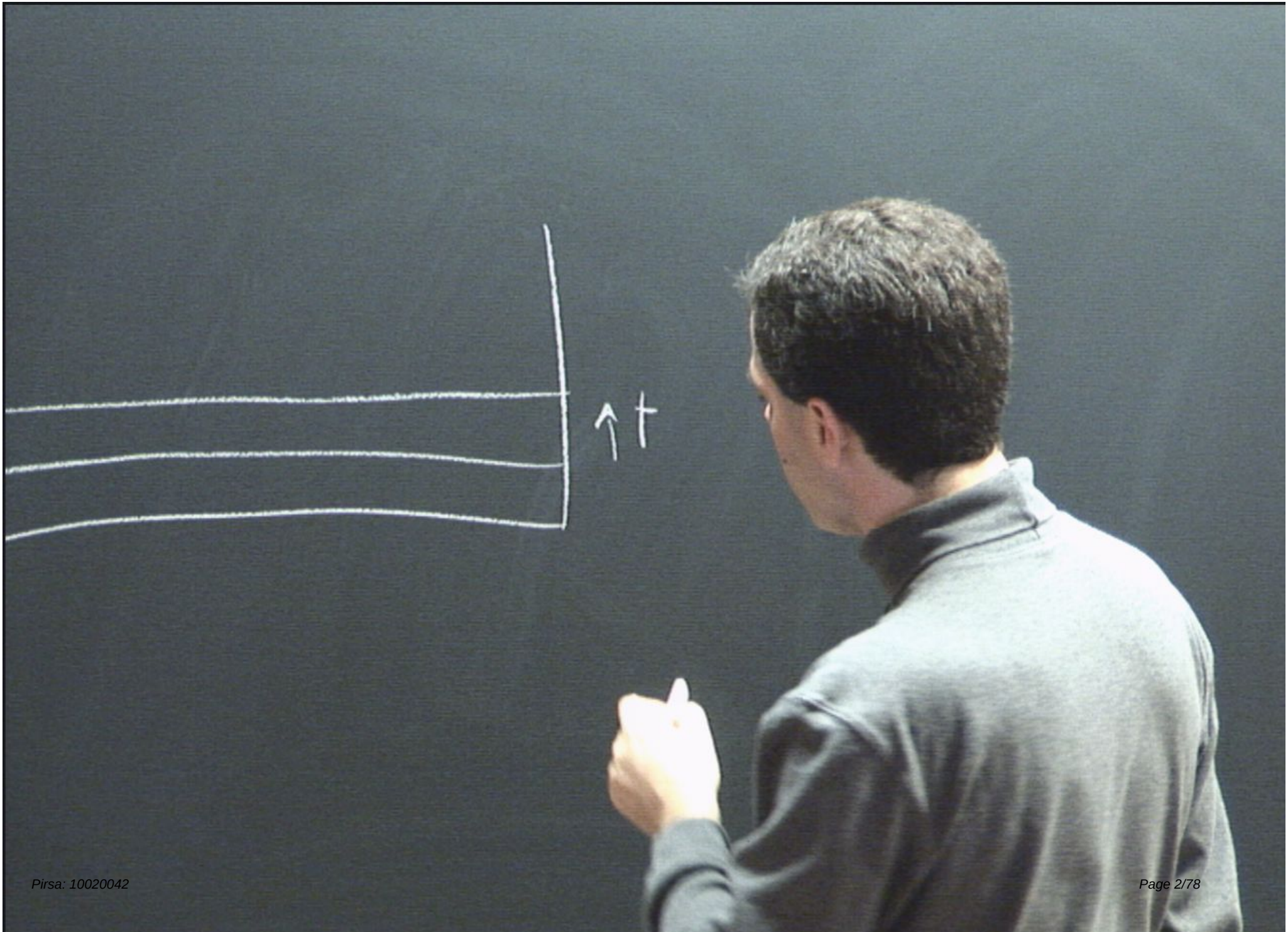
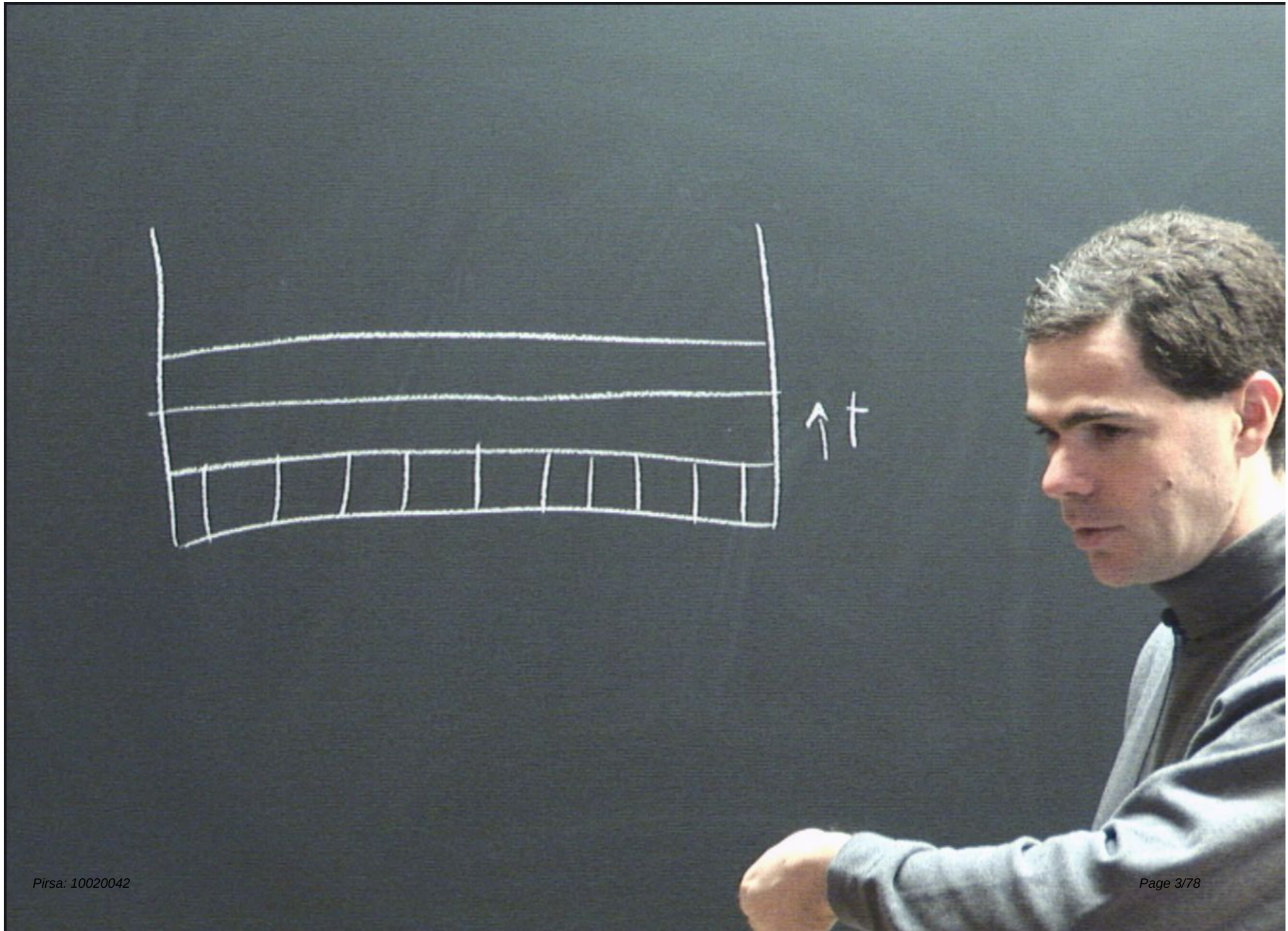
Title: Quantum Information - Review (PHYS 635) - Lecture 10

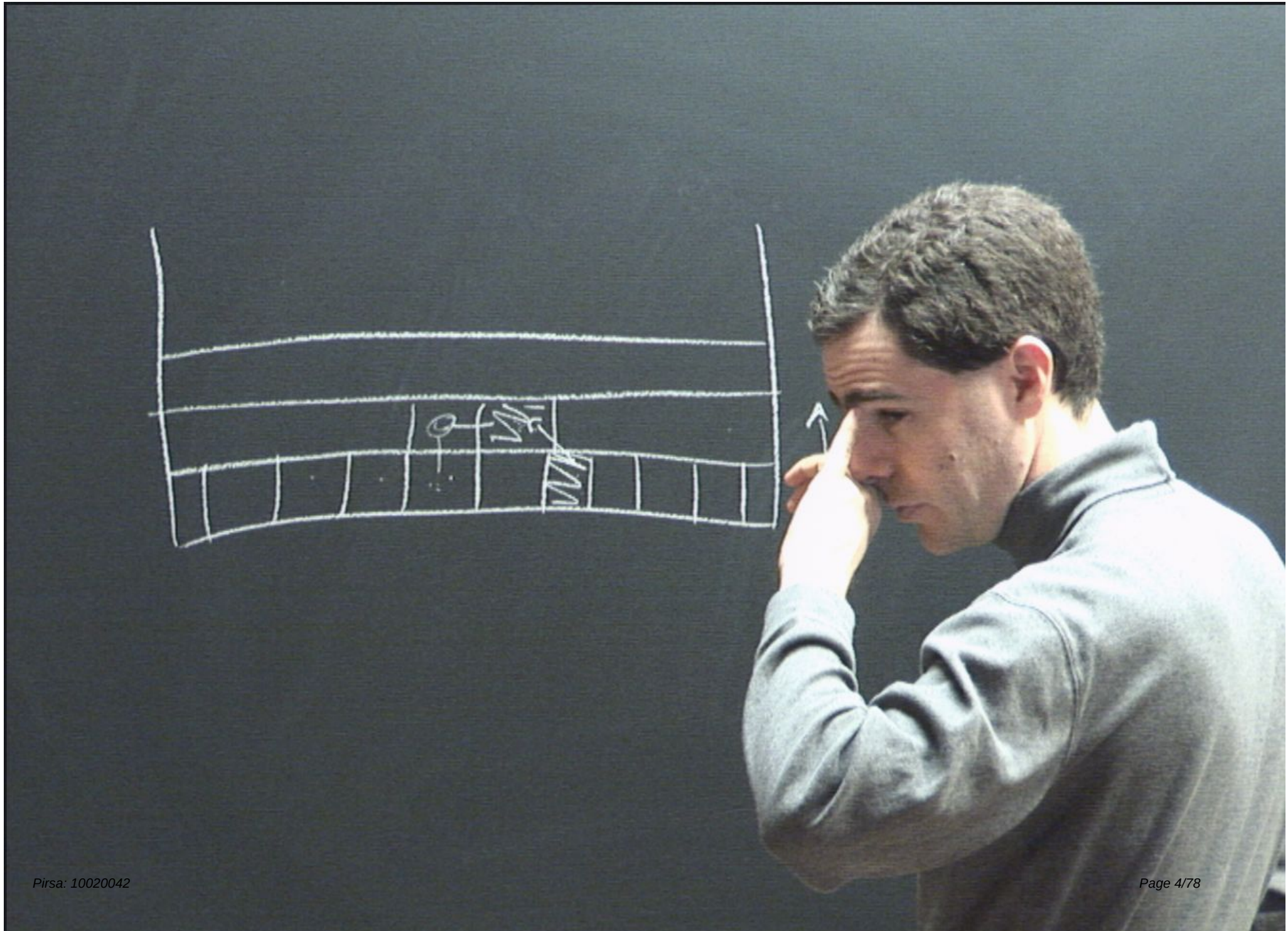
Date: Feb 05, 2010 09:00 AM

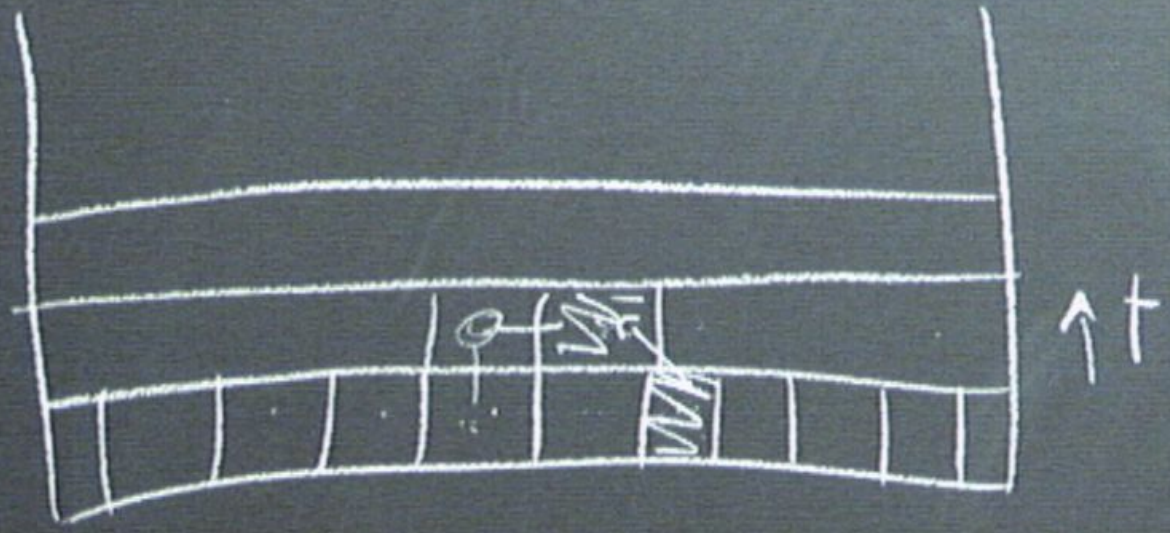
URL: http://pirsa.org/10020042

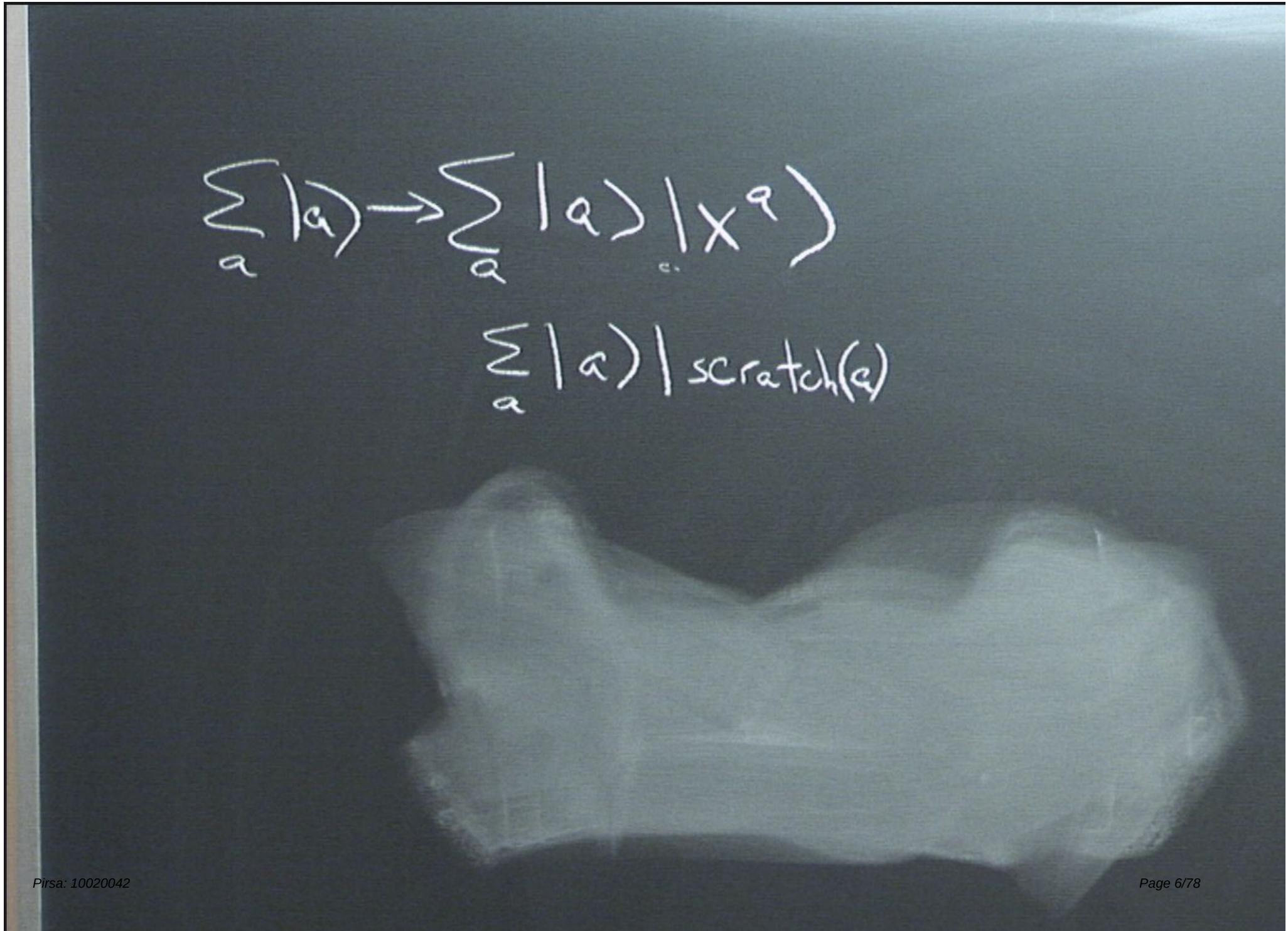
Abstract: Week 1: Basic topics (Qubits, quantum gates, quantum circuits, density matrices, quantum operations, entropy, entanglement) Week 2: Algorithms and complexity (Languages, complexity classes, oracles, RSA, Deutsch-Jozsa algorithm, Shor's algorithm, Grover's algorithm) Week 3: Information theory and implementations (Overview of implementations, quantum error correction, quantum cryptography, quantum information theory)


t


t




t


$\sum_a |a\rangle \rightarrow \sum_a |a\rangle |x^a\rangle$
$\sum_a |a\rangle |\text{scratch}(a)\rangle$

$$\sum_a |a\rangle \rightarrow \sum_a |a\rangle |x^a\rangle$$

$$\sum_a |a\rangle |\text{scratch}(a)\rangle |x^a\rangle$$

measure

$$\sum_a |a\rangle \to \sum_a |a\rangle |x^a\rangle$$

$$\sum_a |a\rangle |\text{scratch}(a)\rangle |x^a\rangle$$

Measure

Collapse

$$\sum_j |a_0 + jr\rangle$$

Instead $\sum_j |a_0 + jr\rangle |\text{scratch}(a_0 + jr)\rangle$

$$\sum_a |a\rangle \rightarrow \sum_a |a\rangle |x^a\rangle$$

$$\sum_a |a\rangle |\text{scratch}(a)\rangle |x^a\rangle$$

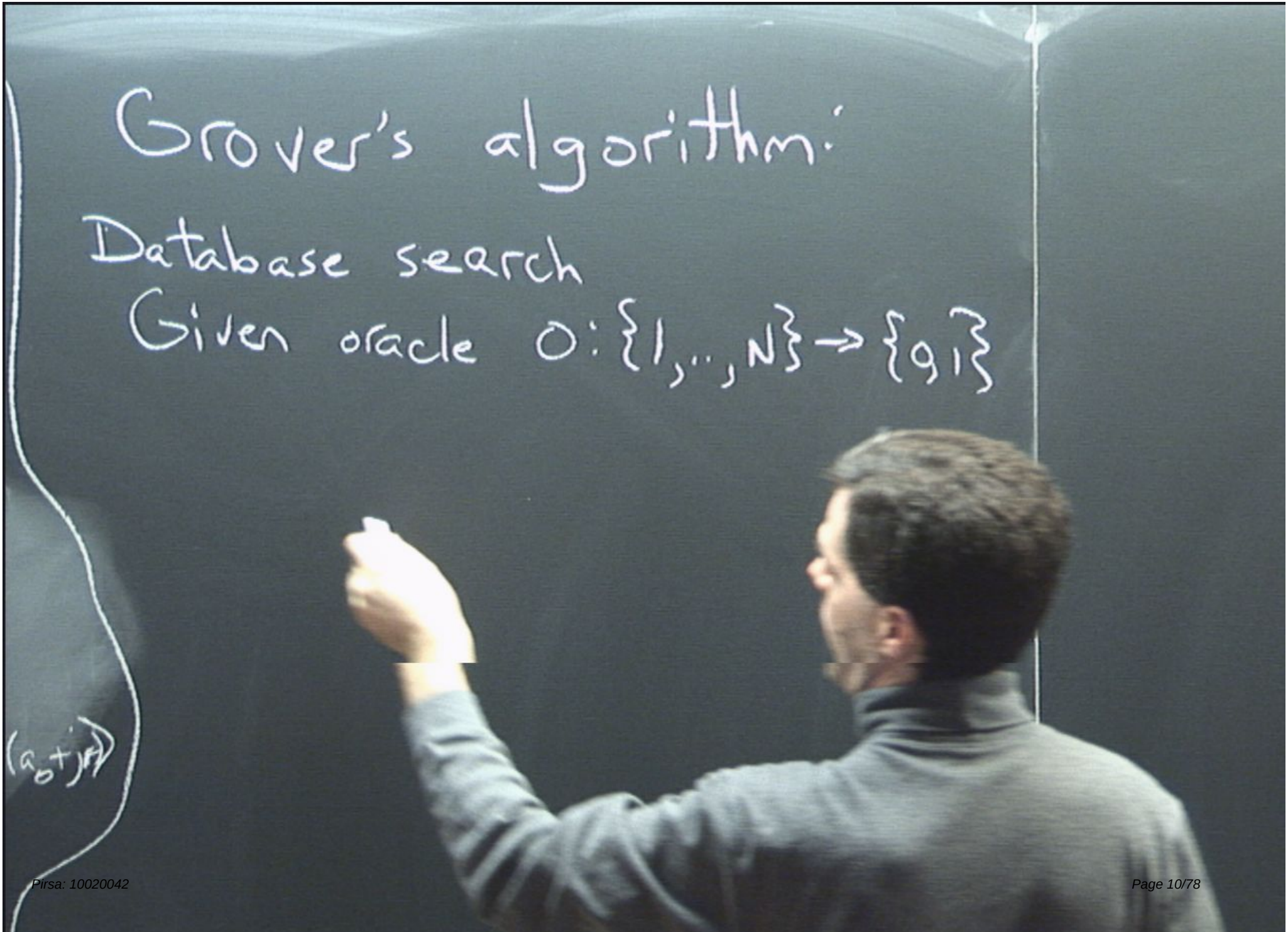
measure

collapse

$$\sum_j |a_0 + jr\rangle$$

Instead $\sum_j |a_0 + jr\rangle |\text{scratch}(a_0 + jr)\rangle$

Algorithm would fail.


