עיקרון דחיית המדידה

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 לבצע אף מדידה 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 ולהוסיף קיוביטי עזר. נראה כיצד מחליפים מדידת ביניים אחת, ואחר כך נחזור על אותה בנייה לאורך החישוב.

1 שומרים את התוצאה בלי למדוד

לפני שנכתוב את הבנייה, נחשוב מה עלינו לשמר. אחרי מדידה יש בידינו גם קיוביט במצבו שלאחר המדידה וגם ביט קלאסי המתאר את התוצאה. אפשר להמשיך לחשב על הקיוביט, ובמקביל להשתמש בביט כדי להחליט אילו שערים להפעיל. למשל, גם אם נפעיל על הקיוביט שנמדד את השער H, תוצאת המדידה ששמרנו עדיין זמינה לנו.

כדי לדמות את שני התפקידים האלה בלי למדוד, נפריד ביניהם: נוסיף קיוביט עזר שישמש כזיכרון לתוצאה, ונשתמש בו כבקרה לפעולות הבאות. כך נוכל להמשיך לחשב על הקיוביט המקורי בלי לאבד את המידע הדרוש לבקרה. הזיכרון הזה יישאר קוונטי עד סוף החישוב; לא נצטרך לקרוא את ערכו כדי להשתמש בו.

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 בבסיס הסטנדרטי, 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 את אותן הסתברויות לתוצאות, ובהינתן כל תוצאה נקבל על AR את אותו מצב מותנה כמו במדידה המקורית.

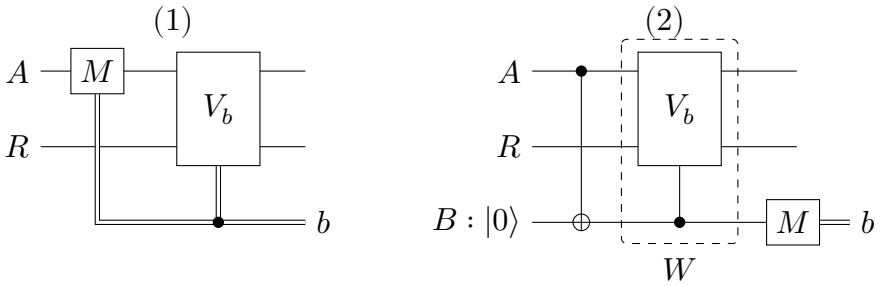
כעת ננית שאחרי המדידה המקורית התכוונו להפעיל פעולה יוניטרית V_b על המערכת AR, בהתאם לתוצאה b. שימו לב שהפעולה הזו יכולה לפעול גם על הקיוביט A עצמו.

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. קוראים כל מעגל משמאל לימין. קו יחיד מייצג מערכת קוונטית, וקו כפול מייצג ביט קלאסי. התיבה M מציינת מדידה בבסיס הסטנדרטי.

כיצד ביט קלאסי משתלב במעגל קוונטי? התרשים מתאר גם את המערכת הקוונטית וגם את הבקרה הקלאסית עליה: מכשיר המדידה מחזיר תוצאה $b \in \{0, 1\}$, שנשמרת בזיכרון קלאסי ומשמשת לבחירת הפעולה הבאה. הקו הכפול מתאר את העברת המידע הזה; למשל, אם התקבל אפס מפעילים את V_0, ואם התקבל אחד מפעילים את V_1. אפשר לייצג את הביט השמור גם באמצעות קיוביט: בהינתן שתוצאת המדידה היא b, קיוביט הזיכרון נמצא במצב הבסיס $|b\rangle$. אבל חשוב להבחין בין תוצאה קלאסית אקראית שכבר התקבלה לבין סופרפוזיציה קוונטית: חוסר הידיעה מראש אם נקבל אפס או אחד אינו אומר שהביט הקלאסי נמצא בסופרפוזיציה. לעומת זאת, במעגל שבו דחינו את המדידה, קיוביט העזר B עדיין עשוי להיות שזור עם שאר המערכת, ומשמש לבקרה בלי שקראנו ממנו תוצאה. לכן הוא מסומן בקו יחיד עד למדידה שבסוף.



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.

