

האלגוריתם של גרובר (Grover)

זו כח האין את היתרון של מחש קוונטי באשר יש מפרק
 קרי - מציאות - ליגד זיקה. מה רגזי קצת מלא מנה?
 דבר קטן של מידת הסידור - השלם - הצי במופ - דבר יחדיו -
 היום בין BPP - NP. במאמר

Strengths & weaknesses of quantum computing 1977 BBBV (Bennett, Bernstein, Brassard & Vazirani)

במה כי קטנה - במחש באורך מילד קוונטי לא יא קטן דלה קיוני
 (אקסטרנליזם) - הצי - NP. סמוך או יגד במקדי, עובד הופד
 כי בזה דמיון לבנה הוא דזיק.

ליגד זיק, היסוד של הקצת הדעה: $F: \{0,1\}^N \rightarrow \{0,1\}$
 נקרא רכיבית הוא קיו x כך $F(x) = 1$ ודקה ס - ממלה
 אחר. הקטן חקצו - $NP \rightarrow$ הוא שליו מאלפני - ע"י מוול
 אפי דיונין קיו x , במולול V נקדי

$$x \in L \Leftrightarrow \exists w \overset{38}{V}(x, w) = 1$$

דיונין הסלתי נקצת דמיון האולף. סמוך, מוח רני ~~x~~
 להיחל F - קיו או Q סלסולציה של קחיה אפי
 לא היסוד F - נקצת דמיון יגד האולפני ענין, עזר
 דעו - NP , נקדי - עזר במולול V הוא דק מוח מול
 קחיה מפי, אפי חקצת בסידור - נוסח קחיהן לבנה - מול האולף
 עזר גינה יגד פול לוסן או Q היסוד ולקדי ומה רחלם ע
 היסוד "היגד" היגד - מוח - V
 117

אין תגית באתר מנהל פורום - אתם יכולים לעזור? !

$$F: [N] \rightarrow \{0,1\}$$

$$\{0,1\}^N \cong$$

$$x \text{ ש } F(x) = 0$$

סדר x^* הוא נאיב (עקב $F(x^*) = 1$), והוא נמצא ב- $\{0,1\}^N$ רגילי x^* . בהמשך נראה שמקרה זה ידוע ויחד עם זאת, למעשה (ואם נרצה) יש הרבה דוגמאות (ראו למשל, משפט של ארמסטרונג על $F \equiv 0$)

זהו דוגמה של פונקציה קלאסית - פונקציות אלו אינן ניתנות לזיוף $\Omega(N)$ למעשה: אדם שמנסה לזייף, צריך לפחות $\frac{2N}{3}$ דגימות. למעשה $\frac{1}{3}$ מהמרחב.

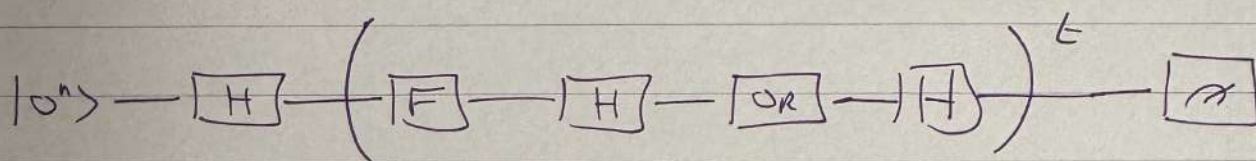
Grover search

נמצא חסותי אלו - תהליך חיפוש - $O(\sqrt{N})$ קוויץ' - חיפוש.

דוגמה: חיפוש - יש מיליון מילים, ויש לזכור $\Omega(\sqrt{N})$ מילים.

ההוכחה הקלאסית - נניח N - מספר המילים. נניח k - מספר המילים הנכונות. אז יש $\frac{N}{k}$ מילים לא נכונות. נניח m - מספר המילים הנכונות. אז יש $\frac{N}{m}$ מילים לא נכונות. אז ההוכחה היא: דוגמה נכונה.

מה יקרה אם ננסה - Rotate-compute-rotate - מה יהיה האורך? כן, נראה F - פונקציה.

