Quantum Computing Algorithms
- Grover's Search Algorithm -

March 26, 2024

Echipa

Stanciu Sergiu-Nicolas
Tudor Haulica
Alexia Aldea Elena
Razvan Dumitriu
Murica Andrei

Contents

1 Introducere in Quantum Computing **2**
1.1 Informatia clasica 2
1.2 Ket & Bra Notations (Dirac Notation) 2
1.3 Operatii probabilistice si matrici stochastice 3
1.4 Informatia quantica 3
1.5 Exemple de stari quantice (qubit states) 4
1.6 Operatii unitare 4

2 Grover's Algorithm Overview **6**
2.1 Cautarea nestructurata 6
2.2 Algoritmi de cautare 6
2.3 Porți de interogare de fază 6
2.4 Descrierea algoritmului 7
2.5 Analiza algoritmului 8

1 Introducere in Quantum Computing

1.1 Informatia clasica

Pentru a putea defini informatia dintr-un sistem quantic, trebuie mai intai sa vedem ce este informatia clasica si cum este reprezentata ea. O analogie foarte buna pentru informatia clasica ar fi un sistem numit X care se poate afla in una dintre starile sale la un moment dat. Multimea starilor acestui sistem se noteaza cu Σ si este o multime finita si nenula. De asemenea, sistemul X se afla se poate afla intr-o singura stare la un moment dat, fapt ce creste gradul ce incertidine despre X. Reprezentarea cunostintelor despre acest sistem se face pe baza unui vector de probabilitati corespunator fiecarei stari in care X se poate afla. (Un exemplu clasic il reprezinta un ban cu cele doua fete ale sale fiecare avand probabilitatea de $\frac{1}{2}$).

Astfel, apare notiunea de masure a unui sistem clasic. Prin masurarea unui sistem, ne referim la analizarea lui si recunoasterea starii in care se afla. In mod intuitiv, acest tip de masurare schimba vectorul de probabilitati al sistemului: daca sistemul X se afla in starea $\alpha \epsilon \Sigma$ (vectorul de stari), atunci noul vector de probabilitati va avea 0 pentru toate celelalte stari si 1 pentru α.

1.2 Ket & Bra Notations (Dirac Notation)

Fie Σ un set de stari intr-un sistem clasic si sa presupunem ca aceste stari au fost ordonate in corespondenta cu multimea de numere 1, 2, 3 ..., $|\Sigma|$(cardinalul multimii).

In acest caz, vom nota $|\alpha\rangle$ vectorul coloana care are 1 pe linia corespunzatoare lui $\alpha \epsilon \Sigma$, si 0 pentru toate celelalte intrari/linii.

Exemplu pentru $\Sigma = \{0, 1\}$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

In acelasi conditii ca mai sus, vom nota $\langle\alpha|$ vectorul linie care are 1 pe coloana corespunzatoare lui $\alpha \epsilon \Sigma$, si 0 pentru toate celelalte intrari/coloane.

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \; \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Pe baza acestor notatii pot aparea operatii deterministe intre vectori ce pot duce atat la un rezultat de tip scalar dar si la o matrice dupa cum se poate observa din urmatoarele operatii:

$$\langle a|b\rangle = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise} \end{cases}$$

*Acest produs se numeste produsul scalar dintre vectorii $|a\rangle$ si $|b\rangle$ intrucat, dupa cum se vede, are ca rezultat un scalar

$|a\rangle \langle b|$ = o matrice $\Sigma \times \Sigma$ in care elementul de pe pozitia (a, b) are valoare 1 si restul valorilor sunt 0.

1.3 Operatii probabilistice si matrici stochastice

Fie un set de stari clasice alese arbitrar. Descriem ca fiind setul cu toate operatiile probabilistice in termeni matematici, toate matricile stochastice care satisfac urmatoarele proprietati:

- Toate valorile din matrice sunt numere reale pozitive
- Suma valorilor de pe o coloana da 1

Echivalent, matricile stochastice sunt matricile ale caror coloane formeaza vectori de probabilitati pentru fiecare stare a sistemului.

De exemplu, sa consideram o operatie pe un bit unde, daca starea sistemului este 0 atunci aceasta nu se schimba, dar daca starea este 1 atunci cu o probabilitate de $\frac{1}{2}$ starea se muta la 0. Aceasta operatie poate fi reprezentata de matricea:

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

1.4 Informatia quantica

Acum vom vedea in ce consta mai exact informatia quantica, in care se alege un tip diferit de vector pentru a reprezenta o stare - in acest caz o stare quantica.

