חשוב ~~[illegible]~~ non-signalling

פעולת ~~[illegible]~~ עיקרון של A עושה, לא משפיעה על הסטטיסטיקה של B.

[אף מונע שהתוצאה של A רנדומלית, ידוע ההסתברות של התוצאות של B]

למשל-

- חישוב לפי הכלל ~~[illegible]~~ ת.ז.ח
- חישוב קוונטי " "

עבור שניים A, B חלקיקים

$\frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$

התוצאות של המדידה הסי' הם קורלציה.

שאלה ל A	שאלה ל B →	0		1	
	תשובה A \ תשובה B	0	1	0	1
0	0	1/2	0	1/2	0
	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
	1	0	1/2	1/2	0

PR Box

non-signalling

חישוב n.s. ~~[illegible]~~, A של 'בחירה' ~~[illegible]~~ על 'תשובה' ~~[illegible]~~ של B
הפוך.

שאלה 5

1

(classical) realism

הנחה בעולם מצב הוא אובייקט שיש קשר של המדידה שלו.
אם (האובייקט) נלקח מהמקום — מקבלים המשתנה זו תוצאה.
אם יש קורל' במדידה מקבלים קורלציה קלאסית.

דוגמה

בהסתברות $\frac{1}{2}$ AB מקבלים 0,0
״ $\frac{1}{2}$ ״ ״ 1,1

אם נמדוד A = תוצאת B.

האם אפשר להסביר את הערך ע״י Hidden classical RV ?

Bell: לפי התורה הקוונטית קיים ... של A ו B מתנגדים

אם יש ראליזם: a_0 - התוצאה של A אם נמדד במדידה 0
״ ״ ״ ״ ״ a_1 ... 1
״ ״ B ״ ״ b_0 ... 0
״ ״ ״ ״ ״ b_1 ... 1

אז $pr(S \wedge T = a_S \oplus b_T) \leq \frac{3}{4}$

אבל שזירה, אפשר להגיע: $pr(S \wedge T = a_S \oplus b_T) \approx 0.86$
אפשר להגיע, והתחלנו בזה!

ובקופסת PR $pr(S \wedge T = a_S \oplus b_T) = 1$

מ Bell נקבל שלא יכול להיות דומה:

- non-signaling
- Classical realism
- ולאפשר לבוב ולאליס לבחור באופן בלתי
  תלוי ערכים מתוך $s,t \in \{0,1\}^2$ ...

אלגוריתמים

1 $BPP \subseteq BQP$

אם $f(x)$ בעלת מעגל קלאסי

אז $T: |x,y\rangle \to |x, f(x)\oplus y\rangle$ ניתן לחישוב יעיל יוניטרי

במעגל יש שערים כמו (and (2 qubits) not, or

ובמעגל מעגל קוונטי יעיל

$$|x,y,\bar{0}\rangle \xrightarrow{T} |x, y\oplus C(x), g(x,y)\rangle$$
$$\to |x, y\oplus C(x), g(x,y), y\oplus C(x)\rangle$$
$$\xrightarrow{T^{-1}} |x, y, \bar{0}\rangle\, |y\oplus C(x)\rangle$$

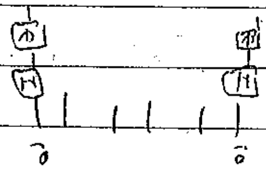
הערה: אם f ניתן לחישוב ע"י מעגל קל' יעיל אז אפשר לחשב $|x,0\rangle \to |x, f(x)\rangle$ ע"י מעגל קוונטי יעיל.
$|x,y\rangle \to |x, y\oplus f(x)\rangle$

הערה: אם גם f, וגם f^{-1}, ניתנות לחישוב ע"י מעגל קל' יעיל אז אפשר לחשב $|x\rangle \to |f(x)\rangle$ ע"י מעגל קוונטי יעיל

הוכחה: $|x,0\rangle \to |x, f(x)\rangle \xrightarrow{f^{-1}} |x\oplus x, f(x)\rangle = |0, f(x)\rangle$

מסקנה: לכל מעגל קל' C, יש מעגל קוונטי שמחשב $|x,y,0\rangle \to |x, y\oplus C(x), 0\rangle$

מסקנה $P \subseteq BQP$



כיוון שיש לנו מטבע אקראי "הוגן"

