EC 880 Homework 4

$\frac{46}{50}$

Name:	Onkar V Apte
USC ID:	[redacted]3

4.41

Exercise 4.41: This and the next two exercises develop a construction showing that the Hadamard, phase, controlled-NOT and Toffoli gates are universal. Show that

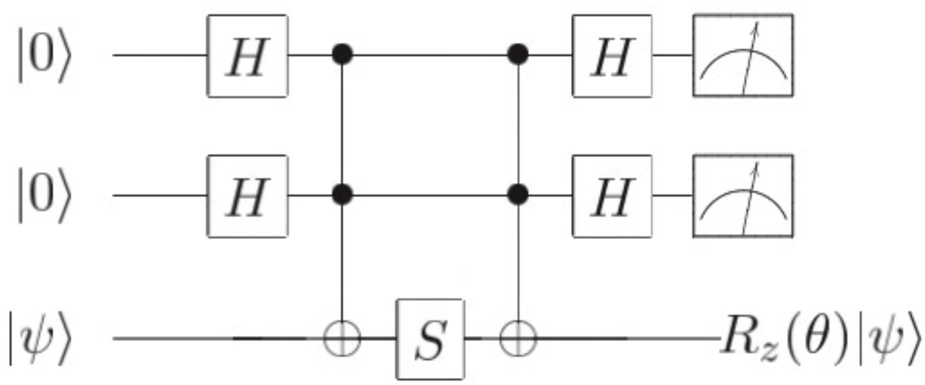


Figure 4.17. Provided both measurement outcomes are 0 this circuit applies $R_z(\theta)$ to the target, where $\cos\theta = 3/5$. If some other measurement outcome occurs then the circuit applies Z to the target.

the circuit in Figure 4.17 applies the operation $R_z(\theta)$ to the third (target) qubit if the measurement outcomes are both 0, where $\cos\theta = 3/5$, and otherwise applies Z to the target qubit. Show that the probability of both measurement outcomes being 0 is $5/8$, and explain how repeated use of this circuit and $Z = S^2$ gates may be used to apply a $R_z(\theta)$ gate with probability approaching 1.

$$|0\rangle|0\rangle|\psi\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |\psi\rangle$$

i.e. $\frac{1}{2}\left(\underline{|0\rangle+|1\rangle} \otimes \underline{|0\rangle+|1\rangle}\right) \otimes |\psi\rangle$

i.e. $\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \otimes |\psi\rangle$

i.e. $\frac{1}{2}\left(|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11\psi\rangle\right)$

$$\longrightarrow \frac{1}{2}\left(|00\psi\rangle + |01\psi\rangle + |10\psi\rangle + |11\,X\psi\rangle\right)$$

$$\longrightarrow \frac{1}{2}\Big(|00S\psi\rangle + |01S\psi\rangle + |10S\psi\rangle + |11SX\psi\rangle \Big)$$

$$\longrightarrow \frac{1}{2}\Big(|00S\psi\rangle + |01S\psi\rangle + |10S\psi\rangle + |11XSX\psi\rangle \Big)$$

$\begin{bmatrix}1\\1\end{bmatrix} \otimes \begin{bmatrix}1\\1\end{bmatrix} \otimes S\cdot|\psi\rangle$ $\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$ $\qquad$ $\begin{bmatrix}1\\1\end{bmatrix} \otimes \begin{bmatrix}1\\-1\end{bmatrix}$ — $\begin{bmatrix}1\\-1\\1\\-1\end{bmatrix}$

$$\longrightarrow \frac{1}{2}\Big(\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} |(0+1)(0+1)S\psi\rangle + \frac{1}{2}|(0+1)(0-1)S\psi\rangle$$

$\begin{bmatrix}1\\-1\end{bmatrix} \begin{bmatrix}1\\1\end{bmatrix}$ - $\begin{bmatrix}1\\1\\-1\\-1\end{bmatrix}$ $\qquad$ $\begin{bmatrix}1\\-1\end{bmatrix} \begin{bmatrix}1\\-1\end{bmatrix}$ — $\begin{bmatrix}1\\-1\\-1\\1\end{bmatrix}$

$$+ \frac{1}{2}|(0-1)(0+1)S\psi\rangle + \frac{1}{2}|(0-1)(0-1)XSX\psi\rangle \Big)$$

i.e.
$$\frac{1}{4}\left(\begin{aligned} &|00\rangle|(S+S+S+XSX)\psi\rangle \\ &+|01\rangle|(S-S+S-XSX)\psi\rangle \\ &+|10\rangle|(S+S-S-XSX)\psi\rangle \\ &+|11\rangle|(S-S-S+XSX)\psi\rangle \end{aligned} \right)$$

