האלגוריתם של Grover

שוב מתבוננים בבעיה ה bb.

נניח נתונה $f:\{0,1\}^n \to \{0,1\}$ נתונה לחישוב יעיל.

כיוון שיש כלי יעיל U $\quad U:|x,b\rangle = |x, b\oplus f(x)\rangle$

נקרא לכל הפעלה של U, **קריאה אורקל ל f**

כל קריאה bb כי אנו משתמשים רק בערך של f מהשאלה, ולא במבנה שלה, או במבנה של האלגוריתם שמחשב אותה.

<u>מטרתנו</u>: לענות על השאלה הבאה: יש x כך ש $f(x)=1$?
ואם כן למצוא אותו.

זהו unstructured search כי אנו לא מניחים שום מבנה על f, (אם למשל, לא מניחים מונוטוניות של f)

הערה 1: לשם הפשטות נניח שיש x בודד שמקיים כך ש $f(x)=1$, ומטרתנו למצוא אותו.
אבל נוכיח שהאלגוריתם יעבוד לכל מספר.

הערה 2: נניח שמספר ה x כך ש $f(x)=1$ יהיה קטן והוא אפסי שונה מ 0, וקטן מ 2^n

(המקרה 0 או 2^n מטופלים בנפרד.
ההנחה שאנו יודעים את מספר הפתרונות הוא יותר מדויק, ולמעשה נראה איך להסיר הנחה זו)

חיפושים

1. קלט: $f:\{0,1\}^n \to \{0,1\}$ נתונה כמעגל
ידוע ש x_0 יחיד כך ש $f(x_0)=1$.

פלט: x_0 (בקירוב).

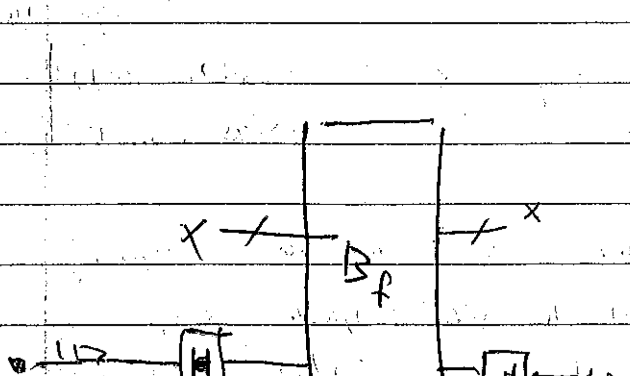
תזכורת: נגדיר כי $Z_f|x\rangle = (-1)^{f(x)}|x\rangle$

$$Z_f = \begin{array}{r} x \neq x_0 \\ x = x_0 \\ \\ \end{array} \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

ונגדיר כי
$$Z_0|x\rangle = \begin{cases} |x\rangle & x \neq 0\ldots0 \\ -|x\rangle & x = 0\ldots0 \end{cases}$$

$$Z_0 \quad \begin{array}{r} x = 0\ldots0 \\ \\ \\ \end{array} \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

מימוש המעגל Z_f:



(1) $\boxed{\text{קריאה אחת ל-} f}$

(2) $Y = \{x \mid f(x)=1\}$
$N = \{x \mid f(x)=0\}$

$x\in Y$, $f(x)=1$: $|x,1\rangle \to |x,0-1\rangle \to |x,f(x)\rangle - |x,\overline{f(x)}\rangle$

$= |x,1\rangle - |x,0\rangle \to -\left[|x,0\rangle - |x,1\rangle\right] = -x\otimes\left[|0\rangle-|1\rangle\right] \to -|x,1\rangle$

$= (-1)^{f(x)}\,|x\rangle \otimes |1\rangle$

$x\in N$, $f(x)=0$: $|x,1\rangle \Rightarrow |x,0-1\rangle \Rightarrow |x,f(x)\rangle - |x,\overline{f(x)}\rangle = |x,0\rangle - |x,1\rangle$

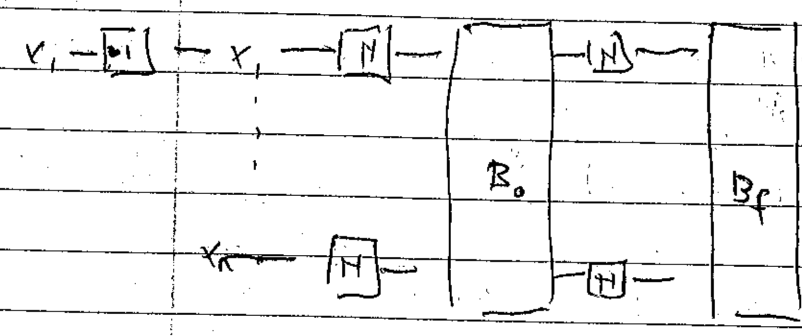
$= |x\rangle\left[|0\rangle-|1\rangle\right] = |x\rangle|1\rangle = (-1)^{f(x)}|x\rangle\otimes|1\rangle$

מגדיר למעשה Z_0, הפך רק שהפעם $f'(x)=\begin{cases}1 & x=0\cdots0\\ 0 & \text{אחרת}\end{cases}$

בשביל זה - קורות אותו דבר f.

