חישוב מהיר של FFT_{2^n} (ההכללה הכללית עד 2^n איברים)

$$|j\rangle \to |x_j\rangle$$

$N=2^n$ $$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} x_j(k)\,|k\rangle$$

$\omega = e^{\frac{2\pi i}{N}}$ $$= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{\frac{2\pi i jk}{N}}|k\rangle$$

$$= \frac{1}{\sqrt{N}}\bigotimes_{l=1}^{n}\left(|0\rangle + e^{2\pi i j\cdot \cancel{k_l}\, 2^{-l}}|1\rangle\right)$$ כלומר

$$\sum_{k=0}^{N-1} e^{\frac{2\pi i jk}{N}}|k\rangle = \sum_{k_1=0}^{1}\dots\sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}}|k_1\dots k_n\rangle$$ הוכחה

$$k = k_1\cdot 2^{n-1} + k_2 2^{n-2} + \dots + k_n\cdot 2^0$$

$$= \sum_{k_1=0}^{1}\dots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n} e^{2\pi i j\, k_l\cdot 2^{-l}}|k_l\rangle$$

$$= \bigotimes_{l=1}^{n}\underbrace{\sum_{k_l=0}^{1} e^{2\pi i j\, k_l 2^{-l}}|k_l\rangle}$$

$$\left(|0\rangle + e^{2\pi i j\,\cancel{k_1} 2^{-1}}|1\rangle\right)\otimes\left(\quad\right)\otimes \quad \otimes\left(|0\rangle + e^{2\pi i j\,\cancel{k_n} 2^{-n}}|1\rangle\right)$$

גם עכשיו לרשום: ש. המכפלה של $|k_1\dots k_n\rangle$ ולכן

$$\left[\ \prod_{l=1}^{n} e^{2\pi i j\, k_l 2^{-l}} = e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} = e^{\frac{2\pi i jk}{N}}\right.$$

$$j = j_1 2^{n-1} + j_2 2^{n-2}\dots + j_n 2^0$$ [illegible]

$e^{2\pi i z} = e^0 = 1$, $$j2^{-l} = \underbrace{j_1 2^{n-l-1} \dots + j_{n-l}\, 2^{n-(n-l)-l}}_{\text{שלם}} + \underbrace{\frac{j_{n-l+1}}{2} + \frac{j_{n-l+2}}{4} + \dots \frac{j_n}{}}_{\text{לא שלם}}$$ [illegible]

(10) [illegible]

