תורת האינפורמציה הקוונטית 116031

24 ביוני 2010

תוכן עניינים

qubit 1

מערכת בת שתי רמות אנרגיה - E_1, E_2. ניתן להתבונן על מערכת בה יש שתי רמות אנרגיה קרובות יחסית ושאר רמות האנרגיה רחוקות, לחילופין ניתן להתייחס לחלקיק עם ספין $\frac{1}{2}$, פולריזציה של פוטון וכו'...
נשתמש בבסיס שיתואר ע"י $|0\rangle, |1\rangle$ ומצב המערכת מתואר ע"י וקטור במרחב הילברט -

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

כאשר α, β מספרים מרוכבים.
מצבים קוונטיים, כידוע, הם "שקרנים". ההסתברות שמערכת במצב $|\psi\rangle$ תענה "כן" על השאלה "האם אתה במצב $|0\rangle$?" היא $|\alpha|^2$, וההסתברות לתשובה "כן" על השאלה ההפוכה היא $|\beta|^2$. מכאן מתקיים -

$$|\alpha|^2 + |\beta|^2 = 1$$

שאלה - כמה אינפורמציה "מסתתרת" בקיוביט?

נשים לב שמבחינה גאומטרית α, β, תחת האילוץ שציינו, מתארים כדור בארבעה מימדים - S^3.
אבל - $|\psi\rangle \cong e^{i\gamma} |\psi\rangle$. כלומר - פאזה שכופלת את כל המצב הקוונטי לא באמת משפיעה עליו, ולמעשה המצב נמצא במרחב -

$$\frac{S^3}{S} = S^2$$

נתאר את $|\psi\rangle$ באופן כללי בצורה -

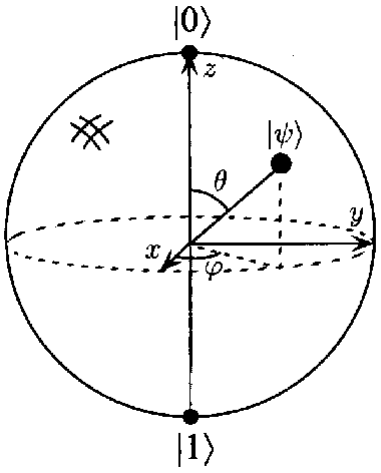
$$|\psi\rangle = e^{i\gamma} \left(cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} sin\left(\frac{\theta}{2}\right) |1\rangle \right)$$

וכיוון ש-γ לא מעניין אותנו נתאר את המצב ע"י שתי זויות -

- $0 \leq \theta < \pi$
- $0 \leq \varphi < 2\pi$

זויות אלו מתארות כדור, שנקרא הכדור של Bloch.

2 כדור Bloch



איור 1: הכדור של Bloch

נחזור לשאלה - כמה אינפורמציה נמצאת במצב קוונטי נתון $|\psi\rangle$?

- ע"מ לתאר את $|\psi\rangle$ יש צורך לספק שני מספרים ממשיים θ, φ - בהם למעשה ניתן לקודד אינסוף אינפורמציה.
- מצד שני - ה"תשובות" של הביט הקוונטי הן "כן" או "לא" - $|0\rangle$ או $|1\rangle$, לכן הוא למעשה לא טוב יותר מביט קלאסי.

אם נשאל את השאלה - "האם $|\psi\rangle$ זהה ל-$|\varphi\rangle$?" כאשר קיימת זווית β בין הייצוג של שני הווקטורים על כדור בלוך, נקבל את התשובה "כן" בהסתברות - $|\langle\varphi\,|\,\psi\rangle|^2 = \cos^2\left(\frac{\beta}{2}\right)$. המצבים היחידים בהם מובצט לנו שהקיוביט לא "ישקר" הם כאשר $\beta = 0, \pi$.

3 2 קיוביטים

אינטואיטיבית - אם קיוביט אחד מתואר ע"י כדור, שני קיוביטים יתוארו ע"י שני כדורים. אבל, זה לא המצב!
ניקח שני קיוביטים -

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle_1 + \beta\,|1\rangle_1 \\ |\varphi\rangle &= \gamma\,|0\rangle_2 + \delta\,|1\rangle_2 \end{aligned}$$

נתאר את המצב של שני הקיוביטים -

$$\begin{aligned} |\psi\rangle \otimes |\varphi\rangle &= (\alpha\,|0\rangle_1 + \beta\,|1\rangle_1) \otimes (\gamma\,|0\rangle_2 + \delta\,|1\rangle_2) = \\ &= \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle \end{aligned}$$

מצב כזה נקרא "מצב מכפלה". אבל במכניקה קוונטית יש מצבים שאינם מצבי מכפלה, לדוגמא -

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

מצב זה נקרא מצב Bell.

אם כך - כמה מימדים צריך ע"מ לתאר 2 קיוביטים?

מצב כללי מתואר ע"י -

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

ומדרישות של הסתברות -

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

כלומר - כדור ב־8 מימדים, כלומר 7 דרגות חופש. אנחנו כבר יודעים שאפשר "לזרוק" פאזה שמכפילה את כל הוקטור, ולכן בסה"כ יש לנו 6 מימדים. כשהצגנו את שני הקיוביטים בעזרת 2 מימדים השתמשנו רק ב־4 מימדים, ולכן אין פלא שלא יכולנו לייצג כך את כל המצבים האפשריים.

4 n קיוביטים

מצב כללי של n קיוביטים מתואר ע"י -

$$|\psi\rangle = \sum_{\substack{a_i \in \{0,1\} \\ 1 \le i \le n}} \alpha_{a_1 a_2 \ldots a_n} |a_1 a_2 \ldots a_n\rangle$$

כלומר - $2 \cdot 2^n - 2$ מימדים, המספר גדל אקספוננציאלית ב־n.

5 שערים קוונטיים

שער של qubit יחיד -

- במקרה הקלאסי יש שתי אפשרויות -
  - שער שלא עושה כלום
  - שער NOT, הופך 1 ל־0 ו־0 ל־1

במרקה הקוונטי יש הרבה יותר אפשרויות, חוקי המשחק הן שהשער U צריך להיות טרנספורמציה אוניטרית, להלן מספר דוגמאות -

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

כלומר -

$$\begin{aligned} X|1\rangle &= |0\rangle \\ X|0\rangle &= |1\rangle \end{aligned}$$

זה הוא המקביל לשער NOT, והוא מבצע סיבוב סביב ציר - $(|0\rangle + |1\rangle)$. נשים לב כי - $X^2 = I$, כלומר $X = X^{-1}$. ומתקיים כמובן - $X^\dagger = X$.

$$e^{i\theta X} = \sum_{n=0}^{\infty} \frac{(i\theta X)^n}{n!}$$

נשים לב כי -

$$\frac{(i\theta X)^n}{n!} = \begin{cases} -\frac{(i\theta)^n}{n!} & n \equiv 0 \ mod 2 \\ -X\frac{(i\theta)^2}{n!} & n \equiv 1 \ mod 2 \end{cases}$$

אופרטורים אחרים יהיו -

$$\begin{aligned} Y &= \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned}$$

ומתקיים -

$$X^2 = Y^2 = Z^2 = I$$

תרגיל -

$$XZ + ZX = 0$$

שער חשוב נוסף הוא שער הדמר -

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (X + Z)$$

ומתקיים -

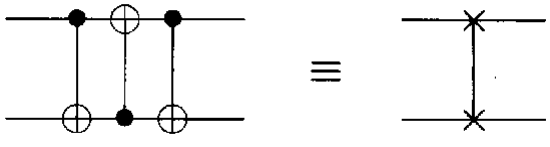
$$\begin{aligned} H^2 &= \frac{1}{2}(X+Z)^2 = \\ &= \frac{1}{2}\left(X^2 + XZ + ZX + Z^2\right) = \frac{2}{2} I = I \end{aligned}$$

6 שערים של שני קיוביטים

שערים על שני קיוביטים הם מטריצות אוניטריות, למשל $CNOT$ -

$$U_{CN} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$

שער $SWAP$ - שער שמחליף בין הערכים של שני הקיוביטים



איור 2: שער $SWAP$

ננתח מה קורה -

$$|a,b\rangle \to |a,a\oplus b\rangle \to |a\oplus a\oplus b, a\oplus b\rangle = |b,a\oplus b\rangle \to |b,a\oplus b\oplus b\rangle = |b,a\rangle$$

זה ניתוח שמתאים לעובדה כי $a,b\in\{0,1\}$, האם הוא תקף גם במקרה הכללי?

$$\begin{aligned} |\psi\rangle\otimes|b\rangle &= (\alpha|0\rangle+\beta|1\rangle)\otimes|b\rangle \to \alpha|b,0\rangle+\beta|b,1\rangle = \\ &= |b\rangle\otimes\alpha|0\rangle+|b\rangle\otimes\beta|1\rangle = |b\rangle\otimes|\psi\rangle \end{aligned}$$

7 אין שכפול No cloning

מה המשמעות של שכפול? נניח שיש לנו מכונה שיכולה לשכפל מצב $|\psi\rangle$ -

$$U|\psi,0,0\rangle \to |\psi,\psi,a\rangle$$

נניח שהיא יכולה לשכפל גם מצב אחר -

$$U|\varphi,0,0\rangle \to |\varphi,\varphi,b\rangle$$

כיוון ש-U אוניטרית ניתן לקחת -

$$(U|\varphi,0,0\rangle)^\dagger = \langle\varphi,\varphi,b|$$

נכפול את התוצאה עם התוצאה של ההפעלה של U על המצב הראשון -

$$(U|\varphi,0,0\rangle)^\dagger (U|\psi,0,0\rangle) = \langle\varphi,\varphi,b\,|\,\psi,\psi,a\rangle$$

ומצד שני -

$$\langle\varphi,0,0|\,U^\dagger U\,|\psi,0,0\rangle = \langle\varphi,0,0\,|\,\psi,0,0\rangle$$

כיוון ששתי המשוואות מתארות את אותה התוצאה נקבל -

$$\langle\varphi\,|\,\psi\rangle = \langle\varphi\,|\,\psi\rangle^2\langle a\,|\,b\rangle$$

זה יכול להתקיים רק אם $\langle\varphi\,|\,\psi\rangle = 0$ או $\langle\varphi\,|\,\psi\rangle = 1$ (ואז גם $\langle a\,|\,b\rangle = 1$), כלומר - מכונת שכפול יכולה לעבוד רק עבור מצבים מאונכים ולא ניתן לבנות מכונה שתשכפל כל מצב קוונטי כללי.

8 שער הדמר ואינטרפולציה[1]

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \\ H|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ H|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{aligned}$$

[1] הרצאה שנייה

שער של קיוביט יחיד מהווה סוג של אינטרפרנציה (תמונת התאבכות). אפשר להתבונן על שער הדמר כעל מראה חצי חדירה הניצבת ב־$45°$ ל־$|0\rangle$ו־$|1\rangle$, כך שכאשר מאירים עם פוטון על המראה הוא יוחזר ב־50% מהמקרים ויעבור בשאר המקרים. ניתן לתת פירוש לשני הכיוונים ולקבל ־

$$|0\rangle \to |0\rangle + 1 = H|0\rangle$$

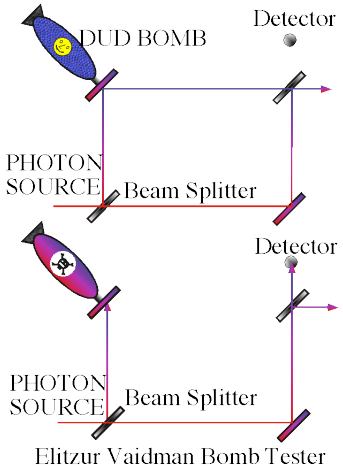
במקרה שנכניס $|1\rangle$ גם כן נקבל מחצית מהפוטונים בכיוון אחד ומחיצת באחר, אבל במקרה זה ־

$$|1\rangle \to |0\rangle - |1\rangle = H|1\rangle$$

מדוע –? כי אופרטור קוונטי הוא אוניטרי, כיוון ש־$|0\rangle, |1\rangle$ ניצבים ־ גם התוצאות שלהם אחרי הפעלת האופרטור ישארו ניצבות. ניתן כמובן להוסיף פאזה כללית, אבל כבר ראינו שזה לא משנה...

9 הפצצה של אליצור־וייזמן

האם ניתן "לבדוק" קיוביט מבלי להרוס אותו?



איור 3:

נתבונן על מערכת לבדיקת פצצות כמתואר בתרשים, המטרה היא לבדוק האם פצצה מסויימת תקינה או תקולה. עבור פצצה "מתה" נקבל "קליק" רק בגלאי אחד. עבור פצצה "חיה" ־ המערכת תתפוצץ ־ אך היא גם בודקת באיזה מסלול הפוטון הלך. נתבונן שוב על התוצאות האפשריות ־

- חלק מהפצצות יתפוצצו
- עבור חלק מהפצצות נקבל קריאה רק בגלאי ה"ימני" ־ עבור קריאה כזו אנחנו לא יודעים האם הפצצה "חיה" או "מתה"
- עבור חלק אחר ־ נקבל קריאה בגלאי ה"עליון" ־ קריאה כזו משמעותה שהפצצה חיה, והפוטון עבר מ"למטה".

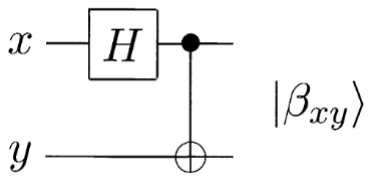
10 מכונה ליצירת מצבי Bell

ראינו שער CNOT, נכיר כעת שער שממית את הבסיס החישובי לבסיס Bell

בבסיס החישובי -

$$\begin{aligned}
|0\rangle \otimes |0\rangle &= |00\rangle = |0\rangle \\
|0\rangle \otimes |1\rangle &= |01\rangle = |1\rangle \\
|1\rangle \otimes |0\rangle &= |10\rangle = |2\rangle \\
|1\rangle \otimes |1\rangle &= |11\rangle = |3\rangle
\end{aligned}$$

נכניס את המצבים $|0\rangle \dots |3\rangle$ למעגל הבא -



איור 4: מעגל קוונטי שיוצר את מצבי Bell

מעגל כזה מייצר, למשל -

$$\begin{aligned}
|00\rangle &\rightarrow (|0\rangle + |1\rangle) \otimes |0\rangle \rightarrow \\
&\rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\beta_0\rangle = |\beta_{00}\rangle \\
|01\rangle &\rightarrow (|0\rangle + |1\rangle) \otimes |1\rangle \rightarrow \\
&\frac{|01\rangle + |10\rangle}{\sqrt{2}} = |\beta_1\rangle = |\beta_{01}\rangle
\end{aligned}$$

ונסמן -

$$\begin{aligned}
|00\rangle &\rightarrow |\beta_{00}\rangle \\
|01\rangle &\rightarrow |\beta_{01}\rangle \\
|10\rangle &\rightarrow |\beta_{10}\rangle \\
|11\rangle &\rightarrow |\beta_{11}\rangle
\end{aligned}$$

וכיוון שהמעגל בנוי משערים אוניטריים הוא אוניטרי בעצמו - המצבים שהכנסנו מאונכים - לכן גם מצבי בל מאונכים.

