Kvantumalgoritmusok
Kvantum keresés - Grover algoritmus

Nem struktúrált keresés

Legyen $f : \{0,1\}^n \to \{0,1\}$ egy függvény, melyet effektíven ki tudjuk számolni. Célunk egy olyan megoldást találni, azaz olyan x sztringet találni, melyre $f(x) = 1$.

Nem struktúrált keresés

Legyen $f : \{0,1\}^n \to \{0,1\}$ egy függvény, melyet effektíven ki tudjuk számolni. Célunk egy olyan megoldást találni, azaz olyan x sztringet találni, melyre $f(x) = 1$.

- Input: $f : \{0,1\}^n \to \{0,1\}$
- Output: $x \in \{0,1\}^n$ úgy, hogy $f(x) = 1$ vagy "Nincs megoldás"

Nem struktúrált keresés

Legyen $f : \{0,1\}^n \to \{0,1\}$ egy függvény, melyet effektíven ki tudjuk számolni. Célunk egy olyan megoldást találni, azaz olyan x sztringet találni, melyre $f(x) = 1$.

- Input: $f : \{0,1\}^n \to \{0,1\}$
- Output: $x \in \{0,1\}^n$ úgy, hogy $f(x) = 1$ vagy "Nincs megoldás"

Ez a keresés nem struktúrált, mivel f tetszőleges és egyáltalán nem biztos, hogy könnyen tudunk megoldást találni.

Jelöljünk $N = 2^n$. Ekkor a nem struktúrált keresés N darab számolással megoldható.

Grover algoritmusa egy kvantum algoritmus, amely ezt a keresést $\mathcal{O}(\sqrt{N})$ lépésben megoldja.

Jelöljünk $N = 2^n$. Ekkor a nem struktúrált keresés N darab számolással megoldható.

Grover algoritmusa egy kvantum algoritmus, amely ezt a keresést $\mathcal{O}(\sqrt{N})$ lépésben megoldja.

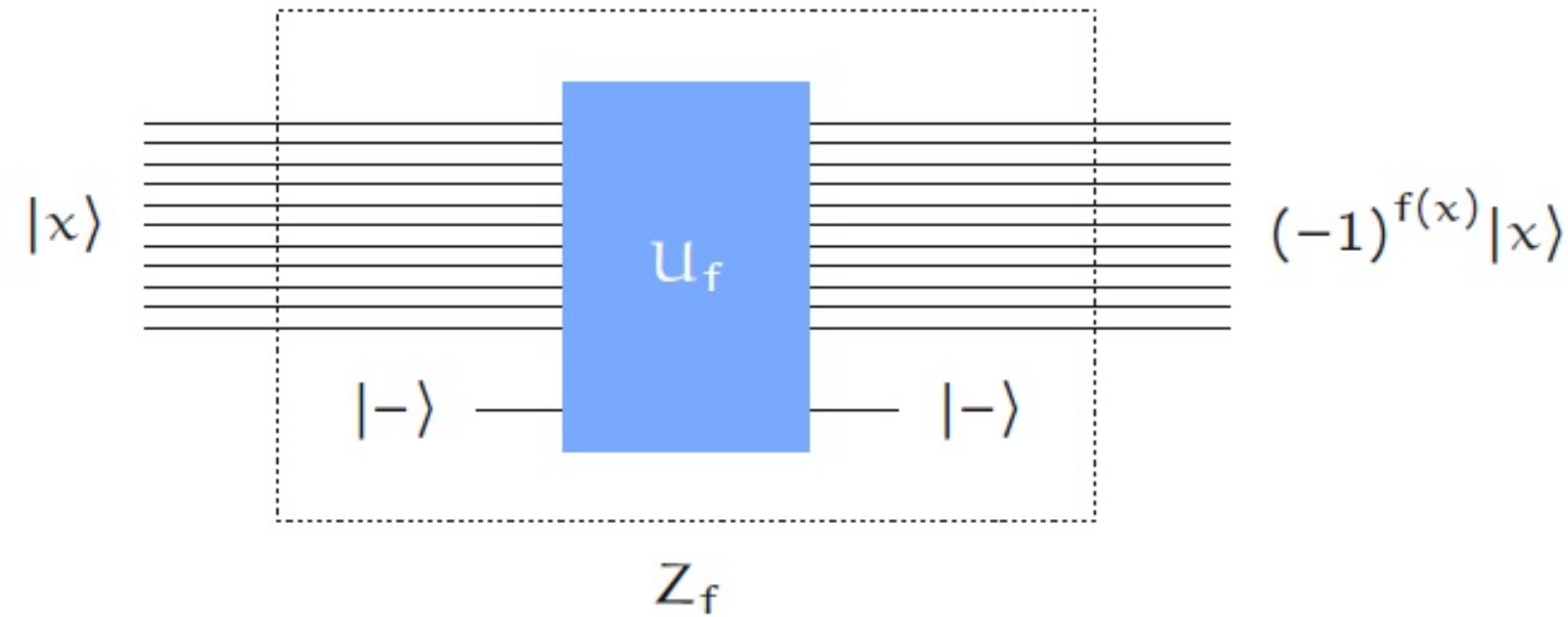
A továbbiakban feltesszük, hogy az f függvényt egy U_f operátorral tudjuk modellezni:

