פתרון תרגיל בקוונטים

שם: מיכאל גרינבאום, **ת.ז:** 211747639

12 בספטמבר 2021

1. **צ"ל:** אלגוריתם שמעביר לכל היותר $O\left(\sqrt{n}\log\left(n\right)\right)$ קיוביטים
הוכחה:
נניח שהאורקל הוא אליס למען הפשטות (בכל מקרה להעביר את הקלט לאליס ומאליס זה $O\left(\log\left(n\right)\right)$).
נגדיר פונקציות עזר $f:\{0,1\}^{\lceil\log_2(n)\rceil+n}\to\{0,1\}^{\lceil\log_2(n)\rceil+1}, g:\{0,1\}^{(\lceil\log_2(n)\rceil+1)+n}\to\{0,1\}$ באופן הבא:

1.1

$$f\left(k,x\right)=\begin{cases}k & x_k=1\\ k+n & x_k=0\end{cases}$$

$$g\left(k,y\right)=\begin{cases}0 & k>n\\ 0 & y_k=0\\ 1 & y_k=1\end{cases}$$

כש־ $n=|y|=|x|$ ו־ k הוא שאר הביטים (ב־ f זה $\lceil\log_2\left(n\right)\rceil$ וב־ g זה $2\cdot\lceil\log_2\left(n\right)\rceil$),
נשים לב כי

$$g\left(f\left(k,x\right),y\right)=x_k\wedge y_k$$

נתאר את האלגוריתם של האורקל:

(א) בהינתן $|\,k\rangle$ כקלט לאליס
(ב) אליס תחשב את

$$|\,k,\underbrace{0,\ldots,0}_{\lceil\log_2(n)\rceil+1},0\rangle\to|\,k,\underbrace{0,\ldots,0}_{\lceil\log_2(n)\rceil+1}\oplus f\left(k,x\right),0\rangle=|\,k,f\left(x,k\right),0\rangle$$

(ג) היא תשלח לבוב את המצב $|\,k,f\left(x,k\right),0\rangle$
(ד) בוב יריץ את המעגל

$$|\,k,f\left(x,k\right),0\rangle\to|\,k,f\left(x,k\right),0\oplus g\left(f\left(x,k\right),y\right)\rangle=|\,k,f\left(x,k\right),x_k\wedge y_k\rangle$$

(ה) בוב יריץ את המעגל

$$|\,k,f\left(x,k\right),x_k\wedge y_k\rangle\to|\,\left(-1\right)^{x_k\cdot y_k}k,f\left(x,k\right),x_k\wedge y_k\rangle$$

(ו) בוב יינקה את $x_k\wedge y_k$ ויישלח את המצב לאליס
(ז) אליס תקבל את $|\,\left(-1\right)^{x_k\cdot y_k}k,f\left(x,k\right),0\rangle$, תנקה את $f\left(x,k\right)$ ותשלח את המצב המתקבל אחרי מדידה כתשובת האורקל (שזה המצב $|\,\left(-1\right)^{x_k\cdot y_k}k\rangle$)

נשים לב שבמקרה והמצב הוא $| \alpha\rangle = \sum_{k\le n}\alpha_k\cdot | k\rangle$, רצף הפעולות שתיארנו יעביר אותו למצב

$$\sum_{k\le n}(-1)^{x_k\cdot y_k}\cdot\alpha_k\cdot | k\rangle$$

באופן דומה למה שקרה במקרה של מצב טהור
כלומר הראנו אורקל שמקיים $\mathcal{O}(| \alpha\rangle)=\mathcal{O}\left(\sum_{k\le n}\alpha_k\cdot | k\rangle\right)=\sum_{k\le n}(-1)^{x_k\cdot y_k}\alpha_k\cdot | k\rangle$ כנדרש.
נשים לב שבכל פנייה לאורקל מתבצע מספר קבוע של שליחות קיוביטים בין בוב לאליס ובכל שליחה נשלחים לכל היותר $2\lceil\log(n)\rceil+2$ קיוביטים ולכן יוצא שבסך הכל ששלחנו $O(\log(n))$ קיוביטים.
נגדיר $z:\{0,1\}^{\lceil\log_2(n)\rceil}\to\{0,1\}$ באופן הבא $z(k)=x_k\cdot y_k$
כלומר הראנו אורקל שמקיים

$$\mathcal{O}(| \alpha\rangle)=\mathcal{O}\left(\sum_{k\le n}\alpha_k\cdot | k\rangle\right)=\sum_{k\le n}(-1)^{x_k\cdot y_k}\alpha_k\cdot | k\rangle=\sum_{k\le n}(-1)^{z(k)}\alpha_k\cdot | k\rangle$$

ששולח לכל היותר $O(\log(n))$ קיוביטים.
עתה נוכל להשתמש באלגוריתם גרובר שמניח שיש פונקציית אורקל כזו וב־ $O\left(\sqrt{2^{\lceil\log_2(n)\rceil}}\right)=O(\sqrt{n})$ איטרציות הוא יחזיר בהסתברות גבוהה האם $1\le\exists k\le n$ כך ש־ $x_k\cdot y_k=z(k)=1$.
נזכר שגרובר ניגש לאורקל לכל היותר פעם אחת בכל איטרציה ולכן ניגש לאורקל לכל היותר $O(\sqrt{n})$ פעמים ובכל פעם נשלח $O(\log(n))$ קיוביטים ולכן בכלליות נשלח לכל היותר $O(\sqrt{n}\cdot\log(n))$ קיוביטים.
כלומר הראנו אלגוריתם שמוצא בהתסברות גבוהה האם $1\le\exists k\le n$ כך ש־ $x_k\cdot y_k=1$ השולח לכל היותר $O(\sqrt{n}\cdot\log(n))$ קיוביטים.
כלומר האלגוריתם שמצאנו הוא להריץ את אלגוריתם גרובר עם האורקל שהצגנו מלעיל ולהחזיר את התשובה של גרובר.

