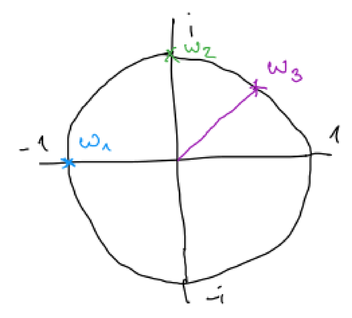
Implementing Quantum Fourier Transform

$$QFT|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{x\cdot y} |y\rangle$$ x, y bitstrings, $\cdot$ is multiplication

$N = 2^n$



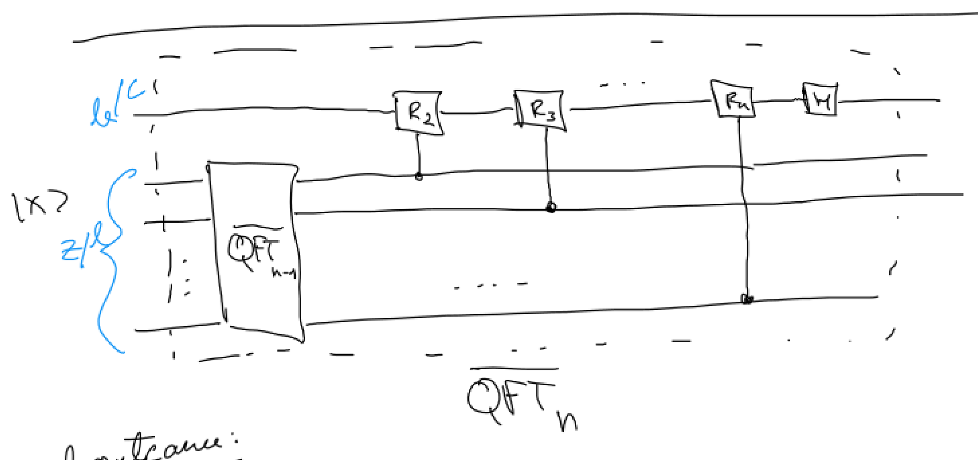
$e^{2\pi i} = 1$

$\omega_n = e^{\frac{2\pi i}{2^n}}$

$\omega_{n+k}^{c} = \omega_n$???

$\omega_n^2 = \omega_{n-1}$

$\omega_n = e^{\frac{2\pi i}{2^n}} = e^{\frac{2\pi i \cdot 2^k}{2^n \cdot 2^k}} = \left(e^{\frac{2\pi i}{2^{n+k}}}\right)^{2^k} = \omega_{n+k}^{2^k}$



$$\overline{QFT}|x\rangle \to \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{\bar{x}\cdot y} |y\rangle$$

$\bar{x} = x$ but bits swapped

$0011 \to 1100$

$QFT_n = \overline{QFT}_n U$

$U|x\rangle \to |\bar{x}\rangle$

Desired outcome:

$|x\rangle = |b\rangle \otimes |z\rangle = |bz\rangle$

$$\overline{QFT}_n |bz\rangle = \frac{1}{\sqrt{2^n}} \sum_{\substack{c\in\{0,1\},\\ l\in\{0,1\}^{n-1}}} \omega_N^{\overline{bz}\cdot cl} |cl\rangle$$

$1\,0\,0\,1\,1$
$2^4\,2^3\,2^2\,2^1\,2^0$

$\overline{bz} \cdot cl = (2\bar{z} + b)(l + c\cdot 2^{n-1}) =$

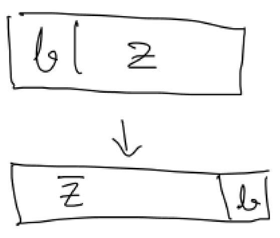
$cl = l + c \cdot 2^{n-1}$

$\overline{bz} = 2\cdot\bar{z} + b$

$= 2\bar{z}l + 2^n \cdot \bar{z} \cdot c + b\cdot l + b\cdot c\cdot 2^{n-1}$

want to get

$357 \cdot 931 = (3\cdot 100 + 57)(9\cdot 100 + 31)$



Basis:

$$\overline{QFT}_1 |x\rangle = \frac{1}{\sqrt{2^1}} \sum_{b\in\{0,1\}} \omega_1^{\bar{x}\cdot b} |b\rangle$$

$$\overline{QFT}_1 |0\rangle = \frac{1}{\sqrt{2}} \underset{-1}{\omega_1^{0\cdot 0}} |0\rangle + \frac{1}{\sqrt{2}} \underset{-1}{\omega_1^{0\cdot 1}} |1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\overline{QFT}\ |1\rangle = \frac{1}{\sqrt{2}} \omega_1^{1\cdot 0}|0\rangle + \frac{1}{\sqrt{2}} \underset{-1}{\omega_1^{1\cdot 1}} |1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$\overline{QFT}_1 = QFT_1 = H$