Grover's algorithm:
Database search
Given oracle O: {1,..,N} → {0,1}

Grover's algorithm:

Database search

Given oracle $O: \{1, \ldots, N\} \to \{0, 1\}$

want to find x_0 s.t. $O(x_0) = 1$.

$(a_0 + i)$

Grover's algorithm:

Database search

Given oracle $O: \{1, \ldots, N\} \to \{0, 1\}$

want to find x_0 s.t. $O(x_0) = 1$

Warm up with single solution case!

(x_0 is unique).

Let us treat $\forall x \neq x_0$ symmetrically

$(a_0 + i)$

Grover's algorithm:

Database search

Given oracle $O: \{1, \ldots, N\} \to \{0, 1\}$

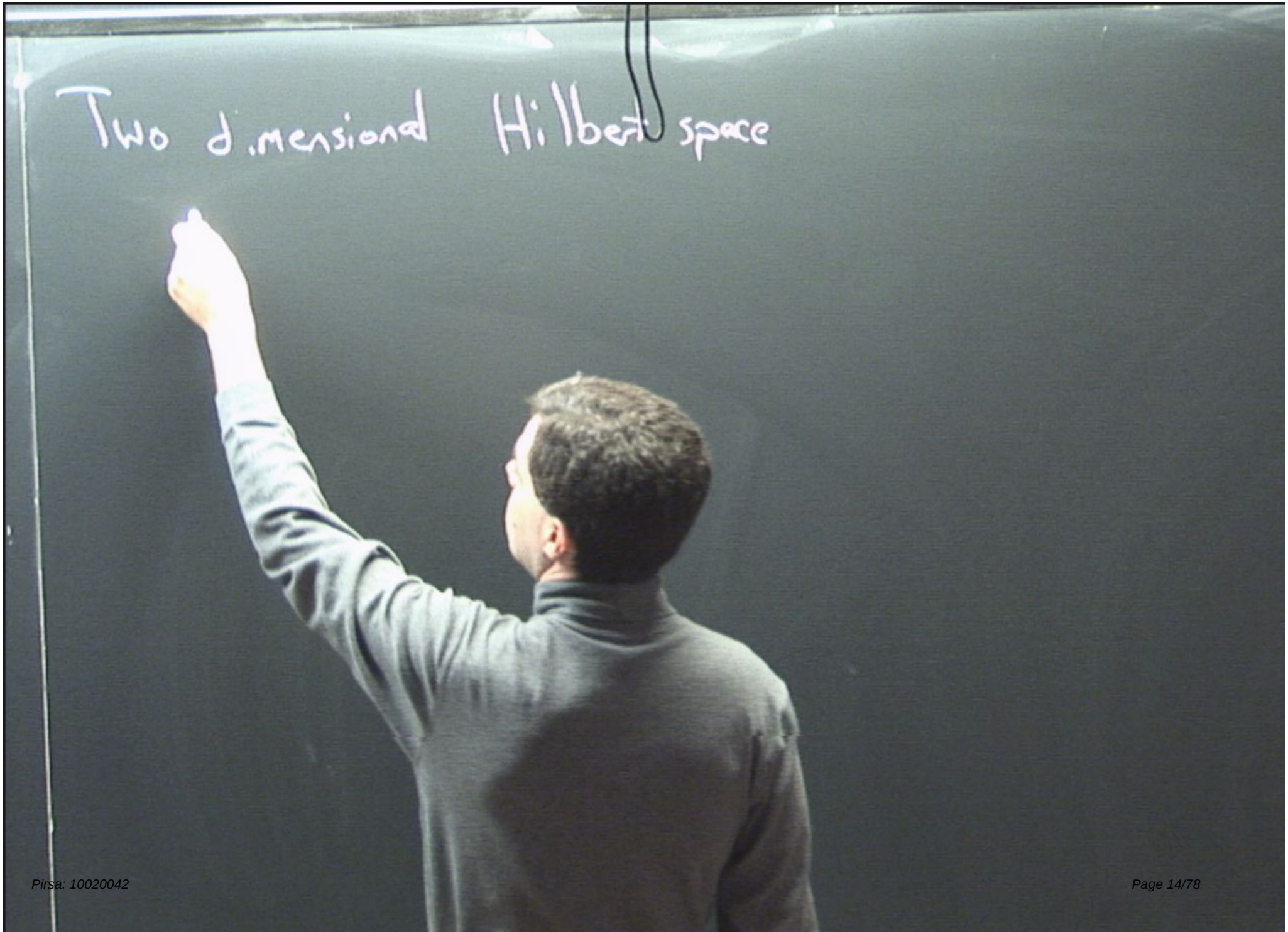
want to find x_0 s.t. $O(x_0) = 1$

Warm up with single solution case:
(x_0 is unique).

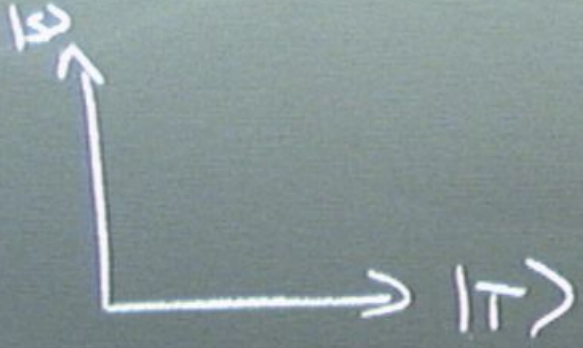
Let us treat $\forall x \neq x_0$ symmetrically

Only deal with states

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

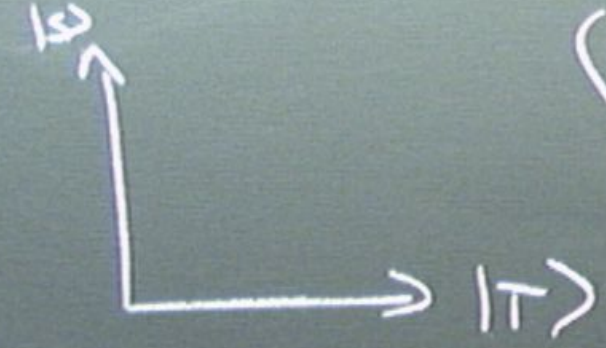

Two dimensional Hilbert space

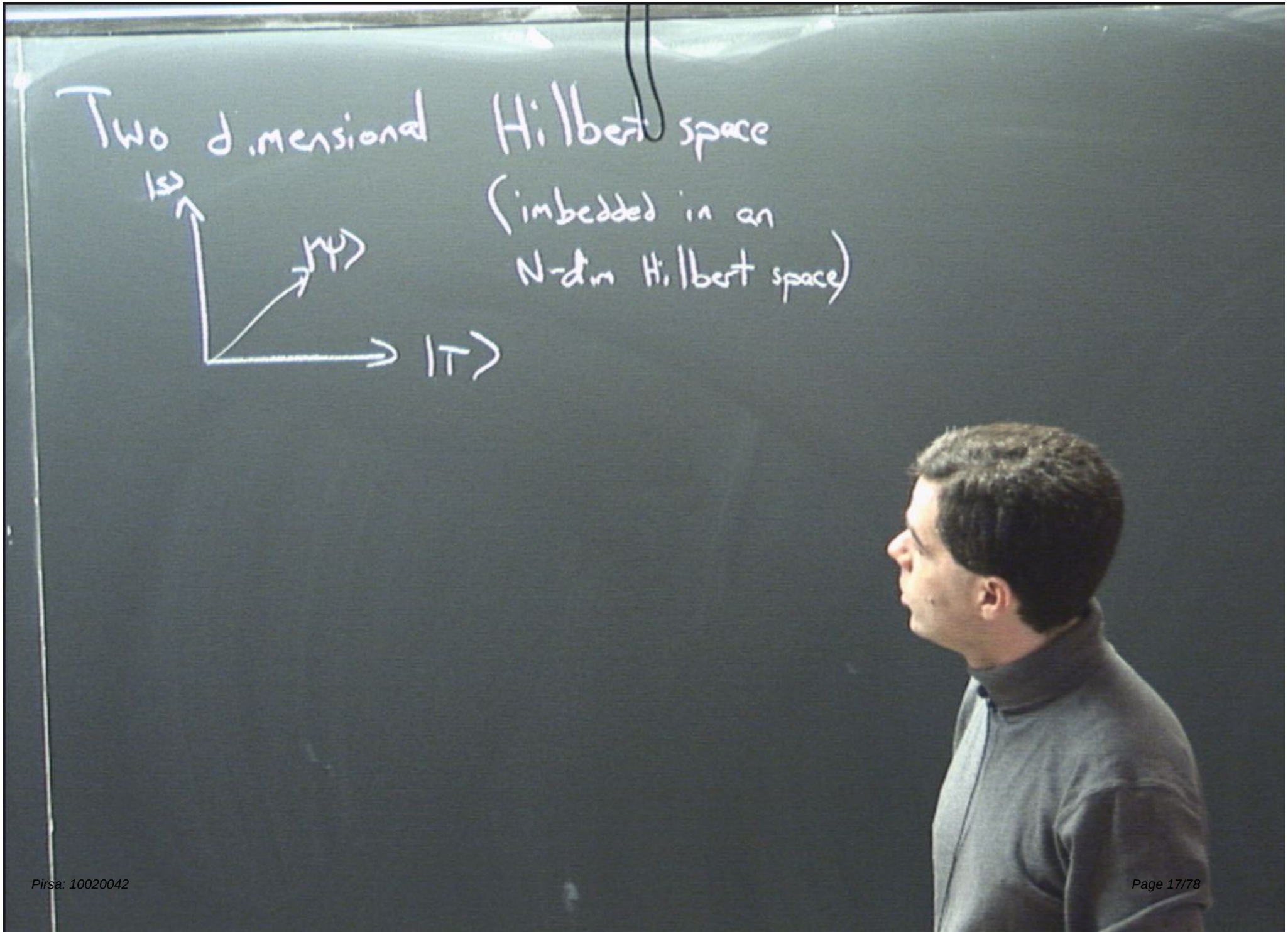
Two dimensional Hilbert space



Two dimensional Hilbert space

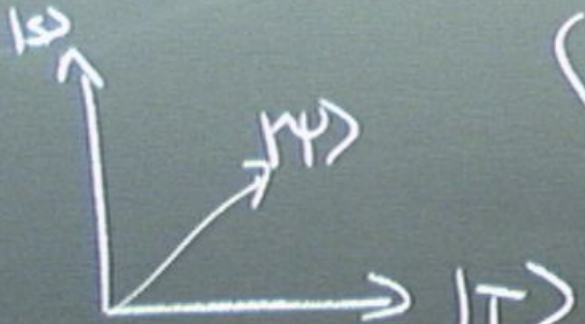
(imbedded in an N-dim Hilbert space)




Two dimensional Hilbert space
(imbedded in an
N-dim Hilbert space)
|S>
|Ψ>
|T>

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase

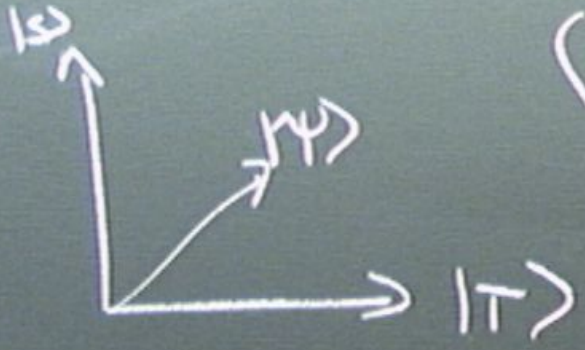
kickback

$|x\rangle \rightarrow (-1)^{O(x)}|x\rangle$

$|s\rangle \rightarrow -|$

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

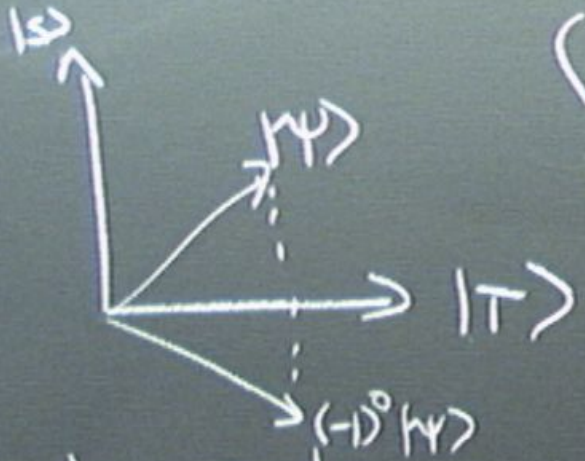
$$|x\rangle \rightarrow (-1)^{O(x)}|x\rangle$$

$$|S\rangle \rightarrow -|S\rangle$$

$$|T\rangle \rightarrow |T\rangle$$

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$|x\rangle \rightarrow (-1)^{o(x)}|x\rangle$

$|S\rangle \rightarrow -|S\rangle$

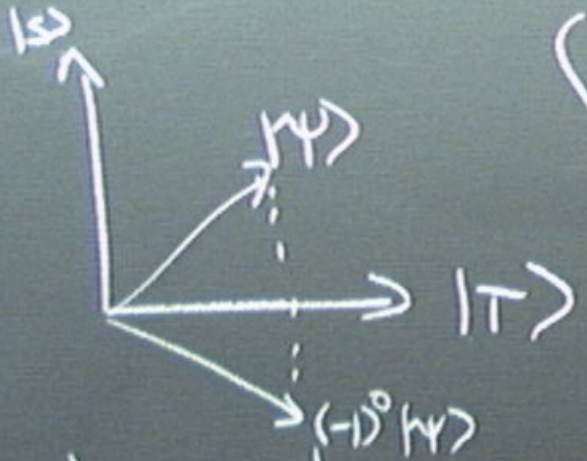
$|T\rangle \rightarrow |T\rangle$

$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \rightarrow -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$$|x\rangle \rightarrow (-1)^{o(x)}|x\rangle$$

$$|s\rangle \rightarrow -|s\rangle$$

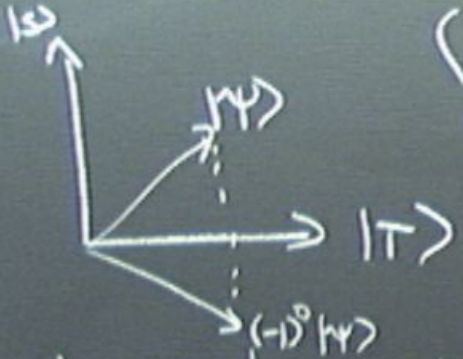
$$|T\rangle \rightarrow |T\rangle$$

$$|\psi\rangle = \alpha|s\rangle + \beta|T\rangle \rightarrow -\alpha|s\rangle + \beta|T\rangle$$

Reflection over $|T\rangle$

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$|x\rangle \rightarrow (-1)^{b(x)} |x\rangle$

$|S\rangle \rightarrow -|S\rangle$

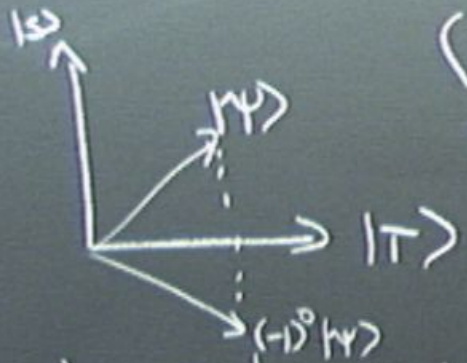
$|T\rangle \rightarrow |T\rangle$

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

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle$ (unnormalized)

Two dimensional Hilbert space (imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$|x\rangle \rightarrow (-1)^{O(x)}|x\rangle$

$|S\rangle \rightarrow -|S\rangle$

$|T\rangle \rightarrow |T\rangle$

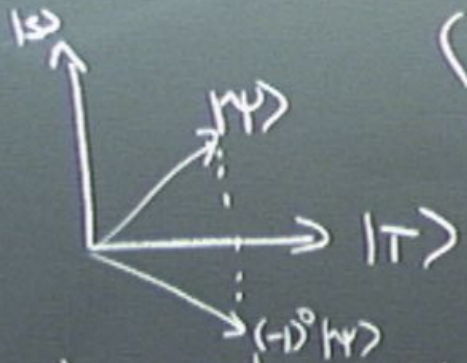
$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \rightarrow -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{\delta(x)}|x\rangle$

$|s\rangle \to -|s\rangle$

$|T\rangle \to |T\rangle$

$|\psi\rangle = \alpha|s\rangle + \beta|T\rangle \to -\alpha|s\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

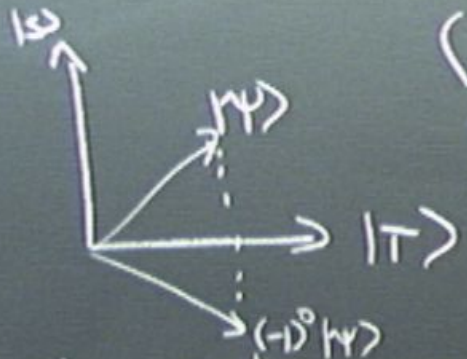
Can create $\sum_x |x\rangle = |s\rangle + |T\rangle = |u\rangle$ (unnormalized)

Can reflect over $|u\rangle = H^{\otimes n}|0..0\rangle$

$|u\rangle \to -|u\rangle$

$|u^\perp\rangle \to +|u^\perp\rangle$

Two dimensional Hilbert space



(imbedded in an N-dim Hilbert space)

Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{\delta(x)}|x\rangle$

$|S\rangle \to -|S\rangle$

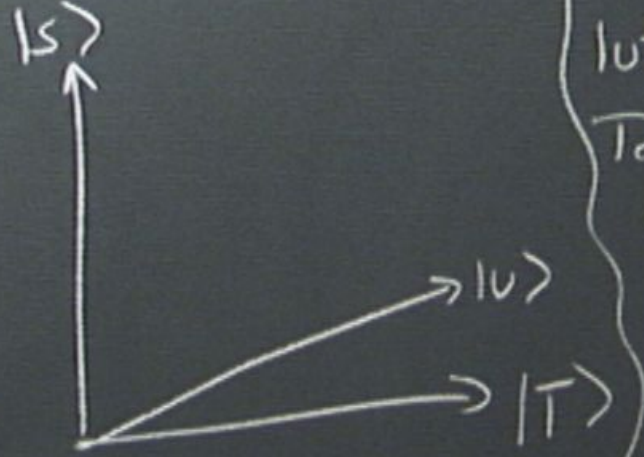
$|T\rangle \to |T\rangle$

$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \to -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Can reflect over $|U\rangle = H^{\otimes n}|0..0\rangle$



$|U\rangle \to -|U\rangle$

$|U^\perp\rangle \to +|U^\perp\rangle$

To reflect over $|0..0\rangle$ do $(-1)^{\overline{|0..0\rangle}\langle 0..0|}$

Two dimensional Hilbert space (imbedded in an N-dim Hilbert space)

Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{\delta(x)}|x\rangle$

$|S\rangle \to -|S\rangle$

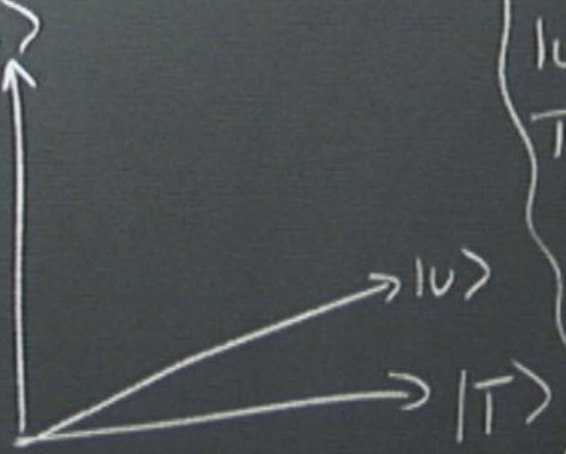
$|T\rangle \to |T\rangle$

$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \to -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Can reflect over $|U\rangle = H^{\otimes n}|0..0\rangle$



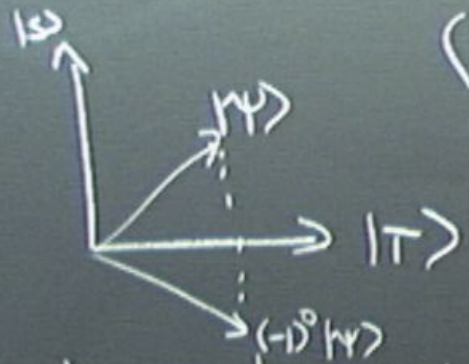
$|U\rangle \to -|U\rangle$

$|U^\perp\rangle \to +|U^\perp\rangle$

To reflect over $|0..0\rangle$ do $(-1)^{|0..0\rangle\langle 0..0|}$

To reflect over $|U\rangle$, do $H^{\otimes n}(-1)^{|0..0\rangle\langle 0..0|}H^{\otimes n}$

