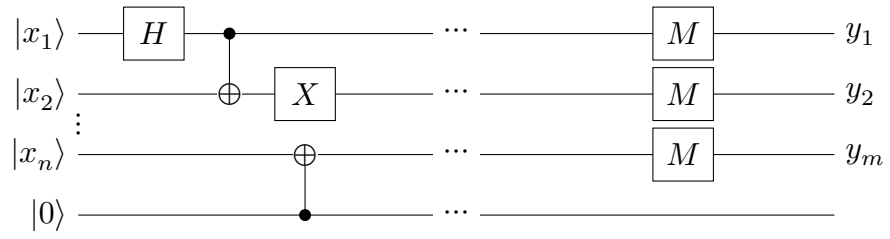
מודל החישוב הקוונטי: מעגלים קוונטיים וחישוב הפיך

1 מהו מעגל קוונטי?

בחישוב קלאסי מקובל לדבר הן על מכונות טיורינג והן על מעגלים. בהקשר של חישוב קוונטי יהיה לנו נוח לעבוד עם מעגלים. עם זאת, לא נרצה להחביא עבודה קשה בתוך בחירת המעגל: נדרוש שאלגוריתם קלאסי יוכל לייצר את תיאור המעגל עבור קלטים באורך נתון, בזמן פולינומי באורך הקלט. משפחה כזו של מעגלים נקראת משפחה *יוניפורמית*.

אז איך נראה מעגל קוונטי? מתחילים בקלט קלאסי $x \in \{0,1\}^n$, המיוצג במצב $|x\rangle$, ומוסיפים קיוביטי עזר במצב $|0\rangle^{\otimes a}$. מפעילים סדרה של שערים יוניטריים, שכל אחד מהם פועל על מספר קבוע של קיוביטים. בסוף מודדים את קיוביטי הפלט בבסיס הסטנדרטי ומקבלים מחרוזת קלאסית. החוטים בתרשים מייצגים קיוביטים, והזמן מתקדם משמאל לימין.



זהו תרשים סכמטי; הסימון M מציין מדידה בבסיס הסטנדרטי. לא חייבים למדוד את כל קיוביטי העזר.

נאמר שמעגל C מחשב פונקציה $F : \{0,1\}^n \to \{0,1\}^m$ בשגיאה לכל היותר 0.1, אם לכל קלט x מתקיים

$$\Pr[C(x) \neq F(x)] \leq 0.1.$$

ההסתברות היא על תוצאות המדידה. הדרישה היא לכל קלט בנפרד, ולא רק בממוצע על הקלטים. הקבוע המסוים אינו חשוב: בחישוב של פונקציה דטרמיניסטית אפשר להקטין את השגיאה באמצעות חזרות בלתי תלויות ובחירת הפלט השכיח.

1.1 כמה הערות על המודל

כדי לדבר על גודל המעגל צריך לקבוע אילו שערים מותרים. נשתמש באוסף קבוע של שערים מקומיים; לא נרשה שער יחיד שמבצע חישוב מסובך כרצוננו. *גודל המעגל* הוא מספר השערים בו, ומספר הקיוביטים מתאר את הזיכרון הדרוש. כשנאמר שהחישוב יעיל, נדרוש שגודל המעגל ומספר קיוביטי העזר יהיו פולינומיים, ושמשפחת המעגלים תהיה יוניפורמית.

בשלב זה נניח שכל המדידות מתבצעות בסוף החישוב. אפשר לשקול גם מודל שבו מודדים באמצע החישוב, ואף בוחרים את הפעולות הבאות לפי תוצאות המדידות. ביחידה הבאה נלמד את עיקרון דחיית המדידה: נראה כיצד לדמות חישוב כזה באמצעות קיוביטי עזר ושערים מבוקרים, כך שכל המדידות יתבצעו בסוף, עם תקורה פולינומית וללא שינוי בהתפלגות הפלט. כך נצדיק את ההנחה שבה נשתמש בינתיים.