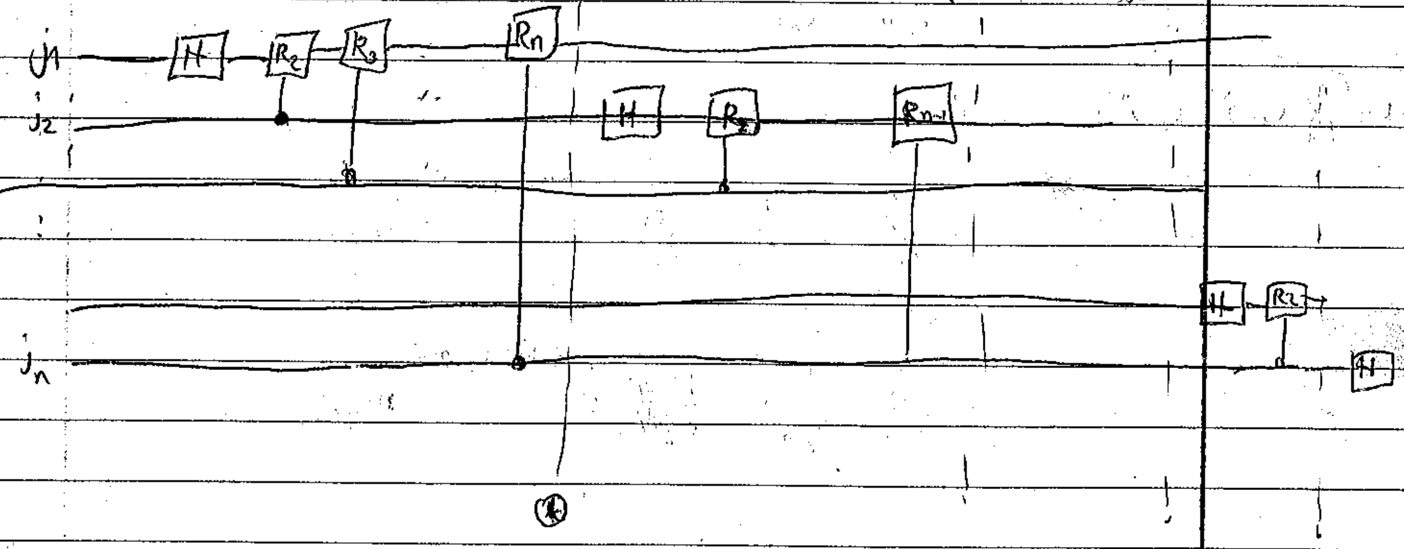
נסמן $0.b_p \ldots b_m$

$$= \frac{b_1}{2} + \frac{b_2}{4} + \ldots + \frac{b_m}{2^{m}}$$

ראינו שניתן לכתוב $|j\rangle \rightarrow \bigotimes_{l=1}^{n} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.j_{n-l+1} \ldots j_n)}|1\rangle\right)$

נסמן $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-k}} \end{bmatrix}$

ונבנה את המעגל!



אחרי ציון ①

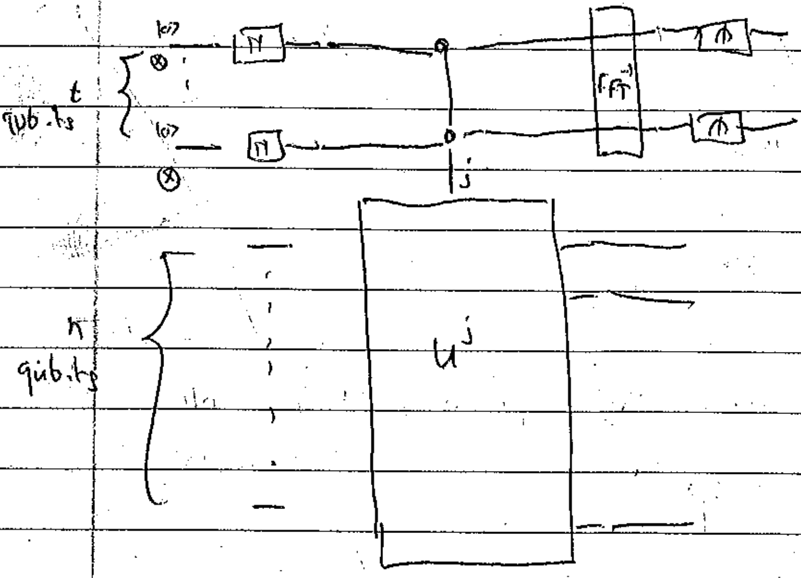
$$\left(|0\rangle + e^{2\pi i \sum_{m=1}^{n} j_m 2^{-m}}|1\rangle\right) \otimes |j_2 \ldots j_n\rangle$$
$$= \left(|0\rangle + e^{2\pi i\, 0.j_1 \ldots j_n}|1\rangle\right) \otimes |j_2 \ldots j_n\rangle$$

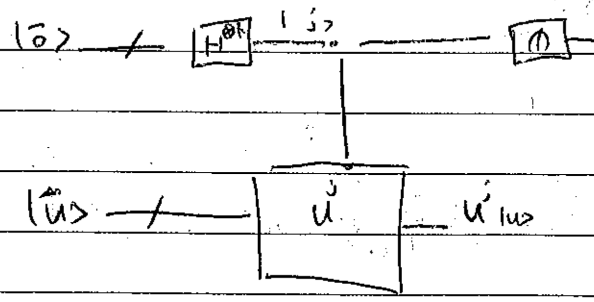
הערה: מקדמי המטריצה:
$FFT = (\omega^{kj})$
ולכן: $FFT^{-1} = FFT^{+} = (\omega^{-kj})$

ועוד הערה...

ⓡ יש בעצם FFT_N ו N [illegible] 2^n?

