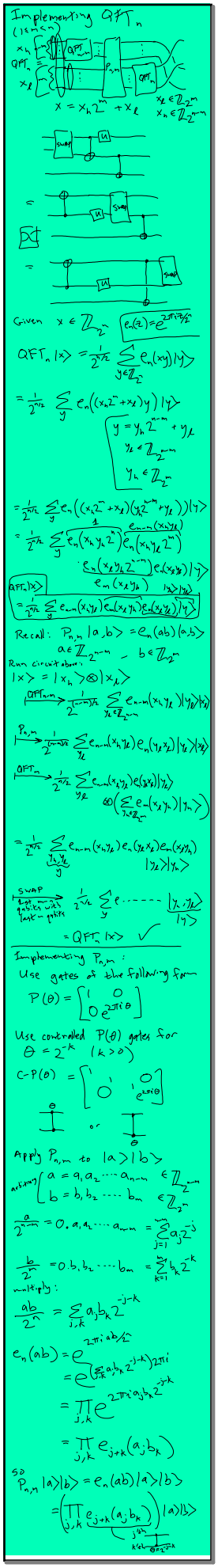
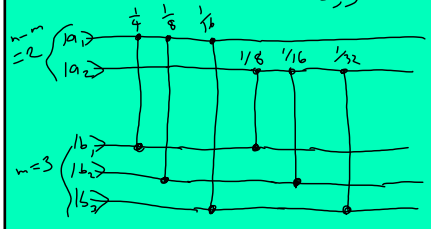

