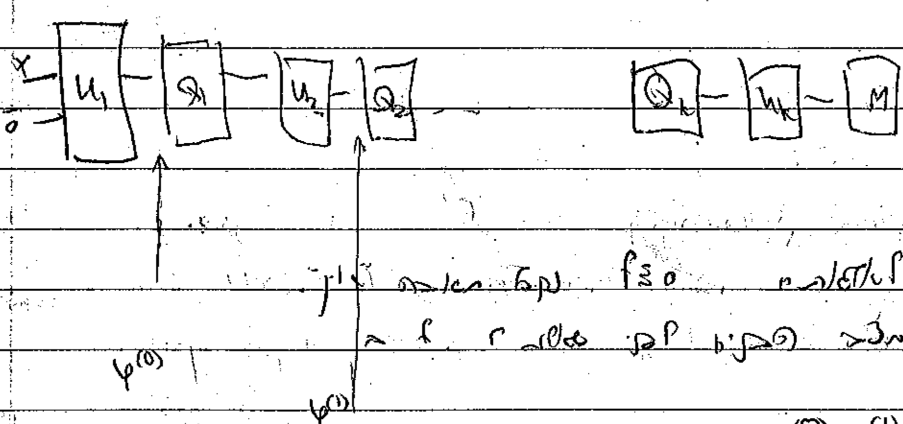
הוכחה שאי אפשר יותר מהר! BBBV 94

~~הוכחה~~ שאי אפשר לעשות את ה search עם פחות מ $\sqrt{N}$ שאלות?

נניח יש לנו אלגוריתם עם k שאלות — הסתברות גבוהה



אם נכניס לאלגוריתם, $f \equiv 0$, נקבל מצב יחיד.
נסמן את מצב הביניים לפני השאלה ה t ב

$$\varphi^{(0)}, \varphi^{(1)}, \ldots, \varphi^{(k)}$$

נסמן

$$\varphi^{(t)} = \sum_x \alpha_x^{(t)} |x, \underbrace{\xi_{x,t}}_{\text{נורמה } 1}\rangle$$

עוצמת שאלה: $|\alpha_x^{(t)}|^2$ - ההסתברות שנשאל על x בזמן t.

ידוע ש $\sum_t \sum_x |\alpha_x^{(t)}|^2 = T$

לכן יש x_0 כך ש $\sum_t |\alpha_{x_0}^{(t)}|^2 \le \frac{T}{N}$

ולכן $\sum_t |\alpha_{x_0}^{(t)}| \le \sqrt{\sum_t |\alpha_{x_0}^{(t)}|^2}\sqrt{T} \le \frac{T}{\sqrt{N}}$

~~אינטואיציה~~ אם $\sqrt{N} >> T$, אז לא שואלים מספיק על x_0

לכן אם נשנה את f ל g כך ש $g(x) = \begin{cases} 1 & x = x_0 \\ 0 & \text{אחרת} \end{cases}$

לא נוכל להבחין בין f ו g והאלגוריתם טועה.

