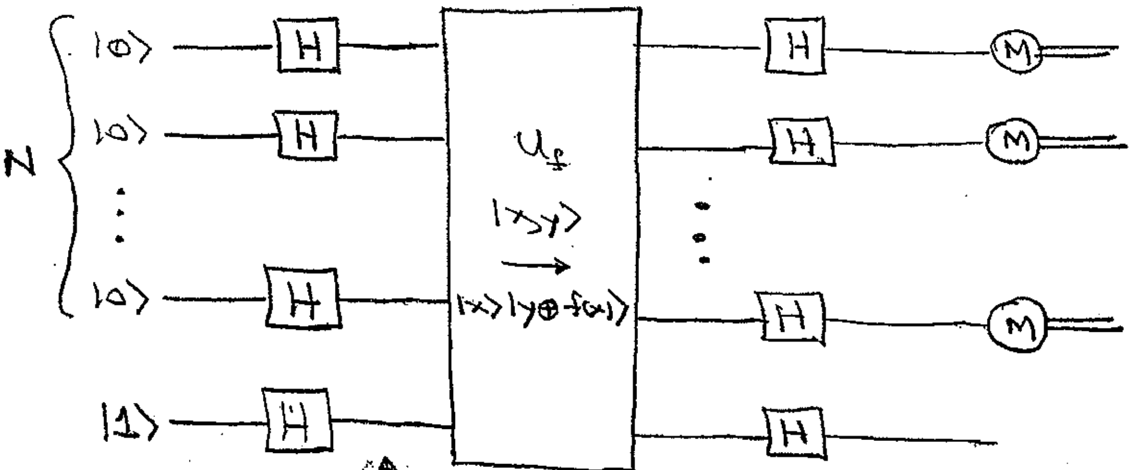
Quantum Computation

Lectures 13-14

Quantum Fourier transform and phase estimation

N-bit Boolean function $f: \{0,1\}^N \to \{0,1\}$, which is either constant or balanced.

Deutsch-Jozsa algorithm:



Number of classical calls to be sure is $\sim 2^N/2 = 2^{N-1}$

$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle$

$$|\psi_1\rangle = H^{\otimes N}|0\rangle^{\otimes N} \otimes H|1\rangle = \frac{1}{\sqrt{2^N}}\sum_x |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^N}}\sum_x |x\rangle \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |\overline{f(x)}\rangle\right)$$

quantum parallelism

$$= \underbrace{\left(\frac{1}{\sqrt{2^N}}\sum_x (-1)^{f(x)}|x\rangle\right)}_{|\phi\rangle} \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

phase kickback

function value written in phase

ancilla qubit left unentangled.

$$|\psi_3\rangle = \underbrace{\left(\frac{1}{\sqrt{2^N}}\sum_{x,y}(-1)^{f(x)+x\cdot y}|y\rangle\right)}_{|X\rangle} \otimes |1\rangle$$

f constant: $|X\rangle = \pm|0\rangle^{\otimes N}$

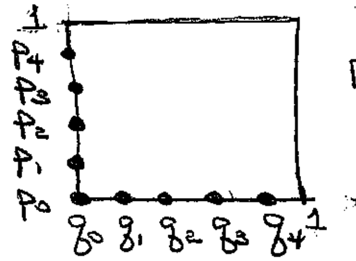
f balanced:

$${}^{\otimes N}\langle 0|X\rangle = \frac{1}{\sqrt{2^N}}\sum_x (-1)^{f(x)} = 0$$

One-shot determination of whether function is constant or balanced.

$$\langle \phi^{\text{constant}} | \phi^{\text{balanced}} \rangle = \pm\frac{1}{2^N}\sum_x (-1)^{f(x)} = 0$$

Quantum Fourier transform



$D = 5$

$2\pi\hbar D = \begin{pmatrix}\text{area of} \\ \text{phase space}\end{pmatrix} = 1$

D-dimensional Hilbert space

Orthonormal "position" basis $\quad |q_j\rangle = |e_j\rangle = |j\rangle, \; j = 0, \dots, D-1$