$$U_f : |\alpha\rangle |x\rangle \mapsto |\alpha \oplus f(x)\rangle |x\rangle \quad \forall \alpha \in \{0,1\} \text{ and } x \in \{0,1\}^n$$

Fáziskeresés

A fáziskereső kapu f esetén működik a következőképpen:

$$Z_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle \quad \forall x \in \{0,1\}^n$$



Fáziskapu OR operátor esetén

Az n-bites OR operátor fáziskapuja a következőképpen néz ki minden $x \in \{0,1\}^n$ esetén:

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

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

A Grover operátor

A Grover operátor definíciója

A Grover operátor

A Grover operátor definíciója

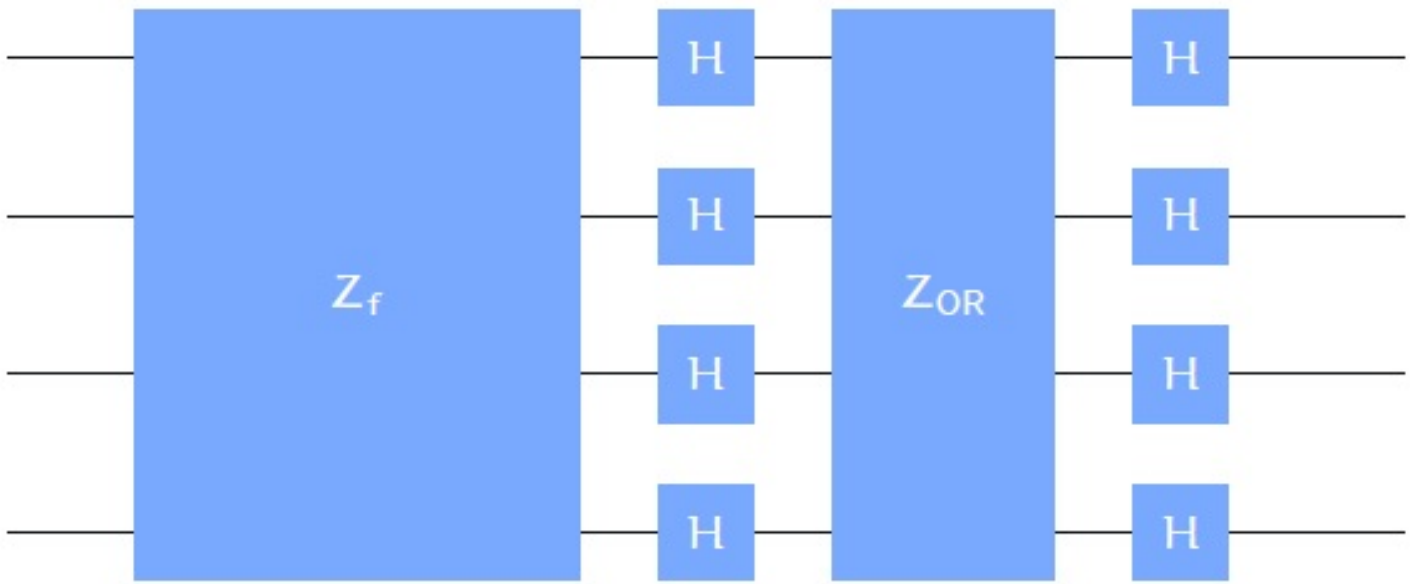
$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f$$

