Title: Quantum Information Theory #4

Date: Mar 20, 2008 06:30 PM

URL: http://pirsa.org/08030009

Abstract: Teleportation, quantum key distribution, and quantum algorithms.

Swipe your finger slower

The image was not accepted. Place the same finger on the fingerprint sensor again.

Quantum Information
Lecture 4: Quantum Computing

Sarah Croke

Perimeter Institute (Office: 252)

scroke@perimeterinstitute.ca

Quantum Information
Lecture 4: Quantum Computing

Sarah Croke
Perimeter Institute (Office: 252)
scroke@perimeterinstitute.ca

Grover's Algorithm

- Search algorithm;
  - Problem is to search for one marked item in an unstructured database of N items.
  - Assume it is easy to recognize the solution, but difficult to find it.
- Classically, need O(N) queries to find item with probability p.
- Same problem solved by a quantum computer in $O(\sqrt{N})$ queries.
- Algorithm is probabilistic.

Quantum Information
Lecture 4: Quantum Computing

Sarah Croke

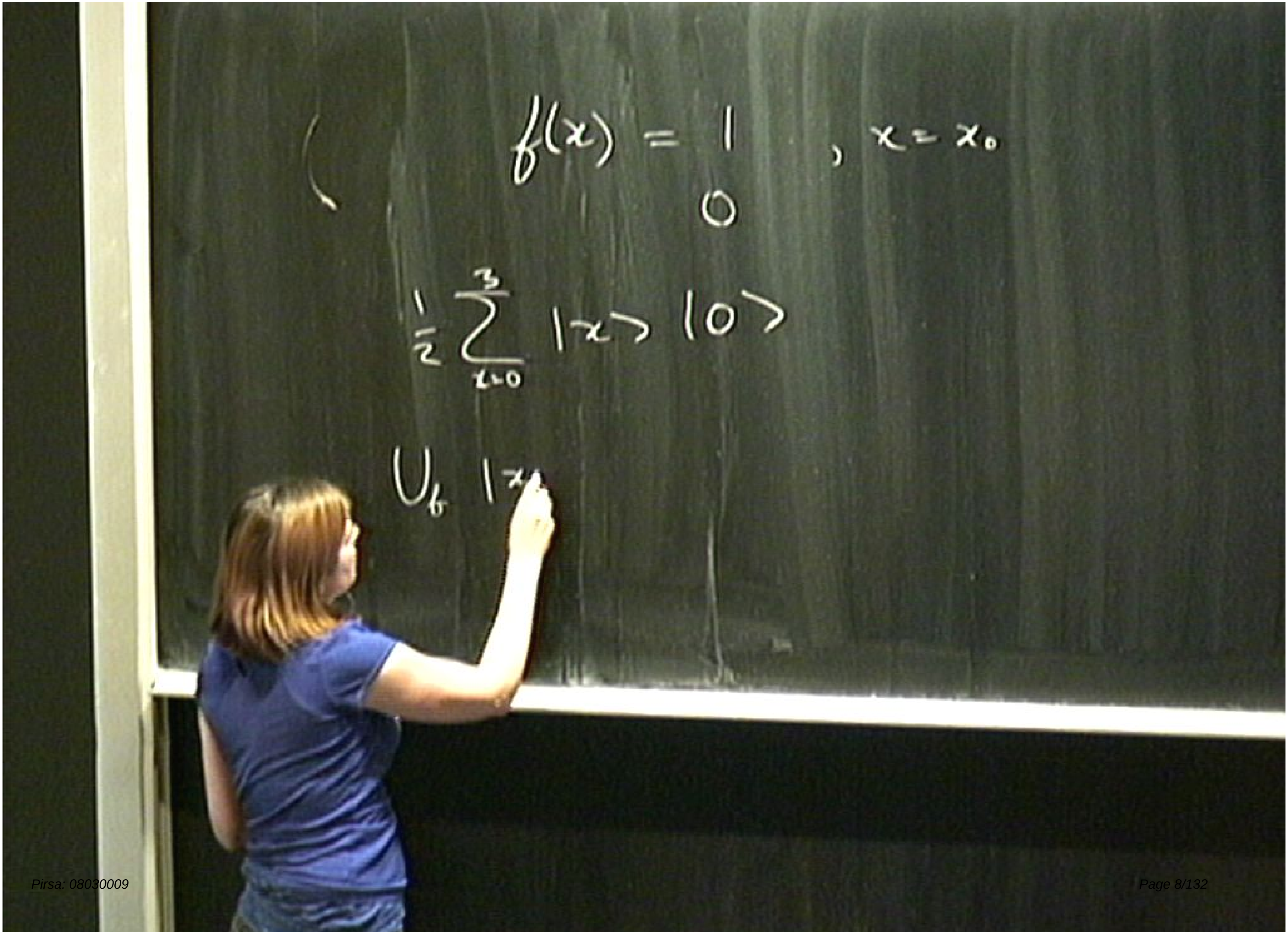
Perimeter Institute (Office: 252)

