Recursos de física

EL RACÓ OBSCUR: LA QUÀNTICA PASSA A L'ACCIÓ? L'ORDINADOR QUÀNTIC

XAVIER JAÉN[1]

En el racó obscur del número 19 vam mirar d'explicar alguns dels fonaments de la mecànica quàntica i com aquesta comporta uns canvis de paradigma en conceptes que fins fa poc semblava que estaven només supeditats a la filosofia. En aquest racó mirarem d'entendre com alguns d'aquests conceptes quàntics es poden utilitzar en enginys amb una capacitat d'incidència sobre la nostra societat que va més enllà de la que pot tenir un debat filosòfic. Mirarem d'entendre com treballa un ordinador quàntic i quina és la raó del seu protagonisme imminent.

Introducció

Al segle XX la física va viure simultàniament dues revolucions que trasbalsaren completament els seus fonaments. La mecànica relativista i la mecànica quàntica. També és al segle XX, especialment en la segona meitat, quan s'inicia una relació de mútua necessitat entre ciència i tecnologia que encara no sabem on ens portarà. Durant el segle XX la tecnologia utilitza molt la física del segle XIX. L'èxit de la relativitat i la quàntica rau en el fet que expliquen molts fenòmens observats. Però la tecnologia no preveu, excepte en alguns pocs cassos, la possibilitat de produir algun enginy que empri aquestes teories. Durant el segle XX la relativitat i la quàntica nodreixen els grans debats filosòfics al voltant de qüestions cosmològiques, paradoxes temporals, l'atzar, el realisme... però res d'això sembla que pugui incidir en les nostres vides si no és per la via del pur plaer de l'intel·lecte.

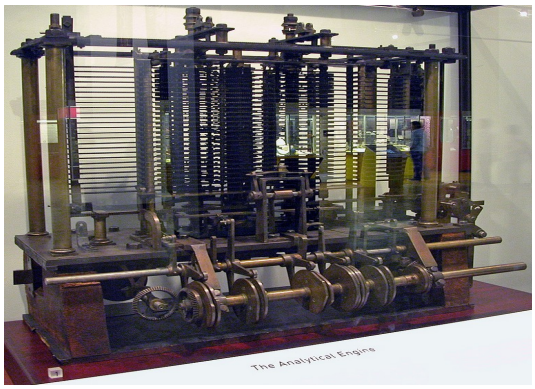


Fig. 1: Charles Babbage (Gran Bretanya, 1791–1871) fou un matemàtic anglès i protocientífic de la computació. Babbage fou dels primers que va tenir la idea de crear un ordinador. A la imatge podem veure reproducció d'una part de l'Analytical Engine, ideat per Babbage i basat en mecanismes (no elèctric), tal com es mostra al Science Museum de Londres.

Al segle XXI aquest panorama està canviant de manera dràstica. Aquests canvis ja s'anaven gestant anys abans. La ciència necessitava cada cop més tecnologia per avançar. A la vegada, la tecnologia ha esdevingut prou precisa i sofisticada per "exigir" a la ciència que es desenvolupi a favor seu.

En el RACÓ OBSCUR del número 13 ja vàrem parlar del GPS (*global positioning system*), una tecnologia que tots fem servir i que es recolza en la relativitat. Un altre dels camps en què la tecnologia està aprofitant intensament la física és el de la computació. Concretament, la mecànica quàntica. Richard Feynman, el 1982, en la *First Conference on the Physics of Computation*, va deixar anar la famosa frase: "La natura és quàntica, maleïda siga! Per tant, si la volem simular, necessitarem un ordinador quàntic." El que llavors era una possibilitat teòrica en pocs anys ha esdevingut pràctica.

En aquest RACÓ OBSCUR intentarem entendre què és un ordinador quàntic. Què fa que un ordinador sigui quàntic i que esdevingui un giny tan revolucionari si a la fi el que fa és calcular allò que nosaltres li ma-

1 Professor de física del Dept. de Física de la Universitat Politècnica de Catalunya (UPC).
Adreça electrònica: Xavier.Jaen@upc.edu

nem que calculi amb les matemàtiques de sempre?

Veurem primer com calcula un ordinador clàssic. Veurem quins són els elements essencials d'un ordinador clàssic i com els combina per executar un algorisme. Els elements d'un ordinador clàssic estan fets d'objectes clàssics. És conceptualment possible fer un ordinador clàssic emprant interruptors de corrent i bobines. Quins canvis substancials d'aquests elements apareixen quant els substituïm, els materialitzem, per objectes quàntics? En un ordinador quàntic els interruptors de corrent i les bobines queden substituïts per objectes de mida atòmica, que es comporten segons la mecànica quàntica. Quines repercussions tenen aquests canvis en el funcionament de l'ordinador?

Anem per feina!

Els bits i la computació clàssica

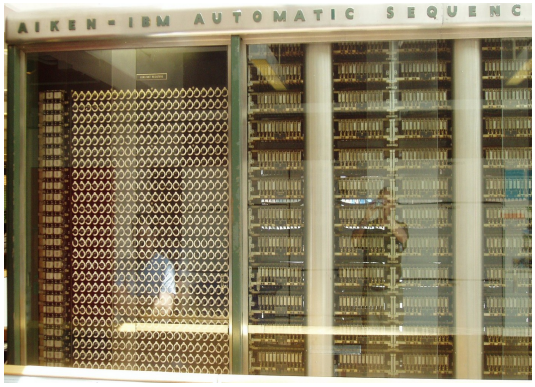


Fig. 2: L'IBM Automatic Sequence Controlled Calculator (ASCC), anomenat Mark I, era una computadora electromecànica de propòsit general que es va utilitzar durant l'última part de la Segona Guerra Mundial.