Implementing QFT_n
$(1 \le m < n)$
QFT_n =
$x = x_h 2^{n-m} + x_\ell$
$x_h \in \mathbb{Z}_{2^m}$
$x_\ell \in \mathbb{Z}_{2^{n-m}}$
swap
R_k
Given $x \in \mathbb{Z}_{2^n}$
$e_n(z) = e^{2\pi i z/2^n}$
$QFT_n|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{Z}_{2^n}} e_n(xy)|y\rangle$
$= \frac{1}{2^{n/2}} \sum_y e_n((x_h 2^{n-m} + x_\ell)y)|y\rangle$
$y = y_h 2^{n-m} + y_\ell$
$y_\ell \in \mathbb{Z}_{2^{n-m}}$
$y_h \in \mathbb{Z}_{2^m}$
$= \frac{1}{2^{n/2}} \sum_y e_n((x_h 2^{n-m} + x_\ell)(y_h 2^{n-m} + y_\ell))|y\rangle$
$= \frac{1}{2^{n/2}} \sum_y e_n(x_h y_h 2^n) e_{n-m}(x_h y_\ell) e_n(x_\ell y_h 2^m) e_n(x_\ell y_\ell)|y\rangle$
$e_n(x_h y_h 2^n) = 1$
$e_n(x_\ell y_h 2^m) = e_{n-m}(x_\ell y_h)$
$e_n(x_\ell y_\ell)$ $|x_h\rangle|y_h\rangle$
$QFT_n|x\rangle$
$= \frac{1}{2^{n/2}} \sum_y e_{n-m}(x_h y_\ell) e_{n-m}(x_\ell y_h) e_n(x_\ell y_\ell)|y\rangle$
Recall: $P_{n,m}|a,b\rangle = e_n(ab)|a,b\rangle$
$a \in \mathbb{Z}_{2^{n-m}}$, $b \in \mathbb{Z}_{2^m}$
Run circuit above:
$|x\rangle = |x_h\rangle \otimes |x_\ell\rangle$
$\xrightarrow{QFT_{n-m}} \frac{1}{2^{(n-m)/2}} \sum_{y_\ell \in \mathbb{Z}_{2^{n-m}}} e_{n-m}(x_\ell y_\ell)|y_\ell\rangle|x_h\rangle$
$\xrightarrow{P_{n,m}} \frac{1}{2^{(n-m)/2}} \sum_{y_\ell} e_{n-m}(x_h y_\ell) e_n(y_\ell x_\ell)|y_\ell\rangle|x_h\rangle$
$\xrightarrow{QFT_m} \frac{1}{2^{n/2}} \sum_{y_\ell} e_{n-m}(x_h y_\ell) e(y_\ell)|y_\ell\rangle$
$\otimes \left(\sum_{y_h \in \mathbb{Z}_{2^m}} e_m(x_\ell y_h)|y_h\rangle \right)$
$= \frac{1}{2^{n/2}} \sum_{y_\ell, y_h, y} e_{n-m}(x_h y_\ell) e_n(y_\ell x_\ell) e_m(x_\ell y_h)$
$|y_\ell\rangle|y_h\rangle$
$\xrightarrow{\text{SWAP}}$ $\frac{1}{2^{n/2}} \sum_y e \cdots |y_h, y_\ell\rangle$
$|y\rangle$
$= QFT_n|x\rangle$ ✓
Implementing $P_{n,m}$:
Use gates of the following form
$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i \theta} \end{bmatrix}$
Use controlled $P(\theta)$ gates for $\theta = 2^{-k}$ $(k > 0)$
$C\text{-}P(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i \theta} \end{bmatrix}$
θ or θ
Apply $P_{n,m}$ to $|a\rangle|b\rangle$
arbitrary $a = a_1 a_2 \cdots a_{n-m} \in \mathbb{Z}_{2^{n-m}}$
$b = b_1 b_2 \cdots b_m \in \mathbb{Z}_{2^m}$
$\frac{a}{2^{n-m}} = 0.a_1 a_2 \cdots a_{n-m} = \sum_{j=1}^{n-m} a_j 2^{-j}$
$\frac{b}{2^m} = 0.b_1 b_2 \cdots b_m = \sum_{k=1}^{m} b_k 2^{-k}$
multiply:
$\frac{ab}{2^n} = \sum_{j,k} a_j b_k 2^{-j-k}$
$e_n(ab) = e^{2\pi i ab/2^n}$
$= e^{\left(\sum_{j,k} a_j b_k 2^{-j-k}\right) 2\pi i}$
$= \prod_{j,k} e^{2\pi i a_j b_k 2^{-j-k}}$
$= \prod_{j,k} e_{j+k}(a_j b_k)$
So $P_{n,m}|a\rangle|b\rangle = e_n(ab)|a\rangle|b\rangle$
$= \left(\prod_{j,k} e_{j+k}(a_j b_k) \right) |a\rangle|b\rangle$
$j+k \le n$
$k \le m$
$\theta = 2^{-j-k}$

Ex: $m=3$, $n=5$ $P_{5,3}$



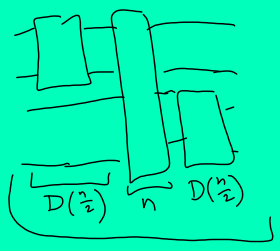
Same pattern holds for any m,n: gate connecting top qubits always has $\theta = \frac{1}{4}$
: as each connection moves down in the register (either one), divide θ by 2.

By applying $C\text{-}P(\theta)$ gates on disjoint pairs of qubits simultaneously (i.e., on the same layer) can reduce the depth of the $P_{n,m}$ circuit to $O(n)$ (instead of $\Omega(n^2)$)

Shor's original implementation:
$m = n-1$ each time,
[depth is asymptotically n^2]

"Divide & conquer" decomp
(i.e., $m \approx \frac{n}{2}$ each time)

Depth $D(n)$ is given by a recurrence:



$$D(n) = 2D\left(\frac{n}{2}\right) + n$$

$$\therefore D(n) = \Theta(n \lg n)$$

Do better?
Shor's algo will work for an approximate QFT,

If $\theta \ll 1$, $P(\theta) \approx I$

Can approximate QFT by throwing out all $C\text{-}P(\theta)$ gates where $\theta > \frac{1}{n^2}$ (versus $\frac{1}{2^n}$)

$\frac{1}{2^{2\lg n}}$

$P_{n,m}$ can be approximated with a depth $O(\lg n)$ circuit.