

מבוא לעיבוד אינפורמציה קוונטית 236990

אינפורמציה:

אינפורמציה עצמית: $\log_2 \frac{1}{p_i} = -\log_2 p_i$

אנטרופיה: $H = \sum_i -p_i \log_2 p_i$

מטבע הוגן $H=1$ שנים $H=2$ לא הוגן $H = h(p) = h(1-p)$
השינוי באנטרופיה אם למדנו את Y :

$$H(X|Y=y) = \sum_x -p(x|y) \log_2 p(x|y)$$

אנטרופיה מותנת: $H(X|Y) = \sum_y P(y) H(X|Y=y)$

בייס: $P(x, y) = P(x|y)P(y) = P(y|x)P(x)$
השינוי באנטרופיה מקבלת Y :

$$0 \leq I(X, Y) = I(Y, X) = H(X) - H(X|Y) \leq \log_2 \frac{abc}{|Z|}$$

$$I(x, y) \leq S(\rho) - \sum_x p_x S(\rho_x) \quad S(\delta) = -\text{tr}(\delta \log(\delta))$$

ערוצי תקשורת:

BSC - בינארי סימטרי - p שגיאה: $I = 1 - h_2(p)$ אחידה

BEC - מחיקה בינארי - p למחיקה: $I = 1 - p$ כניסה אחידה
קיבולת הערוץ: $C = \max_{P(X)} I(X, Y)$ - התפלגות הקלט

ניתן להקטין את השגיאה בערוץ אם לא עוברים את הקיבולת
כל עוד מתקיים $R \cdot \log |\Sigma| < C$ ניתן: $Rn \rightarrow n, error \rightarrow \epsilon$

אינפורמציה:

סיכוי לנכון/טעות $p_c = \langle \phi_0 | \psi_0 \rangle, p_e = \langle \phi_1 | \psi_0 \rangle$

ניתן לשכפל מצבים אורטוגונאליים ע"י C-NOT

אין אפשרות לשכפל מצבים לא אורטוגונאליים נקבל סתירה
בשימור החפיפה בין ההתחלה לסיום.

הנאמנות של מצב - $F = |\langle \psi | \psi' \rangle|^2 = \langle \psi | \rho' | \psi \rangle$

אנו לא אומרים שהמערכת קורסת לאחר מדידה אלה מקבלים
תוצאה זו ע"י trace-out של תת מערכת.

מדידה חלקית - $|\psi\rangle_{AB} = \sum_{ij} \alpha_{ij} |i\rangle_A |j\rangle_B$

בוב מודד $\rho_{AB} = \sum_j p_j |\phi_j\rangle_A |j\rangle_B, \rho_A = \sum_j p_j |\phi_j\rangle\langle\phi_j|$
התעלמות מתת המערכת הנמדדת -

$$\rho_A = \sum_j \langle j |_B \rho_{AB} |j\rangle_B = \sum_j p_j |\phi_j\rangle\langle\phi_j|$$

$$\rho_A = \begin{pmatrix} a_{00,00} + a_{01,01} & a_{00,10} + a_{01,11} \\ a_{10,00} + a_{11,01} & a_{10,10} + a_{11,11} \end{pmatrix} \rho_B = \begin{pmatrix} a_{00,00} + a_{10,10} & a_{00,01} + a_{10,11} \\ a_{01,00} + a_{11,10} & a_{01,01} + a_{11,11} \end{pmatrix}$$

במצב שהוא מכפלה טנזורית (פריק) מתקיים

$$\sum_j p_j [\rho_j(A) \otimes \rho_j(B)], \alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10} \iff \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

אי-ודאות

$$\Delta A = \langle A^2 \rangle - \langle A \rangle^2, \Delta A \Delta B \geq \frac{1}{2} |\langle \psi | AB - BA | \psi \rangle|$$

אקסיומות קוונטים:

1. תיאור ע"י ווקטור במרחב הילברט:

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle = \sum_i \alpha_i |i\rangle$$

אורתונורמאליות של מצבים עצמיים: $\langle \psi_i | \psi_j \rangle = \delta_i^j$

בסיס החישוב: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

בסיס הדמרד: $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

בסיס בל: $|\phi_{\pm}\rangle = \frac{1}{\sqrt{2}} [|00\rangle \pm |11\rangle], |\psi_{\pm}\rangle = \frac{1}{\sqrt{2}} [|01\rangle \pm |10\rangle]$