Two dimensional Hilbert space



Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{\delta(x)}|x\rangle$

$|S\rangle \to -|S\rangle$

$|T\rangle \to |T\rangle$

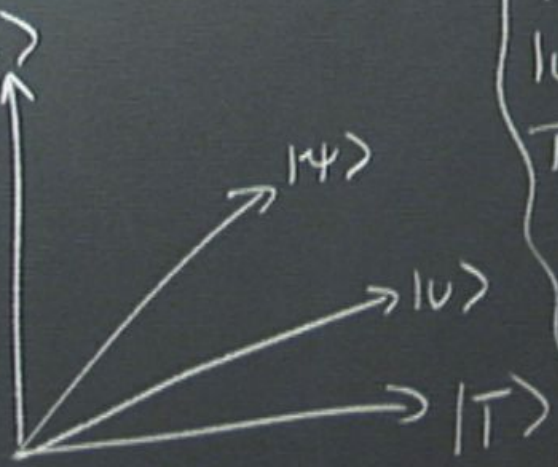
$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \to -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

(imbedded in an N-dim Hilbert space)

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Can reflect over $|U\rangle = H^{\otimes n}|0..0\rangle$



$|U\rangle \to -|U\rangle$

$|U^\perp\rangle \to +|U^\perp\rangle$

To reflect over $|0..0\rangle$ do $(-1)^{|0\ldots0\rangle\langle 0\ldots 0|}$

To reflect over $|U\rangle$, do $H^{\otimes n}(-1)^{|0\ldots0\rangle\langle 0\ldots 0|}H^{\otimes n}$

Two dimensional Hilbert space (imbedded in an N-dim Hilbert space)

Apply oracle w/ phase kickback

$|x\rangle \rightarrow (-1)^{\delta(x)}|x\rangle$

$|S\rangle \rightarrow -|S\rangle$

$|T\rangle \rightarrow |T\rangle$

$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \rightarrow -\alpha|S\rangle + \beta|T\rangle$

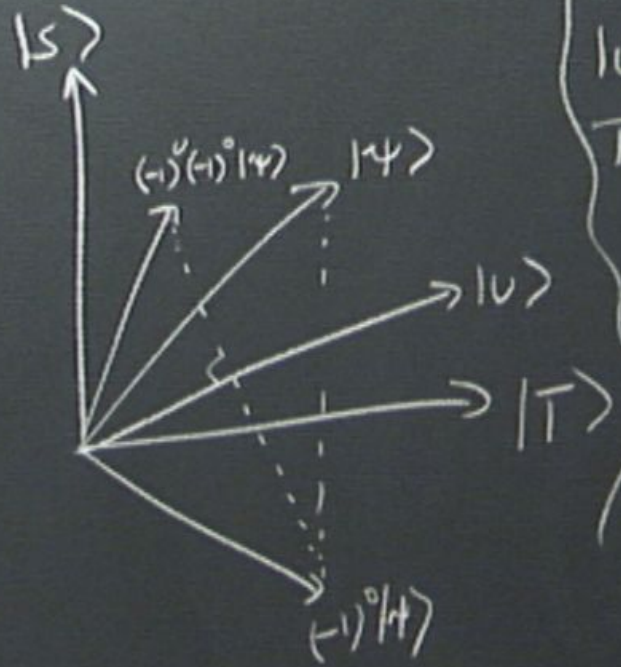
Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Can reflect over $|U\rangle = H^{\otimes n}|0..0\rangle$

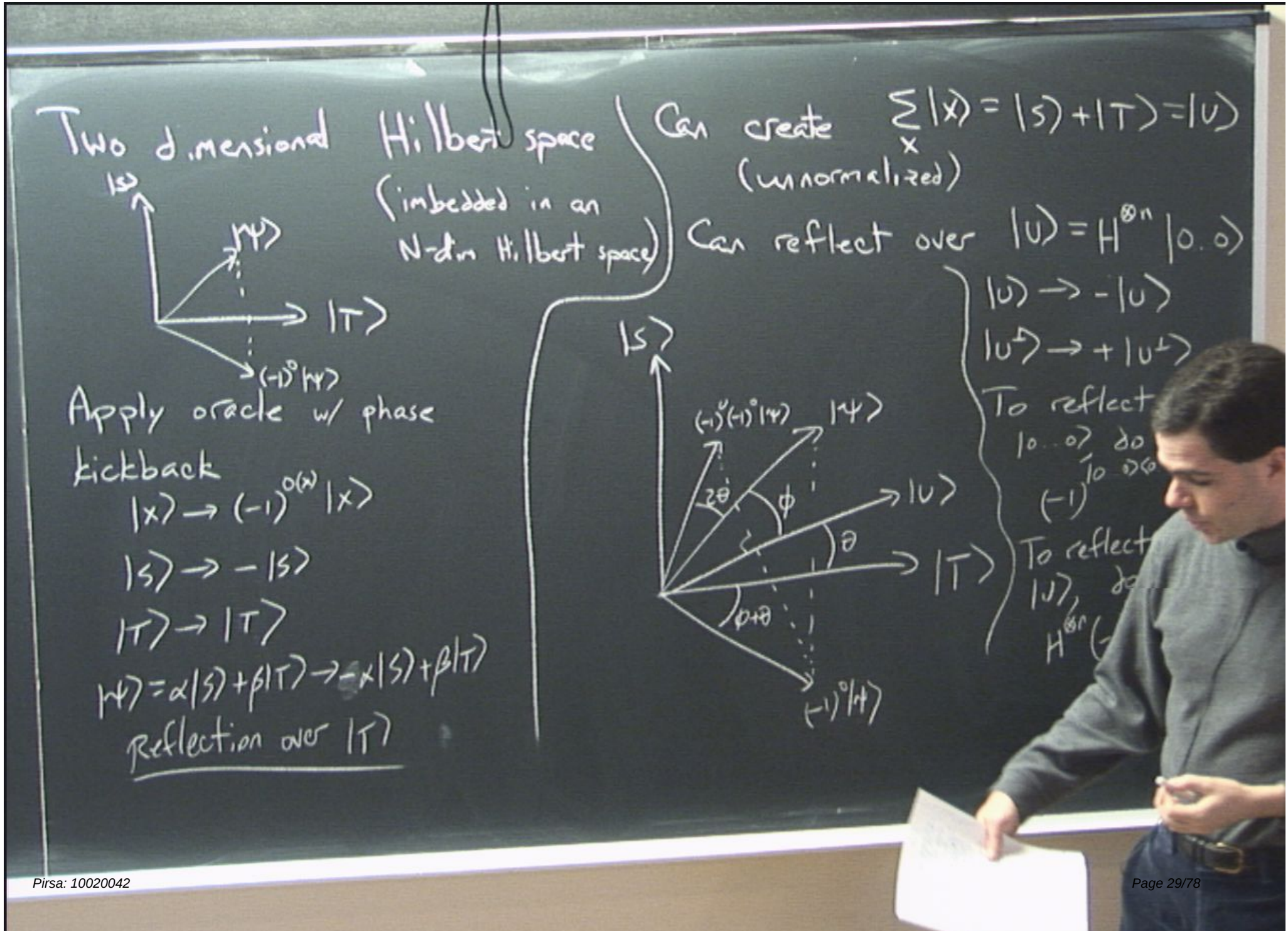
$|U\rangle \rightarrow -|U\rangle$

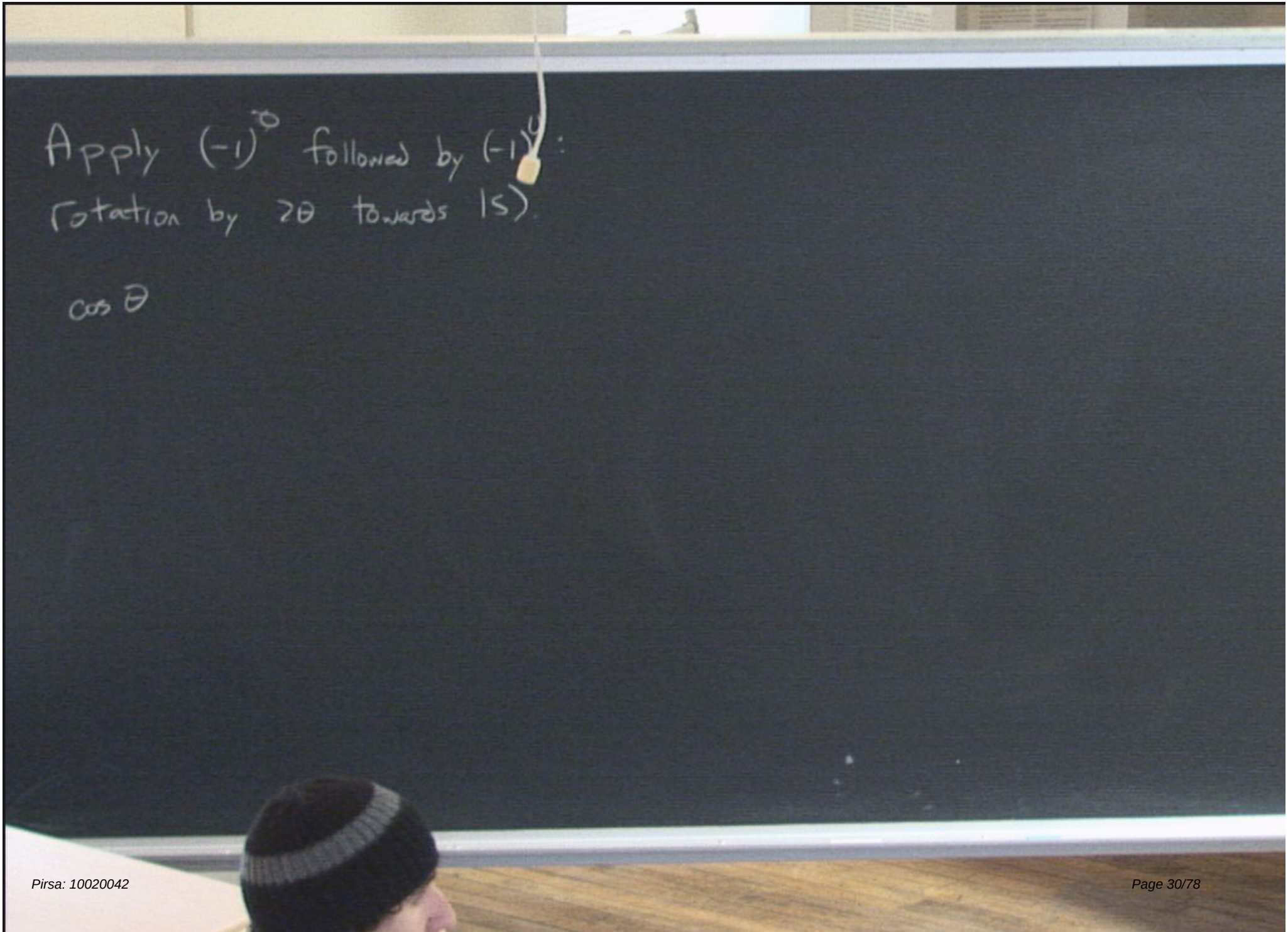
$|U^\perp\rangle \rightarrow +|U^\perp\rangle$



To reflect over $|0..0\rangle$ do $(-1)^{10\ldots0\rangle\langle0\ldots01}$

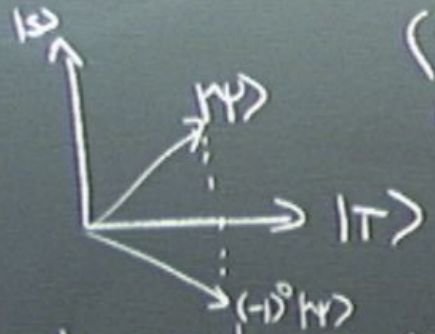
To reflect over $|U\rangle$, do $H^{\otimes n}(-1)^{10\ldots0\rangle\langle0\ldots01}H^{\otimes n}$


Two dimensional Hilbert space
(imbedded in an N-dim Hilbert space)
|S⟩
|Ψ⟩
|T⟩
(-1)^δ|Ψ⟩
Apply oracle w/ phase kickback
|x⟩ → (-1)^{δ(x)}|x⟩
|S⟩ → -|S⟩
|T⟩ → |T⟩
|Ψ⟩ = α|S⟩ + β|T⟩ → -α|S⟩ + β|T⟩
Reflection over |T⟩
Can create Σ_x |x⟩ = |S⟩ + |T⟩ = |U⟩
(unnormalized)
Can reflect over |U⟩ = H^{⊗n}|0..0⟩
|U⟩ → -|U⟩
|U^⊥⟩ → +|U^⊥⟩
To reflect
|0..0⟩ do
(-1)^{|0..0⟩}
To reflect
|U⟩, do
H^{⊗n}
(-1)^δ(-1)^δ|Ψ⟩
|Ψ⟩
2θ
φ
|U⟩
θ
|T⟩
φ+θ
(-1)^δ|Ψ⟩


Apply $(-1)^0$ followed by $(-1)^1$:
rotation by 2θ towards 1S).
$\cos\theta$

Two dimensional Hilbert space

(imbedded in an N-dim Hilbert space)



Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{\delta(x)}|x\rangle$

$|S\rangle \to -|S\rangle$

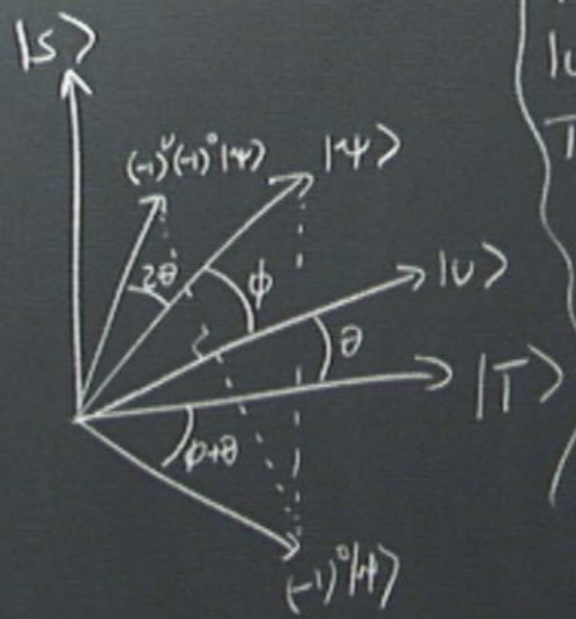
$|T\rangle \to |T\rangle$

$|\Psi\rangle = \alpha|S\rangle + \beta|T\rangle \to -\alpha|S\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)