O stare quantica a unui sistem este reprezentat de un vector de coloana, similar cu vectorii probabilisti. La fel ca inainte, indicii vectorului quantic denumeste starile clasice ale sistemului. Vectorii ce reprezinta starile quantice sunt caracterizati de aceste 2 proprietati:

- Valorile unui vector quantic de stare sunt numere complexe
- Radical din suma valorilor absolute ale intrarilor unei stari quantice este egal cu 1

Norma Euclidiana a unui vector coloana:

$$\mathrm{v} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{pmatrix}$$

este notata si definita astfel:

$$||v|| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}$$

Note: Condiția ca suma valorilor absolute pătrate ale unui vector de stare cuantică să fie egală 1 este deci echivalent cu acel vector având norma euclidiană egală cu 1. Adică, vectorii de stare cuantice sunt vectori unitari în raport cu norma euclidiană.

1.5 Exemple de stari quantice (qubit states)

Termenul de *qubit* se refera la un sistem quantic al carui set de stari clasice este $0, 1$.

Acestea sunt exemple de stare quantice ale unui qubit:

$$\begin{pmatrix}1\\0\end{pmatrix} = |0\rangle \; si \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$$

$$\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

si

$$\begin{pmatrix}\frac{1+2i}{3}\\\frac{-2}{3}\end{pmatrix} = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

Putem spune ca aceste stari sunt valide verificand cele doua conditii enuntate mai sus:

- Toate valorile sunt numere complexe
- Radical din suma valorilor absolute da 1:

$$|1|^2 + |0|^2 = 1 \text{ si } |0|^2 + |1|^2 = 1$$
$$|\frac{1}{\sqrt{2}}|^2 + |\frac{1}{\sqrt{2}}| = \frac{1}{2} + \frac{1}{2} = 1$$
$$|\frac{1+2i}{3}|^2 + |-\frac{2}{3}|^2 = \frac{5}{9} + \frac{4}{9} = 1$$

Note: Toate aceste stari sunt combinatii liniare ale starilor $|0\rangle \, si \, |1\rangle$. Ce este interesant despre ele este faptul ca au o proprietate numita *superpozitie* a starilor 0 si 1. In contextul starilor quantice, "superpozitia" si "combinatia liniara" sunt in esenta sinonime.

In ultim lucru ce trebuie evidentiat: cand vrem sa folosim notatia bra - $\langle\alpha|$ - ne referim, intr-un context quantic, la vectorul linie obtinut prin transpunerea vectorului coloana si conjugarea acestuia (fiecare intrare din vector).

1.6 Operatii unitare

Până acum, s-ar putea să nu fie evident de ce informația cuantică este fundamental diferită de informația clasică. Adică, atunci când se măsoară o stare cuantică, probabilitatea de a obține fiecare stare clasică este dată de valoarea absolută pătrat a intrării vectorului corespunzătoare - așa că de ce să nu înregistrați pur și simplu aceste probabilități într-un vector de probabilitate?

Răspunsul, cel puțin parțial, este că setul de operații permise care pot fi efectuate pe o stare cuantică este diferit față de informațiile clasice. Similar cu setarea probabilistică, operațiile asupra stărilor cuantice sunt mapări liniare -

dar, în loc să fie reprezentate de matrici stocastice, ca în cazul clasic, operațiile pe vectorii de stare cuantică sunt reprezentate de matrici unitare.

O matrice patratica Λ ce are intrari/valori numere complexe este unitara daca si numai daca satisface urmatoarele ecuatii:

$$\Lambda\Lambda^T = 1_n$$
$$\Lambda^T\Lambda = 1_n$$

2 Grover's Algorithm Overview

2.1 Cautarea nestructurata

Fie $\Sigma = 0, 1$ denumit si alfabetul binar. Sa presupunem ca avem urmatoarea functie:

$$f : \Sigma^n \to \Sigma$$

pe care o putem calcula eficient.

Scopul este de a gasi o solutie, ce este un sir binar $x\epsilon\Sigma$ pentru care $f(x) = 1$. In general o astfel de computatie este o problema dificila, iar in particular daca datele de intrare reprezinta un circuit boolean pentru functia f atunci aceasta problema este NP-Complete. Acestea fiind spuse, un astfel de circuit boolean poate fi convertit usor intr-un circuit quantic pentru a implementa o operatie pe interogari sau o poarta de interogare.

Aceasta este o cautare nestructurata deoarece functia f este alease arbitrar - nu avem nicio certitudine/promisiune si nu ne putem baza pe faptul ca aceasta functie are o structura ce face gasirea solutiilor usoara.

