

אייף האר

אקאלר'המים קוואט'ים

• מבנה האל

שור \Leftarrow סימון \Leftarrow צוטל-ג'אזא
Shor Simon Deutsch-Josza



• גיפ'ים ג'ראבר
Grover

מוטיבציה: חיפוש במערך לא ממויין



דוגמה - חיפוש בספר טלפונים באורך N

- חיפוש לפי שם הוא קל ($\log N$ קריאות)
- חיפוש לפי טלפון הוא קשה (N קריאות)

דוגמה – בעיית אילוצים: מצאו את ההשמה

$\underline{x} \in \{0,1\}^n$ שמספקת את כל האילוצים ($N = 2^n$ קריאות)

$$\begin{aligned} &(x_1 \text{ OR } x_3 \text{ OR } x_8) \\ &\text{AND} \\ &(\bar{x}_2 \text{ OR } x_4 \text{ OR } \bar{x}_5) \\ &\text{AND} \\ &\vdots \end{aligned}$$

גרובר מוצא איבר במערך לא ממויין בעזרת \sqrt{N} קריאות בלבד!

← חיסכון ריבועי בהמון בעיות



הבעיה של גרובר – ניסוח פורמלי

הבעיה: נתונה פונקציה $f: \{0,1\}^n \mapsto \{0,1\}$ שפולטת 0 על כל הקלטים פרט לאחד $f(\underline{x}^*) = 1$. מצאו את \underline{x}^* ("הקלט הטוב") בכמה שפחות קריאות ל- f .

המספר הנבדק? מיקום בספר

\underline{x}	$f(\underline{x})$
000	0
001	0
⋮	⋮
\underline{x}^*	1
⋮	⋮
111	0

$N=2^n$

השמה מספר?

$(x_1 \text{ OR } x_3 \text{ OR } x_8)$
 AND
 $(\bar{x}_2 \text{ OR } x_4 \text{ OR } \bar{x}_5)$
 AND
 ⋮

הערות:

- קל להכליל ל- M קלטים "טובים" $\underline{x}_{(1)}^*, \dots, \underline{x}_{(M)}^*$
- ניתן להכליל למספר בלתי ידוע של קלטים "טובים"

x	$f(x)$
000	0
001	0
...	...
x^*	1
...	...
111	0

} $N=2^n$

אלגוריתם גרובר : ניסיון ראשון

• קל ליצור סופרפוזיציה אחידה של כל הקלטים: $\frac{1}{\sqrt{N}} \sum_x |x\rangle \equiv |S\rangle$
 $\left. \begin{matrix} |0\rangle - \boxed{H} - \\ |0\rangle - \boxed{H} - \\ \vdots \\ |0\rangle - \boxed{H} - \end{matrix} \right\}$

☺ $\langle x^* | S \rangle = \frac{1}{\sqrt{N}}$: עם הקלט ה"טוב" של $\frac{1}{\sqrt{N}}$ חפיפה אחידה חפיפה של $\frac{1}{\sqrt{N}}$

אבל

☹ $|\langle x^* | S \rangle|^2 = \frac{1}{N}$ ההסתברות למדוד את הקלט ה"טוב" היא רק $\frac{1}{N}$

