1. Show that the the dagger form of the unitary we found in class for the Fourier transform, $U_{FT}^\dagger = (H_3(V_{32}H_2)(V_{31}V_{21}H_1)(V_{30}V_{20}V_{10}H_0)P)^\dagger$, implements the inverse Fourier transform.

$$V_{ij} = e^{i\pi \frac{n_i n_j}{2^{|i-j|}}} \qquad P^\dagger = P$$

$$V_{ij}^\dagger = e^{-i\pi \frac{n_i n_j}{2^{|i-j|}}}$$

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

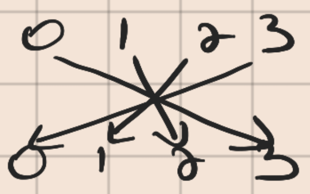
$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^\dagger = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$H^\dagger = H$$

בדגר במכפל כל בנפרד וסדר הפוך

$$U_{QFT}^\dagger = P\, H_0 V_{10}^\dagger V_{20}^\dagger V_{30}^\dagger H_1 V_{21}^\dagger V_{31}^\dagger H_2 V_{32}^\dagger H_3$$

נראה שאפשר להפוך את הסדרים



$0 \to 3$
$1 \to 2$
$2 \to 1$
$3 \to 0$

$$= H_3 V_{23}^\dagger V_{13}^\dagger V_{03}^\dagger H_2 V_{12}^\dagger V_{02}^\dagger H_1 V_{01}^\dagger H_0 P$$

$$= H_3 V_{23} H_2 V_{13} V_{03} V_{12} V_{02} H_1 V_{01} H_0 P$$

$$= H_3 V_{23}^\dagger H_2 V_{13}^\dagger V_{12}^\dagger H_1 V_{03}^\dagger V_{02}^\dagger V_{01}^\dagger H_0 P$$

$U_{QFT}^\dagger$ את בדיוק וקבלנו $V_{ij} = V_{ji}$!

(a) Find an operator U for which the operator U_f used in Shor's algorithm can be written as $U_f = \sum_j |j\rangle\langle j| \otimes U^j$, where the $|j\rangle\langle j|$ part acts on the first (input) register and the U^j part acts on the second (output) register. Hint: for the second register, choose a starting state $|y\rangle = |1\rangle_n$.

$$U_f |x\rangle_n |y\rangle_n = |x\rangle_n |y \oplus f(x)\rangle_n$$

$$f(x) = b^x \pmod N$$

$$U_f |x\rangle_n |1\rangle_n = |x\rangle_n |1 \oplus b^x \bmod N\rangle_n$$

נשים לב ש-U תלוי ב-j, לכן אם נפעיל

את ה-1 -ים ל- $b \bmod N$ נקבל $b^x \bmod N$

כלומר U לא תלוי בכלל ב-x לכן אפשר להגדיר

מהכלל: $U|1\rangle_n = |b \bmod N\rangle$

ובאופן כללי $U|y\rangle_n = |yb \bmod N\rangle$

לכן מתחילים מ- $|1\rangle_n$ → $U^x|y\rangle = |(yb)^x \bmod N\rangle$

ב) פונק' ב mod N תמיד מחזורית, מחזור $N=13$

$b=3$

$3^0 \bmod 13 = 1$ $\quad 3^1 \bmod 13 = 3$ $\quad 3^2 \bmod 13 = 9$

$3^3 \bmod 13 = 1$ $\quad 3^4 \bmod 13 = 3$ $\quad \ldots$

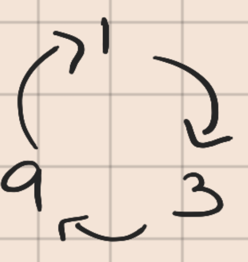
כלומר הפעולה של U^x אחת משלושת המצבים

$|1\rangle_n, |3\rangle_n, |9\rangle_n$ תמיד מחזירה את אחד משלושת המצבים

$U|1\rangle_n = |3\rangle_n$

$U|3\rangle_n = |9\rangle_n$

$U|9\rangle_n = |1\rangle_n$



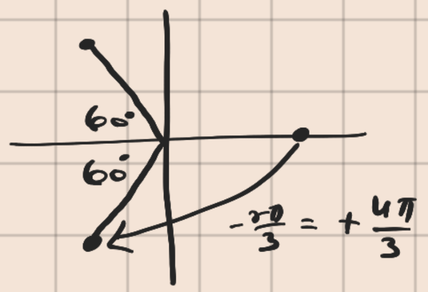
נשים לב שאם היינו מתחילים עם $|2\rangle_n$:

$U|2\rangle_n = |6\rangle_n$ $\quad U|6\rangle_n = |5\rangle_n$ $\quad U|5\rangle_n = |2\rangle_n$

לומר U מחלק את המרחב לתת' מרחבים סגורים
תחת הפעלת U בגודל $r=3$

קל לראות: $U(|1\rangle_n+|3\rangle_n+|9\rangle_n) = (|1\rangle_n+|3\rangle_n+|9\rangle_n) \equiv |\psi_0\rangle$

ולכן $\lambda_0 = 1 = e^{2\pi i 0} \Rightarrow \varphi_0 = 0$



$$U\left(e^{i\frac{2\pi}{3}}|1\rangle + e^{-i\frac{2\pi}{3}}|3\rangle + |9\rangle\right)$$
$$= \left(e^{i\frac{2\pi}{3}}|3\rangle + e^{-i\frac{2\pi}{3}}|9\rangle + |1\rangle\right)$$
$$= e^{-i\frac{2\pi}{3}}\left(e^{i\frac{2\pi}{3}}|1\rangle + e^{i\frac{4\pi}{3}}|3\rangle + |9\rangle\right) = \lambda_1|\psi_1\rangle$$
$$\lambda_1 = e^{-i\frac{2\pi}{3}} \Rightarrow \varphi_1 = -\frac{1}{3}$$

$$|\psi_2\rangle = \left(e^{-i\frac{2\pi}{3}}|1\rangle + e^{i\frac{2\pi}{3}}|3\rangle + |9\rangle\right)$$
$$\lambda_2 = e^{i\frac{2\pi}{3}} \Rightarrow \varphi_2 = \frac{1}{3}$$

לומר אחרי מדידת φ_i ע"י PE תמיד נקבל

$$\varphi_i = \frac{q}{r} \qquad q = 0, \pm 1, \pm 2, \dots$$

אך כפי שראינו לשם

$-\frac{2\pi}{3} = \frac{4\pi}{3}$

$\varphi = -\frac{1}{3}$ $\quad$ $\varphi = \frac{2}{3}$ $\qquad$ $\frac{2\pi}{3} = \frac{1}{3}$

אז כאן 3 $\quad q = 0, 1, 2$

או באופן כללי: $\quad q = 0, 1, \dots, r-1$

ג) נתחיל ב: $\quad |0\rangle_n|1\rangle_n$

נפעיל $H_1^{\otimes n}$: $\quad \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n|1\rangle_n$

נפעיל: $\sum |x\rangle\langle x| \otimes U^x$: $\quad \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n|b^x \bmod N\rangle$

נפעל פורייה או פורייה הפוך על הרגיסטר הראשון

ואז נקבל $\varphi_i = \frac{q}{r}$ ספציפי.

כל זוג ל q,r אין מכנה משותף אפשר מ״ג לדעת

מהו r אם יש אז צריך להפעיל מחדש לקבל φ

איתר עד שאין מכנה משותף.