A Grover operátor

A Grover operátor definíciója

$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f$$

Z_f az f fáziskapuja és Z_{OR} az n-bites OR művelet fáziskapuja.



Grover algoritmus

1. Iniciálás: n qubit a $H^{\otimes n} |0^n\rangle$ állapotban

Grover algoritmus

1. Iniciálás: n qubit a $H^{\otimes n} |0^n\rangle$ állapotban
2. Iteráció: Grover operátor alkalmazása t-szer

Grover algoritmus

1. Iniciálás: n qubit a $H^{\otimes n} |0^n\rangle$ állapotban
2. Iteráció: Grover operátor alkalmazása t-szer
3. Mérés: sztenderd bázis mérés vezet egy lehetséges megoldáshoz

Tipikus alkalmazása

Tipikus alkalmazása

1. Válasszunk egy t számot, hány iterációt szeretnénk.

Tipikus alkalmazása

1. Válasszunk egy t számot, hány iterációt szeretnénk.
2. Alkalmazzuk a Grover algoritmust t-szer, kapunk egy lehetséges megoldást: x

Tipikus alkalmazása

1. Válasszunk egy t számot, hány iterációt szeretnénk.
2. Alkalmazzuk a Grover algoritmust t-szer, kapunk egy lehetséges megoldást: x
3. Ellenőrízzük a megoldást. Ha $f(x) = 1$, akkor x megoldás és output, ha nem akkor "nincs megoldás" az output.

Megoldások és nem-megoldások

Összegyújtjük a megoldásokat és nem-megoldásokat két halmazban:

$$A_0 = \{x \in \{0,1\}^n : f(x) = 0\}, A_1 = \{x \in \{0,1\}^n : f(x) = 1\}$$

Minket egységes szuperpozíciók ezen halmazok felett érdekelnek:

$$|A_0\rangle = \frac{1}{\sqrt{|A_0|}} \sum_{x \in A_0} |x\rangle$$

$$|A_1\rangle = \frac{1}{\sqrt{|A_1|}} \sum_{x \in A_1} |x\rangle$$

Fő ötletek

Inicializálás:

$$|u\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Ez az állapot a $|A_0\rangle$ és $|A_1\rangle$ által generált altérben van, azaz felírható azok segítségével a következőképpen:

Fő ötletek

Inicializálás:

$$|u\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Ez az állapot a $|A_0\rangle$ és $|A_1\rangle$ által generált altérben van, azaz felírható azok segítségével a következőképpen:

$$|u\rangle = \sqrt{\frac{|A_0|}{N}}\,|A_0\rangle + \sqrt{\frac{|A_1|}{N}}\,|A_1\rangle$$

Továbbá, ez az állapot ugyanebben az altérben marad, ahányszor is alkalmazzuk a Grover operátort.