השאלה המרכזית היא האם יש בעיה שמחשב קוונטי יכול לפתור ביעילות, אך מחשב קלאסי הסתברותי אינו יכול לפתור ביעילות. לפני שניגש לכיוון הזה, כדאי לשאול את השאלה ההפוכה: האם מחשב קוונטי מסוגל לפחות לעשות כל מה שמחשב קלאסי עושה?

2 איך מממשים חישוב קלאסי באמצעות שערים הפיכים?

לכאורה יש כאן קושי. כל שער יוניטרי הוא הפיך, ואילו שערים קלאסיים כמו AND ו־ OR אינם הפיכים. למשל, אם הפלט של שער AND הוא אפס, אי אפשר לדעת מה היו שני ביטי הקלט. איך נבנה חישוב כזה רק מפעולות הפיכות?

מעניין שהשאלה הזו נחקרה עוד לפני שהחישוב הקוונטי הפך לנושא מחקר מרכזי, מתוך עניין בעלות האנרגטית של חישוב. לפי עקרון לנדאואר, מחיקה לוגית של מידע כרוכה במחיר תרמודינמי. בניסוח הסטנדרטי, איפוס של ביט אקראי אחיד, ללא מידע צדדי עליו, מחייב פליטת חום ממוצעת של לפחות $k_B T \ln 2$ לסביבה בטמפרטורה T, בגבול האידיאלי. כאן k_B הוא קבוע בולצמן. ההבחנה החשובה היא בין מחיקה בלתי הפיכה לבין חישוב ששומר את המידע. הפיכות לוגית אינה מבטיחה שמחשב מעשי לא יצרוך אנרגיה, אבל היא מסירה את מקור העלות הזה.

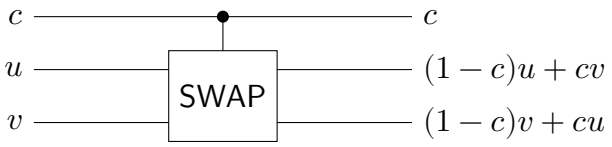
לכן אפשר לנסות לשמור את תוצאות הביניים במקום לדרוס אותן. כך נדע לשחזר את מצב החישוב הקודם בכל שלב. נראה שאפשר לעשות זאת ביעילות, ובהמשך נראה גם איך להחזיר את זיכרון העזר למצבו ההתחלתי. הטכניקה האחרונה מזוהה עם עבודתו של צ׳רלס בנט משנת 1973.

3 שער פְּרֶדְקִין

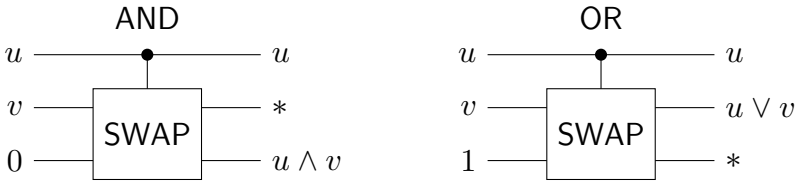
שער שימושי לחישוב הפיך הוא שער פְּרֶדְקִין, או controlled-SWAP, שנסמן CSWAP. זהו שער על שלושה ביטים: הביט הראשון הוא ביט הבקרה, ואם הוא אחד, מחליפים בין שני הביטים האחרים. כלומר,

$$\mathsf{CSWAP}(c,u,v) = \begin{cases} (0,u,v), & c=0, \\ (1,v,u), & c=1. \end{cases}$$

הפעלת השער פעמיים מחזירה אותנו לקלט המקורי, ולכן הוא הפיך. מכיוון שהוא תמורה של מצבי הבסיס הסטנדרטי, ההרחבה הליניארית שלו היא שער יוניטרי.



בעזרת ביטים קבועים אפשר לקבל מהשער הזה את הפעולות הקלאסיות המוכרות. בתרשימים הבאים $*$ מציין פלט שאיננו זקוקים לו כרגע; הוא עדיין קיים במערכת.

