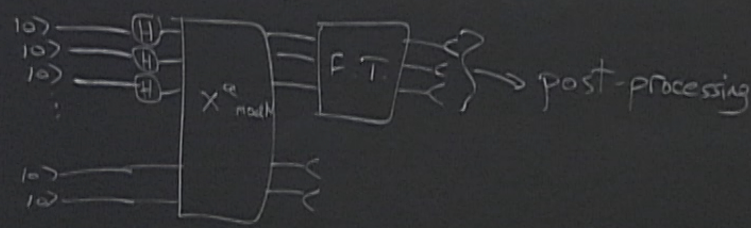
Title: PSI 17/18 - Quantum Information - Lecture 8

Date: Mar 01, 2018 11:30 AM

URL: http://pirsa.org/18030021

Abstract:

Shor's algorithm



Fourier transform:

$$\mathcal{F}|a\rangle = \sum_b \omega^{ab}|b\rangle, \quad \omega = e^{2\pi i/2^n}$$

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

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

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

$2\pi i/2^n$

$\dots + \dots + a_{n-1}$

$\dots + \dots + b_{n-1}$

$b_{n-2} + \dots + a_{n-1} b_0)$

$2^0(a_{n-1} b_{n-1})$

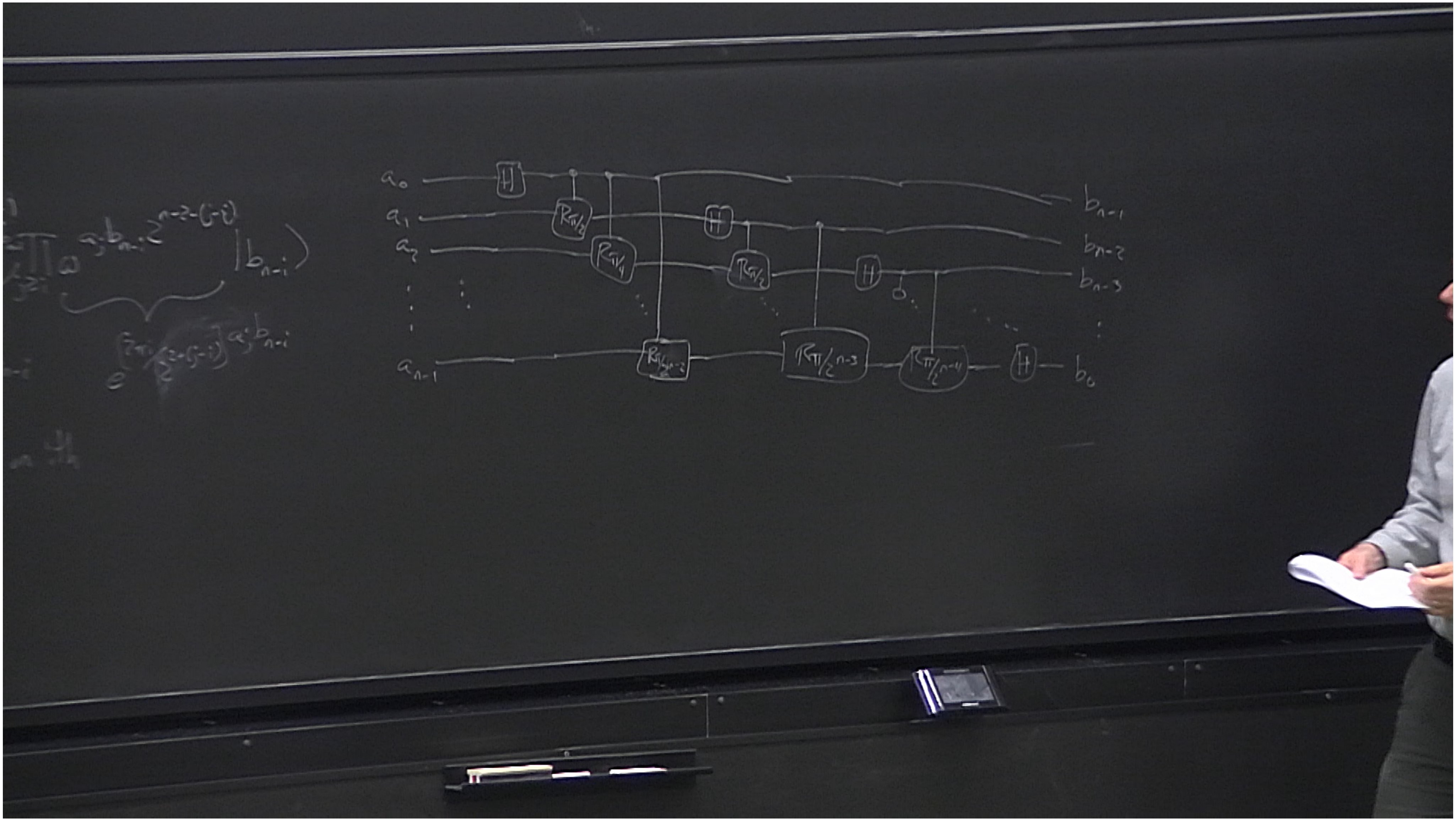
$$|a_0\rangle|a_1\rangle|a_2\rangle\dots|a_{n-1}\rangle$$

