CSCE 785
10/31/2023

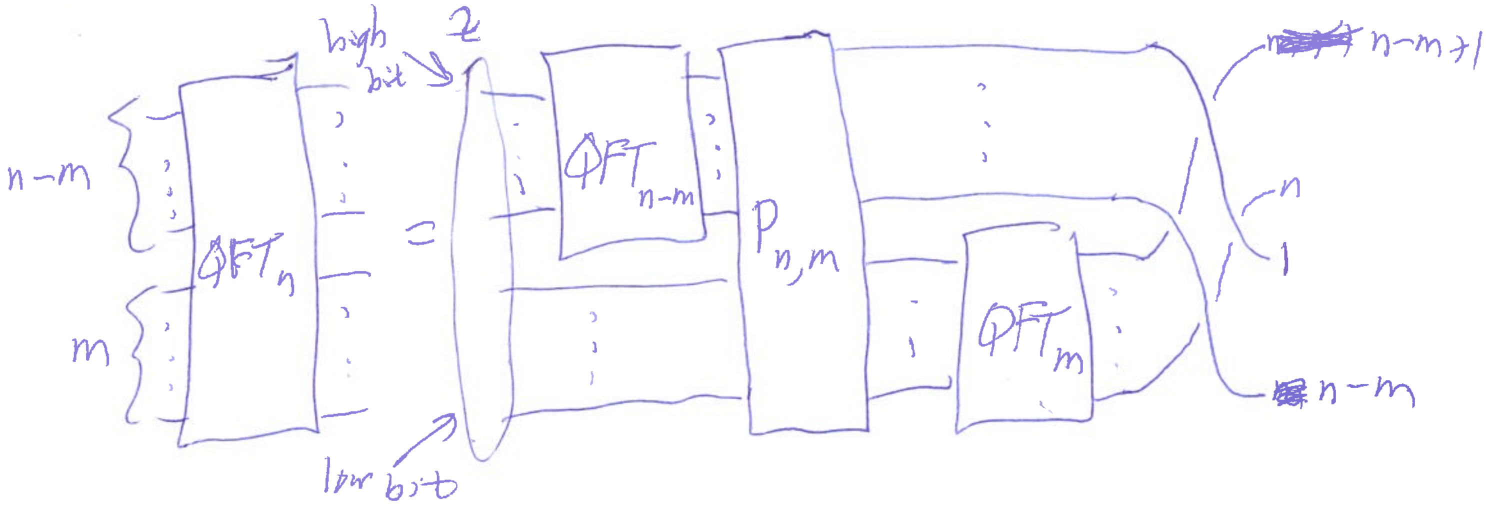
Implementing QFT_n

Finding good rational approximations

1. Base case: $n=1$. $QFT_1 = \frac{1}{2^{1/2}}\begin{bmatrix} e_1(0) & e_1(0) \\ e_1(0) & \underbrace{e_1(1)}_{=e^{\pi i}} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$

$$-\boxed{QFT_1}- \;=\; -\boxed{H}-$$

2. Recursive case: $n \geq 2$. Let $1 \leq m \leq n-1$. Then claim that



Where

$$P_{n,m}\,|x,y\rangle = \underbrace{e_n(xy)}_{e^{2i\pi xy/2^n}}\,|x,y\rangle$$

$$x \in \{0,1\}^{n-m} = \mathbb{Z}_{2^{n-m}}$$
$$y \in \{0,1\}^{m} = \mathbb{Z}_{2^{m}}$$

$e_n(x) := e^{2i\pi x/2^n}$

$= \omega^x$ where $\omega = e^{2i\pi/2^n}$

Correctness claim:

Given $z \in \mathbb{Z}_{2^n}$ show that

$LHS\,|z\rangle = RHS\,|z\rangle$

2

write $z = 2^m z_h + z_\ell$ where

$z_h \in \mathbb{Z}_{2^{n-m}}$, $z_\ell \in \mathbb{Z}_{2^m}$

$e_{n-r}(x) = e_n(2^r x)$

Then

$$(\star)\quad QFT_n|z\rangle = \frac{1}{2^{n/2}} \sum_{y\in\mathbb{Z}_{2^n}} e_n(zy)|y\rangle = \frac{1}{2^{n/2}} \sum_y e_n((z_h 2^m + z_\ell)y)|y\rangle$$

let $y = \cancel{2^m y_h + y_\ell}$ $2^{n-m} y_h + y_\ell$ for unique $y_h \in \mathbb{Z}_{2^m}$, $y_\ell \in \mathbb{Z}_{2^{n-m}}$

$$(\star) = \frac{1}{2^{n/2}} \sum_y e_n((2^m z_h + z_\ell)(2^{n-m} y_h + y_\ell))|y\rangle$$

$$= \frac{1}{2^{n/2}} \sum_y \underbrace{\cancel{e_n(2^n z_h y_h)}}_{=1} \underbrace{e_{n-m}(z_h y_\ell)}_{=e_n(2^m z_h y_\ell)} e_m(z_\ell y_h) e_n(z_\ell y_\ell) |y\rangle$$

$|y_h\rangle \otimes |y_\ell\rangle$

Apply the RHS circuit from left to right:

$$|z\rangle = |z_h\rangle \otimes |z_\ell\rangle \xmapsto[\text{on } |z_h\rangle]{QFT_{n-m}} \frac{1}{2^{(n-m)/2}} \sum_{y_\ell} e_{n-m}(z_h y_\ell)|y_\ell\rangle \otimes |z_\ell\rangle$$

$$\xmapsto{P_{n,m}} \frac{1}{2^{(n-m)/2}} \sum_{y_\ell} e_{n-m}(z_h y_\ell) e_n(y_\ell z_\ell)$$

$$(\star\star)\quad \xmapsto[\text{applied to } |z_\ell\rangle]{QFT_m} \frac{1}{2^{n/2}} \sum_{y_\ell} \sum_{y_h\in\mathbb{Z}_{2^m}} e_{n-m}(z_h y_\ell) e_n(z_\ell y_\ell) e_m(z_\ell y_h) (|y_\ell\rangle \otimes |y_h\rangle)$$