Can reflect over $|U\rangle = H^{\otimes n}|0\ldots0\rangle$

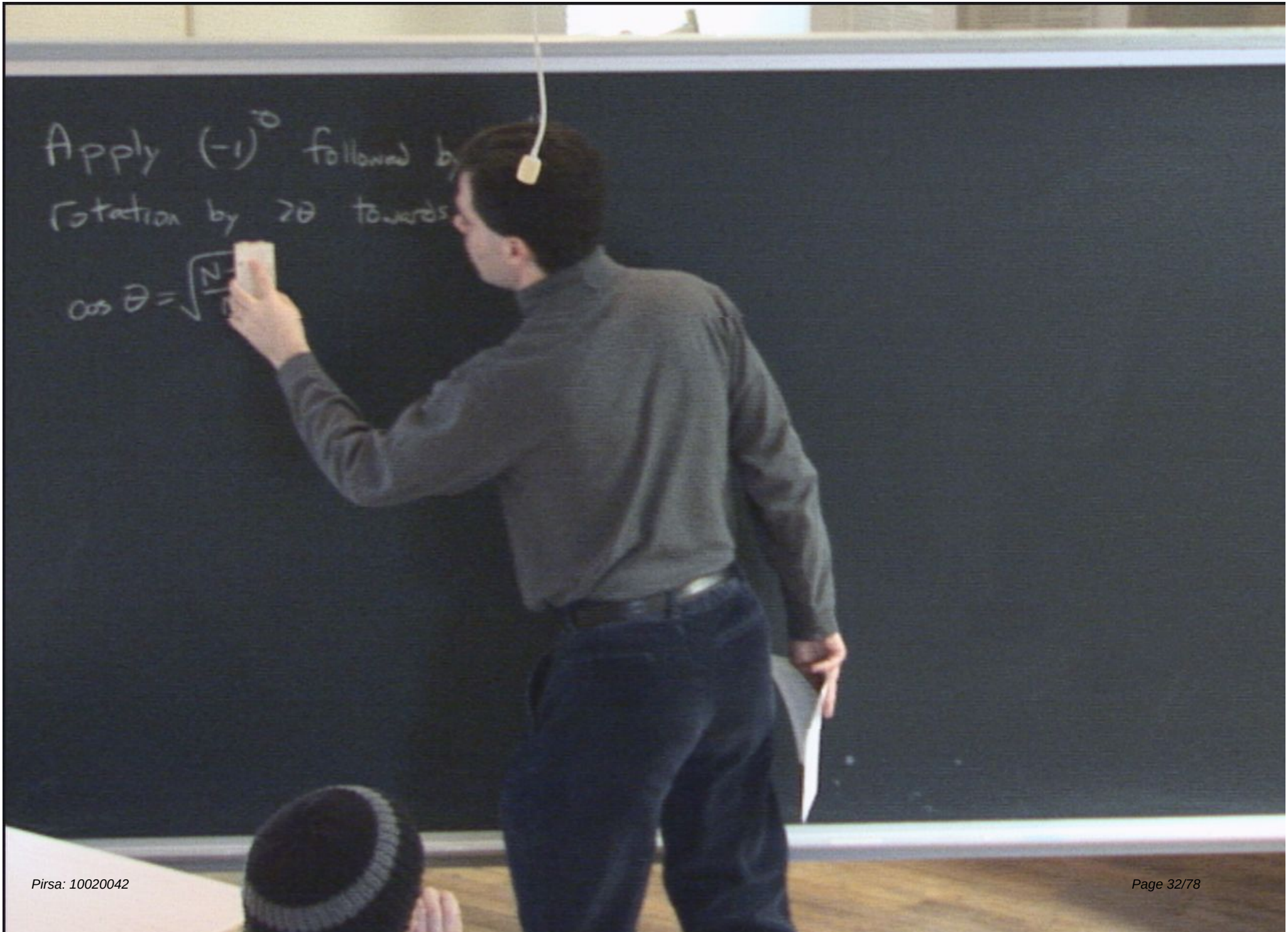


$|U\rangle \to -|U\rangle$

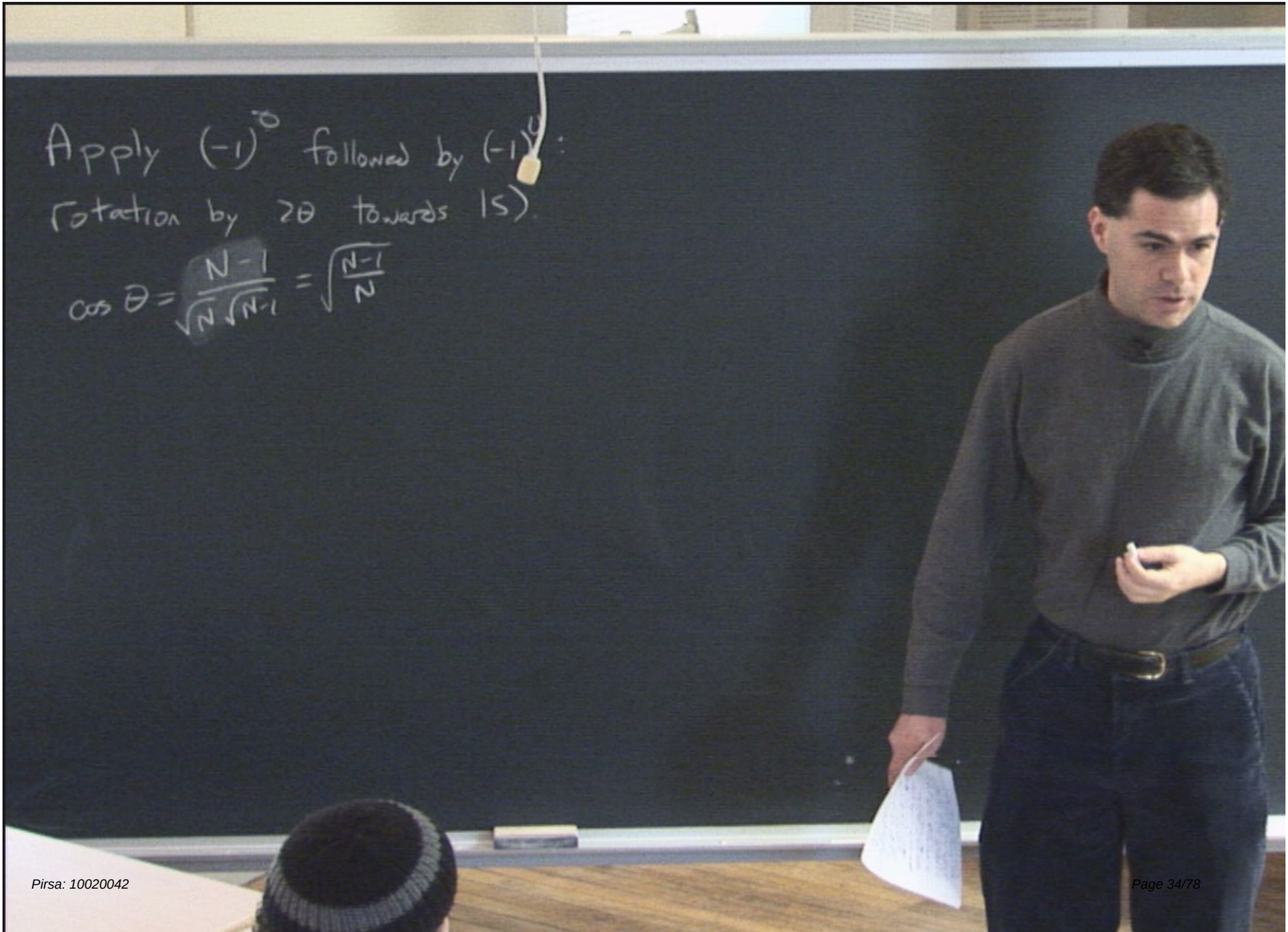
$|U^\perp\rangle \to +|U^\perp\rangle$

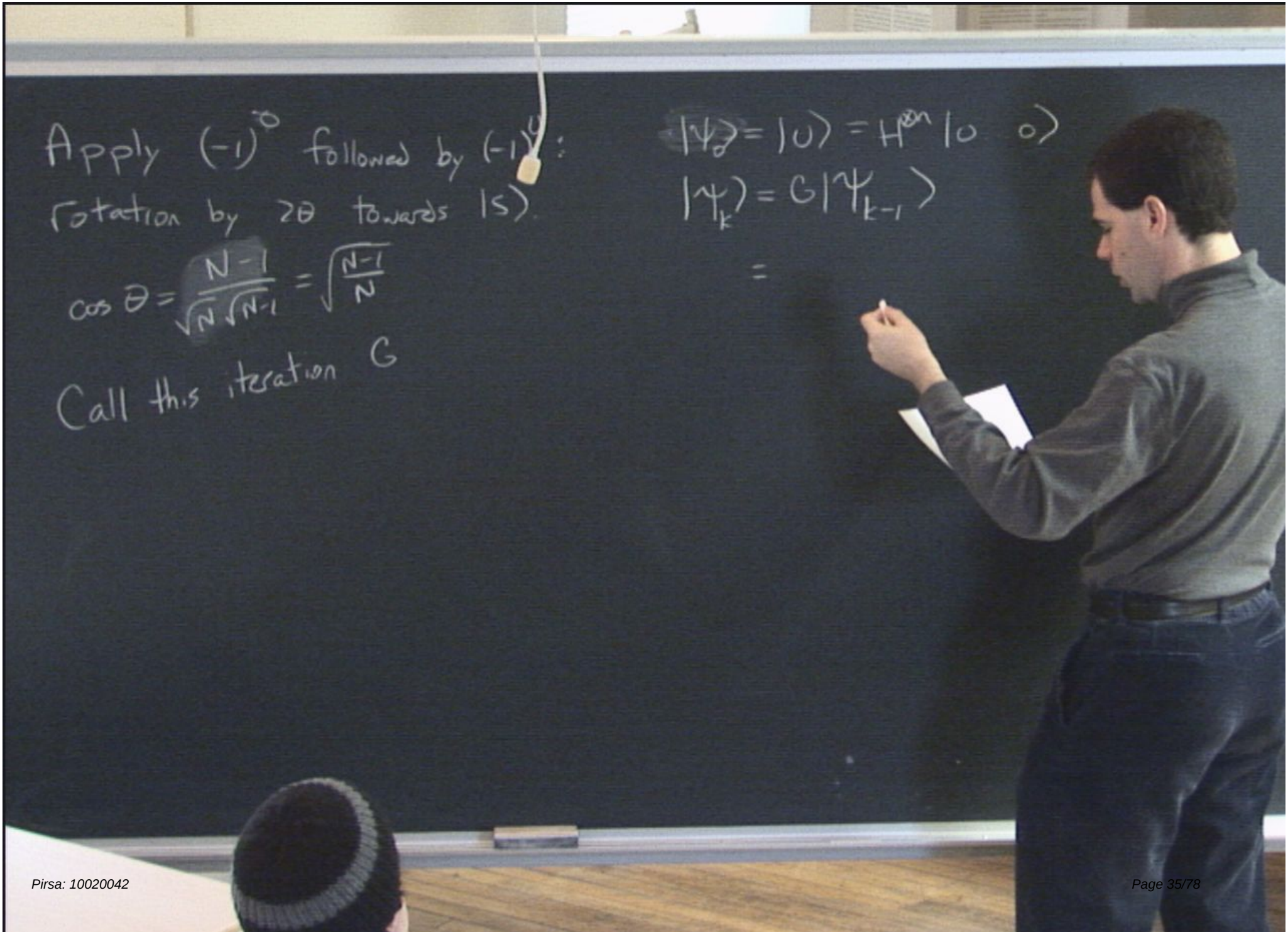
To reflect over $|0\ldots0\rangle$ do $(-1)^{\text{to 000...01}}$

To reflect over $|U\rangle$, do $H^{\otimes n}(-1)^{\text{to 000...01}}H^{\otimes n}$


Apply $(-1)^0$ followed by
rotation by 2θ towards
$\cos\theta = \sqrt{\frac{1}{2}}$


Apply $(-1)^{\vec{0}}$ followed by $(-1)^{\vec{u}}$:
rotation by 2θ towards $\vec{s}$).
$\cos\theta = \frac{N-1}{}$


Apply $(-1)^{\vec{0}}$ followed by $(-1)^{\vec{v}}$:
rotation by 2θ towards $|s\rangle$.
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$


Apply $(-1)^0$ followed by $(-1)^{\psi}$:
rotation by 2θ towards $|s\rangle$.
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$
Call this iteration G
$|\psi_0\rangle = |0\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
=

Apply $(-1)^{f(x)}$ followed by $(-1)^{|s\rangle\langle s|}$:

rotation by 2θ towards $|s\rangle$

$$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$$

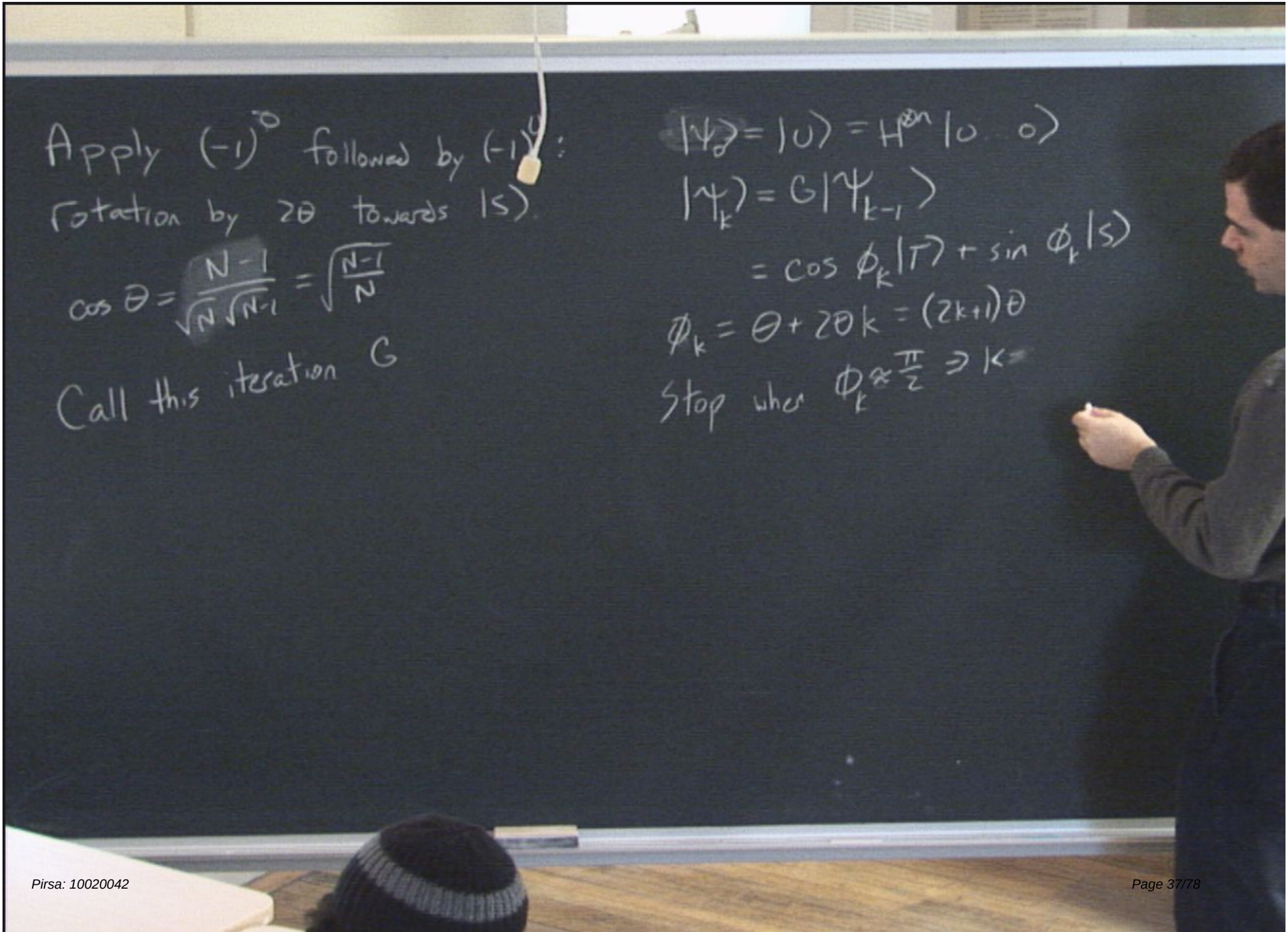
Call this iteration G

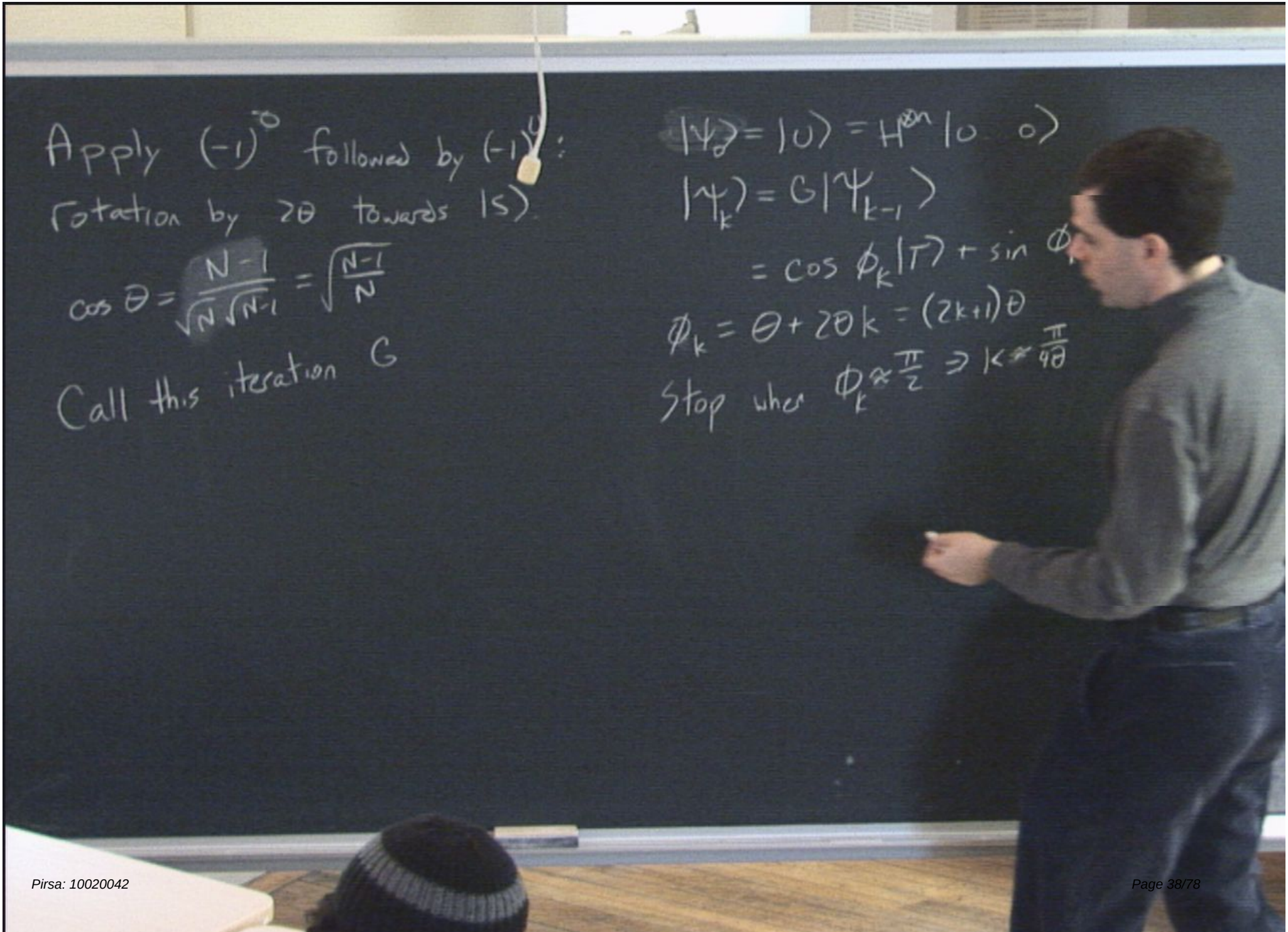
$$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$$

$$|\psi_k\rangle = G|\psi_{k-1}\rangle$$

$$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$$

$$\phi_k = \theta + 2\theta k = (2k+1)\theta$$


Apply $(-1)^{f(x)}$ followed by $(-1)^{y}$:
rotation by 2θ towards $|s\rangle$.
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$
Call this iteration G
$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k =$


Apply $(-1)^{\bar{0}}$ followed by $(-1)^{\psi}$:
rotation by 2θ towards $|s\rangle$.
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$
Call this iteration G
$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$

Apply $(-1)^{f(x)}$ followed by $(-1)^{|s\rangle\langle s|}$:

rotation by 2θ towards $|s\rangle$.

$$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}, \quad \sin\theta = \sqrt{\frac{1}{N}}$$

Call this iteration G

$$|\psi_0\rangle = |U\rangle = H^{\otimes n}|0\ 0\rangle$$

$$|\psi_k\rangle = G|\psi_{k-1}\rangle$$

$$= \cos\phi_k|T\rangle + \sin\phi_k|$$

$$\phi_k = \theta + 2\theta k = (2k+1)\theta$$

Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$

When N is large

Apply $(-1)^{f_0}$ followed by $(-1)^{\psi}$:

rotation by 2θ towards $|s\rangle$.

$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$

Call this iteration G

$|\psi_0\rangle = |U\rangle = H^{\otimes n}|0\ 0\rangle$

$|\psi_k\rangle = G|\psi_{k-1}\rangle$

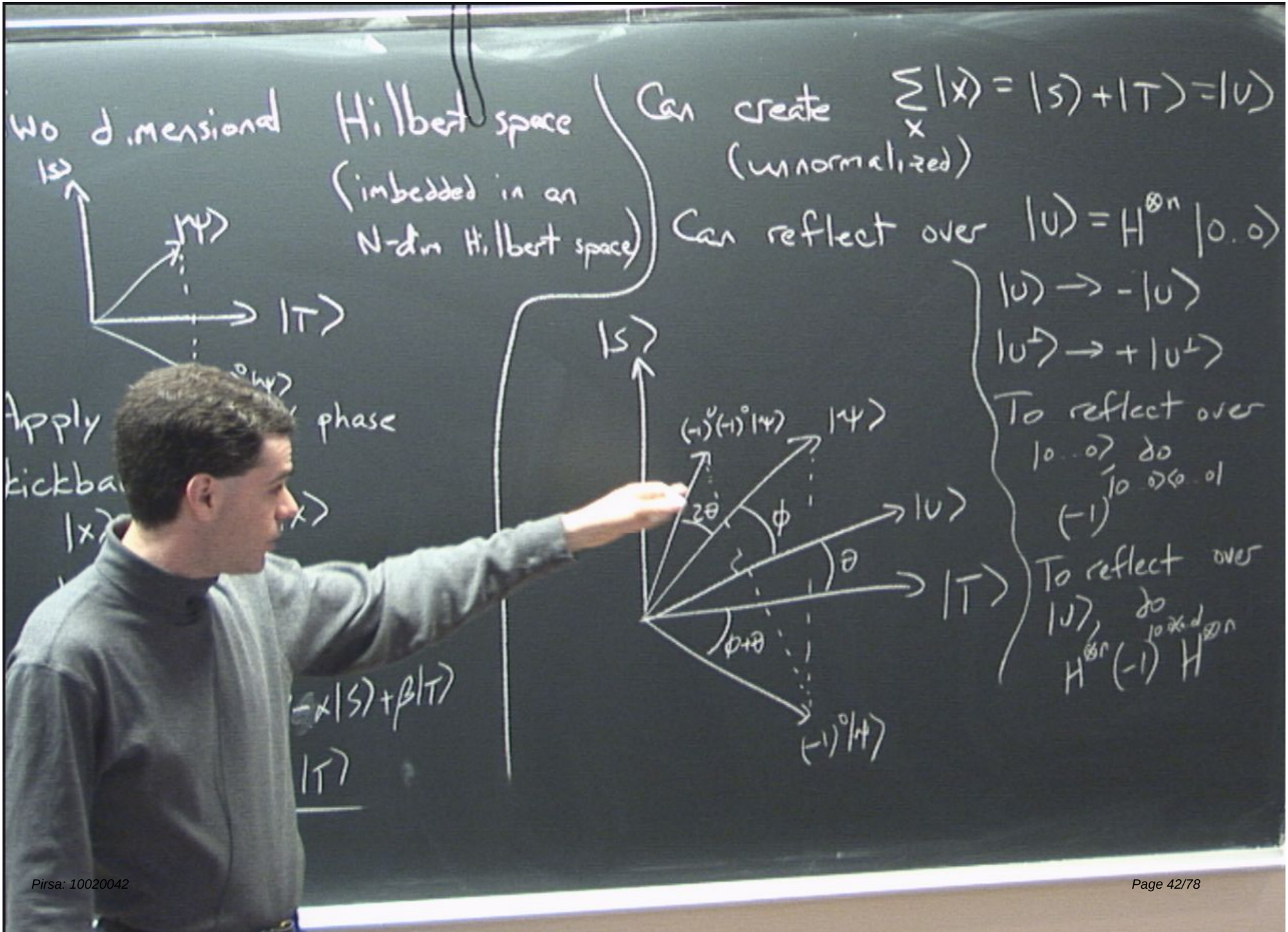
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$

$\phi_k = \theta + 2\theta k = (2k+1)\theta$

Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$

When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow$ $k \approx \frac{\pi}{4}\sqrt{N}$


Two dimensional Hilbert space
(imbedded in an N-dim Hilbert space)
Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$
(unnormalized)
Can reflect over $|U\rangle = H^{\otimes n}|0\ 0\rangle$
$|U\rangle \to -|U\rangle$
$|U^\perp\rangle \to +|U^\perp\rangle$
To reflect over $|0\ 0\rangle$ do
$(-1)^{|0\ 0\rangle\langle 0\ 0|}$
To reflect over $|U\rangle$ do
$H^{\otimes n}(-1)^{|0\ 0\rangle\langle 0\ 0|}H^{\otimes n}$
$|S\rangle$
$|H\rangle$
$|U\rangle$
$|T\rangle$
θ
ϕ
Kickback
$|x\rangle \to$
Apply
Reflect


Wo dimensional Hilbert space
(imbedded in an N-dim Hilbert space)
Can create $\sum_x |x\rangle = |S\rangle + |T\rangle = |U\rangle$ (unnormalized)
Can reflect over $|U\rangle = H^{\otimes n}|0..0\rangle$
$|U\rangle \to -|U\rangle$
$|U^\perp\rangle \to +|U^\perp\rangle$
To reflect over $|0..0\rangle$ do $(-1)^{|0..0\rangle\langle 0..0|}$
To reflect over $|U\rangle$, do $H^{\otimes n}(-1)^{|0..0\rangle\langle 0..0|}H^{\otimes n}$
$|S\rangle$
$|\Psi\rangle$
$|T\rangle$
$|U\rangle$
2θ
ϕ
θ
$\phi+\theta$
$(-1)^{|U\rangle\langle U|}|\Psi\rangle$
$(-1)^{|T\rangle\langle T|}|\Psi\rangle$
Apply phase
kickba
$|x\rangle$
$-\alpha|S\rangle+\beta|T\rangle$
$|T\rangle$

Apply $(-1)^{f_0}$ followed by $(-1)^{f}$:

rotation by 2θ towards $|s\rangle$

$$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}, \quad \sin\theta = \sqrt{\frac{1}{N}}$$

Call this iteration G

$$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$$

$$|\psi_k\rangle = G|\psi_{k-1}\rangle$$

$$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$$

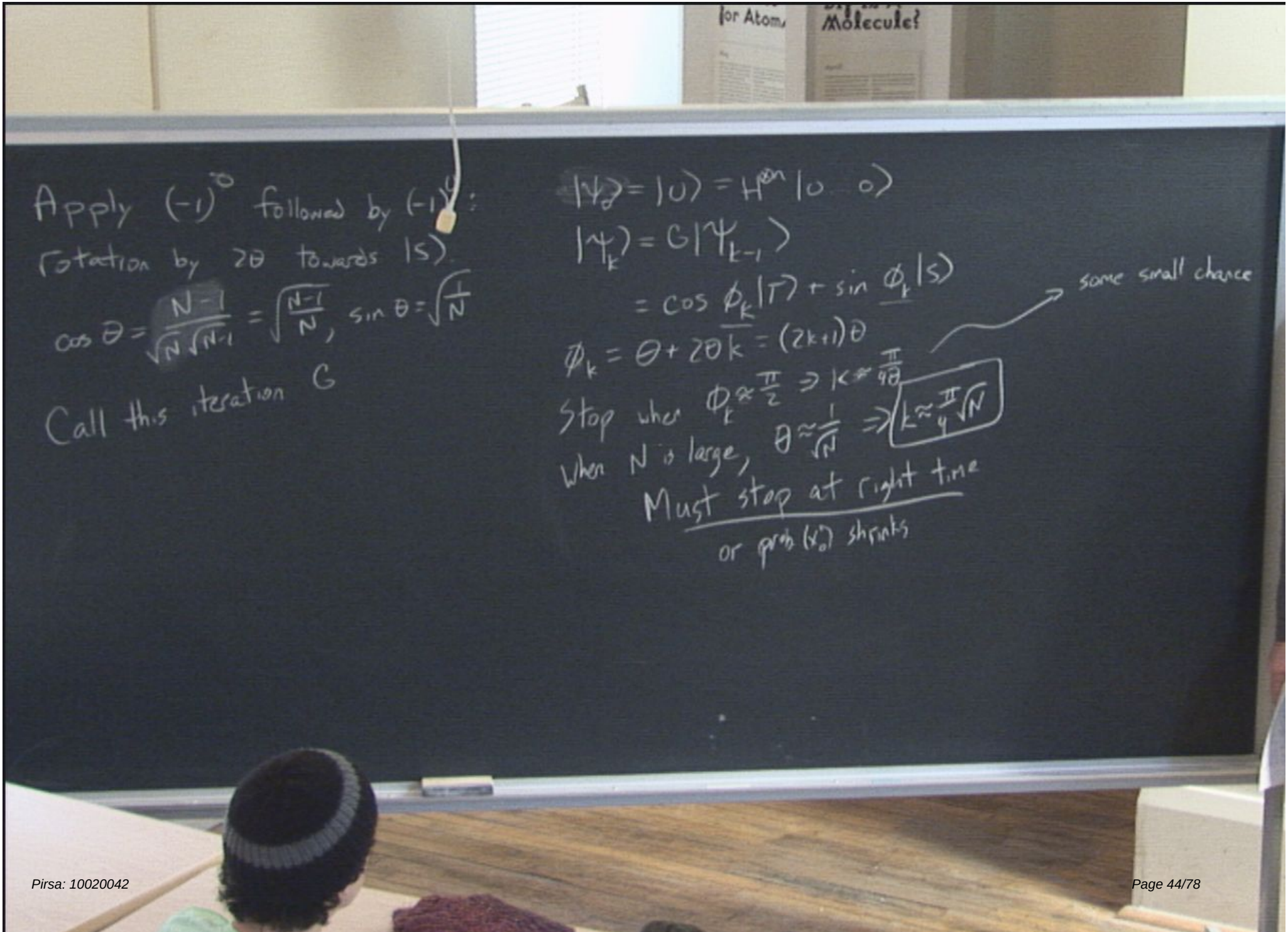
$$\phi_k = \theta + 2\theta k = (2k+1)\theta$$