Phase estimation





אם בקיצור

יהי u ו"ע ל U עם ע"ע $\lambda = e^{2\pi i \alpha \cdot T}$

$$|\bar{0}\rangle \otimes |\bar{u}\rangle \rightarrow \frac{1}{\sqrt{T}}\sum_{j=0}^{T-1} |j\rangle \otimes |\bar{u}\rangle \rightarrow \frac{1}{\sqrt{T}}\sum_{j=0}^{T-1} |j\rangle \otimes \lambda^j |u\rangle$$

$T = 2^t$

$$= \left(\frac{1}{\sqrt{T}}\sum_{j=0}^{T-1} \lambda^j |j\rangle\right) \otimes |u\rangle$$

$$= \underbrace{\frac{1}{\sqrt{T}}\sum_j \omega^{kj} |j\rangle}_{FFT^{-1}}$$

$\alpha = \frac{bk}{T}$ מקרה 1

$$= |k\rangle \otimes |u\rangle$$

תרגיל 2: α כלשהו $\alpha\in[0,1]$

$$\frac{1}{\sqrt{T}}\sum_{j=0}^{T-1}\omega^{\alpha T j}|j\rangle \xrightarrow[FFT^{-1}]{} \frac{1}{T}\sum_{j=0}^{T-1}\sum_{k=0}^{T-1}\omega^{\alpha T j}\omega^{-kj}|k\rangle$$

$$=\sum_{k=0}^{T-1}\left(\frac{1}{T}\sum_{j=0}^{T-1}\omega^{(\alpha T-k)j}\right)|k\rangle$$

אם $\alpha T=j_0$ אז, אז רק $k=j_0$ שונה.

המקרה הכללי:

$$prob(k)=P_k=\frac{1}{T^2}\left|\sum_{j=0}^{T-1}\omega^{(\alpha T-k)j}\right|^2$$

אז:

$$\sum_{j=0}^{T-1}\omega^{(\alpha T-k)j}=\frac{\omega^{(\alpha T-k)T}-1}{\omega^{(\alpha T-k)}-1}$$

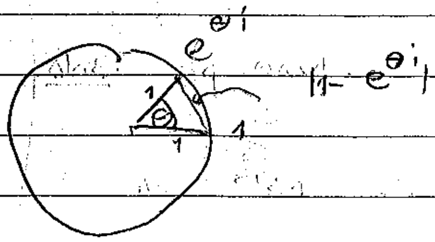
לכן

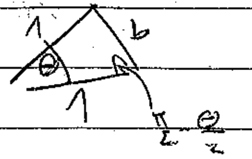
$$P_k=\frac{1}{T^2}\frac{|1-\omega^{(\alpha T-k)T}|^2}{|1-\omega^{\alpha T-k}|^2}\le\frac{2^2}{|1-\omega^{\alpha T-k}|^2}$$

נשים לב ש

$$|1-e^{\theta i}|=2\left|\sin\frac{\theta}{2}\right|$$

כי:





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

$$b=\frac{\sin\theta}{\cos\frac{\theta}{2}}=\boxed{2\sin\frac{\theta}{2}}$$

$$w^{\alpha T-k} = e^{\frac{2\pi i}{T}(\alpha T-k)} = e^{2\pi\cdot\frac{\alpha T-k}{T}i}$$ לכן

$$= e^{2\pi\Delta i}$$

עבור $\Delta = \frac{\alpha T-k}{T} \pmod 1$, מייצג קטן mod 1 $\Rightarrow \Delta\in\left[-\frac{1}{2},\frac{1}{2}\right]$

$$\left|1-w^{\alpha T-k}\right| = 2\sin\left(\frac{2\pi\Delta}{2}\right) = 2\sin(\pi\Delta)$$ לכן

$$\underset{\overset{\downarrow}{\sin(x)\geq\frac{2x}{\pi}}}{\geq} 2\cdot\frac{2\pi\Delta}{\pi} = 4\Delta$$

עבור $-\frac{\pi}{2}\leq x\leq\frac{\pi}{2}$

ולכן, עבור $k=j_0+d$ (כש $\frac{j_0}{T}$ הכי קרוב אפשרי ל α)

$$P_k \leq \frac{2^2}{(4\Delta)^2} \leq \frac{1}{4\Delta^2} \leq \frac{1}{4d^2}$$

$$\Delta = \left|\frac{\alpha T-k}{T}\right| = \frac{k}{T}-\alpha \geq d$$

~~[illegible]~~ עבור $\frac{j_0}{T}$ הכי קרוב ל α, $\varepsilon = \alpha - \frac{j_0}{T}$

מתקיים $|\varepsilon T| = |\frac{j_0}{T} - \alpha T| \le \frac{1}{2}$

$$\omega^{(\alpha T - j_0)T} = e^{2\pi i(\alpha T - j_0)} = e^{\varepsilon T \cdot 2\pi \cdot i}$$

