אלגוריתמים קוונטיים

בעיית דויטש־ג'וזה (DJ)

נתונה פונקציה $f:\{0,1\}^n \to \{0,1\}$, שלגביה מובטח כי היא עונה לתנאי הבא:
הפונקציה מקיימת אחת משתי האפשרויות: או שמתקיים $f(x)=0$ לכל x, או שמתקיים
ש־f מאוזנת (balanced): בדיוק למחצית מהערכים מתקיים $f(x)=0$ ולמחצית מהערכים
מתקיים $f(x)=1$.

<u>הבעיה</u>: יש לזהות האם f הינה אפס או מאוזנת
כאשר נתון רכיב דמיוני (Oracle) המחשב את f ביעילות.

<u>שאלה</u>: כמה פעמים נצטרך לפנות לרכיב ולחשב את f?

DJ – המקרה של קיוביט בודד

בעיה זו נקראת בעיית דויטש (1989), והיא הוצגה שלש שנים לפני הבעיה הכללית של דויטש־ג'וזה [Deutsch and Jozsa, 1992].

למעשה, השאלה מעט שונה: במקום לשאול אם $f(x) = 0$ או מאוזנת, נשאל אם הפונקציה קבועה או מאוזנת.

כלומר, (מאחר ומדובר בביט בודד), יש לחשב את $f(0) \oplus f(1)$

כמה פניות לאורקל נצטרך?

תוכלו להשתכנע בכוחות עצמכם שזה אכן נפתר כמקרה פרטי על ידי האלגוריתם הקוונטי של DJ.

סיבוכיות קלסית – DJ

$1 + \frac{2^n}{2}$ פניות לאורקל על־מנת לדעת בוודאות. (אם הרצנו $\frac{2^n}{2}$ פעמים ייתכן שנקבל תמיד את התשובה 0 למרות ש־f הינה מאוזנת)

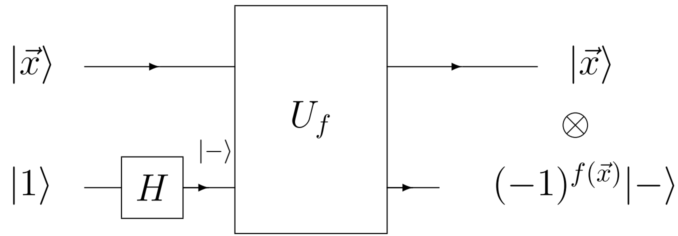
נשים לב שפתרון הסתברותי (קלסי) ניתן להשיג עם $O(1)$ ניסיונות כי נדגום ערכי x אקראיים ואז בלתי־סביר שנקבל רק $f(x) = 0$ אם בעצם f היא מאוזנת. לכן, הבעיה לא כל כך מעניינת (מבחינת היתרון של חישוב קוונטי): כי יש פתרון הסתברותי יעיל.

[הערה: האם מכאן נובע $P \neq BPP$?]

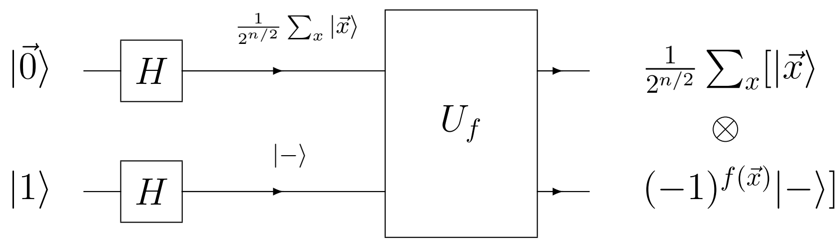
אלגוריתם DJ – סיבוכיות קוונטית

מספיק לפנות לפונקציה f פעם אחת!!!

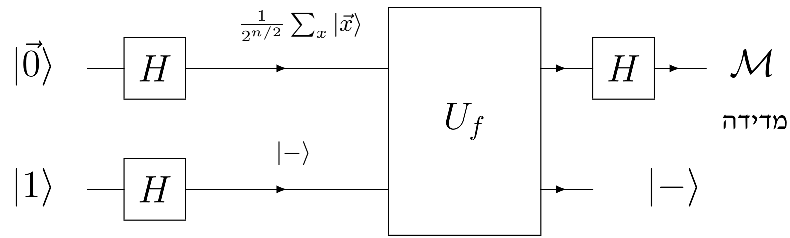
נשתמש בטכניקה שנותנת את ערך הפונקציה בפאזה:



נחשב את f על כל הקלטים (באורך n) במקביל



האלגוריתם כולו



$$
\begin{aligned}
|\vec{0}\rangle|1\rangle \quad &\xrightarrow{H} \quad \frac{1}{2^{n/2}}\sum_x |\vec{x}\rangle|-\rangle \\
&\xrightarrow{f} \quad \frac{1}{2^{n/2}}\sum_x (-1)^{f(\vec{x})}|\vec{x}\rangle|-\rangle \\
&\xrightarrow{H} \quad ?
\end{aligned}
$$

הערה צדדית: בשקפים אלו אנו מסמנים את x כווקטור רק בגלל שאת המספר 0 קריטי לסמן כאן כווקטור.