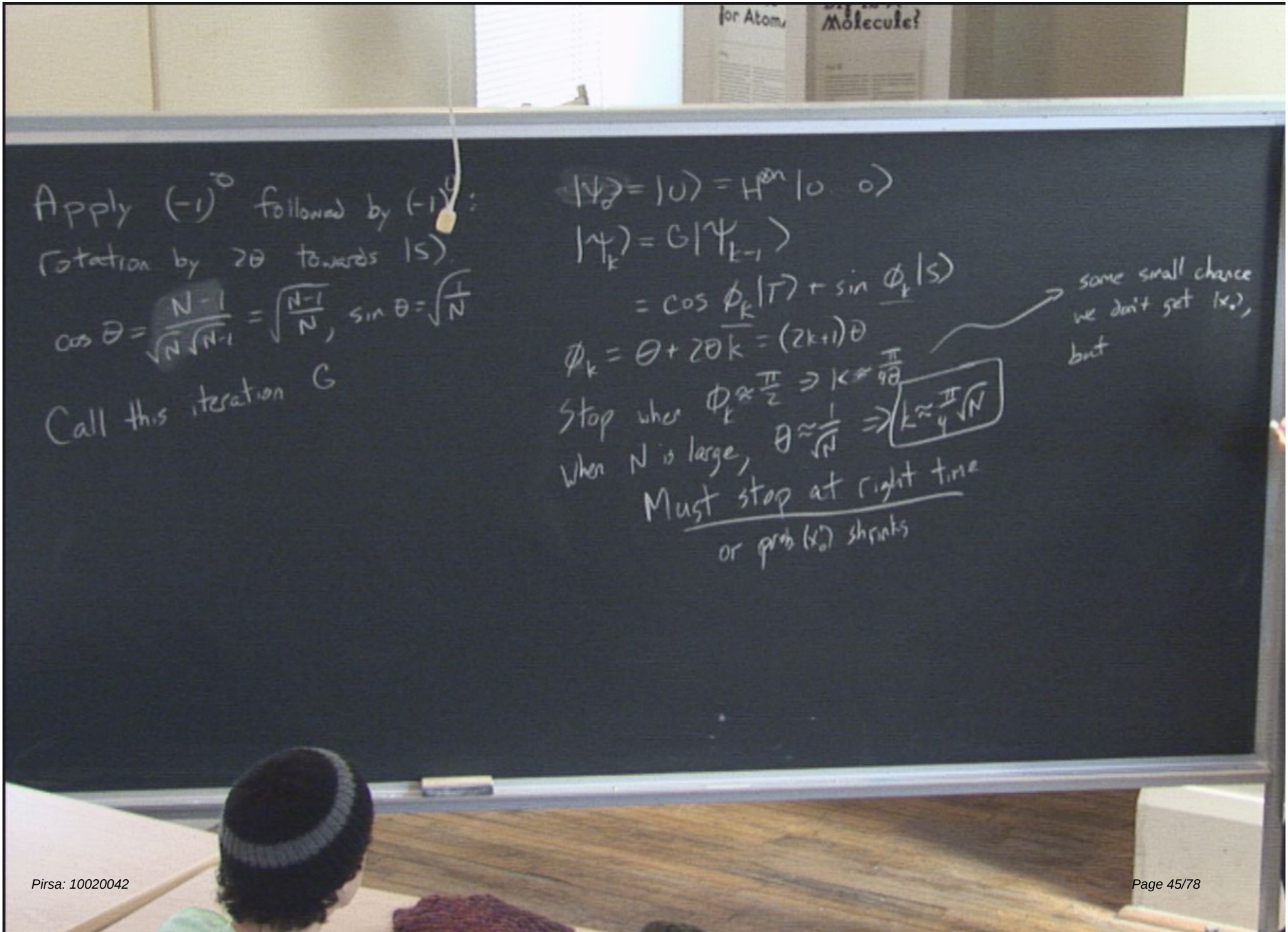
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$

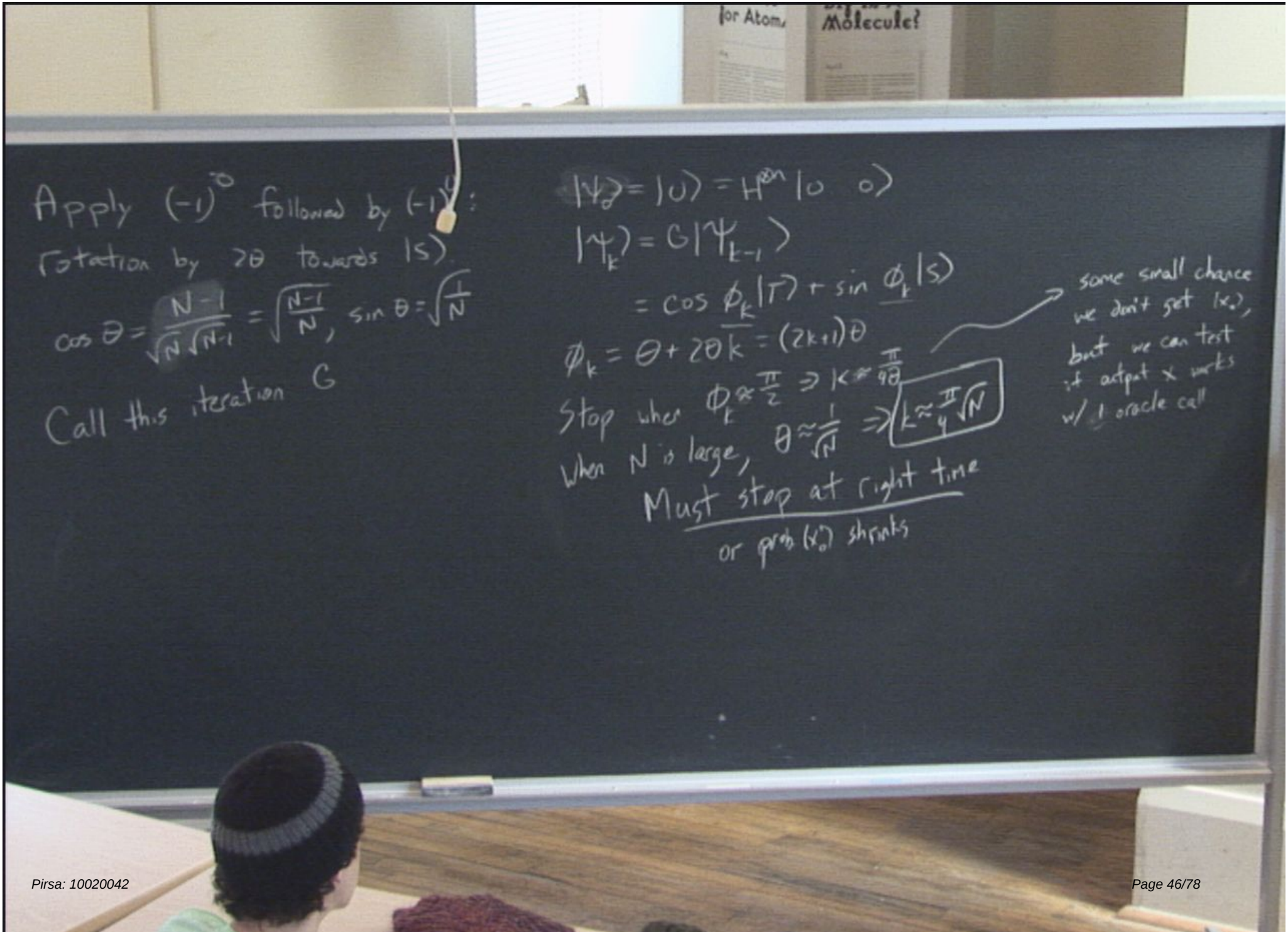
When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow$ $k \approx \frac{\pi}{4}\sqrt{N}$

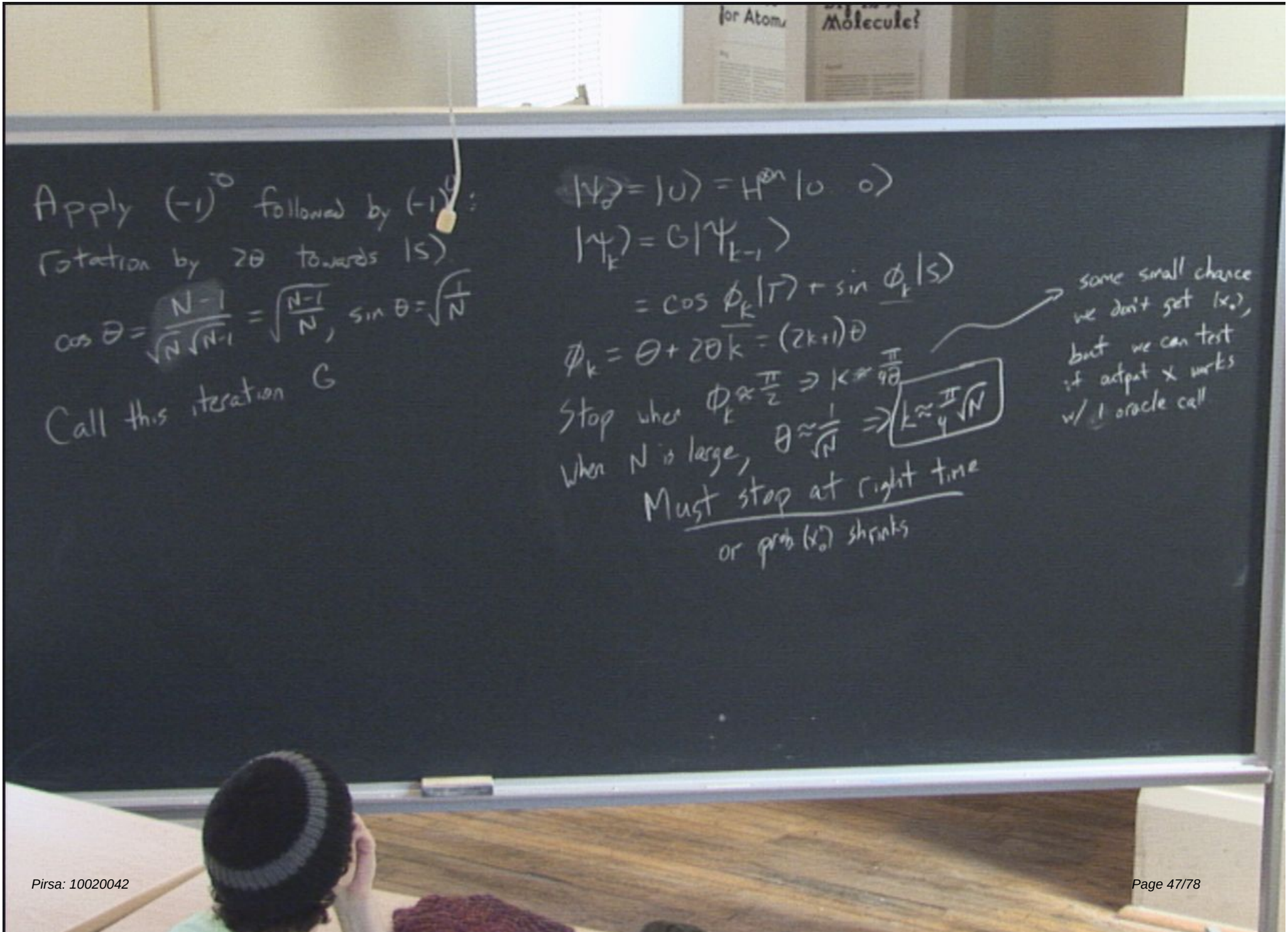
Must stop at right time

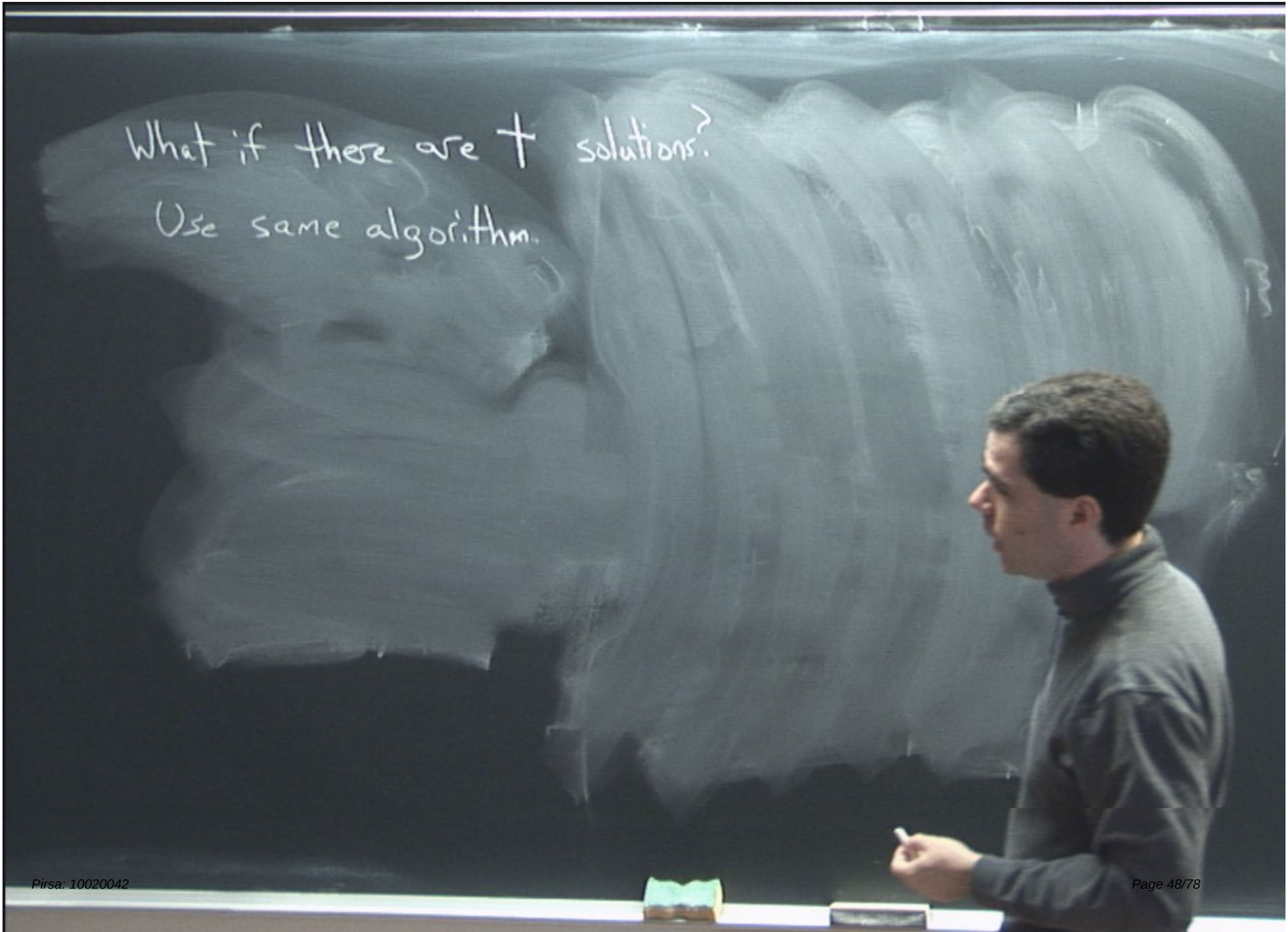
or prob (x_0) shrinks


for Atom
Molecule?
Apply $(-I)^0$ followed by $(-I)^\psi$:
rotation by 2θ towards $|s\rangle$
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$
Call this iteration G
$|\psi_0\rangle = |0\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$
When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow k \approx \frac{\pi}{4}\sqrt{N}$
some small chance
Must stop at right time
or prob (x_0) shrinks


for Atom
Molecule?
Apply $(-1)^0$ followed by $(-1)^1$:
rotation by 2θ towards $|s\rangle$
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$
Call this iteration G
$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$
When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow k \approx \frac{\pi}{4}\sqrt{N}$
some small chance we don't get $|x_0\rangle$, but
Must stop at right time
or prob (x_0) shrinks


for Atom
Molecule?
Apply $(-1)^0$ followed by $(-1)^y$:
rotation by 2θ towards $|s\rangle$
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$
Call this iteration G
$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$
When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow k \approx \frac{\pi}{4}\sqrt{N}$
Must stop at right time
or prob (x_0) shrinks
some small chance we don't get $|x_0\rangle$, but we can test if output x works w/ 1 oracle call


for Atom
Molecule?
Apply $(-1)^0$ followed by $(-1)^{\psi}$:
rotation by 2θ towards $|s\rangle$
$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$
Call this iteration G
$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$
$|\psi_k\rangle = G|\psi_{k-1}\rangle$
$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$
$\phi_k = \theta + 2\theta k = (2k+1)\theta$
Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$
When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow k \approx \frac{\pi}{4}\sqrt{N}$
Must stop at right time
or prob (x_0) shrinks
some small chance we don't get $|x_0\rangle$, but we can test if output x works w/ 1 oracle call


What if there are † solutions?
Use same algorithm.

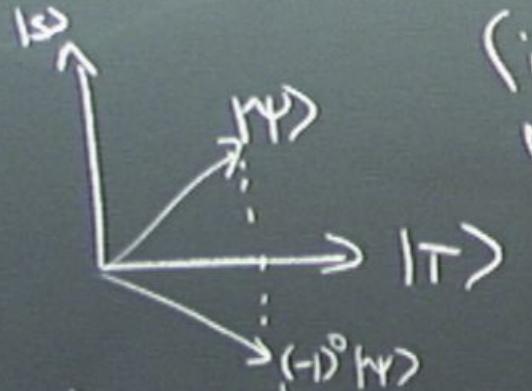
What if there are t solutions?

