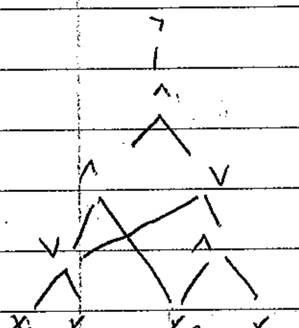
1. חישוב

1.1 חישוב קלט ע"י מעגלים

שפה: $L \subseteq \{0,1\}^*$

מודל חישוב: מעגל בוליאני



מעגל: גרף עם n קלטים ופלט אחד
ושערים שהם $\wedge, \vee, \neg$

גודל מעגל: מס' השערים שבו.

נאמר שאוסף $\{C_n\}_{n\in\mathbb{N}}$ מחשב שפה L
אם לכל $x = x_1 \dots x_n \in \{0,1\}^n$ מתקיים

$$\underbrace{C_n(x_1,\dots,x_n) = 1}_{} \iff x \in L$$

C_n - מעגל על n קלטים

נסמן $0 = False$, $1 = True$

נאמר ש $L \in size(s(n))$ אם יש $\{C_n\}_{n\in\mathbb{N}}$ שמחשב את L
ומתקיים לכל $n\in\mathbb{N}$ $|C_n| \le s(n)$.

טענה: לכל שפה $L \subseteq \{0,1\}^*$ מתקיים $L \in size(n\cdot 2^n)$.

הגדרה: $Psize = \bigcup_{k\in\mathbb{N}} size(n^k)$

מבחינתנו מה שנוח לחשוב ב $Psize$: ניתן לקמפל יעיל

1.2 חישוב קוונטי על ביט אחד

הערה = אוסף המצבים האפשריים = $\mathbb{C}^2$ מנורמל לאורך 1.

כלומר כל הוקטורים $v \in \mathbb{C}^2$, $\|v\|_2 = 1$

אין שקול: נבחר בסיס כלשהו ל-$\mathbb{C}^2$, נאמר

הבסיס הסטנדרטי $e_0 = \begin{pmatrix}1\\0\end{pmatrix}$, $e_1 = \begin{pmatrix}0\\1\end{pmatrix}$

נסמן $|0\rangle = e_0$, $|1\rangle = e_1$

והערה, כל הוקטורים $\alpha|0\rangle + \beta|1\rangle$, $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$

	קלסי	קוונטי
הערות של ביט אחד	$v \in \{0,1\}$	$v \in \{\alpha|0\rangle + \beta|1\rangle \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$

<u>פעולה</u>: מיפוי מצב של הערה למצב של הערה.

לא כל פעולה מותרת.

כל פעולה כזו צריכה להיות פעולה לינארית

ויתרה מזאת היא אוניטרית. (= שומרת זוית)

$A: \mathbb{C}^2 \to \mathbb{C}^2$ לינארית

כך שלכל $u, v \in \mathbb{C}^2$ $\langle u, v\rangle = \langle Au, Av\rangle$

בפרט היא שומרת <u>אורך</u>! $\|u\| = 1 \Rightarrow \langle u, u\rangle = 1$

$\Rightarrow \langle Au, Au\rangle = 1 \Rightarrow \|Au\| = 1$.

דוגמא 1: הפעולה $not: \{0,1\} \to \{0,1\}$
המוגדרת ע"י $not(0)=1,\ not(1)=0$

נרצה להרחיב לפעולה אוניטרית.
כאשר נגדיר $not(|0\rangle)=|1\rangle,\ not(|1\rangle)=|0\rangle$
ונרחיב לינארית:

$$not(\alpha|0\rangle+\beta|1\rangle)=\alpha|1\rangle+\beta|0\rangle$$

מקבלים X

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

שהיא אוניטרית כי $\underset{X^{\dagger}}{X}X^{\dagger}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I$

דוגמא 2:

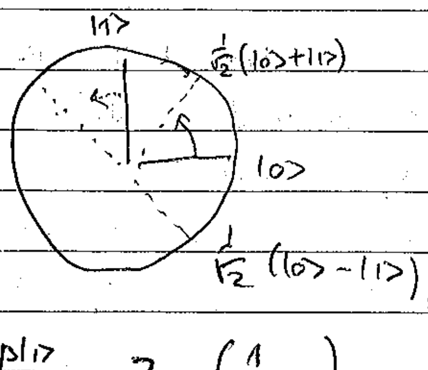
$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$$

$$HH^{\dagger}=\frac{1}{2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\1&-1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}2&0\\0&2\end{pmatrix}=I$$

מי זה H?

$$H(|0\rangle)=H\begin{pmatrix}1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

$$H(|1\rangle)=H\begin{pmatrix}0\\1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$



הזזה בזווית $\frac{\pi}{4}$
בסדר שמור על צירים

דוגמא 3, אני סגה

$$Z=\begin{pmatrix}1&\\&-1\end{pmatrix}$$

$\alpha|0\rangle+\beta|1\rangle \Rightarrow \alpha|0\rangle-\beta|1\rangle$ הופך

מכ׳ $|1\rangle \perp |0\rangle$, $\langle 1,1\rangle = \langle 0,0\rangle = 1$, מכ׳ הקבוצה בסיס ב- $\mathbb{C}^2$.