סינגלט: $\frac{1}{\sqrt{2}} [|01\rangle - |10\rangle]$, טריפלט: $\frac{1}{\sqrt{2}} [|01\rangle + |10\rangle]$

חפיפה: $\langle \phi | \psi \rangle = \left[\sum_j \beta_j^* \langle j | \right] \left[\sum_i \alpha_i |i\rangle \right] = \sum_i \beta_i^* \alpha_i$

$$\sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

מצב טהור - מטריצת הצפיפות ניתנת ללכסון למדידה והאית, $\text{tr}(\rho^2) = 1$

מצב מעורב - מספר האברים השונים מ-0 אחרי לכסון - צבר מינימלי.

טרנספורמציות הרמיטיות:

$A^\dagger = A$ ערכים עצמיים ממשיים, iA אנטי הרמיטי

אקספוננט של הרמיטי הוא אוניטארי. $U = \exp(iA)$

טרנספורמציות אוניטריות: $\psi' = U\psi, U^\dagger U = I$

ניתן להיכתב $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) = \begin{pmatrix} \cos\theta & -e^{-i\phi} \sin\theta \\ e^{i\phi} \sin\theta & \cos\theta \end{pmatrix}$

ערכים עצמיים על מעגל היחידה $e^{i\phi}$

משמר נורמה (ומכפלה פנימית) $\det(U) = 1$

שורות (ועמודות) מהווים בסיס אורתונורמאלי.

משמרות חפיפה: $\langle \phi | \psi \rangle = \langle \phi' | \psi' \rangle$

יכולות להיות פאסיביות (מעבר בסיס), אקטיביות (התפתחות).

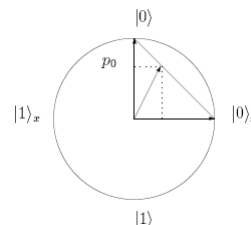
2. התפתחות בזמן: $H|\psi\rangle = i\hbar \partial_t |\psi\rangle$

ולכן לכל המערכת: $|\psi(t)\rangle = \sum_j \alpha_j e^{-iE_j t/\hbar} |\psi_{j(0)}\rangle$

3. לאחר מדידה המערכת במצב עצמי בהסתברות $p_i = |\alpha_i|^2$

4. חיבור מערכות הפועלות במרחבים שונים: $|\phi_1\rangle \otimes |\phi_2\rangle$

מצב שלא יכול להיכתב כמכפלה טנזורית - מצב שזור.



כדור פואנקרה:

מצב טהור על המעטפת - יחיד.

מעורב - אינסוף צברים.

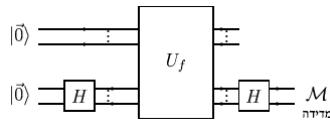
מצבים אורטוגונאליים על ציר.

$$\frac{1}{2} [1 + \mathbf{r} \cdot \hat{\sigma}] = \begin{pmatrix} \cos\frac{\theta}{2} & 0 \\ 0 & e^{i\phi} \sin\frac{\theta}{2} \end{pmatrix}$$

מטריצת הצפיפות $\rho_\psi = |\psi\rangle\langle\psi|$ - מתאים למצבים מעורבים.

ערך תצפית: $\sum_i p_i \langle \psi_i | A | \psi_i \rangle = \text{tr}(A\rho) = \langle \psi | A | \psi \rangle$

בעיית סימון - פונקציה 1 → 2, מצא את s



$$f(x) = f(y) \Leftrightarrow y = x \oplus s$$

קלאסית צריך $2^{n-1} + 1$, קוונטית $O(\log_2 n)$ - פער אקספוננט

לא פרקטי, אורקל ללא מימוש יעיל, לא מוכיח $BPP \neq BQP$.

$$|\psi\rangle = \frac{1}{2^n} \sum_{y,z \in S1} [(-1)^{z \cdot y} + (-1)^{(z \oplus s) \cdot y}] |y\rangle |f(z)\rangle$$