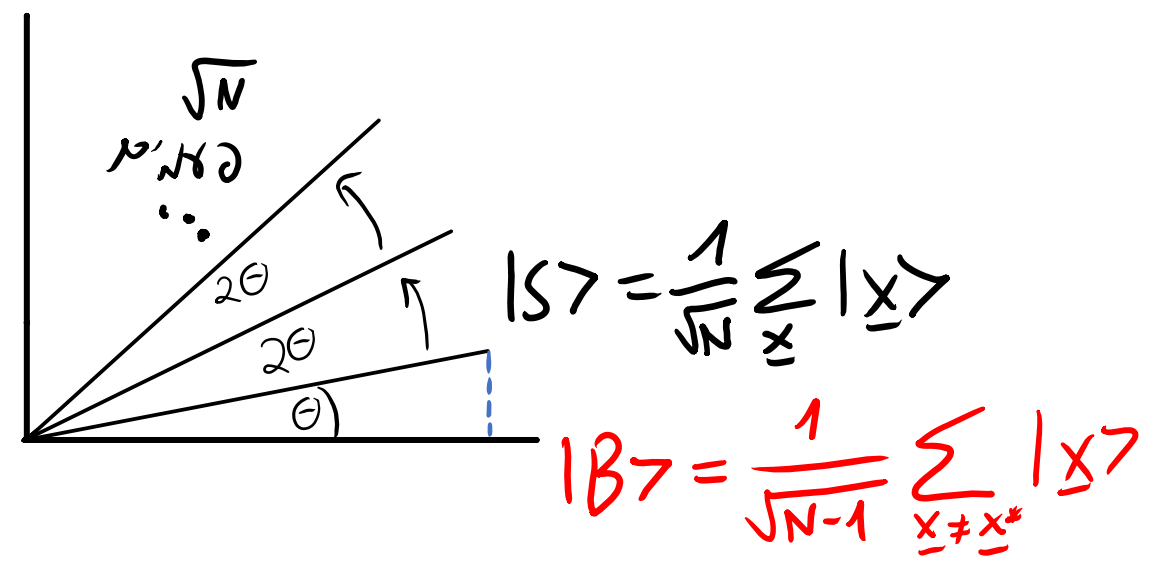
לכך/כך 'מש' ב $\frac{1}{\sqrt{N}}$ בצורה אכזבנית!

\underline{x}	$f(\underline{x})$
000	0
001	0
...	...
\underline{x}^*	1
...	...
111	0

$N=2^n$

הרעיון של גרובר: הטוב, הרע והסופרפוזיציה

$|G\rangle = |\underline{x}^*\rangle$



$|S\rangle = \frac{1}{\sqrt{N}} |G\rangle + \sqrt{\frac{N-1}{N}} |B\rangle$

$\sin\theta = \langle S | G \rangle = \frac{1}{\sqrt{N}}$

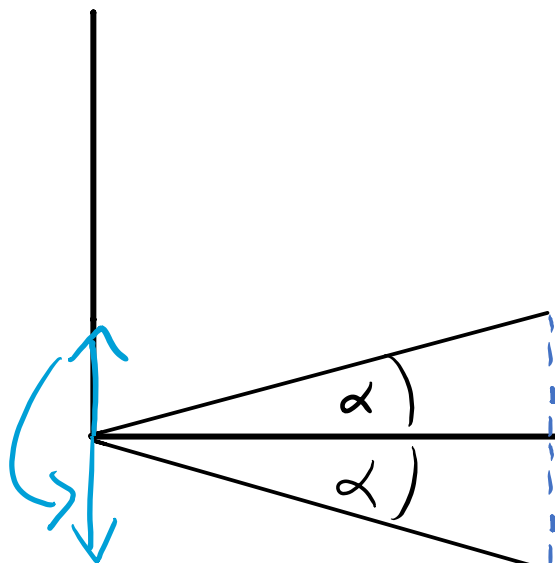
איטרציית גרובר - התמונה הגאומטרית

\underline{x}	$f(\underline{x})$
000	0
001	0
...	...
\underline{x}^*	1
...	...
111	0

מה אורקל פאזה עושה למצב $|\psi\rangle$ במישור $|B\rangle, |G\rangle$? $|\psi\rangle = \tilde{U}_f^{-1} |G\rangle$?

עיקול! ≈ 0 $|B\rangle$

$|G\rangle = |\underline{x}^*\rangle$



$$|\psi\rangle = \sin(\alpha)|G\rangle + \cos(\alpha)|B\rangle$$

$$|B\rangle = \frac{1}{\sqrt{N-1}} \sum_{\underline{x} \neq \underline{x}^*} |\underline{x}\rangle$$

$$\tilde{U}_f |\psi\rangle = -\sin(\alpha)|G\rangle + \cos(\alpha)|B\rangle$$

מלבד זה:

$$|\underline{x}\rangle = \tilde{U}_f^{-1} (-1)^{f(\underline{x})} |\underline{x}\rangle$$

