



# Calculatorul CUANTIC

În ultimele luni, știrile despre câteva contracte comerciale având ca obiect computere cuantice ne aduc în atenție perspective extraordinare în lumea calculatoarelor. Încercăm aici să ne apropiem de subiectul acesta, atât pentru a mai cunoaște un pic aspectele, cât și pentru a lămuri lucrurile, respectiv pentru a tempera cumva așteptările.

MIRCEA BĂDUT

Cum orice lexicon ori dicționar modern ne informează, prudent și cuprinzător, că un „quantum computer” este un dispozitiv de calcul bazat pe fenomene de mecanică cuantică. Iar cum următoarea trimitere ne lămurește că respectiva mecanică este, de fapt, „fizica atomică”, înțelegem atunci că avem de-a face cu legi ale stărilor și interacțiunilor subatomice. Așa că domeniul își are rădăcinile și în eforturile de-acum un secol de a defini modele fizico-matematice care să explice comportamentul dual (de particulă și de undă) al luminii (de la „eter” la „foton”). Cuvântul cheie aici, provenit din latinescul „quanta”, a fost adoptat pentru a sublinia observația (ce apare și în fizica noastră de liceu) că la nivel atomic anu-

mite stări fizice se modifică doar în cantități discrete (discontinue).

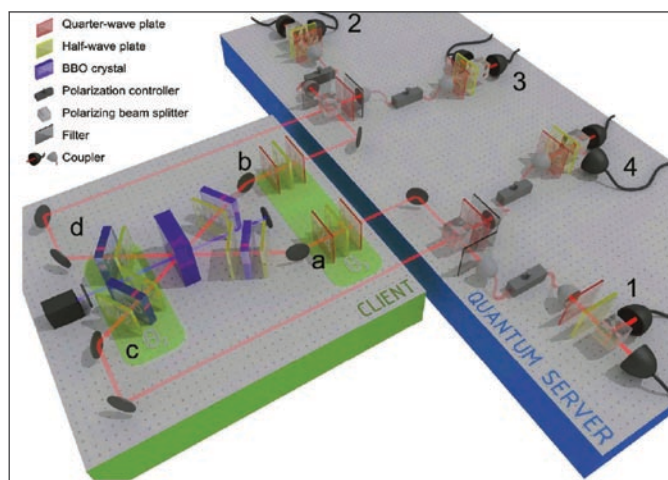
Acea scară microscopică a materiei la care sunt studiate fenomenele cuantice este definită de acțiunea constantei lui Planck ( $h$ -ul din expresia  $E=h\nu$ ). De fapt, Max Planck este considerat părintele fizicii cuantice. Deși primele definiții esențiale din fizica atomică se făceau la începutul secolului 20 (inclusiv prin contribuțiile lui Einstein), formulările teoriei cuantice au loc în perioada 1914-1930 prin contribuțiile lui Werner Heisenberg, Max Born, Pascual Jordan, Louis de Broglie, Erwin Schrödinger, Wolfgang Pauli, Satyendra Nath Bose, Niels Bohr, David Hilbert, Paul Dirac și chiar (!) John von Neumann.

## Premii Nobel pentru fizică cuantică

1918 - Max Planck;  
1929 - Louis De Broglie;  
1932 - Werner Heisenberg;  
1933 - Paul Dirac și Erwin Schrödinger;  
1937 - Clinton Davisson și George Thomson...  
2012 - David J. Wineland și Serge Haroche  
2013 - François Englert și Peter W. Higgs

Definițiile mai ambițioase ne spun despre calculatorul cuantic că-și bazează procesările pe anumite fenomene ale mecanicii cuantice, cum sunt superpoziția și entanglement-ul. Dacă superpoziția stărilor (manifestarea „simultană” a stărilor 0 și 1) am putea-o înțelege și noi, cei deja condiționați de logica binară, cu entanglement-ul (adică empatia dintre particule independente) chestiunile sunt un pic mai confuze. Pentru că lucrurile nu se lămuresc grozav, vom încerca să le înțelegem prin punctarea diferențelor față de calculatoarele digitale actuale. Iar deosebirea esențială constă în faptul că acest „quantum computer” nu codifică datele în cifre binare (biții 0 și 1) materializate electric, ci reprezintă și prelucrează datele prin stări cuantice (stări specifice particulelor subatomice). Adică o codificare dincolo de 0 și 1, printr-o logică mai largă decât logica binară! O logică folosind modele non-deterministe, în care stările (de adevăr) nu sunt concrete, ci „fixate” doar probabilistic.