En lògica i teoria de la informació un ***bit*** és la unitat mínima d'informació. Un bit pot tenir només dos estats, que se solen simbolitzar amb un 0 i un 1. Dins la física clàssica trobem múltiples materialitzacions dels bits. Una bombeta, que pot estar encesa (estat 1) o apagada (estat 0). Un imant o brúixola, que pot estar en la direcció i sentit d'un camp magnètic (0) o en sentit contrari (1). Un interruptor, que pot estar obert (0) o tancat (1). També es poden fer materialitzacions mecàniques dels bits, tal com ho va haver de fer Babbage. Charles Babbage (Gran Bretanya, 1791–1871) fou dels primers que va tenir la idea de crear un ordinador. Els seus ginys, estrictament mecànics (no elèctrics), no es van arribar a realitzar a causa del baix nivell tecnològic de l'època (vegeu la figura 1). Nosaltres estem pensant en les primeres realitzacions electromecàniques d'un ordinador, com l'Automatic Sequence Controlled Calculator (ASCC) d'IBM, del 1944 (vegeu la figura 2).

Realitzarem un bit clàssic amb un interruptor que deixa o no passar un corrent elèctric. Pot tenir dos estats: obert  o 0, o tancat o 1. I què podem fer amb un bit? Emmagatzemar dades. Molt poques dades. Per exemple: 0 o 1. a o b. Blanc o negre. SÍ o NO. Amb un sol bit podem emmagatzemar només una dada d'un total de dues. Diem que és la unitat mínima d'informació perquè per saber quina dada representa el bit n'hi ha prou amb una sola pregunta. Si el bit representa blanc o negre, podem preguntar "és aquest bit blanc?" i amb la resposta ja sabem si és blanc o és negre.

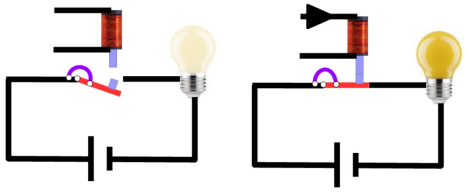


Fig. 3: Un bit i el sistema de lectura i canvi del seu valor. A l'esquerra en l'estat 0 i a la dreta en l'estat 1. També és una porta YES: $Y[0]=0$ i $Y[1]=1$

Podem agrupar bits i emmagatzemar més dades. Un conjunt de bits ordenats per emmagatzemar dades formen un ***registre***. Si tenim dos bits ordenats podem emmagatzemar una dada del conjunt 00, 01, 10 o 11. Una entre $4=2^2$ dades diferents. Si en tenim tres podem emmagatzemar una de les dades del conjunt 000, 001, .

$010, 011, 100, 101$ o 111. Una entre $8 = 2^3$ dades diferents. En general, amb N bits podem emmagatzemar una entre 2^N dades diferents.

Però amb això no n'hi ha prou. També hem de saber llegir aquestes dades... i canviar-les ! Pensem que el fet de tenir un bit *entre les mans* no vol dir que sapiguem quina dada representa: 0 o 1. És com si el bit, entès ara com l'interruptor, tingues una coberta,  , que no en deixés veure què hi ha ha dins. A més, en general, no serem nosaltres qui en vulguem saber l'estat. Necessitem traduir aquests estats en termes de corrent elèctric per tal de poder fer-ne operacions. Si, finalment, som nosaltres els qui en volem saber l'estat, podem utilitzar algun senyal visual. Necessitem un lector de bits adaptat al cas. Com que el nostre bit és un interruptor de corrent, necessitem també un flux de corrent i, si ens cal, un detector d'aquest corrent, una bombeta  , que ens permeti visualitzar l'estat: bombeta apagada $= 0$, bombeta encesa $= 1$. Per canviar l'estat del bit podem fem servir un sistema bobina-molla de retorn que s'accioni amb corrent. Si per la bobina no hi passa corrent, l'interruptor és obert i, si hi passa corrent, l'interruptor és tancat. A la figura 3 podem veure un bit amb tot el necessari per tal que sigui operatiu.

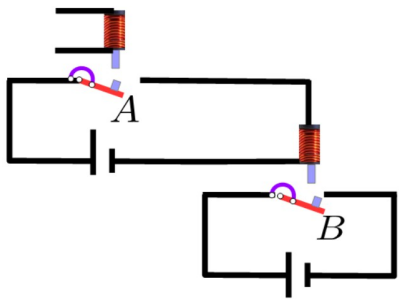


Fig. 4: Un bit A és comandat externament a la vegada que comanda un altre bit B. Si A passa de 0 a 1 B també ho farà.

Fixem-nos que, tal com hem dissenyat els bits, podem ser nosaltres els qui fem o no passar corrent per la bobina, de manera que canviem l'estat del bit, o pot estar comandat per un altre bit, tal com es veu a la figura 4.

