

computació quàntica

Sergi Baila Martínez (www.sargue.net)

Continguts

CONTINGUTS	2
1. INTRODUCCIÓ	3
1.1. EL SEGLE DE L'INCERTESA?	3
1.2. COMPUTADORS LINEALS	3
2. INFORMACIÓ QUÀNTICA	4
2.1. QUBIT	4
2.2. PORTES QUÀNTIQUES	4
2.3. NO DUPLICACIÓ	4
2.4. CODIFICACIÓ DENSA	5
2.5. TELEPORTACIÓ QUÀNTICA	5
3. EL COMPUTADOR QUÀNTIC UNIVERSAL	6
3.1. LA PORTA QUÀNTICA UNIVERSAL	6
4. ALGORISMES QUÀNTICS	6
4.1. COMPUTACIÓ QUÀNTICA	7
4.2. EXEMPLE: CERCAR EL PERÍODE D'UNA FUNCIO	7
5. COMPUTADORS QUÀNTICS EXPERIMENTALS	9
5.1. TRAMPA IÒNICA	10
5.2. RESSONÀNCIA NUCLEAR MAGNÈTICA	10
5.3. RYDBERG SCULPTING	11
6. CORRECCIÓ D'ERRORS QUÀNTICS	11
7. CRIPTOGRAFIA QUÀNTICA	12
8. PERSPECTIVES DE FUTUR	13
9. BIBLIOGRAFIA	14

Aquesta obra està sota una llicència Reconeixement-CompartirIgual de Creative Commons. Per veure'n una còpia, visiteu <http://creativecommons.org/licenses/by-sa/2.0/> o envieu una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.



1. Introducció

La humanitat ha progressat a mida que els científics descobrien nous mètodes d'explotar els recursos físics que ens envolten. Si hom preguntés quin son aquests recursos a un científic d'abans del segle XX, el més probable es que obtingues una resposta triple: materials, forces i energies. Ara bé, resulta que en el segle XX hem afegit un nou recurs que podem manipular, i per al qual tenim unes lleis físiques provades: la informació. A més, la invenció del computador ha permès, per primer cop, dur a terme tractament de informació complexa de manera força ràpida fora del cervell humà.

El tema de la computació quàntica és un tema vast i emergent, que avarca des de la teoria de la informació clàssica, fins la física de partícules, passant per la informàtica i la teoria matemàtica del tractament de la informació. Potser es pot englobar tot en un superconjunt que inclou la computació quàntica, a més d'altres disciplines d'una importància cada cop major per tal d'arribar a comprendre els fonaments de la mecànica quàntica i el món natural. Aquest superconjunt ha estat anomenat *teoria de la informació quàntica*.

1.1. El segle de l'incertesa?

El segle que ara acaba va començar amb teories que van fer trontollar els ciments del que la majoria entenia per física, i indirectament, per la comprensió del món on vivim. Els físics, amb el principi de Heisenberg a les mans, van tirar per terra el determinisme, que unit al reduccionisme havien dominat el pensament científic-filosòfic dels últims segles.

Anàlogament, encara que al principi sense cap tipus de connexió, Gödel feia el paper de Heisenberg, però en aquest cas amb el món matemàtic. Gödel va contestar unes preguntes que ja es feia David Hilbert una mica abans. Hilbert, un veritable pensador matemàtic, va proposar un seguit de qüestions a un congrés que es va celebrar l'any 1900. Segons ell, aquestes qüestions estaven dirigides cap a les generacions futures, per tal de resoldre un seguit de problemes bàsics de les matemàtiques. Aquestes qüestions versaven directament sobre la pròpia natura de les matemàtiques. Resumidament, Gödel va demostrar l'existència de proposicions matemàtiques que eren indecidibles, no es podia demostrar que siguessin certes o falses. Abans, es pensava que les matemàtiques eren *completes*, tota proposició tenia una resposta clara: *cert* o *fals*. Ara, cal primer preguntar-se si la proposició es decidible.

1.2. Computadors lineals

Alan Turing, matemàtic, va ser un dels que cercava un procés automàtic per respondre a la pregunta sobre la decidibilitat d'una qüestió matemàtica. Va idear un dispositiu mecànic ideal, suficientment potent per resoldre qüestions força complicades, essent al mateix temps prou simple per ser analitzat a fons.