11 טלפורטציה קוונטית

בוב ואליס רוצים לדבר בינהם.
בוב מתחיל מ־$|0\rangle_A \otimes |0\rangle_B$ ויכול להפעיל על הביט שלו (B) את X או Z בלבד, כלומר הוא יכול להעביר את המצב ל־

$$X_B |0\rangle_A \otimes |0\rangle_B \rightarrow |0\rangle_A \otimes |1\rangle_B$$

כלומר בוב יכול להתעסק רק בחצי מהעולם.
לעומת זאת, אם אליס ובוב מתחילים ממצב בל -

$$|\beta_0\rangle = |00\rangle + |11\rangle$$

נקבל שעל ידי שינוי של הביט שלו בלבד -

$$X_B\left(|01\rangle + |10\rangle\right) = |\beta_1\rangle$$

אם הוא מפעיל את Z_B על $|\beta_0\rangle$ -

$$Z_B\,|\beta_0\rangle = |00\rangle - |11\rangle = |\beta_2\rangle$$

מה יקרה אם נפעיל גם את X_B וגם Z_B ?

$$X_B Z_B\,|\beta_0\rangle = |\beta_3\rangle$$

אם בוב נותן לאליס גישה למצב שלו לאחר הפעלת האופרטור - היא מקבלת ע"י העברת קיוביט בודד - מידע בהיקף של שני ביטים.

כעת אליס צריכה דרך לדעת איזה מצב מבין ארבעת מצבי בל היא קיבלה? אנחנו יודעים לייצר מכשיר שמפריד בין שני מצבים (ניסוי שטרן־גרלך), אנחנו זקוקים למכשיר דומה שיפריד בין ארבעת המצבים.

במכניקות קוונים ניתן למדוד observables, ע"י אופרטורים הרמיטיים, מי יהיה האופרטור שידע למדוד את ארבעת מצבי בל?

$$B = 0\,|\beta_0\rangle\langle\beta_0| + 1\,|\beta_1\rangle\langle\beta_1| + 2\,|\beta_2\rangle\langle\beta_2| + 3\,|\beta_3\rangle\langle\beta_3|$$

זה הוא אופרטור תיאורטי, שאין לנו מימוש שלו כיום, והוא ממש -

$$B\,|\beta_j\rangle = j\,|\beta_j\rangle$$

11.1 הצגת מצבי בל בבסיס החישובי

ניתן לייצג את מצבי בל באמצעות וקטור ממימד 4, כאשר -

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

המקדמים של -

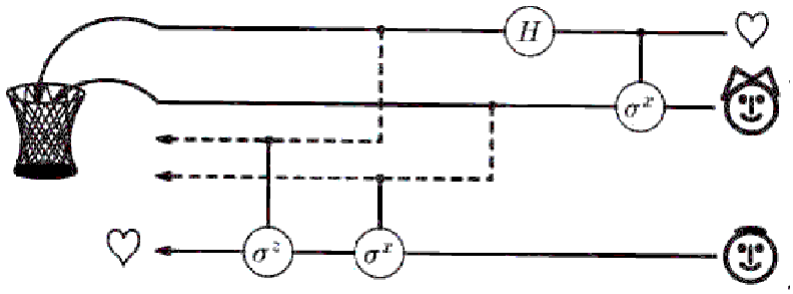
$$\begin{matrix} |0\rangle \\ |1\rangle \\ |2\rangle \\ |3\rangle \end{matrix}$$

בהתאמה. לדוגמא -

$$|\beta_{0/2}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix}$$

11.2 טלפורטציה

לאליס יש שני קיוביטים, ולבוב יש קיוביט יחיד. בסך הכל - 3 קיוביטים.



איור 5:

אחד מהם (העליון) במצב $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ לא ידוע - והיא רוצה להעביר אותו לבוב, שני הקיוביטים האחרים יוצרים מצב שזור $|\beta_0\rangle$ בסך הכל -

$$|\psi\rangle \otimes |\beta_{00}\rangle = |\psi\rangle_A \otimes (|0\rangle_A \otimes |0_B\rangle + |1\rangle_A \otimes |1\rangle_B)$$

קיוביטים אצל אליס מסומנים ב-A ואצל בוב ב-B.

כעת נכפול את המצב ב-1, כלומר ב- $1 = \sum_{j=1}^{3} |\beta_j\rangle_A \langle\beta_j|_A$ -

$$\left(\sum_{j=1}^{3} |\beta_j\rangle_A \langle\beta_j|_A\right) |\psi\rangle_A \otimes (|0\rangle_A \otimes |0_B\rangle + |1\rangle_A \otimes |1\rangle_B) = \sum_{j=1}^{3} |\beta_j\rangle_A \left(\langle\beta_j|_A |\psi_A 0_A\rangle |0\rangle_B + \langle\beta_j|_A |\psi_A 1_A\rangle |1\rangle_B\right)$$

כעת אליס מודדת את שני הקיוביטים שלה בבסיס בל - יש ארבע אפשרויות -

$$\begin{aligned}
|\beta_0\rangle &\rightarrow (\langle\beta_0|_A |\psi_A 0_A\rangle |0\rangle_B + \langle\beta_0|_A |\psi_A 1_A\rangle |1\rangle_B) = \\
&\left(\left(\underbrace{\langle 00| |\psi_A 0_A\rangle}_{\alpha} + \underbrace{\langle 11| |\psi_A 0_A\rangle}_{zero}\right) |0\rangle_B + \left(\underbrace{\langle 00| |\psi_A 1_A\rangle}_{zero} + \underbrace{\langle 11| |\psi_A 1_A\rangle}_{\beta}\right) |1\rangle_B\right) = \\
&\alpha |0\rangle_B + \beta |1\rangle_B = |\psi\rangle \\
|\beta_1\rangle &\rightarrow (\langle\beta_1|_A |\psi_A 0_A\rangle |0\rangle_B + \langle\beta_1|_A |\psi_A 1_A\rangle |1\rangle_B) = \\
&\left(\left(\underbrace{\langle 01| |\psi_A 0_A\rangle}_{zero} + \underbrace{\langle 10| |\psi_A 0_A\rangle}_{\beta}\right) |0\rangle_B + \left(\underbrace{\langle 01| |\psi_A 1_A\rangle}_{\alpha} + \underbrace{\langle 11| |\psi_A 1_A\rangle}_{zero}\right) |1\rangle_B\right) = \\
&\beta |0\rangle_B + \alpha |1\rangle_B = X_B |\psi\rangle \\
|\beta_2\rangle &\rightarrow Z_B |\psi\rangle \\
|\beta_3\rangle &\rightarrow X_B Z_B |\psi\rangle
\end{aligned}$$

12 מצבי מכפלה ומצבי $Bell$[2]

אנו דנים בשני קיוביטים. מצב מכפלה

$$\begin{array}{rcl} |\varphi\rangle \otimes |\psi\rangle & & \\ |\varphi\rangle & = & \alpha_0 |0\rangle + \alpha_1 |1\rangle \\ |\psi\rangle & = & \beta_0 |0\rangle + \beta_1 |1\rangle \end{array}$$

נשתמש בנוטציה -

$$\begin{array}{rcl} a, b, c, d & \in & \{0, 1\} \\ \mu, \nu, \alpha, \beta & \in & \{0, 1, 2, 3\} \end{array}$$

נשתמש גם בהסכם הסכימה של איינשטיין -

$$|\varphi\rangle = \alpha_a |a\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

טענה 12.1 $\sqrt{2} |\beta_0\rangle = |00\rangle + |11\rangle$ אינו מצב מכפלה **הוכחה:** נניח כי הוא כן מצב מכפלה -

$$\begin{array}{rcl} \sqrt{2} |\beta_0\rangle & = & |00\rangle + |11\rangle \\ & = & \alpha_a |a\rangle \beta_b |b\rangle \\ & = & \alpha_a \beta_b |ab\rangle \end{array}$$

נשים לב כי -

$$\begin{array}{rcl} \alpha_0 \beta_1 & = & 0 \\ \alpha_0 \beta_0 & = & 1 \\ \alpha_1 \beta_1 & = & 1 \end{array}$$

וזה לא יכול להתקיים (כי α_0או β_1 חייבים להיות אפס). ■

12.1 טענות פיזיקליות פשוטות

פעולה נקראת לוקאלית, אם כאשר מפעילים - $A \otimes B$ על $|\varphi\rangle \otimes |\psi\rangle$ מתקבל -

$$(A |\varphi\rangle) \otimes (B |\psi\rangle)$$

- אם מתחילים ממצב מכפלה, ומבצעים פעולה לוקאלית, נשארים במצב מכפלה.

איך יוצרים מצב שזור? ראינו למשל בהרצאה הקודמת שכאשר מפעילים את המעגל שיוצר את מצבי בל (איור 4) מקבלים -

$$\begin{array}{rcl} CNOT & = & |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes X \\ & \Downarrow & \\ (|0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes X) & & (H \otimes I) \end{array}$$

השורה האחרונה היא מכפלה של אופרטורים, מפעילים את השמאלי ואז את הימני, זו אינה מכפלה טנזורית! פועלים רק על שני קיוביטים. קיבלנו חיבור של שני מצבים בקיוביט הראשון - זה אינו מצב מכפלה אלא מצב שזור.

[2]הרצאה שלישית

12.2 הנוסחא של עודד

$$
\begin{aligned}
|\mu\rangle &= \frac{1}{\sqrt{2}}\sigma^{\mu}_{ab}\,|a\rangle\otimes|b\rangle \\
\sigma^{\mu} &= (1,\vec{\sigma}) \\
\sigma^{0} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\sigma^{1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\sigma^{2} &= \pm i\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
\sigma^{3} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}
$$

למשל -

$$
\begin{aligned}
|\mu=0\rangle &= \frac{1}{\sqrt{2}}\delta_{a,b}\,|a\rangle\otimes|b\rangle = \\
&= \frac{1}{\sqrt{2}}\,|a\rangle\otimes|a\rangle = \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle\right) \\
|\mu=3\rangle &= \frac{1}{\sqrt{2}}\sigma^{3}_{a,b}\,|a\rangle\otimes|b\rangle = \\
&= \cdots = \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle\right) \\
|ab\rangle &= \frac{1}{\sqrt{2}}\sigma^{\mu}_{ab}\,|\mu\rangle \\
|00\rangle &= \frac{1}{\sqrt{2}}\sigma^{\mu}_{00}\,|\mu\rangle = \\
&= \frac{1}{\sqrt{2}}\left(|\mu=0\rangle+|\mu=3\rangle\right)
\end{aligned}
$$

13 שוויון הטלפורטציה

13.0.1 הכנה

ניקח

$$|\psi\rangle = \alpha_a\,|a\rangle$$

מה יקרה אם נפעיל σ^{μ} -

$$
\begin{aligned}
\sigma^{\mu}\,|\psi\rangle &= \alpha_a\sigma^{\mu}\,|a\rangle = \\
&= \alpha_a\sigma^{\mu}_{ab}\,|b\rangle
\end{aligned}
$$

(זו בסך הכל מכפלה של מטריצה בווקטור)

השוויון עצמו

לאליס יש $|\psi\rangle_A$ במצב לא ידוע. אליס ובוב מחלקים בינהם מצב בל (אפס) בן שני קיוביטים -

$$|\psi\rangle_A \otimes |\beta=0\rangle_{AB}$$

ונייצג - $|\psi\rangle = \alpha_a |a\rangle$אז, באמצעות המשוואה של עודד -

$$\begin{aligned}\alpha_a |a\rangle_A \otimes \frac{1}{\sqrt{2}}\sigma_{bc}^{\beta=0} |b\rangle_A \otimes |c\rangle_B &= \frac{1}{\sqrt{2}}\alpha_a \delta_{bc} |a_A b_A c_B\rangle = \\ &= \frac{1}{\sqrt{2}}\alpha_a |a_A b_A b_B\rangle\end{aligned}$$

כעת אליס רוצה להעביר את שני הקיוביטים של אליס כמצב בל, לכן היא מפעילה את אופרטור בל -

$$\begin{aligned}\left(\frac{1}{\sqrt{2}}\right)^2 \alpha_a \sigma_{ab}^{\mu} |\mu\rangle_A \otimes |b\rangle_B &= \frac{1}{2} |\mu\rangle_A \otimes (\alpha_a \sigma_{ab}^{\mu} |b\rangle_B) = \\ &= \frac{1}{2} |\mu\rangle_A \otimes |\sigma^{\mu}\psi\rangle\end{aligned}$$

המעבר האחרון - מהשוויון שהראנו ב"הכנה".

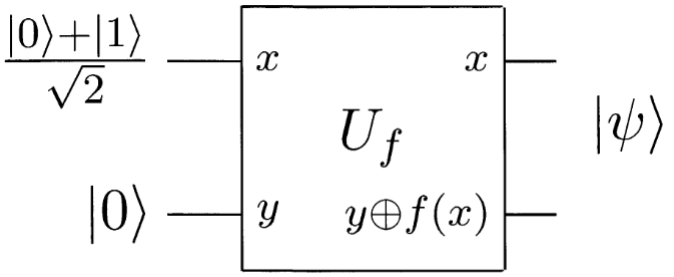
14 שחלוף של שזירה

לאליס ובוב מחלקים מצב $|\beta=0\rangle$ וגם בוב וקרול מחלקים $|\beta=0\rangle$.
לבוב יש שני קיוביטים, הוא יכול למדוד אותם בבסיס בל -

$$\begin{aligned}|\beta=0\rangle_{AB} \otimes |\beta=0\rangle_{BC} &= \frac{1}{2}\left(\sigma_{ab}^0 |a\rangle_A |b\rangle_B\right) \otimes \left(\sigma_{cd}^0 |c\rangle_B |d\rangle_C\right) = \\ &= \frac{1}{2}\delta_{ab}\delta_{cd}\left(|a\rangle_A |b\rangle_B\right) \otimes \left(|c\rangle_B |d\rangle_C\right) = \\ &= \frac{1}{2}\left(|a\rangle_A |a\rangle_B\right) \otimes \left(|c\rangle_B |c\rangle_C\right) \\ \text{Bob Moves to Bell state} \quad &\Rightarrow \quad \frac{1}{2^{\frac{3}{2}}} |a_A\rangle \otimes \sigma_{ac}^{\mu} |\mu\rangle_B \otimes |c\rangle_C = \\ \text{we change the positions of the qubits, for convinece} \quad &= \frac{1}{2^{\frac{3}{2}}} |\mu\rangle_B \otimes (\sigma_{ab}^{\mu} |a\rangle_A \otimes |c\rangle_C) = \\ &= \frac{1}{2} |\mu\rangle_B \otimes |\mu\rangle_{AC}\end{aligned}$$

וכעת הקיוביטים של אליס וקרול שזורים! (בוב צריך לספר להן איזה מצב בל יש להן)

15 חישוב מקבילי



איור 6: דוגמא לשער שמחשב פונקציה של שני קיוביטים

מה נקבל ביציאה של U_f אם נכניס -

$$\begin{aligned} |x\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |y\rangle &= |0\rangle \end{aligned}$$

מכניקה קוונטית היא לינארית, נתעלם מקבועי נרמול ונקבל -

$$\begin{aligned} |+\rangle|0\rangle = (|00\rangle+|10\rangle) \quad &\rightarrow \quad |0\rangle|0\oplus f(0)\rangle + |1\rangle|0\oplus f(0)\rangle = \\ &= |0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle \end{aligned}$$

חישבנו במקביל הן את $f(0)$ והן את $f(1)$.