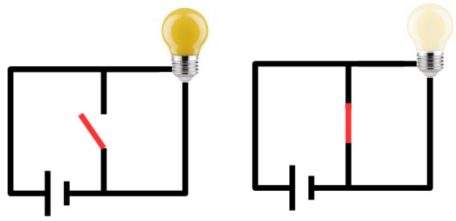


Fig. 5: La porta lògica NOT. No hem explicitat l'electroimant. Utilitzant els símbols de la lògica: $\overline{0} = 1$ i $\overline{1} = 0$.

Un cop disposem de bits podem construir una ***porta lògica***. Una porta lògica és la materialització d'un connector lògic. Un ***connector lògic*** és una operació lògica que té com a ingredients un, dos o més bits i que dona com a resultat un bit. La porta lògica més senzilla és la porta *YES*. De fet un bit és, ell mateix, una porta *YES*.

A la figura 3, quan l'estat del bit és 0 la resposta (mesura feta amb la bombeta) és 0 i quan l'estat del bit és 1 la resposta és 1. La porta *YES* es confon amb un bit. Si utilitzem el símbol $\mathbf{Y}$ per representar l'operador associat a la porta *YES*, el que fa és no fer res: $\mathbf{Y}(0) = 0$ i $\mathbf{Y}(1) = 1$. És per això que no s'acostuma a escriure cap símbol per a la porta *YES*.

Un altre exemple és la porta *NOT*. En podem veure la materialització a la figura 5. Quan el bit és 0, la bombeta diu 1. Quan el bit és 1, la bombeta diu 0. Si fem servir el símbol $\mathbf{N}$ per a *NOT*, tindrem $\mathbf{N}(0) = 1$ i $\mathbf{N}(1) = 0$. També es pot escriure amb la barra sobre el valor. Vegeu la figura 5.

Un exemple de porta més complex és la porta *AND*, que admet una entrada de dos bits i implementa el connector lògic "i". En lògica se simbolitza amb $\wedge$. A la figura 6 podem veure la porta *AND* i el seu funcionament. Si emprem el símbol $\mathbf{A}$ tenim:

$\mathbf{A}(0,0)=0$, $\mathbf{A}(0,1)=0$, $\mathbf{A}(1,0)=0$ i $\mathbf{A}(1,1)=1$

Un resultat important de la lògica és que en tenim prou amb les portes *YES*, *NOT* i *AND* per construir totes les altres portes. Això, resumint moltíssim, vol dir que amb els conceptes explicats fins ara ja podem, potencialment, escriure qualsevol operació matemàtica i traduir-la en un circuit perquè es pugui executar.

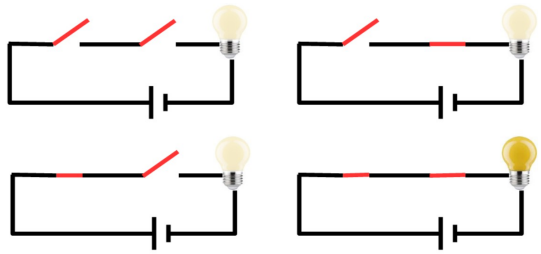


Fig. 6: La porta lògica AND. No hem explicitat els electroimants. Podem veure la resposta de la porta respecte dels estats dels dos bits que la componen. Utilitzant els símbols de la lògica: $(0)\wedge(0)=(0)$, $(1)\wedge(0)=(0)$, $(0)\wedge(1)=(0)$ *i* $(1)\wedge(1)=(1)$

A partir d'agrupacions de bits o **registres** que emmagatzemaran la informació de l'entrada obtindrem, un cop executades les operacions, uns altres bits que emmagatzemaran la informació de la sortida. Tot això requereix un cert ***temps*** de càlcul i un cert ***espai*** de memòria (nombre màxim de bits que s'empren en l'operació). No diem que això sigui senzill. El camí que cal seguir és, si fa no fa, el camí que ha seguit la computació clàssica. Un ordinador clàssic consta d'un nombre gran de bits. Tots estem acostumats a emprar els bytes i no els bits. Un bit ($1\,\mathrm{b}$) és la unitat mínima d'informació. Un byte ($1\,\mathrm{B}$) és un conjunt ordenat d'un nombre especificat de bits. El valor estàndard és $1\,\mathrm{B}=8\,\mathrm{b}$. Els bytes formen registres que se situen en llocs coneguts del circuit o *direccions de memòria*, de manera que quan sigui necessari es puguin llegir per fer-ne operacions amb les portes lògiques, etc. Tot això es complica sobretot pels nombres que es maneguen. Actualment no hi donem gaire importància. Una quantitat d'informació *petita*, com la continguda en una novel·la, es pot emmagatzemar en $1\,\mathrm{MB}$, 1 megabyte, que resulta que són 8 milions de bits. Ja s'entén que el problema més que lògic o conceptual serà *tecnològic*. No podem anar soldant un per un 8 milions d'interruptors i bobines per fer un circuit que emmagatzemi una sola novel·la! La història de la computació està íntimament lligada a la història de la manipulació i miniaturització dels bits. L'avenç en aquest camp es dona aproximadament a partir de la segona meitat del segle XX.

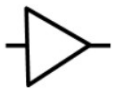
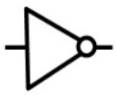
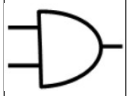
Porta	Símbol	Operació	Taula de veritat
YES		x	$0 \mid 0$ $1 \mid 1$
NOT		$\overline{x}$	$0 \mid 1$ $1 \mid 0$
AND		$x\wedge y$	$0\ 0 \mid 0$ $0\ 1 \mid 0$ $1\ 0 \mid 0$ $1\ 1 \mid 1$

Fig. 7: Nom de la porta, símbol, operació i taula de veritat de les tres portes bàsiques.