La Màquina de Turing va esdevenir una ferramenta bàsica dels matemàtics, essent després adaptada pels informàtics per tal de poder parlar

amb propietat de la complexitat computacional d'una resolució determinada d'un problema (un algorisme).

Els ordinadors d'avui en dia son altament sofisticats tecnològicament, i ens poden semblar molt ràpids. Tanmateix, tenen una potència computacional equivalent a les màquines de Turing, en un sentit tècnic estricte. Estem d'acord que els computadors d'avui en dia (capaços de processar milers de milions de càlculs per segon) estan molts ordres de magnitud per damunt dels primers ordinadors a vàlvules. Però, tant uns com els altres son lineals.

La mecànica quàntica sorgeix aquí amb una possibilitat de canvi.

2. Informació quàntica

Com ja hem dit abans, la informació quàntica es una branca de la ciència força nova, però això no vol dir que ens puguem escapar d'unes quantes definicions.

Abans d'entrar en les definicions, cal aclarir que en algunes hi apareixen dos personatges ficticis: Alice i Bob. Aquest dos personatges ja son famosos entre els investigadors, ja que es fan servir en multitud de exemples. Nosaltres farem el mateix.

2.1. Qubit

Es la unitat mínima de informació quàntica. Pot veure's com un sistema de dos estats, com ara un spin o un àtom de dos nivells, però quan el fem servir per a mesurar informació en qubits, estem realment fent quelcom més abstracte: un sistema quàntic es diu que te n qubits si te un espai de Hilbert de 2^n dimensions, y disposa per tant de 2^n estats quàntics mútuament ortogonals. Aquesta definició es desenvoluparà amb més claredat més endavant.

La notació per escriure qubits es una llista de estats ortogonals amb un nombre binari per a cada estat. Per exemple, dos estats ortogonals d'un sol qubit es poden escriure com $\{|0\rangle, |1\rangle\}$. Per a tres qubits tenim: $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

2.2. Portes quàntiques

Les operacions unitàries simples sobre qubits s'anomenen portes quàntiques, de manera anàloga a les portes lògiques d'un sistema clàssic. Tota porta quàntica ha de ser reversible, el que implica que tota operació que vulguem dur a terme sobre un computador quàntic ha de ser reversible. Això pot semblar, en un primer moment, un problema força greu, perquè la majoria de portes lògiques clàssiques no son reversibles: si fem l'operació AND sobre dos bits, obtenim un bit del qual no podem tornar als dos bits originals sense alguna informació extra.

La solució passa per fer servir unes portes modificades, que treballin amb mes bits, de manera que anem guardant sempre informació suficient per tornar enrere.

2.3. No duplicació

Teorema de la no duplicació: Un estat quàntic desconegut no pot ser duplicat.

Aquest teorema impedeix generar còpies de un estat quàntic donat, a no ser que el estat ja sigui conegut (existeix informació clàssica que el descriu). El fet de duplicar-lo permetria fer diverses còpies i posteriorment, mesurar a cada còpia una propietat diferent, el qual violaria el principi d'incertesa de Heisenberg.

2.4. Codificació densa

L'embrollament quàntic¹ es un recurs informatiu.

Els qubits es poden fer servir per emmagatzemar i transmetre informació clàssica. Alice pot transmetre, per exemple, la seqüència |01001) amb 5 qubits amb els estats corresponents. Bob, posteriorment, pot mesurar cada qubit i extreure la seqüència sense cap tipus d'ambigüitat.

Es pot demostrar que si Alice i Bob disposen de un parell de qubits embrollats, Alice pot transmetre a Bob dos bits clàssics per cada qubit transmès.

La codificació densa es força difícil d'implementar, i no te gaire més utilitat que servir de mètode de comunicació estàndard. Tanmateix, permet una transmissió totalment segura: el qubit enviat per Alice només podrà donar els dos bits clàssics que li corresponen al posseïdor de l'altre qubit embrollat (la parella del d'Alice).

2.5. Teleportació quàntica

Es possible transmetre qubits sense enviar qubits!

Suposem que Alice vol comunicar a Bob un sol qubit. Si Alice ja coneix quin es l'estat, li pot comunicar mitjançant algun sistema convencional. Tanmateix, el problema es si Alice no coneix l'estat. No pot mesurar-lo sense modificar-lo (i només podria enviar a Bob l'estat resultant, que no es tota la informació que hi ha dins un qubit), i tampoc en pot fer una còpia per modificar aquesta còpia (recordem el teorema de no duplicació). Així, sembla que l'única manera es enviar físicament el qubit: enviar l'àtom o electró (o el que sigui) que conté l'estat quàntic. Però enviar un estat quàntic no es fàcil; no podem posar-lo dins una carta i enviar-lo per correu. Hi ha cap manera de enviar l'estat quàntic (desconegut) sense modificar-lo mitjançant informació clàssica?