ניקח -

$$\begin{aligned} x &= 0,1,2,\ldots 2^n-1 \\ &= |x_1\rangle\otimes|x_2\rangle\otimes\cdots|x_n\rangle \ : x_i\in\{0,1\} \end{aligned}$$

נבצע בניה אנלוגית לשני הקיוביטים לעיל, עבור n קיוביטים. נפעיל אופרטור הדמר על $n-1$ אפסים, ונזין את U_f (הפעם - מדובר בפונקציה של n קיוביטים, היא לא משנה את $n-1$ הראשונים, ומחזירה את $f(x_1,x_2,\ldots x_n)$ בקיוביט האחרון. בתור תוצאה נקבל מצב שהוא קומבינציה לינארית של כל התוצאות האפשריות של f.

16 האלגוריתם של דוייטש[3]

נתבונן על כל הפונקציות ממשתנה אחד למשתנה אחד מעל $(0,1)$ -

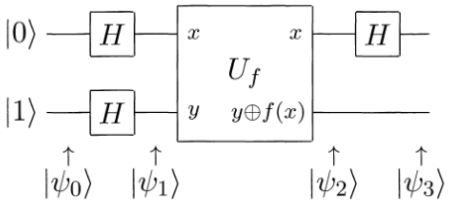
	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0
זוגיות	0	0	1	1

בעולם שלנו יש 4 פונקציות, ונתעניין מה הזוגיות של הפונקציה? ($p(f)=f(0)\oplus f(1)$)

כמה מאמץ חישוב צריך כדי לחשב את הזוגיות באמצעות המעגל הממש את הפונקציה? פעמיים, $f(0)$ ו-$f(1)$. נראה כעת כי ניתן לחשב את הזוגיות בצעד אחד -

[3] הרצאה רביעית - 24/3/10

16.1 האלגוריתם



נכניס לתוך המכונה $|+\rangle$ בביט העליון ו־$|-\rangle$ בתחתון -

$$\begin{array}{rcl}
|+\rangle\otimes|0\rangle & = & (|0\rangle+|1\rangle)\otimes|0\rangle\rightarrow|0\rangle\otimes|0\oplus f\left(0\right)\rangle+|1\rangle\otimes|0\oplus f\left(1\right)\rangle=|0\rangle\otimes|f\left(0\right)\rangle+|1\rangle\otimes|f\left(1\right)\rangle\\
|+\rangle\otimes|1\rangle & \rightarrow & \cdots\rightarrow|0\rangle\otimes|1\oplus f\left(0\right)\rangle+|1\rangle\otimes|1\oplus f\left(1\right)\rangle\\
 & \Downarrow & \\
|+\rangle\otimes|-\rangle & \rightarrow & |0\rangle\otimes(|f\left(0\right)\rangle-|1\oplus f\left(0\right)\rangle)+|1\rangle\otimes(|f\left(1\right)\rangle-|1\oplus f\left(1\right)\rangle)=\\
 & = & (-1)^{f(0)}|0\rangle\otimes|-\rangle+(-1)^{f(1)}|1\rangle\otimes|-\rangle=\\
 & = & (-1)^{f(0)}\left(|0\rangle\otimes|-\rangle+(-1)^{f(1)+f(1)}|1\rangle\otimes|-\rangle\right)=\\
 & = & (-1)^{f(0)}\left(|0\rangle\otimes|-\rangle+(-1)^{p(f)}|1\rangle\otimes|-\rangle\right)=\\
 & = & (-1)^{f(0)}\left(|0\rangle+(-1)^{p(f)}|1\rangle\right)\otimes|-\rangle
\end{array}$$

כלומר אם $p\left(f\right)=0$ נקבל -

$$|+\rangle\otimes|-\rangle$$

ואם $p\left(f\right)=1$ נקבל -

$$|-\rangle\otimes|-\rangle$$

לכן צריך למדוד רק את התוצאה של הקיוביט הראשון, ודרושה קריאה אחת ל־f כדי לקבוע האם היא זוגית או לא זוגית.

17 המצב של GHZ ונפלאותיו

17.1 חוקי המשחק של מכניקה קוונטית

נתון מצב $|\psi\rangle$ וקטור במרחב הילברט
מסתכלים בשני אופרטורים מדידים - M,N - כל אחד מטריצה הרמיטית.
בכדי שנוכל למדוד אותם ביחד נדרוש (או - נניח) כי $[M,N]=0$ ו־$|\psi\rangle$מצב עצי של שניהם -

$$\begin{array}{rcl}
M|\psi_{mn}\rangle & = & m|\psi_{mn}\rangle\\
N|\psi_{mn}\rangle & = & n|\psi_{mn}\rangle
\end{array}$$

בהסתברות 1 מדידה של M,N תיתן את m,n בהתאמה.

17.2 נגדיר משחק -

במשחק שלושה משתתפים - אליס, בוב וקרול - A, B, C
אסור למשתתפים להחליף אינפורמציה אבל מותר להם לעשות הכנות (למשל - לגבש אסטרטגיה משותפת)
שואלים כל אחד מהמשתתפים אחד משני סוגים של שאלות - X או Y כאשר האופציות לשיבוץ השאלות הן -

תשובה נדרשת	A	B	C
-1	X	X	X
$+1$	X	Y	Y
$+1$	Y	X	Y
$+1$	Y	Y	Y

התשובה הנדרשת היא מכפלת שלושת התשובות.

17.3 אין אסטרטגיה (קלאסית) מנצחת

נניח שיש אסטרטגיה כזו -

$$\begin{aligned} f_A(X) &\in \{+1,-1\} \\ f_A(Y) &\in \{+1,-1\} \\ f_B(X) &\in \{+1,-1\} \\ f_B(Y) &\in \{+1,-1\} \\ f_C(X) &\in \{+1,-1\} \\ f_C(Y) &\in \{+1,-1\} \end{aligned}$$

אז נקבל -

תשובה נדרשת	A	B	C	
-1	$f_A(X)$	$f_B(X)$	$f_C(X)$	
$+1$	$f_A(X)$	$f_B(Y)$	$f_C(Y)$	
$+1$	$f_A(Y)$	$f_B(X)$	$f_C(Y)$	
$+1$	$f_A(X)$	$f_B(Y)$	$f_C(Y)$	
-1	$+1$	$+1$	$+1$	מכפלת העמודה

כלומר - לא ייתכן שיש אסטרטגיה מנצחת

17.4 האסטרטגיה הקוונטית

$$|\psi\rangle = |GHZ\rangle = |000\rangle - |111\rangle = |0\rangle_A |0\rangle_B |0\rangle_C - |1\rangle_A |1\rangle_B |1\rangle_C$$

נגדיר -

$$M = X_A \otimes X_B \otimes X_C \quad X_\# = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

ונקבל -

$$M|\psi\rangle = |111\rangle - |000\rangle = -|\psi\rangle$$

ניקח -

$$X_A \otimes Y_B \otimes Y_C |\psi\rangle$$

כאשר -

$$\begin{aligned} Y|0\rangle &= +i|1\rangle \\ Y|1\rangle &= -i|1\rangle \end{aligned}$$

לכן -

$$\begin{aligned} X_A \otimes Y_B \otimes Y_C |\psi\rangle &= -|111\rangle + |000\rangle = |\psi\rangle \\ Y_A \otimes X_B \otimes Y_C |\psi\rangle &= -|111\rangle + |000\rangle = |\psi\rangle \\ Y_A \otimes Y_B \otimes X_C |\psi\rangle &= -|111\rangle + |000\rangle = |\psi\rangle \end{aligned}$$

כלומר אם אליס בוב וקרול היו מחלקים בינהם מצב $|GHZ\rangle$ לפני המשחק, ואז כל אחד מהם מפעיל שטרן־גרלך בכיוון X או Y בהתאם לשאלה שלהם - מובטח שמכפלת התשובות יקבלו את התשובות הנכונות.

18 חוקי המשחק

18.1 מערכת מבודדת

מצב המערכת מתואר ע"י פונקציית גל $|\psi\rangle$, וקטור במרחב הילברט, וההתפתחות שלה בזמן ע"י אופרטור אוניטרי -

$$|\psi\rangle \to U|\psi\rangle$$

ההתפתחות בזמן היא לינארית -

$$|\psi\rangle + |\varphi\rangle = U|\psi\rangle + U|\varphi\rangle$$

אם $|\psi_1\rangle, |\psi_2\rangle \dots |\psi_n\rangle$ אורטוגונליים אזי $U|\psi_1\rangle, U|\psi_2\rangle \dots U|\psi_n\rangle$ אורטוגונליים.
התפתחות אוניטרית נוצרת ע"י אופרטורים הרמיטיים -
נתבונן על U קרוב ליחידה

$$U = I + i\varepsilon A$$

כאשר A מטריצה. וכיוון ש־U אוניטרי -

$$1 = U^\dagger U = \left(I - i\varepsilon A^\dagger\right)(I + i\varepsilon A) =$$

נחשב עד סדר ראשון באפסילון -

$$= 1 + i\varepsilon\left(A - A^\dagger\right) + O\left(\varepsilon^2\right)$$

לכן -

$$\begin{aligned} A - A^\dagger &= 0 \\ A &= A^\dagger \end{aligned}$$

כלומר התפתחות אוניטרית בזמנים קצרים נוצרת ע"י מטריצה הרמיטית, וניתן לייצג גם ע"י -

$$U = e^{i\varepsilon A}$$

18.1.1 דוגמא

קיוביט -

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

כך ש-$\alpha, \beta \in \mathbb{C}$ (השפה של כדור בלוך)

$$U = \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} e^{i\gamma}$$

כך ש-

$$|a|^2 + \left|b^2\right| = 1$$

נשים לב ש-

$$det\left\{\begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix}\right\} = \left|a^2\right| + |b|^2 = 1$$

לכן $\begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} \in SU(2)$.

כתיבה אחרת -

$$\begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} = \frac{a+a^*}{2} I + \frac{b-b^*}{2}\sigma_x + \frac{b+b^*}{2i}\sigma_y + \frac{a-a^*}{2}\sigma_z$$

כלומר -

$$x_0 I + i\vec{x}\cdot\vec{\sigma}$$

כך שכל ה-xים ממשיים

$$\begin{aligned} I &= UU^\dagger = \\ &= (x_0 + i\vec{x}\cdot\vec{\sigma})(x_0 - i\vec{x}\cdot\vec{\sigma}) = \\ &= x_0^2 + (\vec{x}\cdot\vec{\sigma})(\vec{x}\cdot\vec{\sigma}) = \\ &= \end{aligned}$$

נזכור שמטריצות פאולי מקיימות -

$$\sigma_i\sigma_j + \sigma_j\sigma_i = 0 \quad i \neq j$$

לכן נקבל -

$$\cdots = x_0^2 + |\vec{x}|^2 = 1$$

כלומר כדור במרחב ארבע מימדי.

18.1.2 דוגמאות

$$\begin{aligned} NOT \qquad & X = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \\ \text{Hadmard} \qquad & H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{aligned}$$

בעולם P מימדי -

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_p \end{pmatrix}$$

נגדיר $\omega = e^{\frac{2\pi i}{p}}$ ונשים לב ש-

$$\omega^p = 1$$

ונבנה מטריצה $p \times p$ -

$$U = \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & & \omega^{p-1} \\ \vdots & \omega^2 & \omega^4 & & \omega^{2p-21} \\ & \dots & & & \\ 1 & \omega^{p-1} & \omega^{2p-2} & \dots & \omega^{(p-1)^2} \end{pmatrix}$$

זה הוא טרנספורם פורייה -

$$\left(U\left|\psi\right\rangle\right)_k = \sum_l U_{kl} \left|\psi\right\rangle_l = \frac{1}{\sqrt{p}} \sum_{l=0}^{p-1} \omega^{kl} \left|\psi\right\rangle_l = \frac{1}{\sqrt{p}} \sum_{l=0}^{p-1} e^{\frac{2\pi i k l}{p}} \left|\psi\right\rangle_l$$

18.1.3 דוגמא 3

$$\psi\left(x\right) \in L^2\left(\mathbb{R}\right)$$

כאשר -

$$1 = \left\langle \psi \,|\, \psi \right\rangle = \int_{-\infty}^{\infty} \left|\psi\left(x\right)\right|^2 dx$$

$$\hat{\psi}\left(p\right) = \frac{1}{\sqrt{2\pi\hbar}} \int \psi\left(x\right) e^{-\frac{ip}{\hbar}} dx$$

18.2 מדידות

במכניקה קוונטית קיימים observables שמיוצרים ע"י אופרטורים הרמיטיים. ניתן לפרק אופרטור כזהפירוק ספקטרלי -

$$M = \sum_m \mu_m |m\rangle \langle m|$$

כאשר $P_m = |m\rangle \langle m|$ היא הטלה על מצב עצמי m.
באופרטור הרמיטי $\mu_m \in \mathbb{R}$ ו־$P_m P_n = P_m \delta_{mn}$.
מדידה של M תיתן μ_m (ללא תלות ב־$|\psi\rangle$) ההסתברות לקבל כל אחד מה־μ_mים השונים נתותה ע"י -

$$P(\mu_m) = \langle\psi| P_m |\psi\rangle$$

ואחרי המדידה מצב המערכת הוא $|m\rangle$.

18.2.1 דוגמא

ניסוי $S - G$

$$M = \sigma_z = Z = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = |0\rangle \langle 0| - |1\rangle \langle 1|$$

18.2.2 דוגמא 2

$$L^2(\mathbb{R})$$

$$M = X_v(x) = \begin{cases} 1 \\ 0 \end{cases}$$

כאשר -

$$X_v^2(x) = X_v(x)$$

ההסתברות לקליק -

$$P(\text{click}) = \langle\psi | X_v | \psi\rangle = \int_V |\psi(x)|^2 dx$$

מדידות כאלו נקראות מדידות פרוייקטיביות (מדידים).
אבל אנחנו רוצים למדוד n מדידים שונים (עבור n גדול כרצוננו), ולא רק 2 מדידות אפשריות. הדרך לעשות זאת (למשל בניסוי שטרן גרלך) היא על ידי מספר "פיצולים" בטור - מדידה של σ_x ואחריה למשל σ_z וכו'... כך ניתן לפצל לכמה מדידים שנרצה.