הערה: אם n לא חזקה של 2, נרפד את n לחזקה של 2 ונדרוש ש־ $g(k,y)$ יחזיר 0 כאשר $n<k\le 2^{\lceil\log_2(n)\rceil}$ ו־ $2^{\lceil\log_2(n)\rceil}+n<k\le 2^{\lceil\log_2(n)\rceil}+2^{\lceil\log_2(n)\rceil}$. בנוסף לכך מה ש־ f יוסיף ל־ k יהיה $2^{\lceil\log_2(n)\rceil}$. זה לא משנה כלל את נכונות האלגוריתם \ סדר גודל של הקיוביטים שנשלחים אבל מבטיח שאם האורקל יקבל $n<k\le 2^{\lceil\log_2(n)\rceil}$ הוא יחזיר את k. זה חשוב כי האלגוריתם של גרובר מתחיל מספורפוזיציה של כל המצבים אז בהינתן מצב שאין לו אינדקס בוקטור, נחזיר $(-1)^0\cdot k$ ששקול לכך שלא נמצא אותו כפתרון באלגוריתם גרובר ולכן הוא עדיין יחזיר רק האם $1\le\exists k\le n$ כך ש־ $x_k\cdot y_k=1$.

מ.ש.ל.☺

2. **פתרון:**

(א) **צ"ל:** להראות שההסתברות למדוד 0 היא $\frac{1+\left(\langle\phi_x|\phi_y\rangle^2\right)}{2}$
הוכחה:
נשים לב כי בהתחלה היה לנו $| 0,\phi_x,\phi_y\rangle$,
לאחר הפעלת H הראשון, נקבל $| \frac{|0\rangle+|1\rangle}{\sqrt{2}},\phi_x,\phi_y\rangle=\frac{1}{\sqrt{2}}\left[| 0,\phi_x,\phi_y\rangle+| 1,\phi_x,\phi_y\rangle\right]$,
לאחר הפעלת ה־ $controlled-swap$ נקבל $\frac{1}{\sqrt{2}}\left[| 0,\phi_x,\phi_y\rangle+| 1,\phi_y,\phi_x\rangle\right]$,
לאחר הפעלת ה־ H השני נקבל

$$\begin{aligned}&\frac{1}{2}\cdot\left(| 0,\phi_x,\phi_y\rangle+| 1,\phi_x,\phi_y\rangle+| 0,\phi_y,\phi_x\rangle-| 1,\phi_y,\phi_x\rangle\right)\\&=\frac{1}{2}\cdot\left(| 0\rangle\left[| \phi_x,\phi_y\rangle+| \phi_y,\phi_x\rangle\right]+| 1\rangle\left[| \phi_x,\phi_y\rangle-| \phi_y,\phi_x\rangle\right]\right)\end{aligned}$$

כשנמדוד, ההסתברות שנפגוש 0 היא

$$\begin{aligned}
&\left\|\frac{1}{2}\cdot\left(|\ \phi_x,\phi_y\rangle+|\ \phi_y,\phi_x\rangle\right)\right\|^2\\
&=\frac{1}{2}\left(|\ \phi_x,\phi_y\rangle+|\ \phi_y,\phi_x\rangle\right)^*\cdot\frac{1}{2}\left(|\ \phi_x,\phi_y\rangle+|\ \phi_y,\phi_x\rangle\right)\\
&=\frac{1}{4}\cdot\left(\langle\phi_x,\phi_y\ |+\langle\phi_y,\phi_x\ |\right)\cdot\left(|\ \phi_x,\phi_y\rangle+|\ \phi_y,\phi_x\rangle\right)\\
&=\frac{1}{4}\cdot\left(\langle\phi_x,\phi_y\ |\ \phi_x,\phi_y\rangle+\langle\phi_x,\phi_y\ |\ \phi_y,\phi_x\rangle+\langle\phi_y,\phi_x\ |\ \phi_x,\phi_y\rangle+\langle\phi_y,\phi_x\ |\ \phi_y,\phi_x\rangle\right)\\
&=\frac{1}{4}\cdot\left(1+|\langle\phi_x\ |\ \phi_y\rangle|^2+|\langle\phi_x\ |\ \phi_y\rangle|^2+1\right)=\frac{1+|\langle\phi_x\ |\ \phi_y\rangle|^2}{2}
\end{aligned}$$

כלומר הראנו שהסתברות למדוד 0 היא בדיוק $\frac{1+|\langle\phi_x|\phi_y\rangle|^2}{2}$, כנדרש

מ.ש.ל.א.☺

(ב) **צ"ל:** להראות שקיים $c\left(\varepsilon\right)$ כך ש־ $|\langle\phi_k\ |\ \phi_j\rangle|<\varepsilon$ לכל $j\neq k$ כאשר יש $\phi_1,\ldots\phi_{2^{m\cdot c(\varepsilon)}}$

הוכחה:

יהי $\varepsilon>0$, נגדיר $\boxed{c\left(\varepsilon\right)=\frac{1}{2}\cdot\frac{\varepsilon^2}{4\cdot\ln\left(2\right)}}$,

לכל k, נגדיר $\phi_k=\frac{1}{\sqrt{m}}\sum_{i=1}^{m}X_{i,k}\cdot|\ i\rangle$ כאשר $X_{i,k}$ משתנה אקראי שמקיים $\mathbb{P}\left(X_{i,k}=\pm1\right)=\frac{1}{2}$,

יהיו k,j, נשים לב כי

$$\langle\phi_k\ |\ \phi_j\rangle=\frac{1}{m}\sum_{i=1}^{m}X_{i,k}\cdot X_{i,j}=\frac{1}{m}\sum_{i}\begin{cases}1 & X_{i,k}=X_{i,j}\\ -1 & X_{i,k}\neq X_{i,j}\end{cases}$$

נגדיר $X_{i,j,k}=X_{i,k}\cdot X_{i,j}$, נשים לב כי

$$\mathbb{P}\left(X_{i,j,k}=1\right)=\mathbb{P}\left(X_{i,k}=X_{i,j}\right)=\frac{1}{2}\wedge\mathbb{P}\left(X_{i,j,k}=-1\right)=\mathbb{P}\left(X_{i,k}\neq X_{i,j}\right)=\frac{1}{2}$$

ונקבל כי $\langle\phi_k\ |\ \phi_j\rangle=\frac{1}{m}\sum_{i=1}^{m}X_{i,j,k}$ וגם נשים לב כי $\mathbb{E}\left[X_{i,j,k}\right]=0$ ולכן

$$\mathbb{E}\left[\frac{1}{m}\sum_{i=1}^{m}X_{i,j,k}\right]=\frac{1}{m}\cdot\mathbb{E}\left[\sum_{i=1}^{m}X_{i,j,k}\right]=\frac{1}{m}\cdot\sum_{i=1}^{m}\mathbb{E}\left[X_{i,j,k}\right]=\frac{1}{m}\cdot0=0$$