$$\downarrow$$

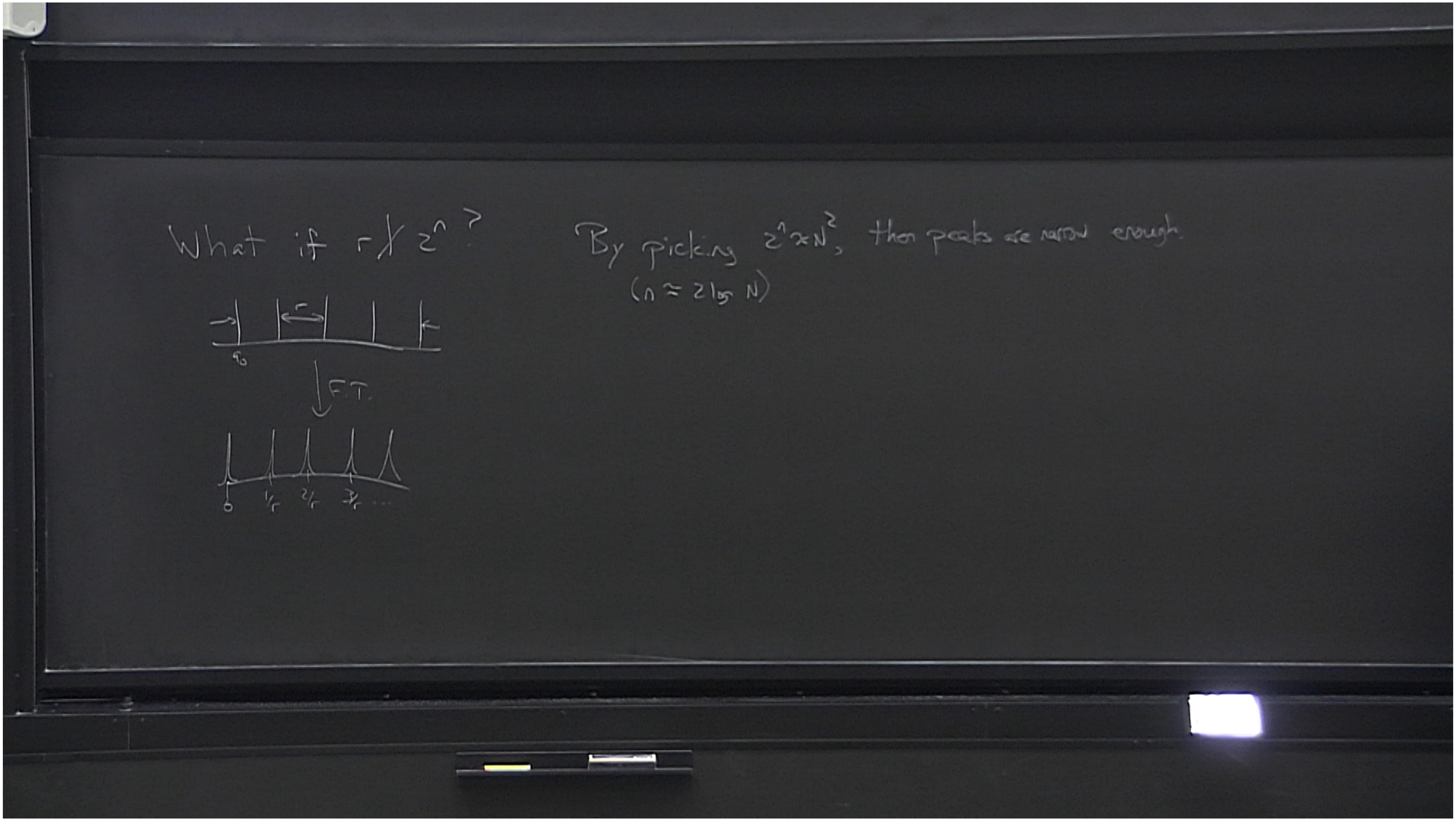
$$\sum_b \omega^{ab}|b_{n-1}\rangle|b_{n-2}\rangle|b_{n-3}\rangle\dots|b_0\rangle$$