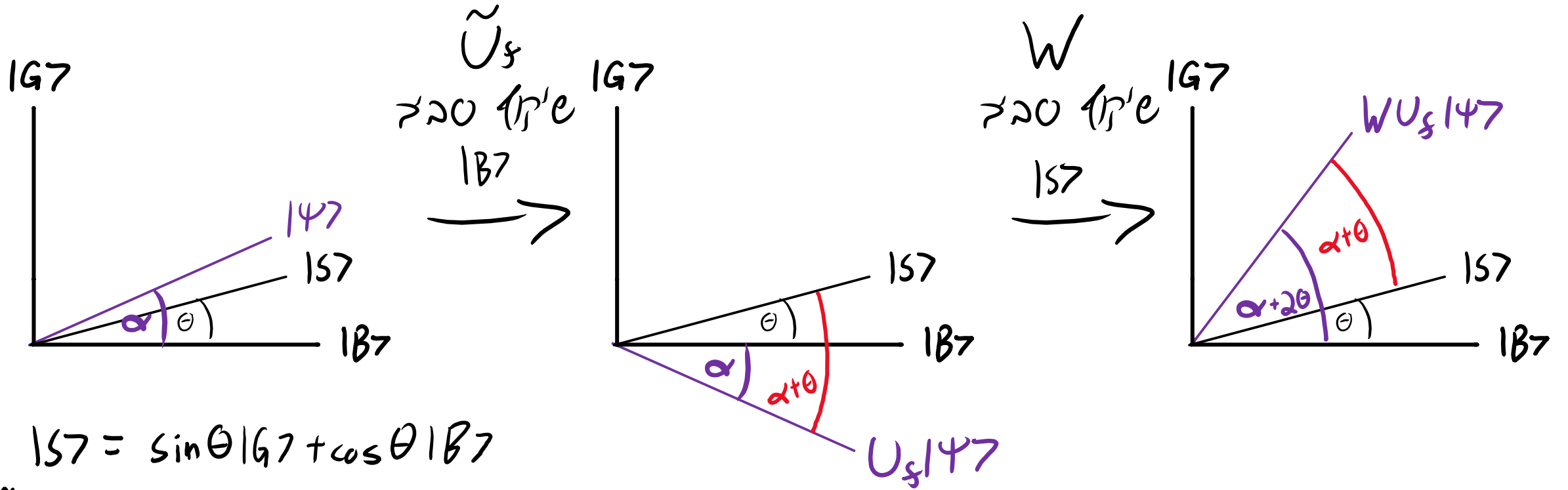


$$|B\rangle = \tilde{U}_f |B\rangle$$

$$|G\rangle = \tilde{U}_f^{-1} -|G\rangle$$

x	$f(x)$
00	0
001	0
...	...
x	1
...	...
111	0

איטרציית גרובר - התמונה הגאומטרית



$$|S\rangle = \sin\theta |G\rangle + \cos\theta |B\rangle$$

$$W U_psi |S\rangle = \sin(3\theta) |G\rangle + \cos(3\theta) |B\rangle$$

$$(W U_psi)^2 |S\rangle = \sin(5\theta) |G\rangle + \cos(5\theta) |B\rangle$$

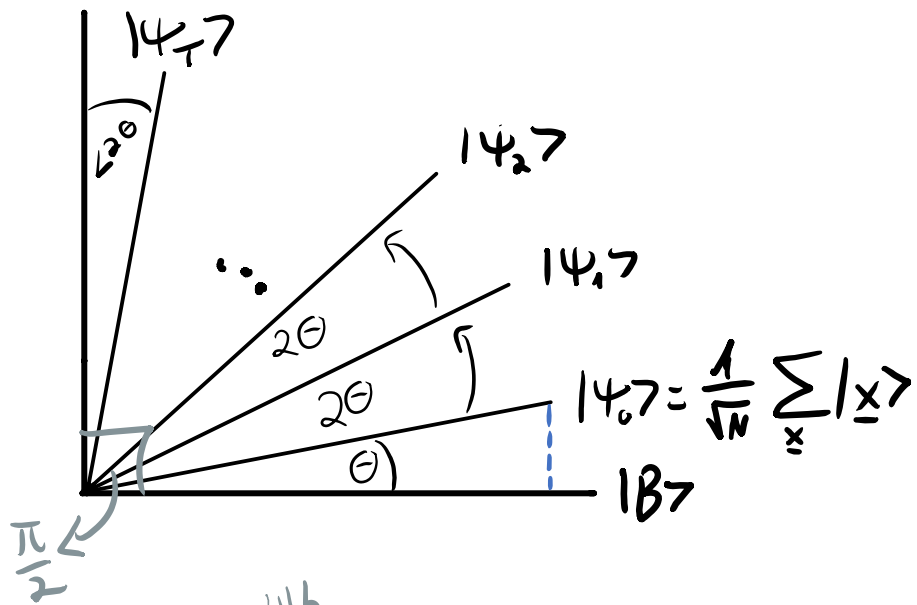
⋮

$$! |B\rangle, |G\rangle \text{ במ'שור } 2\theta \text{ בזוו' } = W \cdot U_psi$$

הצורה: קיים שיקוף W מעגל חוט יחיד (ע.ב)