$q_j = j/D$

↑ use this notation when there's no other basis around to cause confusion

Conjugate "momentum" basis $\quad |p_k\rangle, \; k = 0, \dots, D-1$

$p_k = k/D$

$$|p_k\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |q_j\rangle e^{2\pi i jk/D}$$

j and k are defined mod D; the FT coefficient does mod D arithmetic.

$$\langle q_j | p_k \rangle = \frac{1}{\sqrt{D}} \exp\left(\frac{i}{\hbar} q_j p_k\right) = \frac{1}{\sqrt{D}} e^{2\pi i jk/D}$$

↑ discrete FT coefficients

$$\langle q_j | p_k \rangle = \langle q_k | p_j \rangle = \langle q_{-j} | p_k \rangle^* = \langle p_k | q_{-j} \rangle$$

periodic in j (q) with period $\Delta j = D/k = 1/p_k$ ($\Delta q = 1/k = 1/Dp_k = 2\pi\hbar/p_k$).

Matrix elements of a unitary matrix:

$$\boxed{\frac{1}{D} \sum_{l=0}^{D-1} e^{2\pi i l(j-k)/D} = \frac{1}{D} \frac{1 - e^{2\pi i (j-k)}}{1 - e^{2\pi i (j-k)/D}} = \delta_{jk}}$$

Quantum FT operator: $\quad F|q_j\rangle = |p_j\rangle$

$$\langle q_j | F | q_k \rangle = \langle q_j | p_k \rangle = \frac{1}{\sqrt{D}} e^{2\pi i jk/D}$$

$$y_k = \langle p_k | \psi \rangle = \langle q_k | F^\dagger | \psi \rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} e^{-2\pi i jk/D} \underbrace{\langle q_j | \psi \rangle}_{x_j}$$

$$y_k = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} e^{-2\pi i jk/D} x_j$$

Discrete FT

$$F|p_j\rangle = \sum_k \underbrace{F|q_k\rangle}_{|p_k\rangle}\underbrace{\langle q_k|p_j\rangle}_{\langle p_k|q_{-j}\rangle} = \sum_k |p_k\rangle\langle p_k|q_{-j}\rangle = |q_{-j}\rangle$$

$$\Longrightarrow \underset{\substack{\uparrow\\ \text{parity operator}}}{F^2}|q_j\rangle = |q_{-j}\rangle \Longrightarrow F^4 = 1$$

F has eigenvalues $\pm 1, \pm i$

What does this have to do with qubits? N qubits, $D = 2^N$

Notation: $j = \underbrace{j_1 \cdots j_N}_{\text{binary representation of } j\ (j_\ell = 0,1)} = \sum_{\ell=1}^{N} j_\ell 2^{N-\ell}$ $\qquad |q_j\rangle = |j\rangle = |j_1\rangle \otimes \cdots \otimes |j_N\rangle$

$$q_j = j/D = j/2^N = 0.j_1 \cdots j_N = \sum_{\ell=1}^{N} j_\ell 2^{-\ell}$$

$$j/2^k = j_1 \cdots j_{N-k}.j_{N-k+1} \cdots j_N = \sum_{\ell=1}^{N} j_\ell 2^{N-\ell-k}$$

$$e^{2\pi i j/2^k} = e^{2\pi i (0.j_{N-k+1} \cdots j_N)}$$

__Key qubit representation of F:__

$$|p_j\rangle = \underset{\substack{\uparrow\\ \text{FT on } N \text{ qubits}}}{F_N}|q_j\rangle = F_N|j\rangle = \frac{1}{2^{N/2}}\sum_{k=0}^{2^N-1}|k\rangle\, e^{2\pi i kj/D}$$

$$= \frac{1}{2^{N/2}}\sum_{k_1,\dots,k_N=0}^{1}|k_1\rangle\otimes\cdots\otimes|k_N\rangle \underbrace{\exp\left[2\pi i\left(\sum_{\ell=1}^{N}k_\ell 2^{N-\ell}\right)\frac{j}{D}\right]}_{\prod_{\ell=1}^{N} e^{2\pi i k_\ell j/2^\ell}}$$