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

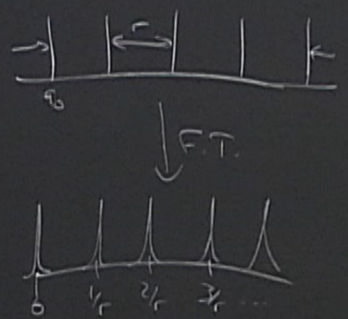
$$\dots\left[\sum_{b_0}\omega^{(a_{n-1}2^{n-1})b_0}|b_0\rangle\right]$$



a_0
a_1
a_2
a_{n-1}
H
$R_{\pi/2}$
$R_{\pi/4}$
$R_{\pi/2^{n-3}}$
$R_{\pi/2^{n-4}}$
b_{n-1}
b_{n-2}
b_{n-3}
b_0


What if r ∤ 2^n ?
By picking 2^n ≈ N^2, then peaks are narrow enough.
(n ≈ 2 log N)
r
x0
F.T.
0 1/r 2/r 3/r ...

What if $r \nmid 2^n$?



By picking $2^n \approx N^2$, then peaks are narrow enough.

$(n \approx 2 \log N)$

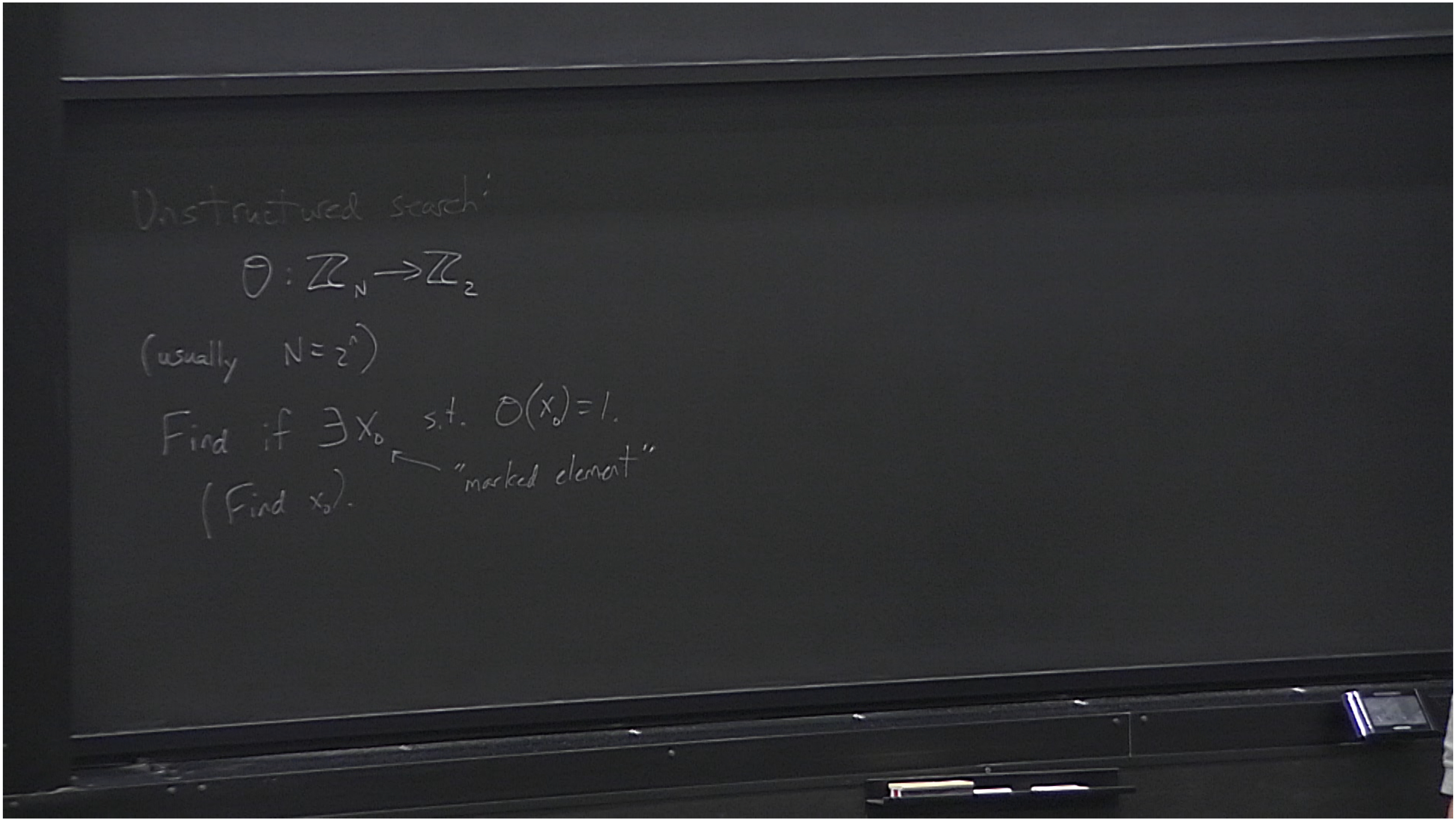
$$b \approx c\, 2^n / r$$

Continued fraction expansion:

$$\frac{b}{2^n} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$$

finitely many terms.

$$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$$


Unstructured search:
$\mathcal{O}: \mathbb{Z}_N \to \mathbb{Z}_2$
(usually $N = 2^n$)
Find if $\exists x_0$ s.t. $\mathcal{O}(x_0) = 1$.
"marked element"
(Find x_0).

Unstructured search:

$\mathcal{O} : \mathbb{Z}_N \to \mathbb{Z}_2$

(usually $N = 2^n$)

Find if $\exists x_0$ s.t. $\mathcal{O}(x_0) = 1$.

"marked element"

(Find x_0).

Classically: $\Theta(N)$ queries.

$\Omega(f(N))$ means $\geq c f(N)$

$\Theta(f(N))$ means $\Omega(f(N))$ & $O(f(N))$

Quantum: $\Omega(\sqrt{N})$ queries

Grover's algorithm $O(\sqrt{N})$

$\Rightarrow \Theta(\sqrt{N})$

$f(N))$

Specialize to unique marked element:

Focus on 2-D subspace:

$|S\rangle = |x_0\rangle$

$|T\rangle = \sum_{x \neq x_0} |x\rangle$

$\langle S|T\rangle = 0.$

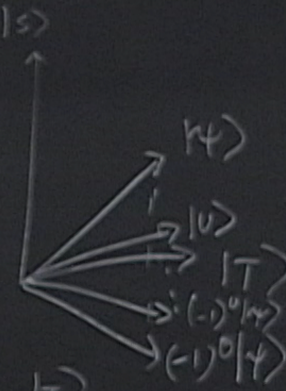
$|\psi\rangle = \alpha|S\rangle + \beta|T\rangle$