$\because$ it is given that measurements on qubit #1 & #2 gives 0, i.e. $|00\rangle$, qubit # 3 is now $\frac{1}{4}|(3S+XSX)\psi\rangle$

$$\therefore \frac{1}{4}(3S+XSX) = \frac{1}{4}\left[3\begin{bmatrix}1&0\\0&i\end{bmatrix} + \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&i\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix} \right]$$

$$= \frac{1}{4}\begin{bmatrix}3+i&0\\0&3i+1\end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix}3+i&0\\0&i(3-i)\end{bmatrix} \qquad \text{———} \ ①$$

compairing $3+i$ with $re^{i\phi}$, $r = \sqrt{9+1} = \sqrt{10}$

$\phi = \tan^{-1}\left(\frac{1}{3}\right)$ ——— (2)

$\therefore$ our matrix (1) becomes,

$$= \frac{1}{4}\begin{bmatrix} \sqrt{10}\, e^{i\phi} & 0 \\ 0 & i\left(\sqrt{10}\, e^{-i\phi}\right) \end{bmatrix}$$

$$= \frac{\sqrt{10}}{4}\begin{bmatrix} e^{i\phi} & 0 \\ 0 & i\, e^{-i\phi} \end{bmatrix}$$

$$= \frac{\sqrt{10}}{4}\, e^{\frac{i\pi}{4}}\begin{bmatrix} e^{i(\phi-\frac{\pi}{4})} & 0 \\ 0 & i\, e^{-i(\phi+\frac{\pi}{4})} \end{bmatrix}$$

Now, Let $R_z(\theta) = e^{\frac{-i\theta Z}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z$

$$= \begin{bmatrix} \cos\theta/2 & 0 \\ 0 & \cos\theta/2 \end{bmatrix} - i\begin{bmatrix} \sin\frac{\theta}{2} & 0 \\ 0 & -i\sin\frac{\theta}{2} \end{bmatrix}$$

$$= \begin{bmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2} & 0 \\ 0 & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2} \end{bmatrix}$$

$$= \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$$

compairing this with our previous result, we get

$$e^{i(\phi-\frac{\pi}{4})} = e^{\frac{-i\theta}{2}}$$

$\therefore \quad \frac{\theta}{2} = \frac{\pi}{4} - \phi$

$\therefore \quad \theta = \frac{\pi}{2} - 2\phi$

$\therefore \cos\theta = \cos\left(\frac{\pi}{2} - 2\phi\right)$

$= \sin(2\phi)$

$= \dfrac{2\tan\phi}{1+\tan^2\phi}$

& $\because \tan\phi = \frac{1}{3}$ —— (from ②)

$= \dfrac{2\left(\frac{1}{3}\right)}{1+\left(\frac{1}{9}\right)} = \frac{\cancel{2}^{1}}{\cancel{3}_{1}} \times \frac{\cancel{9}^{3}}{\cancel{10}_{5}} = \frac{3}{5}$

$\therefore \cos\theta = \frac{3}{5}$

→ Hence, we have proved that when measurement outcome of qubit #1 & #2 is 0 & 0, the circuit perform $R_z(\theta)$ on qubit #3 where $\cos\theta = \frac{3}{5}$

$\because$ Amplitude of first term $\longrightarrow \frac{\sqrt{10}}{4} \cdot e^{i\frac{\pi}{4}}$