Use same algorithm.

$$|s\rangle = \sum_{x \mid \alpha(x)=1} |x\rangle$$

$$|T\rangle = \sum_{y \mid \alpha(y)=0} |y\rangle$$

Two dimensional Hilbert space



(imbedded in an N-dim Hilbert space)

Apply oracle w/ phase kickback

$|x\rangle \to (-1)^{O(x)}|x\rangle$

$|s\rangle \to -|s\rangle$

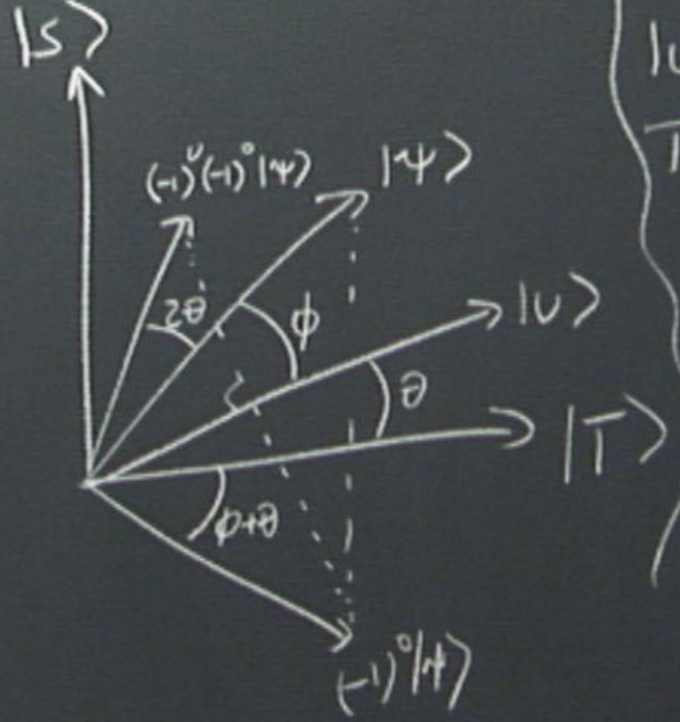
$|T\rangle \to |T\rangle$

$|\psi\rangle = \alpha|s\rangle + \beta|T\rangle \to -\alpha|s\rangle + \beta|T\rangle$

Reflection over $|T\rangle$

Can create $\sum_x |x\rangle = |s\rangle + |T\rangle = |u\rangle$ (unnormalized)

Can reflect over $|u\rangle = H^{\otimes n}|0..0\rangle$



$|u\rangle \to -|u\rangle$

$|u^\perp\rangle \to +|u^\perp\rangle$

To reflect over $|0..0\rangle$ do $(-1)^{|0..0\rangle\langle 0..0|}$

To reflect over $|u\rangle$, do $H^{\otimes n}(-1)^{|0..0\rangle\langle 0..0|}H^{\otimes n}$

Apply $(-1)^{f(x)}$ followed by $(-1)^{0}$:

Rotation by 2θ towards $|s\rangle$

$\cos\theta = \frac{N-1}{\sqrt{N}\sqrt{N-1}} = \sqrt{\frac{N-1}{N}}$, $\sin\theta = \sqrt{\frac{1}{N}}$

Call this iteration G

$|\psi_0\rangle = |u\rangle = H^{\otimes n}|0\ 0\rangle$

$|\psi_k\rangle = G|\psi_{k-1}\rangle$

$= \cos\phi_k|T\rangle + \sin\phi_k|s\rangle$

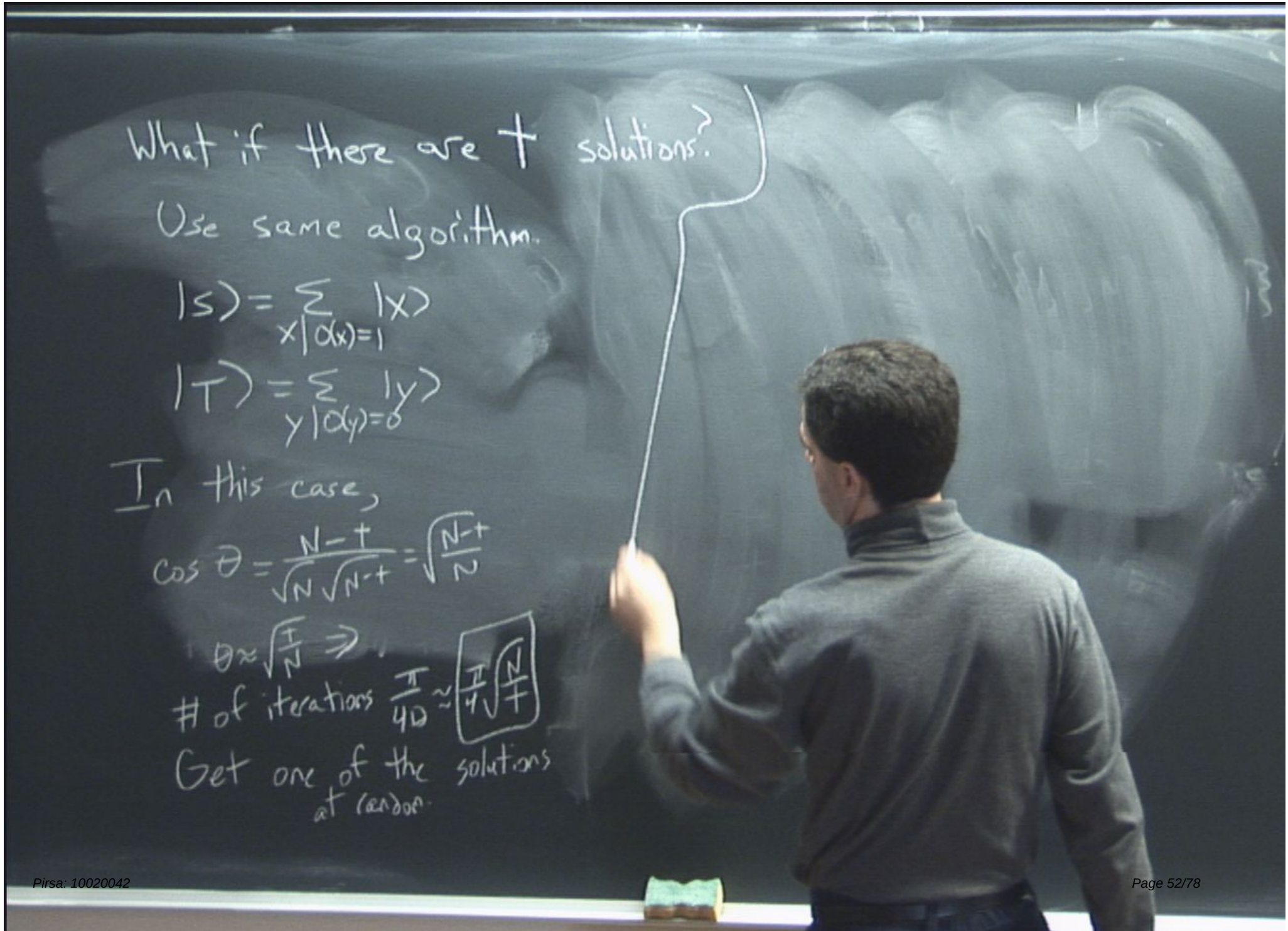
$\phi_k = \theta + 2\theta k = (2k+1)\theta$

Stop when $\phi_k \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi}{4\theta}$

When N is large, $\theta \approx \frac{1}{\sqrt{N}} \Rightarrow$ $k \approx \frac{\pi}{4}\sqrt{N}$

Must stop at right time

or prob (x_0) shrinks


What if there are t solutions?
Use same algorithm.
$|s\rangle = \sum_{x \mid O(x)=1} |x\rangle$
$|T\rangle = \sum_{y \mid O(y)=0} |y\rangle$
In this case,
$\cos\theta = \frac{N-t}{\sqrt{N}\sqrt{N-t}} = \sqrt{\frac{N-t}{N}}$
$\theta \approx \sqrt{\frac{t}{N}} \Rightarrow$
# of iterations $\frac{\pi}{4\theta} \approx \frac{\pi}{4}\sqrt{\frac{N}{t}}$
Get one of the solutions at random.

What if there are t solutions?

Use same algorithm.

$$|s\rangle = \sum_{x|O(x)=1} |x\rangle$$

$$|T\rangle = \sum_{y|O(y)=0} |y\rangle$$

In this case,

$$\cos\theta = \frac{N-t}{\sqrt{N}\sqrt{N-t}} = \sqrt{\frac{N-t}{N}}$$

$$\theta \approx \sqrt{\frac{t}{N}} \Rightarrow$$

# of iterations $\frac{\pi}{4\theta} \approx \boxed{\frac{\pi}{4}\sqrt{\frac{N}{t}}}$

Get one of the solutions at random.

What if we don't know t?

What if there are t solutions?

Use same algorithm.

$$|s\rangle = \sum_{x|f(x)=1} |x\rangle$$

$$|T\rangle = \sum_{y|f(y)=0} |y\rangle$$

In this case,

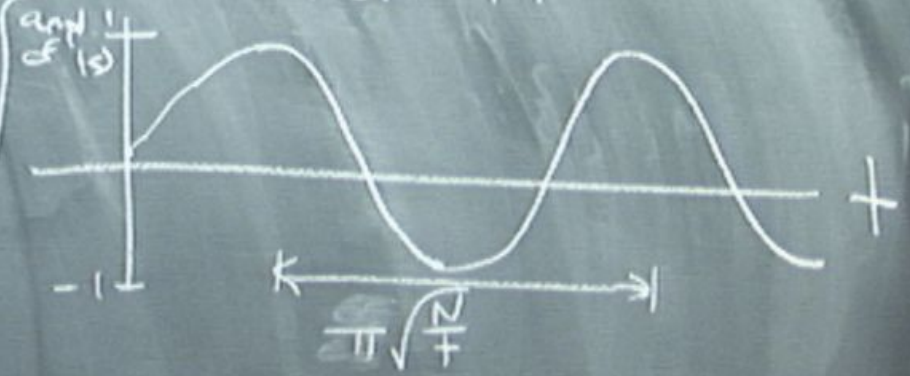
$$\cos\theta = \frac{N-t}{\sqrt{N}\sqrt{N-t}} = \sqrt{\frac{N-t}{N}}$$

$$\theta \approx \sqrt{\frac{t}{N}} \Rightarrow$$

# of iterations $\frac{\pi}{4\theta} \approx \boxed{\frac{\pi}{4}\sqrt{\frac{N}{t}}}$

Get one of the solutions at random.

What if we don't know t?



What if there are t solutions?

Use same algorithm.

$$|s\rangle = \sum_{x|O(x)=1} |x\rangle$$

$$|T\rangle = \sum_{y|O(y)=0} |y\rangle$$

In this case,

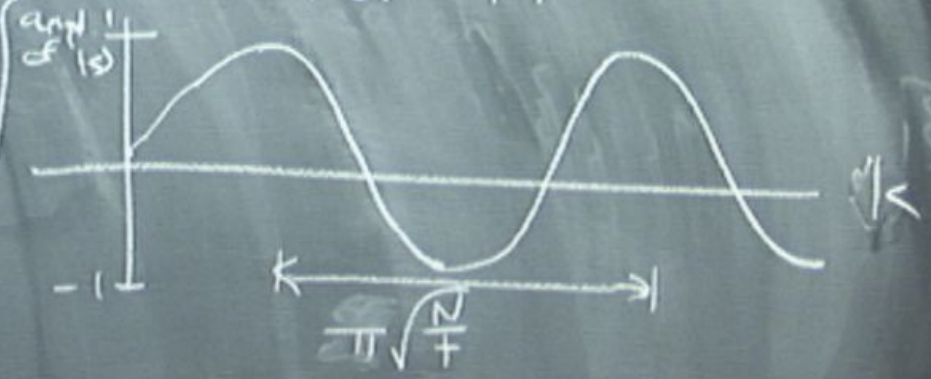
$$\cos\theta = \frac{N-t}{\sqrt{N}\sqrt{N-t}} = \sqrt{\frac{N-t}{N}}$$

$\theta \approx \sqrt{\frac{t}{N}} \Rightarrow$

# of iterations $\frac{\pi}{4\theta} \approx \boxed{\frac{\pi}{4}\sqrt{\frac{N}{t}}}$

Get one of the solutions at random.

What if we don't know t?



Create $\sum_k |k\rangle$, apply k iterations of Grover's algorithm

$\sum_k (|k\rangle \otimes G^k|U\rangle)$ periodic

Apply QFT to first register & get estimate of $\pi\sqrt{\frac{N}{t}}$.

What if there are t solutions?

Use same algorithm.

$$|s\rangle = \sum_{x|O(x)=1} |x\rangle$$

$$|T\rangle = \sum_{y|O(y)=0} |y\rangle$$

In this case,

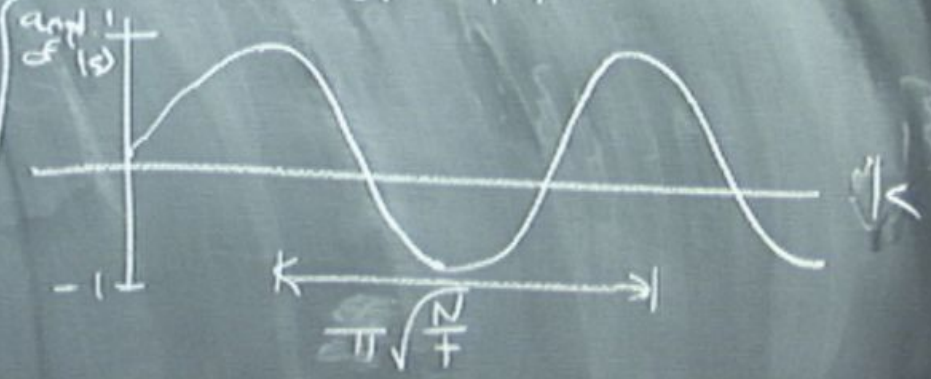
$$\cos\theta = \frac{N-t}{\sqrt{N}\sqrt{N-t}} = \sqrt{\frac{N-t}{N}}$$

$$\theta \approx \sqrt{\frac{t}{N}} \Rightarrow$$

# of iterations $\frac{\pi}{4\theta} \approx \boxed{\frac{\pi}{4}\sqrt{\frac{N}{t}}}$

Get one of the solutions at random.

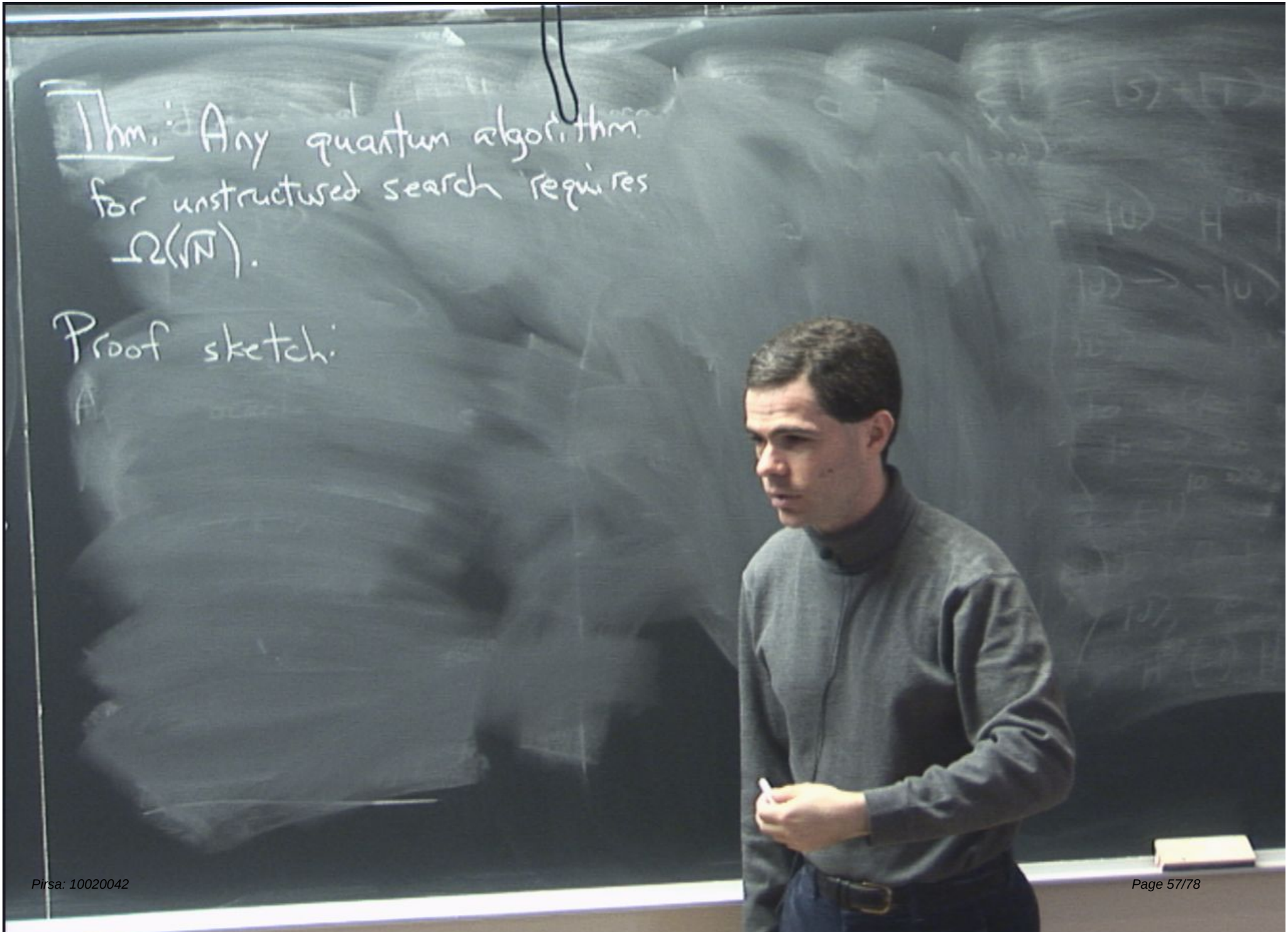
What if we don't know t?

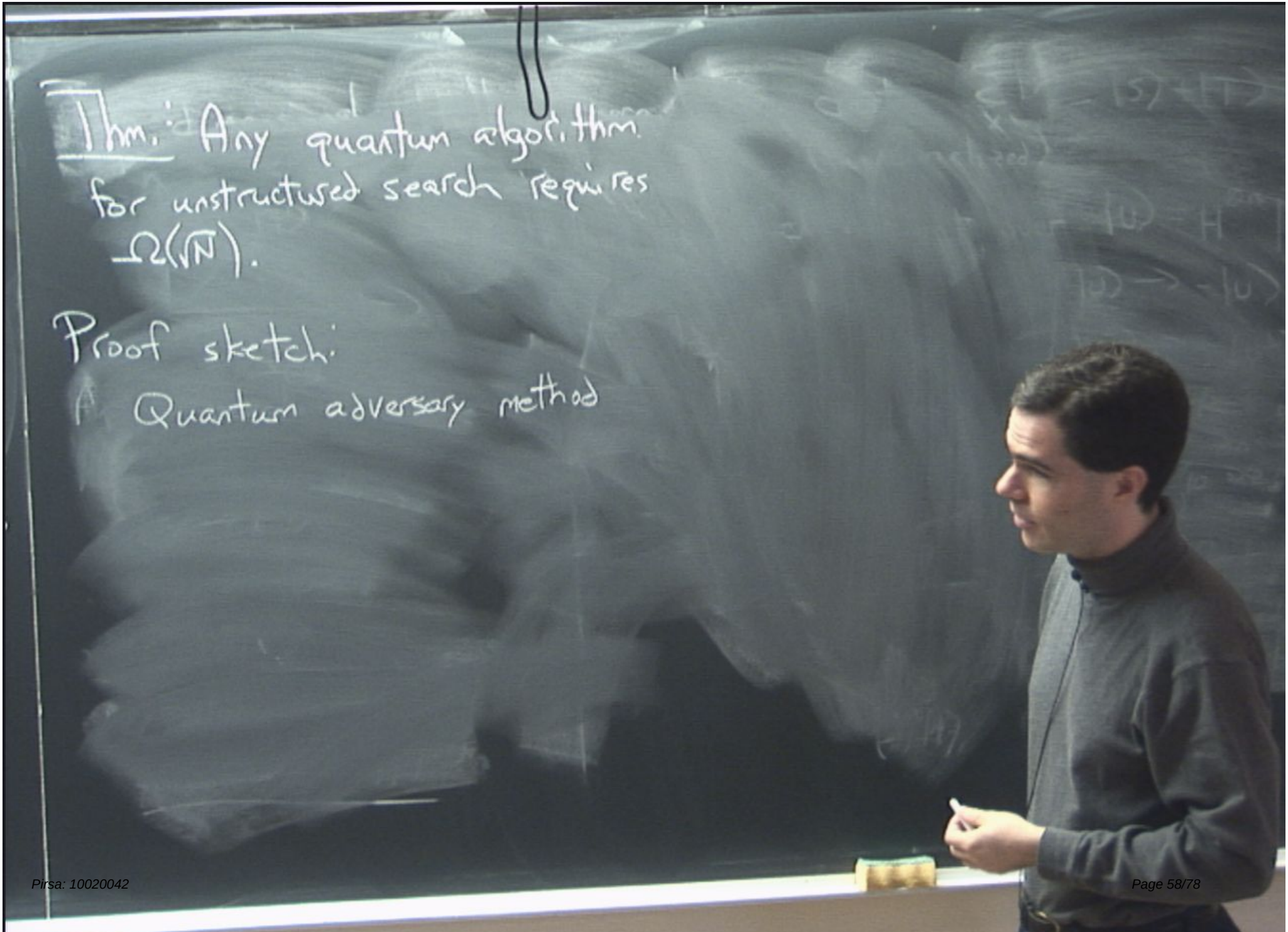


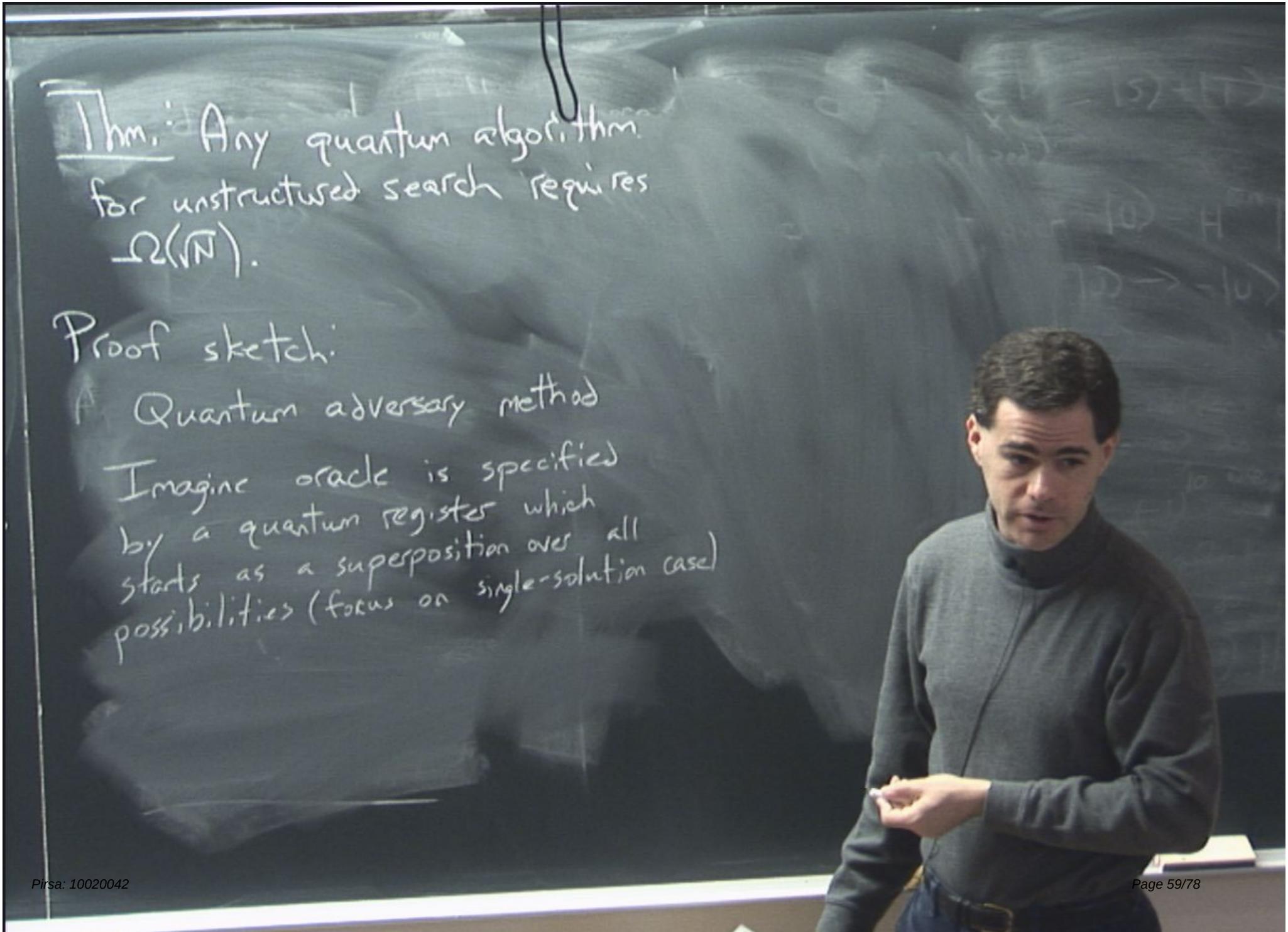
Create $\sum_k |k\rangle$, apply k iterations of Grover's algorithm