La teleportació quàntica permet resoldre aquesta situació, o si més no, trobar un camí alternatiu. Com en la codificació densa, es fa servir l'embrollament quàntic com a recurs informatiu. La idea es que Alice i Bob disposen d'un parell de qubits embrollats, mitjançant els quals es pot demostrar que Alice pot obtenir dos bits clàssics mitjançant unes operacions sobre el qubit

¹ No hem trobat cap traducció de l'expressió *quantum entanglement*, i hem optat per traduir-la, força lliurement, per *embrollament quàntic*. Donada la *flexibilitat* de l'anglès, els autors fan servir moltes variacions de l'expressió, sobre tot del verb, per indicar per exemple *two entangled qubits*, que hem hagut de traduir per *dos qubits embrollats*.

que vol transmetre (que queda destruït –modificat–) i el qubit parella dels dos embrollats que tenen en comú. Bob, posteriorment, pot reproduir el qubit original mitjançant operacions anàlogues amb la seva parella dels qubits embrollats i els dos bits clàssics.

3. El computador quàntic universal

La teoria de la informació quàntica necessita una eina equivalent a la Màquina de Turing de la teoria clàssica de la informació. Aquesta *màquina universal* es el que anomenariem el *computador quàntic universal*. La primera definició seriosa d'una tal màquina s'atribueix a Deutsch.

Un computador quàntic es un conjunt de n qubits, sobre els quals les següents operacions son experimentalment factibles:

1. Cada qubit pot ser preparat en un estat conegut $|0\rangle$.
2. Cada qubit es pot mesurar en la forma $\{|0\rangle, |1\rangle\}$.
3. Una porta quàntica universal (o conjunt de portes) poden ser aplicades a voluntat sobre qualsevol subconjunt de mida fixa dels qubits
4. Els qubits no evolucionen de cap altra manera que no sigui mitjançant alguna de les anteriors transformacions.

Aquesta definició no es totalment completa en un sentit tècnic estricte, però comporta les principals idees.

3.1. La porta quàntica universal

La porta quàntica universal es l'equivalent quàntic de la porta universal clàssica, una porta mitjançant la qual es pot generar l'acció de qualsevol altra porta mitjançant repetides operacions i combinacions.

S'han trobat portes de només dos qubits que son universals, la qual cosa es força important. La porta més estesa està formada per operacions XOR i de rotació de qubits individuals.

4. Algorismes quàntics

Fins ara hem vist com seria un computador quàntic i com faria els seus càlculs. Però de moment no hem demostrat que hi hagi res que pugui fer un computador quàntic, que no ho pugui fer un computador clàssic.

La resposta es clara: no hi ha res. Ara bé, si parlem de l'*eficiència* d'un computador clàssic front a un computador quàntic, la cosa canvia. Problemes que son computacionalment 'difícils' poden ser, a la pràctica, impossibles de resoldre mitjançant computadores clàssics per manca de temps. Exemples d'aquest son factorització de grans nombres o cercar el període d'una funció.

La factorització d'un nombre enter es pensa que te una complexitat que creix més ràpidament que qualsevol potència de N (*superpolinòmica*), encara

que encara no s'ha demostrat. L'algorisme quàntic mostrat per Shor treballa amb una complexitat de N^3 .

A més d'aquest gran resultat, un altre també molt espectacular es el conegut com *algorisme de cerca de Grover*. Aquest algorisme de cerca aconseguir trobar un element a una col·lecció desordenada en un temps de l'ordre de l'arrel de N , mentre que en un computador clàssic està demostrat que com a màxim es pot fer en temps d'ordre N .

4.1. Computació quàntica

Una computació quàntica qualsevol està formada per tres passes. Primer preparem N qubits en un estat inicial determinat. Després, apliquem una transformació unitària U als N qubits (una transformació unitària U no es més que el producte de portes quàntiques convencionals). Finalment, mesurem el valor dels qubits col·lapsant-los en els estats $\{|0\rangle, |1\rangle\}$.