Step:

$$|bz\rangle \xrightarrow{I\otimes \overline{QFT}_{n-1}} \frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_{n-1}^{\bar{z}\cdot l} |bl\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_n^{2\cdot\bar{z}\cdot l} |bl\rangle$$

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

$R_n|0\rangle = |0\rangle$ $\qquad \omega_n^0 = 1$

$R_n|1\rangle = \omega_n|1\rangle$

$R_n|b\rangle = \omega_n^b|b\rangle$

$C_n|00\rangle \to |00\rangle$ (Rotating, control)

$C_n|10\rangle \to |10\rangle$

$C_n|01\rangle \to |01\rangle$

$C_n|11\rangle \to \omega_n|11\rangle$

$C_n|ab\rangle \to \omega_n^{a\cdot b}|ab\rangle$

$y = y_1 y_2 \ldots$

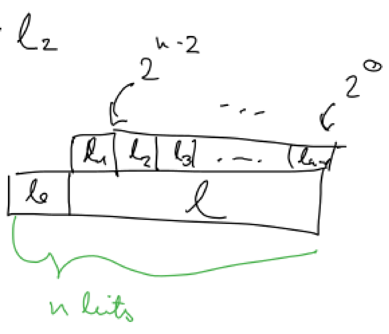
y_1 controls R_2

$\omega_2 = \omega_n^{2^{n-2}}$

R_3 controlled by l_2

$\omega_3^{b\cdot l_2} = \omega_n^{2^{n-3}\cdot b\cdot l_2}$

$R_4 \quad \omega_n^{2^{n-4}\cdot b\cdot l_3}$



$237 = 2\cdot 100 + 3\cdot 10 + 7$

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_n^{2\cdot\bar{z}\cdot l} |bl\rangle \xrightarrow{R_2} \frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_n^{2\bar{z}l} \cdot \omega_2^{b\cdot y_1} |bl\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_n^{2\bar{z}l + 2^{n-2}\cdot b\cdot l_1} \to$$

$\omega_n^{b\cdot y_1}$

$2^{n-2}\cdot b\cdot l_1 + 2^{n-3}\cdot b\cdot l_2 + 2^{n-4}\cdot b\cdot l_3 \ldots =$

$= b\cdot(\underbrace{2^{n-2}\cdot l_1 + 2^{n-3}\cdot l_2 + \ldots}_{l})$

$$\to \frac{1}{\sqrt{2^{n-1}}} \sum_{l=0}^{2^{n-1}-1} \omega_n^{2\bar{z}\cdot l + b\cdot l} \xrightarrow{H\otimes I} \frac{1}{\sqrt{2^{n-1}}} \cdot \frac{1}{\sqrt{2}} \sum_{\substack{l\in\{0,1\}^{n-1}\\ c\in\{0,1\}}} \omega_n^{2\bar{z}l + b\cdot l + b\cdot c\cdot 2^{n-1}} \cdot 1 |cl\rangle =$$

$\omega_n^{2^n\cdot\bar{z}\cdot c}$

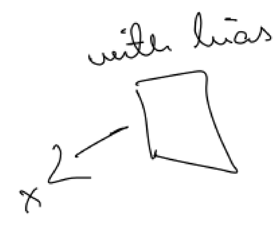
$$\boxed{H|x\rangle \to \frac{1}{\sqrt{2}} \sum_{c\in\{0,1\}} \omega_1^{x\cdot c} |c\rangle}$$

$$\to \frac{1}{\sqrt{2^n}} \sum_{\substack{l\in\{0,1\}^{n-1}\\ c\in\{0,1\}}} \omega_n^{2\bar{z}l + b\cdot l + b\cdot c\cdot 2^{n-1} + 2^n\cdot\bar{z}\cdot c} |cl\rangle =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_n^{\bar{x}\cdot y} |y\rangle$$

Von Neumann extractor

with bias b $\quad$ IID



$P_r[x=0] = b$

$P_r[x=1] = 1-b$

Sample bits x_1, x_2

$00 \to$ Reuse as "0"

$01 \to$ bit $= 0$ $\qquad b\cdot(1-b)$

$\qquad\qquad\qquad\qquad \shortparallel$

$10 \to$ bit $= 1$ $\qquad (1-b)\cdot b$

$11 \to$ reuse "1"

0000

$00|11$

$11|00$

1111