~~המצב של 2-qubits~~

~~מצבים קוונטיים ב- $\mathbb{C}^4$ בנורמה 1~~ $= \{ v \in \mathbb{C}^4 \mid v = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,\ |\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1 \}$

<u>מכפלה טנזורית</u>

יהיו V, W מ"ו.
נגדיר $V \otimes W$

$V \otimes W = \mathrm{span}\{ v \otimes w \mid v \in V,\ w \in W \}$ מעל $\mathbb{C}$

עם חיבור, וכפל בסקלר מ- $\mathbb{C}$ ומוגדרות השוויונות:

$$\sum \alpha_i (v_i \otimes w) = \left(\sum \alpha_i v_i\right) \otimes w$$
$$\sum \alpha_i (v \otimes w_i) = v \otimes \left(\sum \alpha_i w_i\right)$$

<u>טענה</u>: אם V מ"ו ממימד n עם בסיס $E = \{e_1, \dots, e_n\}$
" " W " " m " " $F = \{f_1, \dots, f_m\}$
אז $V \otimes W$ " " $n \cdot m$ " " $E \otimes F = \{ e_i f_j \mid 1 \le i \le n,\ 1 \le j \le m \}$

<u>הוכחה</u> ① $E \otimes F$ פורש.
אם $\sum \alpha_i e_i = v \in V$
$\sum \beta_j f_j = w \in W$

אז $v \otimes w = \sum \alpha_i \beta_j (e_i \otimes f_j)$

ב) $E\otimes F$ הנ״ל

אם c_{ij} לא כולם אפס צ״ל ש $\sum c_{ij} e_i\otimes f_j \neq \vec{0}$
$= 0\otimes 0$

אז יש j_0 כך שלא כל ה-α_{ij_0} הם אפס

ולכן $\sum c_{ij_0}\, e_i\otimes f_{j_0} = (\sum c_{ij_0} e_i)\otimes f_{j_0} \neq \vec{0}$ מאי־תלות לינארית.

תרגיל לבית: אם V, W מרחבי מכפלה פנימית
אז $V\otimes W$ '' '' ''

מ״פ מוגדרת ע״י: $\langle v_1\otimes w_1, v_2\otimes w_2\rangle = \langle v_1, v_2\rangle\cdot\langle w_1, w_2\rangle$

מורחבת ע״י: $\langle \sum \alpha_{ij}(v_i^1\otimes w_j^1), \sum \beta_{kl}(v_k^2\otimes w_l^2)\rangle$

$= \sum_{i,j,k,l} \bar{\alpha}_{ij}\beta_{kl}\langle v_i^1\otimes w_j^1, v_k^2\otimes w_l^2\rangle$

$\boxed{\text{למחשב שמיוצר היום}}$

קוונטי: $\mathbb{C}^2\otimes\mathbb{C}^2$ הוא ממימד 4

נפרש ע״י:

$$
\begin{aligned}
|0\rangle\otimes|0\rangle &\overset{\text{סימון}}{=} |0,0\rangle\\
|0\rangle\otimes|1\rangle &= |0,1\rangle\\
|1\rangle\otimes|0\rangle &= |1,0\rangle\\
|1\rangle\otimes|1\rangle &= |1,1\rangle
\end{aligned}
$$

$\langle 0,0 | 0,1\rangle = \underbrace{\langle 0,0\rangle}_{1}\cdot\underbrace{\langle 0,1\rangle}_{0} = 0$

שני וקטורי בסיס שונים

$\underbrace{\langle e_0, e_0\rangle}_{\|e_0\|=1}$ $\langle e_0, e_1\rangle = 0$

$e_0 \perp e_1$

$|0,0\rangle \quad |0,1\rangle \quad |1,0\rangle \quad |1,1\rangle$

$$\begin{array}{c} 0,0 \\ 0,1 \\ 1,0 \\ 1,1 \end{array} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

הצגה כזה וקטור

למעשה זהו המ"ו הרגיל של $\mathbb{C}^4$.

