עיקרון דחיית המדידה

1 האם חייבים למדוד באמצע?

ביחידה הקודמת הגדרנו מעגל קוונטי כרצף של שערים יוניטריים, שבסופו מודדים ומקבלים פלט קלאסי. אבל לכאורה זו הגבלה משמעותית. אולי כדאי למדוד קיוביט באמצע החישוב, ובהתאם לתוצאה להחליט איזה שער להפעיל בהמשך?

עיקרון דחיית המדידה אומר שאפשר לדמות גם חישוב כזה, בלי למדוד ממש עד הרגע האחרון. לשם כך נוסיף קיוביטי עזר ונחליף החלטות המבוססות על תוצאות מדידה בשערים מבוקרים. התפלגות הפלט תישאר אותה התפלגות.

חשוב לשים לב: לא מדובר פשוט בהזזת סימני המדידה ימינה בתרשים. נצטרך לשנות גם את המעגל, ויש לזה מחיר קל מבחינת גודל המעגל ומספר קיוביטי האנסילה.

2 דוגמה ראשונה

נניח שיש לנו שני קיוביטים במצב

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

נמדוד את הקיוביט הראשון בבסיס הסטנדרטי. אם נקבל אפס, לא נעשה דבר; אם נקבל אחד, נפעיל שער יוניטרי U על הקיוביט השני.

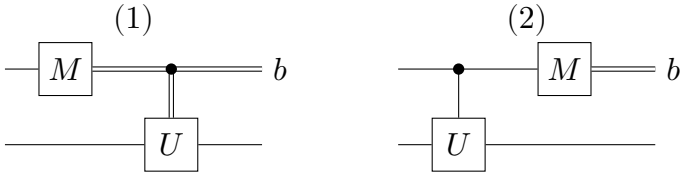
כלומר, בהסתברות $|\alpha|^2$ נקבל את התוצאה אפס והקיוביט השני יישאר במצב $|\psi\rangle$; ובהסתברות $|\beta|^2$ נקבל את התוצאה אחד והקיוביט השני יהיה במצב $U|\psi\rangle$.

כעת נבצע פעולה אחרת: במקום למדוד, נפעיל שער U מבוקר, כשהקיוביט הראשון הוא קיוביט הבקרה. נקבל

$$\alpha|0\rangle|\psi\rangle + \beta|1\rangle U|\psi\rangle.$$

רק עכשיו נמדוד את הקיוביט הראשון.

נשווה את שני המעגלים. כזכור, קוראים כל מעגל משמאל לימין. קו יחיד מייצג קיוביט, וקו כפול מייצג ביט קלאסי. התיבה M מציינת מדידה בבסיס הסטנדרטי, ואת תוצאתה נסמן ב־ b.



במעגל (1) הקו האנכי כפול: בזמן הפעלת השער כבר יש בידינו תוצאת מדידה, ואנו מפעילים את U אם ורק אם $b = 1$. במעגל (2) הקו האנכי יחיד: הקיוביט הראשון עצמו משמש כבקרה, ורק לאחר הפעלת השער המבוקר מודדים אותו ומקבלים את b.

בשני המעגלים נקבל בדיוק אותן הסתברויות לתוצאות המדידה, ובהינתן תוצאת המדידה, גם מצבו של הקיוביט השני יהיה זהה בשניהם. מה אִפשר לנו לדחות את המדידה כאן? גם במעגל המקורי, כל מה שהיינו צריכים לדעת על תוצאת המדידה בשלב הזה הוא אם להפעיל את U על הקיוביט השני. הקיוביט הראשון יכול לשמש בעצמו כבקרה, בלי שנצטרך לקרוא את ערכו. למעשה, אם גם שערים נוספים בהמשך החישוב תלויים באותה תוצאה, נוכל להשתמש בו כבקרה גם עבורם.

אבל מה אם נרצה להמשיך לחשב גם על הקיוביט הראשון? נניח, למשל, שבמעגל המקורי אנחנו שומרים את תוצאת המדידה b לשימוש בהמשך, ואז מפעילים על הקיוביט שנמדד את השער H. כעת לא יספיק לדחות את המדידה: אם נמדוד את הקיוביט רק אחרי הפעלת H, לא נוכל להסיק מתוצאת המדידה מה היה ערכו של b. לכן נפריד בין שני התפקידים: נשתמש בקיוביט עזר כדי לשמור את תוצאת המדידה העתידית, וכך נוכל להמשיך לחשב על הקיוביט הראשון בלי לאבד את המידע הדרוש לבקרה.

תרגיל 2.1. נתחיל בשני קיוביטים במצב $|+\rangle \otimes |0\rangle$. נמדוד את הקיוביט הראשון בבסיס הסטנדרטי, נשמור את התוצאה b, ואז נפעיל על אותו קיוביט את השער H. לבסוף, אם $b = 1$, נפעיל X על הקיוביט השני. מהי ההסתברות לקבל אחד כשמודדים את הקיוביט השני בבסיס הסטנדרטי?