Fig. 8: Ada Lovelace, (Londres, 10 de desembre de 1815-27 de novembre de 1852), va ser la primera programadora en la història dels computadors.

En canvi, la informàtica va començar molt abans que la computació. Hom pot imaginar, i escriure en un paper, ***algorismes*** —així s'anomenen el conjunt d'instruccions que un ordinador és capaç d'interpretar i executar— sense que s'hagi inventat o realitzat encara la màquina que els executi. Tant és així que la primera programadora, tal com avui entenem el terme, va ser Ada Lovelace (Londres, 1815–1852). Curiosament Lovelace va treballar amb Babbage (vegeu la figura 1).

Però sortosament no ens caldrà endinsar-nos en els entrellats de l'algorísmia. El nostre problema és de *temps* i d'*espai*. Podem resumir el que hem fet fins ara amb l'expressió: *tot penja d'un bit*!

Encara que estiguem fent física clàssica podem utilitzar una notació pròxima a la quàntica. Serà exagerada des del punt de vista de la física clàssica, però ens ajudarà a entendre un xic més les diferències amb la quàntica.

Apropant-nos a la notació quàntica, un bit, un bit clàssic, només pot estar en l'estat $|0\rangle$ o en l'estat $|1\rangle$. Si tenim un registre de 2 bits, l'estat pot ser $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Si tenim un registre de 3 bits, $|000\rangle$, $|001\rangle$, $|010\rangle$, etc.

Les portes lògiques es poden representar com a operadors que passen d'un estat a un altre. La porta *YES* serà $\mathbf{Y}|x\rangle = |x\rangle$. La porta *NOT*, $\mathbf{N}|x\rangle = |1-x\rangle$. La porta *AND*, $x \neq 1 \vee y \neq 1 : \mathbf{A}|xy\rangle = |0\rangle$, $\mathbf{A}|11\rangle = |1\rangle$.

Encara que en física clàssica és una obvietat, un cop s'acaba el càlcul, emprant els operadors o portes lògiques, necessitem "extreure'n" el resultat. D'això en diem *mesurar* o *observar*. En el cas d'un bit, això és determinar l'estat no conegut $|x\rangle$ del bit de sortida. La probabilitat que un bit clàssic en un estat $|x\rangle$ estigui en l'estat $|y\rangle$, on x i y poden ser només 0 o 1, es pot representar com $\|\langle x|y\rangle\|^2$. En física clàssica, $\|\langle x|y\rangle\|^2$ només pot donar 0 o 1. Així, per determinar l'estat del bit no conegut $|x\rangle$ podem fer $\|\langle x|0\rangle\|$. Si ens dona 1, l'estat és $|0\rangle$ i, si ens dona 0, l'estat és $|1\rangle$. Aquest procés de mesura clàssica no altera en absolut l'estat del bit original $|x\rangle$ i, en la pràctica, en el cas de l'interruptor, es redueix a veure si passa o no corrent. L'operador que mesura si passa o no corrent el podem representar amb $\mathbf{M}$, en què els valors mesurats possibles seran $+$ si passa i $-$ si no passa: $\mathbf{M}|1\rangle = +|1\rangle$ i $\mathbf{M}|0\rangle = -|0\rangle$. $\langle x|\mathbf{M}|x\rangle$ representa el valor esperat del pas del corrent de l'estat $|x\rangle$. Només té dos valors possibles, $\langle 1|\mathbf{M}|1\rangle = +1$ i $\langle 0|\mathbf{M}|0\rangle = -1$.

Si tenim registres de més d'un bit, podem procedir d'una manera semblant. Així, per a 3 bits tindrem estats del tipus $|s_1 s_2 s_3\rangle$, per exemple $|110\rangle$, i si volem saber si l'estat $|s_1 s_2 s_3\rangle$ és $|110\rangle$ farem $\|\langle 011|s_1 s_2 s_3\rangle\| = \|\langle 0|s_1\rangle\| \, \|\langle 1|s_2\rangle\| \, \|\langle 1|s_3\rangle\|$. Les mesures corresponents seran mirar si al primer bit $|s_1\rangle$ no hi passa corrent, $\langle s_1|\mathbf{M}|s_1\rangle = -1$, i als altres dos sí, $\langle s_2|\mathbf{M}|s_2\rangle = +1$ i $\langle s_3|\mathbf{M}|s_3\rangle = +1$.

Un exemple d'algorisme clàssic

Un problema concret de computació clàssica és trobar un registre específic de 3 bits del conjunt de $N = 8$ registres possibles. Per exemple, si tenim els registres

$$|b_1\rangle = |000\rangle, \;\; |b_2\rangle = |010\rangle, \;\; |b_3\rangle = |011\rangle, \;\; |b_4\rangle = |111\rangle,$$
$$|b_5\rangle = |101\rangle, \;\; |b_6\rangle = |100\rangle, \;\; |b_7\rangle = |110\rangle, |b_8\rangle = |001\rangle$$