Una de les diferències fonamentals ha tenir en compte es que una computació quàntica es sempre un algorisme probabilístic, cada cop que l'executem podem obtenir diferents resultats. De fet, el resultat de una computació quàntica es una distribució de probabilitats dels diferents resultats. El que fem a l'últim pas, la lectura -col·lapse- del resultat, no es més que triar un dels resultats possibles.

4.2. Exemple: cercar el període d'una funció

Aquest es actualment un dels dos algorismes quàntics –junt amb el de factorització- més importants que hi ha desenvolupats. Suposem una funció $f(x)$ que es periòdica amb un període r . Aleshores, $f(x) = f(x+r)$. Suposem a més que $f(x)$ pot ser eficientment calculat donat x (o sigui, f no es una funció computacionalment difícil). Tot el que sabem de r originalment es que

$$N/2 < r < N$$

per algun N . Assumint que no hi ha cap tècnica analítica per deduir el període de $f(x)$, el millor que podem fer amb un computador clàssic es calcular $f(x)$ per de l'ordre de $N/2$ valors de x , i trobar quan es repeteix la funció. Això es ineficient donat que el nombre d'operacions necessàries pel càlcul es d'ordre exponencial sobre l'entrada N .

Aquest càlcul es pot resoldre d'una manera elegant i ràpida mitjançant un computador quàntic. En necessitem un de $2n$ qubits, on $n=2 \cdot \log N$ per tal d'emmagatzemar els operands. Cal notar que cada registre és el doble de gran del màxim valor per un període, per tal de disposar, en el pitjor dels casos, de dos períodes complets. Dividim els qubits disponibles en dos registres de n qubits cadascun, anomenats x i y . Abans de començar, preparem els dos registres a l'estat $|0\rangle$ (posem tots els qubits constituents dels registres a aquest estat).

A continuació, apliquem al registre x una de les operacions bàsiques que es poden fer sobre qubits, l'operació H . Això seria l'equivalent a una porta lògica convencional aplicant alguna de les operacions bàsiques sobre bits (com una AND o una XOR). El resultat d'aquesta operació es una superposició de 2^n estats, corresponents a tots els possibles estats en els que es pot trobat el

registre x . Dit d'una altra manera, el registre x , que tenia longitud n , conté en el seu interior tots els nombres possibles que pot contenir amb n bits. Això s'expressa matemàticament –de manera aproximada– amb la següent expressió:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle |0\rangle \quad \text{on } w = 2^n$$

Posteriorment, apliquem una xarxa de portes a tots dos registres x i y , per a dur a terme la transformació $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$. Aquesta transformació pot ser unitària, ja que l'estat d'entrada $|x\rangle |0\rangle$ està en correspondència bijectiva amb l'estat de sortida $|x\rangle |f(x)\rangle$, així que el procés es reversible, es a dir, la bijectió em proporciona un vincle entre cada parella de qubits respectiva dins els dos registres. Per tant, em garanteix la descodificació. Ara, aplicant U_f a l'estat anterior obtenim:

$$\frac{1}{\sqrt{w}} \sum_{x=0}^{w-1} |x\rangle |f(x)\rangle$$

Fixem-nos amb més deteniment en aquest estat. El valor de $f(x)$ ha estat calculat per a 2^n valors d'un sol cop! Això es el que s'anomena *paral·lelisme quàntic*, i representa un paral·lelisme real impressionant, ja que hem de adonar-nos que el càlcul de tots els valors depèn **exponencialment** de n .

Encara que presents a l'estat quàntic del computador, els 2^n valors de $f(x)$ no son directament accessibles, ja que una mesura provocaria que el valor col·lapsés a un sol estat. Curiosament, aquest es precisament el següent pas de l'algorisme. Recordem (fixant-nos en l'estat que tenim ara mateix) que al registre y tenim tots els valors de $f(x)$. Ara, mesurem el valor d'aquest registre. Això provoca que col·lapse cap a un valor concret (aleatori), suposem que aquest valor es $f(x)=u$. El registre y col·lapsa a $|u\rangle$ i l'estat total esdevé:

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |d_u + jr\rangle |u\rangle$$

on $d_u + jr$, per $j = 0, 1, 2 \dots M-1$, son els valors de x per als quals $f(x) = u$. En altres paraules, la periodicitat de $f(x)$ significa que el registre x es manté en una superposició de $M \approx w / r$ estats, on r era, recordem, el període de la funció $f(x)$, que es la dada que estem calculant. El que tenim ara, resumint, es un valor concret u de $f(x)$ al registre y , i totes les x que satisfan $f(x)=u$ en superposició a l'estat x . El valor d_u no es més que un offset derivat del valor u que s'ha obtingut al col·lapsar y .