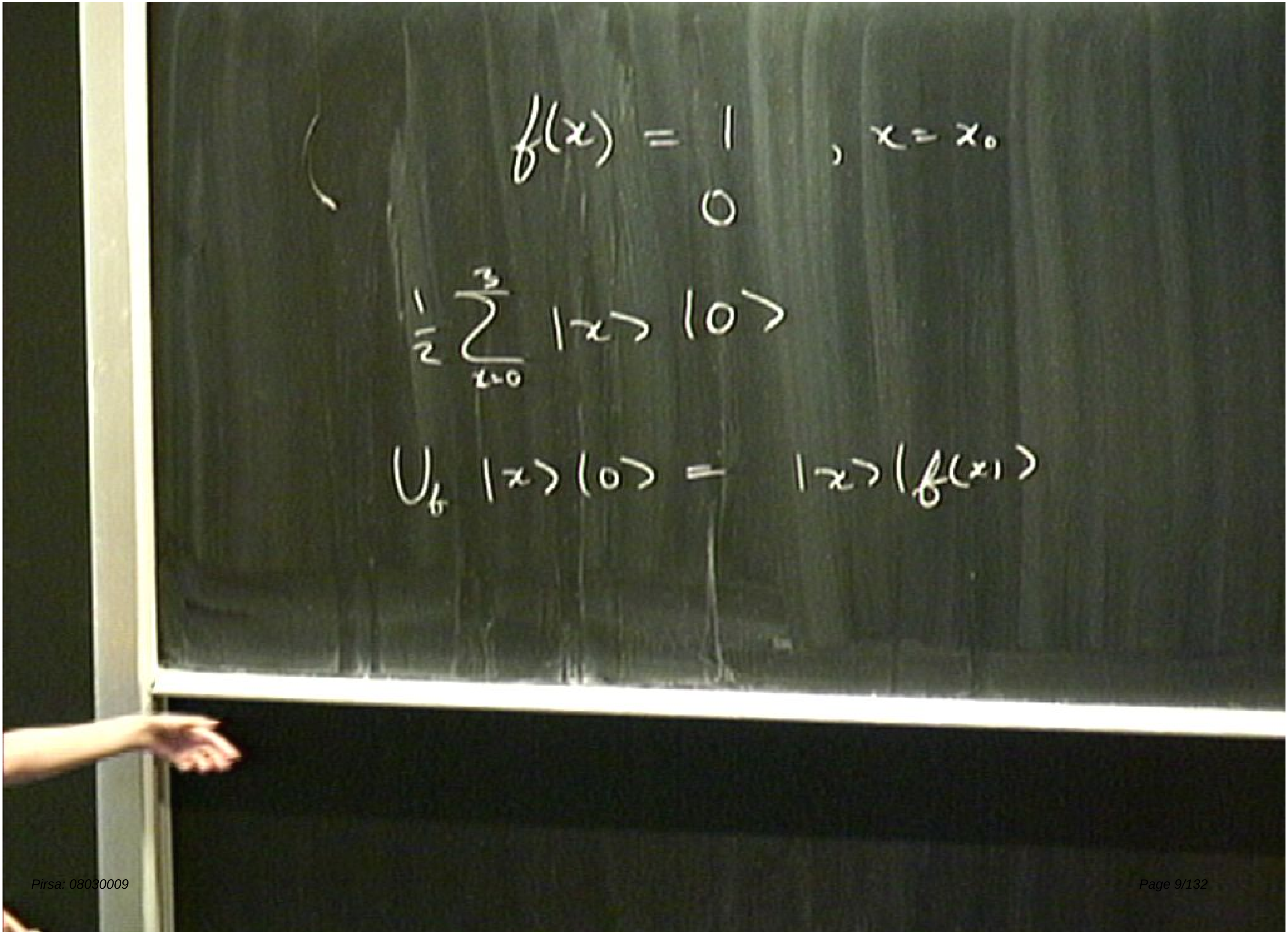
scroke@perimeterinstitute.ca

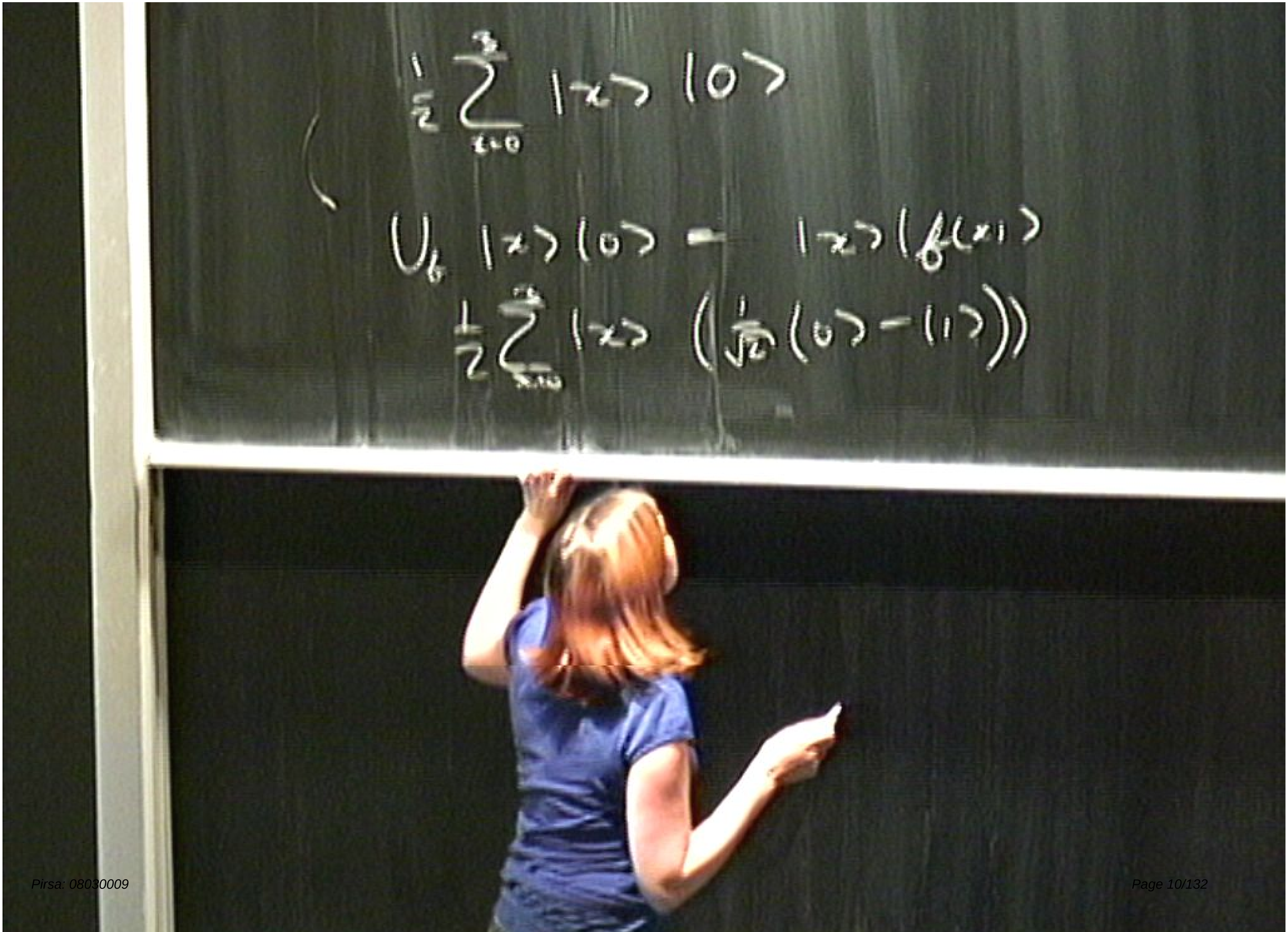
Grover's Algorithm

- Search algorithm;
  - Problem is to search for one marked item in an unstructured database of N items.
  - Assume it is easy to recognize the solution, but difficult to find it.
- Classically, need O(N) queries to find item with probability p.
- Same problem solved by a quantum computer in $O(\sqrt{N})$ queries.
- Algorithm is probabilistic.

$$f(x) = 1 \quad , \quad x = x_0$$


f(x) = 1 , x = x₀
0
½ Σ_{x=0}^{3} |x> |0>
U_f |x


$f(x) = 1 \;,\; x = x_0$
0
$\frac{1}{2}\sum_{x=0}^{3} |x\rangle |0\rangle$
$U_f |x\rangle|0\rangle = |x\rangle|f(x)\rangle$


½ Σ_{x=0}^{3} |x⟩ |0⟩
U_f |x⟩|0⟩ = |x⟩|f(x)⟩
½ Σ_{x=0}^{3} |x⟩ (1/√2 (|0⟩ − |1⟩))

$$f(x) = \begin{cases} 1, & x = x_0 \\ 0 & \end{cases}$$

$$\frac{1}{2}\sum_{x=0}^{3} |x\rangle |0\rangle$$

$$U_f\, |x\rangle |0\rangle = |x\rangle |f(x)\rangle$$

$$\frac{1}{2}\sum_{x=0}^{3} |x\rangle \left(\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right)$$

$$f(x) = \begin{cases} 1, & x = x_0 \\ 0 & \end{cases}$$

$$\frac{1}{2}\sum_{x=0}^{3} |x\rangle |0\rangle$$

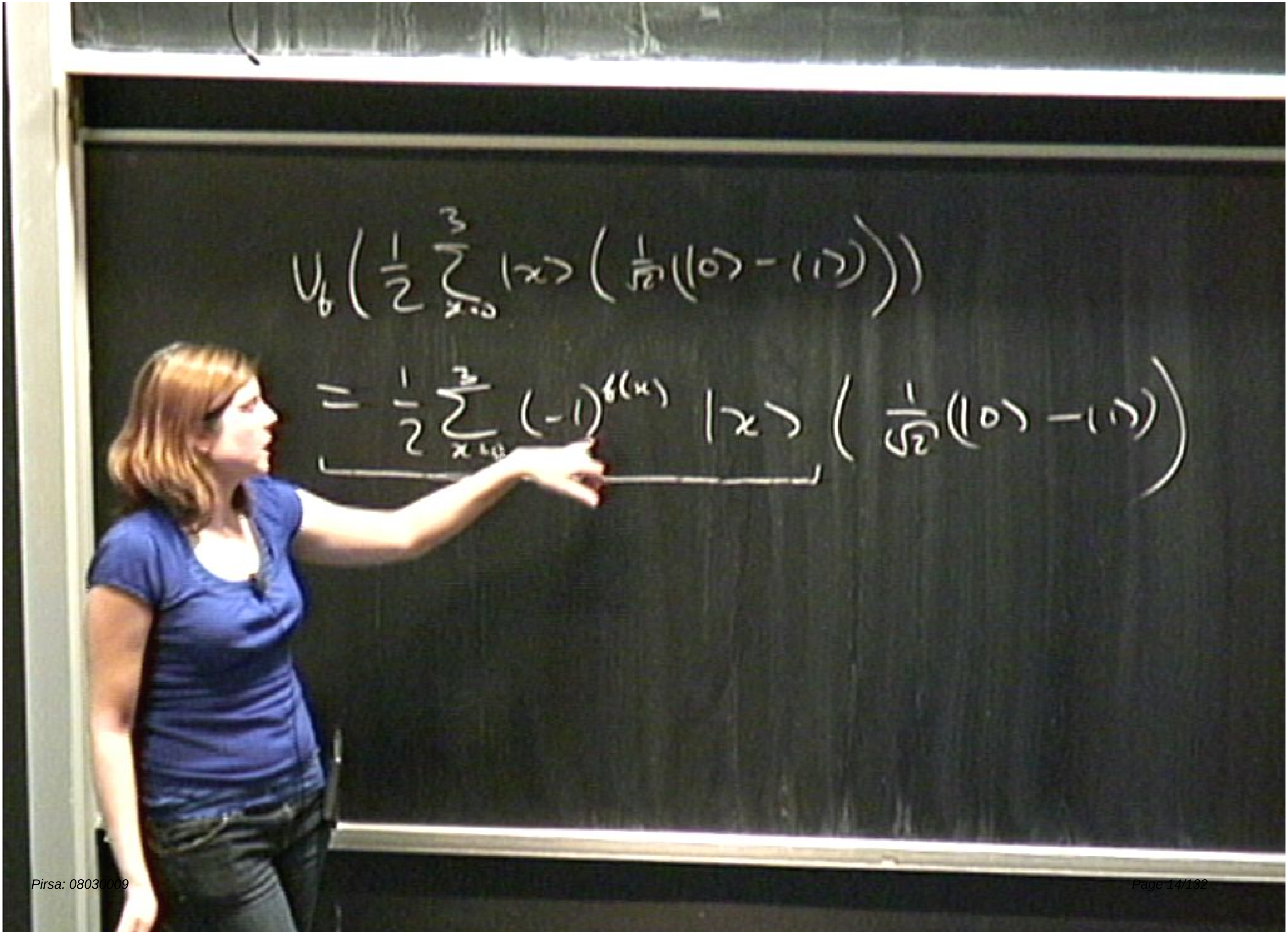
$$U_f |x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

$$\frac{1}{2}\sum_{x=0}^{3} |x\rangle \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$$

$$U_f\left(\frac{1}{2}\sum_{x=0}^{3} |x\rangle \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)\right)$$

$$U_f\left(\frac{1}{2}\sum_{x=0}^{3}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)\right)$$

$$=\frac{1}{2}\sum_{x=0}^{3}(-1)^{f(x)}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)$$