$$= \frac{1}{2^{N/2}}\bigotimes_{\ell=1}^{N}\sum_{k_\ell=0}^{1}|k_\ell\rangle \underbrace{e^{2\pi i k_\ell j/2^\ell}}_{= e^{2\pi i (0.j_{N-\ell+1}\cdots j_N)k_\ell}}$$

$$F_N|j\rangle = \frac{1}{2^{N/2}} \bigotimes_{\ell=1}^{N} \left(|0\rangle + e^{2\pi i j/2^\ell}|1\rangle\right)$$

$$\boxed{\begin{aligned} F_N|j\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i j/2^1}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i j/2^2}|1\rangle\right) \\ &\quad \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i j/2^N}|0\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.j_N)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.j_{N-1}j_N)}|1\rangle\right) \\ &\quad \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.j_1\cdots j_N)}|1\rangle\right) \end{aligned}}$$

product state

This form is crucial because it shows that F can be implemented by separate (controlled) operations on each qubit, giving an $O(N^2)$ algorithm.

<u>Building circuits for F_N:</u>

Define $R_k \equiv e^{2\pi i/2^{k+1}} \underbrace{e^{-iZ\,2\pi/2^{k+1}}}_{\substack{\text{rotation by} \\ 2\pi/2^k = \pi/2^{k-1} \\ \text{about } \vec{e}_z}} \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & e^{+2\pi i/2^k} \end{pmatrix}$

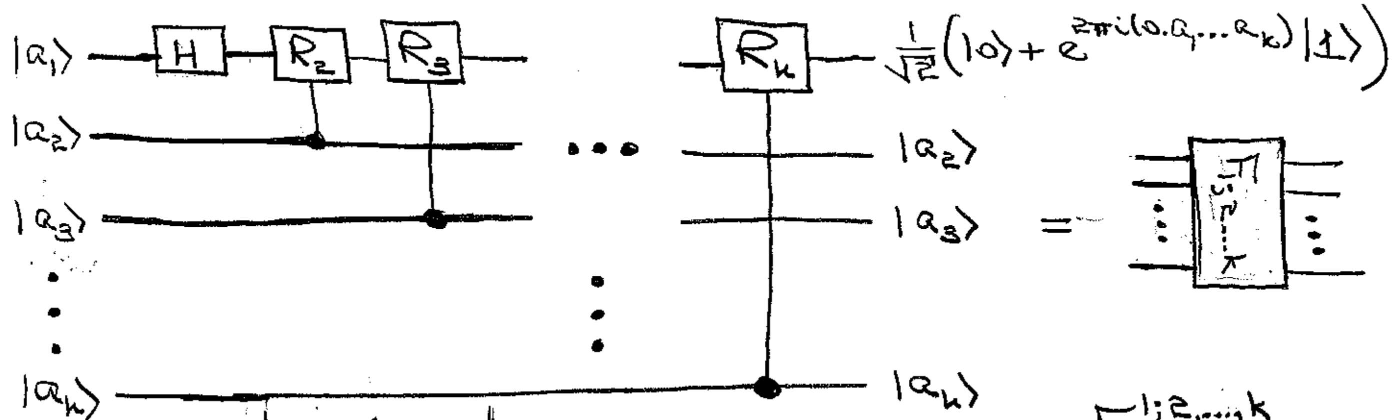
$R_0 = 1$
$R_1 = Z$
$R_2 = S$
$R_3 = T$
$\vdots$

$$R_{k+1}^2 = R_k$$

$$\begin{aligned} H|a\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^a|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi a}|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.a)}|1\rangle\right) \end{aligned}$$

$$\begin{aligned} R_k^a(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle + \beta e^{2\pi i a/2^k}|1\rangle \\ &= \alpha|0\rangle + \beta e^{2\pi i (0.\underbrace{0\cdots0}_{k-1\text{ 0's}}a)}|1\rangle \end{aligned}$$

The basic building block of the circuit is



$F^{1;2,\ldots,k}$

target

control qubits (order of application doesn't matter)

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.a_1)}|1\rangle\right)|a_2,\ldots,a_k\rangle$$