L'estat que ha quedat emmagatzemat dins el registre x sembla com un truc de màgia. El "secret" està en que cada valor de $f(x)$ manté un vincle amb el valor de x que l'ha produït, mitjançant l'embrollament dels qubits dels dos registres, que es va aconseguir al calcular els valors de $f(x)$.

El problema ara s'ha reduït a extraure el període r de l'estat al registre x . Per això es fa servir una transformada de Fourier discreta aplicada al registre x . La transformada que es fa servir es el següent procés unitari:

$$U_{FT}|x\rangle = \frac{1}{\sqrt{w}} \sum_{k=0}^{w-1} e^{i2\pi kx/w} |k\rangle$$

Aquesta operació ja l'hem fet servir, de fet. Aplicada a l'estat $|0\rangle$ ens dona la primera transformació que hem fet a l'algorisme (donar tots els valors possibles al registre x). Es pot demostrar que aquest procés és unitari, es pot idear una xarxa de portes que implementen una versió d'una FFT. Per continuar treballant i simplificar els càlculs, donat que això no és més que un exemple, assumirem que r és divisor de x , així que $M = w/r$. Les idees essencials no queden afectades, i el càlcul complet porta algunes complicacions que poden ser solventades.

El registre y ja no ens interessa, ens fixarem només en el registre x , sobre el qual aplicarem la ja mostrada transformació:

$$U_{FT} \frac{1}{\sqrt{w}} \sum_{j=0}^{w/r-1} |d_u + jr\rangle = \frac{1}{\sqrt{r}} \sum_k \tilde{f}(k) |k\rangle$$

on

$$\tilde{f}(k) = \begin{cases} 1 & \text{si } k \text{ és múltiple de } w/r \\ 0 & \text{altrament} \end{cases}$$

Finalment, mesurem l'estat del registre x , provocant el seu col·lapse. El valor obtingut ha de ser, forçosament, múltiple de w/r . Ara només cal treure r del valor obtingut. Tenim que $x = k w/r$ on k és desconegut. Si k i r no tenen factors comuns, aleshores podem reduir x/w fins a una fracció irreductible, obtenint d'aquesta manera k i r . En el cas que k i r tinguin algun factor comú, cosa força improbable per valors grans de r , l'algorisme falla.

Cal que en aquest punt fem una petita pausa per reflexionar sobre aquest resultat. Estem acostumats a treballar amb algorismes deterministes... i de fet, són els únics algorismes amb els que podem treballar sobre un computador clàssic. Donada una entrada, sempre obtindrem la mateixa sortida. Ara bé, en el cas d'un computador quàntic, hi ha passes dels algorismes que no són deterministes. En el cas d'aquest exemple el pas indeterminista és quan col·lapsem y , ja que no podem controlar quin serà el valor que obtindrem. Això mateix, que ens dona potencia, sembla que ens la lleva, doncs haurem d'anar repetint el càlcul fins que obtinguem una solució correcta.

Afortunadament, es pot demostrar que el nombre de repeticions és força petit, i de fet, la probabilitat d'èxit s'aproxima arbitràriament a 1 amb un nombre de repeticions que és, en aquest cas, de l'ordre del logaritme de r . Per tant, el cost total de l'algorisme continua sent polinòmic.

L'algorisme que hem descrit és eficient sempre i quant el càlcul de $f(x)$ sigui eficient. El nombre total de portes lògiques requerides per a tots els càlculs és d'ordre polinòmic front el valor de n .

El problema de la factorització de grans nombres es pot reduir matemàticament a trobar el període d'una funció. Tot això, inclòs l'algorisme

descriu, va ser publicat per Peter Shor, enginyer informàtic de AT&T, a l'Abril de 1994, demostrant finalment la viabilitat i utilitat d'un computador quàntic ideal.

5. Computadors quàntics experimentals

Fins ara hem parlat de portes quàntiques i qubits d'una manera ideal. Als inicis d'aquesta disciplina, es pensava que, o bé es trigaria molt de temps en trobar una sistema per fer un computador quàntic, o fins i tot es pensava que mai es podria construir un.

