

משפט אי השכפול

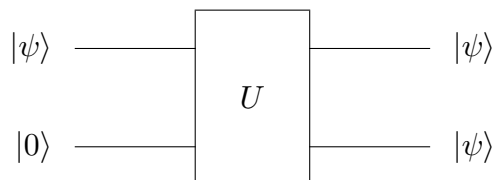
משפט אי השכפול, או בשמו באנגלית No-cloning theorem, קובע כי אין פעולה פיזיקלית היכולה לשכפל באופן מושלם מצב קוונטי לא ידוע. המשפט הוכח על ידי Wootters and Zurek במאמר שפורסם בכתב העת Nature בשנת 1982, ובמקביל על ידי Dieks. מעניין לציין שכבר בשנת 1970 הראה Park ניסוח שקול של התוצאה.

1 מה פירוש לשכפל מצב קוונטי?

דרך אחת לנסח את המשפט בהקשר של קיוביטים היא שלא קיים אופרטור אוניטרי U על זוג קיוביטים, המקיים לכל מצב $|\psi\rangle$ את השוויון

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle.$$

כלומר, הקיוביט הראשון מכיל את המצב שנרצה לשכפל, והקיוביט השני מאותחל לאפס. ביציאה נרצה לקבל שני עותקים של המצב המקורי:

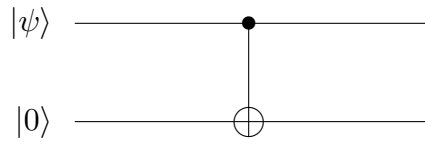


האופרטור U צריך להיות קבוע: אותו אופרטור נדרש לשכפל כל מצב אפשרי. בהמשך נרחיב את הניסוח ונאפשר גם קיוביטי עזר.

2 מדוע שער ההיפוך המבוקר אינו משכפל?

מה רע בשער CNOT? הרי הוא משכפל את שני מצבי הבסיס החישובי:

$$\begin{aligned} \text{CNOT}(|0\rangle \otimes |0\rangle) &= |0\rangle \otimes |0\rangle, \\ \text{CNOT}(|1\rangle \otimes |0\rangle) &= |1\rangle \otimes |1\rangle. \end{aligned}$$



אולם פעולתו על סופרפוזיציה נקבעת על ידי לינאריות. למשל,

$$\begin{aligned} \text{CNOT}(|+\rangle \otimes |0\rangle) &= \text{CNOT}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) \\ &= \frac{1}{\sqrt{2}}(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

זהו מצב בל, והוא שונה מהמצב שרצינו לקבל:

$$|+\rangle \otimes |+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

באופן כללי, אם

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

אז

$$\text{CNOT}(|\psi\rangle \otimes |0\rangle) = \alpha|00\rangle + \beta|11\rangle = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix},$$

בעוד שאנחנו רוצים ביציאה את המצב

$$\begin{aligned} |\psi\rangle \otimes |\psi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \\ &= \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}. \end{aligned}$$

3 מדוע זו עדיין אינה הוכחה?

החישוב האחרון כבר נראה כמו הוכחה: האופרטור U אמור להיות לינארי בקלט, ואילו בביטוי הרצוי מופיעים ריבועים ומכפלות של האמפליטודות. יש שתי בעיות בטיעון הזה.

ראשית, עצם הופעתם של פולינומים ממעלה גבוהה אינה מוכיחה שההעתקה אינה לינארית על קבוצת הקלטים המותרת. למשל, נסתכל לרגע רק על אמפליטודות ממשיות α, β המקיימות $\alpha^2 + \beta^2 = 1$. אז ההעתקה

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha^3 + \alpha\beta^2 \\ \alpha^2\beta + \beta^3 \end{pmatrix}$$

היא למעשה העתקת הזהות על וקטורי היחידה, שכן

$$\begin{pmatrix} \alpha^3 + \alpha\beta^2 \\ \alpha^2\beta + \beta^3 \end{pmatrix} = (\alpha^2 + \beta^2) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

כלומר, ייתכן שלאותה העתקה יהיה ייצוג לינארי וגם ייצוג באמצעות פולינומים ממעלה גבוהה.

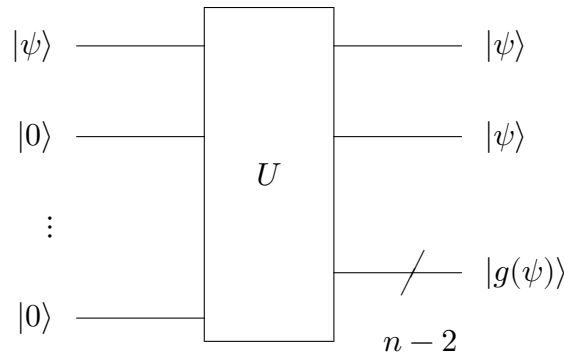
שנית, גם אילו הוכחנו שלא ניתן לשכפל בעזרת קיוביט נוסף יחיד, עדיין היה עלינו לשלול את האפשרות לעשות זאת בעזרת קיוביטי עזר נוספים. קיוביטי עזר המאותחלים לאפס ומשמשים אותנו במהלך החישוב נקראים אנצילות (ancillas). מקור המילה בלטינית, ומשמעותה משרתת או בת לוויה.

4 הניסוח הכללי: גם קיוביטי עזר אינם עוזרים

מה שבאמת נרצה להוכיח, ונציג לכך שתי הוכחות, הוא שלא קיים אופרטור אוניטרי U על מערכת בת $n \geq 2$ קיוביטים, המקיים לכל מצב של קיוביט יחיד $|\psi\rangle$ את השוויון

$$U(|\psi\rangle \otimes |0\rangle^{\otimes(n-1)}) = |\psi\rangle \otimes |\psi\rangle \otimes |g(\psi)\rangle.$$

כאן $|g(\psi)\rangle$ הוא מצב מנורמל של יתר $n - 2$ הקיוביטים. מצב זה עשוי להיות תלוי בקלט; נכנה אותו "זבל" חישובי, garbage. איננו דורשים להחזיר את קיוביטי העזר לאפס.