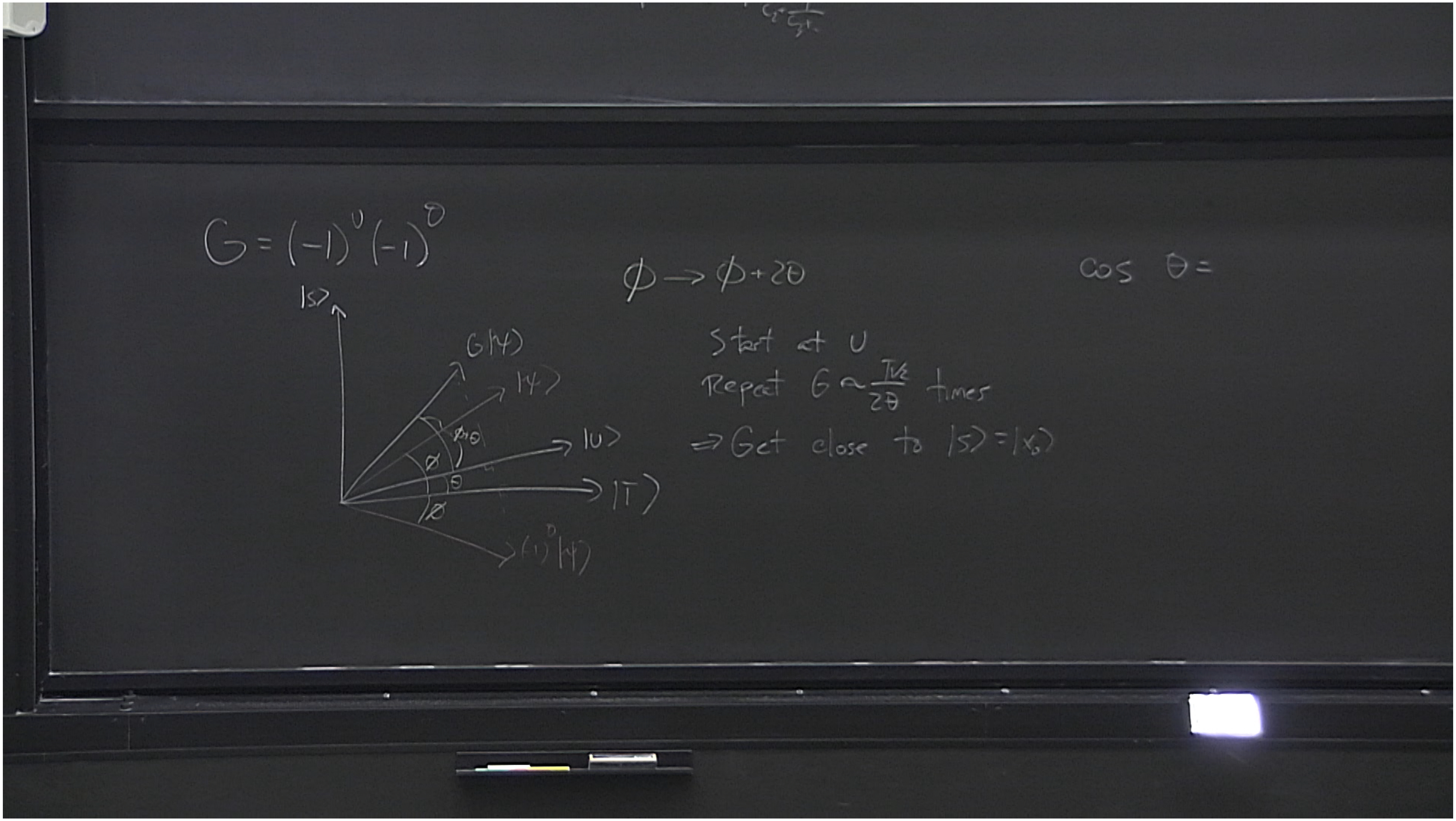
$|\psi\rangle \to (-1)^{O}|\psi\rangle = -\alpha|S\rangle + \beta|T\rangle$

$(-1)^{U} = H^{\otimes n} F_0 H^{\otimes n}$

$|U\rangle = |S\rangle + |T\rangle = \sum_x |x\rangle = H^{\otimes n}|0..0\rangle$

$F_0|0..0\rangle = |0..0\rangle$, $F_0|x\rangle = -|x\rangle \quad x \neq 0..0$




$G = (-1)^{U}(-1)^{0}$
$\phi \to \phi + 2\theta$
$\cos\theta =$
Start at U
Repeat G ~ $\frac{\pi/2}{2\theta}$ times
⇒ Get close to $|s\rangle = |x_0\rangle$
$|s\rangle$
$G|\psi\rangle$
$|\psi\rangle$
$|U\rangle$
$|T\rangle$
$(-1)^{0}|\psi\rangle$
$\phi+\theta$
ϕ
θ