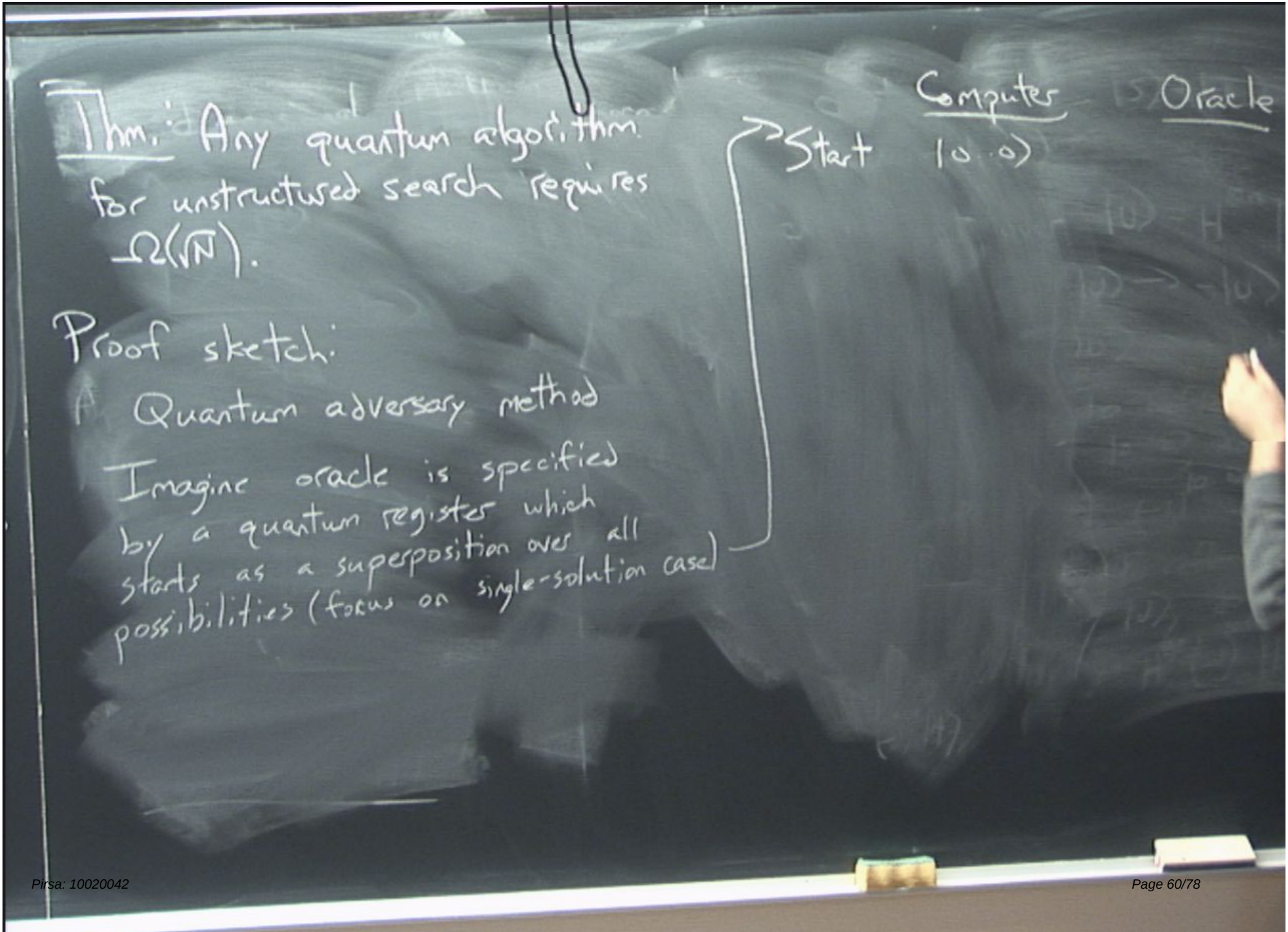
$\sum_k (|k\rangle \otimes G^k|U\rangle)$ periodic

Apply QFT to first register & get estimate of $\pi\sqrt{\frac{N}{t}}$.


Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:


Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Quantum adversary method


Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Quantum adversary method
Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

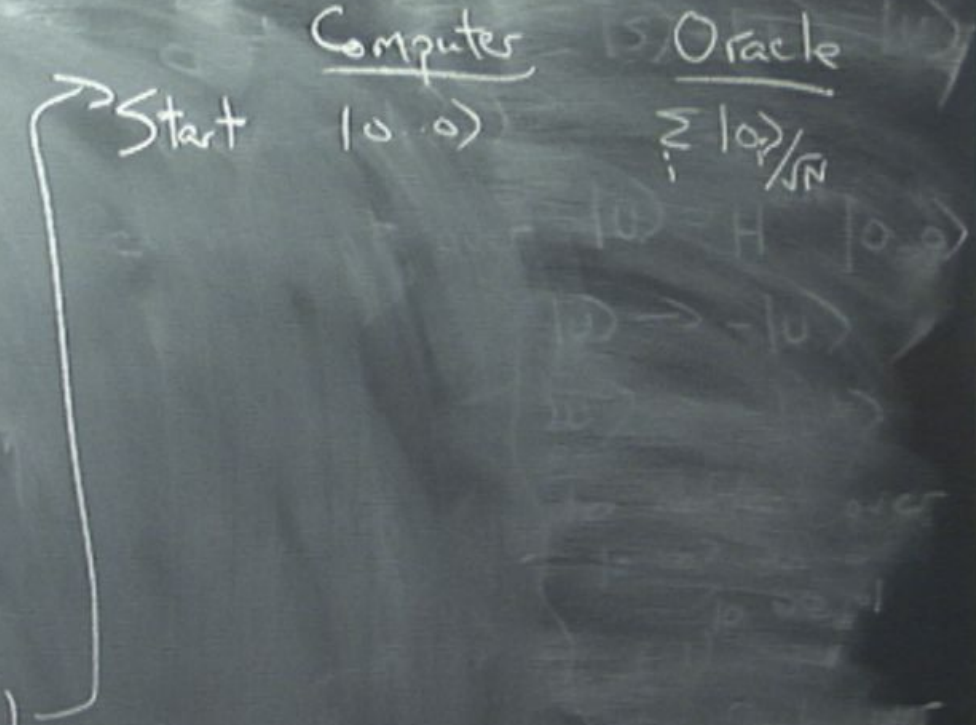

Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Quantum adversary method
Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)
Computer
Oracle
Start
|0 . 0⟩

Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

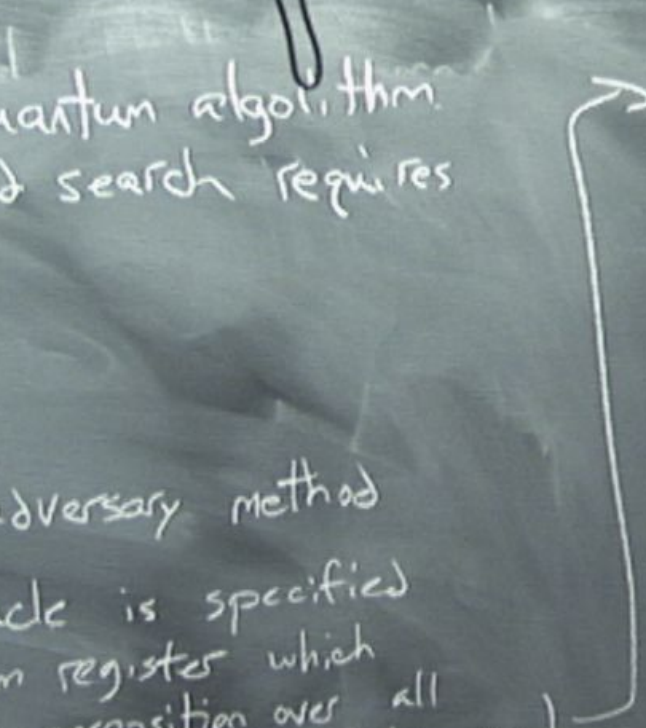


Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)



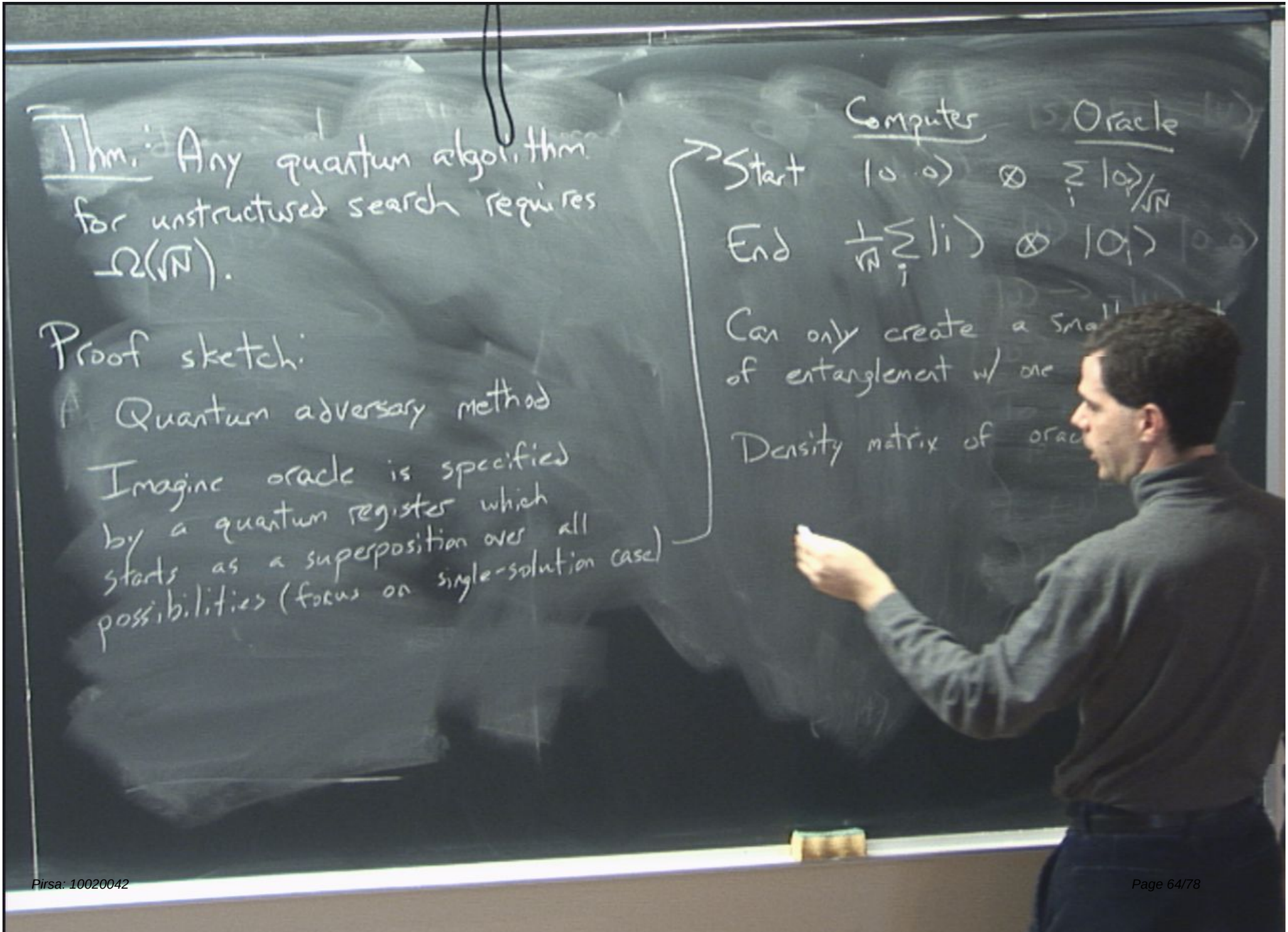
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

	Computer	Oracle
Start	$\|0\ 0\rangle$	$\sum_i \|a_i\rangle/\sqrt{N}$
End	$\frac{1}{\sqrt{N}}\sum_i \|i\rangle \otimes \|0\rangle$	


Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
A Quantum adversary method
Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)
Computer
Oracle
Start $|0\ 0\rangle \otimes \sum_i |a_i\rangle/\sqrt{N}$
End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |a_i\rangle$
Can only create a small
of entanglement w/ one
Density matrix of orac

Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

	Computer	Oracle
Start	$\lvert 0\ 0\rangle$	$\otimes \sum_i \lvert a_i\rangle/\sqrt{N}$
End	$\frac{1}{\sqrt{N}}\sum_i \lvert i\rangle$	$\otimes \lvert a_i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1s)

Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

	Computer	Oracle
Start	$\lvert 0\ 0\rangle$	$\otimes \sum_i \lvert i\rangle/\sqrt{N}$
End	$\frac{1}{\sqrt{N}}\sum_i \lvert i\rangle$	$\otimes \lvert 0\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle

Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1s)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (diagonal)

Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

Computer Oracle

Start $|0\ 0\rangle \otimes \sum_i |a_i\rangle/\sqrt{N}$

End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |a_i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle ρ

Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1s)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (diagonal)

Look at $S = \sum_{k \neq j} |\rho_{kj}|$

Starts at $N-1$

Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

Computer Oracle

Start $|0\ 0\rangle \otimes \sum_i |a_i\rangle/\sqrt{N}$

End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |a_i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle ρ

Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1s)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (diagonal)

Look at $S = \sum_{k \neq j} |\rho_{kj}|$

Starts at $N-1$, ends at $\sqrt{\varepsilon(1-\varepsilon)}$

Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

Computer ⊗ Oracle

Start $|0\ 0\rangle \otimes \sum_i |a_i\rangle/\sqrt{N}$

End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |a_i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle ρ

Starts as $\frac{1}{N}\begin{pmatrix} 1 & 1 & \cdots \\ 1 & 1 & \\ \vdots & & \ddots \end{pmatrix}$ (all 1's)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & 0 & \\ 0 & 1 & \\ & & \ddots \end{pmatrix}$ (diagonal)

Look at $S = \sum_{k \neq j} |\rho_{kj}|$

Starts at $N-1$, ends at $\sqrt{\varepsilon(1-\varepsilon)}(\quad) + O(\varepsilon N)$

Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

	Computer	Oracle
Start	$\|0\ 0\rangle \otimes \sum_i \|i\rangle/\sqrt{N}$	
End	$\frac{1}{\sqrt{N}}\sum_i \|i\rangle \otimes \|0\rangle$	

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle ρ

Starts as $\frac{1}{N}\begin{pmatrix} 1 & 1 & \cdots \\ 1 & 1 & \\ \vdots & & \ddots \end{pmatrix}$ (all 1s)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & 0 & \\ 0 & 1 & \\ & & \ddots \end{pmatrix}$ (diagonal)

Look at $S = \sum_{k \neq j} |\rho_{kj}|$

Starts at $N-1$, ends at $\sqrt{\varepsilon(1-\varepsilon)}(N-1) + O(\varepsilon N)$

Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

Lemma: Under 1 query, $|S(t+1) - S(t)| \leq 2\sqrt{N-1}$

Computer ⊗ Oracle

Start $|0\,0\rangle \otimes \sum_i |a_i\rangle/\sqrt{N}$

End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |a_i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

Density matrix of oracle ρ

Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1's)

Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (diagonal)

Look at $S = \sum_{k \neq j} |\rho_{kj}|$

Starts at $N-1$, ends at $\sqrt{\varepsilon(1-\varepsilon)}(N-1) + O(\varepsilon N)$

Thm.: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.

Proof sketch:

A Quantum adversary method

Imagine oracle is specified by a quantum register which starts as a superposition over all possibilities (focus on single-solution case)

Lemma: Under 1 query, $|S(t+1) - S(t)| \leq 2\sqrt{N-1}$

$\Rightarrow$ Need $\Omega(\sqrt{N})$ steps.

Computer Oracle

Start $|0\ 0\rangle \otimes \sum_i |i\rangle/\sqrt{N}$

End $\frac{1}{\sqrt{N}} \sum_i |i\rangle \otimes |i\rangle$

Can only create a small amount of entanglement w/ one oracle call.

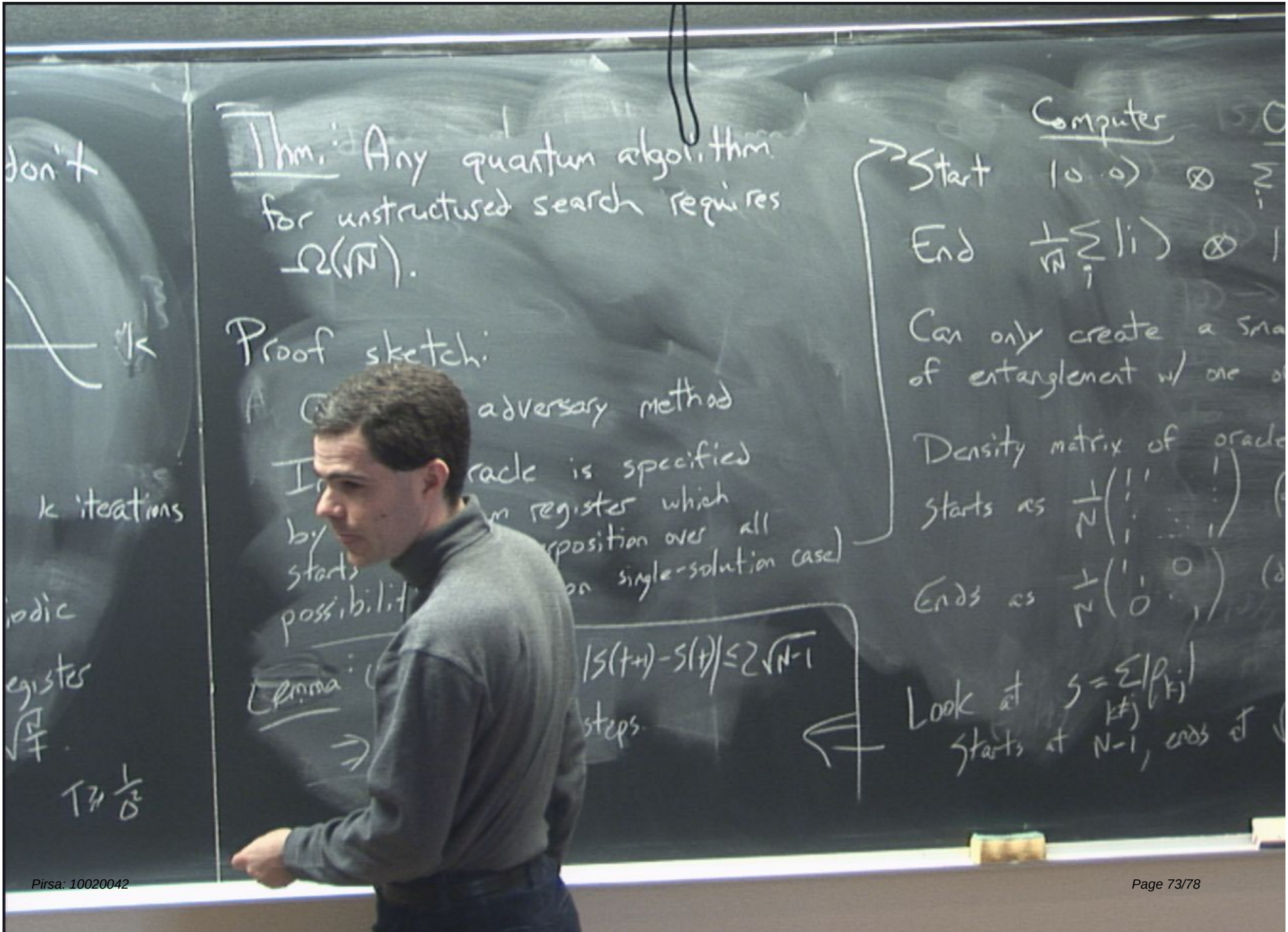
Density matrix of oracle ρ

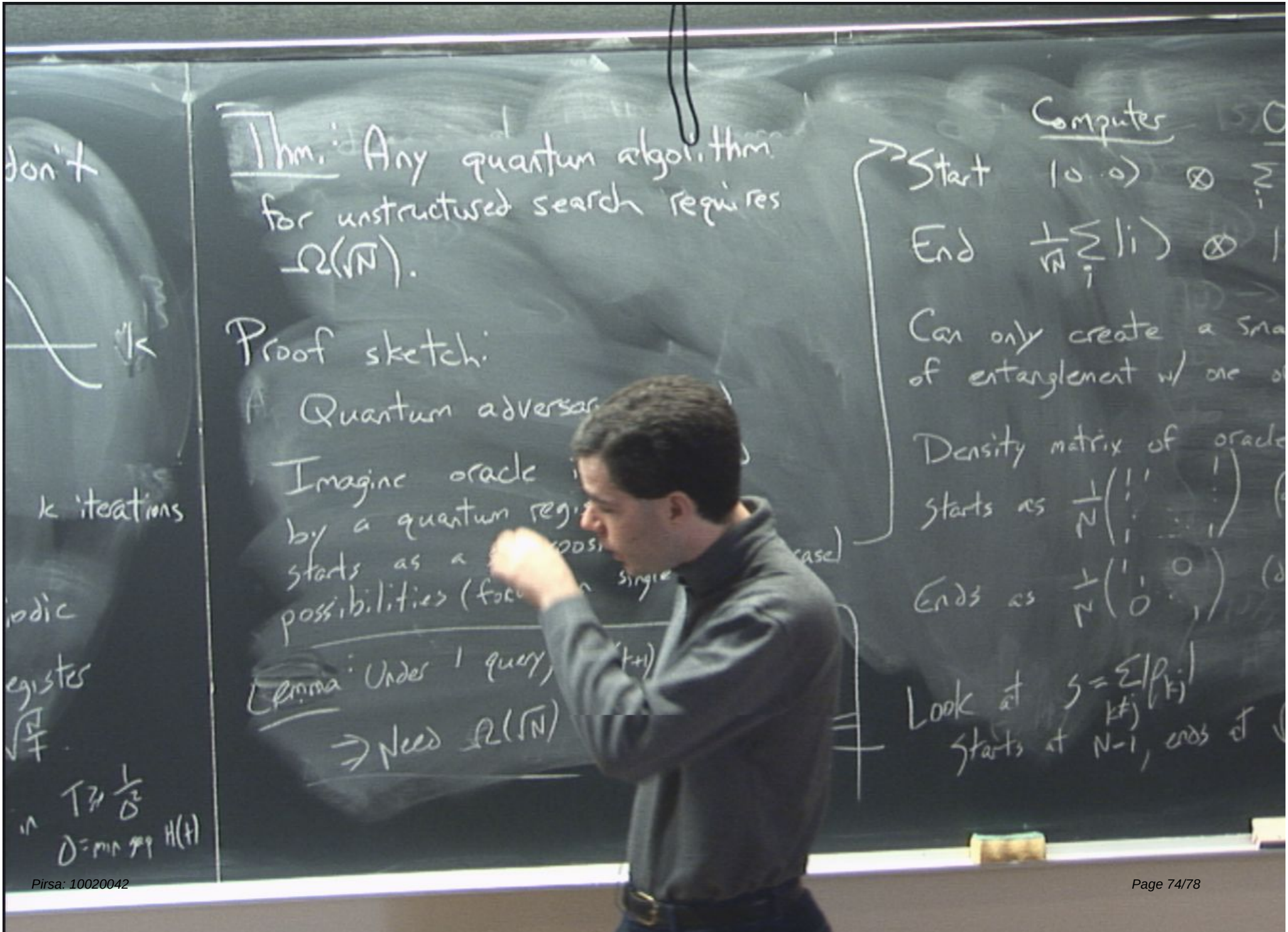
Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ (all 1s)