18.3 מדידה מוכללת

d דטקטורים

$$M_j \quad j \in \{1, 2, \ldots d\}$$

המצב הראשוני הוא $|\psi\rangle$ ואחרי המדידה -

$$\frac{M_j |\psi\rangle}{N}$$

ההסתברות למדוד j -

$$Prob(j) = \left\langle \psi \left| \underbrace{M_j^\dagger M_j}_{\geq 0} \right| \psi \right\rangle = \|M_j |\psi\rangle\|^2$$

ונדרוש כמובן -

$$\begin{aligned} \sum_j Prob(j) &= 1 \\ &\Downarrow \\ \sum_j M_j^\dagger M_j &= \mathbb{1} \end{aligned}$$

18.3.1 דוגמא

$$\begin{aligned} P_{Z+} &= \frac{1+\sigma_z}{2} = M_1 \\ M_1^\dagger &= M_1 \\ M_1^\dagger M_1 &= M_1^2 = M_1 \end{aligned}$$

ובנוסף -

$$\begin{aligned} \left(\frac{1+\sigma_x}{2}\right)\left(\frac{1-\sigma_z}{2}\right) &= M_2 \\ \left(\frac{1-\sigma_x}{2}\right)\left(\frac{1-\sigma_z}{2}\right) &= M_3 \end{aligned}$$

מתקיים -

$$\begin{aligned} M_1^\dagger M_1 &= \left(\frac{1+\sigma_z}{2}\right) \\ M_2^\dagger M_2 &= \left(\frac{1-\sigma_z}{2}\right)\left(\frac{1+\sigma_x}{2}\right)\left(\frac{1-\sigma_z}{2}\right) \\ M_3^\dagger M_3 &= \left(\frac{1-\sigma_z}{2}\right)\left(\frac{1-\sigma_x}{2}\right)\left(\frac{1-\sigma_z}{2}\right) \end{aligned}$$

ו -

$$\left(\frac{1-\sigma_z}{2}\right)^2 = \left(\frac{1-\sigma_z}{2}\right)$$

לכן -

$$\sum_j M_j^\dagger M_j = \mathbb{1}$$

18.3.2 מצבי Positive Operator Values Measurment

בקיצור - POVM

$$E_j = M_j^\dagger M_j \geq 0$$

$$\sum_j M_j^\dagger M_j = 1$$

$$Prob\left(j\right) = \langle \psi \left| E_j \right| \psi \rangle$$

טענה 18.1 אליס מכינה מצב מתוך $|0\rangle, |1\rangle, \ldots |N\rangle$(כולם מאונכים זה לזה) ושולחת אותו לבוב. בוב יכול לדעת מה המצב שאליס שלחה בלי טעות!

נשתמש ב-N דטקטורים

$$\begin{aligned} E_j &= |j\rangle \langle j| \\ E_j^2 &= E_j \geq 0 \\ \sum_j E_j &= \mathbb{1} \end{aligned}$$

נשאל מה ההסתברות לזהות את j בהנחה שאליס שלחה את k -

$$\begin{aligned} Prob\left(j|k\right) &= \langle k \left| E_j \right| k \rangle = \\ &= \langle k| \left|j\right\rangle \langle j| \left|k\right\rangle = \\ &= \delta_{jk} \end{aligned}$$

טענה 18.2 אליס שולחת לבוב קיוביט $|\alpha\rangle$או $|\beta\rangle$ כאשר $\langle \alpha \left| \beta \right\rangle \neq 0$. בוב לא יכול לארגן שום POVM שיבדיל בוודאות בין הביטים.

הוכחה: נניח -

$$\begin{aligned} \langle \alpha \left| E_\alpha \right| \alpha \rangle &= 1 \\ \langle \beta \left| E_\beta \right| \beta \rangle &= 1 \end{aligned}$$

זי -

$$\begin{aligned} 1 &= \langle \alpha \left| \alpha \right\rangle = \langle \alpha \left| E_\alpha + E_\beta \right| \alpha \rangle = 1 + \langle \alpha \left| E_\beta \right| \alpha \rangle \\ &\Downarrow \\ \langle \alpha \left| E_\beta \right| \alpha \rangle &= 0 \\ \langle \beta \left| E_\alpha \right| \beta \rangle &= 0 \end{aligned}$$

נראה שלא ניתן למצא E_α ו-E_β כאלו אם $\langle \alpha \left| \beta \right\rangle \neq 0$ -

$$|\alpha\rangle = |\beta\rangle \langle \beta \left| \alpha \right\rangle + \gamma |\gamma\rangle$$

ואז -

$$|\langle \alpha \left| \beta \right\rangle|^2 + |\gamma|^2 = 1$$

$$\begin{aligned} 1 &= \langle\alpha\,|\,\alpha\rangle = \\ &= \langle\alpha|\,E_\alpha + E_\beta\,|\beta\rangle\,\langle\beta\,|\,\alpha\rangle + \gamma\,|\gamma\rangle = \end{aligned}$$

ראינו כי $E_\beta\,|\alpha\rangle = 0$ לכן כאשר הוא פועל על צד ימין הוא מתאפס - ונשארנו בלי כלום... כאשר מפעילים את E_α על $|\beta\rangle$ מקבלים כנ"ל, לכן נותרנו עם -

$$1 = \langle\alpha\,|\,E_\alpha\gamma\,|\,\gamma\rangle$$

באותה צורה מצד שמאלנ נקבל -

$$1 = \underbrace{|\gamma|^2}_{<1}\underbrace{\langle\gamma\,|\,E_\alpha\,|\,\gamma\rangle}_{\leq 1}$$

וזו סתירה. ■

19 הבחנות - מדידות

בהרצאה הקודמת דיברנו על $POVM$, המקיימים -

$$\begin{aligned} M_j^\dagger M_j &= E_j \geq 0 \\ \sum_j E_j &= 1 \end{aligned}$$

ההסתברות שהגלאי j יעשה "קליק" אם המצב הוא $|\psi\rangle$ היא -

$$P_j = \langle\psi\,|\,E_j\,|\,\psi\rangle$$

ראינו שאם אליס שולחת אחד מתוך N מצבים מאונכים בוב יכול לבצע מדידה <u>ולזהות בוודאות</u> את המצב שנשלח. ע"י -

$$E_j = |j\rangle\,\langle j|$$

ראינו גם שאם אליס שולחת אחד מתוך שני (או יותר) מצבים לא אורטוגונליים אזי אין לבוב אפשרות למדוד <u>בוודאות</u> איזה מצב נשלח. נראה כעט מה כן ניתן להבטיח -

20 מדידות בלי טעות

ניתן להבטיח מדידה ללא טעויות של שני מצבים שאינם אורטוגונליים אם מאפשרים ל-$POVM$ להחזיר אחת משלוש אפשרויות -

1. המצב הוא בוודאות $|\psi\rangle$
2. המצב הוא בוודאות $|\varphi\rangle$
3. לא ניתן לדעת

נגדיר את הוקטורים הדואליים - $\langle\varphi^*|\,,\langle\psi^*|$ כך שיתקיים -

$$\langle\psi^*\,|\,\varphi\rangle = \langle\varphi^*\,|\,\psi\rangle = 0$$

נגדיר את האופרטורים -

$$\begin{aligned} E_\psi &= k\left|\psi^*\right\rangle\left\langle\psi^*\right| \geq 0 \\ E_\varphi &= k\left|\varphi^*\right\rangle\left\langle\varphi^*\right| \geq 0 \\ E &= I - E_\psi - E_\varphi \end{aligned}$$

צריך לוודא ש־E חיובי, לכן שמנו את הקבוע k באופרטורים E_ψ, E_φ.
נראה כיצד האופרטורים פועלים -

$$\begin{aligned} \left\langle\varphi\right| E_\psi \left|\varphi\right\rangle &= k\left|\left\langle\psi^*\right|\left.\varphi\right\rangle\right|^2 = 0 \\ \left\langle\psi\right| E_\varphi \left|\psi\right\rangle &= k\left|\left\langle\varphi^*\right|\left.\psi\right\rangle\right|^2 = 0 \end{aligned}$$

נניח שנקבע את $|\psi\rangle = |0\rangle$, והזווית בין $|\varphi\rangle, |\psi\rangle$ היא θ, נקבל כי -

$$\begin{aligned} \left|\varphi^*\right\rangle &= \left|1\right\rangle \\ \left|\varphi\right\rangle &= \cos\theta\left|0\right\rangle + \sin\theta\left|1\right\rangle \\ \left|\psi^*\right\rangle &= \sin\theta\left|0\right\rangle - \cos\theta\left|1\right\rangle \end{aligned}$$

לכן -

$$\begin{aligned} E_\varphi &= k\left|\varphi^*\right\rangle\left\langle\varphi^*\right| = k\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ E_\psi &= \ldots = k\begin{pmatrix} \sin^2 & -\sin\cos \\ -\sin\cos & \cos^2 \end{pmatrix} \end{aligned}$$

וצריך להתקיים -

$$0 \leq E_1 + E_2 \leq 1$$

$$A = k\begin{pmatrix} \sin^2 & -\sin\cos \\ -\sin\cos & \cos^2+1 \end{pmatrix} \leq 1$$

נמצא ע"ע -

$$\begin{aligned} Tr\left(A\right) &= \sin^2+\cos^2+1 = 2 \\ Det\left(A\right) &= \sin^2\left(\cos^2+1\right) - \sin^2\cos^2 = \sin^2 \end{aligned}$$

לכן -

$$\begin{aligned} \lambda + \frac{\sin^2}{\lambda} &= 2 \\ \lambda^2 - 2\lambda + \sin^2 &= 0 \\ \lambda_\pm &= \frac{2 \pm \sqrt{4-4\sin^2}}{2} = 1 \pm \cos\theta \end{aligned}$$

וה־k הטוב ביותר שניתן לבחור הוא -

$$k = \frac{1}{1+\left|\cos\theta\right|}$$

כעת נבדוק מה ההסתברות שהגלאי של ψ אכן יזהה אותו -

$$\begin{aligned} P_\psi &= \left\langle\psi\right| E_\psi \left|\psi\right\rangle = k\left|\left\langle\psi^*\right|\left.\psi\right\rangle\right|^2 = \frac{\sin^2}{1+\left|\cos\right|} \\ P_\varphi &= \left\langle\varphi\right| E_\varphi \left|\varphi\right\rangle = k\left|\left\langle\varphi^*\right|\left.\varphi\right\rangle\right|^2 = \frac{\sin^2}{1+\left|\cos\right|} \end{aligned}$$

כלומר - אם הזווית θ קטנה מאד, ההסתברות למדוד מידע "מועיל" קטנה מאד, ברור המקרים נקבל "קליק" בגלאי השלישי שאומר "לא ניתן לדעת". לעומת זאת, אם $\theta = \frac{\pi}{2}$ - נקבל מדידה נכונה בכל המקרים (זה למעשה המקרה שכבר ראינו).

21 משפט Bayes

כעת אליס שולחת אחד משני מצבים $|\psi\rangle, |\varphi\rangle$ עם זווית θ בינהם. הפעם בוב לא מוכן לאבד חלקיקים, אבל הוא מוכן לעשות טעויות לפעמים. נשאלת השאלה - עד כמה הוא יכול בטוח להיות במדידות שלו. בוב מבצע שתי מדידות -

$$\begin{aligned} E_1 &= |u\rangle\langle u| \geq 0 \\ E_2 &= |v\rangle\langle v| \geq 0 \end{aligned}$$

כך שמתקיים - $E_1 + E_2 = 1$. איך בוחרים u אופטימלי?
נניח שבוב מדד $|u\rangle$, מה ההסתברות שאליס אכן שלחה את $|\varphi\rangle$? -

$$\begin{aligned} \mathbb{P}(|\varphi\rangle \,||u\rangle) &= \frac{\mathbb{P}(|\varphi\rangle \wedge |u\rangle)}{\mathbb{P}(|u\rangle)} = \\ &= \frac{|\langle u \,|\, \varphi\rangle|^2 P(|\varphi\rangle)}{P(|u\rangle)} = \\ &= \frac{|\langle u \,|\, \varphi\rangle|^2 P(|\varphi\rangle)}{P(|u\rangle, |\varphi\rangle) + P(|u\rangle, |\psi\rangle)} \\ &= \frac{\cos^2\alpha}{\cos^2\alpha + \cos^2(\alpha+\theta)} \end{aligned}$$

כאשר θ הזווית בין $|\psi\rangle, |\varphi\rangle$ ו-α הזווית בין $|\varphi\rangle$ ו-$|u\rangle$.
השאלה ההפוכה פשוטה יותר -

$$P(|u\rangle \,||\varphi\rangle) = |\langle u \,|\, \varphi\rangle|^2$$

22 מטריצות צפיפות (פורמליזם)

עד היום דיברנו על מצב מתואר ע"י $|\psi\rangle$, התפתחות בזמן מתוארת ע"י טרנספורמציה אוניטרית - $u|\psi\rangle$, ו-$POVM$ המקיימים - $P_j = \langle\psi| E_j |\psi\rangle$ כאשר $E_j \geq 0$.
כזכור, לכל צורך אין הבדל בין $|\psi\rangle$ לבין $e^{i\gamma}|\psi\rangle$ (פאזה כללית לא משפיעה!)
פאזה גלובלית של פונקיות הגל אינה מדיד פיסיקאלי.

$$\rho = |\psi\rangle\langle\psi|$$

אובייקט עיוור לפאזה הגלובלית

22.1 חוקי המשחק

$$\rho^2 = |\psi\rangle\langle\psi \,|\, \psi\rangle\langle\psi| = \rho$$

$$\rho \geq 0$$

$$Tr(\rho) = 1$$

נשמור בהמשך על שתי הדרישות האחרונות, לא על הראשונה.

התפתחות בזמן -

$$\rho \to u\rho u^{\dagger}$$

וההסתברות למדידת j -

$$P_j = Tr\left(E_j\rho\right) = Tr\left(E_j\left|\psi\right\rangle\left\langle\psi\right|\right) = \left\langle\psi\right|E\left|\psi\right\rangle$$

23 מערכת מורכבת ומכפלה טנזורית

נניח שלאליס ובוב יש מצבים -

$$\begin{array}{ll} \left|\varphi\right\rangle_A & Alice \\ \left|\psi\right\rangle_B & Bob \end{array}$$

והמצב הוא -

$$\left|\varphi\right\rangle_A \otimes \left|\psi\right\rangle_B$$

במצב מכפלה - אליס ובוב ב"ת.
מדידות של אליס -

$$E_j \otimes \mathbb{1}$$

מדידות של בוב -

$$\mathbb{1} \otimes E_k$$

מדידות משותפות -

$$\begin{array}{rcl} P\left(j,k\right) & = & \left(\left\langle\varphi\right|_A\left\langle\psi\right|_B\right)\left(E_j\otimes E_k\right)\left(\left|\varphi\right\rangle_A\left|\psi\right\rangle_B\right) = \\ & = & \left\langle\varphi\right|E_j\left|\varphi\right\rangle\left\langle\psi\right|E_k\left|\psi\right\rangle \end{array}$$

זה מתאר מצב שבו אליס ובוב בלתי תלויים בינהם.
מצבים שאינם מצבי מכפלה הם מצבים שזורים,

$$\left|\beta_0\right\rangle = \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}$$

ואז -

$$P\left(j,k:\left|\beta\right\rangle\right) = \frac{1}{2}\delta_{jk}$$

יש קורלציה בין המצבים!