Înceiem tentativa aceasta de lămurire a noii paradigme informatice menționând și denumirea cheie de „qubit”, adică de bit cuantic, respectiv de stare logică angrenabilă în reprezentări și prelucrări de date.



Schemă figurativă de calcul client-server bazată pe fotoni.

## Paranteză ternară

Dacă tot a venit vorba de logică deviată de la binarul atât de comun (și de aplicat!) astăzi în electronica digitală, merită amintite și experimentele de logică cu trei stări. Primele încercări teoretice datează din 1921. În 1945, matematicianul român Grigore Moisil are contribuții importante la algebra logicii cu stări multiple.

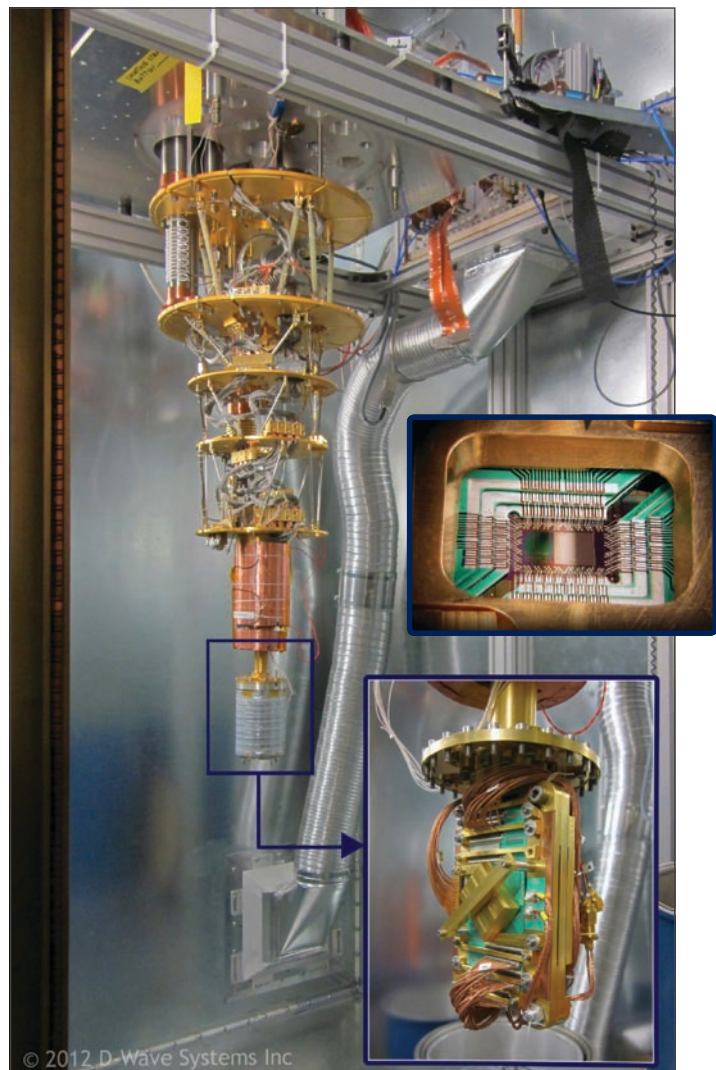
Spre deosebire de logica folosind cifrele 0 și 1, logica ternară angajează trei stări de adevăr: fie stări concrete (gen 0, 1 și 2), fie cu două stări concrete și una indecisă (deci cam similar modelului propus de calculatorul cuantic). În trecut s-au explorat mai multe variante de codificare ternară: unul în sistem cartezian (0, 1, 2), altul cu logică simetrică (-1, 0, 1), altul cu logică redundantă (-1, 0, 0, 1, deci cu zeroul capabil să joace ambele roluri adiacente - cumva similar valorii NULL din SQL). În 1958, la universitatea din Moscova

se concepea primul calculator cu logică ternară (Setun). Și era unul de uz general! Adică programabil (cu limbajul DSSP, derivat din atunci clasicul Forth).