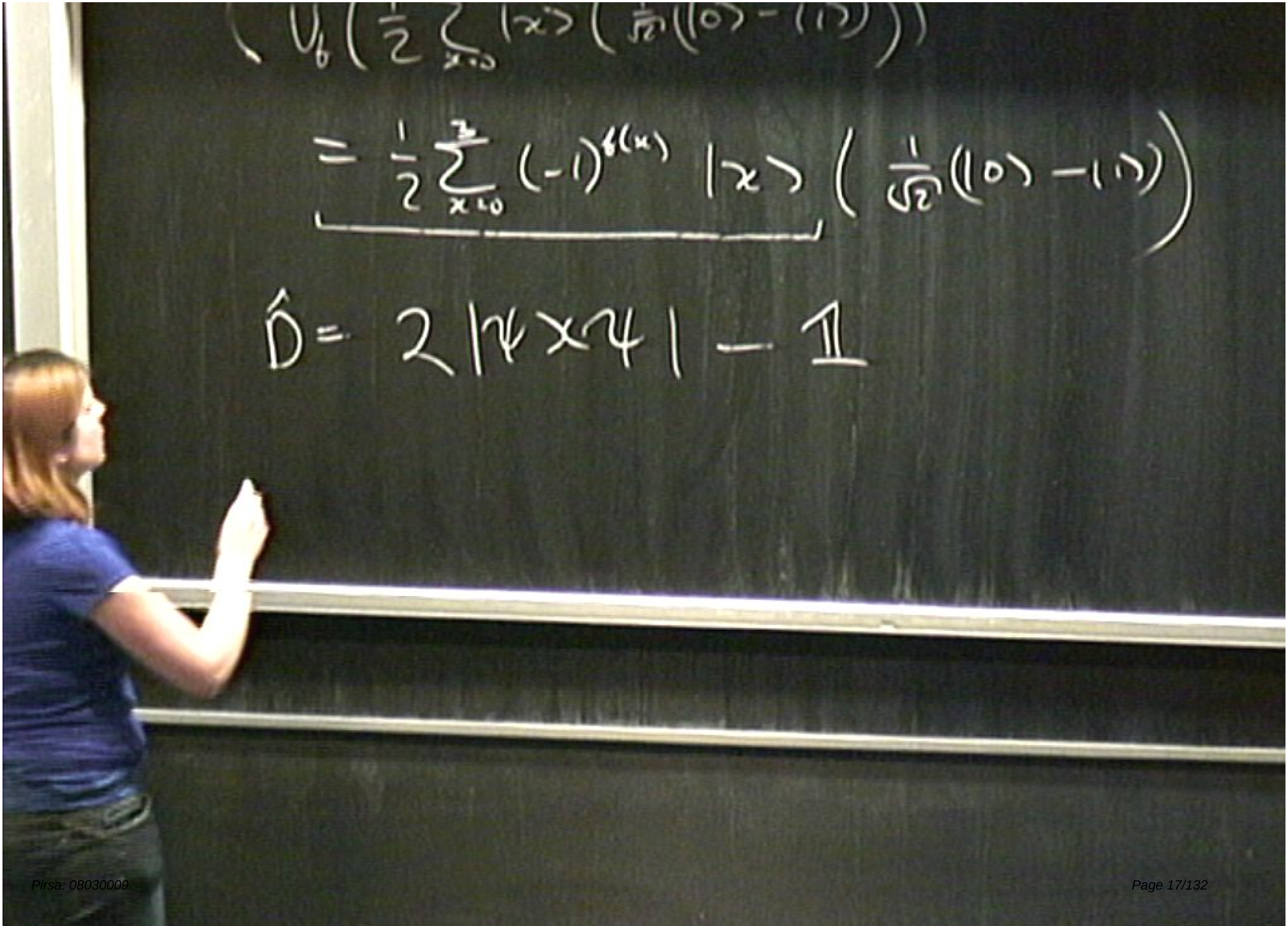

$U_f \left(\frac{1}{2} \sum_{x=0}^{3} |x\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \right)$
$= \frac{1}{2} \sum_{x=0}^{3} (-1)^{f(x)} |x\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$

$$U_f\left(\frac{1}{2}\sum_{x=0}^{3}|x\rangle\left(\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right)\right)$$

$$=\underbrace{\frac{1}{2}\sum_{x=0}^{3}(-1)^{f(x)}\,|x\rangle}\left(\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right)$$

$$U_f\left(\frac{1}{2}\sum_{x=0}^{3}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)\right)$$

$$=\underbrace{\frac{1}{2}\sum_{x=0}^{3}(-1)^{f(x)}|x\rangle}\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)$$

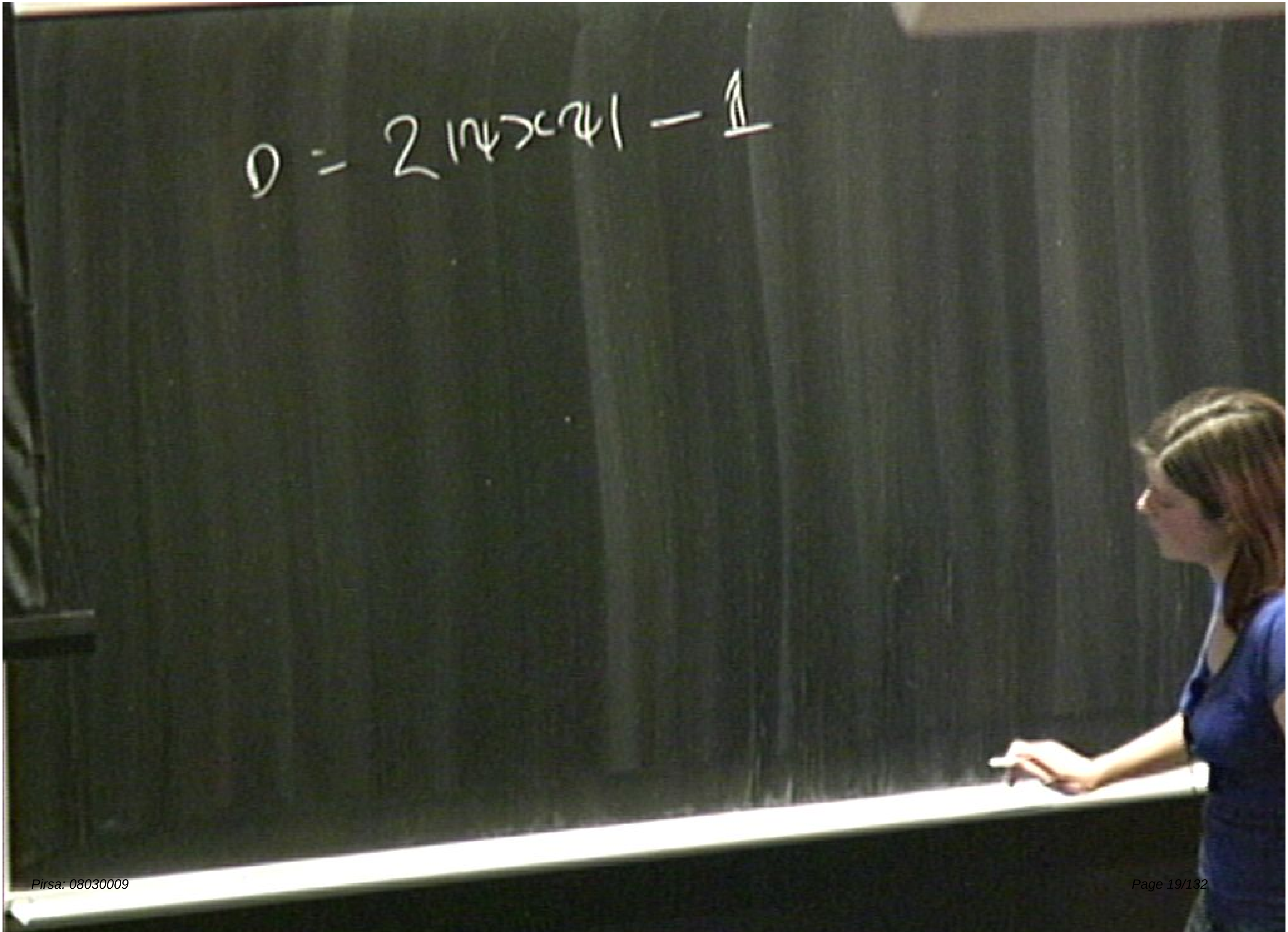

$U_f\left(\frac{1}{2}\sum_{x=0}^{3}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)\right)$
$= \frac{1}{2}\sum_{x=0}^{3}(-1)^{f(x)}|x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)$
$\hat{D} = 2|\psi\rangle\langle\psi| - \mathbb{1}$