Hogyan hat a Grover operátor

A Grover operátort két részre tudjuk bontani:

$$G = (H^{\otimes n} Z_{OR} H^{\otimes n})(Z_f)$$

Tudjuk, hogy Z_f úgy van definiálva hogy

$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle \ \ \forall x \in \{0,1\}^n$$

Ennek a hatása $|A_0\rangle$ és $|A_1\rangle$-n egyszerű:

$$Z_f |A_0\rangle = |A_0\rangle$$

$$Z_f |A_1\rangle = -|A_1\rangle$$

A Z_{OR} hasonlóan:

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

De ezt másképp is lehet leírni:

$$Z_{OR} = 2 |0^n\rangle \langle 0^n| - \mathbb{I}$$

Ezt felhasználva, most a Grover operátor első részét is át lehet írni

$$H^{\otimes n} Z_{OR} H^{\otimes n} = H^{\otimes n}(2 |0^n\rangle \langle 0^n| - \mathbb{I}) H^{\otimes n} = 2 |u\rangle \langle u| - \mathbb{I}$$

Felhasználva az előzőeket, azt kapjuk, hogy a Grover operátor hatása $|A_0\rangle$-n és $|A_1\rangle$-n a következő:

$$G\,|A_0\rangle = (2\,|u\rangle\,\langle u| - \mathbb{I})Z_f\,|A_0\rangle =$$

$$(2\,|u\rangle\,\langle u| - \mathbb{I})\,|A_0\rangle = 2\sqrt{\frac{|\,A_0\,|}{N}}\,|u\rangle - |A_0\rangle =$$

$$2\sqrt{\frac{|\,A_0\,|}{N}}\left(\sqrt{\frac{|\,A_0\,|}{N}}\,|A_0\rangle + \sqrt{\frac{|\,A_1\,|}{N}}\,|A_1\rangle\right) - |A_0\rangle =$$

$$\frac{|\,A_0\,| - |\,A_1\,|}{N}\,|A_0\rangle + \frac{2\sqrt{|\,A_0\,||\,A_1\,|}}{N}\,|A_1\rangle$$

$$G\left|A_1\right\rangle = (2\left|u\right\rangle\left\langle u\right| - \mathbb{I})Z_f\left|A_1\right\rangle =$$

$$(\mathbb{I} - 2\left|u\right\rangle\left\langle u\right|)\left|A_1\right\rangle = \left|A_1\right\rangle - 2\sqrt{\frac{|\ A_1\ |}{N}}\left|u\right\rangle =$$

$$\left|A_1\right\rangle - 2\sqrt{\frac{|\ A_0\ |}{N}}\left(\sqrt{\frac{|\ A_0\ |}{N}}\left|A_0\right\rangle + \sqrt{\frac{|\ A_1\ |}{N}}\left|A_1\right\rangle\right) =$$

$$-\frac{2\sqrt{|\ A_0\ ||\ A_1\ |}}{N}\left|A_0\right\rangle + \frac{|\ A_0\ | - |\ A_1\ |}{N}\left|A_1\right\rangle$$

A G hatása az $\{|A_0\rangle, |A_1\rangle\}$ által generált altérben le lehet írni a következő 2×2-es mátrix segítségével:

$$M = \begin{pmatrix} \frac{|A_0|-|A_1|}{N} & -\frac{2\sqrt{|A_0|\cdot|A_1|}}{N} \\ \frac{2\sqrt{|A_0|\cdot|A_1|}}{N} & \frac{|A_0|-|A_1|}{N} \end{pmatrix} =$$

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix}^2$$

A G hatása az $\{|A_0\rangle, |A_1\rangle\}$ által generált altérben le lehet írni a következő 2×2-es mátrix segítségével:

$$M = \begin{pmatrix} \frac{|A_0|-|A_1|}{N} & -\frac{2\sqrt{|A_0|\cdot|A_1|}}{N} \\ \frac{2\sqrt{|A_0|\cdot|A_1|}}{N} & \frac{|A_0|-|A_1|}{N} \end{pmatrix} =$$

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix}^2$$

Ez pedig egy forgatás mátrixa.

Forgatás mátrix

Legyen $\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$.