לפני ההוכחות, מדוע דרשנו שהזבל יהיה במכפלה טנזורית עם שני העותקים? את התשובה המלאה נוכל לנסח בהמשך באמצעות מצבים מעורבים, אך כבר עכשיו כדאי להבין את העיקרון. אנחנו רוצים שכל עותק יהיה בפני עצמו במצב הטהור $|\psi\rangle$. אילו העותקים היו שזורים עם יתר המערכת, לא היה אפשר לתאר אותם כך בנפרד ממנה. בפרט, מדידה של הזבל הייתה עלולה לשנות את מצבם המותנה בתוצאת המדידה. עותק צריך להיות שימושי בפני עצמו, בלי שנצטרך לשמור בסביבה גם את כל קיוביטי העזר.

4.1 הוכחה ראשונה: לינאריות

נניח בשלילה שקיים אופרטור U כזה. נפעיל אותו על שלושת המצבים $|+\rangle, |1\rangle, |0\rangle$. מתכונת השכפול נקבל

$$\begin{aligned} U(|0\rangle \otimes |0\rangle^{\otimes(n-1)}) &= |00\rangle \otimes |g(0)\rangle, \\ U(|1\rangle \otimes |0\rangle^{\otimes(n-1)}) &= |11\rangle \otimes |g(1)\rangle. \end{aligned}$$

לכן, מלינאריות,

$$U(|+\rangle \otimes |0\rangle^{\otimes(n-1)}) = \frac{1}{\sqrt{2}}(|00\rangle \otimes |g(0)\rangle + |11\rangle \otimes |g(1)\rangle).$$

מצד שני, מתכונת השכפול מחייבת

$$\begin{aligned} U(|+\rangle \otimes |0\rangle^{\otimes(n-1)}) &= |+\rangle \otimes |+\rangle \otimes |g(+)\rangle \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |g(+)\rangle. \end{aligned}$$

שני הביטויים אינם יכולים להיות שווים: בביטוי הראשון אין רכיב שבו שני הקיוביטים הראשונים הם במצב $|01\rangle$, ובביטוי השני יש רכיב כזה. באופן פורמלי, נפעיל על שני האגפים את האופרטור $I \otimes |01\rangle\langle 01|$ ונקבל

$$0 = \frac{1}{2} |g(+)\rangle.$$

□

זו סתירה לכך שהווקטור $|g(+)\rangle$ מנורמל.

4.2 הוכחה שנייה: שימור מכפלות פנימיות

יהיו $|\psi\rangle$ ו- $|\phi\rangle$ שני מצבים לא אורתוגונליים, שאינם זהים עד כדי פאזה גלובלית. כלומר,

$$0 < |\langle\psi|\phi\rangle| < 1.$$

נניח בשלילה שאותו אופרטור אוניטרי U משכפל את שניהם. מכיוון שאופרטור אוניטרי משמר מכפלות פנימיות,

$$\begin{aligned}\langle\psi|\phi\rangle &= \langle U(|\psi\rangle \otimes |0\rangle^{\otimes(n-1)}), U(|\phi\rangle \otimes |0\rangle^{\otimes(n-1)}) \rangle \\ &= \langle |\psi\rangle \otimes |\psi\rangle \otimes |g(\psi)\rangle, |\phi\rangle \otimes |\phi\rangle \otimes |g(\phi)\rangle \rangle \\ &= \langle\psi|\phi\rangle^2 \langle g(\psi)|g(\phi)\rangle.\end{aligned}$$

ניקח ערכים מוחלטים ונקבל

$$|\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2 |\langle g(\psi)|g(\phi)\rangle|.$$

המכפלה הפנימית של שני המצבים אינה אפס, ולכן אפשר לחלק ולקבל

$$1 = |\langle\psi|\phi\rangle| |\langle g(\psi)|g(\phi)\rangle|.$$

אבל שני מצבי הזבל מנורמלים, ולכן לפי אי-שוויון קושי-שוורץ,

$$|\langle g(\psi)|g(\phi)\rangle| \leq 1.$$

□

הגורם הראשון קטן ממש מאחת, ולכן גם המכפלה קטנה ממש מאחת. קיבלנו סתירה.

ההוכחה הזו מראה מעט יותר: אי אפשר לשכפל באופן מושלם אפילו שני מצבים נתונים, אם הם אינם אורתוגונליים ואינם מתארים את אותו מצב פיזיקלי. אין בכך סתירה לכך ששער CNOT משכפל את מצבי הבסיס החישובי, שכן אלה אורתוגונליים.

5 הקשר ללמידה

משפט אי השכפול קשור קשר ישיר למגבלות על היכולת "ללמוד" מצב קוונטי לא ידוע. אילו יכולנו לשכפל אותו, היינו יכולים לייצר עותקים רבים, לבצע על העותקים מדידות ולאסוף סטטיסטיקות, וכך לקבל הערכה הולכת ומשתפרת של המצב. כדי ללמוד גם את הפאזות היחסיות, ולא רק את ערכי המוחלט של האמפליטודות, יש לבצע מדידות בבסיסים שונים.

מצד שני, אילו יכולנו ללמוד באופן מושלם את המצב מתוך עותק יחיד, היינו יכולים להשתמש בתיאור שהתקבל כדי להכין עותקים נוספים שלו. הרי אין מניעה להכין קיוביט במצב ידוע; הקושי הוא לשכפל מצב שאינו ידוע לנו.