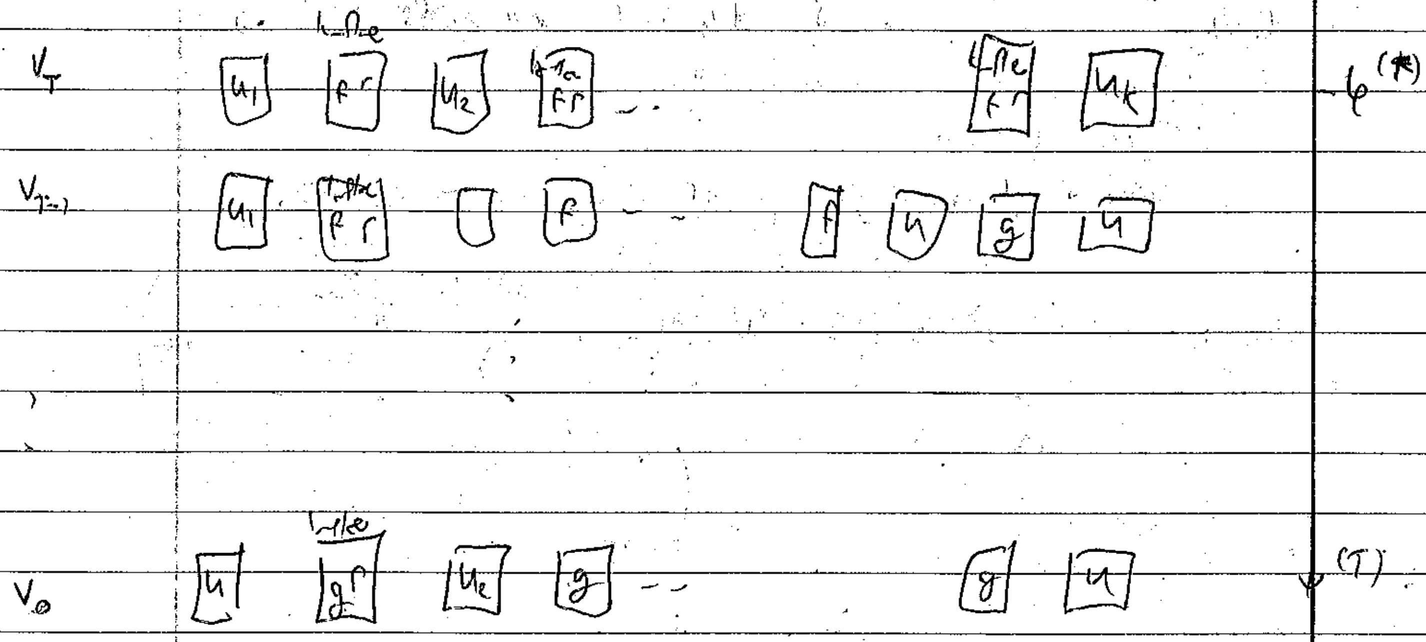
שיעור 10

(1)

נתון ש- $\psi^{(t)}, \dots, \psi^{(0)}$ הם מצבי האלגוריתם בשאילתות ל- g

מהו $\|\psi^{(T)} - \varphi^{(T)}\|$?

נעשה טיעון Hybrid



$$\|V_T - V_0\| \le \sum_{i=1}^{T} \|V_{i+1} - V_i\|$$

מהו $\|V_{i+1} - V_i\|$? – i' הפעולות הראשונות זהות, ולכן מגיעים ל- $\varphi^{(i)}$

במקרה 1 מפעילים שאילתה ל- f ומגיעים ל- $\varphi^{(i+1)}$

" 2 " " ל- g " $\bar{\varphi}$

מקבלים שההפרש רק ב- V_0 ולכן $\|Q_f \varphi^{(i)} - Q_g \varphi^{(i)}\|$

$\le 2|\alpha^{(i)}_{x_0}|$

ואח"כ מפעילים כ"א זהה, נקבל W

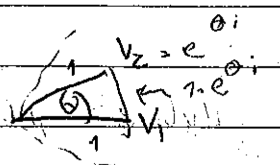
$$\|Wv_1 - Wv_2\| = \|W(v_1 - v_2)\| \le \|W\| \cdot \|v_1 - v_2\| \le \|v_1 - v_2\|$$

לסיכום $\|V_T - V_0\| \le 2\sum_{i=1}^{T} |\alpha^{(i)}_{x_0}| \le \frac{2T}{\sqrt{N}}$

כמה טוב אפשר להבדיל בין 2 מצבים קרובים?

נניח v_1, v_2 ש $\|v_1 - v_2\| \le \delta$.

[illegible]

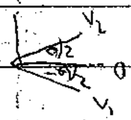


$\frac{\delta}{\sin\theta} = \frac{1}{\sin(\frac{\pi}{2} - \frac{\theta}{2})}$

$$\delta = \|v_1 - v_2\| = 2\sin\frac{\theta}{2}$$

$$\sin\frac{\theta}{2} = \frac{\delta}{2}$$

ראינו שהכי טוב שאפשר להבחין, קבוע היא



$$|v_2\rangle\langle v_2| - |v_1\rangle\langle v_1| = \begin{pmatrix} \cos^2\frac{\theta}{2} & -c(\frac{\theta}{2})s(\frac{\theta}{2}) \\ -c(\frac{\theta}{2})s(\frac{\theta}{2}) & \sin^2\frac{\theta}{2} \end{pmatrix} - \begin{pmatrix} \cos^2\frac{\theta}{2} & + \\ + & \sin^2\frac{\theta}{2} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \sin(\theta) \\ \sin(\theta) & 0 \end{pmatrix}$$

$\lambda_2 = -\lambda_1$ $\qquad -\lambda_1^2 = \lambda_1\lambda_2 = -\sin^2(\theta)$