<u>סימון</u>: $\mathcal{H}_2$ – המ"ו הרגיל ממימד 2.

$\mathbb{C}^2$, עם מ"פ: $|0\rangle \perp |1\rangle$

$\mathcal{H}_{2^m}$ - מרחב הילברט ממימד 2^m

מוגדר ע"י

$$\mathcal{H}_{2^m} = \underbrace{\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2}_{m \text{ פעמים}}.$$

המצב של m-qubits הוא: $\mathcal{H}_{2^m}$

	קלאסי	קוונטי
המצב של m ביטים	$v \in \{0,1\}^m = \{0,1\} \times \{0,1\} \times \dots \times \{0,1\}$	$\|v\|=1,\ v = \sum_{i_1,\dots,i_m \in \{0,1\}} \alpha_{i_1 \dots i_m} \lvert i_1,\dots,i_m\rangle$ $\mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_2$

בפעולה שניתן לחבר על m-qubits:

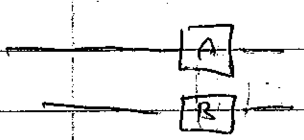
ב. אז $A: H_{2^n} \to H_{2^m}$ אוניטרית.

	קלסי	קוונטי
פעולות	ב. מיפוי	ב. ליני'
	$f: \{0,1\}^m \to \{0,1\}^m$	$A: H_{2^m} \to H_{2^n}$

דוגמא 1: מערכת של 2-qubits

נפעיל A על qubit הראשון $A: H_2 \to H_2$

" B " " השני



פרקטיקה נקרא $A \otimes B$

כיוון שאנו מגדירים פעולה לינארית, מספיק להגדיר איך מוגדר על בסיס, וכן מספיק להגדיר על ~~אברי~~ הבסיס $\{|i\rangle \otimes |j\rangle\}$

$|1\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|0\rangle \otimes |0\rangle = |0,0\rangle$

$$|i\rangle \otimes |j\rangle \xrightarrow{(A \otimes B)} |A_i\rangle \otimes |B_j\rangle$$

~~[illegible]~~

מה ~~[illegible]~~ המטריצה של $A \otimes B$?

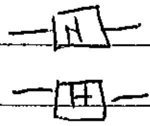
בבסיס הסטנדרטי $\{|i\rangle \otimes |j\rangle\}$

$$(A \otimes B)_{(i,j),(k,l)} =$$

$$\langle |i\rangle \otimes |j\rangle \,|\, A \otimes B \,|\, |k\rangle \otimes |l\rangle \rangle$$

$$= \langle i \otimes j \,|\, A|k\rangle \otimes B|l\rangle \rangle = \langle i|A|k\rangle \cdot \langle j|B|l\rangle = \boxed{A_{ik} \cdot B_{jl}}$$

דוגמא 1:



$$H\otimes H=\begin{pmatrix}1&1\\1&-1\end{pmatrix}\otimes\begin{pmatrix}1&1\\1&-1\end{pmatrix}=\begin{array}{c|c} & 00\quad 01 \\ \begin{matrix}00\\01\\10\\11\end{matrix} & \begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}\end{array}$$

המטריצה H

$i=0,\ k=0$	הבלוק של	$i=1,\ k=1$ הבלוק של
	$\langle i\|H\|k\rangle=1$	$\langle i\|H\|k\rangle=-1$
$B=H$	[illegible]	$-H=-B$ [illegible]

$$(H\otimes H)\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=(H\otimes H)(|0\rangle\otimes|0\rangle)=|H0\rangle\otimes|H0\rangle=\frac{1}{\sqrt2}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt2}(|0\rangle+|1\rangle)$$

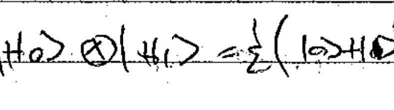
$$=\frac12\left[|00\rangle+|01\rangle+|10\rangle+|11\rangle\right]=\frac12\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

$$(H\otimes H)\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=H\otimes H\,(|0\rangle\otimes|1\rangle)=|H0\rangle\otimes|H1\rangle=\frac12(|0\rangle+|1\rangle)\otimes(|0\rangle-|1\rangle)$$

$$=\frac12\left[|00\rangle-|01\rangle+|10\rangle-|11\rangle\right]=\frac12\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}$$