נשים לב כי

$$\varepsilon\leq|\langle\phi_k\ |\ \phi_j\rangle|=\left|\frac{1}{m}\sum_{i=1}^{m}X_{i,j,k}\right|=\left|\frac{1}{m}\cdot\sum_{i=1}^{m}X_{i,j,k}-0\right|=\left|\frac{1}{m}\cdot\sum_{i=1}^{m}X_{i,j,k}-\mathbb{E}\left[\frac{1}{m}\sum_{i=1}^{m}X_{i,j,k}\right]\right|$$

נשים לב כי $X_{i,j,k}\in[-1,1]$ ולכן נקבל כי

$$\begin{aligned}
\mathbb{P}\left(|\langle\phi_k\ |\ \phi_j\rangle|\geq\varepsilon\right)&=\mathbb{P}\left(\left|\frac{1}{m}\cdot\sum_{i=1}^{m}X_{i,j,k}-\mathbb{E}\left[\frac{1}{m}\sum_{i=1}^{m}X_{i,j,k}\right]\right|\geq\varepsilon\right)\\
&\overset{\text{hoeffding}}{\leq}2\cdot e^{-\frac{2\cdot m^2\cdot\varepsilon^2}{\sum_{i=1}^{m}(1-(-1))^2}}=2\cdot e^{-\frac{\varepsilon^2\cdot m}{2}}
\end{aligned}$$

עתה נקבל כי

4.1

4.2

$$
\begin{aligned}
\mathbb{P}\left(\forall k,j \to |\langle \phi_k \mid \phi_j \rangle| < \varepsilon\right) &= 1 - \mathbb{P}\left(\exists k,j \to |\langle \phi_k \mid \phi_j \rangle| \geq \varepsilon\right) \\
&\overset{\text{union bound}}{\geq} 1 - \sum_{k \neq j} \mathbb{P}\left(|\langle \phi_k \mid \phi_j \rangle| \geq \varepsilon\right) \\
&\geq 1 - \sum_{k,j} \cdot 2 \cdot e^{-\frac{\varepsilon^2}{2}} = 1 - \frac{2^{c(\varepsilon)\cdot m} \cdot \left(2^{c(\varepsilon)\cdot m} - 1\right)}{2} \cdot 2 \cdot e^{-\frac{\varepsilon^2 \cdot m}{2}} \\
&\geq 1 - \frac{2^{c(\varepsilon)\cdot m} \cdot 2^{c(\varepsilon)\cdot m}}{2} \cdot 2 \cdot e^{-\frac{\varepsilon^2 \cdot m}{2}} \\
&= 1 - 2^{2\cdot c(\varepsilon)\cdot m} \cdot e^{-\frac{\varepsilon^2 \cdot m}{2}} = 1 - e^{\ln\left(2^{2\cdot c(\varepsilon)\cdot m}\right)} \cdot e^{-\frac{\varepsilon^2 \cdot m}{2}} \\
&= 1 - e^{\ln(2)\cdot(2\cdot c(\varepsilon)\cdot m)} \cdot e^{-\frac{\varepsilon^2}{2}\cdot m} = 1 - e^{\left[\ln(2)\cdot 2\cdot c(\varepsilon) - \frac{\varepsilon^2}{2}\right]\cdot m}
\end{aligned}
$$

נשים לב כי

$$
\ln(2) \cdot 2 \cdot c(\varepsilon) - \frac{\varepsilon^2}{2} < 0 \iff c(\varepsilon) < \frac{\varepsilon^2}{4 \cdot \ln(2)}
$$

נזכר שבחרנו $\frac{\varepsilon^2}{4\cdot\ln(2)} > \frac{1}{2} \cdot \frac{\varepsilon^2}{4\cdot\ln(2)} = c(\varepsilon)$ ולכן

4.3

$$
\mathbb{P}\left(\forall k,j \to \langle \phi_k \mid \phi_j \rangle < \varepsilon\right) > 1 - e^{-0\cdot m} = 1 - 1 = 0
$$

כלומר יש הסתברות לא אפסית (ואפשר לבחור מקדמים (לדוגמא $c(\varepsilon) = \frac{\varepsilon^2 - \varepsilon}{4\cdot\ln(2)}$ כך שתשאף ל- 1 כפונקציה של m) למציאת $\phi_1, \ldots \phi_{2^{c(\varepsilon)\cdot m}}$ שכולם כמעט אורתוגונליים ולכן קיים בסיס כנ"ל, אחרת ההסתברות לכך הייתה 0. בנוסף לכך, נשים לב ש- $c(\varepsilon)$ לא תלוי ב- m.

נוכל להראות חסם אחר על ידי שימוש בצ'רנוף:
נגדיר $Y_{i,j,k} = \frac{1 + X_{i,k}\cdot X_{i,j}}{2}$, נשים לב כי

$$
\mathbb{P}\left(Y_{i,j,k} = 1\right) = \mathbb{P}\left(X_{i,k} = X_{i,j}\right) = \frac{1}{2} \wedge \mathbb{P}\left(Y_{i,j,k} = 0\right) = \mathbb{P}\left(X_{i,j} \neq X_{i,k}\right) = \frac{1}{2}
$$

כלומר $Y_{i,j,k} \sim Ber\left(\frac{1}{2}\right)$ וגם מתקיים

$$
\begin{aligned}
\varepsilon \leq |\langle \phi_k \mid \phi_j \rangle| = \left|\frac{1}{m}\sum_{i=1}^{m} X_{i,k} \cdot X_{i,j}\right| &\overset{Y_{i,j,k} = \frac{1 + X_{i,k}\cdot X_{i,j}}{2}}{=} \left|\frac{1}{m}\sum_{i=1}^{m} \left(2 \cdot Y_{i,j,k} - 1\right)\right| \\
\iff \sum_{i=1}^{m} Y_{i,j,k} \geq \frac{m}{2} \cdot (1+\varepsilon) &\vee \sum_{i=1}^{m} Y_{i,j,k} \leq \frac{m}{2} \cdot (1-\varepsilon)
\end{aligned}
$$

