חישוב קוונטי

רקע

הברה לא באמת צריך לדעת את הפיסיקה של תורת הקוונטים כדי לדעת לתכנן אלגוריתמים קוונטיסת באותה מידה שלא היינו צריכים ידע באלקטרוניקה של של מחשב קלאסי כדי לתכנן אלגוריתמים עד כה.

ניסוי שני הסדקים

אם נזרוק אבל לבריכה היא תכרום לגל שינוע ממקום הפגיע במים לכל הכיוונים. אם נחסום את גל המים בקיר עם סדק הגל יעצר למעט הסדק מעבר לקיר ינויע גל שתחילתו בסדק. אם המים, לצורך הניסוי, יכתימו את צד הבריכה, נקבל שם כתם מקביל למקום הסדק שככל שנתרחק ממנו הצבע יחלש. אם בקיר יהיו שני סדקים ולא רק אחד, יווצרו מעבר לקיר שני גלים שיתנגשו. שני גלים שמתנגשים יכולים או להתווסף זה לזה או לבטל זה את זה (תלוי במצב של כל אחד, לא קריטי) ולכן נקבל בצד הבריכה לא כתם שהולך ודוהה בקצוות כמקודם אלא תבנית מתחזקת ונחלשת לכל האורך (אם כי גם כאן הצבע יהיה יותר מודגש במרכז).

כמובן שתופעה זו נובעת מהאופי הגלי של תנועת המים. אם היינו מנסים את אותו ניסוי עם חפץ חלקיקי כלשהו (כלומר עשוי חלקיקים, נניח, אבן) החלקיקים, אלה שהיו מצליחים לעבור את הסדק, היו ממשיכים ישירות וצובעים נקודה ותו לא.

בתחילת המאה ה19 בוצע ניסוי שכזה עם אור, במטרה לקבוע אם האור הוא גל או חלקיק, התוצאה היית שהאור התנהג כמו המים ממקודם, כלומר כמו גל. מאוחר יותר התברר שיש לאור גם מאפיינים חלקיקיים והוא מורכב מחלקיקים ששמם "פוטונים", האור, איכשהו, הוא גם גל וגם חלקיק.

בתחילת המאה ה20 ניסו לבצע את הניסוי עם אלקטרונים. למרבה ההפתעה גם האלקטרונים התנהגו כמו גלים ויצרו תבנית גלית על המסך שמאחורי הסדקים.

אז הוחלט לעשות את הניסוי מעט אחרת - במקום לירות כל פעם שני חלקיקים (פוטונים במקרה הזה) אחד לכל סדק, הפעם ירו חלקיק אחד בלבד לכיוון שני הסדקים באופן כזה שיש לו אפשרות לעבור בכל סדק (כתלות ב"ספין" מאפיין כלשהו של פוטונים. הספין לא ידוע במהלך הניסוי). על המסך התקבלה תבנית מתחלפת כאילו ירינו לשני הסדקים בו זמנית. במובן מסוים התברר שהפוטון הבודד "הפריע לעצמו".

תורת הקוונטים סיפקה את ההסבר לתופעה - אין מיקום מוגדר לפוטון (וכן לגבי עוד כמה מאפיינים) אלא מעין התפלגות מיקום במרחב, רק כאשר אנו מנסים למדוד את המיקום ההתפלגות "קורסת" לערך מוגדר, כאילו יש משתנה אקראי שמגדיר את המיקום וניסיון למדוד אותו גורם לו להדגם ולעשות למוחלט. עקרון זה נקרא **עקרון הסופרפוזיציה**[1].

לענייננו

הגדרה: קיוביט (qubit - quantum bit) יחידת זכרון שיכולה להיות במצב קלאסי (כלומר $\{0,1\}$ כמו שראינו עד כה) שאותם נסמן ב־ $|0\rangle, |1\rangle$ או בסופרפוזיציה כלומר

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

[1] להמחשה של הנסוי `http://goo.gl/A5Cje0`

לכל $\alpha_0, \alpha_1 \in \mathbb{C}$ כך ש $|\alpha_0|^2 + |\alpha_1|^2 = 1$

כלומר מצבו של קיוביט שנמצא בסופרפוזיציה הוא משהו שמזכיר הפתלגות אלא שהפעם יש ל"הסתברות" כיוון.

