ALGORITMUL CUANTIC GROVER ÎN SISTEMUL CLASIC DE CALCUL

Autor: Andrei RODIDEAL
Conducător ştiinţific: lec. sup. Galina MARUSIC

Universitatea Tehnică a Moldovei

Abstract: *În lucrare sunt date noţiuni generale despre calculator cuantic, logica cuantică, algoritmi cuantici, noţiune de algoritm Grover şi utilizarea algoritmului Grover.*

Cuvinte cheie: *Paralelism, superpoziţie, qubit, registru.*

1. Calculator cuantic, logica cuantică

Unitatea elementară folosită în informatica cuantică este qubit-ul (corespondentul cuantic al bit-ului clasic). Un calculator cuantic poate fi considerat ca un sistem multi-qubit. Din punct de vedere fizic, un qubit este un sistem fizic cu două stări diferite posibile, cum ar fi electronul cu cele două stări de spin sus şi jos, un foton cu cele două stări de polarizare orizontală şi verticală, sau un atom cu două stări energetice posibile. Un bit clasic este un sistem care poate exista în două stări distincte, care sunt folosite pentru a reprezenta 0 şi 1, adică un singur digit binar. Singurele operaţii posibile (porţi) într-un astfel de sistem sunt identitatea (0→0, 1→1) şi NOT (0→1, 1→0). În contrast, un qubit este un sistem cuantic cu două stări, descris de un spaţiu Hilbert complex, bi-dimensional. În acest spaţiu se poate alege o bază orto-normată formată din două stări cuantice, notate prin 0 şi 1, care constituie corespondentul valorilor 0 şi 1 ale bitului clasic.

Capacitatea unui calculator cuantic este datorată unui paralelism cuantic asociat cu principiul de superpoziţie. Aceasta înseamnă că un calculator cuantic poate procesa un număr mare de intrări clasice într-o singură rulare. Dar, problema mai dificilă o constituie extragerea informaţiei utile din starea de ieşire (starea finală). Această informaţie este, într-un anumit sens, ascunsă. Rezultatul unui proces de măsurare este inerent probabilistic şi probabilităţile diferitor stări de ieşire posibile sunt determinate de postulatele fundamentale ale mecanicii cuantice. În prezent, există totuşi algoritmi cuantici eficienţi care permit extragerea informaţiei utile din starea finală.

Unul dintre algoritmii cuantici a fost propus de Peter Shor în anul 1994 şi acesta rezolvă eficient problema descompunerii în factori primi: dat fiind un număr N impar compus, întreg şi pozitiv, să se găsească factorii primi în care el poate fi descompus. Aceasta este o problemă centrală în ştiinţa calculatoarelor şi se afirmă, deşi nu s-a demonstrat, că folosind un calculator clasic este dificil să se găsească factorii primi pentru un număr N dat. Algoritmul lui Shor rezolvă eficient problema factorizării unui număr întreg prin creşterea considerabilă a vitezei de calcul. Trebuie menţionat că există în prezent sistem de codificare, cum ar fi *RSA*, bazat pe faptul că nu există algoritmi eficienţi pentru rezolvarea problemei descompunerii în factori primi. Deci, algoritmul Shor implementat pe un calculator cuantic va înlocui actualul sistem de codificare *RSA*.

Au fost realizaţi şi alţi algoritmi cuantici care prezintă avantaje faţă de cei clasici. Astfel, L. Grover a arătat că folosind calculatorul cuantic se poate rezolva uşor problema găsirii unui anumit obiect într-o bază de date care conţine $N = 2^n$ obiecte. Cu un calculator clasic, ceea ce se poate face este să se parcurgă baza de date pînă ce se găseşte obiectul respectiv. Această cale va necesita deci N operaţii. În schimb, folosind calculatorul cuantic problema va putea fi rezolvată în $\sqrt{N}$ operaţii.