Forgatás mátrix

Legyen $\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$. Ekkor

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Forgatás mátrix

Legyen $\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right)$. Ekkor

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

és így

$$M = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}$$

Tehát a Grover operátor minden alkalmazásánál a kvantum állapotvektor el lesz forgatva 2θ szöggel.

$$|u\rangle = \cos(\theta)\,|A_0\rangle + \sin(\theta)\,|A_1\rangle$$

$$G\,|u\rangle = \cos(3\theta)\,|A_0\rangle + \sin(3\theta)\,|A_1\rangle$$

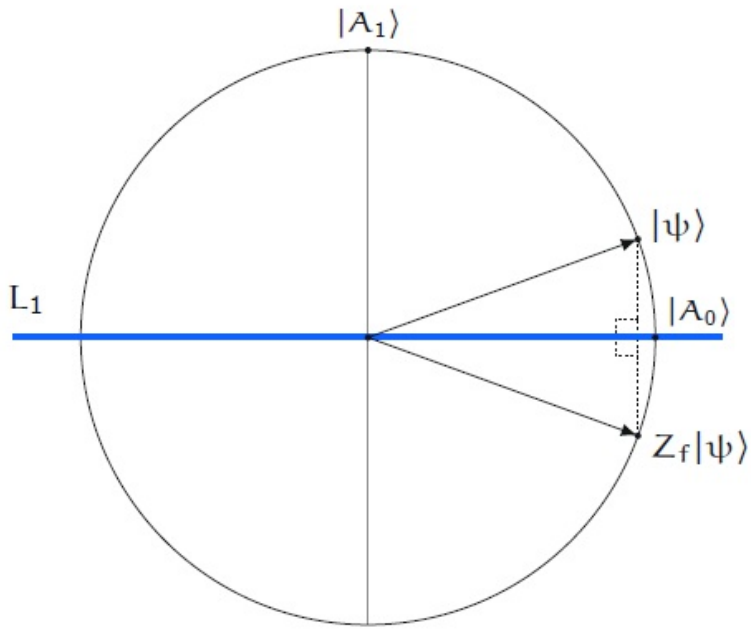
$$G^2\,|u\rangle = \cos(5\theta)\,|A_0\rangle + \sin(5\theta)\,|A_1\rangle$$

$$\vdots$$

$$G^t\,|u\rangle = \cos((2t+1)\theta)\,|A_0\rangle + \sin((2t+1)\theta)\,|A_1\rangle$$

Geometriai jelentősége

A Grover operátor két tükrözés kompozíciója. Két tükrözés kompozíciója pedig egy forgatás.

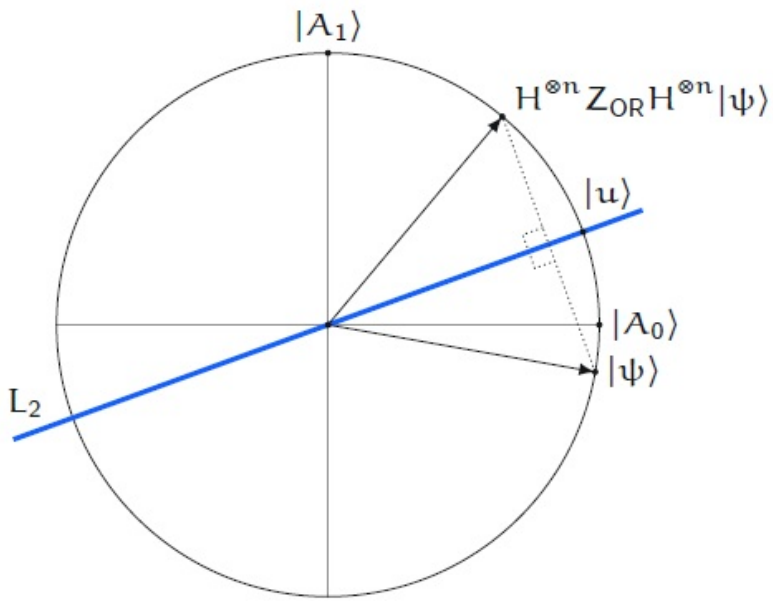


Z_f egy tükrözés az L_1 egyenesre.