$\lambda_{1,2} = \pm\sin(\theta)$ $\qquad |\rho_1 - \rho_2|_{tr} = |\lambda_1| + |\lambda_2| = 2\sin\theta$

ולכן הסתברות ההצלחה היא $\left(\frac{1}{2} + \frac{|\rho_1 - \rho_2|}{4}\right.$ או $\left.\frac{1}{2} - \frac{|\rho_2 - \rho_1|}{4}\right)$

ולכן נקבל $\sin\theta = \frac{|\rho_1 - \rho_2|}{2}$.

$$|\sin\theta| = 2|\sin\tfrac{\theta}{2}||\cos\tfrac{\theta}{2}| \le |2\sin\tfrac{\theta}{2}| \le \delta$$ ∎

ולכן, אם רוצים הסתברות הצלחה קבועה צריך

$$\frac{2T}{\sqrt{N}} = \Theta(1)$$

$$\boxed{T = \Theta(\sqrt{N})}$$ ∎

לסיכום ראינו שאפשר לפתור את חיפוש ב-$\sqrt{N}$ צעדים? BBBV:
מה זה אומר ומה זה לא.

3

מה ראינו עד כה?

סוג הפרדה	קוונטי	קלאסי		
פקטור	1	2 שאילתות	$f:\{0,1\}\to\{0,1\}$	דויטש
[illegible]	1	$\Omega(2^n)$	f קבועה או מאוזנת	DJ
[illegible]	$\Theta(n)$	$\Omega(2^n)$	מוצא s כך ש $f(x)=f(x\oplus s)$	Simon
	$\Theta(\log n)$	$\Omega(n)$	הפרש בזמן ריצה	Order finding
	1	$\Omega(n)$?	query complexity	DLOG
ריבועי	$\Theta(2^{n/2})$	$\Omega(2^n)$	Or	Grover

> האם לכל $f:\{0,1\}^n\to\{0,1\}$ תמיד, יש פער אקספוננציאלי בין סיבוכיות ה-BD של המודל הקוונטי והקלאסי?

מודל הקלאסי:
נחשוב על f כמחרוזת באורך 2^n מתנים $x_0,\dots,x_{N-1}$
x_l הערך של f על l
כש l מספר בין 0 ל $N-1$, מחרוזות ...

f_0 ... f_{N-1}

מודל הקלאסי דטרמיניסטי, פרוטוקול (עבור f) הוא Decision tree

x_a query → x_a
תשובה 0 או 1 → 0 / 1
x_{a_0} query → x_{a_0}

סיבוכיות הוא היא עומקו
מס' השאלות המרבי
שמתשאל מס' שאילתות
מקסימלי.

נסמן סיבוכיות זו ב $D(f)$ (4)

$f(x_0,\dots,x_{N-1})$ 0 או 1 עלים

פרוטוקול הסתברותי: בוחר שאלות מתוך התפלגות, מקבל תשובה, וממשיך.

התפלגות על פרוטוקולים דטרמיניסטיים.

$R_2(f)$ - סיבוכיות פרוטוקול הסתברותי:
לכל f, מוציא בהסתברות $\geq \frac{2}{3}$ את התשובה הנכונה. ([illegible])
[illegible]

<u>מודל קוונטי</u>: אלגו' קוונטי עם הצלחה $\geq \frac{2}{3}$.
$Q(f)$ - מס' שאלות מינ' הנדרש.

דוגמאות:

$Q(f)$	$D(f)$	
1	2	XOR, $f:\{0,1\}^2 \to \{0,1\}$, $f(x,y)=x\oplus y$
$Q(f)=\Theta(\sqrt{N})$	$D(f)=N$ $R_2(f)=\Omega(N)$	$OR(x_0,\dots,x_{N-1})$

במודל הקוונטי, יש אפיון (עד כדי פולינום) לפרמטרים $D(f)$, $Q_2(f)$.