אם מודדים קיוביט, כלומר נבדוק באיזה מצב הוא ובכך נכפה עליו מצב קלאסי, המצב של הקיוביט יהפוך ל $|0\rangle$ או $|1\rangle$ כאשר

$$Pr\left[we\ got\ |0\rangle\right] = |\alpha_0|^2, \qquad Pr\left[we\ got\ |1\rangle\right] = |\alpha_1|^2$$

פעולות על קיוביטים

אנו לא מאפשרים כל פעולה על קיוביט.

פעולה חייבת להיות לינארית. נחשוב על $|0\rangle, |1\rangle$ כבסיס של מרחב וקטורי כלומר

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

ולפי ההגדרות נקבל שסופרפוזיציה היא צירוף לינארי של אברי הבסיס

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

ומאחר ו

$$\left\| \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \right\| = |\alpha_0|^2 + |\alpha_1|^2 = 1$$

הוקטור המייצב את הסופרפוזיציה $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ הוא וקטור יחידה.

מלינארית נובע שפעולה U על קיוביט יחיד $q = \alpha_0|0\rangle + \alpha_1|1\rangle$ כלשהו ניתנת להגדרה כמטריצה $U \in \mathbb{C}^{2\times 2}$ שפעולתה מוגדרת על אברי הבסיס

$$U(|0\rangle) \longmapsto s_0 \in \mathbb{C}^2 \ U(|1\rangle)) \longmapsto s_1 \in \mathbb{C}^2$$

ומכאן ש

$$U(q) = U(\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0 s_0 + \alpha_1 s_1$$

כדי לשמור על עקביות ההגדרה נרצה שתוצאת פעולה תהיה תמיד סופרפוזיציה תקינה של מצבים קלאסים. כלומר שיתקיים

$$\forall v \in \mathbb{C}^2: \ \|v\| = 1 \Rightarrow \|U(v)\| = 1$$

כלומר U מעבירה וקטורי יחידה לוקטורי יחידה, או במילים אחרות, U לא מכווצת ולא מעוות אלא היא מריצת שיקוף ו/או סיבוב. מריצה כזאת, כפי שלמדנו כקורס באלגברה נקראית מטריצה אוניטרית המוגדרת באופן פורמלי

$$U \cdot U^* = 1$$

כאשר $U* = \overline{U^T}$ הוא הצמוד המרוכב (אחרי שעשינו traspose) של U

הגדרה: צירוף של כמה קיוביטים

n קיוביטים יכולים להיות בסופרפוזיציה משותפת שמוגדרת כ

$$\sum_{b_1...b_n\in\{0,1\}^n} \alpha_{b_1...b_n}|b_1...b_n\rangle\rangle$$

כך ש

$$\sum_{b_1...b_n} |\alpha_{b_1...b_n}|^2 = 1$$

הבהרה - $b_1...b_n$ היא מחרוזת של אפסים ואחדות.

במילים - סופרפוזיציה של כמה קיוביטים היא צירוף לינארי של מצבים קלאסים, אלא שבמקום שני מצבים קלאסים בלבד $\langle|0\rangle, |1\rangle\rangle$ יש לנו 2^n מצבים קלאסים $\langle|0...0\rangle, |0...01\rangle, ...|1...1\rangle$.

דוגמה: בשני קיוביטים נקבל את המצבים הקלאסים $\langle|00\rangle, |01\rangle, |10\rangle, |11\rangle$ וסופרפוזיציה של שני קיוביטים תהיה

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

כך ש

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

גם כאן ניתן להתייחס לייצוג כמרחב וקטורי 2^n מימדי והסופר פוזיציה הזאת, של שני קיוביטים תיוצג כ

$$\begin{pmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{pmatrix} \in \mathbb{C}^4$$

כך ש

$$\left\|\begin{pmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{pmatrix}\right\| = 1$$