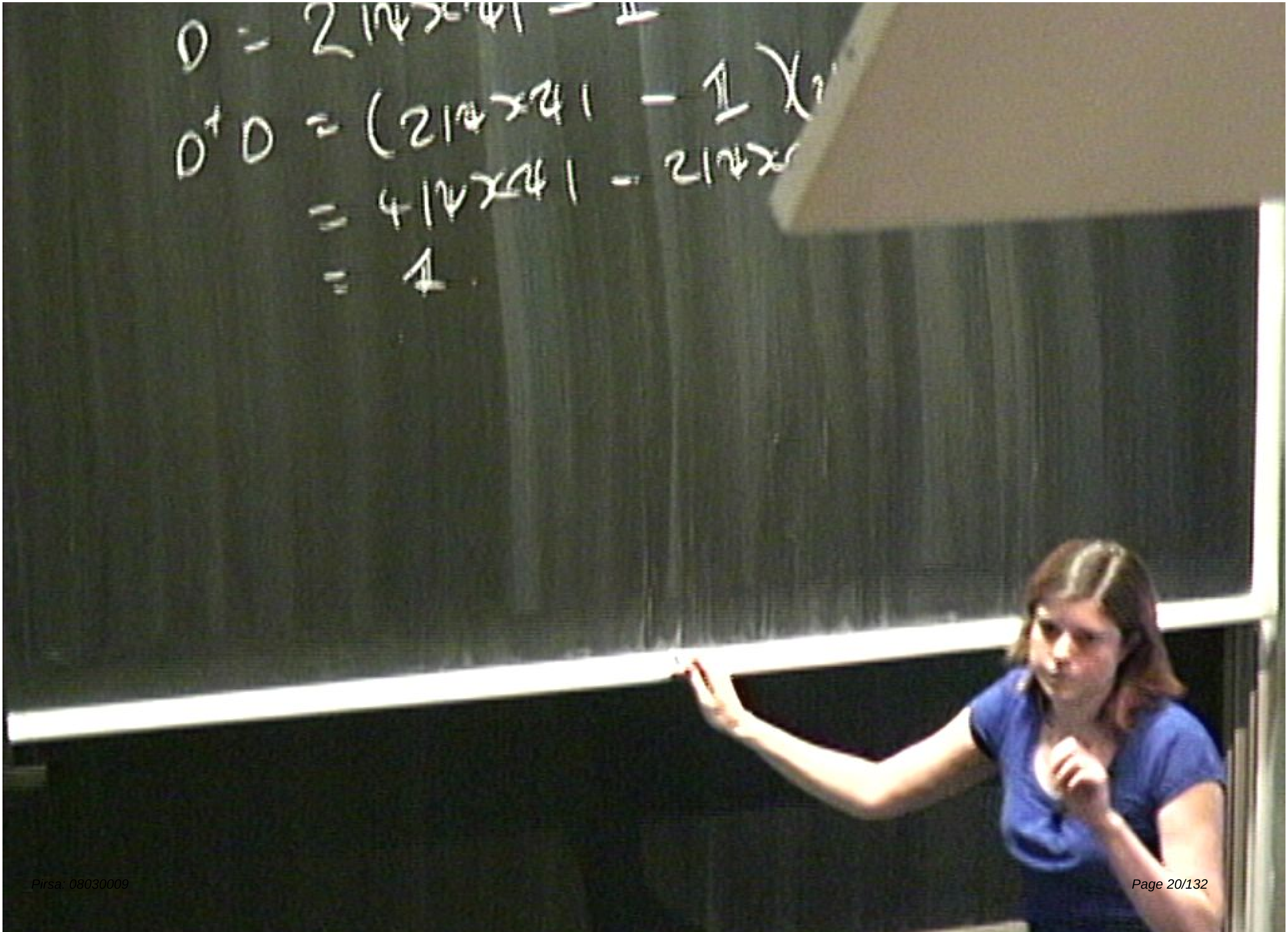
$$\left(U_f \left(\frac{1}{2} \sum_{x=0} |x\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \right) \right)$$

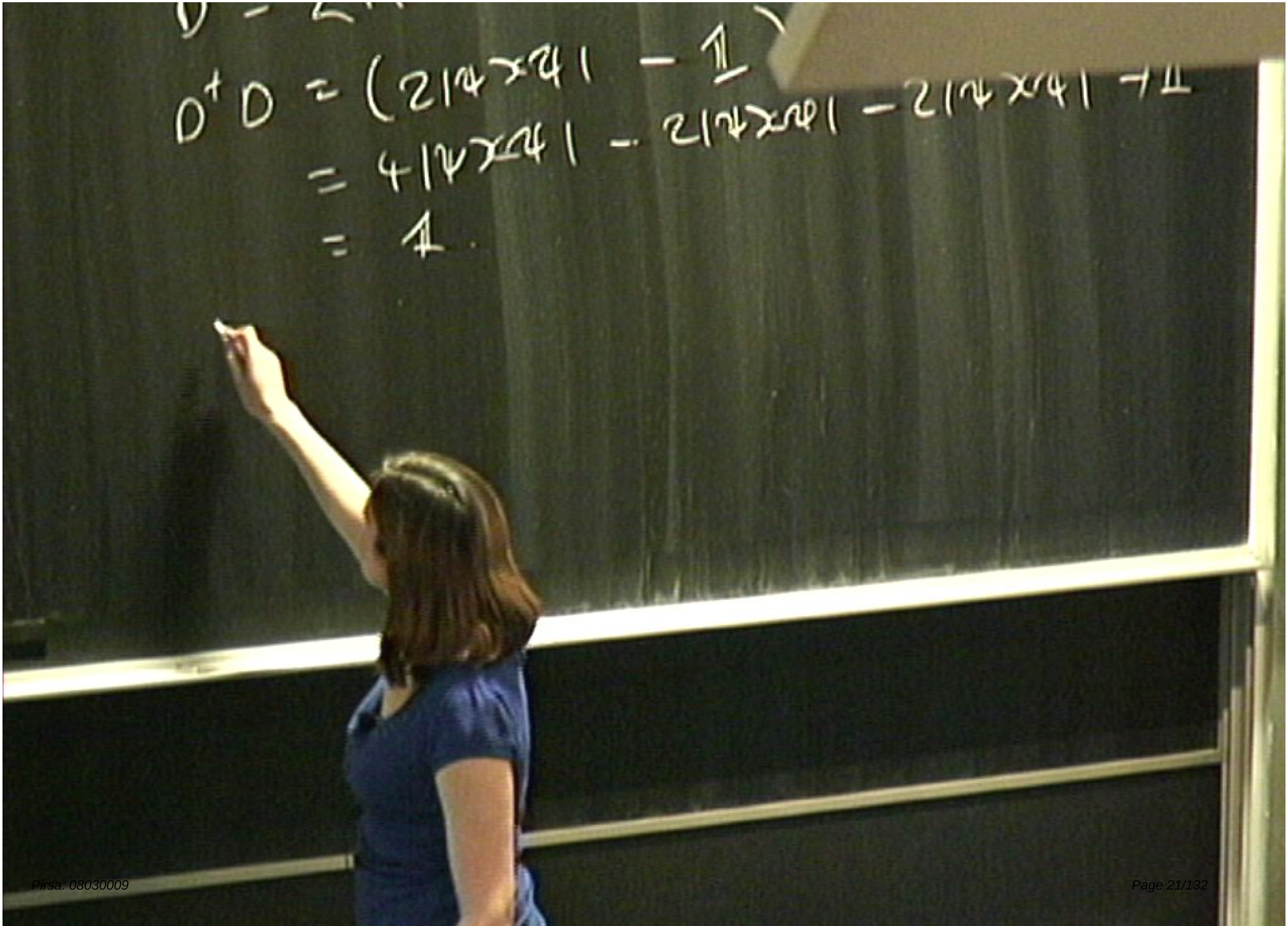
$$= \underbrace{\frac{1}{2} \sum_{x=0}^{3} (-1)^{f(x)} |x\rangle}_{} \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

$$\hat{D} = 2|\psi\rangle\langle\psi| - \mathbb{1}$$

$$|\psi\rangle = \frac{1}{2} \sum_{x=0}^{3} |x\rangle$$


$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$


D = 2|ψ⟩⟨ψ| − 1
D†D = (2|ψ⟩⟨ψ| − 1)(
= 4|ψ⟩⟨ψ| − 2|ψ⟩
= 1



D = 2|ψ⟩⟨ψ| − 𝟙
D†D = (2|ψ⟩⟨ψ| − 𝟙) 4|ψ⟩⟨ψ| − 2|ψ⟩⟨ψ| − 2|ψ⟩⟨ψ| + 𝟙
= 4|ψ⟩⟨ψ|
= 𝟙

