions, té a la seva disposició més eines per resoldre problemes complexos i, en conseqüència, pot arribar a proporcionar solucions a aquests problemes de manera molt més eficient. A aquesta situació se la coneix també com a avantatge quàntic (en anglès, *quantum advantage*). Aquest fet no s'ha d'interpretar com que tots els problemes es resoldran de manera més eficient en un ordinador quàntic i, de fet, existeixen problemes per als quals un ordinador quàntic i un de clàssic ofereixen el mateix rendiment. Però, alhora, es coneixen altres problemes per als quals sí que s'obté un avantatge computacional quàntic.

Seguint amb aplicacions de computació, un camp molt actiu i de gran actualitat és el de l'aprenentatge automàtic (en anglès, *machine learning*), on s'entrenen ordinadors amb moltes dades perquè aprenguin i ens permetin resoldre problemes rellevants. Com aprèn un ordinador quàntic? Aquesta és, de nou, una pregunta fonamental amb potencials aplicacions pràctiques: és el que busca respondre l'aprenentatge automàtic quàntic.

Criptografia quàntica

Però sabem que la informació s'utilitza per a milers d'aplicacions més enllà de la computació. Per exemple, per establir una xarxa de comunicacions a escala global, internet, on els bits són transmesos a qualsevol part del planeta. Quina seria l'estructura d'un internet quàntic, on l'objectiu és transmetre bits quàntics entre dos punts qualssevol? Quines són les lleis de la comunicació quàntica? I un aspecte clau en les comunicacions actuals és el de la privacitat: gairebé tan important com el fet de poder enviar informació d'un lloc a un altre és poder fer-ho de manera segura, per tal que un possible espia o enemic no tingui accés als missatges que s'envien. El camp de la criptografia ens proporciona les eines per dissenyar mètodes de transmissió privada. En aquest cas, els bits quàntics tornen a obrir noves possibilitats per a l'encriptació d'informació i permeten dissenyar els anomenats *protocols de criptografia quàntica*, que proporcionen un nou tipus de seguretat basada en les lleis de la física quàntica.

Podem continuar enumerant tots els possibles usos de la informació en la nostra societat i intentar entendre com es veuen afectats per les lleis de la física quàntica. No ho farem en aquesta introducció, perquè no és el seu objectiu, i perquè la resta del monogràfic de la revista IDEES presenta diferents articles que analitzen moltes d'aquestes possibles

aplicacions. Algunes, com els ordinadors o la comunicació quàntica, són molt naturals; d'altres són més especulatives. Per exemple, els ordinadors s'utilitzen actualment per compondre música, per la qual cosa podem plantejar-nos com generar música utilitzant efectes quàntics. Les contribucions d'aquest monogràfic de la revista IDEES serveixen, per tant, per presentar una visió més detallada i completa del camp.



Conclusions

Ens agradaria concloure aquesta introducció amb dos missatges. El primer hauria de ser clar: la informació és un concepte crucial en la nostra societat i la física quàntica ens proporciona noves eines per al seu processament i transmissió. Aquest missatge ja ha estat assimilat a escala mundial i s'estan duent a terme importants iniciatives i inversions per part de grans i petites empreses, o entitats governamentals. En el nostre entorn local, la Comissió Europea va llançar ja fa uns anys el projecte Quantum Flagship, una iniciativa paneuropea en tecnologies quàntiques. Estem en un moment molt interessant, de gran activitat, en el qual tots els actors rellevants treballen de manera conjunta per entendre com poden explotar tot el potencial de les tecnologies quàntiques.

No obstant això, existeix una gran complexitat a l'hora d'operar amb superposicions quàntiques: qualsevol aplicació d'informació quàntica, com per exemple un ordinador quàntic, fa operacions en bits quàntics. Per obtenir un avantatge és necessari, si bé no suficient, que aquests bits estiguin en estats de superposició. Tanmateix, a la pràctica, mantenir les superposicions és complicat, ja que qualsevol interacció no controlada amb l'entorn les pot destruir. Aquesta fragilitat dels efectes quàntics explica per què el desenvolupament de les tecnologies de la informació quàntica encara ha de resoldre importants desafiaments.

> Gairebé tan important com poder enviar informació d'un lloc a un altre és poder fer-ho de manera segura. La criptografia quàntica obre noves possibilitats per a l'encriptació d'informació i permet dissenyar protocols que proporcionen un nou tipus de seguretat

El segon missatge és una crida a un optimisme prudent o a una prudència optimista. Preparar, manipular, emmagatzemar i transmetre qbits és molt més complicat que en el cas dels bits clàssics. Si el bit quàntic deixa d'estar en una superposició, es converteix en un bit clàssic que només pren els valors de 0 o 1, i es perd qualsevol avantatge quàntic. Però mantenir les superposicions és una tasca complexa, ja que el soroll i les interaccions no controlades amb l'entorn les destrueixen. És necessari, per tant, preparar i processar els qbits en un entorn aïllat de l'exterior, per exemple, a molt baixa temperatura, i que puguem manipular de manera controlada. Aquí rau el gran desafiament tecnològic. Això explica per què, malgrat anys d'esforç, els ordinadors quàntics o esquemes de comunicació quàntica existents presenten encara importants desafiaments que en limiten la implementació pràctica. El camí no és senzill i és ple d'obstacles. Però la motivació i l'objectiu final són clars, i existeixen diferents resultats que demostren que les tecnologies de la informació quàntica permetran resoldre problemes que en l'actualitat limiten el nostre progrés i benestar com a societat.



Ignacio Cirac
Juan Ignacio Cirac Sasturáin és director de la Divisió Teòrica de l'Institut Max Planck d'Òptica Quàntica de Garching (Alemanya) i professor honorari de la Universitat Tècnica de Múnic. Doctor en Ciències Físiques per la Universitat Complutense de Madrid, és especialista en tecnologies quàntiques i un dels experts amb més reconeixement mundial en l'àmbit de la computació quàntica. És membre de les acadèmies de ciències espanyola, alemanya i bavaresa. Ha rebut nombrosos premis i reconeixements, entre els quals el Premi Príncep d'Astúries, les medalles Benjamin Franklin, Max Planck i Niels Bohr, el Premi BBVA Fronteres del Coneixement, el guardó en Computació Quàntica de la Fundació Micius i el Premi Wolf, considerat l'avantsala del Nobel. Les seves investigacions han sigut crucials per avançar en la teoria que sustenta el desenvolupament dels ordinadors quàntics.



Antonio Acín
Antonio Acín Dal Maschio és professor ICREA a l'Institut de Ciències Fotòniques (ICFO), on dirigeix el grup de Teoria de la Informació Quàntica. Doctor en Ciències Físiques per la Universitat de Barcelona, és especialista en tecnologies quàntiques. La seva feina d'investigació ha estat reconeguda per quatre beques del Consell Europeu de Recerca (European Research Council, ERC). Des de l'any 2016, dirigeix la Càtedra AXA en Ciències de la Informació Quàntica.