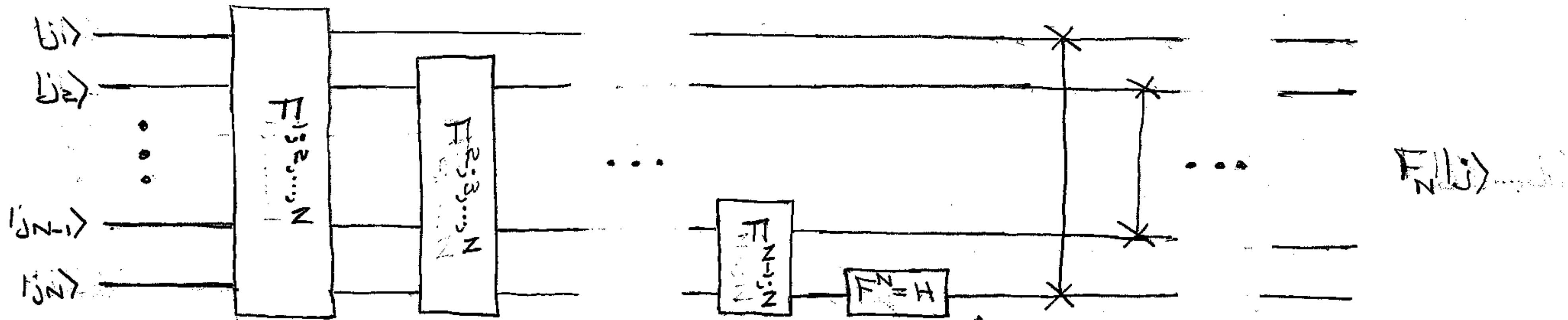
$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.a_1a_2)}|1\rangle\right)|a_2,\ldots,a_k\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.a_1a_2a_3)}|1\rangle\right)|a_2,\ldots,a_k\rangle$$

Resources for $F^{1;2,\ldots,k}$: $O(k)$

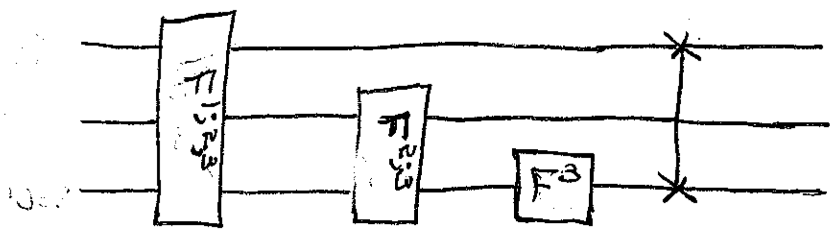
FT circuits:

7



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.j_1\cdots j_N)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.j_2\cdots j_N)}|1\rangle\right)$$
$$\otimes \dots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.j_{N-1}j_N)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.j_N)}|1\rangle\right)$$