מסקנה $BPP_\varepsilon \subseteq BQP_\varepsilon$

בהמשך: נראה בעיה שנמצאת ב-BQP ולא ידוע האם היא ב-BPP

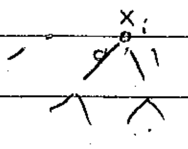
2 הבעיה של דויטש

קלט: $f:\{0,1\}\to\{0,1\}$ (יש 4 פונק' אפשריות כאלה)

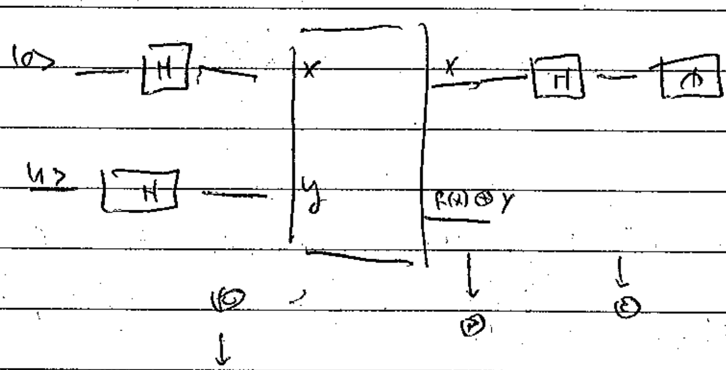
פלט: $f(0)\oplus f(1)$

קלסי: צריך 2 שאילתות ל f.

מודל של Decision trees



קוונטי:



$$\textcircled{0}\quad \frac{1}{\sqrt{2}}\left[(0+1)\otimes(0-1)\right]=\frac{1}{2}\left[00+10-01-11\right]$$

$$\textcircled{1}\quad \frac{1}{2}\left[0,f(0)+1,f(1)-0,\overline{f(0)}-1\,\overline{f(1)}\right]=$$

$$=\frac{1}{2}\left[|0\rangle\otimes\left(f(0)-\overline{f(0)}\right)+|1\rangle\otimes\left(f(1)-\overline{f(1)}\right)\right]$$

$$\textcircled{2}\quad =\underbrace{\frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right]}_{H\to|0\rangle}\otimes\frac{1}{\sqrt{2}}\left[f(0)-\overline{f(0)}\right]\qquad f(0)=f(1),\quad f(0)\oplus f(1)=0 \quad \text{אם}$$

$$=\underbrace{\frac{1}{\sqrt{2}}\left[|0\rangle-|1\rangle\right]}_{H\to|1\rangle}\otimes\frac{1}{\sqrt{2}}\left[f(0)-\overline{f(0)}\right]\qquad f(0)=\overline{f(1)},\ f(0)\neq f(1),\quad f(0)\oplus f(1)=1 \quad \text{אם}$$

$$f(0)-\overline{f(0)}=-\left[f(1)-\overline{f(1)}\right]$$

□

במודל ה Black-box אלגוריתם

קלט: נתונה פונק' (...) f כ Black-box ; [illegible]

יש מופעי Yes: [illegible]
ומופעי No:

צריך להבחין בין השניים
מותר לקרוא קריאות אורקל ל x.

בדוגמא: $f: \{0,1\}^n \rightarrow \{0,1\}$

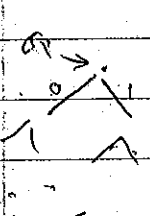
מופעי Yes: f קבועה על 0. [$\forall x$ ...]
מופעי No: f מאוזנת $\sum_x (-1)^{f(x)} = 0$

נשים לב: במקרה זה $\{0,1\}^n \neq Yes \cup No$
זה נקרא Promise problem
כי מבטיחים... מובטח לנו ש $f \in Yes \cup No$ (ואז זה פרומיס אחר).

אילו $\{0,1\}^n = Yes \cup No$ זו בעיה רגילה (למשל כמו הבעיה ב...).

במודל הקלאסי מותר לחשב שאילתות O.O ל f

מודל Decision trees



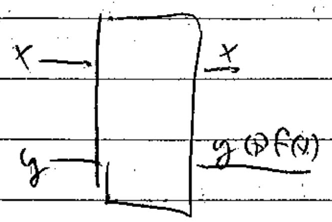
כל אלגוריתם O.O קלאסי דטרמיניסטי צריך לבצע $\frac{2^n}{2}+1$ שאילתות.