Però, com passa sovint a la ciència, els físics experimentals sorprenen pel seu enginy, i ara mateix existeixen diferents computadores quàntics experimentals funcionant, encara que d'una manera molt rudimentària i amb molt pocs qubits.

Actualment hi ha dos candidats que haurien de permetre computació quàntica amb de 10 a 40 qubits. La primera proposta es de Cirac i Zoller (1995), fent servir una línia d'àtoms confinats en una trampa iònica. Aquesta proposta esta essent superada per la més recent de Gershenfeld i Chuang (1997), i simultàniament Cory *et al.* (1996), fent servir ressonància magnètica nuclear.

5.1. Trampa iònica

Una filera de ions son confinats mitjançant una combinació de camps elèctrics oscil·lants i estàtics en un estat d'alt buit (10^{-8} Pa). Un sol feix làser es divideix en força parells de feixos, cadascun il·luminant un ió. Cada ió te dos possibles estats estables (amb un promig d'estabilitat de milers d'anys), que son ortogonals entre ells i formen, per tant, un qubit. Mitjançant els feixos làsers de cada ió es poden aplicar portes quàntiques d'un sol qubit. Per tal d'aplicar portes de dos qubits, imprescindibles per dur a terme qualsevol computació, es recorre a la repulsió de Coulomb entre els ions, i més concretament, a la vibració conjunta de la filera de ions. La llum no només transporta energia, també transporta moment, i es aquest moment el que provoca la vibració del ió que aprofitem per fer interaccionar els diferents ions. El moviment dels ions està quantificat perquè es troben atrapats a la trampa (anomenada *trampa de Paul*).

Per tal de tenir un autèntic computador quàntic encara ens falten dos coses segons la llista donada al principi del punt 3. Hem de poder ser capaços de preparar qualsevol qubit (ió) a l'estat $|0\rangle$ i de poder fer la lectura de qualsevol qubit. El primer es possible mitjançant el mètode de bombeig òptic i refredament per làser, i el segon mitjançant tècniques desenvolupades pels físics nuclears als darrers anys.

A la pràctica, un computador quàntic d'aquestes característiques només s'ha fet funcionar amb un sol ió, donades les dificultats implicades en el tractament tan directe dels mateixos.

5.2. Ressonància nuclear magnètica

El processador quàntic és, en aquest cas, una molècula formada per un *backbone* de uns deu àtoms, amb altres àtoms com hidrogen connectats per a

completar tots els enllaços químics. Els àtoms interessants són els del nucli. Cadascun d'ells té un moment magnètic associat amb l'spin nuclear, essent els estats de l'spin el que ens dona els qubits. La molècula es situa dins un camp magnètic intens, i es controla mitjançant camps magnètics oscil·lants en impulsos de durada controlada.

Fins aquí tot va bé, però com abans, ens falta completar els processos de preparació de l'estat inicial i de lectura de l'estat final. El problema és que l'spin del nucli d'una molècula no es pot mesurar ni preparar. Per tal de resoldre aquest problema no es fa servir una sola molècula, sinó una agrupació de 10^{20} molècules. D'aquesta manera, la conjunció de tots els moments magnètics dels nuclis és prou fort per a ser detectable com un subtil camp magnètic.

Els experiments amb NMR (*nuclear magnetic resonance*) han donat resultats positius en els darrers anys en la manipulació i mesura d'estats equivalents en complexitat a la requerida per un computador quàntic d'uns quants qubits. Sembla ser, per tant, que els primers computadores quàntics funcionals seran sistemes NMR. Tanmateix, aquesta tècnica no escala gaire bé, i amb més qubits la detecció de l'estat roman força limitada.

5.3. *Rydberg Sculpting*

Aquesta és una nova tècnica que permet posar un àtom que es troba molt excitat (àtom de Rydberg) en molts estats energètics diferents simultàniament. Les aplicacions d'aquesta nova tècnica permetran perfeccionar els actuals dissenys de computadores quàntics, que actualment treballen en base a qubits de dos estats. Amb aquest nou mètode, presentat el 27 de Maig de 1999 a la Conferència de Làsers i Electro-òptica de Baltimore, un pols làser constituït per una superposició de diferents longituds d'ona (diferents energies) impacta l'àtom que obliga als electrons de l'àtom a bellugar-se en un complex patró donat pel feix làser. La importància de la tècnica és que permet controlar aquests moviments d'electrons.