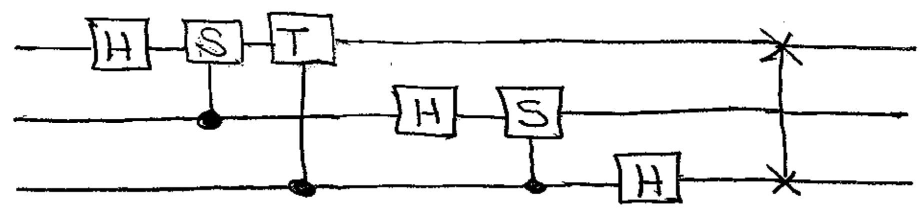
N=3



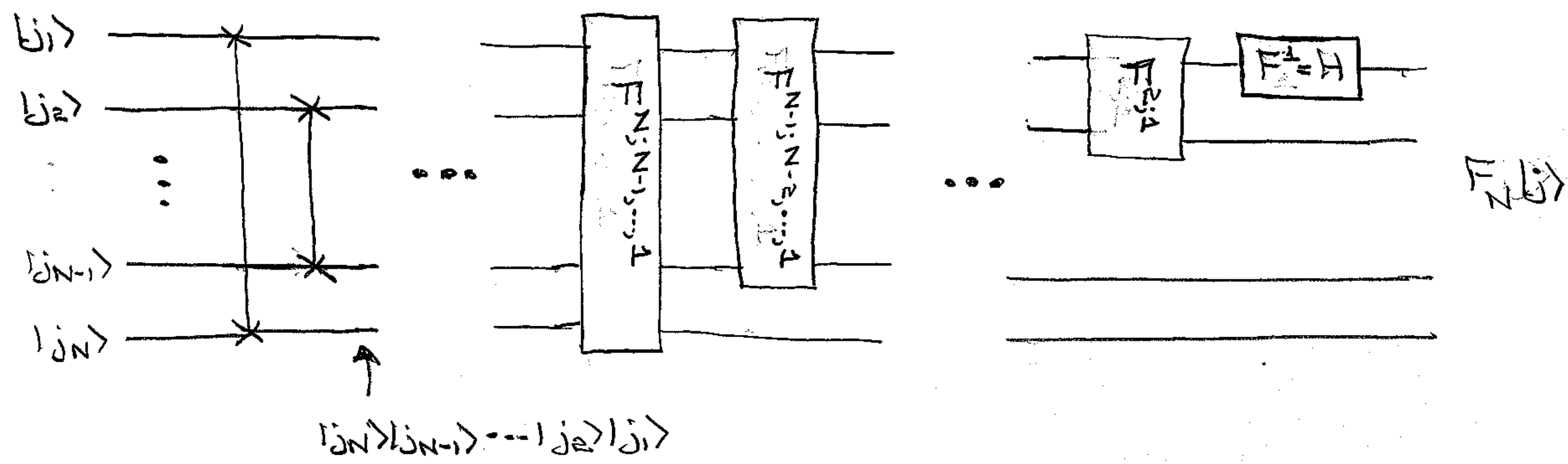
You can leave the swap gates out by swapping the labels of the qubits instead

Resources: $O(N^2)$

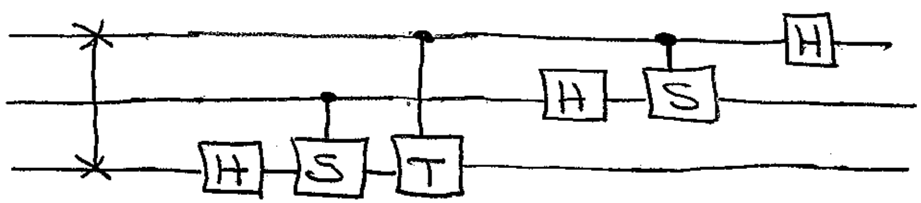
=

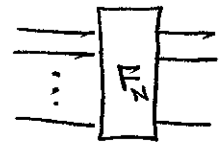


② You can also put the swaps first, which you can see either directly or by moving the swaps through the F's.



$N = 3$



Now we can simply write  when we want to include a Fourier transform.

