

Title: Quantum Information (Review) - Lecture 8

Date: Feb 23, 2012 10:15 AM

URL: <http://pirsa.org/12020040>

Abstract:

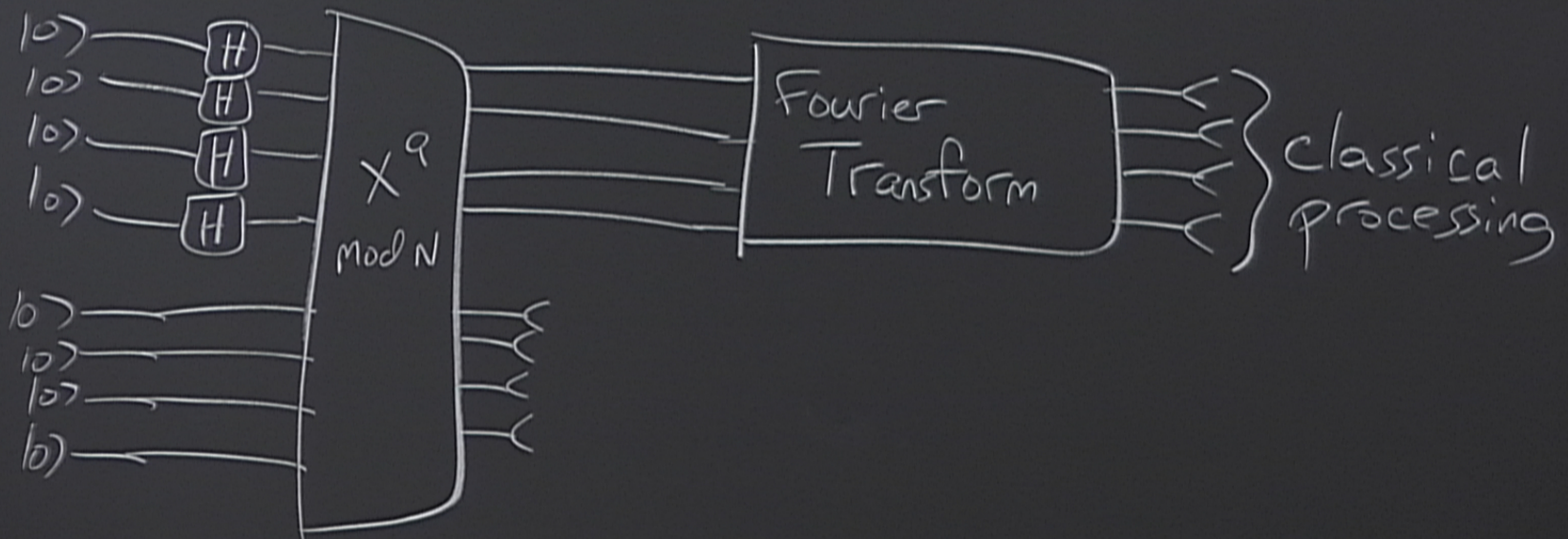
on b , we can deduce $\frac{c}{r}$
 continued fraction expansion:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

When $\frac{b}{z^n} \approx \frac{c}{r}$ then $\frac{c}{r} =$

rationals, expansion ends

Shor's algorithm:



Finds order r of $x^a \bmod N$
for given x, N .

Fourier transform $|a\rangle \mapsto \sum_b w^{ab} |b\rangle$, $w = e^{2\pi i / 2^n}$

Input $a = a_0 z^{n-1} + a_1 z^{n-2} + a_2 z^{n-3} + \dots + a_{n-1}$

Output $b = b_0 z^{n-1} + b_1 z^{n-2} + b_2 z^{n-3} + \dots + b_{n-1}$

$$ab = (\dots) z^n + z^{n-1} (a_0 b_{n-1} + a_1 b_{n-2} + \dots + a_{n-1} b_0) \\ + z^{n-2} (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1) + \dots + z^0 (a_{n-1} b_{n-1})$$