## Calculatoare dedicate

Ah! Aproape că mi-a scăpat porumbelul cheie al acestui articol. Da, computerele cuantice actuale nu sunt calculatoare generale, nu prea pot rezolva mai multe probleme, ci doar pe acea pentru care au fost concepute. Sunt mai degrabă dispozitive dedicate (neavând nici măcar flexibilitatea PLA-urilor din aplicațiile de electronică digitală).

Însă pot rezolva - prin specificul lor de (hai să-i zicem!) logică non-deterministă - alte probleme pe care calculatoarele clasice nu le înțeleg. Sau rezolvă anumite probleme mai rapid (sau mai firesc) decât prin abordarea (limitativă, deci, a) computerelor actuale. Diferențierea o vom înțelege și prin faptul că problemele pretabile pentru „quantum computing” se transpun cu totul altfel, prin algoritmi angajând logica cuantică. În lume deja s-au definit și chiar probat o serie de algoritmi cuantici (precum Shor, Simon, Grover, Deutsch-Jozsa), special concepuți pentru a folosi stările cuantice „scrise” și „citite” în/din particule subatomice. (Aici sesizăm necesitatea de a înțelege și puntea dintre dispozitivele de intrare/ieșire existente - bazate pe bătrâna electronică digitală - și entitățile cuantice care memorează sau prelucrează datele. Sperăm să aflăm mai încolo despre interfațare...)



Cipul de 128 de qubiți de la D-Wave.

Apropo de operațiuni I/O: nu pierdem din vedere faptul că uneori starea inițială a mașinii de calcul trebuie cumva transmisă qubiților angajați (similar unei operații de scriere într-o memorie RAM ori într-un registru de CPU), precum și condiția ca mecanismele/dispozitivele I/O să preia valorile fără să altereze stările qubiților (fie aceștia electroni, fotoni, atomi, ioni sau alte particule).

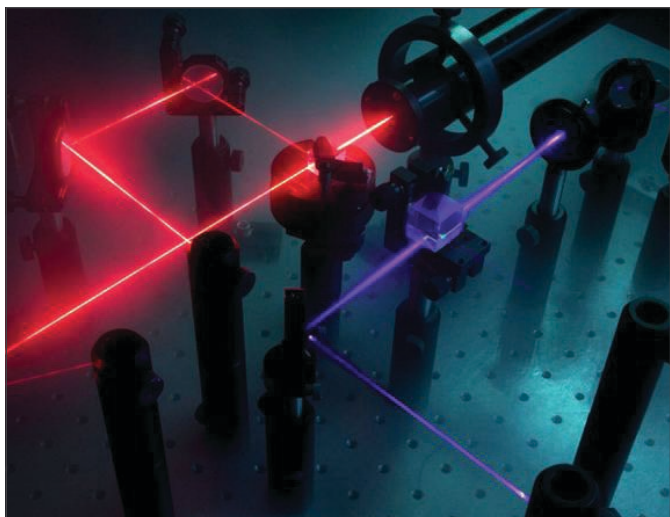
(Facem o paranteză: cercetători de la NIST și de la University of Maryland au reușit stocarea unei imagini optice într-un nor de atomi de rubidiu – deci există premise și pentru memorarea cuantică, nu doar pentru calcul.)

Un calculator clasic ar putea, grație puterii actuale de memorare/prelucrare, să rezolve (sau să simuleze) și algoritmi cuantici (pentru că aceștia de regulă nu încalcă modelul Church-Turing). Însă eficiența implementării ar fi net inferioară calculatorului cuantic, datorită în principal puterii de reprezentare a qubiților. (Un volum de date digitale de un terabyte s-ar putea echivala prin doar 243 qubiți.)