24 מושג Ancilla

נניח שיש לנו מצב $\left|\psi\right\rangle_A$ ש"חי" במרחב הילברט $\mathcal{H}^n$, אפשר להוסיף לו מספר קיוביטים ולקבל -

$$\left|\psi\right\rangle_A \otimes \left|j\right\rangle \in \mathcal{H}^n \otimes \mathcal{H}^m$$

24.1 דוגמא ל־$POVM$ ותרגומם ל־Ancillas

$$\begin{aligned} u\left|\varphi\right\rangle_A \otimes \left|0\right\rangle &= \sum_j M_j \left|\varphi\right\rangle_A \left|j\right\rangle \\ u\left|\psi\right\rangle_A \otimes \left|0\right\rangle &= \sum_j M_j \left|\psi\right\rangle_A \left|j\right\rangle \end{aligned}$$

כאשר ל־Ancilla יש מרחב הילברט ממימד m.
מה קורה כאשר -

$$\begin{aligned} \left\langle \Phi \right| u^\dagger u \left| \Psi \right\rangle &= \sum_j \sum_k \left(\left\langle k \right| \otimes \left(\left\langle \psi \right|_A M_k^\dagger \right) \left(M_j \left|\varphi\right\rangle_A \right) \otimes \left|j\right\rangle \right) = \\ &= \sum_j \left\langle \psi_A \right| \left(M_j^\dagger M_j \right) \left|\varphi\right\rangle_A = \left\langle \psi_A \right| \left. \varphi_A \right\rangle \end{aligned}$$

25 מערכות מורכבות

25.1 קלאסי

נתבונן במערכת רבת חלקיקים -

- חלקיק בודד, קלאסי מתואר ע"י נקודה במרחב הפאזות - $(x,p) \in \mathbb{R}^2$.
- שני חלקיקים, $(x_1, x_2, p_1, p_2) \in \mathbb{R}^4$
- n חלקיקים $(x_1, p_1, x_2, p_2, \ldots x_n, p_n)$ - מערכת ממימד $2n$

25.2 קוונטי

- קיוביט בודד - $\left|\psi\right\rangle = \sum_{a=0}^{1} \psi_a \left|a\right\rangle$ - $(\psi_0, \psi_1) \in \mathbb{C}^2$
- שני קיוביטים - $\left|\Psi_2\right\rangle = \sum_{a,b\in\{0,1\}} \psi_{ab} \left|a\right\rangle \left|b\right\rangle$ - מרחב ממימד 4
- עבור n קיוביטים - $\left|\Psi_n\right\rangle = \sum_{a_1 a_2 \ldots a_n \in \{0,1\}} \psi_{a_1 a_2 \ldots a_n} \left|a_1\right\rangle \left|a_2\right\rangle \ldots \left|a_n\right\rangle$ - יש 2^n מספרים מרוכבים

מימד המערכת גדל אקספוננציאלית עם מספר החלקיקים, לא לינארית!

26 מדידות מרוכבות

מדידה אחת M_j -

$$\sum_{j=1}^{n} M_j^\dagger M_j = 1$$

ואם נמצא j -

$$P\left(j|\psi\right) = \left\langle \psi \right| \left. M_j^\dagger M_j \right| \psi \right\rangle$$

לכן -

$$|\psi\rangle \to \frac{M_j |\psi\rangle}{Factor}$$

כאשר פקטור הנרמול - $Factor = \sqrt{\left\langle \psi \left| M_j^\dagger M_j \right| \psi \right\rangle} = \sqrt{P\left(j|\psi\right)}$ כלומר -

$$|\psi\rangle \to \frac{M_j |\psi\rangle}{\sqrt{P\left(j|\psi\right)}}$$

מדידנה שניה - N_α ($\sum_\alpha N_\alpha^\dagger N_\alpha = 1$) ונשאלת השאלה - מה ההסתברות שנקבל במדידה הראשונה j ובמדידה השנייה α אם נתון שהמצב הראשוני היה ψ -

$$P\left(j,\alpha|\psi\right) = \left\langle \psi \left| M_j^\dagger N_\alpha^\dagger N_\alpha M_j \right| \psi \right\rangle$$

נגדיר -

$$\widetilde{M_{\alpha j}} = N_\alpha M_j$$

ונראה כי -

$$\sum_{\alpha,j} \widetilde{M_{j\alpha}}^\dagger \widetilde{M_{j\alpha}} = 1$$

מתקיים -

$$\begin{aligned} \sum_{\alpha,j} \widetilde{M_{j\alpha}}^\dagger \widetilde{M_{j\alpha}} &= \sum_{\alpha,j} M_j^\dagger N_\alpha^\dagger N_\alpha M_j = \sum_j M_j^\dagger \left(\sum_\alpha N_\alpha^\dagger N_\alpha \right) M_j = \\ &= \sum_j M_j^\dagger M_j = 1 \end{aligned}$$

אחרי המדידה הראשונה -

$$|\psi\rangle \to \frac{M_j |\psi\rangle}{\sqrt{P\left(j|\psi\right)}}$$

ואז מודדים עם N_α -

$$\frac{M_j |\psi\rangle}{P\left(j|\psi\right)} \to \frac{N_\alpha \frac{M_j|\psi\rangle}{\sqrt{P(j|\psi)}}}{P\left(\alpha, \frac{M_j|\psi\rangle}{\sqrt{P(j|\psi)}}\right)}$$

ונקבל -

$$P\left(\alpha,j|\psi\right) = P\left(j,\psi\right) P\left(\alpha,j\right) = \left\langle \psi \left| M_j^\dagger N_\alpha^\dagger N_\alpha M_j \right| \psi \right\rangle$$

27 מטריצות צפיפות

מה היא פונקציית הגל?

בראייה הנדסית - מכונה לחישוב הסתברות לכל שאלה שנוכל לנסח.
איך נתאר מערכת שבה שני מצבים אפשריים $|\varphi\rangle, |\psi\rangle$ כאשר ההסתברות לכל אחד מהמצבים היא p, q בהתאמה (וכמובן $p+q=1$)?
כל האינפורמציה על הסטטיסיטקה של המערכת מוחבאת באובייקט הבא -

$$\rho = p\,|\psi\rangle\langle\psi| + q\,|\varphi\rangle\langle\varphi|$$

מצב המערכת אינו מהצורה -

$$|\Psi\rangle \neq C\,|\psi\rangle + S\,|\varphi\rangle$$

אזי $E_j = M_j^\dagger M_j$

$$\begin{aligned} P(j|\psi) &= \langle\psi\,|\,E_j\,|\,\psi\rangle = Tr\left(E_j\,|\psi\rangle\langle\psi|\right) \\ P(j|\varphi) &= Tr\left(E_j\,|\varphi\rangle\langle\varphi|\right) \end{aligned}$$

לכן -

$$\begin{aligned} P(j) &= P(j|\psi)\,P(\psi) + P(j|\varphi)\,P(\varphi) = \\ &= pTr\left(E_j\,|\psi\rangle\langle\psi|\right) + qTr\left(E_j\,|\varphi\rangle\langle\varphi|\right) = \\ &= Tr\left(E,\rho\right) \end{aligned}$$

קיבלנו דרך פשוטה להבין מה זו מטריצת צפיפות.

27.1 עקרונות

27.2 חוקי המשחק

ראינו כבר שמטריצת הצפיפת היא מטריצה חיובית $\rho \geq 0$ עם עקבה 1 - $Tr[\rho] = 1$. במצב טהור $\rho = |\psi\rangle\langle\psi|$ מטריצת צפיפות היא הטלה אם $\rho = \rho^2$.
לדוגמא - $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ היא הטלה של $|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

תמיד מתקיים - $\rho^2 \leq \rho$, ואי השוויון הוא ממש עבור מצב שאינו טהור. למשל - $\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (זה המצב הכי רחוק מהיות מצב טהור) ועבורו מתקיים - $\rho^2 = \frac{1}{2}\rho$.

מדידה של $E_j = M_j^\dagger M_j$ ($POVM$) - ההסתברות שנקבל את התוצאה j כאשר נתונה מטריצה צפיפות ρ היא $\mathbb{P}(j|\rho) = Tr[E_j\rho]$.
ואם יצאה j אז -

$$\rho \to \frac{M_j \rho M_j^\dagger}{Tr\left[M_j \rho M_j^\dagger\right]} = \frac{M_j \rho M_j^\dagger}{\mathbb{P}(j|\rho)}$$

אם עכשיו יש מערכת $POVM$ בת שני מצבים אפשריים, מודדים את שני המצבים ו"מערבבים" את המצבים המדודים מחדש, נקבל -

$$\rho \to \sum_j P_j \rho_j = \sum_j \mathbb{P}(j|\rho)\,\frac{M_j \rho M_j^\dagger}{\mathbb{P}(j|\rho)} = \sum_j \left[M_j \rho M_j^\dagger\right]$$

נוודא שאכן יש לנו מטריצת צפיפות -

- $Tr\left[\sum_j M_j \rho M_j^\dagger\right] = \sum_j Tr\left[M_j \rho M_j^\dagger\right] = \sum_j Tr\left[M_j^\dagger M_j \rho\right] = 1$
- איך נראה כי המצב החדש מקיים $\rho \geq 0$?

ניתן להראות עלידי כך שלכל $|\psi\rangle$ מתקיים $\langle\psi\,|\,\rho\,|\,\psi\rangle \geq 0$

אבל מטריצת הצפיפות החדשה היא סכום של מטריצות, מספיק להראות כי הקריטריון מתקיים עבור כל אחד מאברי הסכום, ולכן מתקיים גם עבור סכומם -

$$\left\langle\psi\,\middle|\,M_j\rho M_j^\dagger\,\middle|\,\psi\right\rangle = \left\langle\psi M_j^\dagger\,\middle|\,\rho\,\middle|\,M_j\psi\right\rangle \geq 0$$

(אי השווין האחרון - כי מטריצת הצפיפות המקורית חיובית).

28 טומוגרפיה קוונטית

ρ מצב המערכת. יש לנו מכונה, שאנחנו לא יודעים איזה מצב היא מוציאה, אך היא מוציאה את אותו המצב שוב ושוב.

28.1 קיוביט בודד

$\rho = \frac{1+\vec{r}\cdot\vec{\sigma}}{2}$ ונרצה למצא את $\vec{r}$.

$$\sigma_x \to Tr\left[\sigma_x\rho\right] = Tr\left[\sigma_x\left(\frac{1+\vec{r}\cdot\vec{\sigma}}{2}\right)\right]$$

$$\begin{aligned}\langle\sigma_x\rangle &= \frac{1}{2}Tr\left[\sigma_x\left(r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\right)\right] = \\ &= \frac{1}{2}\left[r_x\cdot 2 + 0 + 0\right] = r_x\end{aligned}$$

כלומר - מדידת הממוצע של σ_x תתן את r_x ובדומה גם עבור y ו-z.
כלומר - בהנתן "אינסוף" קיוביטים באותו מצב ניתן לבצע מספיק מדידות כדי לקבוע את מצב המערכת.

28.2 שני קיוביטים

$\rho = \sum_{\mu\nu}\rho_{\mu\nu}\sigma_\mu\sigma_\nu$
כאשר - $\sigma_\mu = (1, \vec{\sigma})$
$Tr\left[\rho\right] = 1 = \rho_{00}\cdot 4$
$\rho_{00} = \frac{1}{4}$ ועבור מצב כללי נצטרך למדוד את כל שאר המקדמים (15)

28.3 n קיוביטים

באותו האופן, מספר המדדים שנצטרך הוא $4^n - 1$. המשמעות היא שטומוגרפיה היא פרקטית רק עבור מספר קטן מאד של קיוביטים.

29 היוצרים של מדידות אינפיניטיסימליות (לא נעשה)

30 עקבה חלקית

יש מערכת המשותפת לאליס ובוב - ρ_{AB}
נתעניין בשאלה הבאה - לאליס אסור לדבר עם בוב, היא יכולה לבצע רק מדידות במעבדה שלה (ρ_A מתאר רק את מה שאליס מסוגלת לעשות) והשאלה היא איך ניתן לקשר בין ρ_A ו-ρ_{AB})
רוצים לחפש $\rho_A \in \mathcal{H}_A$,$\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ כך -

$$Tr_{A+B}\left[\left(E_j \otimes \mathbb{1}\right)\rho_{AB}\right] = Tr_A\left[E_j \rho_A\right]$$

הפתרון הוא העקבה החלקית -

$$\rho_A = Tr_B\left[\rho_{AB}\right]$$

כאשר -

$$Tr_B\left[C \otimes D\right] = \underbrace{Tr\left[D\right]}_{number} \cdot \underbrace{C}_{matrix}$$

לכן במקרה הכללי -

$$Tr_B\left[\sum_i \rho_i A_i \otimes B_i\right] = \sum_i \rho_i \cdot Tr\left[B_i\right] \cdot A_i$$

30.1 דוגמא

$|\beta\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$ נתבונן על מטרית צפיפות -

$$\rho = |\beta\rangle\langle\beta|$$

כיוון שהמצב הוא מצב טהור - אליס ובוב (ביחד) יודעים הכל על המערכת.
$|\beta\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |3\rangle\right]$ לכן -

$$|\beta\rangle\langle\beta| = \frac{1}{2}\begin{pmatrix} 1 & & & 1 \\ & 0 & 0 & \\ & 0 & 0 & \\ 1 & & & 1 \end{pmatrix}$$

אבל איזו מטריצת צפיפות מתארת את המערכת מבחינת אליס לבדה?

$$\rho_A = Tr_B\left[|\beta\rangle\langle\beta|\right] = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\dim \mathcal{H}_A}\mathbb{1}$$

זה הוא מצב מעורב לחלוטין (אפשר לחשוב עליו כסכום של שני מצבים מנוגדים)

30.2 דוגמא נוספת

$\rho_{AB} = \rho_A \otimes \rho_B$ כאשר - $\rho_A = |\psi\rangle\langle\psi|\,,\ \rho_B = |\varphi\rangle\langle\varphi|$ אז -

$$Tr_B\left[\rho_{AB}\right] = \rho_A$$

כצפוי...

31 פרוק שמידט

נניח שיש מצב $|\psi\rangle = \sum \psi_{ij} |i\rangle_A \otimes |j\rangle_B$ כאשר i, j בסיסים לאליס ובוב בהתאמה.
נשאל - מה הצורה הקנונית של סופרפוזיציה כזו?
התשובה - ניתן לבחור בסיס חדש בעולם של אליס ובסיס חדש בעולם של בוב $\mathcal{H}_A, \mathcal{H}_B$ שבסיסיהם - $|k)_A, |l)_B$ כך ש-

$$|\psi\rangle = \sum_j d_j |j)_A |j)_B$$

כלומר - הורדנו את מספר האיברים בסכום מ-n^2 ל-n. כאשר n המימד של $\mathcal{H}_A$ או $\mathcal{H}_B$.