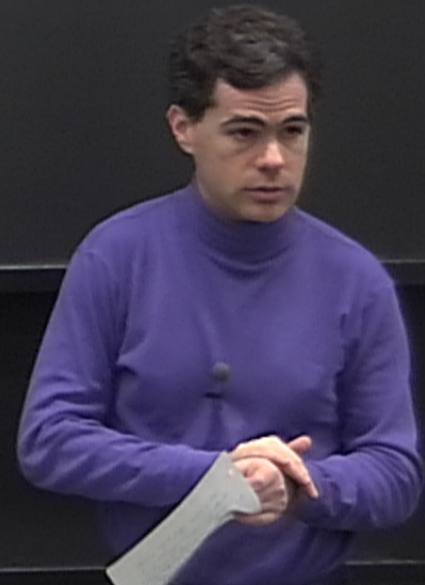
Bits
 $\sum_b w^{ab} |b\rangle$

Bits of b in reverse order

$$\sum_b \omega^{ab} |b\rangle = \sum_b \omega^{ab} |b_{n-1}\rangle |b_{n-2}\rangle \dots |b_0\rangle$$

$$= \left[\sum_{b_{n-1}} \omega^{(a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1} z^0) b_{n-1}} |b_{n-1}\rangle \right] \cdot \left[\sum_{b_{n-2}} \omega^{(a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_{n-1} z^1) b_{n-2}} |b_{n-2}\rangle \right] \cdot \dots \cdot \left[\sum_{b_0} \omega^{(a_{n-1} z^{n-1}) b_0} |b_0\rangle \right]$$

b_{n-1} term is $\sum_{b_{n-1}} \omega^{(a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-1)}) b_{n-1}} |b_{n-1}\rangle$



Bits of b in reverse order

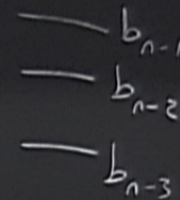
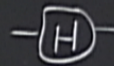
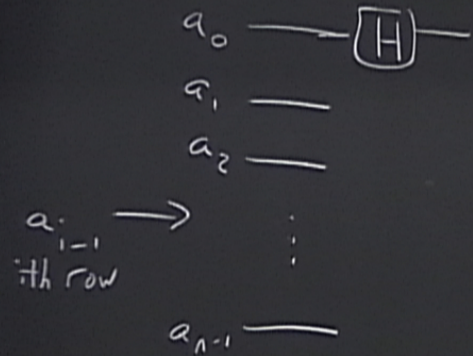
$$\begin{aligned} \sum_b \omega^{ab} |b\rangle &= \sum_b \omega^{ab} |b_{n-1}\rangle |b_{n-2}\rangle \dots |b_0\rangle \\ &= \left[\sum_{b_{n-1}} \omega^{(a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1} z^0) b_{n-1}} |b_{n-1}\rangle \right] \cdot \left[\sum_{b_{n-2}} \omega^{(a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_{n-1} z^1) b_{n-2}} |b_{n-2}\rangle \right] \cdot \dots \cdot \left[\sum_{b_0} \omega^{(a_{n-1} z^{n-1}) b_0} |b_0\rangle \right] \end{aligned}$$

$$b_{n-1} \text{ term is } \sum_{b_{n-1}} \omega^{(a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-1)}) b_{n-1}} |b_{n-1}\rangle$$

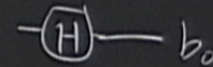
b_{n-1}
 b_{n-2}

$$+ \sum (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1) + \dots + \sum (a_{n-1} b_{n-1})$$