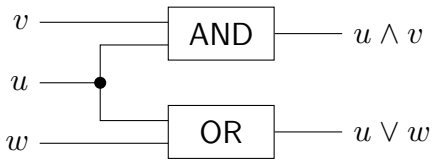


למשל, בקלט $(u,v,0)$ הביט השלישי הוא אפס אם $u=0$, והוא v אם $u=1$. לכן הוא בדיוק $u \wedge v$. בדומה, בקלט $(u,v,1)$ הביט השני הוא $u \vee v$.

3.1 העתקה ושלילה

יש עוד פעולה שמסתתרת במודל המעגלים הקלאסי: שימוש באותו ביט בכמה מקומות, או fan-out.

למשל, במעגל הקלאסי הבא אותו ביט u משמש לחישוב שני פלטים שונים:



הנקודה השחורה מציינת הסתעפות של חוט קלאסי: שני החוטים היוצאים ממנה נושאים את אותו ביט u.

כדי לממש זאת בחישוב הפיך, נרצה ליצור עותקים של הביט בעזרת ביטי עזר.

האם זה לא סותר את משפט אי־השכפול? לא: מותר להעתיק ביט במצב בסיס. למשל, השער CNOT מבצע $|u\rangle|0\rangle \mapsto |u\rangle|u\rangle$ עבור $u \in \{0,1\}$, אבל על סופרפוזיציה הוא פועל כך:

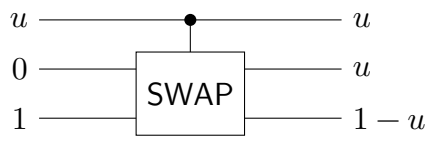
$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \longmapsto \alpha|00\rangle + \beta|11\rangle .$$

בדרך כלל זהו מצב שזור, ולא שני עותקים של מצב הקלט.

נראה כעת כיצד לממש את ההעתקה בעזרת שער פְּרֶדְקִין, ובאותה הזדמנות לקבל גם את שלילת הביט:

$$(u, 0, 1) \longmapsto (u, u, 1-u).$$

קיבלנו גם עותק של הביט וגם את שלילתו. לכן שערי פְּרֶדְקִין, יחד עם ביטי עזר קבועים, מספיקים למימוש כל מעגל בוליאני. ביטי עזר שערכם אחד אפשר להכין מאפס בעזרת השער X.



3.2 סימולציה של מעגל קלאסי

ניקח מעגל קלאסי בגודל s המחשב $F : \{0,1\}^n \to \{0,1\}^m$. נעבור על השערים לפי סדר החישוב, נחליף כל שער במימוש הפיך, ונשמור את תוצאות הביניים. אם צריך להשתמש באותו ביט שוב, ניצור עותקים שלו באופן שתיארנו. כך נקבל מעגל הפיך P המבצע

$$P : |x\rangle|0^a\rangle \longmapsto |x\rangle|F(x)\rangle|g(x)\rangle ,$$

כאשר $g(x)$ היא מחרוזת תוצאות הביניים, המכונה *פסולת חישוב*. מספר הקיוביטים נשמר: אם אורך הפסולת הוא b, אז $a = m + b$. במודל הרגיל של שערים עם מספר קבוע של כניסות, גודל המעגל ומספר קיוביטי העזר הם $O(s + n + m)$. את תיאור המעגל אפשר לייצר בזמן פולינומי בגודל תיאור המעגל המקורי. לכן גם יוניפורמיות נשמרת.

3.3 ומה לגבי אקראיות?

כדי לקבל ביט אקראי אחיד, מספיק להכין $|0\rangle$, להפעיל עליו H ולמדוד בבסיס הסטנדרטי:

$$|0\rangle \xrightarrow{H} |+\rangle \xrightarrow{\text{measurement}} \begin{cases} 0, & \text{probability} 1/2, \\ 1, & \text{probability} 1/2. \end{cases}$$

לחלופין, אפשר לדחות את המדידה: מכינים את סרט האקראיות במצב $|+\rangle^{\otimes r}$, משתמשים בו בחישוב ההפיך ושומרים אותו. מדידת הפלט נותנת בדיוק את התפלגות הפלט של החישוב הקלאסי ההסתברותי.