מצוין

נשים לב כי $\mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] = \sum_{i=1}^{m} \mathbb{E}\left[Y_{i,j,k}\right] = \frac{m}{2}$ ולכן נוכל לכתוב באופן הבא:

$$
\varepsilon \leq |\langle \phi_k \mid \phi_j \rangle| \iff \sum_{i=1}^{m} Y_{i,j,k} \geq \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \cdot (1+\varepsilon) \vee \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \leq \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \cdot (1-\varepsilon)
$$

ולכן נקבל כי

$$
\begin{aligned}
\mathbb{P}\left(|\langle \phi_k \mid \phi_j \rangle| \geq \varepsilon\right) &= \mathbb{P}\left(\sum_{i=1}^{m} Y_{i,j,k} \geq \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \cdot (1+\varepsilon) \vee \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \leq \frac{m}{2} \cdot (1-\varepsilon)\right) \\
&\overset{\text{union bound}}{\leq} \mathbb{P}\left(\sum_{i=1}^{m} Y_{i,j,k} \geq \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \cdot (1+\varepsilon)\right) + \mathbb{P}\left(\mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \leq \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right] \cdot (1-\varepsilon)\right) \\
&\overset{\text{chernoff}}{\leq} e^{-\frac{\varepsilon^2 \cdot \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right]}{3}} + e^{-\frac{\varepsilon^2 \cdot \mathbb{E}\left[\sum_{i=1}^{m} Y_{i,j,k}\right]}{2}} = e^{-\frac{5}{6}\cdot\varepsilon^2\cdot\frac{m}{2}} = e^{-\frac{5\varepsilon^2}{12}\cdot m}
\end{aligned}
$$

ולאחר הפיתוח שעשינו קודם עם החסם החדש נקבל שהדרישה היא

$$\ln(2)\cdot 2\cdot c(\varepsilon)-\frac{5\varepsilon^2}{12}<0 \iff \boxed{c(\varepsilon)<\frac{5\varepsilon^2}{24\cdot\ln(2)}}$$

הצגתי קודם את הפתרון של הופדינג כי לדעתי הוא יותר אלגנטי ולאחר מכן צירפתי את הפתרון לפי הרמז.

מ.ש.ל.ב.☺

(ג) **צ"ל:** אלגוריתם ששוגה לכל היותר ב־ $\frac{1}{100}$

הוכחה:

נגדיר כמו ברמז $\varepsilon=\frac{1}{2}$, $m=\frac{n}{c(\varepsilon)}$, לכן מהסעיף הקודם קיימים $\phi_1,\ldots,\phi_{2^{c(\varepsilon)\cdot m=n}}$ כך ש־ $|\langle\phi_i\mid\phi_j\rangle|\le\varepsilon$ לכל $i\neq j$ בהינתן שאליס ובוב יקבלו x,y, הם יחזירו ל־ R את ϕ_x,ϕ_y בהתאמה. נשים לב שבמרחב ממימד m צריך $\log_2(m)=\log_2\left(\frac{n}{c(\varepsilon)}\right)=O(\log_2(n))$ קיוביטים לפרושו.

ולכן אליס ובוב יישלחו ל־ R לכל היותר $O(\log_2(n))$ קיוביטים.

מה ש־ R יעשה:

i. הוא יקבל ϕ_x,ϕ_y

ii. הוא יקצה 0 אחד

iii. נחזור על הדבר הבא $\boxed{k=10}$ פעמים:

א'. הוא יריץ את swap test על $|0,\phi_x,\phi_y\rangle$

ב'. נמדוד את הקיוביט הראשון, אם הוא פגש 1, הוא יחזיר שהם לא זהים

ג'. אחרת אנחנו במצב $|0,\phi_x,\phi_y\rangle$ ונחזור לשלב הראשון (הוא לא החליף כי הביט של ה־ $control$ יצא 0 במדידה)

iv. נחזיר שהם זהים

נשים לב שבהינתן ו־ $x=y$ אז $\phi_x=\phi_y$ ולכן בכל הרצה של swap test ההסתברות שימדד 0 בסוף היא $=\frac{1+|\langle\phi_x|\phi_y\rangle|^2}{2}$ $\frac{1+1}{2}=1$, כלומר תמיד נצדוק כי תמיד נחזיר שהם זהים.

בהינתן ו־ $x\neq y$, אז ההסתברות שנצדוק ונגיד ש־ $x\neq y$ היא אם מדדנו 1 באחד המדידות, שזה

$$\mathbb{P}(\text{we said } x\neq y)=\mathbb{P}(\text{we measured at least one } 1)$$

$$=1-\mathbb{P}(\text{we measured only } 0)=1-\left(\frac{1+|\langle\phi_x\mid\phi_y\rangle|^2}{2}\right)^k$$

כלומר הטעות שלנו היא לכל היותר $\left(\frac{1+|\langle\phi_x|\phi_y\rangle|^2}{2}\right)^k+0$, נשים לב כי

$$\left(\frac{1+|\langle\phi_x\mid\phi_y\rangle|^2}{2}\right)^k\le\left(\frac{1+\varepsilon^2}{2}\right)^k$$

ולכן

$$\left(\frac{1+\varepsilon^2}{2}\right)^k\le\frac{1}{100}\iff k\cdot\ln\left(\frac{1+\varepsilon^2}{2}\right)\le\ln\left(\frac{1}{100}\right)\iff k\cdot-\ln\left(\frac{2}{1+\varepsilon^2}\right)\le-\ln(100)$$

$$\iff k\ge\frac{\ln(100)}{\ln\left(\frac{2}{1+\varepsilon^2}\right)}\iff k\ge\frac{\ln(100)}{\ln\left(\frac{2}{1+\frac{1}{4}}\right)}=k\ge\frac{\ln(100)}{\ln\left(\frac{8}{5}\right)}=9.79\ldots$$

נשים לב שבחרנו $k=10$, ולכן אכן קיבלנו שהשגיאה שלנו תהיה קטנה מ־ $\frac{1}{100}$, כנדרש

מ.ש.ל.ג.☺

(ד) **צ"ל:** מורכבות המעגלים

הוכחה:

נחשב את מורכבות המעגל של אליס (לא בהכרח הרעיון הכי יעיל):

נגדיר $f_i(x) = \begin{cases} \phi_i & i = x \\ 0 & else \end{cases}$,

היא מקבלת כקלט $x \in \{0,1\}^n$,

i. נתחיל עם $\left(\underbrace{x}_{\lceil \log(n) \rceil \text{ space}}, 0, \underbrace{0, \ldots, 0}_{\text{m times}} \right)$

ii. לכל $1 \le i \le 2^n$:

א'. נריץ $\left(x, 0, \underbrace{?, \ldots, ?}_{\text{m times}} \right) \to \left(x, 1_{i=k}, \left(\underbrace{?, \ldots, ?}_{\text{m times}} \right) \right)$

ב'. נריץ $controlled - \phi_i$ שעושה $\left(x, 0, \underbrace{?, \ldots, ?}_{\text{m times}} \right) \to \left(x, 1_{i=k}, \left(\underbrace{?, \ldots, ?}_{\text{m times}} \right) \oplus \phi_i \right)$ אם הביט $1_{i=k}$ דלוק

ג'. נעשה את הפעולה ההפוכה לפעולה שעשינו בשלב הראשון כדי לחזור למצב $\left(x, 0, \underbrace{?, \ldots, ?}_{\text{m times}} \right)$

iii. נשים לב שתהיה רק ריצה תהיה עם $1_{i=k}$ ולכן נקבל את המצב $(x, 0, \phi_x)$

iv. נחזיר את ה־ m קיוביטים האחרונים שהם בדיוק ϕ_x

אז לאליס יש $O(2^n)$ מעגלים שכל אחד הוא $\left(2^{\lceil \log(n) \rceil + 1 + m}\right) \times \left(2^{\lceil \log(n) \rceil + 1 + m}\right)$ ואז אם סופרים החזרה אז יש עוד מעגל בגודל $2^m \times 2^m$.

באופן סימטרי לבוב יש בדיוק אותו מבנה של מעגלים.

ל־ R יש k הרצה של $swap - test$, k מדידות והחזרה של האם כל המדידות היו 0.

כל הרצה של $swap - test$ היא $2^{m+m+1} \times 2^{m+m+1}$,

יש עוד k מדידות שנחשיב כאילו הן דורשות מעגל לכל אחד (כי אנחנו מציירים זאת בסכימה),

והחזרה אפשר לפתור בצורה קלאסית ב־ $O(k)$ ולכן צריך לכל היותר $O(k)$ מעגלים קוונטים בסדר גודל של $O(k)$.

קיבלנו זמן ריצה די נוראי של $O(2^n)$ לפחות בשביל אליס ובוב עם מעגלים די גדולים אבל העברנו כמות קטנה של קיוביטים ברשת ול־ R רק בזמן פולינומי.

הערה: נשים לב שלחשב את $f(x) = \phi_x$ באופן קלאסי ללא ידע על תכונות מיוחדות של ϕ_x ייקח זמן של $O(2^n)$.
אם באופן קוונטי היינו יכולים לפתור בזמן ריצה פולינומי אז היינו מוצאים בעיה NPC שפתירה בזמן פולינומי והיינו מקבלים ש־ $NP \subseteq QMA$ שזה לא ידוע כיום ולכן זמן הריצה הקוונטי הוא גם אקספוננציאלי.

מ.ש.ל.ד.☺

(ה) **צ"ל:** אלגוריתם ששוגה לכל היותר ב־ $\frac{1}{100}$

הוכחה:

אני אציג פתרון גנרי עם קוד לינארי C חשיב בזמן פולינומי המקיים $[m, n, d]$ כאשר $m = O(n)$ וגם $\forall x, y$ מתקיים $\left(\frac{1}{2} - \delta\right) \cdot m \le \|C(x) - C(y)\|_1 \le \left(\frac{1}{2} + \delta\right) \cdot m$

נתאר את האלגוריתם:

i. אליס תקבל את x, תמיר את x לבסיס q ותשלח ל־ R את $\frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{C(x)_k} \mid i \rangle$

ii. בוב יקבל את y, ימיר את y לבסיס q וישלח ל־ R את $\frac{1}{\sqrt{m}} \sum_{i=1}^{m} (-1)^{C(y)_k} \mid i \rangle$

iii. R יקבל ϕ_x, ϕ_y

iv. הוא יקצה 0 אחד

v. נחזור על הדבר הבא $\boxed{k = \left\lceil \frac{\ln(100)}{\ln\left(\frac{2}{1+\left(\frac{1}{2}+\delta\right)^2}\right)} \right\rceil + 1}$ פעמים:

א'. הוא יריץ את swap test על $|\,0, \phi_x, \phi_y\rangle$

ב'. נמדוד את הקיוביט הראשון, אם הוא פגש 1, הוא יחזיר שהם לא זהים

ג'. אחרת אנחנו במצב $|\,0, \phi_x, \phi_y\rangle$ ונחזור לשלב הראשון (הוא לא החליף כי הביט של ה־ $control$ יצא 0 במדידה)

vi. נחזיר שהם זהים

נשים לב כי $\frac{1}{2} + \delta = \frac{\frac{1+2\delta}{2} \cdot m}{m} \leq \frac{\max\left\{\|C(x)-C(y)\|_1, -\|C(x)-C(y)\|_1\right\}}{m} \leq |\langle \phi_x \mid \phi_y \rangle|$,
כבר ראינו בסעיף קודם שעבור $k \geq \frac{\ln(100)}{\ln\left(\frac{2}{1+\varepsilon^2}\right)}$ נצדוק בשגיאה שהיא לכל היותר $\frac{1}{100}$ עבור וקטורים שמרחקם לכל היותר ε,
נציב $\varepsilon = \frac{1}{2} + \delta$ ונקבל את הנדרש.
נשים לב שהחישובים של בוב ואליס יעילים בזמן פולינומי בעקבות העובדה שדרשנו ש־ C יהיה חשיב בזמן פולינומי.
לאחר מכן אנחנו מבצעים מספר קבוע של פעולות ולכן נקבל שזמן הריצה הוא פולינומי כולו.
בנוסף לכך נשים לב ששלחנו לכל היותר $\log(m) + 1$ קיוביטים מאליס ומבוב ולכן נשלחו $O(\log(n)) = O(\log(m))$ באלגוריתם.
כלומר הראנו אלגוריתם יעיל שמעביר $O(\log(n))$ קיוביטים וטועה לכל היותר בהסתברות $\frac{1}{100}$.

נשאר לנמק את קיום C, וזאת ניתן להראות על ידי קוד לינארי אקראי שקיים קוד המקיים תכונות אלה שנדרשו. הוכח כבר שקיים קוד המקיים את הנדרש ולכן אשתמש בו כקופסא שחורה.