נוכל למדוד רק y המקיימים $s \cdot y = 0$

אלגוריתם הפיקטור של שור

טרנספורם פורייה קוונטי - QFT

מחשב קוונטי טוב בלמצוא מחזור של פונקציה $f(x) = f(x+jr)$

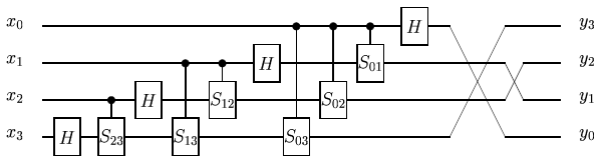
$$|x\rangle \xrightarrow{QFT} \frac{1}{(\sqrt{2})^n} \sum_y e^{i2\pi xy/2^n} |y\rangle$$

הגדרה - (הכללת הדמרד).

יעילות:

$$xy / 2^n = y_{n-1}(0.x_0) + y_{n-2}(0.x_1x_0) + \dots + y_0(0.x_{n-1}\dots x_0)$$

$$|x\rangle \rightarrow \frac{1}{(\sqrt{2})^n} [|0\rangle + e^{2\pi i(0.x_0)} |1\rangle] \otimes \dots \otimes [|0\rangle + e^{2\pi i(0.x_{n-1}\dots x_1x_0)} |1\rangle]$$



$$S_{jk} = \begin{pmatrix} 1 & \\ & \exp(i\pi/2^{k-j}) \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} [|0\rangle + e^{2\pi i(0.x_0)} |1\rangle]$$

סה"כ $\frac{1}{2}n(n+1)$ שערים.

אם נדרוש רגיסטר מספיק גדול ($2^n > N^2$) נקבל בסיכוי

$$|y \cdot 2^{-n} - d/r| \leq 2^{-n-1}$$

נמצא ע"י עיגול של $y/2^n$ את r (אם $\gcd(d,r)=1$)

$$\frac{5}{12} = \frac{1}{12/5} = \frac{1}{1 + \frac{2}{5}} = \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}$$

חישוב יעיל של $a^x \bmod N$

$$a^x \bmod N = [a^{2^{n-1}}]^{x_{n-1}} [a^{2^{n-2}}]^{x_{n-2}} \dots [a^{2^1}]^{x_1} [a^{2^0}]^{x_0} \bmod N$$

הקבועים בסוגרים יחושבו מראש $a^{2^j} = [n^{2^{j-1}}]^2 \pmod N$.

מציאת הפקטורים ע"פ המחזור $a^r \bmod N = 1$

$$a^r - 1 = (a^{r/2} + 1)(a^{r/2} - 1) = 0 = kN = k_p k_q N_p N_q$$

דרישות:

- $a^j = 0$ זר ל-N כדי שלא יתקיים
- r זוגי
- N יתחלק בין הסוגרים (סיכוי גדול)

EPR - ע"י הנחה של ריאלייות ולוקאליות מגיעים לבעיה בתורת הקוונטים (שינוי מה שמודדים). התשובה יש ריאלייות רק לאחר המדידה ואין ערך מוכן מראש.

טלפורטציה - $\Psi_{init} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_{A'} \otimes \frac{1}{\sqrt{2}} [|01\rangle - |10\rangle]_{AB}$

$$\Psi = \frac{1}{2} [|\phi_+\rangle \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} + |\phi_-\rangle \begin{pmatrix} \beta \\ \alpha \end{pmatrix} + |\psi_+\rangle \begin{pmatrix} -\alpha \\ \beta \end{pmatrix} + |\psi_-\rangle \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix}]$$

מודדים בבל וצריך עדיין להעביר 2 ביטים קלאסיים אך לסובב

ניתן לשלוח 2 ביט קלאסיים ע"י טרנספורמציה $I, \sigma_x, \sigma_y, \sigma_z$. ע"פ חסם חולבו בקיוביט ניתן לשמור בנאמנות 1 ביט.