[illegible]

עצמו קח'ה רב'ה ע' ו' א' OR כ' F מ'ק'ה ק'ה'ה:
מ'ק'ה ק'ה'ה ו'כ'ה:

$$\text{OR } |x_x\rangle = \frac{2}{\sqrt{2}} |0\rangle - |x_x\rangle$$

כאשר, $\alpha \in \mathbb{R}$ OR $\alpha \in \mathbb{C}$ "משפחה" $\rightarrow$ הקבוצה $\langle \chi_\alpha \rangle$ (x) סדר גודל הסדר "מסומן".

$$\text{OR } |x_x\rangle = \text{OR } \frac{1}{\sqrt{N}} \sum_y K_x(y) |y\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_y (-1)^{\langle x, y \rangle} \text{OR} |y\rangle$$

$$= \frac{1}{\sqrt{N}} \left[|0\rangle - \sum_{y \neq 0} (-1)^{\langle x, y \rangle} |y\rangle \right]$$

$$= \frac{1}{\sqrt{N}} \left[2|0\rangle - \sum_y (-1)^{\langle x, y \rangle} |y\rangle \right]$$

$$= \frac{1}{\sqrt{2}} |0\rangle - |x_x\rangle$$

! ^J)

$$|g\rangle = \alpha \underbrace{\sum_{x \neq x^*} |x\rangle}_{\triangleq |\bar{x}^*\rangle} - \beta |x^*\rangle$$

6 ארסו: מ נ קר]

$$|g\rangle \xrightarrow{\textcircled{1}} |F\rangle \xrightarrow{\textcircled{2}} |H\rangle \xrightarrow{\textcircled{3}} |OR\rangle \xrightarrow{\textcircled{4}} |H\rangle$$

מכאן

$$\textcircled{1} = F|g\rangle = \alpha |\bar{x}^*\rangle + \beta |x^*\rangle$$

$$\textcircled{2} = \alpha \sum_{x \neq x^*} |x_x\rangle + \beta |x_{x^*}\rangle$$

$$= \alpha \sum_x |x_x\rangle + (\beta - \alpha) |x_{x^*}\rangle$$

גור

$$\sum_x |x_x\rangle = \sqrt{N} |0\rangle$$

מכאן

$$\sum_x |x_x\rangle = \sum_x \frac{1}{\sqrt{N}} \sum_y (-1)^{\langle x, y \rangle} |y\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_y |y\rangle \left[\underbrace{\sum_x (-1)^{\langle x, y \rangle}}_{= \begin{cases} 0 & y \neq 0 \\ N & y = 0 \end{cases}} \right] = \sqrt{N} |0\rangle$$

15

pd

$$\textcircled{2} = \alpha \sqrt{N} |0\rangle + (\beta - \alpha) |\chi_{x^*}\rangle$$

$$\textcircled{3} = \text{OR } \textcircled{2} = \alpha \sqrt{N} |0\rangle + (\beta - \alpha) \left[\frac{2}{\sqrt{N}} |0\rangle - |\chi_{x^*}\rangle \right]$$

$$= \left(\alpha \sqrt{N} + \frac{2(\beta - \alpha)}{\sqrt{N}} \right) |0\rangle + (\alpha - \beta) |\chi_{x^*}\rangle$$

⇐

$$\textcircled{4} = H\textcircled{3} = \underbrace{\left(\alpha \sqrt{N} + \frac{2(\beta - \alpha)}{\sqrt{N}} \right)}_{\triangleq \delta} \underbrace{|\chi_0\rangle}_{\frac{1}{\sqrt{N}} \sum_x |x\rangle} + (\alpha - \beta) |x^*\rangle$$

$$= \frac{\delta}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle - \left(\beta - \alpha - \frac{\delta}{\sqrt{N}} \right) |x^*\rangle$$

$$= \left(\alpha + \frac{2(\beta - \alpha)}{N} \right) |x\rangle - \left(\beta - 2\alpha - \frac{2(\beta - \alpha)}{N} \right) |x^*\rangle$$