<u>הגדרה</u>: יהי $I\subseteq[N]$, נסמן ב- X_I את המונום
$$x_1^{i_1} x_2^{i_2} \cdots x_N^{i_N}$$
כאשר $i_j=1$ אם $j\in I$
$i_j=0$ אם $j\notin I$

נסמן גם: $\mathbb{C}[\mathbb{Z}_2^N]$

בסיס אחד הוא הסטנדרטי (פונקציות מציינות $\mathbb{Z}_2^N$) של כל ה $f_x(y)=\begin{cases}1 & x=y\\ 0 & \text{אחרת}\end{cases}$

ובסיס אחר הוא של הקרקטרים

$$\chi_S(y)=(-1)^{S\cdot y}=\prod_{j\in S}(-1)^{y_j}$$

בסיס אחר, הוא של הפונק' χ_I עבור $I\subseteq[N]$,

[$\chi_I((-1)^{y_1},\dots,(-1)^{y_N})=(-1)^{y\cdot I}=\chi_I(y_1,\dots,y_N)$ שים לב ש]

(א) לכל I, $\chi_I\in\mathbb{C}[\mathbb{Z}_2^N]$

(ב) הם פורשים את $\mathbb{C}[\mathbb{Z}_2^N]$

כי: תהי $f:\mathbb{Z}_2^N\to\mathbb{C}$

טבלת ערכי f

$0\dots0$	$e_{00\dots0}$
$1\dots1$	e_{11}

$$f=\sum_x f(x)\cdot f_x$$

וכל f_x אפשר לרשום כ $f_x(y)=\prod_{i=1}^{N}\left(1-(y_i-x_i)\right)$

וכך נכתוב לפי χ_I.

$$f=\sum_I \alpha_I\chi_I$$

המקדמים הנ"ל של f.

הגדרה: תהי $f:\mathbb{Z}_2^N\to\mathbb{C}$.

נגיד ש $\deg(f)=k$, אם דרגת הפולינום הנ"ל של f היא k.

נגיד ש $\widetilde{\deg}(f)=k$, אם הדרגה המינימלית של פולינום p ש $\frac{1}{3}$ מקרב את f, היא k.

p $\frac{1}{3}$ מקרב את f, אם לכל $x\in\mathbb{Z}_2^N$, $|p(x)-f(x)|\le\frac{1}{3}$.

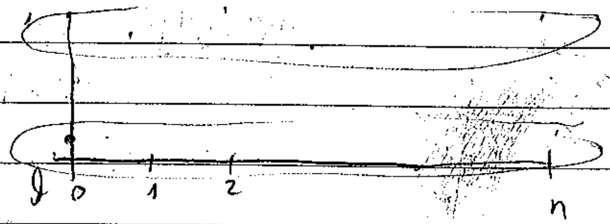
<u>דוגמא:</u> $OR: \{0,1\}^N \to \{0,1\}$ $\quad OR(\bar{0}) = 0$
אחרת $OR(x) = 1$

$OR(x_1 \ldots x_N) = 1 - (1-x_1) \cdots (1-x_N)$
$\deg(OR) = N$

$\widetilde{OR}$: נקרא לו פונקציה $l: \{0, \ldots, N\} \to \{0,1\}$

$l(0) \approx 0$
$l(i) \approx 1 \quad i > 0$

ונגדיר
$p(x_1 \ldots x_n) = l(\sum x_i)$



יש l כזה עם דרגה $\Theta(\sqrt{N})$.

ולכן $\widetilde{\deg}(OR) = \Theta(\sqrt{N})$.

<u>משפט ([illegible]):</u> לכל f: $\quad \deg(f) \leq D(f) \leq 2(\deg(f))^4$

$\widetilde{\deg}(f) \leq R_2(f) \leq 216 \, (\widetilde{\deg}(f))^6$

<u>משפט ([illegible]):</u> לכל f $\quad D(f) \geq Q_E(f) \geq \frac{\deg(f)}{2}$

[illegible]

$Q_2(f) \geq \frac{\widetilde{\deg}(f)}{2}$

ומסקנה $Q_2(f) \ge \Omega(\widetilde{\deg}(f)) = \Omega\left((R_2(f))^{1/6}\right)$

וגם $Q_2(OR) \ge \frac{\widetilde{\deg}(OR)}{2} = \Omega(\sqrt{N})$!

$Q_E(f) \ge \Omega(\deg(f)) = \Omega\left((D(f))^{1/4}\right)$

וכן, עבור f טוטלית $f:\{0,1\}^N \to \{0,1\}$

אין פערים יותר מפולינומיאליים בין סיבוכיות קוונטית לקלאסית.

אם f עם הבטחה (כלומר f חלקית)

ייתכנו פערים אקספוננציאליים, למשל עבור הבעיה של Simon.