$$Z_f |A_0\rangle = |A_0\rangle$$

$$Z_f |A_1\rangle = -|A_1\rangle$$

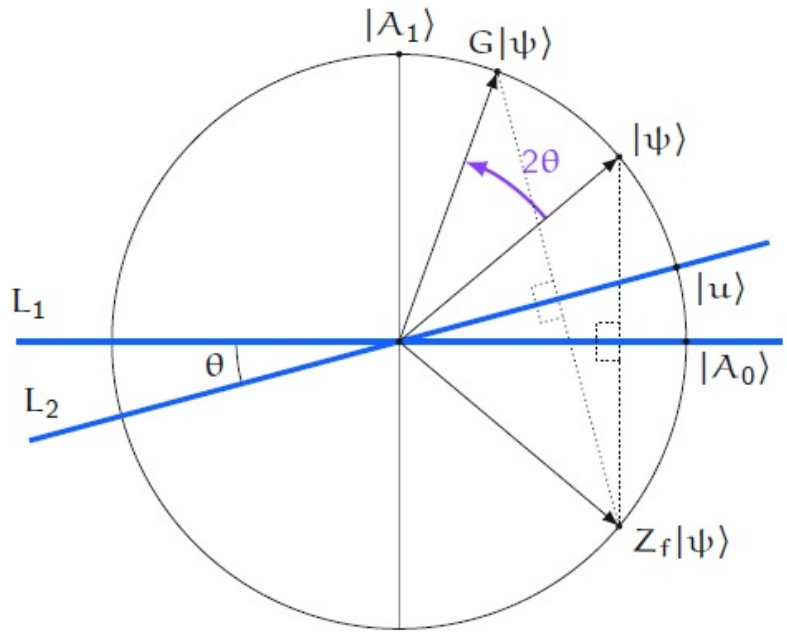
Geometriai jelentősége



$H^{\otimes n} Z_{OR} H^{\otimes n}$ egy tükrözés az L_2 egyenesre.

$$H^{\otimes n} Z_{OR} H^{\otimes n} = 2 |u\rangle \langle u| - \mathbb{I}$$

Geometriai jelentősége



Két tükrözés kompozíciója pedig egy forgatás a két tükrözési tengely közti szög (θ) kétszeresével.

Mérés

A

$$\alpha \left| A_0 \right\rangle + \beta \left| A_1 \right\rangle$$

kvantumállapot mérésekor kapunk egy $x \in A_1$ megoldást $\mid \beta \mid^2$ valószínűséggel.

Mérés

A

$$\alpha \left| A_0 \right\rangle + \beta \left| A_1 \right\rangle$$

kvantumállapot mérésekor kapunk egy $x \in A_1$ megoldást $|\ \beta\ |^2$ valószínűséggel.
Ha mérünk t iteráció után, akkor

$$\sin^2((2t+1)\theta)$$

valószínűséggel kapunk egy $x \in A_1$ megoldást.

Mérés

A

$$\alpha \left| A_0 \right\rangle + \beta \left| A_1 \right\rangle$$

kvantumállapot mérésekor kapunk egy $x \in A_1$ megoldást $\mid \beta \mid^2$ valószínűséggel.
Ha mérünk t iteráció után, akkor

$$\sin^2((2t+1)\theta)$$

valószínűséggel kapunk egy $x \in A_1$ megoldást.
Ezt a valószínűséget szeretnénk maximalizálni. Tehát $\left| A_1 \right\rangle$ a célállapotunk.

Ahhoz, hogy a valószínűség minél közelebb legyen 1-hez és t minimális legyen, azt szeretnénk elérni, hogy

$$(2t+1)\theta \approx \frac{\pi}{2} \Leftrightarrow t \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

Tehát $t = \lfloor \frac{\pi}{4\theta} \rfloor$.