6. Correcció d'errors quàntics

Anteriorment hem vist alguns exemples d'algorismes quàntics, però aquests només ens donen un avantatge real sobre màquines clàssiques amb problemes que necessiten un nombre de qubits de l'ordre de milers. Ara hem vist que hi ha sistemes experimentals que només ens apropen a "computadors" quàntics d'uns quants qubits. Aquests sistemes no es poden anomenar amb propietat computadores quàntics, donat que no són suficientment versàtils. Són més bé, processadors d'informació quàntica.

Arribarem a disposar algun dia de veritables computadores quàntics de milers o milions de qubits? El problema rau en la descripció del *computador quàntic universal* que hem donat anteriorment. El quart punt és físicament impossible. No hi ha res que sigui una porta quàntica perfecta, ni hi ha cap manera de disposar d'un sistema totalment aïllat. El problema és que pel mateix que una porta quàntica aprofita la correlació entre diferents qubits per dur a terme el càlcul, aquest qubit també estaran correlacionats amb d'altres qubits de l'entorn que no pertanyen al sistema, destorbant d'aquesta manera els càlculs. Això es coneix com *decoherència*. És força complicat trobar un

sistema amb un factor de decoherència menor que una part per milió cada cop que actua una porta. Això significa que la decoherència al factoritzar, per exemple, un nombre de 130 dígit es 10^7 cops superior al màxim tolerable per dur a terme el càlcul.

Els computadors clàssics són fiables no perquè siguin perfectes, sinó perquè són immunes al soroll. La estabilitat d'un dispositiu clàssic es basa en una combinació d'amplificació i dissipació. Fan servir una amplificació per passar d'un estat a un altre, i després, per estabilitzar-se en l'altra posició dissipen l'energia en forma, normalment, de calor. Dos exemples: un interruptor mecànic i un biestable (circuit lògic bàsic que emmagatzema un bit). A l'interruptor l'amplificació la dona, normalment, una molla o similar, de tal forma que fins que no li donem una certa energia, l'interruptor no varia, però si ho arriba a fer, disposa de més energia de la que li cal per canviar d'estat. Al biestable, els transistors fan aquesta feina. En quant a la dissipació, en el cas de l'interruptor, un cop ha canviat d'estat, hi ha un xoc molt inelàstic que dissipa l'energia en forma de calor i só. Si no, l'interruptor aniria saltant d'un estat a l'altre. Per al biestable, hi ha unes resistències que dissipen l'energia sobrant en forma de calor.

Tanmateix, aquests mètodes no ens serveixen per als computadors quàntics. El teorema de no duplicació implica que l'amplificació de estats quàntics desconeguts és impossible, i la dissipació és incompatible amb l'evolució unitària.

Aquestes consideracions han dut a l'acceptació general que les regles de la mecànica quàntica juguen contra l'estabilitat d'un computador quàntic, i que aquest no podrà funcionar mai eficientment. Tanmateix, podem fer servir els mateixos principis de correcció d'errors que ja es fan servir a la teoria de la informació clàssica. Així neix la correcció d'errors quàntics (QEC).

La QEC fa servir uns circuits especials, que durant els primers estadis de la investigació no es sabia si havien de ser necessàriament perfectes. Posteriorment, es van trobar xarxes correctores d'errors que eren tolerants als errors... o sigui, circuits que corregien més errors dels que introduïen amb la seva presència. Aquests circuits tenen l'avantatge que permeten computadors quàntics de tamany arbitràriament gran, sempre i quan estem disposats a perdre una part de l'espai disponible per als circuits correctors, evidentment.

Recentment, s'han estimat els requeriments per a computació quàntica fiable mitjançant QEC tolerant a errades. Són força alts, però viables. Per exemple, un computador quàntic útil (que pugui efectuar càlculs per sobre de qualsevol computador clàssic) requeriria de l'ordre de 1000 qubits i 10^{10} portes. Sense QEC, això requeriria un nivell de soroll de només 10^{-13} per cada qubit i porta, que és totalment impossible. Aplicant QEC només necessitaríem 10^{-5} per cada qubit i porta, que és difícil però no impossible. L'efecte lateral seria que necessitem un computador de 10 a 100 cops més gran.