$\therefore$ Probability $= \left(\frac{\sqrt{10}}{4}\right)^2 = \frac{5}{8}$

$\therefore$ Probability of both measurement outcomes being 0 is $\frac{5}{8}$

when two states are not $|0\rangle|0\rangle$,

third qubit is in state $\frac{1}{4}\,|(S - XSX)\psi\rangle$

$$\frac{1}{4}(S - XSX) = \frac{1}{4}\left[\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} - \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right]$$

$$= \frac{1}{4}\begin{bmatrix}1-i & 0\\ 0 & i-1\end{bmatrix}$$

compairing with $re^{i\phi}$, $r = \sqrt{2}$, $\phi = \tan^{-1}(-1)$

$$= \frac{\pi}{4}$$

$$= \frac{\sqrt{2}}{4}\begin{bmatrix}e^{i\frac{\pi}{4}} & 0\\ 0 & ie^{-i\frac{\pi}{4}}\end{bmatrix}$$

factoring out global phase $\frac{\pi}{4}$ gives us

$$= \frac{\sqrt{2}}{4}\,e^{i\pi/4}\begin{bmatrix}e^{\frac{i\pi}{4} - \frac{i\pi}{4}} & 0\\ 0 & ie^{-\frac{i\pi}{4} + \frac{\pi}{4}}\end{bmatrix}$$

$$= \frac{\sqrt{2}}{4}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$= \frac{\sqrt{2}}{4}\,Z$$

$\boxed{\text{Hence we have shown that for measurement } M_1M_2 \neq 00 \text{, i.e. } M_1M_2 = 01 \text{ or } 10 \text{ or } 11 \text{, the given circuit performs } Z \text{ gate on third qubit}}$

Now, if circuit is used,

$R_z(\theta)|\psi\rangle$ is applied w/ $p = 5/8$

& $Z|\psi\rangle$ is applied w/ $p = 3/8$

if $Z|\psi\rangle$ is applied, then applying Z again gives us $|\psi\rangle$.

Now again apply the circuit until $R_z(\theta)|\psi\rangle$ occurs.

$\therefore$ Probability of applying $R_z(\theta)$ like this $\rightarrow$

$$\frac{5}{8} + \frac{3}{8} \cdot \frac{5}{8} + \frac{3}{8} \cdot \frac{3}{8} \cdot \frac{5}{8} + \cdots$$

$$= \frac{5}{8} + \frac{3}{8} \cdot \frac{5}{8} + \left(\frac{3}{8}\right)^2 \frac{5}{8} + \left(\frac{3}{8}\right)^3 \frac{5}{8}$$

if $a = \frac{5}{8}$, $r = \frac{3}{8}$, geometric sum $= \frac{a}{1-r}$

$$= \frac{\frac{5}{8}}{1 - \frac{3}{8}}$$

$$= 1$$

Hence, with the use of the given circuit & Z gate, we can apply $R_z(\theta)$ such that its probability approaches 1.

4.42

Exercise 4.42: (Irrationality of θ) Suppose $\cos\theta = 3/5$. We give a proof by contradiction that θ is an irrational multiple of 2π.

(1) Using the fact that $e^{i\theta} = (3+4i)/5$, show that if θ is rational, then there must exist a positive integer m such that $(3+4i)^m = 5^m$.

(2) Show that $(3+4i)^m = 3+4i \pmod 5$ for all $m > 0$, and conclude that no m such that $(3+4i)^m = 5^m$ can exist.

assume θ is a rational multiple of 2π.

$\therefore \theta = 2\pi \cdot \frac{n}{m}$ ——— ($n, m \to$ integers)

$\because e^{i\theta} = \frac{3+4i}{5}$, $e^{i\frac{2\pi n}{m}} = \frac{3+4i}{5}$

$\therefore e^{i\left(\frac{2\pi n}{\cancel{m}}\right)\cancel{m}} = \frac{(3+4i)^m}{5^m}$

$\therefore e^{i2\pi n} = \frac{(3+4i)^m}{5^m}$

$\therefore 1 = \frac{(3+4i)^m}{5^m}$

$\therefore \boxed{(3+4i)^m = 5^m}$

consider $m = 2$.