כעת ננסה לדחות את המדידה בלי להוסיף קיוביט עזר: נפעיל תחילה H על הקיוביט הראשון, ואחר כך נשתמש בו כבקרה בשער CNOT שהקיוביט השני הוא קיוביט המטרה שלו. מהי כעת ההסתברות לקבל אחד במדידת הקיוביט השני? הסבירו מדוע הקיוביט הראשון כבר אינו יכול למלא את תפקידו של הביט השמור b.

3 שומרים את התוצאה בלי למדוד

נסמן את הקיוביט שאותו רוצים למדוד ב־ A, ואת שאר המערכת ב־ R. המצב המשותף שלהם ניתן לכתיבה בצורה

$$|\Psi\rangle_{AR} = |0\rangle_A |\phi_0\rangle_R + |1\rangle_A |\phi_1\rangle_R .$$

כאן הווקטורים $|\phi_0\rangle$ ו־ $|\phi_1\rangle$ אינם בהכרח מנורמלים, וגם אינם בהכרח אורתוגונליים. מתקיים

$$\|\phi_0\|^2 + \|\phi_1\|^2 = 1.$$

הכתיבה הזו כוללת גם את המקרה שבו A שזור עם שאר המערכת.

אם נמדוד את A, נקבל תוצאה $b \in \{0,1\}$ בהסתברות

$$p_b = \|\phi_b\|^2.$$

בהינתן תוצאה שהסתברותה חיובית, המצב לאחר המדידה יהיה

$$\frac{|b\rangle_A |\phi_b\rangle_R}{\sqrt{p_b}}.$$

במקום למדוד, נוסיף קיוביט חדש B במצב $|0\rangle$, ונפעיל CNOT מ־ A אל B. בסדר האוגרים A, R, B, נקבל

$$|0\rangle_A |\phi_0\rangle_R |0\rangle_B + |1\rangle_A |\phi_1\rangle_R |1\rangle_B .$$

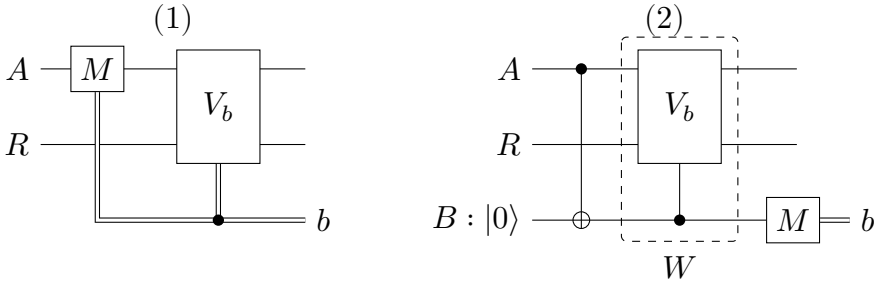
הקיוביט B ישמש כזיכרון לתוצאה. לא מדדנו אותו, ובדרך כלל הוא שזור עם שאר המערכת. ובכל זאת, אם נמדוד אותו בבסיס הסטנדרטי, נקבל בדיוק את התוצאה ואת המצב המותנה שהיינו מקבלים במדידה המקורית.

כעת נניח שאחרי המדידה המקורית התכוונו להפעיל V_b על המערכת AR, בהתאם לתוצאה b. שימו לב שהפעולה הזו יכולה לפעול גם על הקיוביט A עצמו.

במעגל החדש נפעיל את הפעולה המבוקרת

$$W = V_0 \otimes |0\rangle\langle 0|_B + V_1 \otimes |1\rangle\langle 1|_B .$$

נשווה את שני המעגלים. בשניהם הקלט הוא אותו מצב משותף של A, R, והוא עשוי להיות שזור.



במעגל (1) המדידה של A נותנת ביט קלאסי b, הקובע אם להפעיל על A, R את V_0 או את V_1. שימו לב לחוט העליון: הקיוביט שנמדד ממשיך בחישוב, במצבו שלאחר המדידה.

במעגל (2) מוסיפים קיוביט עזר B ומפעילים CNOT מ־ A אל B. המסגרת המקווקוות מסמנת את הפעולה W על שלושת האוגרים: בכל רכיב שבו B נמצא במצב $|b\rangle$, מופעלת על A, R הפעולה V_b, ואוגר הבקרה B נשאר במצב $|b\rangle$. זו פעולה יוניטרית: בכל אחד משני תתי־המרחבים האורתוגונליים שמוגדרים על ידי B מופעלת פעולה יוניטרית.