O a treia clasă de probleme importante privind algoritmii cuantici o constituie cea a simulării sistemelor fizice. De exemplu, se ştie că simularea unui sistem cuantic compus din mai multe particule aflate în interacţiune pe un calculator clasic este foarte dificilă deoarece dimensiunea spaţiului Hilbert al stărilor acestui sistem creşte exponenţial cu numărul de particule. Astfel, pentru un lanţ uni-dimensional compus din n particule cu spinul 1/2, dimensiunea acestui spaţiu este $2n$ şi deci o stare posibilă a sistemului respectiv este determinată de $2n$ numere complexe. În schimb, cu un calculator cuantic creşterea de memorie necesară este proporţională cu numărul n de particule şi este necesară o bază compusă numai din n qubiţi. Ca urmare, un calculator cuantic operînd pe un registru compus din cîteva zeci de qubiţi poate depăşi în performanţă orice calculator clasic actual. Desigur, această afirmaţie este adevărată numai dacă se pot realiza algoritmi cuantici

eficienți pentru extragerea informației utile din calculatorul cuantic. Este foarte interesant de observat că un calculator cuantic poate fi folosit nu numai pentru studiul proprietăților sistemelor multi-particule dar şi pentru determinarea dinamicii sistemelor clasice şi cuantice complexe [1].

2. Algoritmul Grover

Algoritmul Grover este un algoritm cuantic pentru căutare în baze de date nesortate cu N intrări în $O(N$ 1/2) timp şi folosind $O(\log N)$ spațiu de stocare (unde I este notația Landau, notația Bachmann–Landau, şi notația asimptotică). Acesta a fost inventat de Lov Grover în 1996.

În modele de calcul clasice, căutarea în baze de date nesortate, nu poate fi făcută mai rapid decît în timpul linear (doar căutarea prin fiecare element este optimă). Algoritmul Grover ilustrează faptul că, în modelul cuantic căutarea se poate face mai rapid decât în acest sens; de fapt complexitatea timpului $O(N1/2)$ este asimptotic cel mai rapid posibil pentru căutarea în baze de date nesortate în modelul cuantic. Algoritmul oferă o accelerare pătratică, spre deosebire de alți algoritmi cuantici, care pot oferi accelerare exponențială față de omologii clasici. Cu toate acestea, viteza pătratică este considerabilă cînd N este destul de mare.

Ca mulți algoritmi cuantici, algoritmul Grover este probabilist, în sensul că dă răspunsul corect cu grad ridicat de probabilitate. Probabilitatea de eşec poate fi redusă prin repetarea algoritmului. Un exemplu de un algoritm cuantic determinist este algoritmul Deutsch-Jozsa, care produce întotdeauna răspunsul corect.)

Algoritmul Grover este specific pentru a fi utilizat în calculatore cuantice, şi realizarea lui cu utilizarea tuturor posibilităților, pe maşinile cu arhitectura clasică este imposibilă. Cu toate acestea posibilitățile de calcul maşinilor obişnuite, permit modelarea comportării arhitecturii calculatorului cuantic.

În maşinele de calcul cuantice - cuantul informației (bit) este redat prin cubiți (qubit sau q-bit), sitemul cuantic bidimensional. În maşina clasică de calcul bitul poate fi în una din 2 stări: pentru simplețe 0 şi 1. În teoria cuantică qubit-ul se află în două sau mai multe stări – simultan, în fiecare din stările posibile el se află cu o anumită probabilitate.

De exemplu, se măsoară starea, în care se află qubit-ul, astfel avem probabilitatea q_0, că qubit-ul va fi in starea 0 şi probabilitatea q_1, că qubit-ul va fi in starea 1. În concordanță cu principiul superpoziției nu se poate spune în care stare se află qubit-ul în momentul de față, dar este posibil de dat probabilitatea unei sau altei stări ale qubit-ului:

$$|A\rangle = q_0|0\rangle + q_1|1\rangle \tag{1}$$

În condiții obişnuite $q_0 = q_1$. Acum dacă se vor lua 2 qubiți, fiecare la rîndul său avînd schema probabilistică de stări proprie, atunci ambii qubiți, în general, pot fi caracterizați prin înmulțirea tenzorială a spațiilor probabilistici:

$$|AB\rangle = \left[q_0|0\rangle + q_1|1\rangle\right]\left[q_0|0\rangle + q_1|1\rangle\right] = q_0q_0|00\rangle + q_0q_1|01\rangle + q_1q_0|10\rangle + q_1q_1|11\rangle \tag{2}$$