<u>איטרציה שלמה של האלגוריתם של Grover !</u>

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$



מפעילים את האלגוריתם k איטרציות (עוצר אם k הושג)

ואז מודדים x בבסיס הסטנדרטי.

ואם $f(x)=1$ מוצאים אותו בסוף (אחרת, לא הצלחנו).

$k = \left\lfloor \frac{\pi}{4\theta} \right\rfloor$, $\theta = \arcsin\left(\sqrt{\frac{a}{N}}\right)$

a מס' הפתרונות המספקים

מצב התחלתי $\vec{\psi} = \frac{1}{\sqrt{2^n}}\sum_x |x\rangle$

$a = |A|$ נגדיר שני קבוצות

$b = |B|$

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

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

נסמן: Z_f, $H^{\otimes n} Z_0 H^{\otimes n}$ ו G ונבחן את $|A\rangle$ $|Y\rangle$ ו $|B\rangle$

בנוסף

$$Z_f |A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} \underbrace{Z_f |x\rangle}_{(-1)^{f(x)}|x\rangle} = -\frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle = -|A\rangle$$

$$Z_f |B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} Z_f(x) = |B\rangle$$

Z_f

$$Z_0 = I - 2|0\rangle\langle 0|$$

$$-H^{\otimes n} Z_0 H^{\otimes n} = -H^{\otimes n} (I - 2|0\rangle\langle 0|) H^{\otimes n}$$

$$= \underbrace{-H^{\otimes n} H^{\otimes n}}_{} + 2 H^{\otimes n} |0\rangle\langle 0| H^{\otimes n}$$

$$= -I + 2|\vec{1}\rangle\langle\vec{1}| \stackrel{?}{=} B$$

$$|\vec{1}\rangle = \sqrt{\frac{a}{2^n}} \sum_{x \in A} \frac{|x\rangle}{\sqrt{a}} + \sqrt{\frac{b}{2^n}} \sum_{x \in B} \frac{|x\rangle}{\sqrt{b}} = \sqrt{\frac{a}{2^n}} |A\rangle + \sqrt{\frac{b}{2^n}} |B\rangle$$

$$H^{\otimes n} Z_0 H^{\otimes n} |A\rangle = |A\rangle - 2|\vec{1}\rangle \sum_{x \in A} \frac{1}{\sqrt{N}} \frac{1}{\sqrt{a}}$$ מכך

$|B\rangle \perp |A\rangle$

$$= |A\rangle - 2\sqrt{\frac{a}{N}} |\vec{1}\rangle$$

$$H^{\otimes n} Z_0 H^{\otimes n} |B\rangle = |B\rangle - 2\sqrt{\frac{b}{N}} |\vec{1}\rangle$$

(4)

$$B\,|1\rangle = (2\,|1\rangle\langle 1| - I)\,|1\rangle = |\vec{1}\rangle$$

$$|1\rangle = \underbrace{\sqrt{\frac{a}{N}}}_{\sin(\theta)}\,|Y\rangle + \underbrace{\sqrt{\frac{b}{N}}}_{\cos(\theta)}\,|N\rangle$$

$$\theta = \arcsin\left(\sqrt{\frac{a}{N}}\right)$$

$$|1^{\perp}\rangle = \cos\theta\,|Y\rangle - \sin(\theta)\,|N\rangle$$

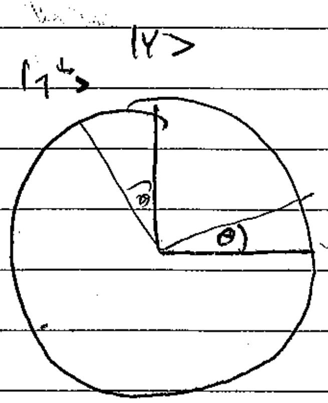
$$\langle 1 | 1^{\perp}\rangle = \sin\theta\cos\theta - \cos\theta\sin\theta = 0$$

$$B\,|1^{\perp}\rangle = (2\,|1\rangle\langle 1| - I)\left(\sqrt{\frac{b}{N}}\,|Y\rangle - \sqrt{\frac{a}{N}}\,|N\rangle\right)$$