הוכחה: A,B אוניטריות, אז $A\otimes B$ אוניטרית

$$(A\otimes B)^\dagger=A^\dagger\otimes B^\dagger$$



$$(A\otimes B)\cdot(C\otimes D)=AC\otimes BD$$

$$(I\otimes H)(H\otimes I)=H\otimes H$$

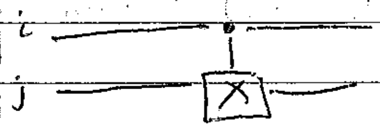
$$(A\otimes B)(A\otimes B)^\dagger=(A\otimes B)\cdot(A^\dagger\otimes B^\dagger)=AA^\dagger\otimes BB^\dagger=I\otimes I=I$$

מטריצת [illegible]

גיליון 2

CNOT :

$$\mathrm{CNOT}\left(|i\rangle \otimes |j\rangle\right) = \begin{cases} |i\rangle|j\rangle & |i\rangle = |0\rangle \\ |i\rangle \otimes X|j\rangle & |i\rangle = |1\rangle \end{cases}$$



עם מטריצה

$$\begin{array}{c|c} & \begin{matrix} 00 & 01 & & \end{matrix} \\ \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \left(\begin{array}{cc|cc} 1 & 0 & \multicolumn{2}{c}{0} \\ 0 & 1 & & \\ \hline & & 0 & 1 \\ \multicolumn{2}{c|}{0} & 1 & 0 \end{array}\right) \end{array}$$

$|0,0\rangle \to |0,0\rangle$

$|0,1\rangle \to |0,1\rangle$

$|1,0\rangle \to |1,1\rangle$

$|1,1\rangle \to |1,0\rangle$

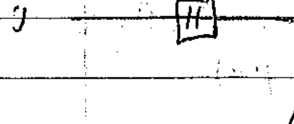
מטריצת פרמוטציה, היא אוניטרית.

תרגיל: Π היא פרמוטציה, אז $\Pi^{\dagger} = \overline{(\Pi^{t})}^{*} = \Pi^{t} = \Pi^{-1}$

כי זו פרמוטציה ממשית

ולכן $\Pi\Pi^{\dagger} = I$, Π אוניטרית.

דוג': Controlled Hadamard - CH



[illegible] אוניטרי

$$\left(\begin{array}{cc|cc} 1 & 0 & \multicolumn{2}{c}{0} \\ 0 & 1 & & \\ \hline \multicolumn{2}{c|}{0} & 1 & 1 \\ & & 1 & -1 \end{array}\right)$$

$|0,0\rangle \Rightarrow |0,0\rangle$

$|0,1\rangle \Rightarrow |0,1\rangle$

$|1,0\rangle \to |1,+\rangle$

$|1,1\rangle \Rightarrow |1,-\rangle$

השוואה: מכפלה קרטזית מול מכפלה טנזורית

V, W

	מכפלה קרטזית	מכפלה טנזור
חיבור:	קורדינטה קורדינטה $(V,W) = (V,0) + (0,W)$	(V,W) לינארי בכל אחד בנפרד $\sum \alpha_i (v_i, w) = (\sum \alpha_i v_i, w)$ $\sum \alpha_i (v, w_i) = (v, \sum \alpha_i w_i)$
בסיס	$\{(v_i,0)\} \cup \{(0,w_j)\}$ מימד $\dim(V) + \dim(W)$	$\{(e_i, f_j)\}$ מימד $\dim(V) \cdot \dim(W)$

מדידה

איך מקבלים תוצאה בחישוב קוונטי?

מדידה: חלוקה של המרחב $\mathcal{H}_{2^m}$ לתתי אורתוגונלים

$$\mathcal{H}_{2^m} = W_1 \oplus W_2 \oplus \dots \oplus W_k$$

כל W_i תתי אורתוגונלים אחד לשני שסכומם פורש את $\mathcal{H}_{2^m}$

תוצאת המדידה: $v \in \mathcal{H}_{2^m}$

נסמן E_i ההטלה של $\mathcal{H}_{2^m}$ על W_i

E_i הם אופרטורים $(\sum E_i = I, \ E_i \geq 0)$

אם הוא במצב $v \in \mathcal{H}_{2^n}$, מקבלים תוצאה i בהסתברות $\|E_i v\|$

ובהנתן שקבלנו תוצאה i נכנסים למצב $\frac{E_i v}{\|E_i v\|}$.

<u>דוגמא:</u> מודדים את ה-qubit הראשון

חלוקה ל-2 תמ"ו $W_0 = \text{span}\{|0\rangle \otimes \Psi_{2^{m-1}}\}$

$W_1 = \text{span}\{|1\rangle \otimes \Psi_{2^{m-1}}\}$

תמ"ו אורתוגונליים שסכומם פורשים את Ψ_{2^m}.