$(3+4i)^2 = 9 - 16 + 24i$

$= -7 + 24i$

$= (3+4i) \bmod 5$

$\therefore$ to Show, $(3+4i)^m = (3+4i) \mod 5 \longrightarrow$ assume is true.

consider $(3+4i)^{m+2} = (3+4i)^m \cdot (3+4i)^2$

$= (3+4i)^m + (3+4i) \mod 5$

$= (3+4i)^{m+1} \mod 5$

$\therefore$ By inductive reasoning, our assumption

$\boxed{(3+4i)^m = (3+4i) \mod 5 \quad \text{is true.}}$ *

but $\because (3+4i)^m = 5^m$,

$5^m = 3+4i \mod 5$

$\therefore 0 = 3+4i$ ——— Contradiction

Hence our original assumption was wrong.

$\therefore$ $\boxed{\text{no } m \text{ exist such that } (3+4i)^m = 5^m}$

$\therefore$ $\boxed{\theta \text{ is NOT a rational multiple of } 2\pi.}$

4.43

Exercise 4.43: Use the results of the previous two exercises to show that the Hadamard, phase, controlled-NOT and Toffoli gates are universal for quantum computation.

Since, for irrational multiple of 2π, we know that:

$$E\left(R_z(\alpha), R_z(\theta)^n\right) < \frac{\varepsilon}{3},$$

for any α, $H R_z(\alpha) H = H\left(\cos\frac{\alpha}{2} I - i \sin\frac{\alpha}{2} Z\right) H$

$\because$ $HIH = I$,
$HZH = X$,

$$= \cos\frac{\alpha}{2} I - i \sin\frac{\alpha}{2} X$$

$$= R_x(\alpha)$$

$$\therefore \quad E\left(R_x(\alpha), R_x(\theta)^n\right) < \frac{\varepsilon}{3}$$

$\because$ we can perform any unitary along two axis with three rotations, $U = R_n(\beta) R_m(\gamma) R_n(\delta)$,

For our R_x & R_z, $E\left(U, R_z(\theta)^{n_1} H R_z(\theta)^{n_2} H R_z(\theta)^{n_3}\right) < \varepsilon$

Hence, we can approximate any unitary gate w/ H, S, CNOT & Toffoli

5.4

Exercise 5.4: Give a decomposition of the controlled-R_k gate into single qubit and CNOT gates.

R_k gate is given by :

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i2\pi}{2^k}} \end{bmatrix}$$

$$\therefore \quad R_k^{\,2} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i2\pi}{2^k}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i2\pi}{2^k}} \end{bmatrix}$$

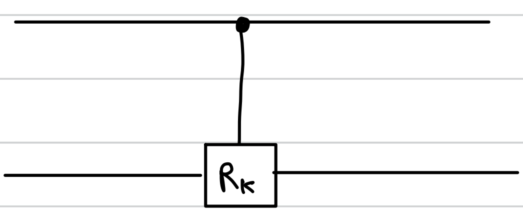
$$= \begin{bmatrix} 1 & 0 \\ 0 & e^{\left(\frac{i2\pi}{2^k}\right)^2} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i2\pi}{2^{k-1}}} \end{bmatrix} = R_{k-1}$$

$\therefore \quad R_k^{\,2} = R_{k-1}$

$\therefore \quad R_{k+1}^{\,2} = R_k$

controlled R_k

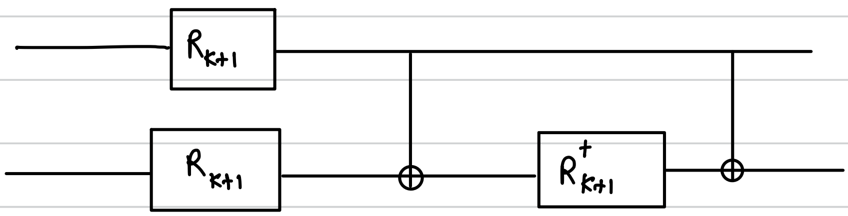


$$\Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{i2\pi}{2^k}} \end{bmatrix}$$

$\therefore$ identity for $|00\rangle$, $|01\rangle$, $|10\rangle$.

Controlled - R_k only changes $|11\rangle$.