מ.ש.ל.ה.☺

7.1

סיכום מאמר בקוונטים

שם: מיכאל גרינבאום, **ת.ז.:** 211747639

10 בספטמבר 2021

המאמר שבחרתי לעבוד עליו הוא

Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem

.

תחילה אגדיר את המושגי יסוד שמשתמשים בהם במאמר ולאחר מכן אראה את התוצאות ואסביר איך הגיעו אליהם.

- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$. יהי A אלגוריתם דטרמניסטי שמחשב את $f\left(x\right)$ על ידי שאילתות על הביטים של x כך ש־ $A\left(x\right)=f\left(x\right)$. נסמן ב־ $D_A\left(f\right)$ את מספר השאילתות במקרה הכי גרוע לאלגוריתם. ונגדיר $D\left(f\right)=\min_A D_A\left(f\right)$.
- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$. יהי A אלגוריתם רנדומלי קלאסי שמחשב את $f\left(x\right)$ על ידי שאילתות על הביטים של x כך ש־ $\mathbb{P}\left(A\left(x\right)=f\left(x\right)\right)\geq\frac{2}{3}$. נסמן ב־ $R_A\left(f\right)$ את מספר השאילתות במקרה הכי גרוע לאלגוריתם. ונגדיר $R\left(f\right)=\min_A R_A\left(f\right)$. ובאופן דומה נגדיר $Q\left(f\right)$ כשהאלגוריתם קוונטי.

אחת המטרות העיקריות של המאמר היא לתת קשר בין $D\left(f\right)$ ו־ $Q\left(f\right)$ כדי לדעת כמה כוח אלגורתמי הוספה של אפשרות קוונטית יכול להוסיף.

- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$, קיים פולינום $q\in\mathbb{F}_2[x]$ כך ש־ $f\left(x\right)=q\left(x\right)$ לכל $x\in\{0,1\}^n$. נאמר כי $\boxed{\deg f=\deg q}$ כש־ $\deg q$ היא דרגת הפולינום.
- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$, קיים פולינום $q\in\mathbb{F}_2[x]$ כך ש־ $\left|f\left(x\right)-q\left(x\right)\right|\leq\frac{1}{3}$ לכל $x\in\{0,1\}^n$ וגם לכל $x\in\{0,1\}^n$ מתקיים כי $q\left(x\right)\in[0,1]$. נאמר כי $\boxed{\widetilde{\deg}f=\deg q}$ כש־ $\deg q$ היא דרגת הפולינום.

? $\mathbb{F}_2$

- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$ ויהי $x\in\{0,1\}^n$. נאמר ש־ x רגיש לבלוק $B\subseteq[n]$ אם מתקיים $f\left(x\oplus 1_B\right)\neq f\left(x\right)$. נגדיר את $bs_x\left(f\right)$ את מספר הבלוקים המקסימלי שחיתוכם ריק והם כולם רגישים ל־ x. נגדיר $\boxed{bs\left(f\right)=\max_x bs_x\left(f\right)}$.
- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$, נגדיר את הגרף הספקטרלי G_f להיות תת הגרף של הקוביה ה־ n מימדית שיש צלע בין x ל־ y אם"ם $\left\|x\oplus y\right\|_1=1\wedge f\left(x\right)\neq f\left(y\right)$, כלומר מרחקם 1 והם לא מסכימים על f.
- <u>הגדרה:</u> תהי $f:\{0,1\}^n\to\{0,1\}$, נגדיר $\lambda\left(f\right)=\left\|A_f\right\|_{op}$ כש־ A_f זאת מטריצת השכינויות של הגרף הספקטרלי של f. נשים לב ש־ G_f הוא דו צדדי ולכן לכל ערך עצמי חיובי יש שלילי עם אותו מרחק והפוך ולכן ניתן להגדיר את $\lambda\left(f\right)$ כערך העצמי הגדול ביותר.
- <u>הגדרה:</u> יהיו $\{D_i\}_{i=1}^n$ ו־ F מטריצות כך ש־ $D_i\left[x,y\right]=1_{x_i\neq y_i}$ ו־ $F\left[x,y\right]=1_{f(x)\neq f(y)}$, ותהי $\Gamma\circ F=\Gamma$. נגדיר $\boxed{SA\left(f\right)=\max_{i\in[n]}\frac{\left\|\Gamma\right\|}{\left\|\Gamma\circ D_i\right\|}}$. (הערה: המדד של SA יכול להיות מוגדר בהרבה צורות שונות של בעיות מינימום ומקסימום על ידי הוכחות מ־ $BSS03, SS06, Kou93, LLS06$ והן מצורפות בסוף המאמר).

לאחר כל ההגדרות האלה, סוף סוף אפשר להתחיל לדבר מה מיוחד במאמר:

9.1

1. תחילה הבנייה של הגרף הספרקטרלי בפני עצמה היא מעניינת, למה דווקא קוביה n מימדית ולא גרף אחר.
האבחנה החשובה של המאמר היא שאפשר לצרף הרבה תוצאות שהוכיחו במאמרים קודמים בעזרת הערך $\lambda\left(f\right)$ ולהסיק מכך תוצאות מעניינות.
התוצאה הראשונה מראה כי לכל $f:\{0,1\}^n\to\{0,1\}$ מתקיים כי $\deg f\le\lambda^2\left(f\right)$. ההוכחה נובעת מהמאמר $Hua19$.
רעיון ההוכחה היא להגדיר רקורסיבית מטריצה $B_k=\begin{bmatrix}B_{k-1} & I_{k-1}\\ I_{k-1} & -B_{k-1}\end{bmatrix}$ כאשר $B_1=\begin{bmatrix}0&1\\1&0\end{bmatrix}$.
במאמר הוכח של- B_n יש 2 ערכים עצמיים והם $\pm\sqrt{n}$ וכל אחד מהם ממימד $\frac{n}{2}$.
ההוכחה מניחה ש- $\deg f=n$ (אחרת אפשר לצמצם את המרחב) ומשתמשת בוקטור עצמי כדי לקבל שיש וקטור המקיים

$$A_f\cdot v\ge\sqrt{n}\cdot v$$

ומפה הם מסיקים שיש ערך עצמי שגודלו יותר מ- $\sqrt{n}$ ולכן מתקבל כי $\boxed{\deg f\le\lambda^2\left(f\right)}$.