Compare $(\star\star)$ with $(\star)$

$$\xmapsto{\text{swaps}} \frac{1}{2^{n/2}} \sum_{y_\ell, y_h} \cdots\cdots (|y_h\rangle \otimes |y_\ell\rangle)$$ matches $(\star)$

(QED)

Implementing $P_{n,m}$ — use gate of the following form: Define 1-qubit <u>phase-shift gate</u>

$$P(\theta) = e^{\pi i \theta} \underbrace{R_z(2\pi\theta)}_{\cancel{\cos(2\pi\theta) I + i \sin(2\pi\theta) Z}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i \theta} \end{bmatrix}$$

[any $\theta \in \mathbb{R}$]

<u>Example:</u>

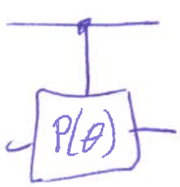
$$I = P(1)$$

$$Z = P\left(\tfrac{1}{2}\right)$$

$$S = P\left(\tfrac{1}{4}\right) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$T = P\left(\tfrac{1}{8}\right) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{bmatrix}$$

$P_{n,m}$ uses controlled phase-shift gates

$C\text{-}P(\theta) :=$ 

$=$ 

$$= \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i \theta} \end{bmatrix} =:$$ 

Note: $\forall a, b \in \{0,1\}$ $\quad$ $[(C\text{-}P(\theta)) \cdot SWAP = SWAP\,(C\text{-}P(\theta))]$

$$C\text{-}P(2^{-k})(|a\rangle \otimes |b\rangle) = e_k(ab)(|a\rangle \otimes |b\rangle)$$

Given $x \in \mathbb{Z}_{2^{n-m}}$, $y \in \mathbb{Z}_{2^m}$ $\quad$ [all $x_j, y_k \in \{0,1\}$]

$$\frac{x}{2^{n-m}} = \underbrace{0.x_1 x_2 \cdots x_{n-m}}_{\text{in binary}} = \sum_{j=1}^{n-m} x_j 2^{-j} \quad \Bigg| \quad \frac{y}{2^m} = 0.y_1 \cdots y_m = \sum_{k=1}^{m} y_k 2^{-k}$$

$$\frac{xy}{2^n} = \left(\frac{x}{2^{n-m}}\right)\left(\frac{y}{2^m}\right) = \sum_{j=1}^{n-m}\sum_{k=1}^{m} x_j y_k 2^{-j-k}$$

Then

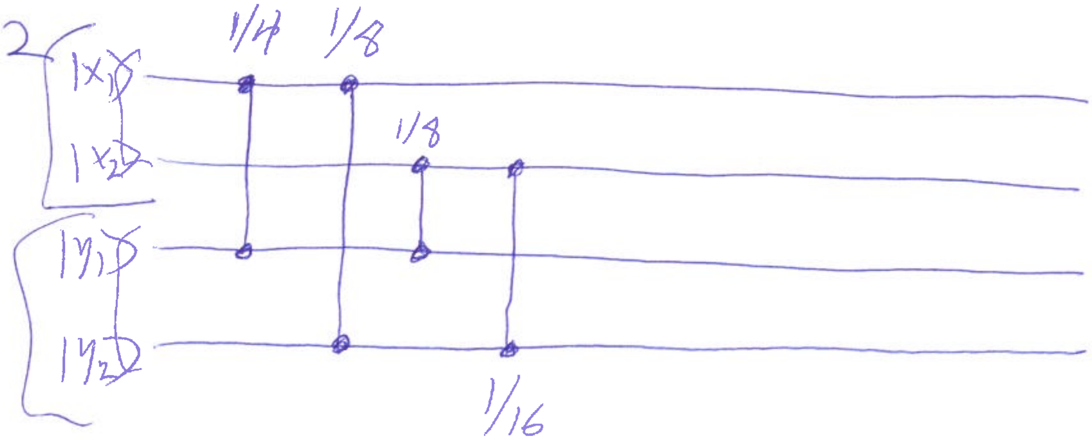
$$e_n(xy) = e^{2i\pi\left(\frac{xy}{2^n}\right)} = \prod_{j,k} \exp\left(2\pi i\, x_j y_k 2^{-j-k}\right)$$

$$\prod_{j,k} e_{j+k}(x_j y_k)$$

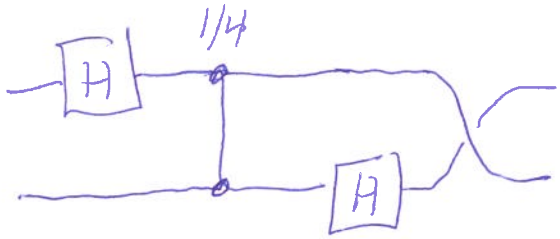
So then

$$P_{n,m}\left(|x\rangle\otimes|y\rangle\right) = \overbrace{\left(\prod_{j,k} e_{j+k}(x_j y_k)\right)\left(|x\rangle\otimes|y\rangle\right)}^{C\text{-}P(2^{-j-k})(|x\rangle\otimes|y\rangle)}$$

Ex: $n=4,\ m=2$



$QFT_2 =$



QFT_{2n} uses $Q\text{-}P(2^{-n})$ ← Infeasible to be implemented exactly (bad news)

Good news: $Q\text{-}P(2^{-n}) \approx I$ for large n, so just drop it from the circuit.