הוכחה: ... $\frac{2^n}{2}$ שאילתות
התשובה נותנת ...
[illegible] בהסתברות $\frac{1}{2}$ ... 0 [אם f קבועה 0]
$\frac{1}{2}$ [... מאוזנת]

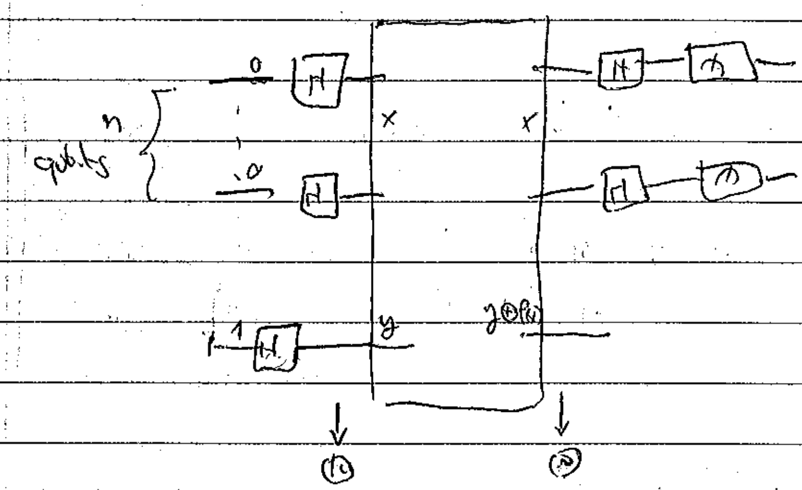
(6)

נראה אלגוריתם D.J קוונטי לבעיה ההבטחה הזו
עם שאילתא אחת.

<u>אלגוריתם D.J קוונטי</u>: מעגל קוונטי,
שאילתא: הפעלה של הקופסא



האלגוריתם:
(מדידה בבסיס הסטנדרטי)



אם במדידה נקבל 0...0 נחזיר "f קבועה"
״ ״ תוצאה אחרת ״ "f מאוזנת"

$$① \quad \frac{1}{\sqrt{2^n}}\sum_x |x\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle-|1\rangle\right] = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_x\left[|x,0\rangle-|x,1\rangle\right]$$

$$② \quad \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_x\left[|x,f(x)\rangle-|x,\overline{f(x)}\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle\otimes|0-1\rangle$$

$$= \frac{1}{\sqrt{2^n}}\underbrace{\sum_x (-1)^{f(x)}}\ |x\rangle\otimes|-\rangle$$

נדבר מה נעשה! ③

מקבלים כך שמשתמש פעם אחת ב BB $\sum_x(-1)^{f(x)}|x\rangle$

מה קורה כשמפעילים על Had^n ?

א) y_i ביט.

$$H(y_i) = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^{y_i} |1\rangle \right]$$

$$= \frac{1}{\sqrt{2}} \sum_{z_i \in \{0,1\}} (-1)^{y_i \cdot z_i} |z_i\rangle$$

ב) n ביטים: $H^{\otimes n} |y_1 \dots y_n\rangle = H|y_1\rangle \otimes H|y_2\rangle \dots \otimes H|y_n\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{y_1 \cdot z_1} |z_1\rangle \otimes (-1)^{y_2 \cdot z_2} |z_2\rangle \dots \otimes (-1)^{y_n \cdot z_n} |z_n\rangle$$

$$= \boxed{\frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{y \cdot z} |z\rangle}$$

$$y \cdot z = \sum_{i=1}^{n} y_i z_i \ (\text{mod } 2)$$

לדוגמה:

אם f קבועה אז:

$$H^{\otimes n} (\underbrace{H^{\otimes n} |0\rangle}_{\frac{1}{\sqrt{n}} \sum_x |x\rangle}) = (H^2)^{\otimes n} |0\rangle = I^{\otimes n} |0\rangle = |0\rangle \quad \text{נקבל}$$

$H^2 = I$

$—[H]—[H]—$

H אוניטרית, $H = H^\dagger$.

$—[H]—[H]—$

אם f מאוזנת:

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \xrightarrow[H^{\otimes n}]{} \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle$$

$$= \frac{1}{2^n} \sum_z \left[\sum_x (-1)^{f(x)} (-1)^{x \cdot z} \right] |z\rangle$$

ג) ומקדם $z=0$ הוא $\sum_x (-1)^{f(x)} = 0$ כי f מאוזנת, ולכן לא נקבל את 0 בהסתברות!