7. Criptografia quàntica

El propòsit de la criptografia és crear una comunicació segura de informació. Actualment, els algorismes criptogràfics més estesos són els

anomenats de *clau pública*, pel seu funcionament asimètric: hi ha una clau pública per encriptar la informació, i una clau privada per descriptar-la. D'aquesta manera es va eliminar el gran problema que suposava intercanviar la clau (abans única) d'encriptació i descriptació. El problema, però, és que aquests sistemes es basen en algunes operacions matemàtiques que són força fàcils de dur a terme en un sentit, però al contrari és difícil i requereix molts de càlculs... fins ara.

Els computadors quàntics han mostrat, teòricament encara, que són capaços de fer els càlculs necessaris per a descriptar un missatge codificat mitjançant aquestes tècniques en un temps raonable. De moment, encara no disposem de computadors quàntics útils per a aquestes tasques, però en el moment que disposem d'ells, tots els sistemes de comunicació segura que hi ha avui dia seran completament inútils.

Afortunadament, la pròpia teoria que pot destruir aquests sistemes ens ofereix una alternativa encara millor: la criptografia quàntica. Basada en el principi d'incertesa de Heisenberg, i en l'embrollament quàntic, la criptografia quàntica proporciona un mètode per tal que dos parts intercanvien una clau d'encriptació amb una seguretat absoluta, garantida per les pròpies lleis de la física.

Actualment hi ha tres mètodes de sistemes criptogràfics quàntics. Per exemple, hi ha un basat en l'embrollament quàntic i el teorema de Bell, proposat per A.K.Ekert el 1990.

L'idea bàsica es transmetre una seqüència de parelles de partícules correlacionades, amb un membre de cada parella essent detectat per cadascuna de les dues parts. Un espia en aquesta comunicació, hauria de llegir alguna de les partícules, i retransmetre-la per tal que la seva presència romangués desconeguda. Tanmateix, l'acte de la detecció d'una partícula d'un parell destruiria la seva correlació, i les dues parts ho podrien verificar sense cap dificultat fent servir qualsevol mitjà de comunicació obert, sense necessitat de mostrar els resultats dels seus descobriments.

A la pràctica, aquests sistemes ja funcionen als laboratoris, i de fet, amb la tecnologia actual és possible implementar sistemes de distribució de claus sobre grans xarxes d'àrea local (alguns quilòmetres) transmetin a 20K per segon.

8. Perspectives de futur

Les paraules "computació" i "quàntica" plegades sonen força espectaculars, i han generat, i generen de tant en tant, articles en premsa no especialitzada (en física), que ens posen en un parell de dècades un computador quàntic a la taula de casa o el despatx. Res més lluny de la realitat. Els computadors quàntics mai substituiran als computadors clàssics de la mateixa manera que per calcular la trajectòria d'una míssil no es fa servir la teoria de la relativitat general simplement perquè no fa falta complicar-se la vida: la teoria de la gravitació de Newton, més simple, és més que suficient.

De la mateixa manera, la majoria dels problemes computacionals poden ser resolts amb la mateixa eficiència per un sistema quàntic i per un clàssic.

Perquè complicar-nos amb un sistema molt més complex (i car) si ho podem fer amb un simple PC? Els computadors quàntics seran màquines molt útils per a problemes que son inabordables mitjançant computadors clàssics, però difícilment els arribaran mai a substituir.

9. Bibliografia

Barenco A, Ekert A *et al* 1996 *Un saut d'échelle pour les calculateurs*
(*La Recherche* Nov 1996)

Bucksbaum P 1999 *Rydberg Sculpting*
(paper QTHA1, May 97, Conference of Lasers and Electro-Optics meeting in Baltimore)

Deutsch D, Ekert A 1993 *Quantum communication moves into the unknown*
(*Physics World*, June 1993)

Ekert A 1995 *What is Quantum Cryptography*
(Center for Quantum Computation - Introductions : www.qubit.org)

Gershenfeld N A, Chuang I L 1997 *Bulk Spin-Resonance Quantum Computation*
(*Science* vol. 275 p 350-355 17 Jan 1997)

Preskill J 1997 *Quantum Computing: Pro and Con*
(pre-print quant-ph/97050032)

Preskill J 1998 *Quantum Information and Computation*
(Lecture Notes : <http://www.theory.caltech.edu/~preskill/ph229>)

Steane A 1997 *Quantum Computing*
(pre-print quant-ph/9708022)

Steane A 1997 *The ion trap quantum information processor*
(pre-print quant-ph/9608011)