După cum se vede, este posibil de obținut din sistemul de 2 qubiți (registru biqubit) – patru rezultate posibile de măsurare. În cazul de față toate rezultatele de măsurare sunt la fel posibile, dar se poate de modificat cerințele exterioare astfel ca să se mărească probabilitatea rezultatului măsurat, de care este nevoie. Presupunem că vom mări q_1 q_1 pînă 0,9. Aceasta înseamnă, că dacă se vor lua în continuare măsurările stării registrului atunci cu probabilitatea 0,81 (0,90×0,90=0,81) vom primi starea $|00\rangle$ (sau la fel ca la măsurarea cazului 81 din 100 vom primi starea $|00\rangle$). În general qubiții sunt reprezentați prin 2^N diferite stări posibile ale registrului cuantic (este numit astfel analog registrului clasic – depozitul biților clasici) [3].

3. Descrierea schemei algoritmului Grover

Fie avem un registru cuantic cu N qubiți. Probabilitatea tuturor stărilor posibile se poate de prezentat sub formă de vector cu 2^N componente.

De exemplu vectorul de undă $|AB\rangle$ va fi reprezentat astfel:

$$\Psi = \begin{bmatrix} q_0^2 \\ q_0 q_1 \\ q_0 q_1 \\ q_1^2 \end{bmatrix} \tag{3}$$

Algoritmul Grover constă din 3 paşi:

a) Trecem registrul în starea de superpoziție $\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, ..., \frac{1}{\sqrt{N}}\right)$, adică egalăm probabilitatea tuturor stărilor *N*. Acest lucru poate fi făcut prin $O(\log N)$ operații. După legile mecanicii cuantice este posibil de schimbat vectorul de undă cu ajutorul operațiilor unitare, utilizăm „poarta Adamara". Ca rezultat, se obține un vector, toate componentele cărui sunt egale cu $\frac{1}{\sqrt{N}}$. Pe noi ne interesează doar starea *i*.

b) Repetăm cîteva ori următoarele transformări unitare: *R* (transformare din faza de rotație) şi *D* (transformarea de difuzie), de $O(\sqrt{N})$ ori. După fiecare iterație amplituda stării necesare se va schimba pînă la $2M(\Psi)+\Psi_i$, unde $M(\Psi)$ - valoarea medie componentelor vectorului după transformarea *R*, iar Ψ_i - amplituda stării dorite pînă la *R*.

$$R = \begin{bmatrix} 1 & 0 & 0 & \text{""} & 0 \\ 0 & 1 & 0 & \text{""} & 0 \\ 0 & 0 & -1 & \text{""} & 0 \\ \text{""} & \text{""""} & \text{""} & \text{""} & \text{""} \\ 0 & 0 & 0 & \text{""} & 1 \end{bmatrix} \tag{4}$$

Unde (4) este transformare din faza de rotație. Schimbă simbolul la starea necesară, la restul stărilor influențează ca operatorul unic. În matricea diagonală dată elementul în liniea *i* este –1, în restul 1.

$$D = W = \begin{bmatrix} -1+\frac{2}{N} & \frac{2}{N} & \text{""} & \frac{2}{N} \\ \frac{2}{N} & -1+\frac{2}{N} & \text{""} & \frac{2}{N} \\ \text{""} & \text{""} & \text{""} & \text{""} \\ \frac{2}{N} & \frac{2}{N} & \text{""} & -1+\frac{2}{N} \end{bmatrix} \tag{5}$$

Unde (5) este transformara de difuzie. Aceasta transformare poate fi interpretată ca inversiea în jurul mediei. Matricea de transformare poate fi elaborată prin diferența a 2 matrice: $W = T - I$, unde T – constă din $\frac{2}{N}$, I – matricea unitară.

c) Măsurăm starea sitemului. La măsurare vom obține starea dorită cu probabilitatea cel puțin 0,5.