Phase estimation

$$U|u\rangle = e^{2\pi i \phi}|u\rangle$$

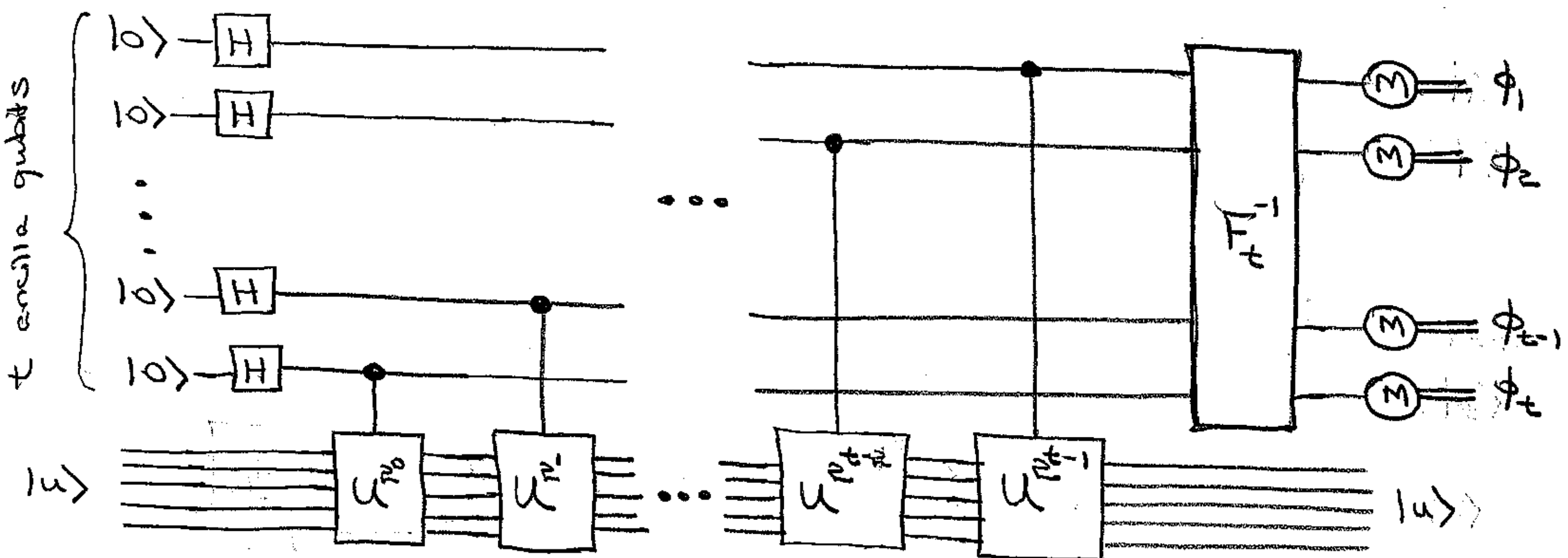
ϕ → unknown phase as fraction of 2π

$|u\rangle$ – eigenvector of U that can be prepared reliably

U ↑ unitary such that U^{2^l}, $l=0,\dots,t-1$, can be implemented efficiently.

① Assume that $\phi = 0.\phi_1\dots\phi_t = \phi_1\dots\phi_t / 2^t$

Phase estimation circuit



$|\phi_1\rangle\otimes\dots\otimes|\phi_t\rangle\otimes|u\rangle$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{t-1}\phi)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{t-2}\phi)}|1\rangle\right)$$

$$\otimes\dots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{1}\phi)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(2^{0}\phi)}|1\rangle\right)\otimes|u\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\phi_t)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\phi_{t-1}\phi_t)}|1\rangle\right)$$

$$\otimes\dots\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\phi_2\dots\phi_t)}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0.\phi_1\dots\phi_t)}|1\rangle\right)\otimes|u\rangle$$

$$= F_t|\phi\rangle = F_t|\phi_1\rangle\otimes|\phi_2\rangle\otimes\dots\otimes|\phi_t\rangle$$

The controlled unitaries prepare a momentum state

$$|p_{2^t\phi}\rangle = F_t|\phi\rangle = \frac{1}{\sqrt{D}}\sum_{k=0}^{2^t-1} e^{2\pi i k\phi}|k\rangle$$

periodic in position with period $\Delta q = 1/\phi = 2\pi\hbar/p_\phi$

We can determine ϕ, i.e., the period $2\pi\hbar/p_\phi$, from a measurement in the momentum basis, but we don't assume we know how to do that. So we do a FT to put the phase information in the standard basis (the inverse FT is an interferometer with 2^t inputs and outputs).

(12) What happens when $\phi = .\phi_1\phi_2\cdots$ has more than t digits? Now let $|\phi\rangle$ denote the state that is input to the inverse FT:

$$|\phi\rangle = \frac{1}{2^{t/2}}\bigotimes_{l=1}^{t}\left(|0\rangle + e^{2\pi i(2^{t-l}\phi)}|1\rangle\right)$$

Reverse the steps leading to the qubit form of the FT:

$$|\phi\rangle = \frac{1}{2^{t/2}}\bigotimes_{l=1}^{t}\underbrace{\left(|0\rangle + e^{2\pi i\underbrace{(2^t\phi)}_{j}/2^l}|1\rangle\right)}_{\sum_{k_l=0}^{1}|k_l\rangle e^{2\pi i k_l(2^t\phi)/2^l}}$$

$$= \frac{1}{2^{t/2}}\sum_{k_1,\dots,k_N}|k_1\rangle\otimes\cdots\otimes|k_N\rangle \exp\left[2\pi i\underbrace{\left(\sum_{l=1}^{t}k_l 2^{t-l}\right)}_{k}\phi\right]$$