În vreme ce bitul din memoria clasică reține cifre binare, qubitul reprezintă – datorită efectului de superpoziție – fie „0”, fie „1”, fie un „intermediar” (indefinit). Mai mult, qubiții dintr-un duet pot fi într-o superpoziție cuantică de patru stări, iar trei qubiți pot reprezenta o superpoziție de 8 stări. (Astfel, mașina cuantică lucrând cu o secvență de  $n$  qubiți se poate afla oricând în oricare dintre cele  $2^n$  stări posibile. Pe când calculatorul nostru poate fi doar într-una dintre cele  $2^n$  stări, și anume în cea stare complet constrânsă de logica binară.)

Ne putem imagina că mașina de calcul cuantic pornește secvența de procesare dintr-o stare inițială (controlată conform datelor problemei de rezolvat) și apoi trece acei qubiți printr-o serie de procese subatomice (asimilabile unor porți logice). După aplicarea acestui algoritm cuantic, se măsoară (citesc) stările qubiților (acestea revelând soluția problemei delegate calculatorului), însă „forțându-i” să adopte una dintre cele două stări stabile/determinate (asigurând astfel interpretarea clasică a rezultatelor). În anumite implementări de mașini cuantice, forțarea/înghețarea aceasta poate altera stările qubiților, de aceea se recurge la repetarea (statistică a) procesării, pentru obținerea unui rezultat cât mai probabil.

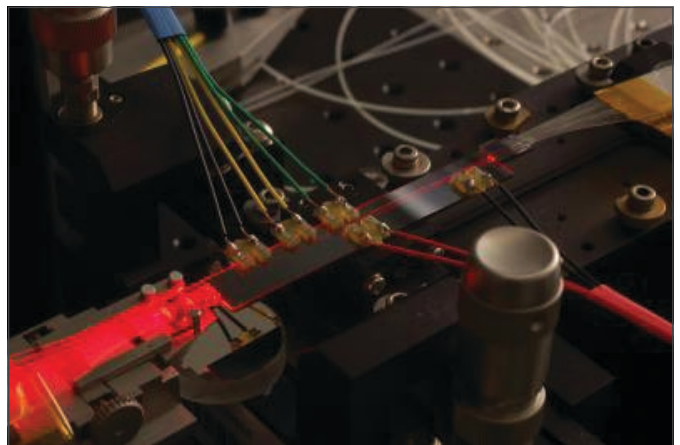
Un exemplu clasic de „materializare” a qubitului îl constituie particulele subatomice ce au proprietatea de spin (direcția rotației proprii), spin care se poate regăsi după un timp într-o stare diferită. Dar vom vedea că se folosesc mai multe genuri de particule și diverse proprietăți (fluctuând non-mecanicist). Aceasta ne conduce la o concluzie practică: qubiții sunt constituiți atât din particule care pot fi controlate, cât și din mecanismul de control (dispozitivul de captură și de comutație).



Experimente de calcul cuantic prin eșantionarea bosonilor.

Cum starea finală a qubiților este dincolo de logica „mecanicistă”, combinațiile de stări (grație superpoziției) sugerează mai degrabă modele stocastice. Însă paralela cu computerele probabiliste doar deschide înțelegerea: computerele cuantice pot fi eventual considerate ca hiper-probabiliste (ori meta-probabiliste, dacă aplicarea lor se potrivește schimbării de perspectivă). În logica binară clasică un dispozitiv gestionând cuvinte de trei biți se va regăsi (la încheierea procesării) într-una din cele  $2^3=8$  stări (000, 001, 010, 011, 100, 101, 110, 111). În vreme ce la final calculatorul binar se află cu probabilitate 1 în exact acea stare (logică), un calculator probabilistic poate avea orice probabilitate (între 0% și 100% șanse) de a fi în acea stare, pe când calculatorul cuantic are orice probabilitate de a fi în oricare dintre cele 8 stări (cu restricția ca suma probabilităților pentru cele opt stări să completeze unitatea evenimentului). Observăm că avem aici, de fapt, un vector de probabilități (pe când la calculatorul clasic avem doar un vector de stări).