הגדרה: אוסף של קיוביטים יכולים להיות במצב **שזור** (כלומר, יש מעין תלות בין המצבים שלהם, יוסבר בהמשך) או במצב לא שזור ואז ניתן לפרק את הסופרפוזיציה ל**מכפלה טנזורית** כלומר למכפלה הבאה[2]

$$q_1\otimes...\otimes q_n = \left(\alpha_0^1|0\rangle + \alpha_1^1|1\rangle\right)\otimes...\otimes(\alpha_0^n|0\rangle + \alpha_1^n|1\rangle) = \sum_{b_1...b_n}\left(\prod_{k=1}^n \alpha_{b_k}^k\right)|b_1...b_n\rangle$$

[2]בדומה לפירוק של הסתברות על משתנים בלתי תלויים למכפלת הסתברויות

כלומר במכפלה טנזורית אנחנו סוכמים על כל האינדקסים $b_1 ... b_n$ (מחרוזות מאורך n של אפסים ואחדות) ולכל אינקדס שכזה המקדם של המצב הקלאסי בעל האינקדס יהיה המכפלה של המקדמים המתאימים בכל קיוביטץ לדוגמה עבור 3 קיוביטים ועבור אינדקס $b_1 b_2 b_3 = 001$ המקדם של $|001\rangle$ יהיה

$$\prod_{k=1}^{3} \alpha_{b_k}^{k} = \alpha_0^0 \alpha_0^1 \alpha_1^2$$

אם, לעומת זאת $q_1, ..., q_n$ היו שזורים לא היינו יכולים לבטא את הסופרפוזיציה (את הצירוף הלינארי) בתור מכפלה טנזורית באופן הזה.

דוגמה:

$$\alpha_0^1 \alpha_0^2 |00\rangle + \alpha_0^1 \alpha_1^2 |01\rangle + \alpha_1^1 \alpha_0^2 |10\rangle + \alpha_1^1 \alpha_1^2 |11\rangle = \left(\alpha_0^1 |0\rangle + \alpha_1^1 |1\rangle\right) \otimes \left(\alpha_0^2 |0\rangle + \alpha_1^2 |1\rangle\right)$$

ולכן המצבים לא שזורים.

מדידה חלקית

אם נבצע מדידה של k קיוביטים הראשונים בסופרפוזיציה אזי לכל תוצאת מדידה אפשרית $a_1 ... a_k \in \{0,1\}^k$ (במדידה נקבל תמיד מצבים קלאסים)

$$Pr\left[{}^{the\ measurement}_{will\ return\ a_1 ... a_k}\right] = \sum_{b_{k+1} ... b_n} |a_1 ... a_k b_{k+1} ... b_n|^2$$

כלומר הסיכוי לקבל תוצאה חלקית מסוימת שווה לסכום ה"גדלים" של תוצאות המדידה (של כל הקיוביטים) האפשרויות ש"מסכימות" עם התוצאה החלקית.

נכנה הסתברות זו $P_{a_1 ... a_k}$

לאחר מדידה חלקית אם קיבלנו $a_1 ... a_k$ אזי שאר $n-k$ הקיוביטים נמצאים עדיין בסופרפוזיציה שנובעת מהסופרפוזיציה שהיית כאשר k הקיוביטים הראשונים כבר לא חלק ממנה אלא הם כבר "נקבעו" כלומר

$$\sum_{b_{k+1} ... b_n} \frac{\alpha_{a_1 ... a_k b_{k+1} ... b_n}}{\sqrt{P_{a_1 ... a_k}}} |b_{k+1} ... b_n\rangle$$

כלומר המקדם של המצבים הקלאסים (הצירוף הלינארי כולל רק את האינדקסים שלא נמדדו) הוא סכום של המקדמים האפשריים בהינתן ש $\alpha_0 = a_0, ..., \alpha_k = a_k$. חילקנו ב $\sqrt{P_{a_1 ... a_k}}$ כדי לנרמל את המקדמים באופן כזה שנשאר עם קואורדינאטות שסכומם 1 כך שהסופרפוזיציה תקינה.