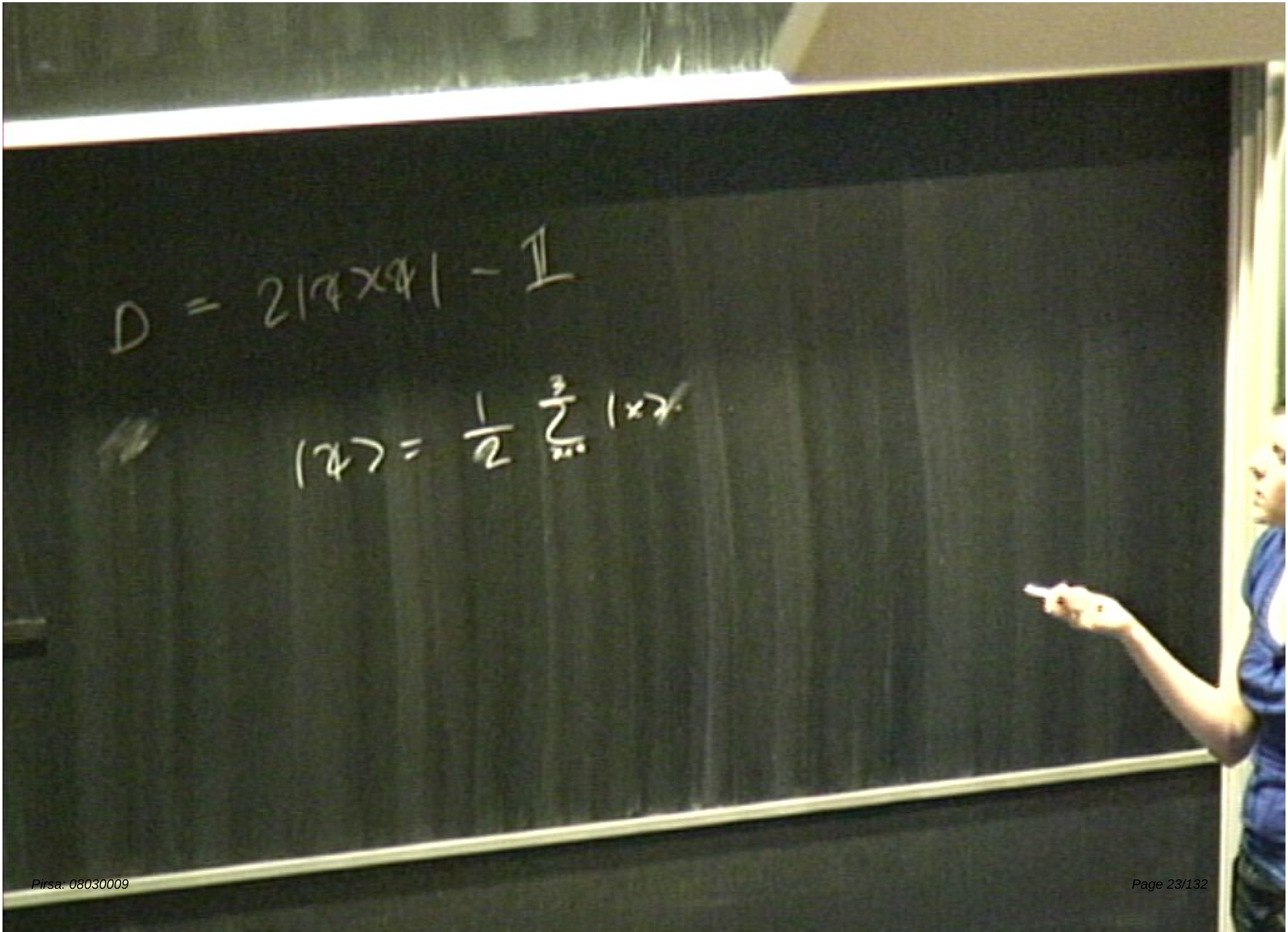
$D = 2 \ldots$

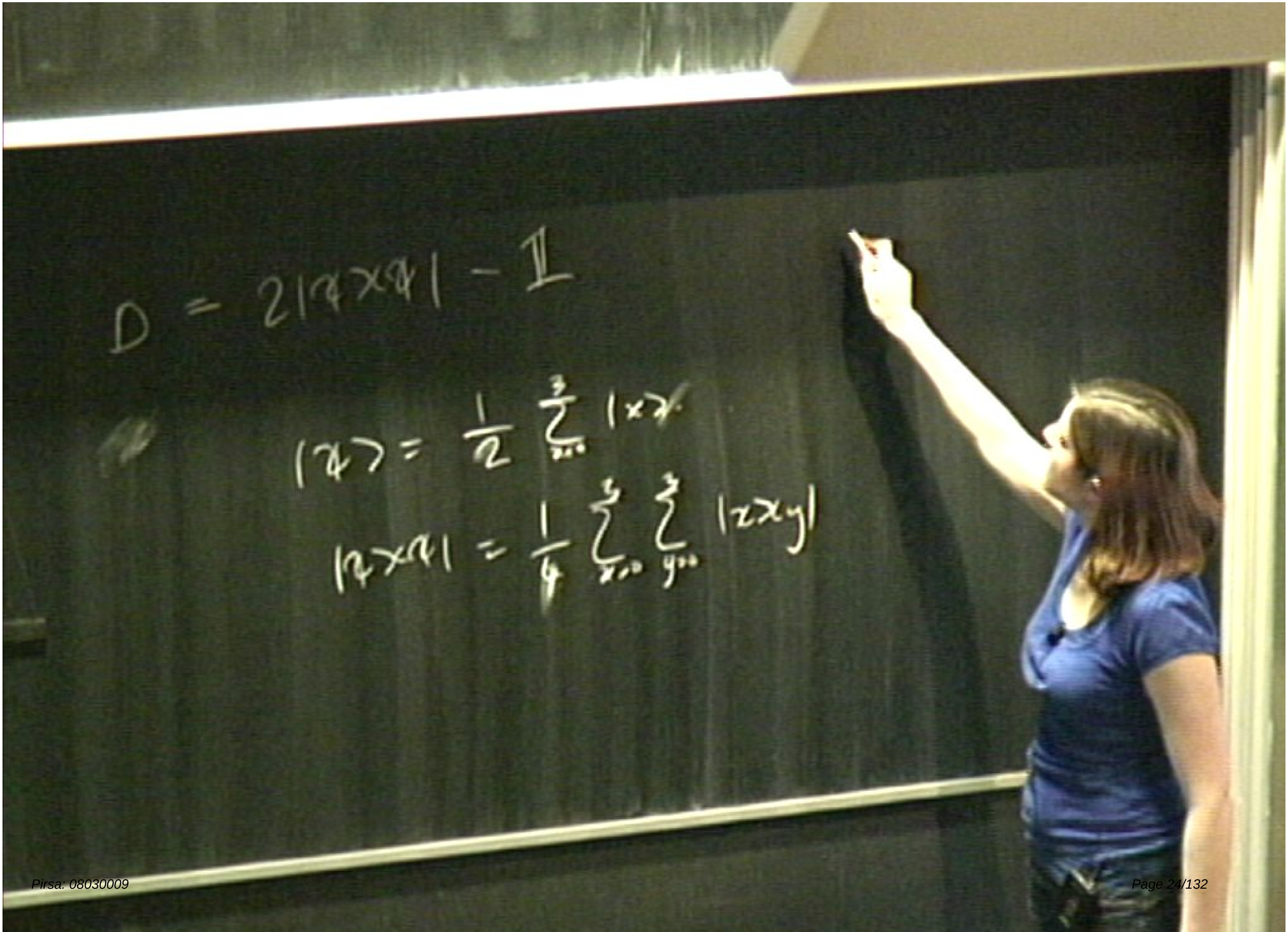
$D^\dagger D = (2|\psi\rangle\langle\psi| - \mathbb{1}) \ldots 2|\psi\rangle\langle\psi| + \mathbb{1}$