הוכחה: נניח שיש לנו אלגוריתם $U_0, O_0, U_1, \ldots, U_T O_T$

המצב ההתחלתי $\bar{0}$ (כי אפשר להכניס אותו כחלק מ U_0)

כמו קודם נסמן ב $\varphi^{(i)}$ את המצב בזמן i.

$$\varphi^{(i)} = \sum_w \alpha_w^{(i)} |w\rangle$$

המקדמים $\alpha_w^{(i)}$ תלויים בקלט $o_1, \ldots, o_N$ (התשובות לאורקל)

והם הם פונק',

לכל w, i: $\alpha_w^{(i)} : \{0,1\}^N \to \mathbb{C}$

ואנו מעוניינים ב $\deg(\alpha_w^{(i)})$.

$\boxed{\text{למה: לכל } t, w \text{ מתקיים } \deg(\alpha_w^{(t)}) \le t}$

הוכחה: $\alpha_w^{(0)}$ קבועים, ולכן $\deg(\alpha_w^{(0)}) = 0$.

– נניח כי נכון עבור t, ונוכיח עבור t+1 ע"י אינדוקציה

כל $\alpha_w^{(t+1)}$ תלוי לינארית ב $\alpha_x^{(t)}$, ולכן $\alpha_w^{(t+1)}$

$$\deg(\alpha_w^{(t+1)}) \le t$$

אם הקוונטי מגיע t לצעד t+1 ע"י קריאה
לאורקל O, אזי

$$\alpha_{w=(x,0)}^{(t+1)}(|x,0\rangle) = \begin{cases} |x,0\rangle & O_x=0 \\ |x,1\rangle & O_x=1 \end{cases}$$

$$\alpha_w^{(t+1)}(|x,1\rangle) = \begin{cases} |x,1\rangle & O_x=0 \\ |x,0\rangle & O_x=1 \end{cases}$$

$$\alpha_w^{(t+1)} =$$

w מצב שבו x, וביט b משוחרר (לפני האורקל)
w' " " " 1-b "

$$\alpha_w^{(t+1)} = \underbrace{(1-O_x)}\,\alpha_w^{(t)} + \underbrace{O_x}\,\alpha_{w'}^{(t)}$$

1 אם נשאר 0   1 אם השתנה
0 אחרת   0 אחרת

לכן $t+1 \ge 1+\deg(\alpha_w^{(t)}) \ge \deg(\alpha_w^{(t+1)})$

בסוף, ההסתברות שנקבל 1 היא $\sum_{w\ \text{מקבל}} |\alpha_w^{(T)}|^2$

לכן פולינום מדרגה $\le 2T$.

מצאנו פולינום שמחשב [illegible] $a_1 \ldots a_N$ אם $f(a_1 \ldots a_N)=1$
ההסתברות [illegible] גדולה, ואחרת ההסתברות [illegible]

כלומר מצאנו פולינום ב $O_1,\dots,O_N$ ממעלה $\le 2T^*$

שמחשב $f(O_1 \dots O_N)$, ולכן $\deg(f) \le 2T^*$

$Q_E(f) \ge \frac{\deg(f)}{2}$ $\qquad$ $T \ge \frac{\deg(f)}{2}$

אם אנו מחשבים f עם שגיאה $\frac{1}{3}$

אז עבור $O_1,\dots,O_N$ עם $f(O_1 \dots O_N)=1$ ($=0$) הסתברות $\ge \frac{2}{3}$ ($\le \frac{1}{3}$)

ולכן מצאנו פולינום ממעלה $\le 2T$ שמקרב f

ולכן $\widetilde{\deg}(f) \le 2T$ $\qquad$ $Q_2(f) \ge T \ge \frac{\widetilde{\deg}(f)}{2}$ ∎

סיבוכיות תקשורת

יש שני שחקנים A, B

A יודע קלט מ X

B " " מ Y

ורוצים לחשב ביחד פונקציה $f: X \times Y \to \{0,1\}$

פרוטוקול:

A שולח ביט

B " "

⋮

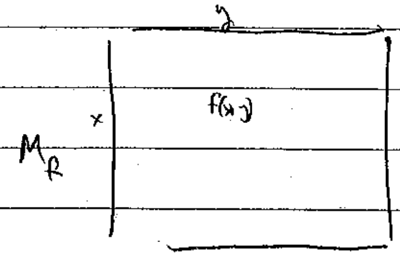
ובסוף מחליטים על תשובה.