מקרה א', f היא תמיד 0. נקבל

$$\frac{1}{2^{n/2}}\sum_x(-1)^0|\vec{x}\rangle|-\rangle = \frac{1}{2^{n/2}}\left[\sum_x|\vec{x}\rangle\right]|-\rangle$$

ואחרי H נקבל $\xrightarrow{H} |\vec{0}\rangle|-\rangle$

הערה צדדית: בשקף זה אנו עדיין מסמנים את x כווקטור. בשקף הבא אנו חוזרים לסימון המקובל בקורס, כלומר ללא סימון הווקטור.

מקרה ב', f מאוזנת. נקבל (בהתעלמות מהביט $|-\rangle$)

$$\begin{aligned}
&\xrightarrow{H} \frac{1}{2^{n/2}}\sum_x(-1)^{f(x)}\left[H|x\rangle\right] \\
&= \frac{1}{2^{n/2}}\sum_x(-1)^{f(x)}\frac{1}{2^{n/2}}\sum_y(-1)^{x\cdot y}|y\rangle = \frac{1}{2^n}\sum_y\sum_x(-1)^{f(x)}(-1)^{x\cdot y}|y\rangle
\end{aligned}$$

נשים לב שלעולם לא נקבל $y=\vec{0}$, כי המקדם של $|y\rangle=|\vec{0}\rangle$ הוא

$$\sum_x(-1)^{f(x)}(-1)^{x\cdot 0}=\sum_x(-1)^{f(x)}=0$$

כי f מאוזנת ובחצי מהמקרים $(-1)^{f(x)}=1$ ובחצי השני $(-1)^{f(x)}=-1$.

הערה: הסיכוי לקבלת ערך y' מסוים כאשר f מאוזנת:

$$\begin{aligned} P(y') &= \left| \langle y' | \frac{1}{2^n} \sum_y \sum_x (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \right|^2 \\ &= \left| \frac{1}{2^n} \sum_x (-1)^{f(x)} (-1)^{x \cdot y'} \right|^2 \end{aligned}$$

DJ – סיכום

אם מקבלים $y=0$ יודעים ש־$f=0$

אם מקבלים $y\neq 0$ יודעים ש־f מאוזנת

* * *

זוהי בעיית הכרעה: בתשובה יש רק ביט אחד של אינפורמציה: האם f היא 0 או מאוזנת

* * *

היתרון הקוונטי לעומת BPP הינו קטן, כלומר הרצה אחת לעומת מספר קבוע של הרצות.

* * *

בעיות בהן מובטח ש־f מתנהגת בצורה מסוימת נקראות בעיות הבטחה (promise problems)

* * *

הנחנו שלכל קלט נתון החישוב של f הינו יעיל קלסית – כי נעשה על ידי האורקל

* * *

ניתן לפתור גם בעיה דומה (שכבר ראינו בשקף של בעיית דויטש): לשאול האם f מאוזנת או קבועה

בעיית סיימון

נתונה פונקציה $f:\{0,1\}^n \to \{0,1\}^n$ שהיא $1 \to 2$ [כלומר, לכל x קיים y יחיד (ושונה ממנו) כך ש־$f(x)=f(y)$.]

מובטח שקיים s כך שמתקיים $f(x)=f(y)$ אם"ם $y = x \oplus s$.

הבעיה: מצא את s.

השאלה: כמה פעמים צריך להפעיל את f?

(הערה: ניתן לנסח כבעיית הכרעה)

סיימון – סיבוכיות קלסית

s מכיל n ביטים ויש לו $2^n - 1$ אפשרויות (כי $s \neq 0$), כך שלנחש אותו זה רעיון גרוע.

מסתבר, שאין פתרון קלסי טוב הרבה יותר:

נניח שניקח $2^{n/4}$ ערכים של $f(x)$. מספר הזוגות עבורם חישבנו את הפונקציה f הוא $2^{n/2} = (2^{n/4})^2 < \binom{2^{n/4}}{2}$ כי $k^2 < \frac{k(k-1)}{2} = \binom{k}{2}$.