$= 4|\psi\rangle\langle\psi| - 2|\psi\rangle\langle\psi| - 2|\psi\rangle\langle\psi| + \mathbb{1}$

$= \mathbb{1}$

$\frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle + |11\rangle\right)$


D = 2|ψ⟩⟨ψ| − 𝟙
|ψ⟩ = 1/2 Σ_{x=0}^{3} |x⟩


$D = 2|\psi\rangle\langle\psi| - \mathbb{I}$
$|\psi\rangle = \frac{1}{2}\sum_{x=0}^{3} |x\rangle$
$|\psi\rangle\langle\psi| = \frac{1}{4}\sum_{x=0}^{3}\sum_{y=0}^{3} |x\rangle\langle y|$

$$D = \sum_{x,y} |x\rangle\langle x| D |y\rangle\langle y|$$

$$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$$

$$|\psi\rangle = \frac{1}{2}\sum_{x=0}^{3} |x\rangle$$

$$|\psi\rangle\langle\psi| = \frac{1}{4}\sum_{x=0}^{3}\sum_{y=0}^{3} |x\rangle\langle y|$$

$$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$$

$$|\psi\rangle = \frac{1}{2}\sum_{x=0}^{3} |x\rangle$$

$$|\psi\rangle\langle\psi| = \frac{1}{4}\sum_{x=0}^{3}\sum_{y=0}^{3} |x\rangle\langle y|$$

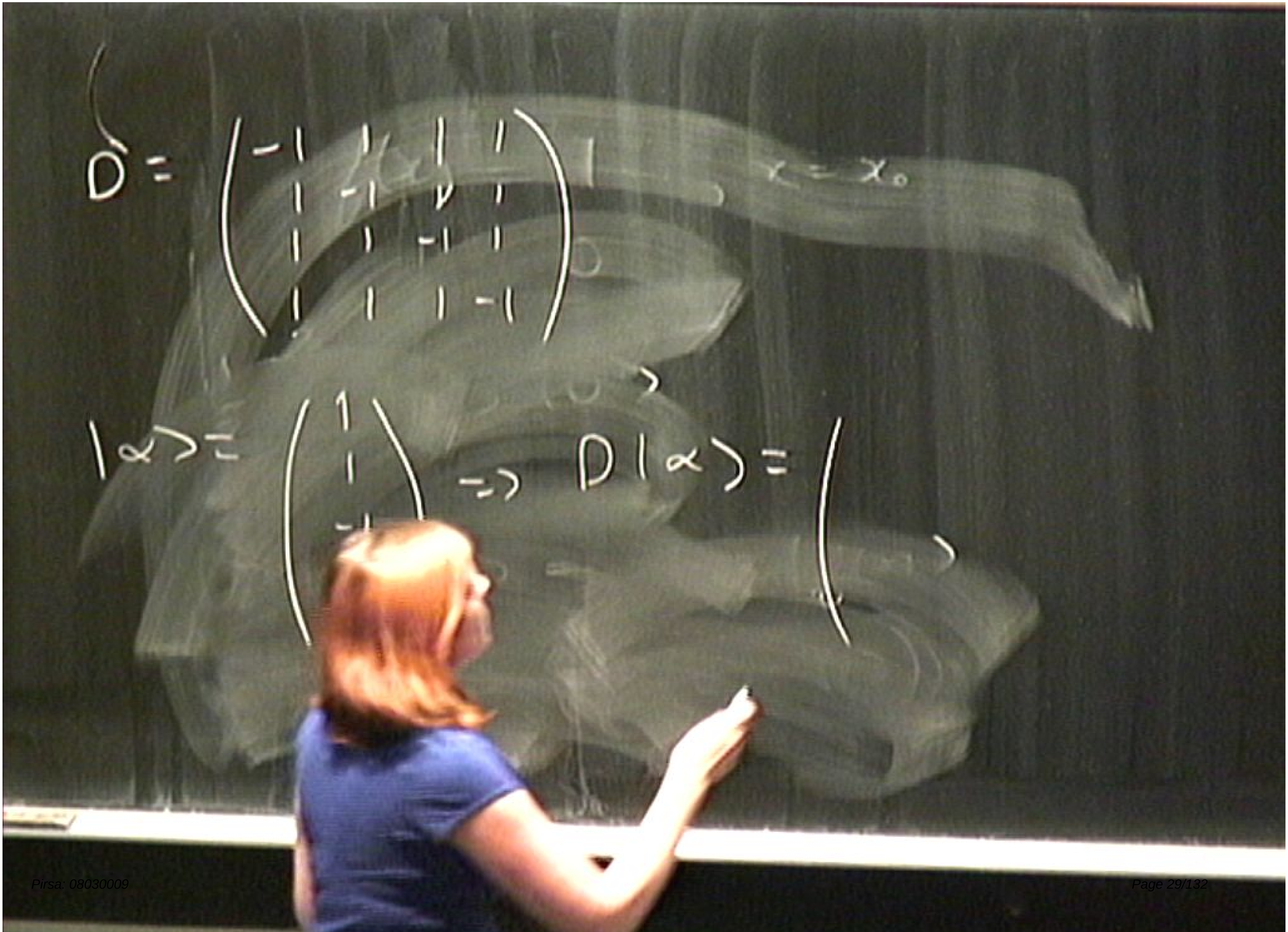
$$D = \sum_{x,y} |x\rangle\langle x| D |y\rangle\langle y|$$

$$= \sum_{x,y} \frac{1}{2} |x\rangle\langle y| - \mathbb{1}$$


Q =
x = x0

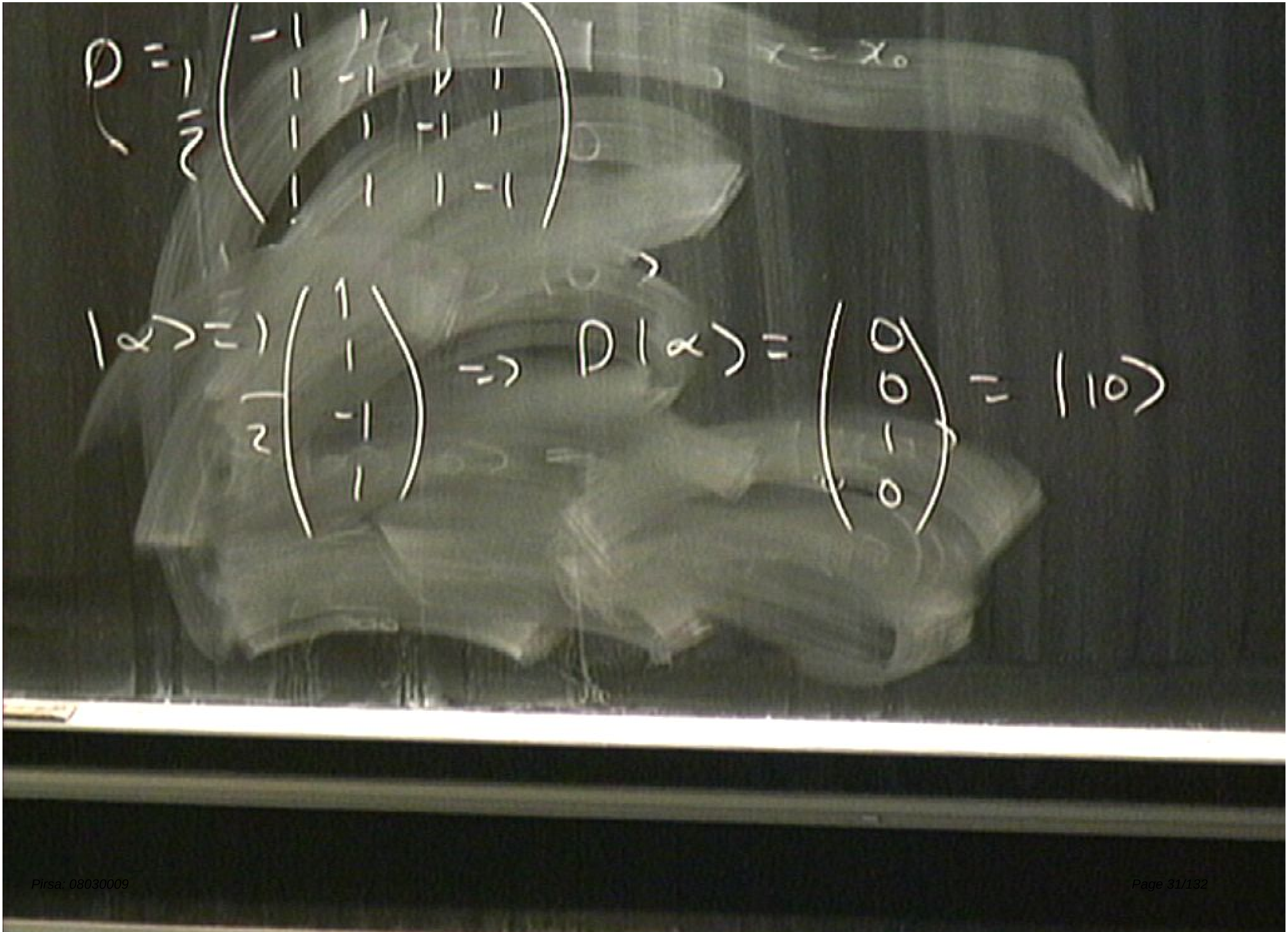
$$Q = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \quad x = x_0$$