הערה: מדידה חלקית מזכירה קצת הסתברות מותנית - מה ההתפלגות בהינתן שחלק מהמשתנים הם נקבעו.

דוגמה: שני קיוביטים עם סופרפוזיציה משותפת [3]

$$\frac{-i}{\sqrt{2}} |00\rangle + 0 |01\rangle - \frac{1}{\sqrt{6}} |10\rangle + \frac{i}{\sqrt{3}} |11\rangle$$

[3] את המחובר השני רשמנו רק למען הבהירות, סתם כך לא צריך לרשום מחוברים שהמקדם שלהם הוא 0

נמדוד את הקיוביט הראשון בלבד

$$Pr\left[q_1=1\right]=Pr\left[q_1q_2=1q_2\right]=\left|\alpha_{10}\right|^2+\left|\alpha_{11}\right|^2=\left|-\frac{1}{\sqrt{6}}\right|^2+\left|\frac{i}{\sqrt{3}}\right|^2=\frac{1}{6}+\frac{1}{3}=\frac{1}{2}$$

ומכך נובע שבמקרה המשלים [4]

$$Pr\left[q_1=0\right]=Pr\left[q_1q_2=0q\right]=\frac{1}{2}$$

לאחר המדידה:

- אם קיבלנו 0 - מאחר והמקדם של $|01\rangle$ הוא 0 הרי שההקיוביט השני חייב להיות [5]

$$\frac{\alpha_{00}}{\sqrt{P_0}}|0\rangle=\frac{\frac{-i}{\sqrt{2}}}{\sqrt{\frac{1}{2}}}|0\rangle=-i|0\rangle$$

- אם קיבלנו 1 - אזי הקיוביט השני יהיה

$$P_1=\frac{1}{2}\Rightarrow\frac{1}{\sqrt{P_1}}=\sqrt{2}\Rightarrow\sqrt{2}\left(\alpha_{10}|0\rangle+\alpha_{11}|1\rangle\right)=-\frac{1}{\sqrt{3}}|0\rangle+\sqrt{\frac{2}{3}}|1\rangle$$

ניסוי/פרדוקס $EPR - Einstein\ Podolsky\ Rosen$

בשנת 1935 הציעו אלברט איינשטיין, בוריס פודולסקי ונייתן רוזן ניסוי מחשבתי במטרה להדגים את הבעייתיות של תורת הקוואנטים.

נניח שיש בידינו שני קיוביטים $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$ (שאר המקדמים הם 0 ולכן לא טרחנו לרשום אותם). אם נעשה את החישוב כמו שעשינו מקודם (לא נתעכב על זה) נגלה שהם מתואמים לחלוטין, במובן שאם נמדוד קיוביט אחד הקיוביט השני בהכרח מקבל את אותו הערך. נניח שהפרדנו את הקיוביטים (בלי לפגוע בסופר פוזיציה המשותפת, זה אפשרי מבחינה פיזיקלית, לא משנה לנו איך) וכעת אנסטסיה מחזיקה בקיוביט הראשון ובוריס בשני.

שניהם מתפצלים כך שמהרחק ביניהם גדול, נניח בוריס טס למאדים. שניהם, בתיאום מראש, מודדים את הקיוביט שיש בידיהם באותו הזמן.

באופן "פלאי" שניהם יקבלו את אותה התוצאה. הבעיה היא שעל פניו, בשביל תוצאה מתואמת איזשהי אינפורמציה היית צריכה לעבור מאחד מהם לשני, אבל אם כך הרי שהמעבר הזה היה מהיר מאוד - מרחק גדול כרצוננו בשבריר שניה, מה שסותר את תורת היחסות שטוענת שאין אפשרות לעבור את מהירות האור.