הסיכוי שזוג אקראי יקיים $y = x \oplus s$ ("התנגשות") ונקבל $f(x) = f(y)$ הינו בערך 2^{-n}.

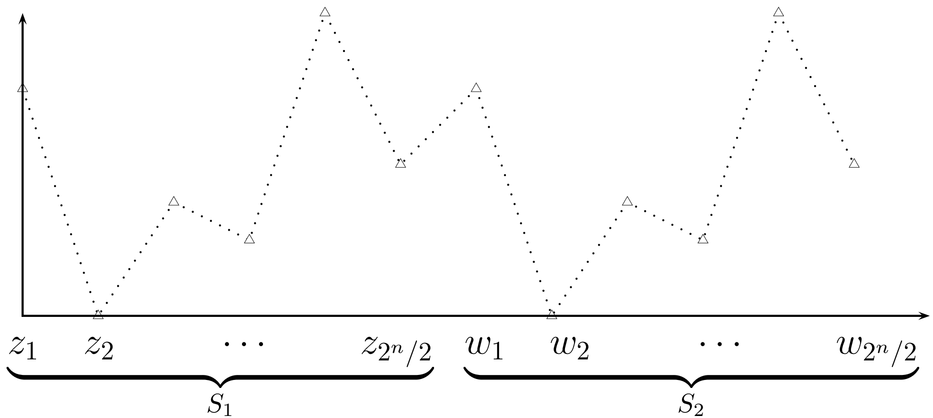
לכן הסיכוי שמצאנו התנגשות קטן מ-$2^{-n/2} = 2^{-n}2^{n/2}$ (מאד קטן!).

וזאת למרות שניסינו מספר אקספוננציאלי של פעמים.

הערה – f הינה מחזורית

נסדר את הקלטים כך שקודם מופיעה קבוצת x־ים בלי אף התנגשות, כלומר קלטים עבורם f אינה מקבלת את אותו ערך פעמיים. נקרא להם $S_1 = \{z_1, z_2 \ldots z_{2^n/2}\}$.

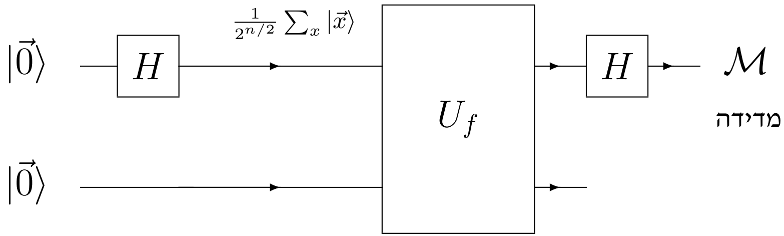
אחריהם נסדר את שאר ה־x־ים, כך שהסדר הוא $w_1 = z_1 \oplus s$, $w_2 = z_2 \oplus s$ וכו' (שינינו את השם ל־w כדי שיהיו מסודרים בסדר עולה), ולהם נקרא S_2.



במובן מסוים, s הוא המחזור של f, כי ע"י "הזזה" של z_i ב־s נקבל את w_i.

אלגוריתם סיימון – סיבוכיות קוונטית

האלגוריתם:



$$|\vec{0}\rangle|\vec{0}\rangle \xrightarrow{H_n} \frac{1}{2^{n/2}}\sum_x |x\rangle|0\rangle \xrightarrow{f} \frac{1}{2^{n/2}}\sum_x |x\rangle|f(x)\rangle$$

$$\xrightarrow{H_n} \frac{1}{2^n}\sum_x\sum_y (-1)^{x\cdot y}|y\rangle|f(x)\rangle = |\psi\rangle$$

כעת נסכם בנפרד על x־ים השייכים ל־S_1 ועל אלו שב־S_2.

$$|\psi\rangle = \frac{1}{2^n}\sum_y \left[\sum_{x\in S_1}(-1)^{x\cdot y}|f(x)\rangle + \sum_{x\in S_2}(-1)^{x\cdot y}|f(x)\rangle\right]|y\rangle$$

$$= \frac{1}{2^n}\sum_y \left[\sum_{z\in S_1}\left\{(-1)^{z\cdot y}|f(z)\rangle + (-1)^{(z\oplus s)\cdot y}|f(z)\rangle\right\}\right]|y\rangle$$

בסכום השני מופיע $f(z)$ כי $f(z\oplus s)=f(z)$.