$$|\alpha\rangle = ($$


D = (-1 1 1 1 / 1 -1 1 1 / 1 1 -1 1 / 1 1 1 -1)
x = x₀
|α> = (1 1 -1) => D|α> = ( )

$$D = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

$$|\alpha\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \Rightarrow D|\alpha\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$


$D = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$
$x = x_0$
$|\alpha\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \Rightarrow D|\alpha\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$

$$\frac{1}{\sqrt{N}} \sum_{x} |x\rangle \left(\frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) \right)$$

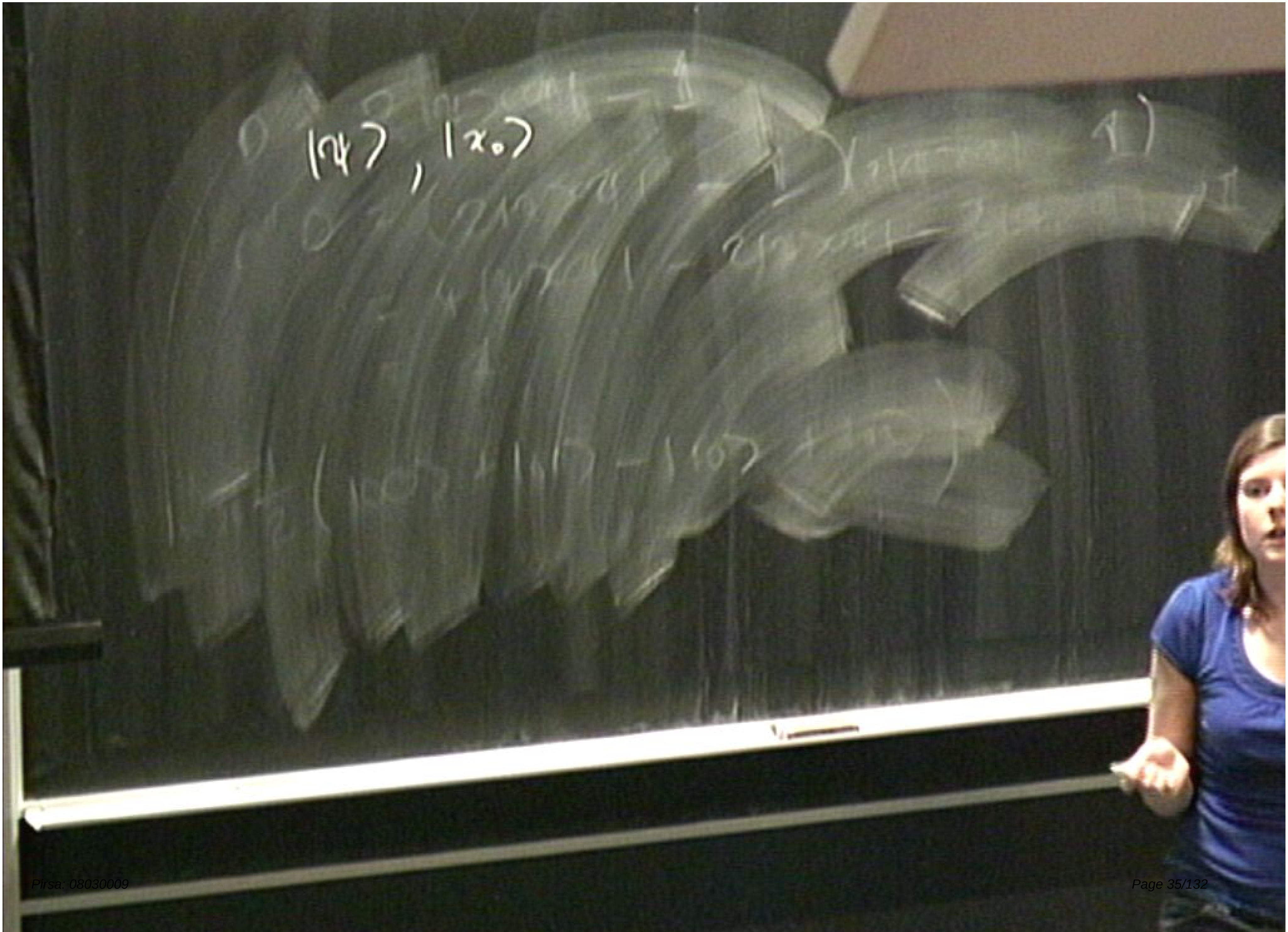
$$\frac{1}{\sqrt{N}} \sum |x\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

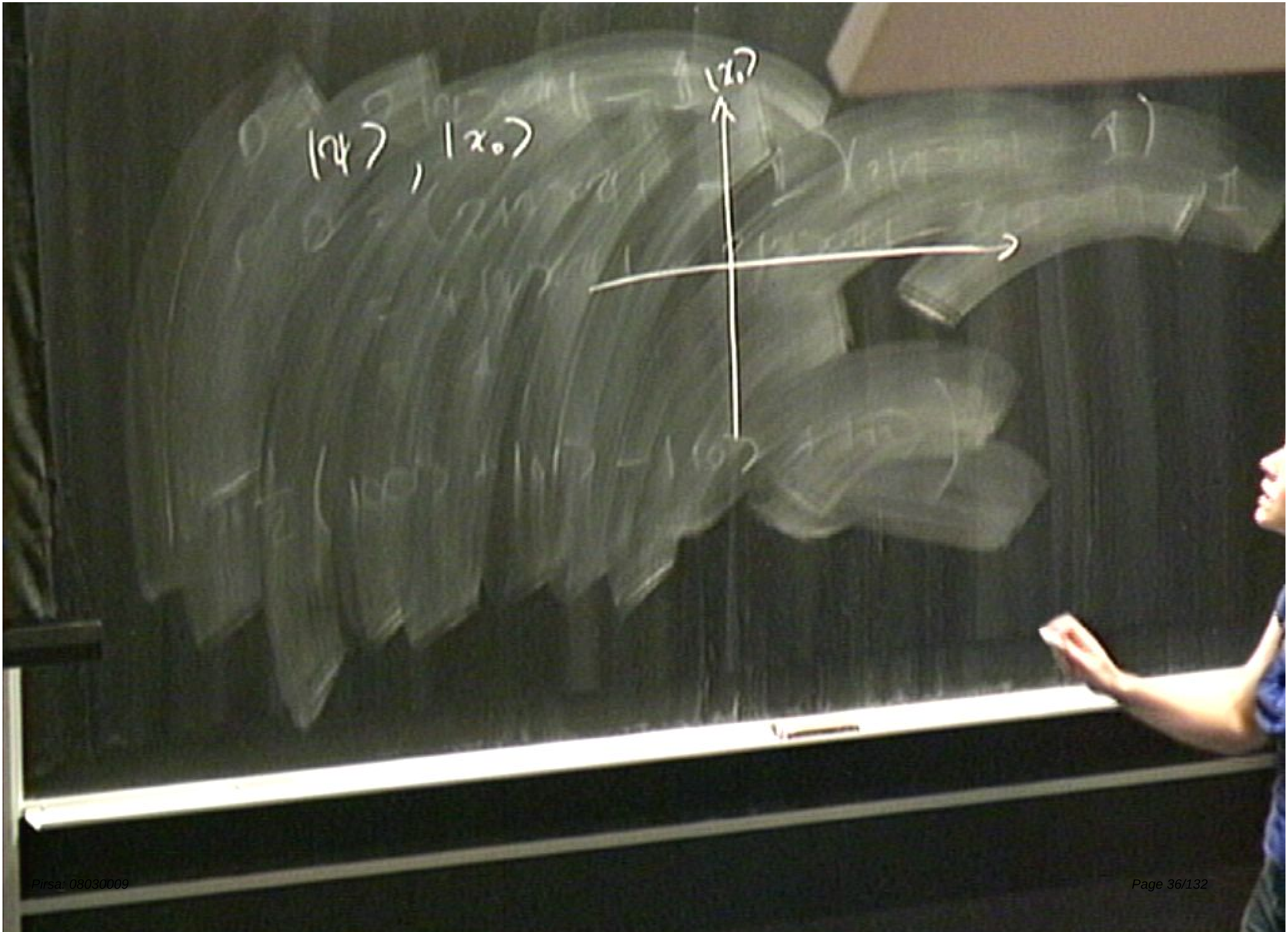
$$\rightarrow U_f \quad \frac{1}{\sqrt{N}} \sum (-1)^{f(x)} |x\rangle$$