31.0.1 שמות

- מספר האלמנטים d_j השונים מאפס נקרא מספר שמידט
  $1 \leq Schmidt\ number\ \leq \min\{\dim \mathcal{H}_A,\ \dim \mathcal{H}_B\}$
- אם מספר שמידט הוא אחד (כלומר כל ה-d_jים הם אפס פרט לאחד) אזי $|\psi\rangle = |i\rangle \otimes |i\rangle$ - כלומר $|\psi\rangle$ הוא מצב מכפלה בבסיס מסויים.
- אם מספר שמידט גדול מאחד אזי לא ניתן להביא אותו למצב של מספר מכפלה - וזו היא ההגדרה של מצב טהור שזור

מצב בל הוא מצב שזור ונתון בפרוק שמידט של

$$|\beta\rangle = \frac{1}{\sqrt{2}} [|00\rangle + |11\rangle]$$

$$\psi_{ij} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

הוכחה: (למשפט שמידט)
$M^\dagger M \geq 0$ לכן

$$M^\dagger M = U D^2 U^\dagger$$

כאשר U אוניטרית, ו-D^2 מטריצה אלכסונית שמקדמיה חיוביים
כנ"ל לגבי $MM^\dagger$ לכן -

$$MM^\dagger = V D^2 V^\dagger$$

(זה נובע מכך של-$MM^\dagger$ ו-$M^\dagger M$ יש אותם ע"ע)
לכן -

$$M = VDU$$

זה נקרא SVD (Singular Value Decomposition) לכן -

$$\begin{aligned} |\psi\rangle &= \sum M_{ij} |i\rangle_A \otimes |j\rangle_B = \\ &= \sum_{ij} (VDU)_{ij} |i\rangle \otimes |j\rangle = \\ &= \sum_{ij} \left(\sum_k V_{ik} D_{kk} U_{kl} |i\rangle \otimes |j\rangle \right) = \\ &= \sum_k D_k \left(\sum_i V_{ik} |i\rangle \right) \otimes \left(\sum_j U_{kj} |j\rangle \right) \end{aligned}$$

זו היא למעשה העברת בסיס! לכן -

$$= \sum_k D_k \left|k'\right) \otimes \left|k''\right)$$

■

32 פירוק שמידט - דוגמאות

אם אנחנו יודעים לחלק את העולם לשניים - A, B ובכל אחד מהם מספר קיוביטים.
ומתקיים -

$$\begin{aligned} \dim \mathcal{H}_A &= m \\ \dim \mathcal{H}_B &= n \\ n &\geq m \\ |j\rangle &\in \mathcal{H}_A \\ |\alpha\rangle &\in \mathcal{H}_B \end{aligned}$$

מצב כללי הוא מהצורה -

$$|\psi\rangle = \sum_n C_{\alpha j} \left|j\right\rangle_A \otimes \left|\alpha\right\rangle_B$$

ואז C היא מטריצה $n \times m$.
השאלה היא מה ההצגה הקנונית (בחירת בסיס שיאפס את האיברים הלא אלכסוניים של C)?
כפי שראינו לעיל, ניתן לבחור בסיס כנ"ל, ואז נקבל -

$$|\psi\rangle = \sum_m \sqrt{p_j} \left|j\right\rangle_A \otimes \left|\alpha_j\right\rangle_B$$

כאשר - $p_j \geq 0$ לכל j ובנוסף - $\sum_j p_j = 1$. (נשים לב שקיבלנו m מקדמים, במקום $n \times m$!)

32.1 הדרך לחשב את p_j

$$\left(C^\dagger C\right)_{jk} = \left(C^\dagger\right)_{j\alpha} C_{\alpha k} = \sum C^*_{\alpha j} C_{\alpha k}$$

המטריצה $C^\dagger C$ היא מטריצה ריבועית $m \times m$ ו-p_j הם הע"ע העצמיים שלה.

- מספר הע"ע השונים מאפס נקרא מספר שמידט
- מספר שמידט $= 1$ הוא מצב מכפלה - $|\psi\rangle = \left|\varphi\right\rangle_A \otimes \left|\varphi'\right\rangle_B$
- מספר שמידט גדול מאחד נקרא מצב שזור.

למעשה - גודלו של מספר שמידט מצביע על "שזירותו" של המצב, ונהוג לקחת כמדד את הלוגריתם של מספר שמידט.

32.2 דוגמא - מצבי Bell

מצבי בל הם כבר מפורקים שמידט, למשל -

$$\begin{aligned} |\beta\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \\ C &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

כאן המצב כבר מפורק שמידט ומספר שמידט הוא 2.

32.3 מצב שזור

$$|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

זה כמובן איננו מפורק שמידט

32.4 דוגמא עם מספר שמידט ענק

נניח שלאליס יש n קיוביטים ולבוב יש n קיוביטים אחרים. מצב כללי נראה כך -

$$|\psi\rangle = \sum_{\substack{j=1\\k=1}}^{2^n} C_{jk}\,|j\rangle \otimes |k\rangle$$

אם כך, המצב הכללי מיוצג ע"י מטריצה בגודל $2^n \times 2^n$ (סה"כ 2^{2n} איברים)
פירוק שמידט יראה שניתן לכתוב מצב ע"י 2^n מחוברים -

$$|\psi\rangle = \sum_{j=1}^{2^n} C'_j\,|j\rangle \otimes |j'\rangle$$

לדוגמא מצב כזה -

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=1}^{2^n} |j\rangle \otimes |j\rangle$$

ניתן ליצור מצב כזה ע"י הפעלת $H^{\otimes n}$ (n שערי הדמר) על $|0\rangle^{\otimes n}$.

32.4.1 תרגיל

נניח שיש לנו מצב שזור כנ"ל, איך נראית מטריצת הצפיפות של אליס?

$$\begin{aligned}
\rho_A &= \frac{1}{2^n}\sum_j Tr_B\left[|j\rangle \otimes |j\rangle\langle k| \otimes \langle k|\right] = \\
&= \frac{1}{2^n}\sum_{jk} |j\rangle\langle k|\, Tr_B\left[|j\rangle\langle k|\right] = \\
&= \frac{1}{2^n}\sum_j |j\rangle\langle j| = \\
&= \mathbb{1}
\end{aligned}$$

זוהי מטריצת היחידה - כלומר אין כל מידע (מטריצת היחידה מייצגת את הנקודה שבמרכז כדור בלוך).

33 טיהור purification

משפט 33.1 כל מטריצת צפיפות ρ_A ניתן להפוך למצב טהור (לטהר) ע"י הוספת אנסילה מגודל $\dim \mathcal{H}_A$. **הוכחה:** כל ρ_A ניתן להציג ע"י פירוק ספקטרלי -

$$\rho_A = \sum p_j\,|j\rangle\langle j|$$

כך - $\sum_j p_j = 1$ ו-$p_j \geq 0$.

ניקח -

$$|\psi\rangle = \sum_j \sqrt{p_j} \overbrace{|j\rangle}^{\substack{\text{Original} \\ \text{Hilbert space}}} \otimes \overbrace{|j\rangle}^{\substack{\text{Hilbert space} \\ \text{for ancillas}}}$$

כעת -

$$\rho_A = Tr_{Ancilla} \left[|\psi\rangle \langle\psi| \right]$$

■

34 מצב פריק separable

נקרא למצב מצה מכפלה אם הוא מהצורה -

$$\rho_A \otimes \rho_B$$

זה הביטוי הקוונטי למושג ההסתברותי של "אי תלות". נדגים -

$$\begin{aligned} \mathbb{P}(j,k|\rho) &= Tr\left[E_j \otimes E_k \rho\right] = \\ &= Tr_A\left[E_j \rho_A\right] Tr\left[E_k \rho_B\right] = \\ &= \mathbb{P}(j|\rho_A)\,\mathbb{P}(k|\rho_B) \end{aligned}$$

כעת - נרצה לייצר קורלציות בין אליס ובוב - כלומר - ליצור מאורעות תלויים.

$$\mathbb{P}(j,k) = \sum_a p_a P^a(j)\, P^a(k)$$

כאשר p_a ההסתברות "שלי" לבחור התפלגות a. P^a פילוג הסתברות מספר a.
עכשיו ההסתברויות j,k אינן ב"ת, אבל משפט מתורת ההסתברות מבטיח שכל התפלגות ניתן לכתוב בצורה הנ"ל.
ρ נקרא מצב פריק אם -

$$\rho = \sum p_a \rho_A^a \otimes \rho_B^a$$

הפלא של מכניקה קוונטית הוא שיש מצבים שאינם פריקים. מצבים אלו נקראים שזורים.

טענה 34.1 יש מצבים במכניקה קוונטית המקיימים -

$$Tr[\rho] = 1 \quad \rho \geq 0$$

אבל

$$\rho = \sum p_a \rho^a \otimes \rho^a \qquad \rho_a \geq 0$$

הגדרה 34.2 מצב שזור הוא מצב שאינו פריק

34.1 שחלוף חלקי Partial transpose

$$A \to A^t$$

$$A \otimes B \to A \otimes B^t$$

נניח ש־M היא מטריצה 4×4, שחלוף חלקי על בוב יבצע ־

$$\begin{pmatrix} \cdot & \nearrow & \cdot & \nearrow \\ \swarrow & \cdot & \swarrow & \cdot \\ \cdot & \nearrow & \cdot & \nearrow \\ \swarrow & \cdot & \swarrow & \cdot \end{pmatrix}$$

החצים מסמנים חילוף מקומות, בהתאמה, נקודות ־ איברים שנשארים במקומם.
במקרה של שחלוף חלקי על אליס, יתחלפו הבלוקים של 2×2 ־

$$\begin{pmatrix} \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix} & [\nearrow] \\ [\swarrow] & \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix} \end{pmatrix}$$

35 קריטריון פרס לשזירות

אם $\rho \geq 0$, פריק אזי ־ $\rho^{pt} \geq 0$
$\rho = \sum p_a \rho_A^a \otimes \rho_B^a$ אזי
$\rho^{pt} = \sum p_a \rho_A^a \otimes \rho_B^t$
מתקיים כמובן ־ $\rho = \rho^\dagger$ אזי ־ $\rho^t = \left(\rho^\dagger\right)^t = \rho^*$ ו־$\rho_B^a \geq 00$ אזי גם ־

$$(\rho_B^a)^t \geq 0$$

ולכן ־

$$\left\langle \varphi \middle| \rho^t \middle| \varphi \right\rangle = \langle \varphi | \rho^* | \varphi \rangle \geq 0$$

לכן ־

$$\rho^{pt} \geq 0$$

לדוגמא ־
מצב בל ־

$$|\beta\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

לכן ־

$$|\beta\rangle \langle\beta| = \begin{pmatrix} 1 & & & 1 \\ & 0 & 0 & \\ & 0 & 0 & \\ 1 & & & 1 \end{pmatrix}$$

ולכן (לא משנה אם על אליס או בוב) -

$$\left(\left|\beta\right\rangle\left\langle\beta\right|\right)^{pt}=\begin{pmatrix}1 & & & 0\\ & 0 & 1 & \\ & 1 & 0 & \\ 0 & & & 1\end{pmatrix}$$

המטריצה הזו איננה חיובית (יש ע"ע -1 עם הו"ע $\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$).

36 אי שוויונות Bell ומשמעותם

36.1 משתנים נסתרים

פרט למכניקת הקוונטים, בכל תחום אחר בפיזיקה שבה אנו משתמשים בתאור סטטיסטי אנחנו "מודים" שאין לנו רצון או יכולת לתאר את כל פרטי המערכת באופן מלא, ולכן אנחנו מעדיפים תיאור סטטיסטי. הנתונים המלאים קיימים באמת, אנחנו פשוט לא יכולים או רוצים לעבד את כולם. לעומת זאת - במכניקה קוונטית **אין למערכת תכונות לפני המדידה**, והתיאור הסטטיסטי הוא התיאור האמיתי של המערכת. אנחנו לא "לא יכולים" או "לא רוצים" לפרט את המידע המלא, הוא פשוט **לא קיים**.

בעבר חשבנו שייתכן שלמערכות קוונטיות יש "משתנים נסתרים" - "צבע", "טעם", "ריח" וכו'... הם מכריעים את המצב בצורה דטרמיניסטית - אבל אנחנו פשוט לא יודעים למדוד אותם, ולכן נראה לנו שהתיאור הוא סטטיסטי.

בל הראה באופן חד משמעי שאין משתנים נסתרים, והתיאור הסטטיסטי הוא באמת ובתמים נכון!

36.2 $CHSH$

נתבונן במערכת של שני ספינים - אחד אצל אליס ואחד אצל בוב.

אליס יכולה לצע ניסוי שטרן גרלך בכיוון R - ולכן יכולה למדוד ±1. היא יכולה למדוד בכיוון S ולקבל ±1.

באותו האופן בוב יכול למדוד בכיוון P או Q.

נניח שיש מציאות (☺) כלומר -

- אין ערכים רק למה שמדדנו, אלא יש ערכים לכל דבר והמדידה רק חשפה את הערכים הקשורים למה שמדדנו.
- המדידה חושפת את המציאות ולא מקלקלת אותה
- מדידה של אליס לא מקלקלת את המצב של בוב

נגדיר כעת -

$$\beta=S\left(P+Q\right)+R\left(P-Q\right)$$

נשים לב כי -

$$\beta=\pm2$$

ומתקבל -

$$\left\langle\beta\right\rangle=\sum\mathbb{P}\left(p,q,r,s\right)\beta\left(p,q,r,s\right)$$

לכן -

$$\left|\left\langle\beta\right\rangle\right|\leq\sum\mathbb{P}\left(p,q,r,s\right)2$$

לכן -

$$-2 \leq \langle \beta \rangle \leq 2$$

אבל ניתן למדוד במעבדה -

$$\langle \beta \rangle = \langle SP \rangle + \langle SQ \rangle + \langle RP \rangle - \langle RQ \rangle$$

לעומת זאת במכניקה קוונטית, כפי שאנחנו מכירים אותה, יתקיים -

$$-2\sqrt{2} \leq \langle \beta \rangle \leq 2\sqrt{2}$$

ונראה מיד שעבור מצבי בל נקבל - $\langle \beta \rangle = \pm 2\sqrt{2}$.

36.2.1 ניסוח קוונטי (הזהות של צירלסון)

מי המצבים שמפרים את אי שוויון $CHSH$ באופן מקסימלי?

$$B = R \otimes (P + Q) + S \otimes (P - Q)$$

נחפש ρ שיתן ערך תצפית מקסימלי עבור -

$$\langle B \rangle = Tr\left[B\rho\right]$$

למעשה - אנחו מחפשים את הו"ע ρ שמתאים לע"ע הגדול ביותר של B.
ראשית, נמצא את הע"ע של B -
B היא מטריצה 4×4 ומתקיים -

$$R^2 = P^2 = Q^2 = S^2 = \mathbb{1}$$

לכן נתבונן ב-B^2 -

$$\begin{aligned} B^2 &= (P+Q)^2 + (P-Q)^2 + RS \otimes (P+Q)(P-Q) + SR \otimes (P-Q)(P+Q) = \\ &= 4 \cdot \mathbb{1} + RS \otimes [Q,P] + SR \otimes [Q,P] = \\ &= 4 \cdot \mathbb{1} + [R,S] \otimes [Q,P] \end{aligned}$$

וזו נקראת הזהות של צירלסון.
כעת נבחר את מערכות הצירים עבור אליס ובוב.
אצל אליס -

$$\begin{aligned} R &= \hat{Z} \\ S &= \cos\theta_A \hat{Z} + \sin\theta_A \hat{X} \end{aligned}$$

ואצל בוב -

$$\begin{aligned} Q &= \hat{Z} \\ P &= \cos\theta_B \hat{Z} + \sin\theta_B \hat{X} \end{aligned}$$

(אלו מערכות צירים שונות בינתיים)

לכן -

$$[R,S] = 2\sin\theta_A \hat{Y}$$

ובאופן דומה אצל בוב. ובסך הכל (עם זהות צירלסון) קיבלנו -

$$B^2 = 4 - 4\sin\theta_A \sin\theta_B \hat{Y_A} \otimes \hat{Y_B}$$

הע"ע של $\hat{Y_A} \otimes \hat{Y_B}$ הם ± 1לכן הע"ע של B^2 הם -

$$4\left(1 \pm \sin\theta_A \sin\theta_B\right)$$

לכן הע"ע המקסימלי הוא 8 (למשל עבור $+$, ושתי הזויות הן $\frac{\pi}{2}$) ואז הע"ע השני הוא אפס.
במקרה זה הע"ע של B הם -

$$\pm\sqrt{8} = \pm 2\sqrt{2}, \quad 0$$

36.2.2 איך נמצא את המצב האופטימלי, זה שיפר באופן ברור את אי השוויון?