תוספת העשרה: איינשטיין התנגד נחרצות לפרשנות המקובלת לתוצאות של תורת הקוונטים (ובראשה מה שמכונה "אסכולת קופנהגן") שהסבירה שאין מאפיינים מוגדרים אלא

[4] גם אותו ניתן, כמובן, לחשב אך במקרה הזה אין צורך
[5] למעשה, במצב שהתקבל ברור שמדידת הקיוביט השני תחזיר 0

סופרפוזיציה[6]. לטענת איינשטיין הפיזיקה מתנהגת באופן מוגדר ולכן הוא סבר שיש "משתנים חבויים" כלומר ישנם משתנים נוספים, שאנו לא יודעים עליהם עדיין, שנקבעים בשלב מוקדם יותר בניסוי והם קובעים, מראש את תוצאתו. ניסוי EPR (כמו גם הניסוי המחשבתי המפורסם על החתול של שרדינגר) בא להראות שהפרשנות הרווחת של תורת הקוונטים בעייתית. לצערו של איינשטיין, ניסויים רבים, ביניהם מימוש של הניסוי שהוא עצמו הגה, הראו שוב ושוב שדווקא פרשנות קופנהגן תואמת את הנתונים ושלא יתכן להניח את קיומם של משתנים חבויים[7].

שער הדמר ($Hadamard$)

רכיב לוגי, בדומה לשערי NOT, AND וכד' במחשב קלאסי, שמבצע את הפעולה הבאה:

$$H\left(|0\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H\left(|1\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

בבסיס שלנו (שמוגדר על ידי המצבים הקלאסים) $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \ |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ ולכן בכתיב מטריציוני הפעולה תוגדר כ

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

כלומר עבור קיוביט כלשהו $\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}$ הפעלת שער הדמר על הקיוביט היא למעשה הכפלה שלו במטריצה H כלומר $H \cdot \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}$

פעולה חוקית על k קיוביטים

פעולה על k קיוביטים היא בעצם פעולה לינארית ואוניטרית מעל מרחב ממימד 2^k היא תפעל על וקטורים מהסוג

$$\begin{pmatrix}\alpha_{0\ldots0}\\ \cdot\\ \cdot\\ \cdot\\ \alpha_{1\ldots1}\end{pmatrix} = \sum_{j_1\ldots j_k\in\{0,1\}} \alpha_{j_1\ldots j_k}|j_1\ldots j_k\rangle$$

[6] או בניסוחו המפורסם מתוך מכתב לחבר "מכניקת הקוונטים בהחלט מרשימה. אך קול פנימי אומר לי שהיא עדיין איננה הדבר האמיתי. התאוריה אומרת הרבה, אך לא באמת מקרבת אותנו במאומה לסודו של "הזקן" [אלוקים]. **אני, איך שלא יהיה, משוכנע שהוא אינו מטיל קוביות**"

[7] או כמו שהגיב הפיזיקאי נילס בוהר בתגובה לאימרה של איינשטיין "תפסיק לומר לאלוקים מה לעשות עם הקוביות שלו!" וכמו שהוסיף עשרות שנים אחר כך סטיבן הוקינג "לא זו בלבד שאלוקים משחק בקוביות הוא גם לפעמים זורק אותם למקומות בהם לא ניתן לראות אותם".

ואם כבר אז אצטט גם את הסופר טרי פראצ'ט ז"ל "אלוקים לא משחק בקובייה עם היקום: הוא משחק משחק בלתי ברור שהוא המציא, שאפשר להשוות, מנקודת המבט של שאר השחקנים (כלומר: כולם), לגרסה של משחק פוקר מבולבל, מוזר בחדר חשוך לחלוטין עם קלפים ריקים על סכומים אינסופיים, עם מחלק שלא אומר לך את החוקים ומחייך כל הזמן!"

נזכור שכאשר יש לנו אוסף של k קיוביטים אנו מתייחסים אל הבסיס המורכב מהמצבים הקלאסים $|0...0\rangle, |0...01\rangle ..., |1...1\rangle$ וכל סופרפוזיציה היא צירוף לינארי של אברי הבסיס. נשים לב, בסכום כאן האינדקס רץ מ$0...0$ עד $1...1$.