WB

$$(\alpha, \beta) \mapsto (\alpha', \beta')$$

$$\alpha' = \alpha + \frac{2(\beta - \alpha)}{N}$$

$$\beta' = \beta - 2\alpha - \frac{2(\beta - \alpha)}{N}$$

19.10

$$\alpha_0 = \beta_0 = \frac{1}{\sqrt{N}}$$

כנסת דמיון

חלק מהמאמר מתייחס לנקודה

$$\alpha_1 = \frac{1}{\sqrt{N}} \quad \beta_1 = -\frac{1}{\sqrt{N}}$$

אם $\frac{2(\beta_0)}{N}$ נחלקים נקבלים
ההפרש

$$\alpha' \approx \alpha \quad \beta' \approx \beta - 2\alpha$$

בואו נקבע $\alpha = 1$ ונחלק $\beta - 1$ ב- N

$$\beta_2^* = -\frac{3}{\sqrt{N}} \quad \beta_3 = -\frac{5}{\sqrt{N}} \quad \dots$$

למה $\Theta(\sqrt{N})$

המאמר מתייחס ל- β שגודלו $\Theta(\sqrt{N})$ במקרה של $\beta \in \mathbb{R}$, במקרה של $\beta \in \mathbb{R}$ regime-1, $\beta \in \mathbb{R}$ regime-2, $\beta \in \mathbb{R}$ regime-3.

לפי ההנחה של β חסום β על ידי $\sqrt{N}$

$$t = \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor$$

אם β חסום β על ידי $\sqrt{N}$ אז X^* קרוב ל-1, כלומר $P[X^*] \geq 1 - \frac{1}{N}$

$$P[X^*] \geq 1 - \frac{1}{N}$$

המאמר מתייחס ל- β שגודלו $\Theta(\sqrt{N})$ במקרה של $\beta \in \mathbb{R}$, במקרה של $\beta \in \mathbb{R}$ regime-1, $\beta \in \mathbb{R}$ regime-2, $\beta \in \mathbb{R}$ regime-3.

→ הרצון של שומר המזל הוא שיהיה מסוגל לדעת
 מהו המספר של המזל הזה שיש לו מספר של המזל הזה.

2-to-1 Problem

$$F: [N] \rightarrow \text{Colors}$$

נתון פונקציה

היא מקבלת מספר מ-1 עד N ומחזירה צבע

הפונקציה היא 2-1

כל צבע c מופיע בדיוק פעם אחת. כלומר, הפונקציה היא 2-1.

השאלה היא: האם ניתן למצוא את המספר x כך ש-

$F(x) = c$

בזמן $O(N^{1/3})$ או פחות. (הערה: הפונקציה היא 2-1).

במקרה (ספיקה)

הפונקציה היא 2-1, כלומר, לכל צבע c יש בדיוק שני מספרים x, y כך ש- $F(x) = F(y) = c$.
 הפונקציה היא 2-1, כלומר, לכל צבע c יש בדיוק שני מספרים x, y כך ש- $F(x) = F(y) = c$.

$$G: [N] \setminus L \rightarrow \{0, 1\}$$

$$x \mapsto \begin{cases} 1 & \text{if } F(x) \in A \\ 0 & \text{otherwise} \end{cases}$$

נתון פונקציה G המקבלת מספר מ-1 עד N ומחזירה 0 או 1.

הפונקציה G היא 2-1, כלומר, לכל מספר x יש בדיוק שני מספרים y, z כך ש- $G(y) = G(z) = x$.

השאלה היא: האם ניתן למצוא את המספר x כך ש- $G(x) = 1$ בזמן $O(N^{1/3})$ או פחות.

הפונקציה G היא 2-1, כלומר, לכל מספר x יש בדיוק שני מספרים y, z כך ש- $G(y) = G(z) = x$.

הפונקציה G היא 2-1, כלומר, לכל מספר x יש בדיוק שני מספרים y, z כך ש- $G(y) = G(z) = x$.
 הפונקציה G היא 2-1, כלומר, לכל מספר x יש בדיוק שני מספרים y, z כך ש- $G(y) = G(z) = x$.

הפונקציה G היא 2-1, כלומר, לכל מספר x יש בדיוק שני מספרים y, z כך ש- $G(y) = G(z) = x$.

$$\# \text{queries} = N^{1/3} + \sqrt{\frac{N}{K}} = O(N^{1/3})$$