Fontos észben tartanunk, hogy t egész szám, és θ függ a megoldások számától A_1-ben.

Egyértelmű keresés

Tegyük fel, hogy van pontosan egy $z \in \{0,1\}^n$, melyre $f(z) = 1$.

Egyértelmű keresés

Tegyük fel, hogy van pontosan egy $z \in \{0,1\}^n$, melyre $f(z) = 1$.

Ebben az esetben $s = \mid A_1 \mid = 1$ és így

$$\theta = \sin^{-1}\left(\sqrt{\frac{1}{N}}\right) \approx \sqrt{\frac{1}{N}}.$$

Egyértelmű keresés

Tegyük fel, hogy van pontosan egy $z \in \{0,1\}^n$, melyre $f(z) = 1$.

Ebben az esetben $s = |\ A_1\ | = 1$ és így

$$\theta = \sin^{-1}\left(\sqrt{\frac{1}{N}}\right) \approx \sqrt{\frac{1}{N}}.$$

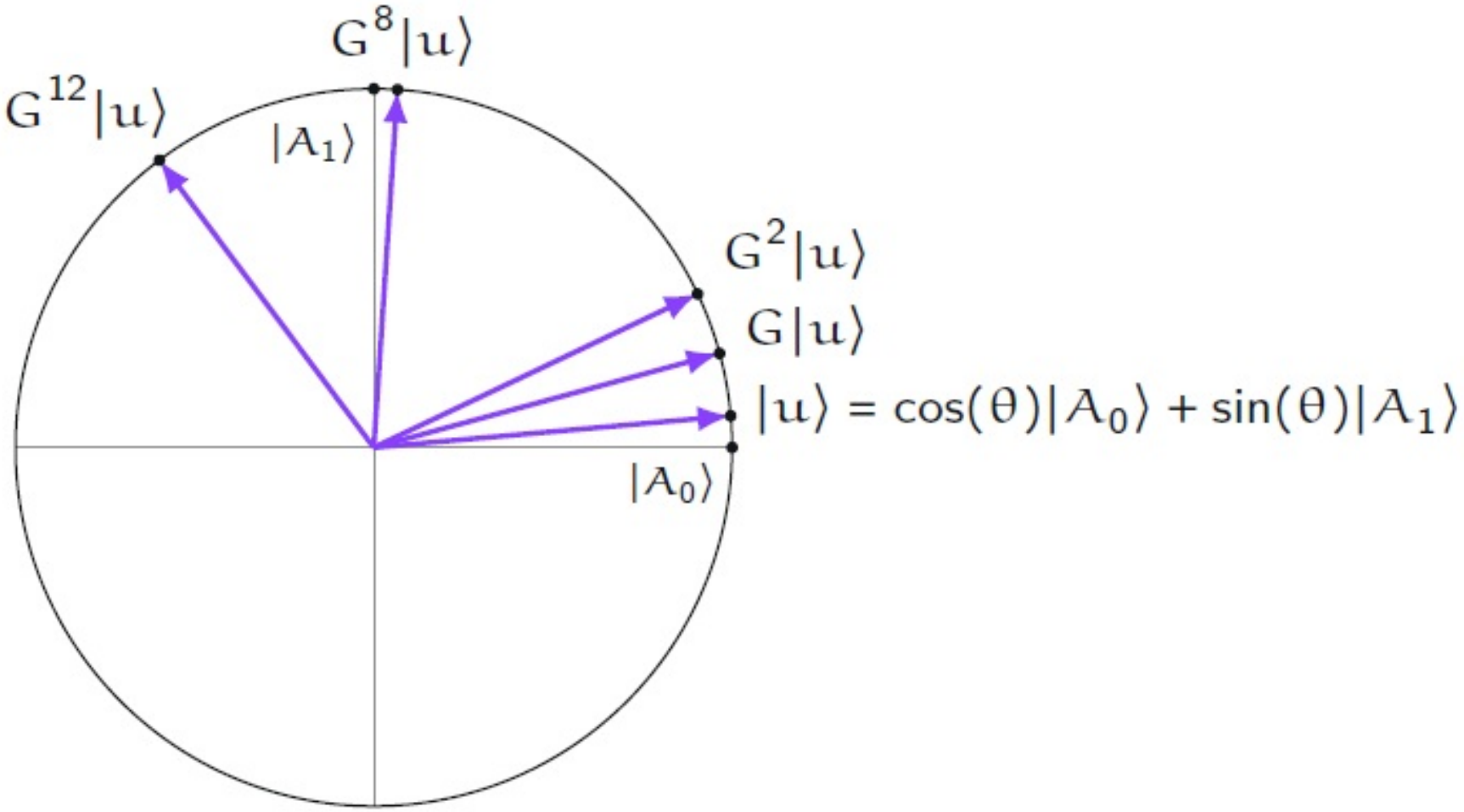
Ekkor

$$t \approx \lfloor \frac{\pi}{4}\sqrt{N} \rfloor.$$

Ami azt jelenti, hogy $\mathcal{O}(\sqrt{N})$ lépést fog tenni az algoritmus.

Példa

Ha $N = 128$, akkor $t\lfloor \frac{\pi}{4\theta} \rfloor = 8$.



t iteráció után méréskor megkapjuk az $x \in A_1$ megoldást

$$P(N, 1) = \sin^2((2t + 1)\theta)$$

valószínűséggel.

t iteráció után méréskor megkapjuk az $x \in A_1$ megoldást

$$P(N,1) = \sin^2((2t+1)\theta)$$

valószínűséggel.

Bizonyítható, hogy $P(N,1) \geq 1 - \frac{1}{N}$.

Több megoldás

Ha $N = 128$ és $s = 4$ (s a megoldások száma), akkor

$$\theta = \sin^{-1}\left(\sqrt{\frac{s}{N}}\right) = 0.17777...$$