2.2 Algoritmi de cautare

Sa presupun ca avem urmatoare problema:

- Input: $f : \Sigma^n \to \Sigma$
- Output: un sir x $\epsilon\Sigma^n$ ce satisface relatia f(x) = 1, sau "nicio solutie" daca nu exista astfel de siruri

Drept urmare putem face urmatoarea notatie:

N = 2^n

Prin iterarea tuturor sirurilor de forma $x\epsilon\Sigma^n$ si evaluand f la fiecare sir, putem rezolva problema Cautarii de mai sus folosind N interogari. Acesta este cel mai bun rezultat pe care il putem obtine cu un algoritm determinist intr-un context bazat pe un model de intergori.

Algoritmii probabilistici ofera imbunatatiri minore, dar tot necesita un numar linear de interogari fata de N.

Algoritmul lui Grover este un algoritm quantic pentru problema Cautarii ce necesita $O(\sqrt{N})$ interogari

2.3 Porți de interogare de fază

Multi algoritmi quantici specifici modelelor bazate pe interogari sunt exprimati in mod natural folosind porti de interogare de faza. Algoritmul lui Grover este un astfel de exemplu.

Presupunem ca avem acces la o functie de tipul $f : \Sigma^n \to \Sigma$ printr-o poarta de interogare:

$U_f : |a\rangle |x\rangle \rightarrow |a \oplus f(x)\rangle |x\rangle$ (pentru toate combinatiile de forma a $\epsilon \Sigma si x \epsilon \Sigma^n$

Poarta de interogare de faza pentru functia f opereaza astfel:

$Z_f : |x\rangle \rightarrow (-1)^f(x) |x\rangle$ (pentru orice x $\epsilon \Sigma^n$)

Pe langa operatia Z_f definita mai sus, vom mai avea nevoie de inca o poarta de interogare pentru function OR pe n-biti, ce este definita astfel:

$$\text{OR(x)} = \begin{cases} 0 & \text{if } x = 0^n \\ 1 & \text{if } x \neq 0^n \end{cases}$$

In mod explicit, poarta de interogare de faza specifica acestei functii opereaza astfel:

$$Z_O R |x\rangle = \begin{cases} |x\rangle & x = 0^n \\ -|x\rangle & x \neq 0^n \end{cases}$$

2.4 Descrierea algoritmului

Acum ca am putut defini cele 2 operatii necesare algoritmului, il putem descriere intr-un mod mai succint. Algoritmul lui Grover se bazeaza pe un numar t, ce reprezinta atat numarul de iteratii pe care le face, cat si numarul de interogari facute de functia f. Acest numar t nu este ales aleator sau specificat de Grover in planificarea algoritmului sau, ci poate fi determinat pe baza unor calcule.

Algoritmul lui Grover (pseudocod)

1. Initializam un registru Q de n biti cu starea $|0^n\rangle$ si aplicam operatorul Hadamard pe fiecare qubit din Q.
2. Aplicam operatia unitara $G = H^{\oplus} n Z_O R H^{(} \oplus n) Z_f$ pe registrul Q
3. Masuram qubitii din registrul Q si afisam sirul rezultat.

Algoritmul lui Grover poate fi aplicat pe o problema de cautare astfel:

- Alegem un numar t descris anterior
- Rulam algoritmul lui Grover pe functia f, folosind orice alegere am facut pentru t, pentru a obtine un sir $x \epsilon \Sigma^n$
- Interogam functia f cu sirul x si verificam daca e o solutie valida:
  - Daca f(x) = 1, atunci am gasit o solutie, drept urmare ne oprim si afisam x
  - Altfel, daca f(x) = 0 atunci putem rula procedura din nou, alegand un alt t, sau putem decide ca nu exista solutie.

2.5 Analiza algoritmului

Acum vom analiza algoritmul lui Grover pentru a înțelege cum funcționează. Vom începe cu ceea ce ar putea fi descris ca o analiză simbolică, în care calculăm modul în care operația Grover G acționează asupra anumitor stări, apoi vom lega această analiză simbolică de o imagine geometrică care este utilă pentru vizualizarea modului în care funcționează algoritmul.

2.5.1 Solutii si Non-solutii

Incepem prin a ne defini doua seturi de siruri:

$$A_0 = x\epsilon\Sigma^n : f(x) = 0$$
$$A_1 = x\epsilon\Sigma^n : f(x) = 1$$

Setul A_1 contine toate solutiile problemei noastre de cautare, iar A_0 contine sirurile care nu sunt solutii.