שערים לוגיים:

σ_x - NOT

פאזה כללית - $U_\phi = \sigma_z^\theta = \begin{pmatrix} 1 & \\ & \exp(i\phi) \end{pmatrix}$

סיבוב - $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$ (det = 1)

הדמרד - $\left. \begin{matrix} |0\rangle \rightarrow |+\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow |-\rangle \rightarrow |1\rangle \end{matrix} \right\} H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\sigma_z + \sigma_x)$

ניתן לרישום: $H|x\rangle = \sum_i (-1)^{i \cdot x} |i\rangle$

מספר ביטים: $H_n |0\rangle = \sum |i\rangle, H_n = \frac{1}{(\sqrt{2})^n} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \dots \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

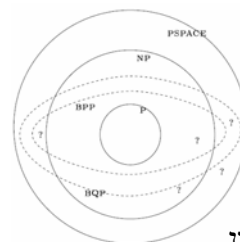
ניתן לרישום: $H_n |x\rangle = \sum_i (-1)^{x \cdot i} |i\rangle$

C-NOT $\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ (טופולי - C-C-NOT)

דויטש-Deutsch - $C - C = \begin{pmatrix} i \cos\theta & \sin\theta \\ \sin\theta & i \cos\theta \end{pmatrix}$

פרדקין C-swap - FAN-OUT

כדי להפוך אורקל פאזה לאורקל קוונטי או להפך מוסיפים H לפני ואחרי הכניסה הנוספת.



סיבוכיות:

P - חישוב בזמן פולינומיאלי.

NP - ניתן לוודא בזמן פולינומיאלי.

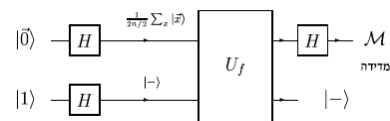
BPP - מותר מטבע וצריך 2/3 נכון.

PSPACE - מקום פולינומיאלי.

BQP - קוונטי, זמן פולינומיאלי, 2/3 נכון.

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE, \text{ השאלה } BQP \neq BPP?$$

דויטש-ג'וזה DJ - הבדלה בין פונקציה מאוזנת, אפסה:



קלאסית צריך $2^{n-1} + 1$ (או רק $O(n)$), קוונטית 1.

אנו מודדים את y ו- $f_{balanced}$ $y = 0 \rightarrow f_0, y \neq 0 \rightarrow f_{balanced}$

3. מדוד בבסיס החישוב

$$|k\rangle \equiv |\psi_r\rangle = (-H(I-2|0\rangle\langle 0|)H(I-2|k\rangle\langle k|))^T H|0\rangle$$

$$T\omega = \frac{\pi}{2} \leftarrow \omega \approx \frac{2}{\sqrt{N}} \text{ - סיבוב } Q = \begin{pmatrix} 1-\frac{2}{N} & 2\frac{\sqrt{N-1}}{N} \\ -2\frac{\sqrt{N-1}}{N} & 1-\frac{2}{N} \end{pmatrix}$$

$$P_r(T) = \frac{1}{2}(1 - \cos 2\omega T) \quad \omega = 2\sqrt{r/N} \text{ כללי } r \text{ עבור}$$

תקשורת - תיאום פגישה:

אליס ובווב מבצעים יחד גרובר

1. חזור שלוש פעמים

2. אליס מכינה n+1 ביטים במצב $H_n|0\rangle_n \otimes |0\rangle$

3. חוזרים $t \in \{0, \dots, \sqrt{N}\}$ אקראי על:

א. אליס: $|x\rangle|0\rangle \rightarrow |x\rangle|f_A(x)\rangle$

ב. בווב: $|x\rangle|a\rangle \rightarrow (-1)^{a \wedge f_B(x)} |x\rangle|a\rangle$

ג. אליס: $|x\rangle|a\rangle \rightarrow |x\rangle|a \oplus f_A(x)\rangle = |x\rangle|0\rangle$

ד. אליס: מפעילה הדמדר.

4. אליס מודדת את הרגיסטר

5. אם מדדה זמן פנוי שולחת קלאסית לבוב.