כאן חשוב להבחין בין הקיוביט המקורי לבין קיוביט הזיכרון. מותר להמשיך להפעיל שערים על A, כפי שמאפשרת הפעולה V_b. לעומת זאת, את B נשמור עד סוף החישוב, ונשתמש בו רק כבקרה שאינה משנה את ערך הבסיס שלו. כך המידע על התוצאה נשמר גם אם מצבו של A משתנה. התרגיל הבא ממחיש מדוע אי אפשר פשוט לוותר על הזיכרון הזה.

תרגיל 1.1. 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.

2 העיקרון הכללי

משפט 2.1 (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.

הוכחה. בסעיף הקודם ראינו כיצד לדחות מדידה אחת, גם כאשר ממשיכים לחשב על הקיוביט שנמדד. כדי להוכיח את המשפט נחזור על הבנייה בכל מדידת ביניים, ונסביר כיצד לטפל גם בפעולות התלויות בכמה תוצאות קודמות.

החלפת המדידות ושמירת התוצאות. בכל מדידת ביניים נבצע את ההחלפה הבאה:

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.

החלפת העיבוד הקלאסי בבקרה קוונטית. נותר לפרט כיצד מחליפים החלטה התלויה בכמה תוצאות מדידה, ולא רק בתוצאה אחת. 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.

את אוגרי העזר של החישוב ההפיך אפשר לשמור עד סוף החישוב גם כן. ערכיהם נקבעים על ידי תוצאות המדידות השמורות, ולכן הם אינם משנים את ההסתברויות שנקבל.

מדוע התפלגות הפלט נשמרת? נעקוב אחר הבנייה לפי סדר הפעולות במעגל המקורי. בכל שלב, לכל היסטוריה של תוצאות מדידה יש רכיב בסופרפוזיציה, שמסומן על ידי אותה היסטוריה באוגרי התוצאות. ריבוע הנורמה של הרכיב הוא ההסתברות להיסטוריה הזו בתהליך המקורי, עבור היסטוריה שהסתברותה חיובית, המצב המנורמל של מערכת החישוב ברכיב הזה הוא המצב המותנה באותה היסטוריה.

בתחילת החישוב הטענה נכונה, שכן עדיין אין תוצאות מדידה. פעולה המבוקרת על ידי התוצאות השמורות מפעילה בכל רכיב בדיוק את הפעולה שהמעגל המקורי היה מפעיל בהינתן אותה היסטוריה, ואינה משנה את נורמתו. כשמגיעים למדידה נוספת, הבנייה מהסעיף הקודם מפצלת כל רכיב לשני רכיבים, ושומרת את התוצאה החדשה בקיוביט עזר נפרד. כפי שחישבנו שם, גם ההסתברויות וגם המצבים המותנים הם בדיוק אלה של המדידה המקורית. לכן הטענה נשמרת לאורך כל החישוב.

לבסוף, היסטוריות שונות שמורות במצבי בסיס אורתוגונליים של אוגרי התוצאות. מדידת האוגרים האלה בוחרת כל היסטוריה בדיוק בהסתברות שבה הייתה מתקבלת בתהליך המקורי. בהינתן ההיסטוריה, גם מצב מערכת החישוב

זהה, ולכן מדידת הפלט נותנת את אותה התפלגות מותנית. מכאן שגם ההתפלגות המשותפת של כל תוצאות המדידות ושל הפלט נשמרת. □

לאחר שהוכחנו את העיקרון, נוסיף שתי הערות על אופן השימוש בו. הראשונה נוגעת לעלות החישובית של הבנייה, והשנייה מרחיבה אותה לבסיסי מדידה אחרים.

הערה: מהי עלות הבנייה? כאשר מספר צעדי החישוב חסום פולינומית וגם העיבוד הקלאסי של התוצאות יעיל, הבנייה כרוכה בתקורה פולינומית. ביחידה הבאה נדון בשאלה כיצד לממש שערים רצויים באמצעות אוסף קבוע של שערי בסיס, ונגדיר מהו אוסף שערים אוניברסלי. במסגרת הזו ייתכן שנצטרך לקרב גם את השערים המבוקרים שבבנייה שלנו. נראה שם כיצד לבחור את דיוק הקירוב כך שהשגיאה הכוללת תהיה קטנה כרצוננו.

הערה: מדידה בבסיס 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.