עתה מראים במאמר כי מתקיים $\lambda\left(f\right)\le SA\left(f\right)$.
ההוכחה נובעת מהאבחנה שאם $\Gamma=G_f$ אז מתקיים $\|\Gamma\circ D_i\|\le1$ ולכן $\lambda\left(f\right)\le\max_{i\in[n]}\frac{\|G_f\|}{\|G_f\circ D_i\|}\le SA\left(f\right)$.
ב- $BSS03$ הוכח כי $Q\left(f\right)=\Omega\left(SA\left(f\right)\right)$ ולכן מחיבור הטענות מתקבל כי

$$\boxed{\deg\left(f\right)\le\lambda^2\left(f\right)\le SA^2\left(f\right)\le O\left(Q^2\left(f\right)\right)}$$

ב- $Mid04$ הוכח כי $D\left(f\right)\le bs\left(f\right)\cdot\deg\left(f\right)$ ועם חיבור תוצאות מ- BBC^+01 ו- $NS94$ אפשר לקבל כי $bs\left(f\right)\le O\left(Q^2\left(f\right)\right)$.
מחיבור התוצאות הללו ניתן לקבל כי

$$D\left(f\right)\le bs\left(f\right)\cdot\deg\left(f\right)\le O\left(Q^2\left(f\right)\right)\cdot O\left(Q^2\left(f\right)\right)=O\left(Q^4\left(f\right)\right)$$

ב- ABB^+17 הראו כי $D\left(f\right)=\Omega\left(Q^4\left(f\right)\right)$ (עד כדי לוג) ולכן התוצאה הזאת מראה כי $\boxed{D\left(f\right)=\Theta\left(Q^4\left(f\right)\right)}$ (עד כדי לוג!). תוצאה זאת נותנת שלמות לשיפור חישובי אורקל קוונטים על פני אלגוריתמים דטרמניסטים!

2. נגדיר מטריצה $H_{x,y}=\left(-1\right)^{\langle x,y\rangle}\cdot2^{-\frac{n}{2}}$, מטריצה אלכסונית $\left[diag\left(f\right)\right]_{x,y}=1_{x=y}\cdot f\left(x\right)$ ומטריצה אלכסונית $X_{x,y}=1_{x=y}\cdot\|x\|_1$.
תחילה מוכיחים כי $\lambda\left(f\right)=\max_{\|v\|=1}v^T\left(RXR-X\right)\cdot v$ כש- $R=H\cdot diag\left(g\right)\cdot H$ ו- $g=1-2f$.
הדרך שמוכיחים זאת היא על ידי האבחנה ש A_f סימטרית ולכן ניתן לכתוב $\lambda\left(f\right)=\max_{\|v\|=1}v^T\cdot A_f\cdot v$.
לאחר מכן יש אבחנה מתמטית יפה שמתקיים $A_f=\frac{1}{2}\cdot\left[A_H-diag\left(g\right)\cdot H\cdot diag\left(g\right)\right]$ כאשר A_H הוא הגרף הספקטרלי של $h\left(x\right)=1$ לכל $x\in\{0,1\}^n$.
מקבלים עוד נוסחא יפה ואפשר לקבל כי $H\cdot A_H\cdot H=n\cdot1-2X$ וגם $H^2=I_n$
עושים פיתוח מתמטי על הנוסחא עם הנוסחאות ואפשר לקבל כי $\lambda\left(f\right)=\max_{\|v\|=1}v^T\left(RXR-X\right)\cdot v$ בעזרת התכונות היפות של המטריות A_H,H.

עתה המאמר רוצה להראות את החשיבות של המטריצה R, מוכיחים במאמר שמתקיים $R_{x,y}=\hat{g}\left(x\oplus y\right)$ כאשר $\hat{g}\left(z\right)=\frac{1}{2^n}\sum_{y\in\{0,1\}^n}\left(-1\right)^{\langle z,y\rangle}\cdot g\left(y\right)$ וזה יוצא מתמטית מההגדרה באופן מיידי ובפרט מתקיים $R_{x,y}=0$ אם $\|x\oplus y\|\ge\deg\left(f\right)$.
בעזרת פיתוח מתמטי והנחה ש- $\|R\|\le1$ אפשר לקבל ש- $v^T\left(RXR-X\right)\cdot v\le\deg\left(f\right)$ לכל $\|v\|\le1$. (נובע מחיבור אי שוויונות).
עתה קיבלנו כי $\lambda\left(f\right)=\max_{\|v\|=1}v^T\left(RXR-X\right)\cdot v\le\deg\left(f\right)$ אבל זאת טענה יחסית חלשה לעומת מה שהמאמר מוכיח בהמשך.

המאמר משתמש בעובדה שאפשר לקרב כל פונקציה f עם פולינום עד כדי הסתברות ε במקום $\frac{1}{3}$ עם $\widetilde{\deg}_\varepsilon\left(f\right)=O\left(\widetilde{\deg}\left(f\right)\cdot\log\left(\frac{1}{\varepsilon}\right)\right)$ על ידי בנייה שגילו ב- $BNRdW07$.
עתה אפשר לעשות את הפיתוח שעשינו במקור כדי לקבל $\lambda\left(f\right)=\max_{\|v\|=1}v^T\left(RXR-X\right)\cdot v$ ונקבל $\lambda\left(f\right)=\max_{\|v\|=1}v^T\left(\widetilde{R}X\widetilde{R}-X\right)\cdot v+3\varepsilon n$ עם פולינום $\widetilde{g}$ הוא ε מקרב את g ו- $\widetilde{R}$ מוגדר ביחס ל- $\widetilde{g}$.