אם

$V = \sum \alpha_{i_1 \dots i_m} |i_1, \dots, i_m\rangle$ $\quad \alpha_{i_1}, \dots, \alpha_{i_m} \in \mathbb{C}$

$i_1, \dots, i_m \in \{0,1\}$ $\quad \sum_{i_1, \dots, i_m} |\alpha_{i_1 \dots i_m}|^2 = 1$

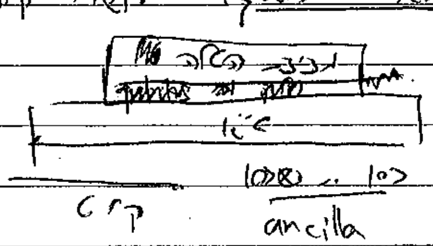
אז בהסתברות $\sum_{i_2 \dots i_m} |\alpha_{0, i_2 \dots i_m}|^2$ נקבל 0

ונפול למצב $|0\rangle \otimes \sum_{i_2 \dots i_m} \alpha_{0, i_2 \dots i_m} |i_2, \dots, i_m\rangle$ מנורמל

ובהסתברות $\sum_{i_2 \dots i_m} |\alpha_{1, i_2 \dots i_m}|^2$ נקבל 1

ונפול למצב $|1\rangle \otimes \sum_{i_2 \dots i_m} \alpha_{1, i_2 \dots i_m} |i_2, \dots, i_m\rangle$ מנורמל

<u>משפט שקול המדידה:</u> חישוב קוונטי כמו שקול לו:



<u>דוגמא:</u> מצב $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |10\rangle)$ מודדים qubit ראשון

בהסתברות $\frac{1}{3}$ נקבל 0, ונפול ל-$|0\rangle$, בהסתברות $\frac{2}{3}$ נקבל 1 ונפול ל-$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

א

מטרתנו: לפתור בעיה (למשל פירוק מספרים, ...) עם מעגלים קוונטים קטנים.

מעגל קוונטי: מורכב רק משערים לוקליים (על מס' קבוע קטן של qubits) מקבוצה קטנה של שערים ידועים.

העולם הקלסי: כל פונק' שניתנת לחישוב ניתנת לחישוב בעזרת רק שערי $\neg, \vee, \wedge$

העולם הקוונטי: כל פעולה ניתנת לקירוב ע"י מעגל קוונטי המשתמש בשערי:

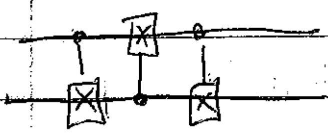
$$H, \ \underset{T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}}{\underset{\parallel}{\pi/8}}, \ CNOT$$

$\underbrace{QSize(s(n))}_{\text{abuse}}$ — כל הפונק' שניתנות לחישוב ע"י מעגלים קוונטים שגודלם לכל היותר $s(n)$

$$\underbrace{\bigcup_k QSize(n^k)}_{BQP}$$

abuse
של אלגוריתמים
non-uniform

lunc13



$|a,b\rangle \xrightarrow[\text{[illegible]}]{} |a, a\oplus b\rangle$

$\xrightarrow[\text{[illegible]}]{} |a\oplus a\oplus b,\ a\oplus b\rangle = |b, a\oplus b\rangle$

$\xrightarrow[\text{[illegible]}]{} |b, a\oplus b\oplus b\rangle = |b, a\rangle$

No cloning Thm

טענה: אין A לינ׳ על $\mathcal{H}_{2^2}$ כך שלכל $\varphi\in\mathcal{H}_2$

$$(*)\qquad A(|\varphi\rangle\otimes|0\rangle)=|\varphi\rangle\otimes|\varphi\rangle$$

הוכחה: נניח e e_0,e_1 ~~for some~~ ~~the~~ מקיימים את התכונה (*)

$$A(|e_i\rangle\otimes|0\rangle)=|e_i\rangle\otimes|e_i\rangle$$

כלומר:

$$A(|e_0\rangle\otimes|0\rangle)=|e_0\rangle\otimes|e_0\rangle$$
$$A(|e_1\rangle\otimes|0\rangle)=|e_1\rangle\otimes|e_1\rangle$$

A יוניטרי, ולכן: $\langle x,y\rangle=\langle Ax,Ay\rangle$

$$\langle e_0,e_1\rangle=\langle e_0,0|e_1,0\rangle=\langle e_0,e_0|e_1,e_1\rangle=\langle e_0,e_1\rangle\langle e_0,e_1\rangle$$

ולכן $\langle e_0,e_1\rangle\in\{0,1\}$, ולכן או $e_0=e_1$ או $e_0\perp e_1$. □