Pentru a nu ne afunda prea mult, ieșim, subit, cu o concluzie interesantă în tentativa noastră de lămurire: problemele rezolvabile cuantic sunt probleme cu nuanță statistică (tratarea datelor și interpretarea rezultatelor corespunzând calculului probabilist) la care mecanismele clasice de randomizare nu se pretează pentru simularea incertitudinii (norma euclidiană/L2 de însumare a probabilităților neputând fi atinsă de funcțiile RANDOM din limbajele de programare actuale).



Calcul cuantic folosind eșantionarea bosonilor: fotoni singulari sunt injectați sincron printr-un ghidaj încrucișat de unde electromagnetice, iar la ieșirea din ghidaj – o rețea cu sute de noduri – aceștia se regăsesc grupați în modele greu de calculat clasic.

## Aplicabilitate

Un exemplu clasic de problemă care distinge categoric între calcularea clasică și cea cuantică este „factorizarea numerelor întregi mari”. Ea nu se pretează computerului binar, pentru că produsele de numere prime depășesc ușor câteva sute de cifre, însă merge bine cu algoritmul lui Shor. Și, cum multe chei publice de încifrare a datelor folosesc factorizarea întregilor, iată că potențialul de aplicabilitate al calculatoarelor cuantice iese la iveală.

În lume apar uneori probleme a căror rezolvare, de neconceput în abordarea algoritmilor clasici, se potrivește bine la calcul cuantic. Din diverse domenii: simulări de farmaceutică și biochimie; simulări meteo-climatice; instruirea automatelor/mașinilor (vezi Google); analize de rețelistică; matematică (logaritmi discreți, polinoamele Jones, ecuația Pell, determinarea coliziunilor din arborii NAND). Nesurprinzător, una dintre aplicațiile de succes constă în simularea proceselor de fizică cuantică sau de fizică stării solide.

La căutările în baze de date mari, prin folosirea algoritmului Grover se aplică mult mai puține iterații de sub-interogări decât prin algoritmii clasici (cu un ordin pătratic de mărime).

Înceiem cu o concluzie cu valoare de adevăr între 0 și 1, aplicând o simplificare didactică: genul de problemă cu aderență la calculul cuantic este cea în care singura cale de a o rezolva este să presupunem repetat niște răspunsuri oarecare și să le aplicăm spre verificare.

**Cercetătorii de la IBM defineau anterior un set de cerințe generice pentru construirea calculatorului cuantic:**

- » Să fie redimensionabil fizic (să i se poată crește numărul de qubiți);
- » qubiții să poată fi inițializați la orice valori;
- » timpii de parcurgere a porților logice cuantice să fie inferiori timpilor de „întinare” a proceselor (timpul tipic de evitare a contaminărilor din mediu poate baleia de la nano-sekunde la secunde, în funcție de temperatura mediului);
- » setul de porți logice să poată fi reconfigurat;
- » stările qubiților să poată fi citite cu ușurință.

## Abordări practice

Deja s-au cristalizat o serie de abordări concrete pentru materializarea computerelor cuantice, distincția făcând-o, desigur, principiul fizic exploatat:

- calculatoare bazate pe supraconductibilitate, în care qubitul este implementat prin starea unui minuscul circuit superconductor (la temperatură aproape de zero absolut);
- calculatorul cuantic folosind capcane de ioni – qubitul fiind constituit de starea internă a ionilor capturați;
- calculatorul cu latice optică, la care qubitul este dat de starea internă a unor atomi neutri capturați în laticia optică;
- calculatoare cu puncte cuantice, în care qubitul este dat de starea de spin a unui electron captat în „quantum dot”;
- calculatoare cu puncte cuantice de semiconductor, unde starea qubitului este dată de poziția electronului din interiorul unui „quantum dot” dublu;
- calculatorul cu rezonanță magnetică nucleară în lichid – qubitul este furnizat de spinul nuclear dintr-o moleculă dizolvată în câmp NMR;
- calculatorul cu rezonanță magnetică nucleară în solid – qubitul corespunde spinului nuclear al unui donator de fosfor aflat în siliciu;
- calculator cuantic cu electroni de heliu – qubitul este dat de spinul electronului;
- calculator bazat pe electrodinamica cuantică a cavității – qubitul se constituie din starea internă a atomilor capturați/cuplați în cavități;
- calculatoare cuantice optice – qubiții sunt realizați de către diverse stări ale câmpului electromagnetic;
- calculatorul cuantic cu diamant – qubitul este dat de spinul (electronic sau nuclear) al centrelor eliberate de azot în cristalul de diamant;
- calculatoare cuantice bazate pe tranzistori (sic!) – stările cuantice se obțin prin antrenarea golurilor pozitive folosind o capcană electrostatică;
- calculatoare cuantice cu cristale anorganice dopate cu ioni telurici – qubitul este realizat prin stările electronice interne ale unor dopanți din fibra optică.

## Calculatorul cuantic – de la concret la comercial

În lume sunt mai multe centre de cercetare (fie ale unor universități de prestigiu, fie din instituții private) care au imaginat și produs mașini de calcul cuantic, funcționând ca experimente sau aduse în stare de aplicare la rezolvarea unor probleme reale. Dintre acestea ne vom opri la compania canadiană D-Wave, știrile recente subliniind realizările acesteia în domeniul „quantum computing”.

În 2011, D-Wave Systems anunța primul dispozitiv cuantic comercial, pentru care compania a realizat un procesor de 128 qubiți (un cip folosind 128 de elemente logice superconductoare capabile de cuplări programabile pentru a realiza operațiuni utile). În același an, demara un contract cu Lockheed Martin (companie recunoscută îndeosebi pe piața proiectelor militare) având ca obiect sistemul „D-Wave One” găzduit la University of Southern California. (Lockheed Martin căuta o soluție avansată pentru testarea software-ului: în abordarea clasică, timpul necesar parcurgerii tuturor stărilor posibile în aplicațiile software crește exponențial cu creșterea complexității, pe când în abordarea cuantică creșterea ar fi liniară. Ne putem ușor imagina că dezvoltarea de software CAE complex – CFD, FEA – poate ridica probleme.)

Abordarea D-Wave a fost una pragmatică: ei s-au concentrat pe proiectarea unui cip cuantic destinat a rezolva anumite probleme date, și nu pe urmărirea principiilor cuantice ale unei mașini universale. Au urmat apoi realizările concrete ale cercetătorilor de la University of Bristol (calculator cuantic funcțional, pe principiu optic) și cele ale companiei IBM (efecte cuantice în circuite integrate cu supraconductibilitate). În 2012, apar în cursă mai multe universități (Oxford, Southern California, Delft, Iowa, California - Santa Barbara, New South Wales, Queensland). În noiembrie 2012 se raporta prima teleportare cuantică între obiecte macroscopice.

În mai 2013, Google anunța înființarea lui „Quantum Artificial Intelligence Lab”, găzduit la un centru de cercetare al NASA (Ames). Laboratorul va fi dotat cu un computer cuantic de 512 qubiți furnizat de... D-Wave Systems. Ne întoarcem, deci, la cei mai concreți. Deocamdată.

REDACȚIE@CHIP.RO

# SERVICII EDITORIALE ȘI TIPOGRAFICE COMPLETE

  
**3 D MEDIA  
COMMUNICATIONS**



**Tehnoredactare,  
pre-press, tipărire  
pliante, afișe,  
cataloge, reviste, cărți  
și alte materiale  
promoționale.**

**Producție CD-uri,  
DVD-uri 5GB, 9GB**



**Contact: 0741.248.348  
info@3dmc.ro**