∴ consider the circuit:



$|00\rangle \rightarrow |00\rangle \rightarrow |00\rangle \rightarrow |00\rangle \rightarrow |00\rangle$

$|01\rangle \rightarrow R_{k+1}|01\rangle \rightarrow R_{k+1}|01\rangle \rightarrow R^\dagger_{k+1} R_{k+1}|01\rangle$

i.e. $|01\rangle \rightarrow |01\rangle$

$|10\rangle \rightarrow R_{k+1}|10\rangle \rightarrow R_{k+1}|11\rangle \rightarrow R^\dagger_{k+1} R_{k+1}|11\rangle$

i.e. $|11\rangle \rightarrow |10\rangle$

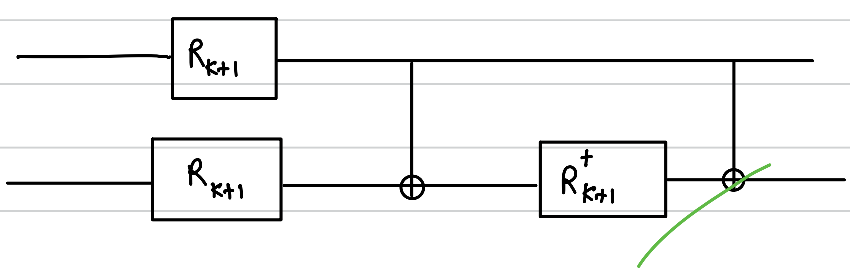
identity on i/p $|00\rangle, |10\rangle, |11\rangle$.

$|11\rangle \rightarrow R^2_{k+1}|11\rangle$

i.e. $R_k|11\rangle \rightarrow R_k|10\rangle \rightarrow R_k|10\rangle \rightarrow R_k|11\rangle$

R_k rotation on $|11\rangle$.

∴ This is the required decomposition of controlled R_k

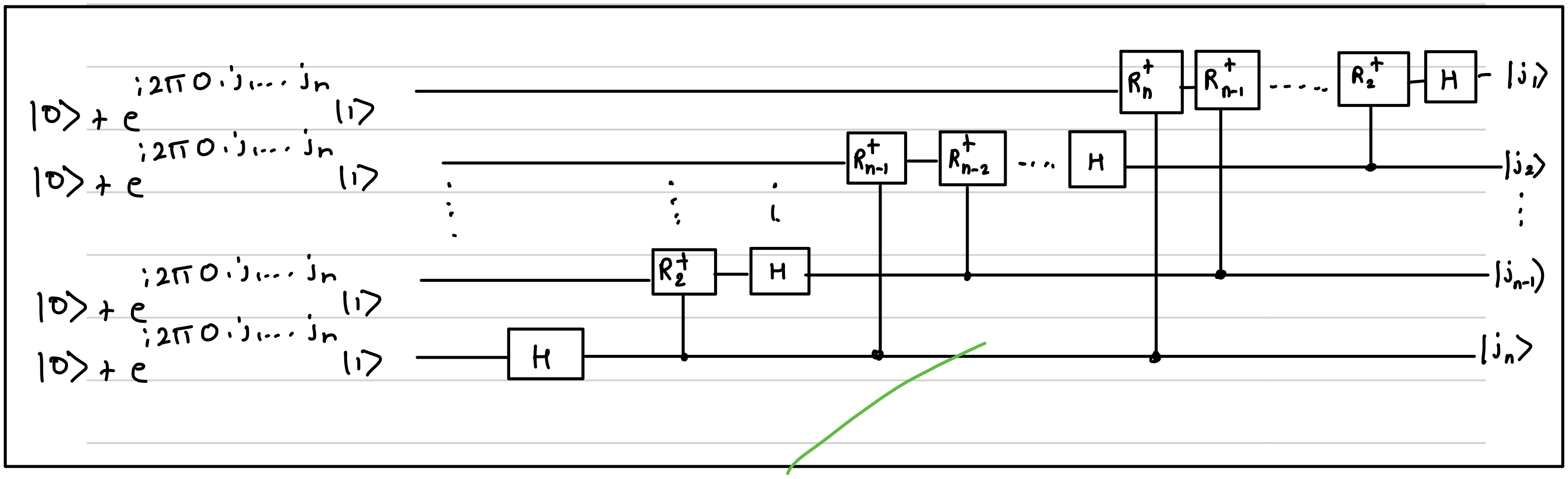


5.5

Exercise 5.5: Give a quantum circuit to perform the inverse quantum Fourier transform.

inverse QFT would just be applying all QFT transformation's hermitian conjugate.