és

$$t = \lfloor \frac{\pi}{4\theta} \rfloor = 4$$

Minden $s \in \{1, \ldots, N\}$ esetén

$$P(N, s) \geq max\{1 - \frac{s}{N}, \frac{s}{N}\}$$

Iterációk száma t

A Grover algoritmus minden iterációjánál egy számítást végez.
Hogyan függ össze t N-nel és s-sel?

Iterációk száma t

A Grover algoritmus minden iterációjánál egy számítást végez.
Hogyan függ össze t N-nel és s-sel?
Mivel $\theta = \sin^{-1}\left(\sqrt{\frac{s}{N}}\right)$ és $t = \lfloor \frac{\pi}{4\theta} \rfloor$ így

$$t \leq \frac{\pi}{4\theta} \leq \frac{\pi}{4}\sqrt{\frac{N}{s}}$$

ami azt jelenti, hogy

$$t = \mathcal{O}\left(\sqrt{\frac{N}{s}}\right)$$

Nem ismert számú megoldás van

Ha nem tudjuk hány megoldás van, akkor válasszunk $t \in \{1, \ldots, \lfloor \frac{\pi}{4}\sqrt{N} \rfloor\}$ véletlenül, egyenletes eloszlás szerint.

Nem ismert számú megoldás van

Ha nem tudjuk hány megoldás van, akkor válasszunk $t \in \{1, \ldots, \lfloor \frac{\pi}{4}\sqrt{N} \rfloor\}$ véletlenül, egyenletes eloszlás szerint.

1. A valószínűsége, hogy találjunk megoldást legalább 40%.
2. A lépések száma $\mathcal{O}(\sqrt{N})$.

Összefoglaló megjegyzések

- Grover algoritmusa azimptotikusan optimális.
- Grover algoritmusa széleskörűen alkalmazható.
- A módszert, melyet a Grover algoritmusban használjuk, általánosítható.