$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}|k\rangle e^{2\pi i k\phi}$$

$$|0\rangle^{\otimes t}|u\rangle \longrightarrow |\phi\rangle|u\rangle = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}|k\rangle U^k|u\rangle \longleftarrow$$ This is the state before the $F^\dagger$

$$\langle q_j|F^\dagger|\phi\rangle = \frac{1}{2^t}\sum_{k=0}^{2^t-1} e^{2\pi i k(\phi - j/2^t)}$$

The calculation at the bottom of page 9 shows that

$$|0\rangle^{\otimes t}\,|u\rangle \longrightarrow \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle\, U^k |u\rangle,$$

which implies

$$|0\rangle^{\otimes t}\,|\psi\rangle \longrightarrow \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle\, U^k |\psi\rangle .$$

We can get at this result more directly by working with the circuit: After the Hadamards, the controlled unitaries do the transformation

$$|j\rangle|\psi\rangle \longrightarrow |j_1\rangle\otimes\cdots\otimes|j_t\rangle\, \underbrace{U^{2^{t-1}j_1}\cdots U^{2^1 j_{t-1}}\, U^{2^0 j_t}}_{U^{\sum_{k=1}^{t} 2^{t-k} j_k} = U^j}|\psi\rangle$$

$$|j\rangle|\psi\rangle \longrightarrow |j\rangle\, U^j|\psi\rangle$$

So with the Hadamards, the transformation is

$$|0\rangle^{\otimes t}\,|\psi\rangle \longrightarrow \frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} |j\rangle\, U^j |\psi\rangle .$$

So, if $|\psi\rangle$ is a superposition of several eigenstates of U, the output measurement will yield one of the eigenvalues with the probability from the superposition

$$\langle g_j | F^\dagger | \phi \rangle = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i(\phi - j/2^t)} \right)^k$$

$$= \frac{1}{2^t} \frac{1 - e^{2\pi i(\phi 2^t - j)}}{1 - e^{2\pi i(\phi - j/2^t)}}$$

$b \equiv \lfloor \phi 2^t \rfloor$ and $\phi 2^t = b + \delta$, $0 \le \delta < 1$

$$\phi = b 2^{-t} + \delta 2^{-t}$$

$\delta 2^{-t}$: error in the t-bit approximation

$b 2^{-t}$: t-bit approximation to ϕ

> $\delta 2^{-t}$ is error in determination of ϕ because ϕ has more than t bits.
> $\ell 2^{-t}$ is error in determination of ϕ because the measurement doesn't yield b.

$$\langle g_{b+\ell} | F^\dagger | \phi \rangle = \frac{1}{2^t} \frac{1 - e^{2\pi i(\delta - \ell)}}{1 - e^{2\pi i(\delta - \ell)/2^t}}$$

$$= \frac{1}{2^t} \frac{e^{i\pi(\delta-\ell)} \sin(\pi(\delta - \ell))}{e^{i\pi(\delta-\ell)/2^t} \sin(\pi(\delta-\ell)/2^t)}$$

$$|\langle g_{b+\ell} | F^\dagger | \phi \rangle|^2 = \frac{1}{2^{2t}} \frac{\sin^2 \pi(\ell - \delta)}{\sin^2(\pi(\ell-\delta)/2^t)}$$

$|\ell| \le 2^{n-1}$ means an error $\le n$ bits, giving ϕ to $N = t - n$ bits.

$$\underbrace{P(|\ell| > 2^{n-1})}_{} = \sum_{\ell=-2^{t-1}+1}^{-2^{n-1}-1} |\langle g_{b+\ell} | F^\dagger | \phi \rangle|^2 + \sum_{\ell=2^{n-1}+1}^{2^{t-1}} |\langle g_{b+\ell} | F^\dagger | \phi \rangle|^2$$