què podem fer per trobar el registre b_x que estigui en l'estat $|011\rangle$ si no coneixem el valor dels registres b_i? No cal fer cap operació que involucri portes lògiques. Anirem **mesurant** $\|\langle 011|b_i\rangle\|$ fins que trobem 1 com a resultat. És clar que haurem de fer un màxim de $N = 8$ mesures o operacions simples. Si ho fem moltes vegades veurem que hem de fer, de mitjana, unes $\frac{N+1}{2} = \frac{8+1}{2} \approx 4$ mesures, ja que la probabilitat que ens en sortim amb 1 mesura és $\frac{1}{N}$, amb 2 mesures és $\frac{2}{N}$, amb 3 és $\frac{3}{N}$ i així fins a N mesures, en què segur que ens en sortim. Sumant aquestes probabilitats $\sum_{i=1}^{N} \frac{i}{N}$ obtenim el resultat. Pel que

ens interessa podem dir que el nombre de mesures que cal fer per trobar un bit concret en un conjunt de N bits és d'ordre N. Aquest fet determinarà el $temps$ de càlcul que empri l'ordinador encarregat de fer la feina.

Els qbits i la computació quàntica

Si en lloc d'utilitzar *material clàssic* en la realització del concepte de bits utilitzem *material quàntic*, ens trobarem amb alguna sorpresa, com tot seguit veurem.

Encara que hi ha moltes maneres de concebre i realitzar, amb entitats quàntiques, estats binaris $|0\rangle$ i $|1\rangle$, la més coneguda és la utilització dels estats de spin dels electrons. Ja en vàrem utilitzar en el **Racó obscur** del número 19. Resumint: l'spin dels electrons és l'anàleg al moment angular d'un cos degut a la rotació intrínseca, com la Terra, portada al terreny de les partícules quàntiques. Quan mesurem el valor de l'spin dels electrons en una direcció determinada de l'espai, obtenim sempre el mateix mòdul de spin i només es diferencia el sentit de la rotació, horària o $-$ o antihorària o $+$. Això pot voler dir, com en el cas clàssic, que l'spin de l'electró ja està en aquesta direcció i sentit, però en la mecànica quàntica en general no és així. Podem representar els dos estats bàsics de l'spin de l'electró en la forma $|0\rangle$, corresponent a $+$, i $|1\rangle$, corresponent a $-$. Deixant de banda el seu origen físic, si els estats $|0\rangle$ i $|1\rangle$ de l'electró tinguessin un comportament clàssic podríem emprar-los per realitzar un bit exactament igual al que hem fet amb un interruptor. De fet, això es pot fer si només aprofitem una petita part de les propietats de l'spin de l'electró. És possible fer un ordinador clàssic emprant només una petita part de la mecànica quàntica. Això no és estrany si tenim en compte que la mecànica quàntica és una teoria més *gran* que la mecànica clàssica i, per tant, la quàntica inclou la clàssica. Però en la realització d'aquest bit clàssic fet amb els spins dels electrons ***observem*** que tenen comportaments no aprofitats en els bits usuals, com és el cas dels interruptors.

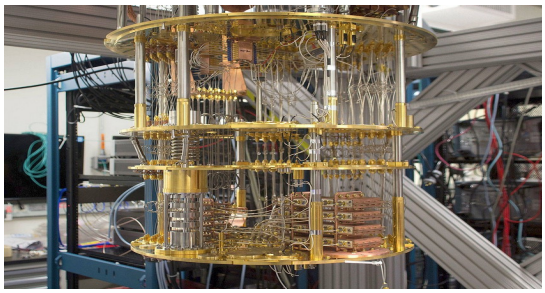


Fig. 9: Aspecte d'un ordinador quàntic d'IBM en l'actualitat. Malgrat que l'ordinador pugui tenir unes mides de nou descomunals, s'hi pot accedir usant el mòbil amb una senzilla app.

Anomenem ***qbit*** la realització en estats quàntics d'un bit. Recordem que un bit és, més enllà de la seva realització material, un concepte emprat en teoria de la informació i en lògica. Que als científics els sigui profitós promocionar un comportament físic, el del qbit, a un concepte que transcendeixi la física i parlar d'una ***lògica quàntica*** no vol dir en absolut que la ***lògica clàssica*** deixi de ser certa. En tot cas, la lògica quàntica serà una extensió convenient de la lògica clàssica. Una altra cosa és que ens agradi o ens sigui d'utilitat en la vida quotidiana a tots plegats...

A causa de les característiques de la mecànica quàntica, un qbit pot estar en un estat $|0\rangle$, en un estat $|1\rangle$ i, en general, en una superposició ponderada d'aquests dos estats! Un qbit és un estat quàntic, $|\psi\rangle$, que es pot expressar com a combinació de dos estats bàsics $|0\rangle$ i $|1\rangle$ en la forma

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \qquad (1)$$

on a_0 i a_1 són nombres complexos anomenats *amplituds de probabilitats*.

$|0\rangle$ i $|1\rangle$ actuen com una base ortonormal de vectors (com els $\hat{\imath}, \hat{\jmath}$ de la base euclidiana de vectors usual). Així, tindrem els productes

$$\langle 0|0\rangle = 1, \langle 0|1\rangle = 0, \langle 1|0\rangle = 0, \langle 1|1\rangle = 1 \tag{2}$$

La probabilitat que en mesurar $|\psi\rangle$ ens doni l'estat $|0\rangle$ o $|1\rangle$ és $\|\langle 0|\psi\rangle\|^2 = a_0 a_0^*$ i $\|\langle 1|\psi\rangle\| = a_1 a_1^*$, respectivament (amb el superíndex $*$ indiquem el complex conjugat). És clar que cal que es compleixi $a_0 a_0^* + a_1 a_1^* = 1$. Qualsevol combinació de 2 nombres complexos a_0 i a_1 que compleixi aquesta condició defineix un possible estat del qbit. Això inclou els casos $a_0 = 1$ i $a_1 = 0$, que corresponen a l'estat $|0\rangle$, i $a_0 = 0$ i $a_1 = 1$, que corresponen a l'estat $|1\rangle$. Així, és clar que un qbit és una extensió brutal d'un bit. Però abans de veure el caràcter d'aquesta extensió, avancem una mica més.