b_{n-1} term is $\sum_{b_{n-1}} \omega$



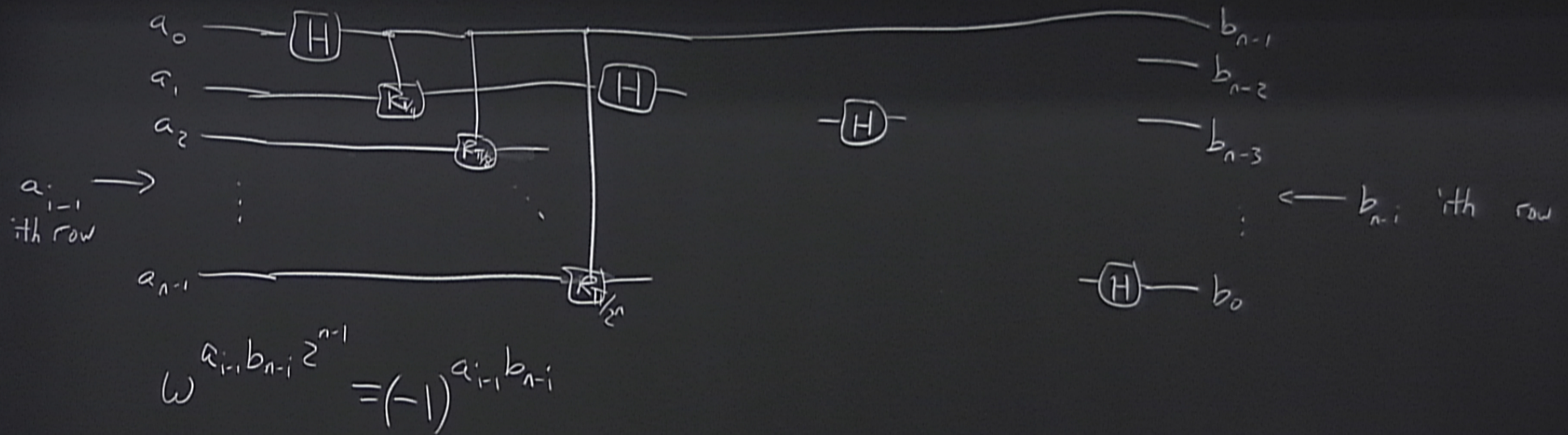
$\leftarrow b_{n-i}$ 'ith row



$$\omega^{a_{i-1} b_{n-i}} z^{n-1} = (-1)^{a_{i-1} b_{n-i}}$$

$$+ z^{n-2} (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1) + \dots + z^0 (a_{n-1} b_{n-1})$$

b_{n-1} term is $\sum_{b_n: \omega}$



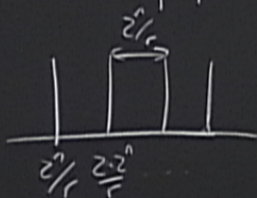
Complexity of QFT:

$$n + (n-1) + (n-2) + \dots + 1 = O(n^2)$$

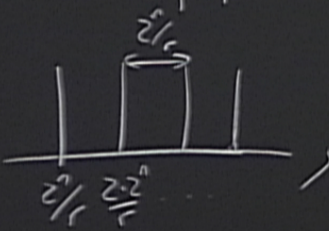
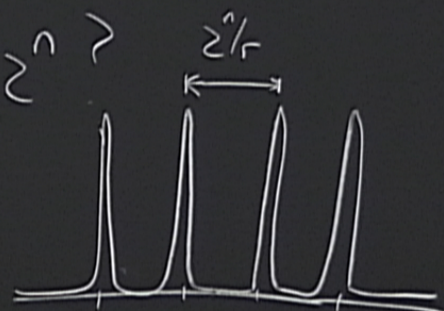
← b_{n-i} 'ith row

$H^{\otimes n}$ is Fourier transform for $(\mathbb{Z}_2)^n$

What happens when $\tau \propto z^n$?

Not 

What happens when $\pm \sqrt{z^n}$?

Not , instead: 

From

When $z^n \sim N^2$, peaks are narrow enough
 that, with high probability, we get measurement outcome $b \approx \frac{cz^n}{r}$

From b , we can deduce $\frac{c}{r}$
using continued fraction expansion:

$$\frac{b}{z^n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

For rationals, expansion ends

From b , we can deduce $\frac{c}{r}$
using continued fraction expansion:

$$\frac{b}{z^n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} \quad \text{When } \frac{b}{z^n} \approx \frac{c}{r}, \text{ then } \frac{c}{r} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

For rationals, expansion ends

"Unstructured search" / "Database search"

$$\theta : \mathbb{Z}_N \rightarrow \mathbb{Z}_2$$

Find if $\exists x_0$ s.t. $\theta(x_0) = 1$

And find an x_0 .

Classically: The best algorithm
for unstructured search takes $\Omega(N)$ queries

Def: A function $f(n)$ is $\Omega(N)$
if

"Unstructured search" / "Database search"

$$\theta : \mathbb{Z}_N \rightarrow \mathbb{Z}_2$$

Find if $\exists x_0$ s.t. $\theta(x_0) = 1$

And find an x_0 .

Classically: The best algorithm
for unstructured search takes $\Omega(N)$ queries

Def: A function $f(n)$ is $\Omega(g(n))$
if $\exists c$ s.t. $f(n) \geq c g(n) \forall n$.

Grover's algorithm is a quantum
algorithm that solves the problem
in $O(\sqrt{N})$ queries.
(Any quantum alg requires $\Omega(\sqrt{N})$ queries)