În deosebire de algoritmi clasici strictețea obținerii rezultatului corect nu este proporțional numărului de iterații. Există un număr de itarații, după care probabilitatea rezultatului necesar se va micşora. Numărul de iterații optimal (*RD* repetări) va fi aproximativ $\frac{2}{\pi}\sqrt{N}$. Aceasta abordare este una din cele mai principale aparențe a metodicii cuantice [2].

4. Utilizarea Algoritmului Grover

Calculatoarele cuantice mult timp promit posibilitatea procesării super-rapide şi super-eficiente, şi în anul 2009 giantul căutării Google a sărit în viitor. Rapoartele ştiințifice afirmă că Google a cheltuit 3 ani

pentru dezvoltarea algoritmului cuantic care ar putea automat recunoaşte şi sorta obiecte ca imagini sau video.

Diferite echipe de cercetare lucrează asupra creării procesoarelor cuantice care stochează informaţiea în qubiţi (biţii cuantici), care pot reprezenta ambele stări a biţilor 0 şi 1 în acelaşi moment de timp. Aceasta dualitate a stării permite o procesare mai eficientă de stocare a informaţiei.

Un exemplu, dat din partea echipei Google, un calculator clasic ar putea avea nevoie, în mediu undeva într-un milion de sertare, pentru a găsi o minge ascunsă, dintre 500 de mii de imagini, iar un calculator cuantic ar putea găsi mingea doar căutînd în o mie de sertare – acest lucru fiind efectuat de către algoritmul Grover.

Google a utilizat un dispozitiv de calcul cuantic creat de către firma canadiană D-Wave. Dar lipsa de informaţii despre cum funcţionează cipul D-Wave a dus la scepticism şi anume la afirmaţia că dispozitivul nu funcţionează ca un calculator cuantic.

„Din păcate, nu este uşor de demonstrat că un sistem multi-qubit, cum ar fi cipul D-Wave într-adevăr emulează comportamentul cuantic dorit şi experimentale fizice diferitor instituţii se află încă în proces de caracterizare a cipului" a scris Hartmut Neven, liderul echipei Google a imaginii echipei de recunoaştere, pe blog-ul de cercetare Google.

Echipa de recunoaştere a imaginilor Google a elaborat acest algoritm special pentru căutarea imaginilor on-line şi pentru organizarea automată a fotografiilor.

Concluzii:

Este posibil să fie construit un calculator cuantic, în cît timp? Răspunsul este afirmativ privind posibilitatea de construire, dar cu privire la durata necesară trebuie de menţionat că există dificultăţi majore în realizarea lui. Pe lângă problema decoerenţei cuantice, trebuie să menţionăm şi dificultatea găsirii unor algoritmi cuantici noi şi eficienţi.

Este posibil de simulat algoritmi cuantici pe calculatoare clasice? Nu se cunoaşte, însă ce clasă de probleme pot fi simulate eficient pe un calculator cuantic? Se poate afirma că un calculator cuantic deschide perspective noi, dar el nu va putea fi realizat practic în următorii câţiva ani. Pentru a ne face o idee asupra duratei necesare trebuie să ne amintim de efortul enorm care a fost necesar pentru realizarea calculatorului clasic.

Experimente demonstrative, deşi modeste, au pus în evidenţă rezultate remarcabile nu numai pentru informatica cuantică, dar şi pentru verificarea principiilor fundamentale ale mecanicii cuantice. Se ştie că mecanica cuantică nu este o ştiinţă intuitivă şi deci informatica cuantică va conduce şi la o înţelegere mai bună a principiilor şi rezultatelor sale. Cercetările respective vor permite să se pună la punct metode experimentale de control a sistemelor cuantice individuale (atomi, electroni, fotoni, etc.).

Bibliografie

1. Grover L. K. *A Fast Quantum Mechanical Algorithm for Database Search // Proc. of 28th Ann. ACM Symp. on the Theory of Computing*, 1996, p.212-219.
2. G. Benenti, G. Casati, G. Strini *Principles of Quantum Computation and Information, Vol. IŞ Basic Concept*s, World Scientific, Singapore, 2004.
3. M. A. Nielsen, I. L. Chuang *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.