Des de l'inici i fins no fa gaire, la mecànica quàntica era una teoria l'èxit de la qual es mesurava per la quantitat de fenòmens físics que explicava. La gran majoria de persones podien prescindir-ne. Només els arribava el debat filosòfic que aquesta teoria generava. Vinga discutir si el gat de Schrödinger està viu o mort! Aquesta mena de debats encara són vigents, però a poc a poc ens hem tornat més pragmàtics. Encara que aquest pragmatisme no em fa sentir particularment còmode, l'actitud que recomanem prendre en aquest punt és també la mateixa que van prendre els pioners de la computació quàntica, i d'altres aplicacions de la mecànica quàntica, a les acaballes del segle anterior. L'expressió (1) i d'altres de semblants, més enllà de com la interpretem en termes clàssics, descriu un fet quàntic que, com altres cops ha passat en la física, pot ser estudiat des d'un punt de vista tecnològic per construir ginys que facin *quelcom*.

No és fins fa molt poc que s'ha començat a desenvolupar una tecnologia netament quàntica. En el cas que ens ocupa, aquesta tecnologia permet la realització física i la manipulació dels qbits. Actualment sabem actuar sobre els qbits canviant-ne l'estat a voluntat. Sabem també fer mesures amb les subtils restriccions que la quàntica imposa en aquest terreny i que podem resumir en:

> *La mecànica quàntica permet, i per tant només serà una qüestió tecnològica,* ***preparar*** *un qbit de la forma* $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ *amb les amplituds* a_0 *i* a_1 *que vulguem, de manera que compleix* $a_0 a_0^* + a_1 a_1^* = 1$. *Però no permet* ***mesurar*** *que l'estat del qbit que hem preparat és* $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ *sense alterar aquest estat.*

L'eficiència de la computació quàntica rau a saber aprofitar aquests marges de maniobra i, sobretot, entendre que, un cop entrades les dades *només ens cal mesurar al final del càlcul* per aconseguir el resultat d'aquest càlcul. Deixant de banda les mesures, les manipulacions que es poden fer sobre els qbits són representades en la teoria per operadors unitaris $\mathbf{U}$. Són u*nitaris* perquè el resultat d'aplicar un operador $\mathbf{U}$ a un estat com $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ complint $a_0 a_0^* + a_1 a_1^* = 1$ és $\mathbf{U}|\psi\rangle = b_0|0\rangle + b_1|1\rangle$, que ha de complir també $b_0 b_0^* + b_1 b_1^* = 1$.

Ens quedarem amb la idea que sabem fer les manipulacions sobre els qbits i sabem representar-les matemàticament.

> *El operadors unitaris sobre el qbits seran l'extensió dels operadors que representen portes lògiques sobre els bits clàssics.*

Més amunt hem quedat que un bit pot emmagatzemar ***una dada entre dues***. En general amb registres de N bits podem emmagatzemar **una** entre 2^N dades. Un qbit pot també emmagatzemar una dada

entre dues sempre que vulguem accedir (mesurar) a aquestes dades. En això no es diferencia d'un bit. Però la gran diferència entre el bit i el qbit és que ara podrem tenir un qbit en una superposició del tipus (1) que contingui ***simultàniament les dues dades entre dues***. Tenim també un marge de manipulació molt ample. Amb un sol bit clàssic, diguem $|0\rangle$, podem fer que passi de $|0\rangle$ a $|1\rangle$ o que es quedi igual. Això és tot. En canvi amb un qbit, diguem $|0\rangle$, i amb l'operador unitari adequat $\mathbf{U}$ podem fer-lo passar a qualsevol dels estats en superposició de $|0\rangle$ i $|1\rangle$: $\mathbf{U}|0\rangle = a_0|0\rangle + a_1|1\rangle$. I podem fer passar aquests nous estats a d'altres, amb la qual cosa podem provocar una cascada exponencial d'estats que ***treballen en paral·lel***.

Per tal de fer-nos una imatge, de tant en tant toca, més enllà dels qbits, posem l'exemple d'una partícula que va d'un punt A a un altre punt B. Si es tracta d'una partícula clàssica anirà de A a B passant per un únic camí C_1. Aquesta partícula podria ser una càrrega que es passeja per un circuit d'un ordinador clàssic. Diguem que aquesta partícula ***"fa" una cosa darrere l'altra.*** Ara, si la partícula és quàntica, en anar de A a B el camí quàntic pel qual es mou la partícula és una superposició de camins C_i. En anar de A a B pot ***"fer" moltes coses alhora***.