פרוטוקול יכול להיות דטרמיניסטי / הסתברותי / קוונטי

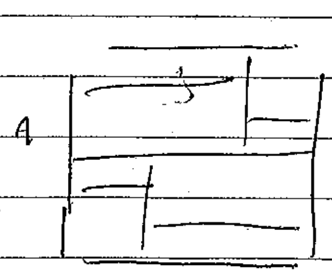
דטרמיניסטי: לכל קלט $x \in X$, $y \in Y$ בסוף הפרוטוקול ש.א. יודעים $f(x,y)$

$D(f)$ - מס' ביטים הנדרש בפרוטוקול הטוב ביותר ל f.

M_f



פרוטוקול:



אפשר לחלק המטריצה למלבנים מונוכרומטיים.

מס' המלבנים $\leq 2^{\text{מס' ביטים}}$

$\boxed{D(f) \geq \lg Rank(M_f)}$ $\quad rank(M_f) \leq$ מס' המלבנים $\leq 2^{D(f)}$

הגדרה:

$R_\varepsilon(f)$ — A,B פרוטוקול הסתברותי

לכל $x \in X$, $y \in Y$

$$\Pr_{\text{מטבעות } A,B}[\text{מוציא נכון}] \geq 1-\varepsilon$$

דוגמה 1:

$EQ: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

ראינו: $D(EQ) = n$

$R_{\frac{1}{3}}(EQ) = O(\lg n)$

($A \to B$ $p, x \bmod p$
ראשוני p
בתחום $[1,n^2]$
(ECC :פתרון נוסף

דוגמה 2:

$IP: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$$IP(x_1,\ldots,x_n, y_1,\ldots,y_n) = \sum_{i=1}^{n} x_i y_i \pmod 2 = \bigoplus (x_i \wedge y_i)$$

$D(IP) = n$

$R_{\frac{1}{3}}(IP) = \Omega(n)$

דוגמה 3:

$$DISJ(x_1,\ldots,x_n, y_1,\ldots,y_n) = \begin{cases} 1 & \exists i\; x_i \wedge y_i \\ 0 & \text{אחרת} \end{cases}$$

$D(DISJ) = n$

$R_{\frac{1}{3}}(DISJ) = \Omega(n)$

$\underline{Q(f)}$

מודל קוונטי, מקבלים קוד קוונטי

ובכך של $x \oplus X$, $x \oplus y$

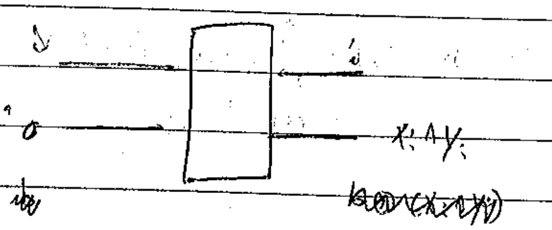
$$\Pr_{\text{על כל } x}\left[\text{מוציאים } A,B \text{ נכון}\right] \geq 1-\varepsilon$$

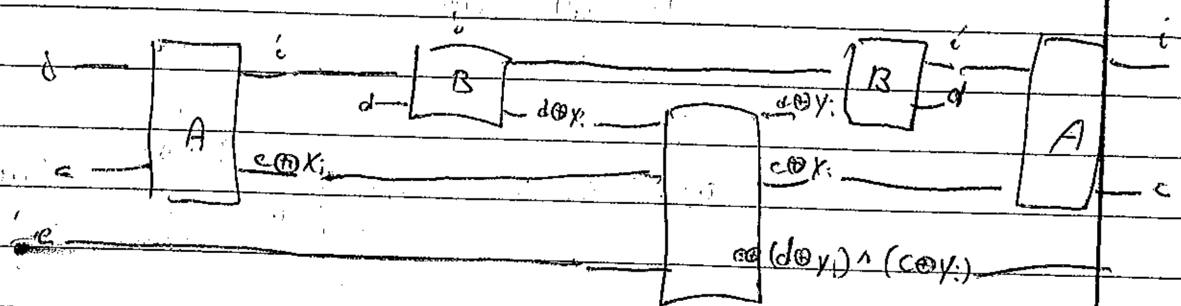
$Q_\varepsilon(f)$

משפט BCW $\quad Q_{\frac{1}{3}}(DISJ) = O(\sqrt{n}\lg n)$

הוכחה: נריץ את האלגוריתם של Grover על $z_i = (x_i \wedge y_i)$

מאיפה מקבלים z_i?





ביחד $O(\lg n)$ ... בכל סיבוב

, $O(\sqrt{n}\lg n)$ סה"כ

משפט (תזכורת) $\quad Q_{\frac{1}{3}}(DISJ) = \Omega(\sqrt{n})$

הוכחה לא ⓑ