האלגוריתם של Simon

קלט: $f:\{0,1\}^n \to \{0,1\}^m$

הבטחה

קיים $s \in \{0,1\}^n$

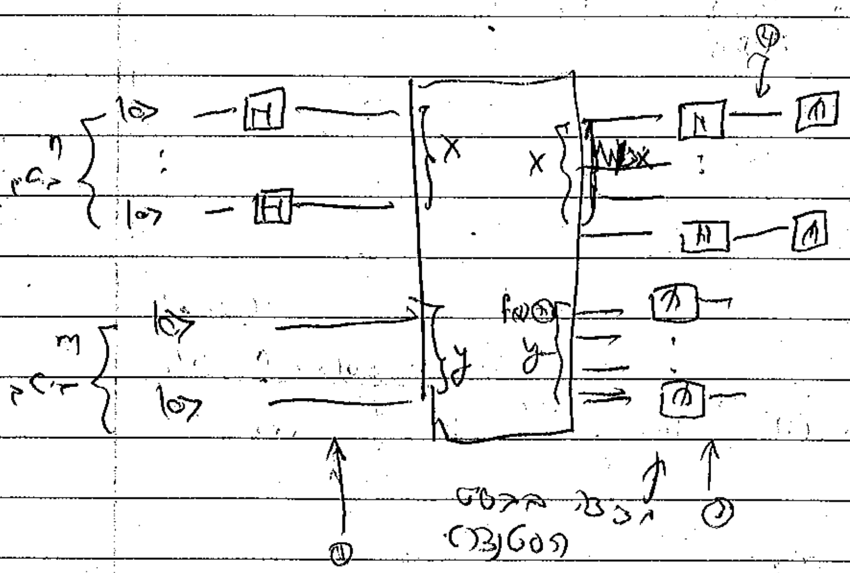
כך שלכל x $f(x) = f(x \oplus s)$

פלט: s. הערה: (בלי הרבה צורך, רק s אחד)

קלסי (דטרמיניסטי, בזמן אקספוננציאלי) בזמן קלט B.B בערך $\Omega(2^n)$

אלגוריתם קוונטי (Simon)

אלגברה בודד:



נבין 2 מצב סתם אלגברי.

המצב ב-① נתון ב $\sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle$

② $\sum_{x \in \{0,1\}^n} |x, f(x)\rangle$

אחרי המדידה ב-③ נותן מצבים עבור $w \in \{0,1\}^m$ ⑨

ולכן נקבל $\alpha\sum_{x\in R}\left(|x\rangle+|x\oplus s\rangle\right)\otimes|\tilde{z}\rangle$

כי $f(x)=f(x\oplus s)$, ולכן כל x נמצא בזוג, ...

לאחר $H^{\otimes n}$ נקבל:

$$\sum_{x\in R}\frac{\alpha}{\sqrt{2^n}}\left[\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle+\sum_{z\in\{0,1\}^n}(-1)^{(x+s)\cdot z}|z\rangle\right]$$

$$\alpha'\sum_{x\in R}\sum_{z\in\{0,1\}^n}\underbrace{\left[(-1)^{x\cdot z}+(-1)^{(x+s)\cdot z}\right]}_{\left(1+(-1)^{s\cdot z}\right)(-1)^{x\cdot z}}|z\rangle$$

בפרט, אם $s\cdot z=0$ מקבלים $1+1=2$

$(s\cdot z=1\ (2))$ אז $1-1=0$

ולכן $=\alpha''\sum_{x\in R}\sum_{z\in\{0,1\}^n\,:\,z\perp s}|z\rangle$

בפרט כשמודדים z, מקבלים z אקראי רק ש $s\perp z$.

וכך נוכל לקבל משוואות עד $s=s_1\ldots s_n$

$z_1\cdot s_1+z_2\cdot s_2+\ldots+z_n\cdot s_n=0$ מעל F_2

$\dim(S^\perp)=n-1$

סיבוכיות: לאחר $\Omega(n\log n)$ ... משוואות

... $\mathrm{poly}(n)$ ... של המשוואות

!...

הערה לסיום! ... f ... $x, x\oplus s$

... cosets ... $f(x')=f(x)$ $\Leftarrow$ $x\oplus x'\in\{0,s\}$

... $\exists s: f(x)=f(x\oplus s)$