De manera semblant als bits clàssics podem, amb conjunts de qbits, construir registres quàntics que podrem manipular també amb els operadors unitaris corresponents. Amb un registre de N qbits podem emmagatzemar, no ***una*** entre 2^N com en el cas dels bits, sinó ***simultàniament*** les 2^N dades, almenys a l'efecte de manipulació interna, és a dir, que no hi podem accedir mesurant. Suposarem que sempre que utilitzem operadors unitaris aquest poden ser implementats tecnològicament amb portes quàntiques, tal com passa amb les portes clàssiques. No ens allargarem en aquest punt. És un fascinant problema tecnològic, però "només" és tecnològic. Anem directes a veure com podem dissenyar un algorisme quàntic que ens resolgui el mateix problema que hem resolt amb un l'algorisme clàssic.

Un exemple d'algorisme quàntic

L'algorisme que ens resol el problema de trobar un registre específic de 3 bits del conjunt de $N = 8$ registres possibles. Com abans, tenim els registres

$$|b_1\rangle = |000\rangle,\ |b_2\rangle = |010\rangle\,,\ |b_3\rangle = |011\rangle,\ |b_4\rangle = |111\rangle,$$
$$|b_5\rangle = |101\rangle,\ |b_6\rangle = |100\rangle,\ |b_7\rangle = |110\rangle, |b_8\rangle = |001\rangle$$

com ho podem fer, per trobar el registre b_x que estigui en l'estat $|011\rangle$ si no coneixem el valor dels registres b_i? Un algorisme quàntic senzill que resol aquest problema és el que devem a Lov Kumar Grover el 1966 i que coneixem com *algorisme de Grover*. El primer pas és construir un registre quàntic inicial $|\psi_0\rangle$ que sigui la superposició homogènia dels 8 registres bàsics b_i:

$$|\psi_0\rangle = \frac{1}{\sqrt{8}} \sum_{i=1}^{8} |b_i\rangle \tag{3}$$

Cal dir que és possible fer-ho utilitzant l'operador unitari o porta lògica quàntica de Hadamard, $\mathbf{H}$. L'operador $\mathbf{H}$ sobre els estats bàsics és

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \ \ ; \ \ \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{4}$$

Però tampoc ens cal entrar en més detalls. Només cal dir que per aplicar-lo sobre un registre bàsic, diguem $|b_1\rangle$, per produir $|\psi_0\rangle$ ens cal fer el mateix nombre d'operacions que qbits tingui el registre, en el nostre cas 3. A més, aquest registre inicial $|\psi_0\rangle$ ens servirà per a qualsevol altra cerca. El següent pas és

fer el que s'anomena *iteració de Grover*. Cada iteració consisteix en dues parts:

1) Apliquem l'operador unitari anomenat ***oracle*[2] *quàntic*** $\mathbf{O}$. $\mathbf{O}$ sobre cada $|b_i\rangle$ en canvia el signe si $|b_i\rangle$ és el que cerquem o no fa res si no és el que cerquem. En el nostre cas, en la primera iteració tindrem

$$\mathbf{O}|\psi_0\rangle = \frac{1}{\sqrt{8}}\left(|b_1\rangle + |b_2\rangle - |b_3\rangle + |b_4\rangle + |b_5\rangle + |b_6\rangle + |b_7\rangle + |b_8\rangle\right) \tag{5}$$

2) Apliquem l'operador unitari $2|\psi_0\rangle\langle\psi_0| - I$, on I és la identitat, és a dir, I no fa res.

Si $\mathbf{G} = [2|\psi_0\rangle\langle\psi_0| - I]\,\mathbf{O}$ és l'operador unitari corresponent a l'operació conjunta 1) i 2), un càlcul senzill ens mostra que el resultat en la primera iteració és

$$\mathbf{G}|\psi_0\rangle = \tfrac{1}{4\sqrt{2}}|b_1\rangle + \tfrac{1}{4\sqrt{2}}|b_2\rangle + \tfrac{5}{4\sqrt{2}}|b_3\rangle + \tfrac{1}{4\sqrt{2}}|b_4\rangle + \tfrac{1}{4\sqrt{2}}|b_5\rangle + \tfrac{1}{4\sqrt{2}}|b_6\rangle + \tfrac{1}{4\sqrt{2}}|b_7\rangle + \tfrac{1}{4\sqrt{2}}|b_8\rangle \tag{6}$$

on notem que el que ha passat és que tots els registres tenen la mateixa amplitud excepte el que cerquem, que té una amplitud més gran, $\frac{5}{4\sqrt{2}}$.

Si fem una segona iteració tindrem

$$\mathbf{G}^2|\psi_0\rangle = -\tfrac{1}{8\sqrt{2}}|b_1\rangle - \tfrac{1}{8\sqrt{2}}|b_2\rangle + \tfrac{11}{8\sqrt{2}}|b_3\rangle - \tfrac{1}{8\sqrt{2}}|b_4\rangle - \tfrac{1}{8\sqrt{2}}|b_5\rangle - \tfrac{1}{8\sqrt{2}}|b_6\rangle - \tfrac{1}{8\sqrt{2}}|b_7\rangle - \tfrac{1}{8\sqrt{2}}|b_8\rangle \tag{7}$$

on de nou veiem que l'amplitud del registre que cerquem ha tornat a créixer, $\frac{11}{8\sqrt{2}}$, respecte de la resta, que ha disminuït. Podem seguir fent més iteracions o aturar-nos aquí. Si és el cas, podem fer l'últim pas, que no és res més que mesurar l'estat resultant, amb què trobarem que, amb una probabilitat $\left(\frac{11}{8\sqrt{2}}\right)^2 \approx 94,5\%$, el registre b_3 coincideix amb el que cerquem.