המצב שיתקבל הוא

$$\sum_{b\in\{0,1\}} V_b(|b\rangle_A |\phi_b\rangle_R) \otimes |b\rangle_B .$$

נמדוד כעת את B. מכיוון ש־ V_b שומר נורמות, ההסתברות לקבל b היא עדיין p_b. בהינתן התוצאה הזו, מצב המערכת האחרת הוא

$$\frac{V_b(|b\rangle_A |\phi_b\rangle_R)}{\sqrt{p_b}}.$$

זהו בדיוק המצב שמתקבל בתהליך המקורי: קודם מדידה, ואחריה הפעולה המתאימה לתוצאה.

לכן מתקבלת אותה התפלגות משותפת של תוצאת המדידה ושל כל פלט שנפיק בהמשך מהמערכת.

4 העיקרון הכללי

משפט 4.1 (עיקרון דחיית המדידה)**.** *לכל מעגל קוונטי הכולל מדידות בבסיס הסטנדרטי ופעולות המותנות בתוצאותיהן, קיים מעגל עם קיוביטי עזר שבו כל המדידות מתבצעות בסוף, והתפלגות הפלט הקלאסי שלו זהה לזו של המעגל המקורי.*

אפשר לשמר גם את ההתפלגות המשותפת של כל תוצאות המדידות המקוריות ושל הפלט.

הבנייה חוזרת על אותו רעיון בכל מדידת ביניים:

1. מוסיפים קיוביט עזר חדש במצב $|0\rangle$, ובמקום למדוד מפעילים אליו שער CNOT מהקיוביט שאותו רצינו למדוד.
2. בכל מקום שבו השתמשנו בתוצאת המדידה כביט בקרה קלאסי, משתמשים כעת בקיוביט העזר כבקרה קוונטית.
3. שומרים את קיוביט העזר עד סוף החישוב, ומודדים אותו רק אז בבסיס הסטנדרטי.

מדוע צריך קיוביט חדש בכל פעם? כי תוצאת המדידה הישנה היא חלק מההיסטוריה של החישוב. גם אם בתוכנית הקלאסית היינו דורסים אותה, בסימולציה נשמור אותה באוגר נפרד.

מה קורה אם הבחירה אם להפעיל שער תלויה בכמה תוצאות מדידה? נניח, למשל, שבמעגל המקורי מפעילים את השער U אם ורק אם שתי תוצאות המדידה b_1, b_2 שונות זו מזו.

במעגל שבו דחינו את המדידות, נוסיף קיוביט עזר במצב $|0\rangle$. נפעיל אליו שני שערי CNOT, אחד מכל אחד משני אוגרי התוצאות. כך נממש את הפעולה

$$|b_1\rangle |b_2\rangle |0\rangle \longmapsto |b_1\rangle |b_2\rangle |b_1 \oplus b_2\rangle .$$

כעת נשתמש בקיוביט העזר כבקרה להפעלת U. מליניאריות, גם כאשר אוגרי התוצאות נמצאים בסופרפוזיציה, השער מופעל בדיוק ברכיבים שבהם שתי התוצאות שונות. לא היינו צריכים למדוד אף אחד מהאוגרים כדי לעשות זאת.

אותו רעיון עובד לכל תנאי בוליאני על תוצאות המדידה: כפי שראינו ביחידה הקודמת, אפשר לחשב את ערך התנאי באופן הפיך לתוך קיוביט עזר, ואז להשתמש בו כבקרה.

כך, בכל שלב, לכל היסטוריית תוצאות יש רכיב נפרד בסופרפוזיציה. אוגרי התוצאות שומרים היסטוריות שונות במצבי בסיס אורתוגונליים. מדידה שלהם בסוף בוחרת היסטוריה בדיוק בהסתברות שבה הייתה מתקבלת בתהליך המקורי.

כאשר מספר צעדי החישוב חסום פולינומית וגם העיבוד הקלאסי של התוצאות יעיל, הבנייה כרוכה בתקורה פולינומית. כרגיל, בשימוש באוסף שערים אוניברסלי קבוע, ייתכן שנצטרך לקרב את השערים המבוקרים; אפשר לבחור את דיוק הקירוב כך שהשגיאה הכוללת תהיה קטנה כרצוננו.

ומה לגבי בסיס אחר? נניח שרוצים למדוד קיוביט בבסיס אורתונורמלי $\{|v_0\rangle, |v_1\rangle\}$. נבחר שער יוניטרי T המקיים

$$T|v_b\rangle = |b\rangle .$$

נפעיל את T, נעתיק את ערך הבסיס לקיוביט עזר בעזרת CNOT, ואז נפעיל $T^\dagger$ על הקיוביט המקורי.

כך מתקבלת הפעולה

$$|v_b\rangle_A |0\rangle_B \longmapsto |v_b\rangle_A |b\rangle_B .$$

לכן אותו טיעון עובד גם למדידה בבסיס הזה. החזרה באמצעות $T^\dagger$ מבטיחה שגם המצב שנותר בקיוביט המקורי מתאים למדידה שרצינו לדמות.