ולכן $|1 - \omega^{(\alpha T - j_0)T}| = 2|\sin(\frac{2\pi}{2} \cdot \varepsilon T)| = 2|\sin(\pi \varepsilon \cdot T)|$

$$\ge 2 \cdot \frac{2\pi \varepsilon T}{\pi} = 4\varepsilon T$$

$|\varepsilon T| \le \frac{1}{2}$

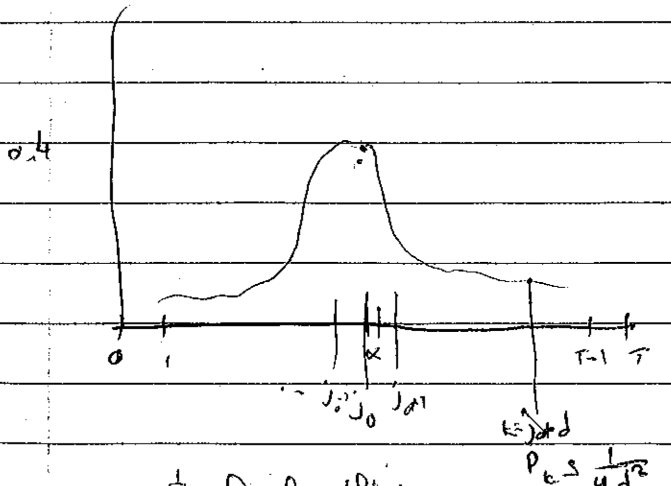
$-\frac{\pi}{2} \le x \le \frac{\pi}{2} \quad \sin(x) \ge \frac{2x}{\pi}$

$$|1 - \omega^{\alpha T - k}| = 2\sin(\pi\Delta) \underset{\forall x \sin(x) \le x}{\le} 2\pi\Delta = 2\pi\varepsilon$$

ונקבל ~~[illegible]~~

כאשר $\Delta = \frac{\alpha T - j_0}{T} = \alpha - \frac{j_0}{T} = \varepsilon$

ולכן $P_{j_0} \ge \frac{1}{T^2} \cdot \frac{(4\varepsilon T)^2}{(2\pi\varepsilon)^2} = \frac{16\varepsilon^2 T^2}{4\pi^2 \varepsilon^2 T^2} = \frac{4}{\pi^2} \approx 0.4$!



α [illegible] $\frac{1}{T}$

⑥

משפט: אם $t = \lceil \lg \frac{1}{\varepsilon} \rceil + \lceil \lg \frac{1}{\delta} \rceil$

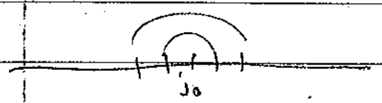
אז $pr\left[\begin{array}{c} \text{נקודת הערכה} \\ \text{שגויה ב } \varepsilon \end{array} \right] \leq \delta$

הוכחה: נשגה, אם נקח $k = j_0 \pm \varepsilon \cdot T$

כש j_0 השלם, הבא שמאלה, δ נק' ו $\frac{j_0}{T}$ הכי קרוב ל δ α.

$$pr(\text{נשגה}) = 2 \cdot \sum_{\underset{\text{מרחק}}{\overset{\downarrow}{d = \varepsilon T}}}^{\infty} \overset{k=j_0+d}{pr([illegible])} \leq \frac{2}{4} \sum_{d=\frac{1}{\delta}}^{\infty} \frac{1}{d^2} \leq \frac{1}{2} \int_{\frac{1}{\delta}}^{\infty} \frac{1}{x^2} dx = \frac{1}{2} \left(-\frac{1}{x}\right) \Big|_{\frac{1}{\delta}}^{\infty}$$

$$= \frac{1}{2} \cdot \frac{1}{\frac{1}{\delta}} = \boxed{\frac{\delta}{2}}$$



□

$\varepsilon T = \frac{1}{\delta}$

$T = \frac{1}{\varepsilon} \cdot \frac{1}{\delta}$

עובדה: רק בתנאי שיודעים לחשב ביעילות U^T !!!

אם רוצים דיוק של n ביטים, צריך לדעת לחשב $U^{(2^n)}$ יעיל!!!

[illegible] FFT$_n$ [illegible] גרף [illegible]

(א) קיילי גרף

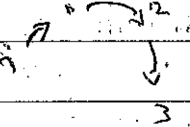
$G=(V,E)$ אם $A_{n\times n}$ אז $A_{ij}=f(\dots)$,

1. V חבורה

2. $A_{ij}=f(ij^{-1})$ עבור איזה $f: G\to \mathbb{C}$.