לכן מהמשפט שהוכח קודם, ניתן לקבל כי עבור $\boxed{\varepsilon = \frac{1}{3n}}$ נקבל

$$\lambda(f) = \max_{\|v\|=1} v^T\left(\widetilde{R}X\widetilde{R} - X\right)\cdot v + 3\varepsilon n \le O\left(\widetilde{\deg(f)}\cdot \log(n)\right)$$

עתה עכשיו בעזרת רעיון מגניב של ניפוח, אפשר לקבל כי $\lambda(f) = O\left(\widetilde{\deg(f)}\right)$,
ידוע שמ־ $n \ge n_0$ קיים c כך ש־

$$\lambda(f) \le c\cdot \widetilde{\deg(f)}\cdot \log(n)$$

נגדיר f^k להיות f k פעמים על עצמה ובעזרת משפט ב־ $She13b$ שמתקיים $\widetilde{\deg(f\circ g)} \le c'\cdot \widetilde{\deg(f)}\cdot \widetilde{\deg(g)}$.
ולכן נקבל כי

$$\lambda^k(f) = \lambda\left(f^k\right) \le c\cdot \widetilde{\deg\left(f^k\right)}\cdot \log\left(n^k\right) = c\cdot k\cdot \widetilde{\deg\left(f^k\right)}\cdot \log(n) \le c\cdot (c')^{k-1}\cdot k\cdot \widetilde{\deg(f)}^k$$

ולכן נקבל $\lambda(f) \le \left(c\cdot (c')^{k-1}\cdot k\right)^{\frac{1}{k}}\cdot \widetilde{\deg(f)}$ ומהיות וזה נכון לכל k זה נכון גם לגבול ונקבל כי $\boxed{\lambda(f) = O\left(\widetilde{\deg(f)}\right)}$.

עכשיו נזכר שהוכחנו בהתחלה של החלק הראשון כי $\boxed{\deg(f) \le \lambda^2(f) = O\left(\widetilde{\deg^2(f)}\right)}$ כלומר קיבלנו חסם בין פולינום לקירוב שלו וחשוב להדגיש שזה אופטימלי ל־ OR לדוגמא, כלומר על ידי חיבור תוצאות של אחרים, המאמר הראה שוב חסם מאוד חזק ואף אופטימלי ושיפר פי 3 את התוצאה הידועה הקודמת.
הערה: חשוב לציין שהמאמר מראה עוד דרך להוכיח זאת בלי שימוש במשפטים של אחרים, אך העדפתי להסתכל על ההוכחה הזאת.

3. תחילה נגדיר $\deg_2(f)$ להיות הדרגה של הפולינום שמייצג את f כשהמקדמים הם מעל ל־ $\mathbb{F}_2$.
ידוע כי $\deg_2(f) \le \deg(f) \le O\left(Q^2(f)\right)$,
בנוסף לכך ידוע שלכל $f:\{0,1\}^n \to \{0,1\}$ לא מונוטוני ולא קבוע מתקיים $\deg_2(f) = \Omega\left(n^2\right)$.
הערה: מונוטוניות זאת תכונה שבהינתן $x \le y$ מתקיים $f(x) \le f(y)$.

ולכן נקבל כי $\Omega\left(n^2\right) \le \deg_2(f) \le \deg(f) \le O\left(Q^2(f)\right)$, כלומר $\boxed{Q(f) = \Omega(n)}$, כלומר קיבלנו שכל אלגוריתם קוונטי יצטרך לכל הפחות n שאילתות כש־ f ~~לא~~ מונוטונית!
זאת תוצאה מדהימה שמשפרת את מה שהיה ידוע קודם ומראה שאפילו קוונטים יכולים לעשות דברים באופן הרבה יותר טוב מקלאסי, זה לא רחוק כל כך מקלאסי.

4. תחילה נשים לב שאפשר להוכיח באינדוקציה כי $\deg(f) = n$ כש־ $f:\{0,1\}^n \to \{0,1\}$ בעזרת חוקי דה מורגן.
ידוע ממאמר $BBC^{+}01$ כי $\widetilde{\deg(f)} \le Q(f)$ וידוע שלכל read once formula (כל משתנה מופיע פעם אחת בהצגה של f) מתקיים $Q(f) = O(\sqrt{n})$ ולכן $\widetilde{\deg(f)} = O(\sqrt{n})$.
בנוסף לכך הוכחנו כי $n = \deg(f) \le \widetilde{\deg^2(f)}$ ולכן $\Omega(\sqrt{n}) = \widetilde{\deg(f)}$.
כלומר קיבלנו כי $\widetilde{\deg(f)} = \Theta(\sqrt{n})$ כלומר כל פורמולה שניתן לחשב בקריאה אחת, אפשר לקרב על ידי דרגה $\sqrt{n}$!

לסיכום, המאמר הזה מאוד עניין וריגש אותי אישית כי הוא הראה שכלי שלמדתי באוניברסיטה (לגבי $\lambda(f)$ שנתי אוהב ללמד עליו) הוא שמיש גם במחקר עכשווי והביא להרבה תוצאות יפות ומעניינות.
הרעיון הכללי של המאמר הזה היא לעשות מחקר של $20-10$ שנה ולחבר את החלקים של הפאזל כדי לקבל תוצאות טובות.
נשארו עוד הרבה שאלות פתוחות אבל האחת שהכי מעניינת אותי אישיתת היא מה הקשר בין $R(f)$ ל־ $Q(f)$ ואיך בכלל ניגשים לבעיה הזאת.
השתדלתי להשאיר רק את החלקים העיקריים של ההוכחות, דילגתי על כל השקילויות של SA שנמצאות לאחר הנספחים.

Index of comments

1.1 Correct but too complicated:
Alice could do: |k,0> --> |k,x_k>
and that would be enough for Bob to continue as you have outlined.

4.1 Why take nagation twice. Using the union bound directly on what you got earlier works just as well.

4.2 Using just 2^(cm) is enough. All you need is that you can add another new almost orthogonal vector to the set as long as you haven't passed the bound.

4.3 אין צורך לכתוב שטויות. התכוונת למשהו נכון אך הביטוי הזה הוא שלילי'.

6.1 מה NPC פה?

7.1 השאלה בקשה להציג אלגורתם מפורש ולכן בין השאר יש להציג קוד ליניארי מפורש. העובדה שקימים קודים כאלו משאירה את בעיית מציאת הקוד לאלגורתם וללא שיטה מפורשת יעילה זה דורש זמן אקספוננציאלי'.

8.1 עברית: הוספה - יכולה

8.2 מדובר במאמר בפולינום עם מקדמים ממשייםץ.
זה בולט במיוחד עבור הנקודה השנייה (שמאבדת את אפשרות הקירוב אם מדובר בפולינום מעל השדה בן שני אברים.

9.1 זה מה שמופיע כבר במאמר של Huang

10.1 בכל הסעיף הזה מדובר רק בתכונות מונוטוניות (לא טריוויאליות)

10.2 חסרה הערה שכאן מדובר בתכונות גרפיות המתיחסות לתכונה של הגרף

10.3 מוטב היה להתחיל את הפיסקה באמירה שמדובר ב-Once Formula Read