נשים לב ש־$\left\{|f(z)\rangle\right\}_{z\in S_1}$ היא קבוצת מצבים אורתוגונליים כי $f(z_i)\neq f(z_j)$.

$$|\psi\rangle = \frac{1}{2^n}\sum_y\sum_{z\in S_1}\left[(-1)^{z\cdot y} + (-1)^{(z\oplus s)\cdot y}\right]|y\rangle|f(z)\rangle$$

$$= \frac{1}{2^n}\sum_y\sum_{z\in S_1}(-1)^{z\cdot y}\left[1+(-1)^{s\cdot y}\right]|y\rangle|f(z)\rangle$$

אם $s\cdot y = 0_{\mathrm{mod}\,2}$ אזי נקבל $1+(-1)^{s\cdot y}=2$ ואילו אם $s\cdot y = 1_{\mathrm{mod}\,2}$
אזי נקבל 0 בסוגריים, כלומר התאבכות הורסת לאותו $|y\rangle$.

נגדיר $S^{\perp} = \{y \mid y \cdot s = 0_{\mathrm{mod}\, 2}\}$. אנו רואים שרק $y \in S^{\perp}$ תורמים אמפליטודה שאינה אפס.

$$|\psi\rangle = \frac{1}{2^{n-1}} \sum_{y \in S^{\perp}} \sum_{z \in S_1} (-1)^{z \cdot y} |y\rangle |f(z)\rangle$$

גם y וגם z מקבלים 2^{n-1} ערכים.

כעת מדידה של $|y\rangle$ תיתן y מסוים, נאמר y', בסיכוי:

$$P_{y'} = \frac{1}{2^{n-1}}$$

ועל ידי מציאת $n-1$ וקטורים בלתי תלויים y', כך שמתקיים $y' \in S^{\perp}$, נלמד מהו s.

חשוב שהסיכוי של כל y' הינו זהה, כדי שמספר kn (כאשר k קבוע) של הפעלות ייתן לנו את כל $n-1$ הווקטורים הדרושים בסיכוי טוב כרצוננו.

בעיית סימון נפתרת ביעילות על מחשב קוונטי – פער אקספוננציאלי מוכח!!!

הוכחה שהתפלגות y' אחידה:

$$\begin{aligned}
P_{y'} &= \left|\langle y'|\psi\rangle\right|^2 \\
&= \left|\langle y'|\frac{1}{2^{n-1}}\sum_{y\in S^{\perp}}\sum_{z\in S_1}(-1)^{z\cdot y}|y\rangle|f(z)\rangle\right|^2 \\
&= \left(\frac{1}{2^{n-1}}\right)^2\left|\sum_{z\in S_1}(-1)^{z\cdot y'}|f(z)\rangle\right|^2 \\
&= \left(\frac{1}{2^{n-1}}\right)^2\sum_{z'\in S_1}(-1)^{z'\cdot y'}\langle f(z')|\sum_{z\in S_1}(-1)^{z\cdot y'}|f(z)\rangle \\
&= \left(\frac{1}{2^{n-1}}\right)^2\sum_{z'\in S_1}\sum_{z\in S_1}(-1)^{z\cdot y'}(-1)^{z'\cdot y'}\delta_{zz'} \\
&= \left(\frac{1}{2^{n-1}}\right)^2\sum_{z\in S_1}1 = \left(\frac{1}{2^{n-1}}\right)^2 2^{n-1} = \frac{1}{2^{n-1}} \quad \text{QED}
\end{aligned}$$

ההתפלגות בלתי־תלויה ב־z כך שאם נמדוד את y וגם את z [דרך מדידת $f(z)$], נקבל כל זוג (y,z) בהסתברות משותפת $\left(\frac{1}{2^{n-1}}\right)^2$.

למעשה אין כלל צורך למדוד את $f(z)$.

כל הפעלה של f נותנת וקטור אקראי y המאונך ל־s (במובן $y \cdot s = 0_{\bmod 2}$). כמה דגימות צריך כדי לדעת את s?

נרצה לקבל $n-1$ וקטורים בלתי־תלויים המאונכים ל־s ואז קל לבודד את s (מערכת משוואות לינאריות). ניתן להוכיח (תרגיל בית!?) שלשם כך צריך $O(n)$ הפעלות; אם ניקח kn הפעלות אזי הסיכוי שאין בידינו לפחות $n-1$ וקטורים ב"ת הוא אקספוננציאלית קטן $2^{-O(n)}$.

לסיכום:

מוכח כאן פער אקספוננציאלי

אבל

א. הבעיה אינה בעלת חשיבות פרקטית

ב. זוהי בעיית אורקל, ולא קיים מימוש יעיל לאורקל זה

ג. זוהי בעיית אורקל, ולכן אין בכך הוכחה ש־ $BPP \neq BQP$