∴ the required circuit is :



5.7

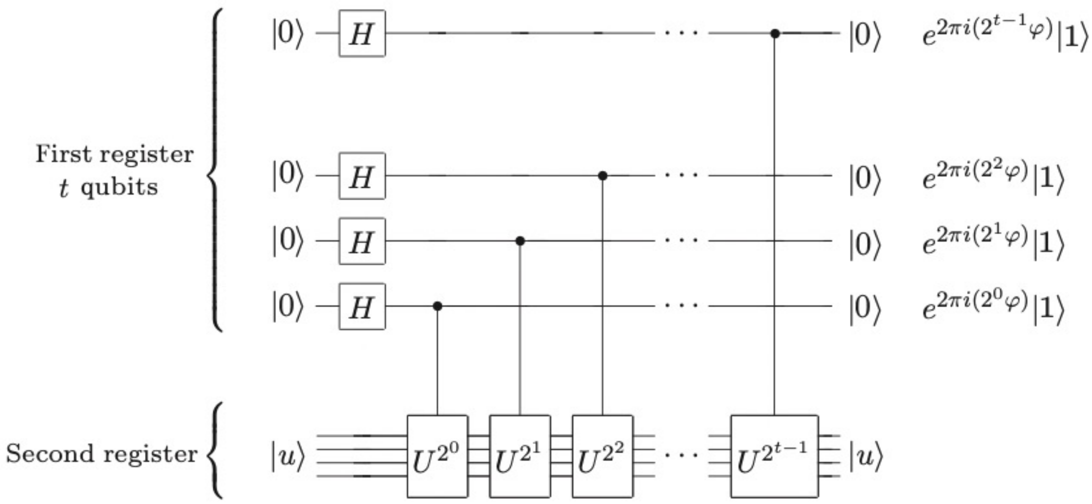


Figure 5.2. The first stage of the phase estimation procedure. Normalization factors of $1/\sqrt{2}$ have been omitted, on the right.

Exercise 5.7: Additional insight into the circuit in Figure 5.2 may be obtained by showing, as you should now do, that the effect of the sequence of controlled-U operations like that in Figure 5.2 is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j|u\rangle$. (Note that this does not depend on $|u\rangle$ being an eigenstate of U.)

$$|j_0\rangle \ldots |j_{t-1}\rangle U^{j_0 2^0} \ldots U^{j_{t-1} 2^{t-1}} |u\rangle$$

$$= |j\rangle U^{j_0 2^0} \ldots U^{j_{t-1} 2^{t-1}} |u\rangle$$

$$= |j\rangle U^{j_0 2^0 + j_{t-1} 2^{t-1}} |u\rangle$$

$$= |j\rangle U^{j} |u\rangle$$

- Hence we showed that effect of given sequences of control-Us is $|j\rangle|u\rangle \longrightarrow |j\rangle U^j |u\rangle$

$\boxed{5.10}$

Exercise 5.10: Show that the order of $x = 5$ modulo $N = 21$ is 6.

<u>To prove</u> : (order of 5 mod 21) = 6

$\therefore$ we have to show $5^6 = 1 \mod 21$

$\therefore$ LHS $= 5^6$
$= 125 \times 125$
$= 15625$

$\therefore$ RHS $= 1 \mod 21$
$= 1 + 21n$
for $n = 744$,

$= 1 + 21(744)$
$= 1 + 15624$
$= 15625$

$\therefore$ LHS = RHS.

Hence showed that order of 5 mod 21 is 6

5.14

Exercise 5.14: The quantum state produced in the order-finding algorithm, before the inverse Fourier transform, is

$$|\psi\rangle = \sum_{j=0}^{2^t-1} |j\rangle U^j |1\rangle = \sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle\,, \tag{5.46}$$

if we initialize the second register as $|1\rangle$. Show that the same state is obtained if we replace U^j with a *different* unitary transform V, which computes

$$V|j\rangle|k\rangle = |j\rangle|k + x^j \bmod N\rangle\,, \tag{5.47}$$

and start the second register in the state $|0\rangle$. Also show how to construct V using $O(L^3)$ gates.

