Groverov algoritam

Kvantna računala (SI)

8. siječnja 2021.

Pretraga nestruktururane baze

Razmatra se problem pretrage nestrukturirane baze podataka.

Neka je $f : \{0, \ldots, 2^n - 1\} \to \{0, 1\}$ takva da

$$f(x) = \delta_{xw} = \begin{cases} 0 & \text{za} \quad x \neq w \\ 1 & \text{za} \quad x = w \end{cases}$$

pri čemu je w, tzv. "winner", nepoznati broj koji želimo odrediti.

U potrazi za w (pretraga baze) klasični algoritam mora izvrijedniti f u prosijeku $2^n/2$ puta.

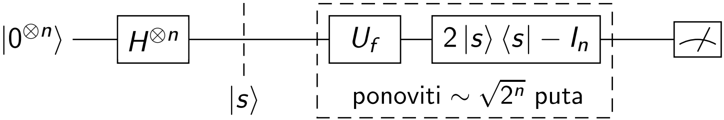
Kvantna implementacija funkcije $f(x) = \delta_{xw}$ ostvaruje se n-qubitnim unitarnim operatorom U_f sa svojstvom

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle , \qquad x = 0, \dots, 2^n - 1.$$

Unitarnost operatora U_f vidljiva je iz svojstva $U_f^2 = I$.

Operatore poput gore opisanog čije djelovanje smatramo nepoznatim, a algoritmom ga nastojimo razotkriti, zovemo *Quantum oracle* (kvantni prorok).

Logički krug Groverovog algoritma:



Uokvireni operator zovemo Groverovim operatorom. Njegovo djelovanje ponavljamo približno $\sqrt{2^n}$ puta.

Izlazno stanje sustava se u velikoj mjeri podudara s traženim stanjem $|w\rangle$.

Analiza toka Groverovog algoritma:

- Svaki od n qubitova početno u stanju $|0\rangle$ propušta se kroz Hadamardov operator. Time se sustav dovodi u stanje superpozicije svih stanja računalne baze s međusobno jednakim realnim koeficijentima,

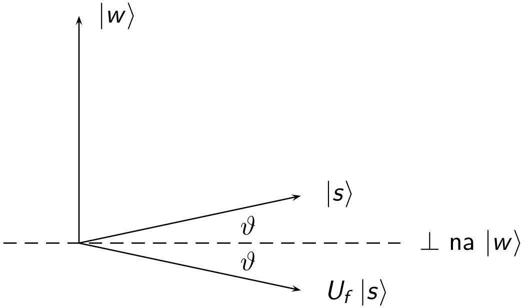
$$|s\rangle = H^{\otimes n} |0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle .$$

- Zahvaljujući realnosti koeficijenata, analizu toka algoritma moguće je provesti u Euklidovom prostoru dimenzije 2^n.

- Uočavamo da je, za velik n, stanje $|s\rangle$ "gotovo okomito" na svako stanje računalne baze, pa tako i na traženo stanje $|w\rangle$.
- Možemo reći da stanje $|s\rangle$ s "plohom" koja je okomita na $|w\rangle$ (u toj "plohi" leže sva stanja okomita na $|w\rangle$ te je njena dimenzija $n-1$) "zatvara kut ϑ" za koji vrijedi

$$\langle w|s\rangle = \frac{1}{\sqrt{2^n}} = \sin\vartheta \simeq \vartheta.$$

- Učinak operatora U_f na općenit vektor stanja sastoji se u promjeni predznaka koeficijenta uz bazni vektor $|w\rangle$. Promatramo li stanje kao vektor u ravnini koju razapinju $|w\rangle$ i $|s\rangle$, djelovanje U_f možemo shvatiti kao refleksiju stanja u osi koja je okomita na $|w\rangle$. Slika prikazuje refleksiju stanja $|s\rangle$:

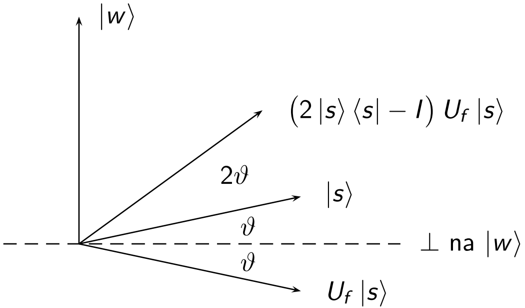


- Učinak operatora

$$|s\rangle\langle s| - (I - |s\rangle\langle s|) = 2|s\rangle\langle s| - I$$

možemo shvatiti kao refleksiju stanja u osi određenoj vektorom $|s\rangle$.

- Slika prikazuje stanje $U_f|s\rangle$ i refleksiju tog stanja:



- S obzirom da je kompozicija dvaju refleksija u osima koje zatvaraju kut α istovjetna rotaciji za kut 2α, djelovanje Groverovog operatora

$$G = \left(2\left|s\right\rangle\left\langle s\right| - I\right) U_f$$

možemo shvatiti kao rotaciju stanja u ravnini razapetoj s $|w\rangle$ i $|s\rangle$ za kut

$$2\vartheta.$$

- Početno stanje sustava $|s\rangle$ zakrenuto je u odnosu na os koja je okomita na $|w\rangle$ za kut ϑ, a nakon k primjena Groverovog operatora, ono je zakrenuto za kut

$$(2k+1)\,\vartheta.$$

- Groverov operator primijenit ćemo onoliko puta koliko je potrebno da bi se početno stanje sustava $|s\rangle$ zakrenulo što je moguće bliže traženom stanju $|w\rangle$. Iz uvjeta

$$(2k+1)\vartheta \simeq \pi/2,$$

  uz $2^n \gg 1$, slijedi

$$k \simeq \sqrt{2^n}$$

Pokazali smo da Groverov algoritam omogućuje nalaženje tražene vrijednosti uz $\sqrt{2^n}$ evaluacija funkcije f, dok je klasičnim algoritmom za to potrebno $2^n/2$ evaluacija. S obzirom da je omjer tih brojeva razmjeran n-toj potenciji, Groverov algoritam predstavlja eksponencijalno ubrzanje u odnosu na klasični algoritam.