Un estudi més aprofundit d'aquest algorisme ens mostra que, per a una cerca en un conjunt de $N = 2^n$ registres, el nombre d'iteracions òptim és de $\frac{\pi}{4}\sqrt{2^n}$ i la probabilitat de trobar un resultat augmenta moltíssim amb n, de manera que es pot considerar una certesa. Quant al nombre de passos a donar, resulta que és de l'ordre de $O(\sqrt{N})$, de manera que per a N gran augmenta moltíssim l'eficiència i, per tant, disminueix el temps, respecte de l'algorisme clàssic corresponent.

Hem exposat aquest algorisme perquè es pot explicar fins al final. Aquest algorisme ja mostra com aprofitant les característiques quàntiques podem augmentar l'eficiència. Algorismes més elaborats, que aprofiten, a més de la superposició quàntica, el fenomen de l'entrellaçament, donen eficiències que aug-

2 Un oracle fou la paraula usada a l'època clàssica per designar les revelacions dels deus als homes i el lloc on aquestes revelacions eren fetes. Escollir aquesta paraula en un context quàntic no és gratuït. Quan s'invoca l'oracle quàntic no podem accedir al que decideix fins al final del procés. No està al nostre abast.

menten exponencialment amb N.

L'ordinador quàntic, una revolució?

Dins el camp de la computació, els més *granadets* hem viscut sempre amb la sensació que l'ordinador que acabàvem d'adquirir seria la *repera* i veient com en molt pocs anys esdevenia una tartana que calia substituir pel nou Pentium amb doble capa i molt de *core*. Al cap de menys anys aquest últim esdevenia també una tartana. Els ordinadors anaven sempre darrere de les seves possibilitats. És en aquests últims anys que això, sembla, s'està apaivagant. Sense gaires problemes, potser sí algun entrebanc de tipus comercial, podem veure una pel·lícula sencera amb un mòbil d'antepenúltima generació. I per descomptat podem escriure, dibuixar, fotografiar, filmar, navegar, calcular i més, sempre que no entrem en un terreny excessivament professional, on cada vegada hi entrem més. Què té l'ordinador quàntic que el fa tan revolucionari?

D'entrada cal dir, sempre creuant els dits, que l'ordinador quàntic no substituirà l'ordinador clàssic. No anirem amb un ordinador quàntic a la butxaca. Tot el que fem fins ara amb l'ordinador clàssic ho seguirem fent amb aquest. L'ordinador quàntic no representa una millora substancial en aquest terreny. L'ordinador quàntic marca la diferència quan el nombre de dades que cal manipular és gran. Per exemple, per cercar una clau de pas un ordinador clàssic ha d'anar provant, amb algun algorisme eficient, les combinacions que es puguin fer. Triga un cert temps, que actualment és molt llarg, segons l'ordinador, és clar, però molt llarg també per a un gran ordinador. Si aquest temps s'escurcés n'hi hauria prou a complicar amb un o dues dades la clau de pas per tornar a allargar el temps. En canvi un ordinador quàntic, en aquest terreny, és tan escandalosament més ràpid que en molt poc temps pot trobar les complicades claus de pas que es fan servir avui en dia. L'ordinador quàntic representarà un repte de seguretat per a tot el sistema de transferència d'informació confidencial que hi ha muntat actualment. Imagineu vosaltres mateixos què pot representar l'ordinador quàntic com a eina en la gestió de les *big data.*

En el terrenys de la ciència i tecnologia, on la presència dels ordinadors ha anat creixent any rere any, l'ordinador quàntic representarà una autèntica revolució de la capacitat de càlcul. Per exemple, en fer un càlcul del tipus simulació, anirà més ràpid. Però no és que anirà solament més ràpid . És que anirà escandalosament més ràpid. I podrà manegar internament un nombre escandalosament superior de dades. Amb aquesta desmesurada capacitat de càlcul és completament incert com faran evolucionar la ciència i la tecnologia. I això tindrà una repercussió ben incerta en el conjunt de la societat.

L'ordinador quàntic no és res més que un dels variats ginys que apareixeran en el futur fruit d'aquesta aliança entre ciència i tecnologia. Com la nostra societat anirà entomant aquests ginys? Qui o com es decideix quins ginys es fan i quins no? És decidible? Podem modelar el nostre futur com a societat? Pot ser que aquestes qüestions siguin més difícils de respondre que les plantejades per la mateixa mecànica quàntica.

Adéu amics!

Algunes referències a la xarxa

De referències per a "no experts" n'hi ha moltíssimes i de molts tipus. Aquí n'hem recollit unes quantes per tal que us en feu una idea i perquè les hem trobat significatives en algun aspecte.

[1] *How Does a Quantum Computer Work?* Vídeo disponible a: https://youtu.be/g_IaVepNDT4

[2] Emma Strubell, *An Introduction to Quantum Algorithms.* Document en format pdf disponible a: *https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf*

[3] *Quantum Computing for Dummies : A Simple Explanation for Normal People.* Vídeo disponible a: https://www.youtube.com/watch?v=lypnkNm0B4A

[4] Michael Nielsen, *Quantum computing for everyone.* Text en xarxa disponible a: *http://michaelnielsen.org/blog/quantum-computing-for-everyone/*