נגדיר φ - הזווית בין צירי Z של אליס ובוב. לכן -

$$\begin{aligned} X_B &= X \\ Z_B &= Z \\ X_A &= -\sin\varphi \hat{Z} + \cos\varphi \hat{X} \\ Z_A &= \cos\varphi \hat{Z} + \sin\varphi \hat{X} \end{aligned}$$

במקרה הזה (כאשר אליס ובוב שניהם מודדים על הצירים שלהם) נקבל -

$$\begin{aligned} B &= \left(\cos\varphi \hat{Z} + \sin\varphi \hat{X}\right) \otimes (Z+X) + \left(-\sin\varphi \hat{Z} + \cos\varphi \hat{X}\right) \otimes (Z-X) = \\ &= (\cos\varphi - \sin\varphi)(Z \otimes Z) + (\sin\varphi - \cos\varphi)(X \otimes X) + (\cos\varphi + \sin\varphi)(Z \otimes X) + (\cos\varphi + \sin\varphi)(X \otimes Z) \end{aligned}$$

כדי לאפס את שני האיברים האחרונים נבחר $\cos\varphi + \sin\varphi = 0$ כלומר $\varphi = -\frac{\pi}{4}$, ואז -

$$\begin{aligned} B &= (\cos\varphi - \sin\varphi)(Z \otimes Z) + (\sin\varphi - \cos\varphi)(X \otimes X) = \\ &= \sqrt{2}(Z \otimes Z) - \sqrt{2}(X \otimes X) \end{aligned}$$

הע"ע של $X \otimes X$ ו-$Z \otimes Z$ הם ± 1 לכן הע"ע הם -

$$0, \ \pm 2\sqrt{2}$$

מי הו"ע המתאים ל-$-2\sqrt{2}$?
זה הוא - $|01\rangle + |10\rangle$. נראה -

$$\begin{aligned} (Z \otimes Z)(|01\rangle + |10\rangle) &= -(|01\rangle + |10\rangle) \\ (X \otimes X)(|01\rangle + |10\rangle) &= (|01\rangle + |10\rangle) \end{aligned}$$

לכן הע"ע של B על המצב הזה הוא -

$$-2\sqrt{2}$$

37 הנסיון של Aspet

38 מודלים למחשב קוונטי

מחשב קלאסי = מכונת טיורינג

יחידת המידע הבסיסית של מחשב קלאסי היא הביט, ופועלים עליו עם שערים לוגיים. די במעט מאד שערים לוגיים (למעשה - אחד, NAND למשל) כדי ליצור "מערכת פעולת שלמה" וממנה ליצור כל שעל לוגי על כל מספר ביטים.

במחשב קוונטי יש לנו כאמור קיוביטים, והפעולות הן טרנספורמציות אוניטריות. נשאלת השאלה - האם ניתן למצא "מערכת פעולות שלמה" דומה?

38.1 קיוביט יחיד

טרנספורמציה אוניטרית כללית על קיוביט בודד היא למעשה סיבוב (על כדור בלוך) סביב ציר כלשהו, בזווית סיבוב כלשהי.

נראה שאפשר לממש כל סיבוב כזה ע"י שער הדמר ו- $\begin{pmatrix} e^{i\varphi} & \\ & e^{-i\varphi} \end{pmatrix}$

38.2 שערים אוניברסליים

נראה שמספיק לבנות שערים מהצורה -

$$\begin{pmatrix} e^{i\phi} & \\ & e^{-i\phi} \end{pmatrix}$$

וכן שער הדמרד -

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

ושער $CNOT$ -

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}$$

כל סיבוב על כדור בלוך מיוצג על ידי סיבובים בזוויות α, β, γ (זוויות אויילר) סיבוב סביב ציר z, אחר כך סביב ציר x ואז סביב z החדש. כיוון שהמשפחה הראשונה שהצגנו יודעת לסובב בכל זווית סביב ציר $\hat{z}$, ושער הדמרד מעביר את ציר z לציר x - למעשה אין לנו בעיה לממש כל סיבוב על כדור בלוך - ולממש כל טרנספורמציה (אוניטרית) על קיוביט בודד.

כעת נראה איך משערים כאלו בונים טרנספורמציה על N קיוביטים. ניקח שער U כלשהו, ונפרק אותו לכל קומבינציה אפשרית של שתי שורות ושתי עמודות, אם נתבונן רק על הערכים בהן - הם נראים כמו מטריצה הפועלת על קיוביט יחיד. נראה דרך ל"משחק" עם $CNOT$ כדי "להחליף" שורות ועמודות במטריצה U כך שלמעה נוכל, באמצעות קומבינציה של פעולותעל קיוביטים בודדים, לבנות את המטריצה U כולה.

השער $CNOT$ מחליף את עמודות או שורות $3, 4$ במטריצה 4×4 (על שני קיוביטים), $CNOT$ "הפוך" -

$$\begin{pmatrix} 1 & & & \\ & 0 & & 1 \\ & & 1 & \\ & 1 & & 0 \end{pmatrix}$$

מחליף בין 2 ו-4.

אם נפעיל $CNOT$, אחריו $CNOT$ הפוך ושוב $CNOT$ ניתן להחליף את שורות (עמודות) $2, 3$, שער זה נקרא שער $swap$, כיוון שהוא מעביר -

$$|a\rangle \otimes |b\rangle \mapsto |b\rangle \otimes |a\rangle$$

על ידי החלפת שורות ועמודות מתאימות ניתן להגיע ל־

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \alpha & -\bar{\beta} \\ & & \beta & \bar{\alpha} \end{pmatrix}$$

ואם נקרא ל־$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$ ־ U אזי קיבלנו ־ $controlled-U$. בדומה ניתן להכליל לכל מספר קיוביטים, וכל מטריצה אוניטרית (זו ממש לא הוכחה, רק הקווים הכלליים).

39 האלגוריתם של שור

39.1 מוטיבציה ־ הצפנת RSA

אלגוריתם RSA הוא אלגוריתם "pubic key", מי שרוצה לקבל מידע מוצפן מפרסם "מפתח ציבורי" הכולל מספר ענק ־ N ומספר ראשוני קטן e. כאשר $N = pq$ כך ש־p, q ראשוניים (שידועים רק למי שפרסם את המפתח).

39.1.1 איך מצפינים?

נניח שרוצים להצפין הודעה, המיודעת ע"י המספר m, אזי שולחים ־

$$c = m^e \pmod N$$

הפענוח נעשה ע"י ־

$$c^d \pmod N$$

כאשר d הוא המספר המקיים ־

$$d \cdot e = 1 \pmod{(p-1)(q-1)}$$

לכן ־ כדי לשבור את ההצפנה צריך למצא p, q כך ש־$N = p \cdot q$. וכפי שאנחנו יודעים (ואם לא ־ יש ויקיפדיה שמסבירה את זה יותר טוב מפיזיקאים :)) זה לא פרקטי.

39.2 לוג מודולרי

39.2.1 מה הבעיה?

איך פותרים, למשל $5^x \equiv 1 \pmod{21}$?
אין ברירה אלא (בקירוב) לעבור על כל הערכים של x עד שמוצאים...

39.2.2 איך פותרים עם מעגל קוונטי?

הגדרה 39.1 נתונים a, N זרים. מחזור של a נקרא המספר r ־

$$a^r \equiv 1 \pmod N$$

המינימלי (הגדול מאפס).

ממשפט פרמה הקטן (משפט אויילר) יש למשוואה פתרון. אם הם לא זרים - קל לראות שאין בהכרח פתרון (למשל $2^x = 1 \ \ (mod\ 6)$).

אין אלגוריתם קלאסי יעיל לחישוב המחזור, אבל אם נתון מחשב קוונטי עם התכונות הבאות אז חישוב המחזור הוא קל. נרצה -

$$U\left|u_s\right\rangle = e^{2\pi\varphi_s}\left|u_s\right\rangle$$

נניח שיש לנו מחשב פאזה, כלומר -

$$\left|0\right\rangle \mapsto \left|\varphi_s\right\rangle$$

(עד כדי שגיאת ייצוג). נכניס וקטור כללי למעגל שמפעיל את מחשב הפאזה (על N הביטים הראשונים) ו-U (על הביטים הבאים) -

$$\left|0\right\rangle\left|\varphi\right\rangle = \left|0\right\rangle\left(\sum\alpha_s\left|u_s\right\rangle\right) \mapsto \sum\alpha_s\left|\varphi_s\right\rangle\left|u_s\right\rangle$$

מה קורה אם מודדים את רגיסטר הפאזה?

$$\mapsto \left|\varphi_i\right\rangle\left|u_i\right\rangle$$

קיבלנו בביטים הראשונים את הפאזה של u_i -

39.3 כדי למצא סדר (מחזור a, N) -

$$\begin{aligned} U_a\left|y\right\rangle &= \left|ya\ mod\left(N\right)\right\rangle \\ \left(U_a\right)^2\left|y\right\rangle &= \left|ya^2\ mod\left(N\right)\right\rangle \\ &\vdots \\ \left(U_a\right)^r\left|y\right\rangle &= \left|y\ mod\left(N\right)\right\rangle \end{aligned}$$

ראינו שבאמצעות מעגל שיודע להגיד מה הפאזה φ של טרנספורמציה אוניטרית -

$$U\left|u\right\rangle = e^{2\pi i\varphi}\left|u\right\rangle$$

ניתן למצא את המחזור של $x^r \equiv 1 \ \ (mod\ n)$ (המחזור הוא r).

39.3.1 למה זה בכלל מעניין?

נסתכל על המשוואה - $x^2 \equiv 1 \ \ (mod\ N)$
יש שני פתרונות טריוויאליים - $x = \pm 1$
נתבונן כעת על -

$$\begin{aligned} x^2 - 1 &\equiv 0 \ \ (mod\ N) \\ \left(x-1\right)\left(x+1\right) &\equiv 0 \ \ (mod\ N) \end{aligned}$$

למשוואה הזו שני פתרונות טריוויאליים - $1, -1$. אבל אז בהכרח מתקיים - $\left(x-1\right)\left(x+1\right)$ מחלק את N, כלומר אם $x \neq 0$ אזי -
$\left(x+1\right) = np$ ו-$\left(x-1\right) = mq$ כאשר $pq = N$. ולמעשה ניתן לחפש $gcd\left(\left(x+1\right), N\right)$ כדי למצא את p, q שיצרו את N.

40 טרנספורם פורייה קלאסי

תזכורת על טרנספורם פורייה קלאסי -
ניקח וקטור מרוכב -

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

כאשר $N = 2^n$. אזי טרנספורם פורייה מוגדר -

$$y_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-ijk\frac{2\pi}{N}} x_k$$

נתבונן על שורשי היחידה מסדר N, נגדיר - $w = e^{-i\frac{2\pi}{N}}$ ואז ניתן לכתוב -

$$y_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N} w^{jk} x_k$$

ונסמן -

$$\vec{y} = \mathcal{FT}\left[\vec{x}\right]$$

נצייר את המטריצה של טרנספורם פורייה -

$$FT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & \dots & w^{N-1} \\ 1 & w^2 & w^4 & \dots & w^{2N-2} \\ 1 & w^3 & w^6 & \dots & w^{3N-3} \\ \vdots & & & & \\ 1 & w^{N-1} & & \dots & w^{N^2-2N+1} \end{pmatrix}$$

נשים לב ששורות ועמודות מנורמלות ל־1. כמו כן השורות מאונכות (מכפלת זוג שורות יתנו את כל שורשי היחידה, וסכומם הוא אפס). לכן - FT אוניטרית. ומתקיים -

$$FT^{-1} = FT^T$$

אבל נקבל למעשה -

$$FT^{-1} = FT^*$$

למטריצה הזו יש 4 ע"ע - $\pm 1, \pm i$. **הוכחה:** נתבונן על $\left((FT)^2 \vec{x}\right)_j$ -

$$\begin{aligned} \left((FT)^2 \vec{x}\right)_j &= \frac{1}{\sqrt{N}} \sum_k w^{jk} \left(FT\left(X\right)\right)_k = \\ &= \frac{1}{\sqrt{N}} \sum_k w^{jk} \frac{1}{\sqrt{N}} \sum_l w^{kl} x_l = \\ &= \frac{1}{N} \sum_l \sum_k w^{k(l+j)} x_l \end{aligned}$$

אנחנו מסכמים על כל שורשי היחידה, אלא אם כן $l + j = N$ כלומר נשאר רק עם העיבר המתאים ל־$l = N - j$ -

$$= \frac{1}{N} \sum_k x_{N-j} = x_{N-j}$$

כלומר טרנספורם פורייה בריבוע הוא שיקוף! ולכן הע"ע שלו הם ± 1ולכן הע"ע של טרנספורם פורייה הם $\pm 1, \pm i$. ■

40.1 טרנספורם פורייה טוב לזיהוי מחזור!

למשל, $x_j = (-1)^j$ כלומר -

$$\vec{x} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ \vdots \\ -1 \end{pmatrix}$$

לאחר טרנספורם פורייה -

$$y_j = \frac{1}{\sqrt{N}} \sum_k w^{jk} (-1)^k$$

נשים לב שכיוון ש- $N = 2^n$ הוא בהכרח זוגי, ואז -

$$w^{\frac{N}{2}} = e^{-\frac{2\pi i N}{2N}} = -1$$

ולכן -

$$y_j = \frac{1}{\sqrt{N}} \sum_k w^{jk} w^{k\frac{N}{2}} = \frac{1}{\sqrt{N}} \sum_k w^{k(j+\frac{N}{2})}$$

וכיוון שזה סכום על שורשי היחידה, הסכום יתאפס אלא אם כן $j + \frac{N}{2} = N$. כלומר -

$$y_j = \begin{cases} \sqrt{N} & j = \frac{N}{2} \\ 0 & j \neq \frac{N}{2} \end{cases}$$

41 טרנספורם פורייה קוונטי

הגדרה 41.1 בסיס החישובי - $|j\rangle_{j=0,\ldots N-1}$ כך ש-

$$\begin{aligned} |0\rangle &= |000\ldots0\rangle \\ |1\rangle &= |000\ldots1\rangle \\ |2\rangle &= |00\ldots10\rangle \\ &\vdots \\ |N-1\rangle &= |111\ldots1\rangle \end{aligned}$$

זה הוא בסיס למרחב הילברט של n קיוביטים.

באנלוגיה למה שראינו קודם לכן, טרנספורם פורייה קוונטי מוגדר על אברי הבסיס החישובי -

$$FT\,|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk}\,|k\rangle$$

לדוגמא -

עבור קיוביט בודד, $N = 2$, $n = 1$ אז - $w = -1$ ונקבל -

$$\begin{aligned} FT\,|0\rangle &= \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] = |+\rangle \\ FT\,|1\rangle &= \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right] = |-\rangle \end{aligned}$$

כלומר 0 במקרה הזה QFT (על קיוביט בודד) הוא שער הדמרד.

41.1 במקרה הכללי -

$$
\begin{aligned}
|0\rangle \mapsto \frac{1}{\sqrt{N}} \sum_k |k\rangle &= H^{\otimes n} |0\rangle \\
|1\rangle \mapsto \frac{1}{\sqrt{N}} \sum_k w^k |k\rangle &= \frac{1}{\sqrt{N}} \prod_{j=0}^{n-1} \left(|0\rangle + w^{2^j} |1\rangle \right) \\
&\vdots \\
|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_k w^{jk} |k\rangle &= \frac{1}{\sqrt{N}} \prod_{l=0}^{n-1} \left(|0\rangle + w^{j \cdot 2^l} |1\rangle \right)
\end{aligned}
$$

כעת, איך ניתן לתרגם אם הנוסחא הנ"ל למעגל קוונטי?