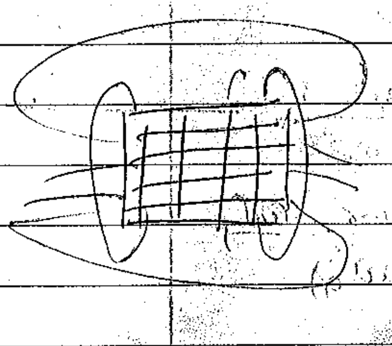
דוגמאות: 1. $G=C_q$ $C_n=(\mathbb{Z}_q, + \bmod q)$

$$A_{ij}=\begin{cases} 1 & j-i=1 \\ 0 & \text{אחרת} \end{cases}$$



2. $G=C_q\times C_q$

$$A_{ij}=\begin{cases} 1 \\ 0 & \text{אחרת} \end{cases}$$



3. קובייה $G=\mathbb{Z}_2^n$

$$f_{ij}=\{1 \iff j-i\in\{e_1,\dots,e_n\}$$

הכללה: גרף קיילי $Cay(G,S)$

$$A_{ij}=\{1 \iff ji^{-1}\in S\}$$ אם ⑧

אם S סגורה תחת הופכי, G אבל אז לא-מכוון.

משפט: יהי G אבלית, A מטריצת קיילי של G עם יוצרים S

כל הו"ע של A הם הקרקטרים של G
והע"ע של A ~~עם~~ עם ו"ע χ, הוא $\sum_{s\in S}\overline{\chi(s)}$

הוכחה: $(A\chi)_w = \sum_{v\in G} A_{wv}\,\chi(v) = \sum_{v\in G} f(wv^{-1})\,\chi(v)$

$$= \sum_{\substack{v'\in G\\ v'=wv^{-1}\\ v=}} f(v')\,\chi(w(v')^{-1}) = \underbrace{\left(\sum_{v'} f(v')\,\chi((v')^{-1})\right)}_{\text{צ"ל הע"ע}} \chi(w)$$

$\chi(z^{-1}) = (\chi(z))^{-1} = \overline{\chi(z)}$

$$= \sum_{v'} f(v')\,\overline{\chi(v')}$$

$$= \langle \chi, f\rangle$$

דוגמא: עבור q טבעי

$G = (\mathbb{Z}_n, +\bmod q)$

$S = \{1\}$

הו"ע הם $\chi_t = \sum_{k=0}^{q-1} \chi_t(k)\,|k\rangle$

הע"ע הם $\lambda_t = \overline{\chi_t(1)} = w^{-t} = e^{-\frac{2\pi i t}{q}}$

קירוב FFT_q עבור q כלשהו

יהי n הטבעי הראשון כך ש $q \le 2^n$

נגדיר

$$U: x \to (x+1) \pmod q$$

המטריצה U - אוניטרית על $B = span\{|0\rangle, \ldots, |q-1\rangle\}$

ו"ע שלו

$$x_t = \frac{1}{\sqrt q}\sum_k x_t(k)\ |k\rangle$$

עם ע"ע $\lambda_t = \omega^{-t} = e^{-\frac{2\pi i t}{q}}$

אנחנו רוצים לממש את FFT_q^{-1} שמעבירה $|x_t\rangle$ ל $|t\rangle$

רעיון ההוכחה:

$$|x_t\rangle \otimes |0\rangle \xrightarrow[\text{phase estimation}]{\text{קירוב}} |x_t\rangle \otimes |t\rangle$$

Ancilla

[illegible]

נשים לב שניתן לחשב U^m ביעילות לכל m

$$\xrightarrow{\text{Swap}} |t\rangle \otimes |x_t\rangle$$

$$\to |t\rangle \otimes |x_0\rangle$$

$$|t\rangle \otimes |x_t\rangle = \sum_k x_t(k)\ |t,k\rangle$$

נבצע הזזה

$|t,k\rangle \to \overline{x_t(k)}\ |t,k\rangle$ פעולה זו אוניטרית כי יש שבור

לסיכום: בהסתברות $1-\delta$ קירוב ε סיבוכיות בזמן qubits נוסף $O(\lg\lg\frac{1}{\delta} + \lg\frac{1}{\varepsilon})$