$$= 2\sqrt{\frac{b}{N}}\,\underbrace{\langle 1|Y\rangle}_{\sqrt{\frac{a}{N}} = \frac{a}{\sqrt{aN}}}\,|1\rangle - 2\sqrt{\frac{a}{N}}\,\underbrace{\langle 1|N\rangle}_{\sqrt{\frac{b}{N}}}\,|1\rangle - \sqrt{\frac{b}{N}}\,|Y\rangle + \sqrt{\frac{a}{N}}\,|N\rangle$$

$$= \left(\cancel{2\frac{\sqrt{ab}}{N}} - \cancel{2\frac{\sqrt{ab}}{N}}\right)|1\rangle - \left[\underbrace{\sqrt{\frac{b}{N}}}_{\cos\theta}\,|Y\rangle - \underbrace{\sqrt{\frac{a}{N}}}_{\sin\theta}\,|N\rangle\right] = -\,|1^{\perp}\rangle$$

$$B\,1^{\perp} = (2\,|1\rangle\langle 1| - I)\,1^{\perp} = 2\,|1\rangle\underbrace{\langle 1|1^{\perp}\rangle}_{0} - 1^{\perp} = -1^{\perp}$$



זה המישור $\mathbb{R}^2$ הנפרש ע"י $|N\rangle$ ו־$|Y\rangle$

נסכם מה שראינו:

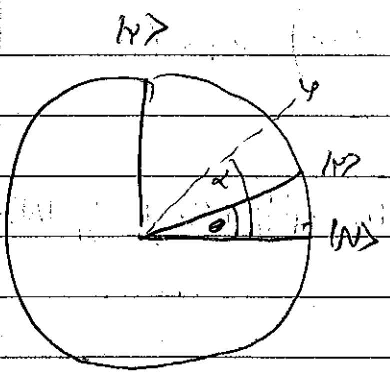
עלינו לא ממש!

~~[illegible]~~

$|\vec{1}\rangle = \cos\theta\,|N\rangle + \sin\theta\,|Y\rangle$

הטרנספורמציה B: שיקוף סביב $|\vec{1}\rangle$
הטרנספורמציה Z_f: " סביב $|N\rangle$

הטרנספורמציה G: שיקוף סביב $|\vec{1}\rangle$ ואז שיקוף סביב $|N\rangle$.

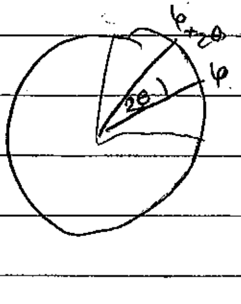


מה עושה G? $G = B \cdot Z_f$

אם נקח וקטור כלשהו α מ־$|N\rangle$

שלב 1 שיקוף סביב $|N\rangle$
נקבל $\varphi_{-\alpha}$

שלב 2 שיקוף סביב $|Y\rangle$
נקבל $\varphi_{\alpha+2\theta}$



זה סיבוב בזווית 2θ.

אנחנו מחפשים את כזה שהוא $\psi_{+\theta}$.

אם נפעיל את θ בערך $\frac{\pi}{4\theta} = \left(\frac{\pi/2}{2\theta}\right)$ פעמים,

נגיע קרוב מאוד לשם

ובשיטה הזאת נקבל [illegible] בסיכוי גבוה.

הערה: [illegible] רק שאנו יודעים כמה x

אנו גם [illegible] קרוב מספיק לשם

שזה אומר [illegible].

כיון ש $\psi_{k\theta}$ רק קרוב לשם [illegible] לשם

[illegible] הסבר [illegible].

אבל כיון שאנחנו מוליכים בקפיצות של 2θ

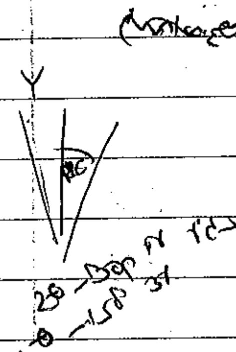
[illegible] $\theta \Rightarrow$ [illegible]

$a = o(N)$ במקרה

~~[illegible]~~

~~[illegible]~~

~~[illegible]~~



[גודל השגיאה n $\sin \cos^2(\theta)$ זה

$\sin\theta = \sqrt{\frac{a}{N}}$ כאשר

$\sin^2\theta = \frac{a}{N}$

בפרט $a = \frac{N}{2}$ (שאז [illegible] $\theta = 45$) ~~[illegible]~~ $\frac{1}{N}$

ולכן $\frac{1}{2}$ שגיאה, ובהסתברות [illegible].