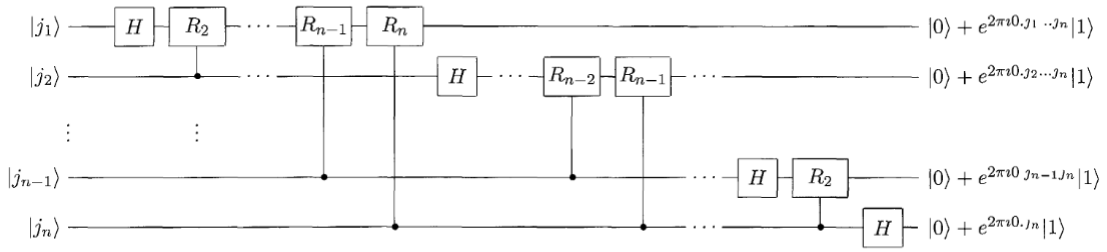


Figure 5.1. Efficient circuit for the quantum Fourier transform. This circuit is easily derived from the product representation (5.4) for the quantum Fourier transform. Not shown are swap gates at the end of the circuit which reverse the order of the qubits, or normalization factors of $1/\sqrt{2}$ in the output.

$$
R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}.
$$

כאשר -

42 הערכת פאזה

כעת אפשר לבנות את המכונה המופלאה שמבצעת את הערכת הפאזה. למעשה אנחנו מעוניינים ב־

$$
e^{2\pi i \varphi} = e^{2\pi i \frac{M}{N}} = w^{-M}
$$

כלומר - למצא את φ עד לדיוק שמתאפשר ב־n ביטים, כלומר מספר $\frac{M}{N}$ כאשר $0 \leq M \leq 2^n = N$.

42.1 טרנספורם פורייה

נתבונן בוקטורים באורך נתון $N = 2^n$, נסמן $\omega = \frac{2\pi i}{N}$

$$
FT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \\ \vdots & \omega^2 & \ddots & \\ 1 & & & \end{pmatrix}
$$

$$U|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{jk} |k\rangle$$

דוגמה - $N = 2$

$$FT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

דוגמה - $N = 4$

$$FT = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$|00\rangle \to (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$|01\rangle \to (|0\rangle - |1\rangle)(|0\rangle + i|1\rangle)$$

$$|10\rangle \to (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$|11\rangle \to (|0\rangle - |1\rangle)(|0\rangle - i|1\rangle)$$

נסתכל על הביט הימני בכניסה ועל הביט השמאלי ביציאה. אם נקרא את הביטים ביציאה בכיוון ההפוך נקבל שעל ה־lsb פועל H. נסתכל על הביט השמאלי בכניסה והימני ביציאה. נקבל כי פועל הדמר ופאזה מבוקרת

$$C_i = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \pm i \end{pmatrix}$$

נכליל להרבה קיוביטים

$$|j\rangle \to \left(|0\rangle + \omega^{2^{n-1}j}|1\rangle\right) \cdots \left(|0\rangle + \omega^{2j}|1\rangle\right)\left(|0\rangle + \omega^{j}|1\rangle\right)$$

הערה 42.1 נשים לב כי $\langle k|j = \delta_{jk}$. אנו מתחילים ממצבים אורתוגונליים, טרנספורם פורייה הוא אופרטור אוניטרי, כלומר המצבים נשארים אורתוגונליים. נתון $|0\rangle + \omega^j|1\rangle$, מצב אורתוגונלי $|0\rangle + \omega^{N/2-j}|1\rangle = |0\rangle - \omega^j|1\rangle$. עבור שני קיוביטים

43 האלגוריתם של שור

- פירוק מספר ל־pq למציאת המחזור של $x^r = 1 \bmod N$
- מציאת מחזור

מעוניינים במעגל שמודד פאזה. התמרת פורייה הפוכה.
האלגוריתם של שור בונה על התופעה הקוונטית של התאבכות בונה

44 אלגוריתם החיפוש של גרובר

נניח שנתון לנו ספר טלפונים, אנו מעוניינים לחפש את הטלפון של עודד קנת. יש לנו N אובייקטים, אפשר למצוא שם ב־$\log N$ בחיפוש בינארי. לעומת זאת, אם נקבל מספר טלפון, יהיה לנו מאוד קשה למצוא למי הוא שייך (יערה - אפשר להתקשר ולבדוק). נרצה לפתור את הבעיה של חיפוש במערך לא מסודר.
נניח כי $x \in \{0,\dots,N-1\}$. נגדיר פונקציה $f(x)$ המקיימת $f(x)=1$ אם x פתרון, 0 אחרת

$$|x\rangle|a\rangle \to |x\rangle|a \oplus f(x)\rangle$$

נבחר $|a\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. אם x פתרון

$$|x\rangle|-\rangle \to |x\rangle(|1\rangle - |0\rangle)$$

אם x לא פתרון

$$|x\rangle|-\rangle \to |x\rangle(|0\rangle - |1\rangle)$$

אם כן

$$|x\rangle|-\rangle \to (-1)^{f(x)}|x\rangle|-\rangle$$

נראה כי ניתן לחפש ב־$\sqrt{N}$ שאילתות לידיעוני (oracle) נניח לשם פשטות כי קיים x יחיד עבורו $f(x)=1$, $|x\rangle \to |\alpha\rangle$.
ניתן להזין למכשיר

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle$$

אנו יודעים ליצור מצב כזה ע"י הפעלת H על מצב התחלתי $|0\rangle$ של הרבה קיוביטים. נשים לב כי

$$\langle\alpha|\psi\rangle = \frac{1}{\sqrt{N}}$$

כלומר $|\alpha\rangle, |\psi\rangle$ כמעט מאונכים. נרצה להגדיל את האמפליטודה. מצב מאונך ל־$|\alpha\rangle$ הוא $|\beta\rangle = \frac{1}{\sqrt{N-1}}\sum_{j\neq x}|j\rangle$. מה עושה תשאול של הידעוני?

$$|\alpha\rangle \mapsto -|\alpha\rangle$$

$$|\beta\rangle \mapsto |\beta\rangle$$

$$G = 1 - 2|\alpha\rangle\langle\alpha|$$

$$G|\alpha\rangle = -|\alpha\rangle$$

$$G|\beta\rangle = |\beta\rangle$$

אם כן, תשאול משקף סביב המישור המאונך ל־$|\alpha\rangle$. נרצה לשחק עם שיקופים. נגדיר שיקוף נוסף

$$J = 1 - 2|\psi\rangle\langle\psi|$$

הם מקיימים $J^2 = 1,\ G^2 = 1$. מה עושה פעולת JG? מכפלה של שני שיקופים היא סיבוב. נניח שיש לנו שני וקטורים, $|\alpha\rangle,\ |\psi\rangle$ שהזווית ביניהם היא θ. נקבל כי JG סיבוב בזווית $\pi - 2\theta$ (נשים לב שכאן $\theta \approx \frac{\pi}{2}$, לכן הסיבוב הוא בזווית קטנה).

הראנו עבור דו מימד אבל בעצם כל מה שמשנה הוא המרחב שנפרש ע"י $|\psi\rangle$, $|\alpha\rangle$. מכפלת השיקופים נותנת סיבוב קטן בזווית $\frac{2}{\sqrt{N}}$ בקירוב (למעשה, $\sin\left(\frac{2}{\sqrt{N}}\right)=\sin\left(2^{-\frac{n}{2}+1}\right)$)

$$\begin{aligned}\cos(\theta) &= \frac{1}{\sqrt{N}}\\ \sin\left(\frac{\pi}{2}-\theta\right) &= \frac{1}{\sqrt{N}}\\ \frac{\pi}{2}-\theta &\approx \frac{1}{\sqrt{N}}\\ \pi-2\theta &\approx \frac{2}{\sqrt{N}}\\ \theta &\approx \frac{\pi}{2}-\frac{2}{\sqrt{N}}\end{aligned}$$

כאמור, אנחנו מעוניינים בסיבוב בן $\frac{1}{\sqrt{N}}-\frac{\pi}{2}$ רדיאנים. וכל סיבוב הוא ב־$\frac{2}{\sqrt{N}}$ רדיאנים. לכן בסך הכל דרושים לנו $\frac{\pi\sqrt{N}}{4}-1$ סיבובים כדי נקבל מצב שכמעט מזדהה עם המצב המבוקש $|x\rangle$ ומדידה שלו תתן את המצב הזה בהסתברות גבוהה מאד (למעשה, ככל ש־N גדול יותר כך ההסתברות גדולה יותר!) קיבלנו כי גם אם ספר הטלפונים לא ממויין ניתן למצא את הטלפון המבוקש ב־$O\left(\sqrt{N}\right)$ פעולות, במקום ב־N פעולות במקרה הסטנדרטי.

45 האלגוריתם של גרובר, חזרה

האלגוריתם של גרובר מאפשר חיפוש במסד נתונים לא ממויין (או - לא מסודר). באופן קלאסי - אין אפשרות לחפש בצורה יעילה יותר מ־$O(N)$. לעומת זאת, ניתן לבצע חיפוש קוונטי (בהסתברות גבוהה כרצוננו) ב־$O\left(\sqrt{N}\right)$.

האלגוריתם מתבסס על $oracle$ ("נביא") שמבצע היפוך של הפאזה עבור הפתרון ה"נכון" ולא מבצע כלום עבור פתרונות "שגויים". כלומר, אם $|x\rangle$ הוא הפתרון המבוקש, האורקל U יפעל באופן הבא -

$$\begin{aligned}U|x\rangle &= -|x\rangle\\ U|y\rangle &= |y\rangle \quad \forall y\neq x\end{aligned}$$

האלגוריתם יוצר את המצב $|\psi\rangle$ שהוא סופרפוזיציה של כל המצבים האפשריים -

$$|\psi\rangle=\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle$$

אם נסמן כעת את הפתרון ב־$|\alpha\rangle$ ואת המצב המאונך לו ב־

$$|\beta\rangle=\frac{1}{\sqrt{N-1}}\sum_{i\neq\alpha}|i\rangle$$

וניתן לכתוב -

$$|\psi\rangle=\frac{1}{\sqrt{N}}|\alpha\rangle+\sqrt{1-\frac{1}{N}}|\beta\rangle$$

ולכן -

$$\langle\alpha\,|\,\psi\rangle=\frac{1}{\sqrt{N}}$$

ולכן, ההסתברות שנקבל את α כאשר נמדוד את $|\psi\rangle$ היא -

$$|\langle\alpha\,|\,\psi\rangle|^2$$

נשים לב שסיבוב הוא תוצאה של שני שיקופים. כאשר משקפים דרך שני וקטורים $\vec{a},\vec{b}$ כאשר הזווית בינהם היא θ מקבלים סיבוב בזווית 2θ. בפרט אצלנו משקפים סביב $|\alpha\rangle$ ו־$|\psi\rangle$, ולכן זווית הסיבוב המתקבלת היא $\frac{2}{\sqrt{N}}$.

45.1 מה קורה כאשר ישנם m פתרונות?

הניתוח דומה מאד. ההבדל המרכזי הוא ש־

$$\cos\theta = \langle\alpha\,|\,\psi\rangle = \sqrt{\frac{m}{N}}$$

ולכן (אם ידוע לנו m) ניתן למצא מהר יותר פתרון ראשון. או בזמן דומה ($O\left(\sqrt{N}\right)$) את כל הפתרונות.

46 חלוקת מפתח קוונטי QKD

הצפנה קלאסית "מושלמת" אפשרית בעזרת פנקס חד פעמי. אבל, להצפנה כזו חסרונות רבים. בין היתר ־

- המפתח צריך להקבע מראש
- השימוש במפתח הוא חד פעמי! [4]
- יש צורך במפתח ארוך

אליס ובוב רוצים להעביר בינהם הודעה באופן בטוח, מבלי לקבוע מפתח מראש, כאשר איב מאזינה על הקו. מה ניתן לעשות (קוונטית) כדי לסייע לאליס ובוב?

ראשית, נשים לב שבעוד קלאסית איב יכולה לייצר עותק של התשדורת ולפענח אותה מאוחר יותר בבית, קוונטית זה לא אפשרי אלא אם כן היא יודעת באיזה בסיס מועבר המידע (ראינו בתחילת הסמסטר את עקרון no cloning). שנית, אם איב תנסה להקשיב לתשדורת ולהוסיף לה anncillas משלה, היא "תקלקל" את התקשורת. כלומר ־ היא לא יכולה להאזין לתקשורת מבלי לקלקל, אם היא מאזינה היא בהכרח משפיעה על התקשורת.

46.1 פרוטוקול $BB84$

אליס יוצרת שתי סדרות אקראיות של ביטים, a,b (אלו סדרות קלאסיות) ־

a	0	1	1	0	1	0	...	1
b	1	0	0	0	1	0	...	0

כעת היא מגדירה שני בסיסים. בסיס Z המכיל את $|0\rangle,|1\rangle$ ובסיס X המכיל את $|+\rangle,|-\rangle$.

היא שולחת לבוב את a כאשר כל ביט i מקודד באחד מהבסיסים, X אם $b[i]$ הוא 0 או Z אם $b[i]$ הוא 1.

כעת בוב מגריל סדרה אקראית b' (שוב, קלאסית, אפסים ואחדים). על פי הסדרה b' הוא מחליט איך למדוד את הקיוביטים של אליס (על פי אותו עקרון) אך בהתאם לסדרה b' שלו. יש לו עכשיו סדרה חדשה a'.

אחרי שבוצעה המדידה בוב ואליס יכולים לפרסם את הבסיסים (b,b') ולראות על אילו ביטים הם הסכימו. הביטים המתאימים ב־a,a' (סטטיסטית, מחצית מהביטים) בהכרח זהים אצל שניהם, ויכולים לשמש כמפתח לצורך הצפנת הודעות עתידיות. איב לא יכלה לשמור את התשדורת או למדוד אותה, ולכן כעת כשהמפתחות גלויים היא לא יכולה לדעת מה היה השדר המקורי, ולכן לא יכולה לדעת מה הוא המפתח שבו ישתמשו אליס ובוב להעברת ההודעה הבאה.

46.2 פרוטוקול $B92$

לא ילמד הסמסטר. דומה, אבל יותר מסובך, משתמש רק ב־$|1\rangle$ ו־$|+\rangle$

[4] אחרת, המאזין יכול לבצע xor בין שתי ההודעות, ולקבל את $m_1 \oplus m_2$, כעת יש לו די הרבה מידע.

47 נושאים נוספים, שלא נספיק לכסות

- תיקון שגיאות קוונטי. מחשבים דיגיטליים עובדים במרחב בדיד, שבו ניתן לתקן שגיאות בצורות רבות. לעומת זאת במחשבים אנלוגיים (לו היו קיימים) תיקון שגיאות הוא מסובך יותר (ואולי אך בלתי אפשרי במתארים מסויימים). במחשבים קוונטיים קיימים אלגוריתמים לזיהוי ותיקון שגיאות.
- דיברנו על מחשבים קוונטיים דרך מעגלים, קיימות גישות אחרות
- לא דיברנו על אופטיקה קוונטית, בוזונים פרמיונים וכו'...