המעגל של גרובר

$$|G\rangle = |x^*\rangle$$

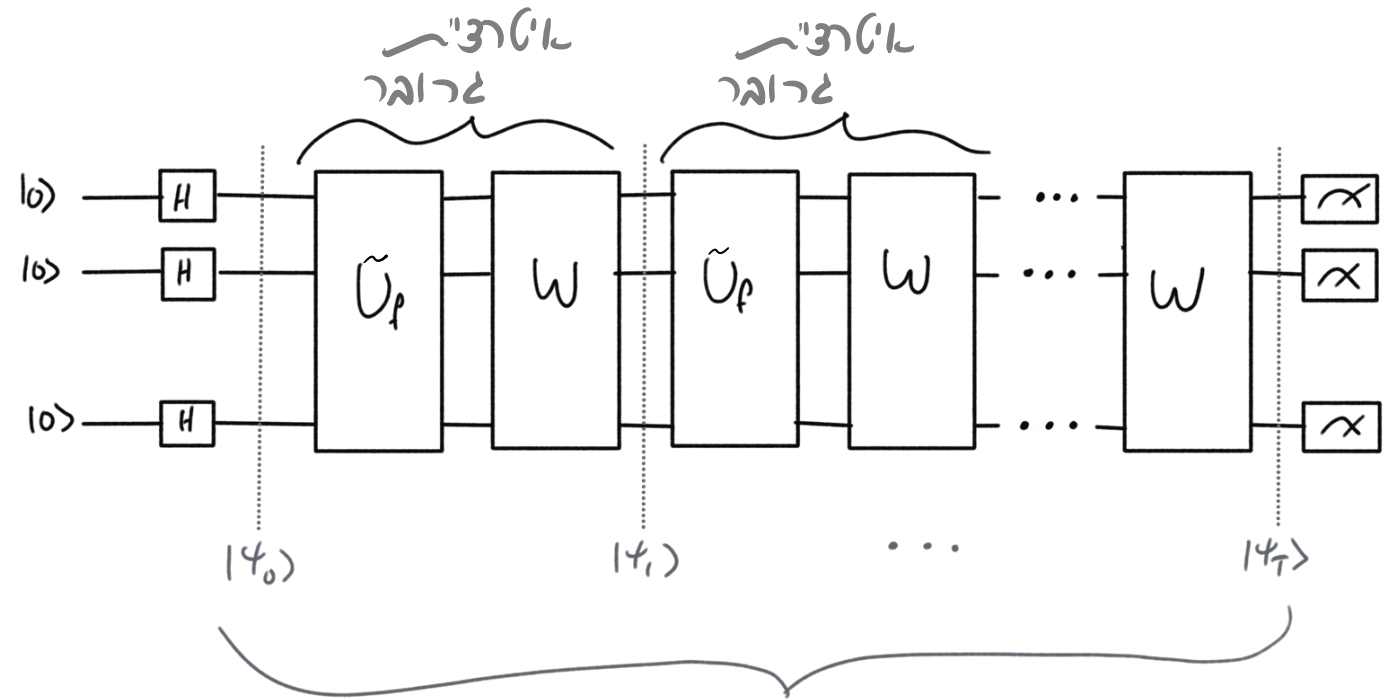


$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

כללי קטנה \rightarrow

$$\theta \approx \sin \theta = \langle G | S \rangle = \frac{1}{\sqrt{N}}$$

$$\theta \cdot (2T+1) \approx \frac{\pi}{2} \Rightarrow T \approx \frac{\pi}{4\theta} \approx \sqrt{\frac{\pi}{4} N}$$

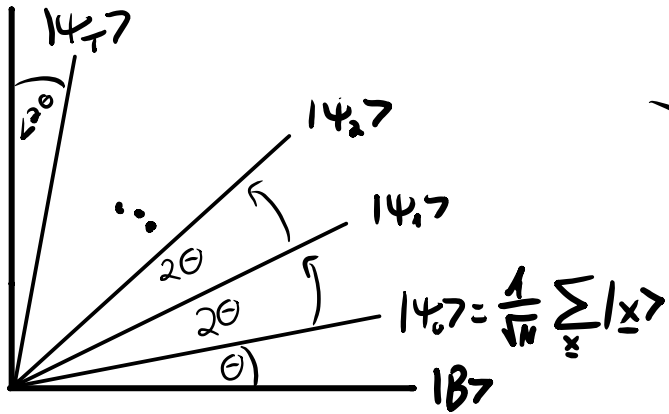