סיבוכיות תקשורת של $O(\sqrt{N} \log_2 N)$

מתמטיקה:

הזווית בין שני וקטורים כלשהם: $\cos \gamma = \cos \theta_0 \cos \theta + \sin \theta_0 \sin \theta \cos(\varphi - \varphi_0)$

הזווית מעולם המרוכבות: $|r_1 e^{i\alpha} - r_2 e^{i\beta}|^2 = r_1^2 + r_2^2 + 2r_1 r_2 \cos(\alpha - \beta)$

$$\sin(ix) = i \sinh(x) \quad \cos(ix) = \cosh(x)$$

Trigonometric Identities:

- $\sin(-\alpha) = -\sin \alpha$
- $\cos(-\alpha) = \cos \alpha$
- $\tan(-\alpha) = -\tan \alpha$
- $\sin(90 - \alpha) = \cos \alpha$
- $\cos(90 - \alpha) = \sin \alpha$
- $\tan(90 - \alpha) = \cot \alpha$
- $\cot(90 - \alpha) = \tan \alpha$
- $\sin(180 - \alpha) = \sin \alpha$
- $\cos(180 - \alpha) = -\cos \alpha$
- $\tan(180 - \alpha) = -\tan \alpha$
- $\tan \alpha = \sin \alpha / \cos \alpha$
- $\tan \alpha \cdot \cot \alpha = 1$
- $\sin^2 \alpha + \cos^2 \alpha = 1$
- $1 + \tan^2 \alpha = 1 / \cos^2 \alpha$
- $1 + \cot^2 \alpha = 1 / \sin^2 \alpha$
- $\sin(2\alpha) = 2 \sin \alpha \cos \alpha$
- $\cos(2\alpha) = \cos^2 \alpha - \sin^2 \alpha$
- $\cos(2\alpha) = 2 \cos^2 \alpha - 1$
- $\cos(2\alpha) = 1 - 2 \sin^2 \alpha$

$$\left| \int_a^b e^{ix} dx \right|^2 = |e^{ib} - e^{ia}|^2 = 4 \sin^2 \left(\frac{\alpha - \beta}{2} \right)$$

- $\tan(2\alpha) = 2 \tan \alpha / (1 - \tan^2 \alpha)$
- $\sin(3\alpha) = 3 \sin \alpha - 4 \sin^3 \alpha$
- $\cos(3\alpha) = 4 \cos^3 \alpha - 3 \cos \alpha$
- $\sin \alpha + \sin \beta = 2 \sin(a/2 + \beta/2) \cos(a/2 - \beta/2)$
- $\sin \alpha - \sin \beta = 2 \sin(a/2 - \beta/2) \cos(a/2 + \beta/2)$
- $\cos \alpha + \cos \beta = 2 \cos(a/2 + \beta/2) \cos(a/2 - \beta/2)$
- $\cos \alpha - \cos \beta = -2 \sin(a/2 + \beta/2) \sin(a/2 - \beta/2)$
- $\sin \alpha \cos \beta = 1/2 (\sin(a + \beta) + \sin(a - \beta))$
- $\sin \alpha \sin \beta = 1/2 (\cos(a - \beta) - \cos(a + \beta))$
- $\cos \alpha \cos \beta = 1/2 (\cos(a + \beta) + \cos(a - \beta))$
- $\sin(\alpha + \beta) = \sin \alpha \cos \beta + \cos \alpha \sin \beta$
- $\sin(\alpha - \beta) = \sin \alpha \cos \beta - \cos \alpha \sin \beta$
- $\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$
- $\cos(\alpha - \beta) = \cos \alpha \cos \beta + \sin \alpha \sin \beta$
- $\tan(\alpha + \beta) = (\tan \alpha + \tan \beta) / (1 - \tan \alpha \tan \beta)$
- $\tan(\alpha - \beta) = (\tan \alpha - \tan \beta) / (1 + \tan \alpha \tan \beta)$
- $\tan(\alpha + \beta) - \tan \alpha - \tan \beta = \tan(\alpha + \beta) \tan \alpha \tan \beta$
- $\arcsin \alpha + \arccos \alpha = \pi / 2$

$$\sum_{n=A}^B a_n = \frac{(B-A+1)(a_A + a_B)}{2}$$

$$\sum_{n=A}^B q^n = q^A \left(\frac{1 - q^{B-A+1}}{1 - q} \right)$$

$$\sum_{l=0}^L (-1)^l (2l+1) = (-1)^L (L+1)$$

סכומי טורים:

הבחנה בין שני מצבים לא אורטוגונאליים

$$|\psi_{0,1}\rangle = \begin{pmatrix} \cos \theta \\ \pm \sin \theta \end{pmatrix} \text{ - אליס שולחת}$$

$$|\overline{\psi}_{0,1}\rangle = \begin{pmatrix} \cos \theta \\ \mp \sin \theta \end{pmatrix} \text{ - בווב מגדיר}$$

בוחר באקראי בסיס - $\{|\psi_0\rangle, |\overline{\psi}_0\rangle\}, \{|\psi_1\rangle, |\overline{\psi}_1\rangle\}$

מדידה של נגדי מתפרשת כנכון ושל מקורי כלא ידוע.

A \ B	0	?	1	
0	$\frac{1}{2} \sin^2 2\theta$	$\frac{1}{2} \cos^2 2\theta$	0	0.5
1	0	0.5	0	0.5
	$\frac{1}{2} \sin^2 2\theta$	$\frac{1}{2} (1 + \cos^2 2\theta)$	0	

דרך שניה: בווב מוסיף עוד Qbit במצב $|0\rangle$

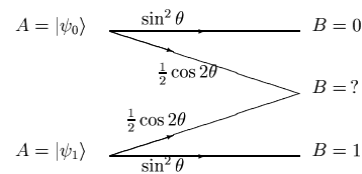
$$|00\rangle \rightarrow \frac{\sin \theta}{\cos \theta} |00\rangle + \frac{\sqrt{|\cos 2\theta|}}{\cos \theta} |11\rangle$$

$$|01\rangle \rightarrow |01\rangle \quad |10\rangle \rightarrow |10\rangle \quad \text{מבצע טרנספורמציה} \quad \left(\begin{matrix} 1 & \cos \theta \\ 0 & \pm \sin \theta \end{matrix} \right)_a$$

$$|11\rangle \rightarrow \frac{\sqrt{|\cos 2\theta|}}{\cos \theta} |00\rangle - \frac{\sin \theta}{\cos \theta} |11\rangle$$

מקבל: $\begin{pmatrix} \sin \theta \\ \pm \sin \theta \\ 0 \\ \sqrt{|\cos 2\theta|} \end{pmatrix}$ מדידה של 0,1, $2 \sin^2 \theta - ?$, $\cos 2\theta - ?$

לבווב יש $I = 2 \sin^2 \theta$ אינפורמציה זמינה.



אי שוויון בל

$$E(\alpha\beta) - E(\alpha'\beta) + E(\alpha'\beta') + E(\alpha\beta') \leq 2$$

ע"י סיבוב של הסינגלט ומדידה נפרדת של a, a' כאשר ניתן

למדוד רק אחד מהם כל פעם ($\alpha = (-1)^{\langle \psi \rangle}$, $\alpha' = (-1)^{\langle H \psi \rangle}$)

מקבלים שתירה חוק הסטטיסטי.

כל טרנספורמציה אוניטרית יכולה להירשם כ-2 מעניינת.

$$U_1 = \frac{1}{C} \begin{pmatrix} a^* & b^* \\ b & -a \\ & \sqrt{|a|^2 + |b|^2} \end{pmatrix} \quad U = U_1 U_2 U_3 = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

$$U_2 = \frac{1}{C} \begin{pmatrix} a^* & c^* \\ \sqrt{|a|^2 + |c|^2} & -a' \end{pmatrix} \quad U_3 = \frac{1}{C} \begin{pmatrix} 1 & \\ e^* & f^* \\ h^* & j^* \end{pmatrix}$$

אלגוריתם החיפוש של גרובר:

קיימת פונקציה עבורה $f_x = \begin{cases} 1 & x \in \{X\} \\ 0 & \text{else} \end{cases}$, $f|x\rangle|0\rangle = |x\rangle, |f(x)\rangle$

1. הפעל הדמדר על 0 באורך n ביטים.

2. חזור $T = \frac{\pi}{4} \sqrt{N}$ פעמים (שונה עבור $r > 1$).

א. הפעל U_f

ב. הפעל הדמדר H_n

ג. הפוך פאזה של מצב $|0\rangle$

ד. הפעל הדמדר H_n

ה. הפוך פאזה גלובלית (רק מפשט הוכחה)