4 ביטול פסולת חישוב

הצלחנו לבצע את החישוב, אבל נשארנו עם פסולת. בחישוב קלאסי אפשר לעיתים להתעלם ממנה; בחישוב קוונטי היא עלולה להישזר עם הפלט ולהפריע להתאבכות בהמשך. היינו רוצים להחזיר את קיוביטי העזר לאפס, בלי לאבד את התשובה. הפעולה הזו מכונה uncomputing garbage.

הרעיון פשוט ויפה: מחשבים, מעתיקים את התשובה לאוגר נוסף, ואז מריצים את החישוב לאחור. נוסיף אוגר של m קיוביטים במצב בסיס כלשהו $|y\rangle$. שלושת השלבים הם

$$\begin{aligned} |x\rangle |0^a\rangle |y\rangle &\xrightarrow{P} |x\rangle |F(x)\rangle |g(x)\rangle |y\rangle \\ &\xrightarrow{\text{CNOT}^{\otimes m}} |x\rangle |F(x)\rangle |g(x)\rangle |y \oplus F(x)\rangle \\ &\xrightarrow{P^{-1}} |x\rangle |0^a\rangle |y \oplus F(x)\rangle . \end{aligned}$$

בשלב האמצעי מפעילים שער CNOT מכל ביט של הפלט אל הביט המתאים באוגר החדש. הפעולה $\oplus$ היא חיבור מודולו שתיים בכל קואורדינטה.

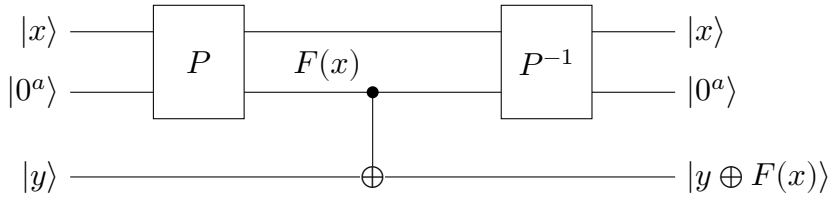
מדוע ההעתקה אינה מפריעה לביטול החישוב? בפיתוח שלעיל התחלנו במצב בסיס קבוע $|x\rangle |0^a\rangle |y\rangle$. במקרה הזה אין שזירה באף אחד משלושת השלבים: בכל שורה מופיע מצב מכפלה של מצבי בסיס. השער CNOT יכול ליצור שזירה, אבל אינו יוצר אותה בכל הפעלה. בפרט, העתקת ערך בסיס ידוע לאוגר נוסף אינה יוצרת שזירה. לאחר ההעתקה, האוגרים שעליהם פעל P עדיין נמצאים בדיוק במצב $|x\rangle |F(x)\rangle |g(x)\rangle$, ולכן P^{-1} מחזיר

אותם למצב $|x\rangle|0^a\rangle$. האוגר האחרון אינו משתתף בפעולה הזו, ולכן נשאר במצב $|y \oplus F(x)\rangle$. בפרט, כאשר $y = 0^m$, נשמרת בו התשובה $F(x)$.

ומה קורה אם הקלט הוא סופרפוזיציה? כאן אכן יכולה להיווצר שזירה אמיתית, אבל אותו חישוב תקף בכל רכיב בנפרד, מליניאריות:

$$\sum_x \alpha_x |x\rangle |F(x)\rangle |g(x)\rangle |F(x)\rangle$$
$$\xrightarrow{P^{-1}\otimes I} \sum_x \alpha_x |x\rangle |0^a\rangle |F(x)\rangle .$$

לשם הפשטות בחרנו כאן את האוגר האחרון בתחילה במצב אפס. אין כאן מחיקה של כל המידע על x: אוגר הקלט נשמר, והוא עדיין עשוי להיות שזור עם אוגר התשובה. רק קיוביטי העבודה חוזרים לאותו מצב אפס בכל רכיבי הסופרפוזיציה, ולכן הם נפרדים משאר המערכת. כלומר, איננו מבטלים את השזירה בין אוגר התשובה לבין כל שאר האוגרים; אנחנו מסלקים ממנה את קיוביטי העבודה, תוך שמירת הקלט והתשובה.