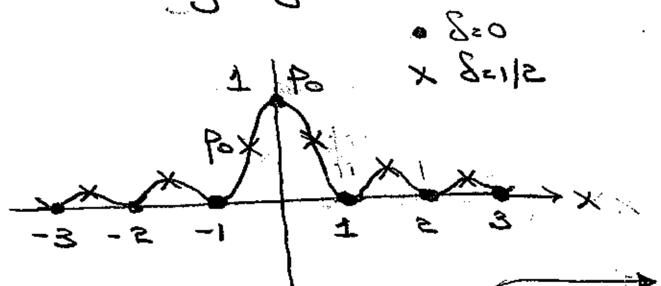
(probability of getting less than $N = t-n$ bits)

$\ell = -2^{t-1}+1, \ldots, 2^{t-1}$

(center summing range at $\ell = 0$).

$$|\langle g_{b+\ell} | F^\dagger | \phi \rangle|^2 = \frac{1}{2^{2t}} \frac{\sin^2 \pi x}{\sin^2 \pi x / 2^t}$$

$x = \ell - \delta$

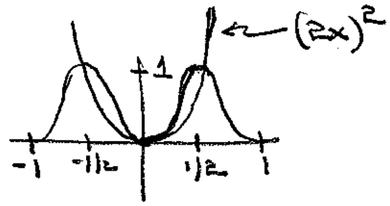


recurrences

Bound below is based on worst case ($\delta = 1/2$).

$$\sin^2 \pi x \leq 1$$

$$\sin^2 \pi x \geq (2x)^2$$



$$\frac{l-\delta}{2^t} \leq \frac{1}{2^t}\left(2^{t-1} - \delta\right) = \frac{1}{2} - \frac{\delta}{2^t} \leq \frac{1}{2}$$

$$\frac{l-\delta}{2^t} \geq \frac{1}{2^t}\left(-2^{t-1} + 1 - \delta\right) = -\frac{1}{2} + \frac{1-\delta}{2^t} \geq -\frac{1}{2}$$

$$\left|\frac{l-\delta}{2^t}\right| \leq \frac{1}{2}$$

$$\Longrightarrow \quad \sin^2\left(\frac{\pi(l-\delta)}{2^t}\right) \geq \left(\frac{2(l-\delta)}{2^t}\right)^2 = \frac{4(l-\delta)^2}{2^{2t}}$$

$$|\langle \tilde{b}+l | F^\dagger | \phi\rangle|^2 \leq \frac{1}{4(l-\delta)^2}$$

$$p(|l| > 2^{n-1}) \leq \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-2^{n-1}-1} \underbrace{\frac{1}{(l-\delta)^2}}_{\leq \frac{1}{l^2}} + \sum_{l=2^{n-1}+1}^{2^{t-1}} \underbrace{\frac{1}{(l-\delta)^2}}_{\leq \frac{1}{(l-1)^2}}\right)$$

$$\leq \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-2^{n-1}} \frac{1}{l^2} + \sum_{l=2^{n-1}}^{2^{t-1}-1} \frac{1}{l^2}\right)$$

$$= \frac{1}{2} \sum_{l=2^{n-1}}^{2^{t-1}-1} \frac{1}{l^2}$$

$$\leq \frac{1}{2} \int_{2^{n-1}-1}^{2^{t-1}-1} \frac{dl}{l^2}$$

$$\leq \frac{1}{2} \int_{2^{n-1}-1}^{\infty} \frac{dl}{l^2}$$

$$= \frac{1}{2} \frac{1}{2^{n-1}-1}$$

$$\epsilon \equiv \begin{pmatrix}\text{probability of getting less} \\ \text{than } N = t - n \text{ bits of } \phi\end{pmatrix} \leq \frac{1}{2}\,\frac{1}{2^{n-1}-1} = \frac{1}{2}\,\frac{1}{2^{t-N-1}-1}$$

$$\parallel$$

$$1 - \begin{pmatrix}\text{probability of getting} \\ N = t - n \text{ bits or more}\end{pmatrix}$$

$$\boxed{n \leq \log(2 + \epsilon^{-1})}$$