T איטרציות

כמה איטרציות T ?
 נרצה כללי קטנה $\approx \frac{\pi}{2}$

אלגוריתם גרובר - סיכום

$|x^*\rangle$



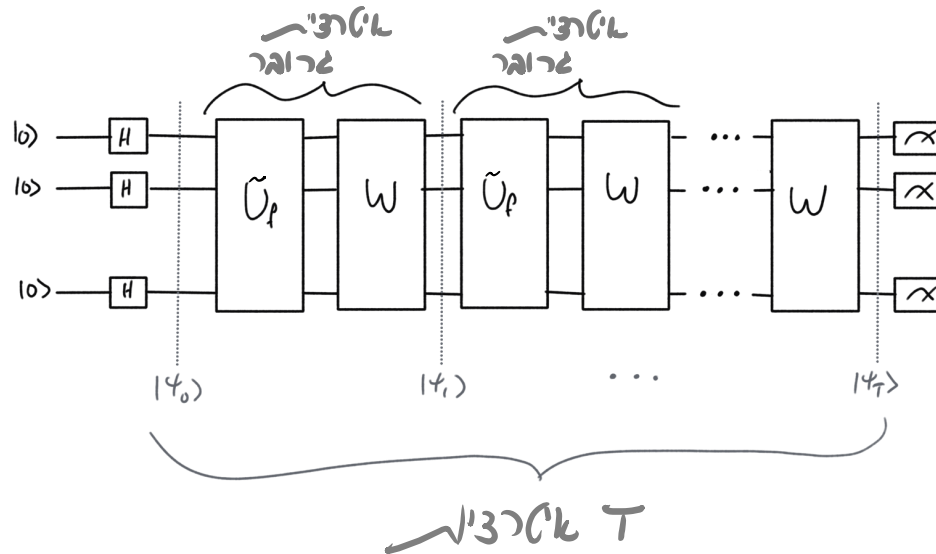
הרעיון: מסוגל ל
הסופרפולציה, הנחיצה
עיקר הטובה

x	$f(x)$
000	0
001	0
\vdots	\vdots
x^*	1
\vdots	\vdots
111	0

הבעיה: איבוס
בהערכת עמ
ממיון

מאצו המציבה: (הקל) ה"טוב"

x^* בהסתברות $< 1 - 4/N$ (ע.ב.)



(המאגל) \sqrt{N} $\sim T$
טאיטרציות סבוב