אם $N \gg a$, השגיאה ~~[illegible]~~ $= \sqrt{\frac{a}{N}}$

[illegible] שגיאה [illegible]. ~~[illegible]~~

~~$\sin(2\theta) = 2\sin\theta\cos\theta = 2\sqrt{\frac{a}{N}}\sqrt{\frac{b}{N}} = \frac{2\sqrt{ab}}{N}$ [illegible]~~

(בגלל סדרי גודל [illegible] $2(n)$ [illegible] $(\ast)$ [illegible])

מה לעשות אם לא ידוע את a?

סעיף 1 — אם $a=\Omega(n)$ אפשר פשוט לנחש.

תרגיל 2 — אחרת, ננסה $k=2^0, 2^1, \dots, 2^{\log n}$ כל פעם הקוד מוסיף לב (הסתברות הצלחה $\geq \frac{1}{3}$ להצליח) אם $x\in A$, אחרת לא יש בעיה בכל הערך (הנכון) עם אמפליטודה הסתברות הצלחה שאר ה-t המקורי $\geq 1-\frac{1}{n}$, ומספר שאלות $\sqrt{n}\log(n)$.

~~[illegible]~~

סעיף 2: G הוא סיבוב ב-2θ

$$G=\begin{pmatrix}\cos 2\theta & -\sin 2\theta\\ \sin 2\theta & \cos 2\theta\end{pmatrix}$$

ערכים עצמיים: $\lambda_1+\lambda_2=2\cos 2\theta$, $\lambda_1\cdot\lambda_2=1$, $\lambda_1=\bar{\lambda}_2=\lambda_2^{-1}$

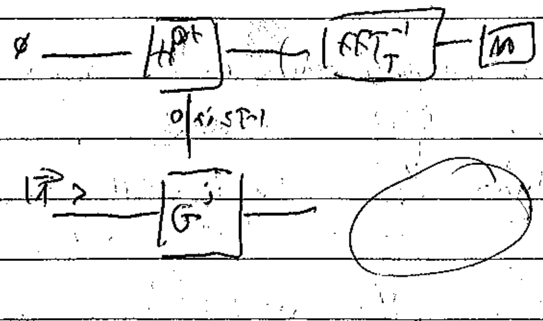
$$\lambda_1+\lambda_2=2\,\mathrm{Real}(\lambda_1)=2\cos 2\theta$$

$$\boxed{\begin{aligned}\lambda_1&=\cos 2\theta+b\,i & b&=\sin(2\theta)\\ \lambda_2&=\cos 2\theta-\sin(2\theta)\,i\end{aligned}}$$

כלומר $\lambda_1=e^{2\theta i}$, $\lambda_2=e^{-2\theta i}$

לכן ל-G יש ו"ע v_1,v_2 (לא מקסימום [illegible])

נעשה phase estimation!



אפשר לחשב בבסיס v_1, v_2.

במקרה של V_1 מקבלים הערכה ל-$\tilde{\theta}$ ס

במקרה השני ל- θ (וזה נעשה ...)

בכל מקרה אנו מקבלים הערכה ל $\tilde{\theta} = \arcsin\sqrt{\frac{a}{N}}$

$\sin\tilde{\theta} = \sqrt{\frac{a}{N}}$

כאן בעיה

להכניס כופל

$\sqrt{N}\sin\tilde{\theta} = \sqrt{a}$

כיון שאנו מעריכים θ' ע"י הבדיקה של Grover

אנו מבצעים ל $T = c\sqrt{N}$

ולכן הקירוב הוא עם $\delta = \frac{3}{4}$ מוצא θ' כך ש $|\theta' - \theta| \le \frac{1}{c\sqrt{N}}$

$$|\sin\tilde{\theta} - \sin\theta| \overset{?}{=} \cos(z)\,|\tilde{\theta} - \theta| \le |\tilde{\theta} - \theta| \le \frac{1}{c\sqrt{N}}$$ מתקיים

משפט ערך הביניים

$$|\underbrace{\sqrt{N}\sin\tilde{\theta}}_{\sqrt{a}} - \sqrt{N}\sin\theta| \le \frac{1}{c} < 1$$

ומכאן

ולכן אפשר לקרב את $\sqrt{a}$ עד כדי 1

ולכן את a עד כדי $2a$ כלומר a קבוע. $(a+1)^2 - a^2 = 2a+1$

כלומר השגת קירוב בסדר a הכי ...

• אפשר לחזור על הניסוי כמה פעמים, ולקחת את התוצאה

הכי שכיחה, ולהגדיל את הסתברות ההצלחה.