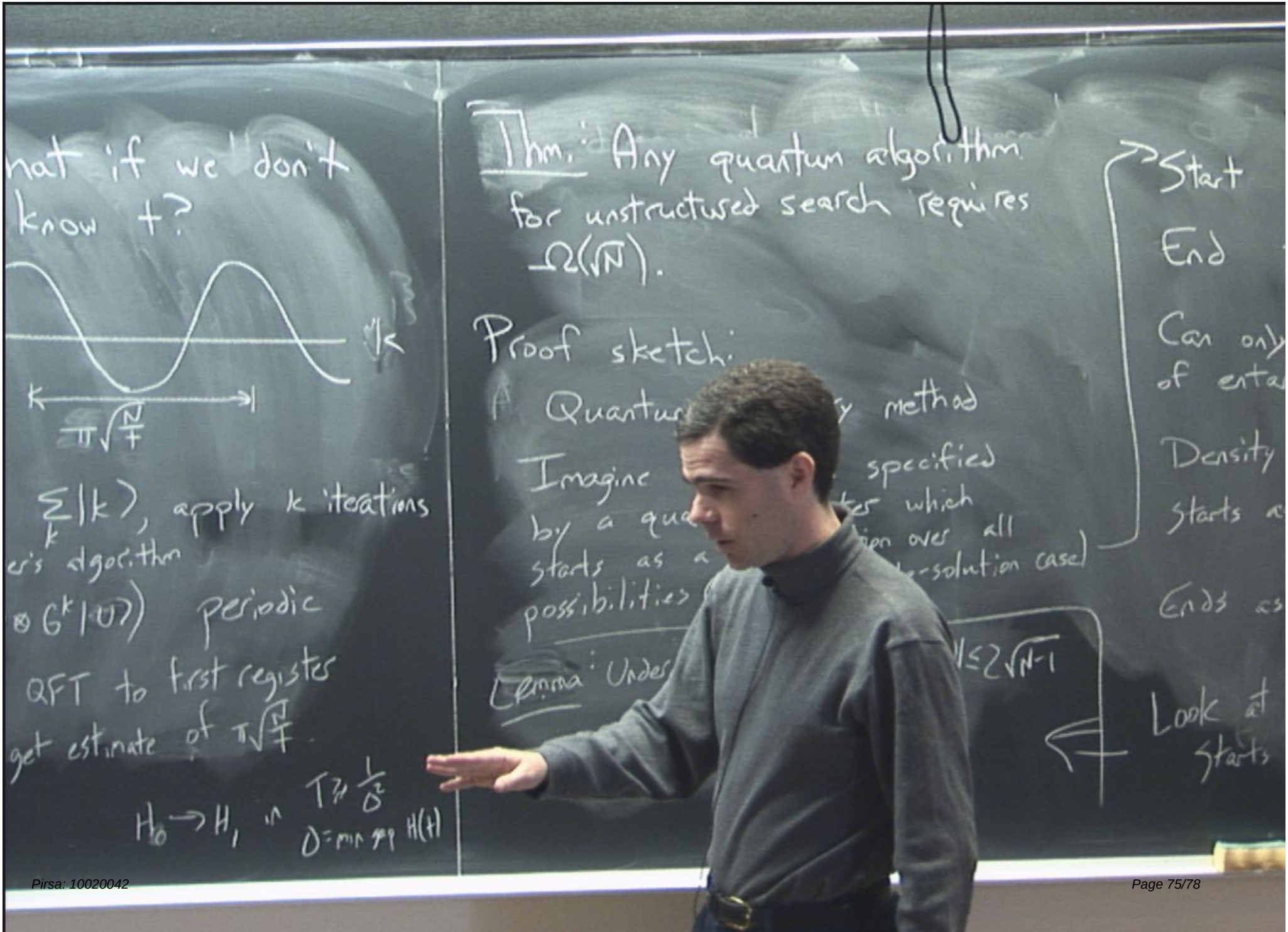
Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ (diagonal)

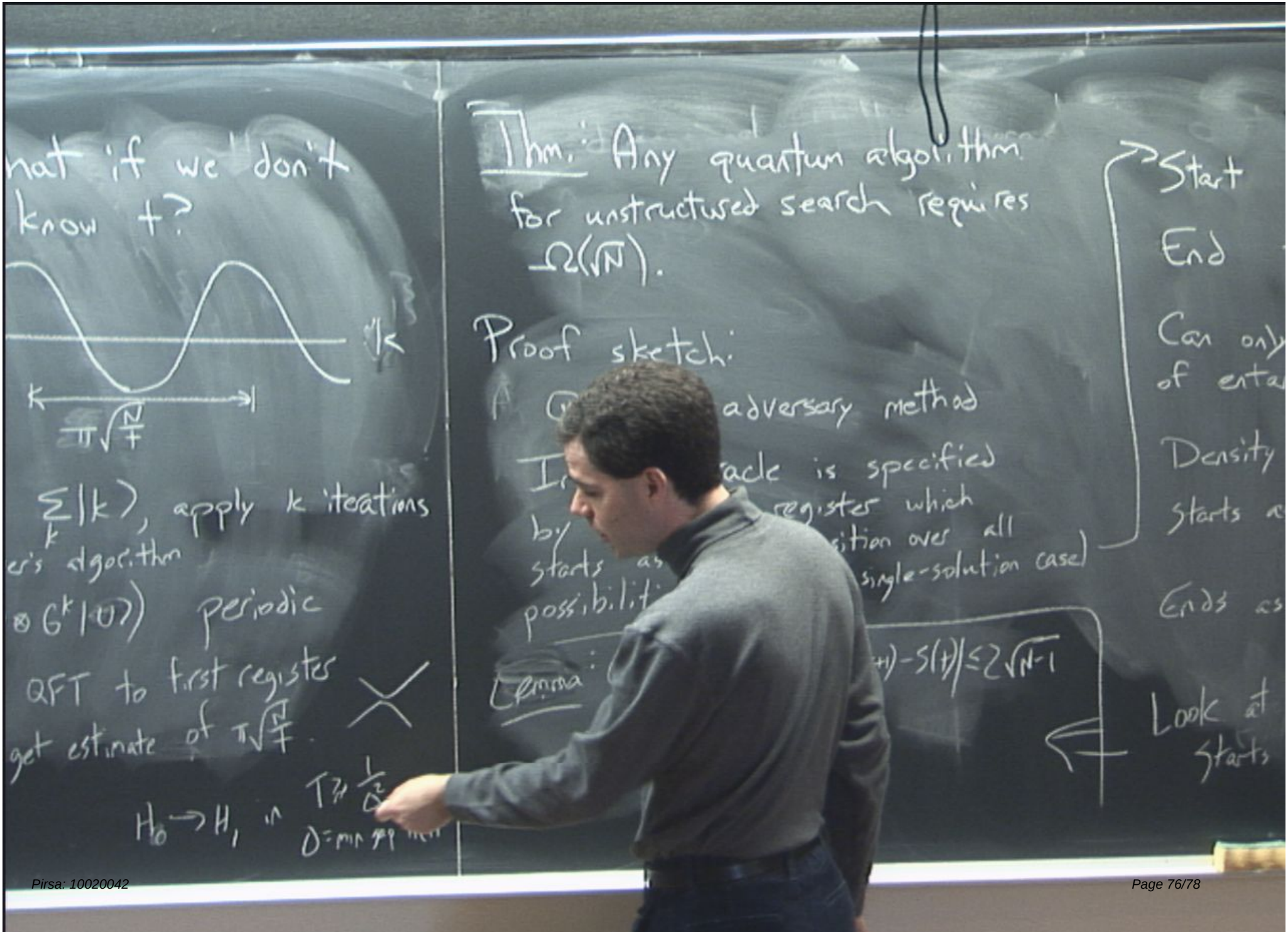
Look at $S = \sum_{k \neq j} |\rho_{kj}|$

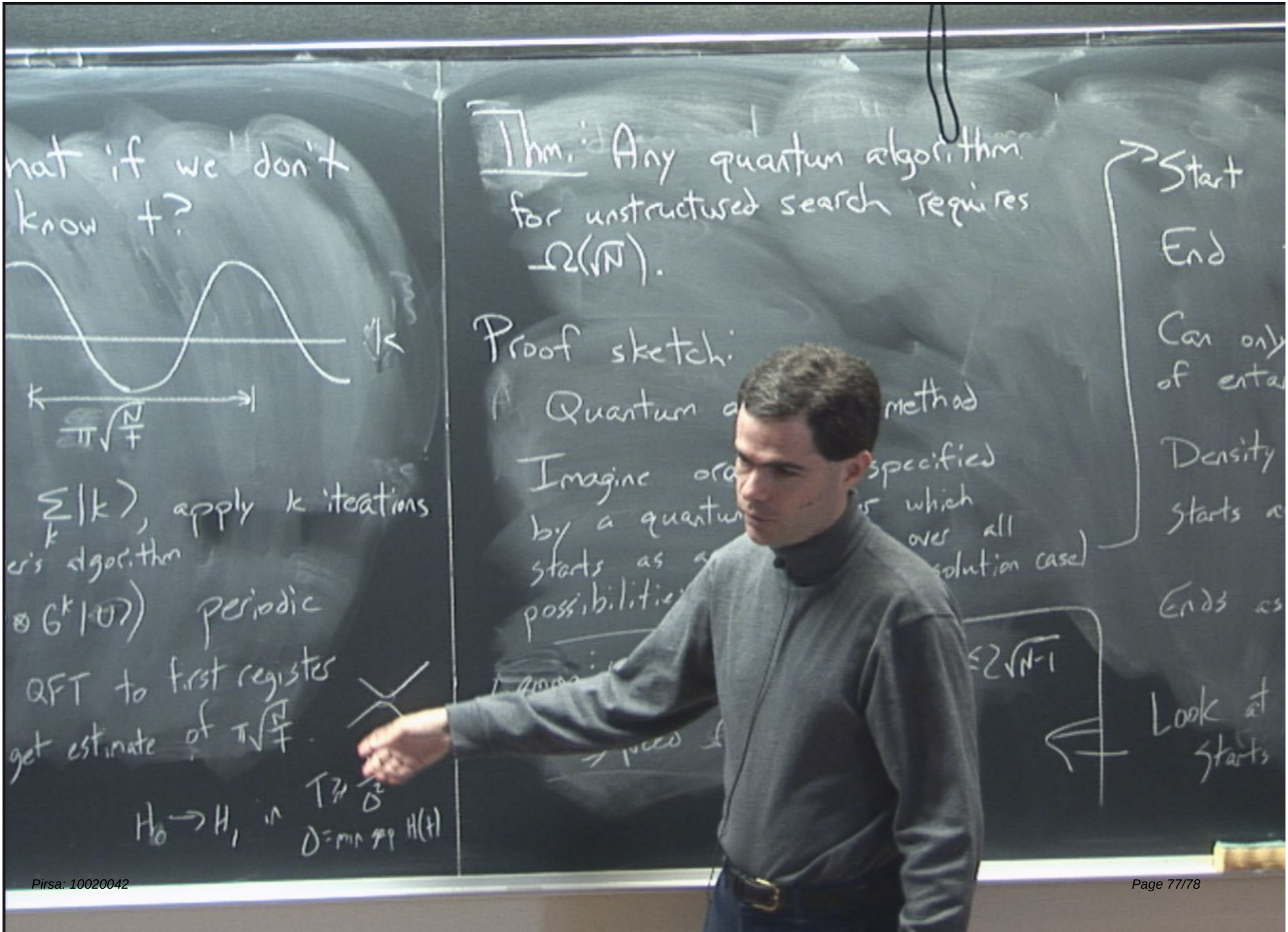
Starts at $N-1$, ends at $\sqrt{\varepsilon(1-\varepsilon)}(N-1) + O(\varepsilon N)$

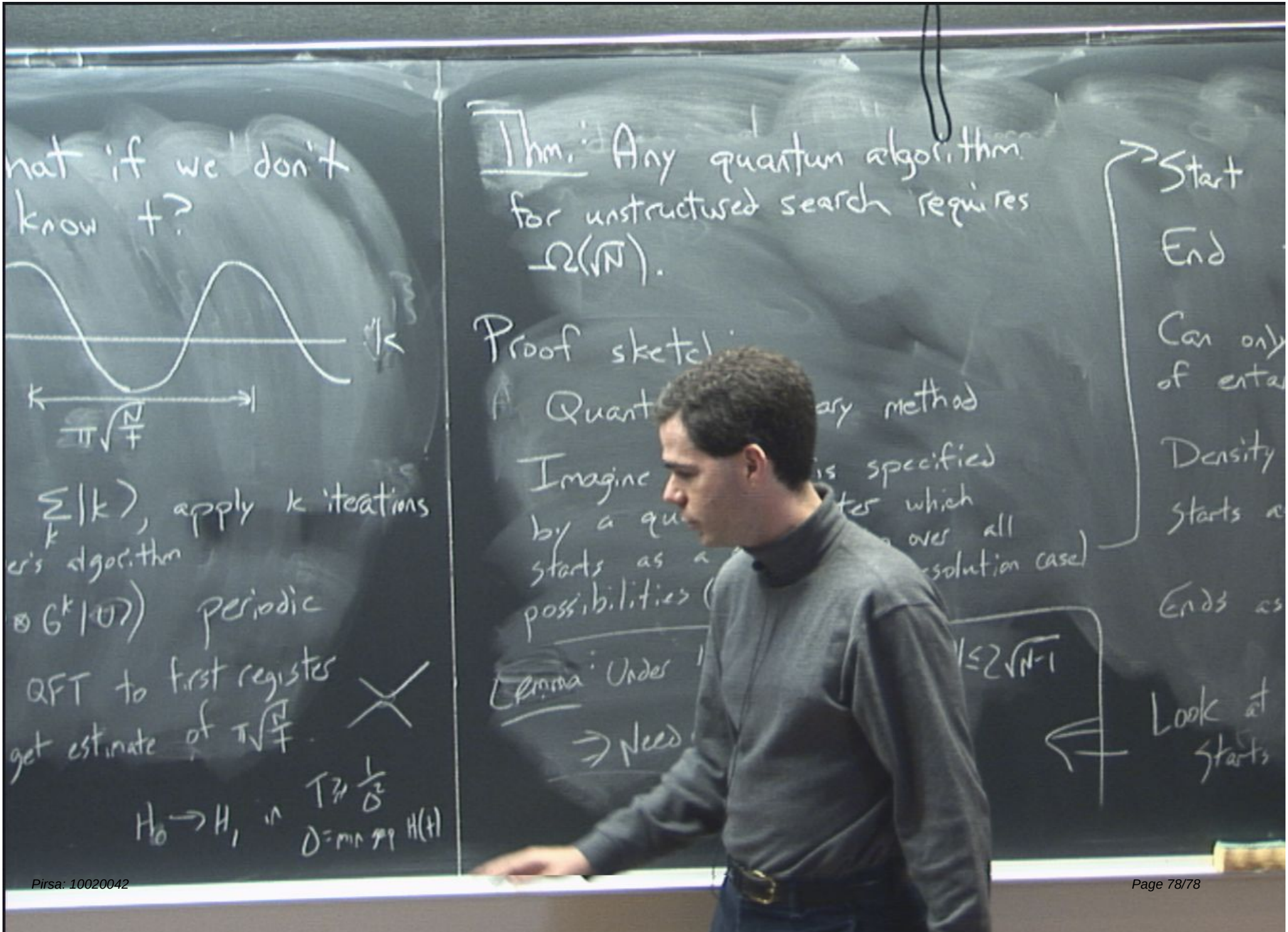

don't
k iterations
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
adversary method
Lemma:
steps.
Computer
Start $|0\ldots0\rangle \otimes \frac{1}{\sqrt{N}}\sum_i |i\rangle$
End $\frac{1}{\sqrt{N}}\sum_i |i\rangle \otimes$
Can only create a sma
of entanglement w/ one
Density matrix of oracle
Starts as $\frac{1}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$
Ends as $\frac{1}{N}\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$
Look at $S = \sum_{k \neq j} |\rho_{kj}|$
starts at N-1, ends at


don't
k iterations
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Quantum adversar
Imagine oracle
by a quantum reg
starts as a
possibilities (foc
Lemma: Under 1 query,
⇒ Need $\Omega(\sqrt{N})$
Computer
Start $|0\ldots0\rangle \otimes \frac{1}{\sqrt{N}}\sum_i |i\rangle$
End $\frac{1}{\sqrt{N}}\sum_i |i\rangle \otimes$
Can only create a sma
of entanglement w/ one
Density matrix of oracle
starts as $\frac{1}{N}\begin{pmatrix}1 & \cdots & 1\\ \vdots & & \vdots\\ 1 & \cdots & 1\end{pmatrix}$
Ends as $\frac{1}{N}\begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$
Look at $S = \sum_{k\neq j} |\rho_{kj}|$
starts at N-1, ends of


hat if we don't know t?
$\pi\sqrt{\frac{N}{t}}$
$\sum_k |k\rangle$, apply k iterations
er's algorithm
periodic
QFT to first register
get estimate of $\pi\sqrt{\frac{N}{t}}$
$H_0 \to H_1$ in $T \geq \frac{1}{\delta^2}$
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Quantum
method
Imagine
specified
by a qua
which
starts as a
over all
possibilities
-solution case)
Lemma: Under
$\leq 2\sqrt{N-1}$
Start
End
Can only
of entan
Density
starts a
Ends as
Look at
starts


hat if we don't know t?
$\pi\sqrt{\frac{N}{t}}$
$\sum_k |k\rangle$, apply k iterations
er's algorithm
periodic
QFT to first register
get estimate of $\pi\sqrt{\frac{N}{t}}$
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
adversary method
Lemma:
$|S(t+1) - S(t)| \leq 2\sqrt{N-1}$
Start
End
Density
Ends as
Look at
starts


hat if we don't know t?
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch:
Start
End
Can only
of entan
Density
starts a
Ends as
Look at
starts
$\pi\sqrt{\frac{N}{t}}$
$\sum_k |k\rangle$, apply k iterations
er's algorithm
$G^k|\psi\rangle$ periodic
QFT to first register
get estimate of $\pi\sqrt{\frac{N}{t}}$.
$H_0 \to H_1$ in $T \geq \frac{1}{\delta^2}$
$\delta = \min_t$ gap $H(t)$
$\leq 2\sqrt{N-1}$


hat if we don't know t?
$\pi\sqrt{\frac{N}{t}}$
$\sum_k |k\rangle$, apply k iterations
er's algorithm
periodic
QFT to first register
get estimate of $\pi\sqrt{\frac{N}{t}}$
$H_0 \to H_1$
Thm: Any quantum algorithm for unstructured search requires $\Omega(\sqrt{N})$.
Proof sketch
Quant
ary method
Imagine
is specified
by a qu
ter which
starts as a
over all
possibilities (
solution case)
Lemma: Under
$\leq 2\sqrt{N-1}$
Need
Start
End
Can only
of entan
Density
starts a
Ends as
Look at
starts