בתרשים כל חוט עשוי לייצג אוגר שלם, והפעולה המבוקרת באמצע מייצגת m שערים, אחד לכל ביט פלט.

כדי לבנות את P^{-1}, הופכים את סדר השערים ומחליפים כל שער בהופכי שלו. שערי פְּרֶדְקִין והשער X הם ההופכיים של עצמם. אם גודל המעגל P הוא S, הבנייה החדשה משתמשת ב־ $2S + m$ שערים. כלומר, ניקוי הפסולת עולה רק בתקורה קטנה בגודל המעגל.

בפרט, עבור $y = 0^m$ נקבל עותק של התשובה וכל קיוביטי העבודה יחזרו לאפס. מאחר שהזהות נכונה לכל מצב בסיס, מליניאריות היא נכונה גם לסופרפוזיציות. כשמשמיטים מהסימון את קיוביטי העבודה, שנכנסים ויוצאים במצב אפס, מקבלים את הפעולה

$$U_F : |x\rangle |y\rangle \longmapsto |x\rangle |y \oplus F(x)\rangle .$$

שימו לב: הטיעון משתמש בכך שהמעגל המקורי מחשב פונקציה קלאסית *בדיוק*. אין כאן טענה שאפשר להעתיק פלט קוונטי שרירותי של אלגוריתם כלשהו.

5 חישוב בפאזה

לפעמים נוח שהתשובה לא תיכתב באוגר נפרד, אלא תופיע בפאזה. נניח כעת שהפונקציה בוליאנית:

$$F : \{0,1\}^n \to \{0,1\}.$$

נפעיל את U_F כאשר אוגר התשובה, שהוא כעת קיוביט יחיד, נמצא במצב $|-\rangle$. מה נקבל?

$$\begin{aligned} U_F(|x\rangle|-\rangle) &= \frac{1}{\sqrt{2}}U_F(|x\rangle|0\rangle - |x\rangle|1\rangle) \\ &= \frac{1}{\sqrt{2}}|x\rangle\left(|F(x)\rangle - |1\oplus F(x)\rangle\right) \\ &= (-1)^{F(x)}|x\rangle|-\rangle . \end{aligned}$$

אם $F(x)=0$, לא קורה דבר לקיוביט העזר. אם $F(x)=1$, מופעל עליו השער X, ומכיוון ש־ $X|-\rangle = -|-\rangle$, מתקבל סימן מינוס. קיוביט העזר נשאר במצב $|-\rangle$ ואינו שזור עם אוגר הקלט בסוף הפעולה.

אפשר להכין אותו מתוך $|0\rangle$ על ידי הפעלת X ואחריו H, ובסוף להחזיר אותו לאפס באמצעות H ואחריו X. כך, כאשר משמיטים את קיוביטי העזר מהסימון, מתקבלת הפעולה

$$Z_F : |x\rangle \longmapsto (-1)^{F(x)}|x\rangle .$$

התופעה הזו מכונה phase kickback.

רגע, הרי אמרנו שפאזה גלובלית אינה ניתנת למדידה. אז מה הרווחנו? עבור קלט יחיד במצב בסיס, באמת אין הבדל שניתן למדוד. אבל על סופרפוזיציה מתקבל

$$\sum_x \alpha_x|x\rangle \longmapsto \sum_x (-1)^{F(x)}\alpha_x|x\rangle .$$

כאן הסימנים עשויים להשתנות בין רכיבי הסופרפוזיציה, ולכן מדובר בפאזות יחסיות. הן יכולות להשפיע על ההתאבכות ועל תוצאות המדידה אחרי הפעלת שערים נוספים.