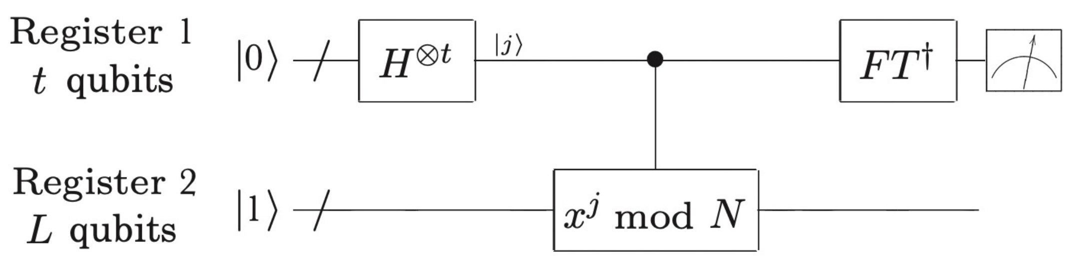


Figure 5.4. Quantum circuit for the order-finding algorithm. The second register is shown as being initialized to the $|1\rangle$ state, but if the method of Exercise 5.14 is used, it can be initialized to $|0\rangle$ instead. This circuit can also be used for factoring, using the reduction given in Section 5.3.2.

$\because \quad |z\rangle|y\rangle = |z\rangle U^{z_t 2^{t-1}} \cdots U^{z_1 2^0} |y\rangle$

$= |z\rangle |x_1^{z_t 2^{t-1}} \cdots x^{z_1 2^0} y \ (\mathrm{mod}\ N)\rangle$

Substituting $x^z \bmod N$ for $(x^{z_1 2^{t-1}} (\mathrm{mod}\ N)) \ldots (x^{z_1 2^0} (\mathrm{mod} N))$,

we get $|z\rangle|y\rangle \rightarrow |z\rangle x^2 y\ (\mathrm{mod}(N)))$

Substituting some V where $V|j\rangle|k\rangle = |j\rangle|k + x^j \bmod N\rangle$,

gives $w \sum_{j=0}^{2^t-1} |j\rangle V|1\rangle \rightarrow \underline{\underline{\sum_{j=0}^{2^t-1} |j\rangle |x^j \bmod N\rangle}}$

same state!

Problem 1

Problem 1 (Another Universal Set–*originally Problem 3 from HW 3*)

Show that the controlled-$(iR_x(\pi a))$ and controlled-$(iR_z(\pi a))$ gates, with a an irrational number, together form a universal set of quantum gates, provided that ancilla qubits (initialized in states $|0\rangle$ or $|1\rangle$) are available.

$\because$ a is irrational, πa is irrational multiple of π.

$\alpha = \pi a$.

$\because$ we know, $E\left(R_z(\alpha)\ R_z(\theta)^n\right) < \frac{\varepsilon}{3}$

& $\because$ $R_x(\alpha) = H R_z(\alpha) H$ ——— (shown in 4.43)

$\therefore$ $E\left(R_x(\alpha),\ R_x(\theta)^n\right) < \frac{\varepsilon}{3}$

& $\because$ any unitary can be written as

$$U = R_z(\beta)\ R_x(\gamma)\ R_z(\delta),$$

$$E\left(U,\ R_z(\theta)^{n_1},\ R_x(\theta)^{n_2},\ R_z(\theta)^{n_3}\right) < \varepsilon$$

$\therefore$ Controlled $R_x(\pi a)$ & $R_z(\pi a)$ form a universal set.

$\because$ Controlled $iR_x(\pi a)$ & $iR_z(\pi a)$ only add a global phase of i,

$\boxed{\text{controlled } iR_x(\pi a) \text{ \& } iR_z(\pi a) \text{ gates are also universal.}}$

Problem 2

Problem 2. Consider the Fourier transform on *n* qubits, as shown in section 5.1 of the book, whose circuit is given on page 219. Suppose that we replace all the controlled-*R* gates for $k > \log(n) + c$ with the identity instead, for some small constant integer *c*. Put a bound on the total error that will result.

for one R gate, error after replacing would be $\| R_k - I \|$. if largest eigenvalue of R_k is λ, this value would be $\lambda - 1$.

$\times$

-4