דוגמה: שער $CNOT - Controlled\ NOT$

השער מקבל 2 קיוביטים q_1, q_2 והופך את q_2 אמ"ם $q_1 = |1\rangle$

נשים לב שאנו צריכים רק לתאר מה הפעולה עושה למצבים הקלאסים. במקרה של סופרפוזיציה תוצאת הפעולה תתקבל מהלינאריות של הפעולה ומכך שהסופרפוזיציה היא למעשה צירוף לינארי של הבסיס.

$$CNOT\left(|0q_2\rangle\right) = |0q_2\rangle,\ CNOT\left(|1q_2\rangle\right) = |0\left(1-q_2\right)\rangle$$

ובכתיב מטריציוני

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

אפשר להגיע למטריצה על ידי כך שעבור כל וקטור בסיס e_i נשאל מה קורה כשמפעילים את הפעולה עליו ואת התשובה נכתוב בטור הi. לדוגמה עבור

$$e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle \Rightarrow q_1 = 1 \Rightarrow CNOT\left(e_3\right) = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

ולכן בטור השלישי במטריצה כתבנו $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

פעולה חלקית

מה קורה כשמפעילים פעולה על k קיוביטים מתוך n?

$$\sum_{j_1...j_n \in \{0,1\}} \alpha_{j_1...j_n} |j_1...j_n\rangle \longmapsto \sum_{j_1...j_n \in \{0,1\}} \alpha_{j_1...j_n} U\left(|j_1...j_k\rangle\right) \otimes |j_{k+1}...j_n\rangle$$

כלומר נניח ויש לנו שלושה קיוביטים בסופרפוזיציה

$$q_1q_2q_3 = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$

$$+\alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

ונפעיל שער $CNOT$ על שני הקיוביטים הראשונים q_1q_2 (כלומר אם $q_1 = 1$ נהפוך את q_2) כל שנעשה הוא להפעיל את הפעולה על המצבים הקלאסים וההשלכה על הסופרפוזיציה תנבע מהלינאריות. כלומר נקבל

$$CNOT\left(q_1q_2\right)q_3 = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$

$$+\alpha_{100}|110\rangle + \alpha_{101}|111\rangle + \alpha_{110}|100\rangle + \alpha_{111}|101\rangle$$

$$= \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$

$$+\alpha_{110}|100\rangle + \alpha_{111}|101\rangle + \alpha_{100}|110\rangle + \alpha_{101}|111\rangle$$

דוגמה: נתחיל משני קיוביטים במצב הקלאסי $q_1, q_2 = |00\rangle$

נפעיל שער H על q_1 נקבל

$$H(q_1) \otimes q_2 = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

עכשיו נעפיל שער $CNOT$ על שני הקיוביטים

$$\frac{1}{\sqrt{2}}CNOT(|00\rangle) + \frac{1}{\sqrt{2}}CNOT(|10\rangle) = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

וקבילנו את הקיוביטים שהיינו צריכים לצורך ניסוי EPR

חשוב לשים לב שהתחלנו מקיוביטים במצב קלאסי (וכמובן לא שזור) וסיימנו עם סופרפוזיציה של קיוביטים שזורים.

איך אנו יודעים שהם שזורים?

1. לפי תוצאות מדידה - אם נמדוד קיוביט אחד זה ישפיע על המצב של הקיוביט השני.
2. אם הם לא היו שזורים היה היינו יכולים לבטא את הסופרפוזיציה כמכפלה טנזורית כלומר

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

וזה לא אפשרי (אם ננס הלפתוח את המכפלה ולהשוות מקדמים נקבל מערכת משוואת ב4 נעלמים שאין לה פתרון)

טלפוטציה קוונטית

לאנסטסיה יש קיוביט $q_1 - 1$ בסופרפוזיציה $\alpha_0|0\rangle + \alpha_1|1\rangle$ לא ידועה. היא רוצה לשלוח את הקיוביט לבוריס (ליתר דיוק היא רוצה להביא למצב שלבוריס יהיה העתק זהה של הקיוביט הזה).

הבנה: אנסטסיה ובוריס מייצרים זוג קיוביטים כמו בניסוי EPR $q_2q_3 = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

המצב המשותף (אם מסופים את הקיוביט q_1 של אנסטסיה ומסתכלים על שלושתם כעל סופרפוזיציה משותפת)

$$(q_1q_2q_3) = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$