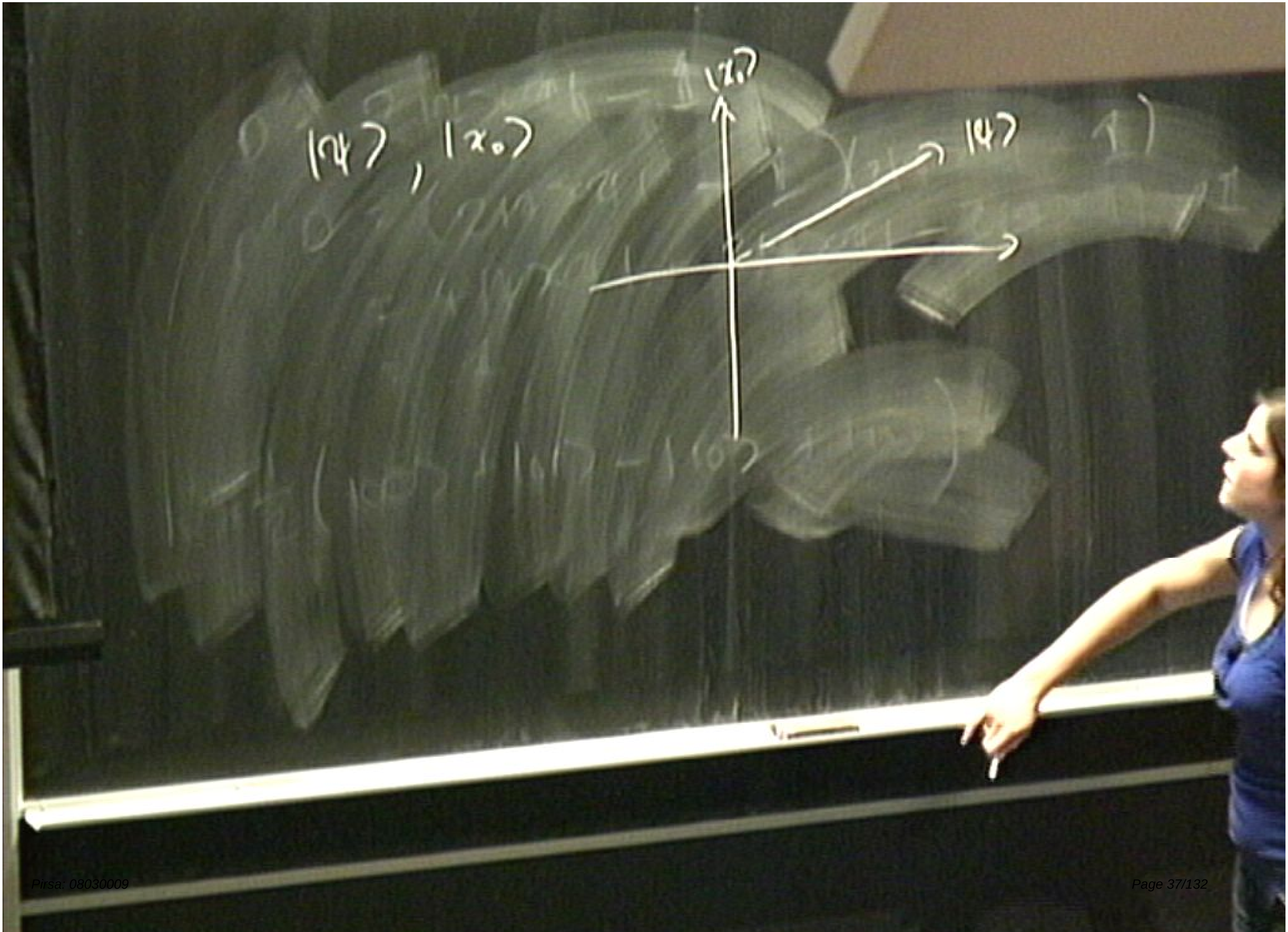
$$\frac{1}{\sqrt{N}} \sum |x\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$$

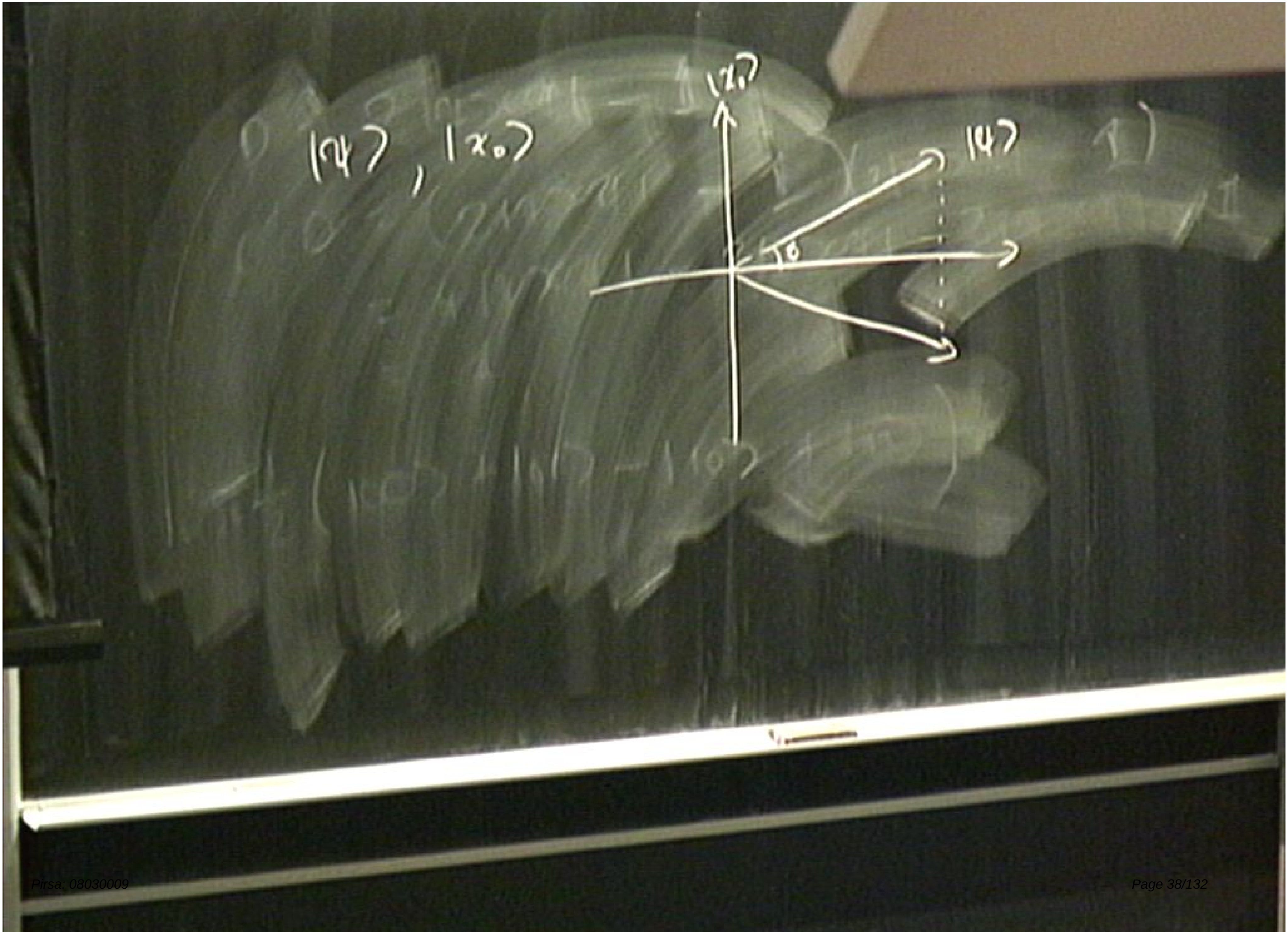
$$\rightarrow U_f \quad \frac{1}{\sqrt{N}} \sum (-1)^{f(x)} |x\rangle$$

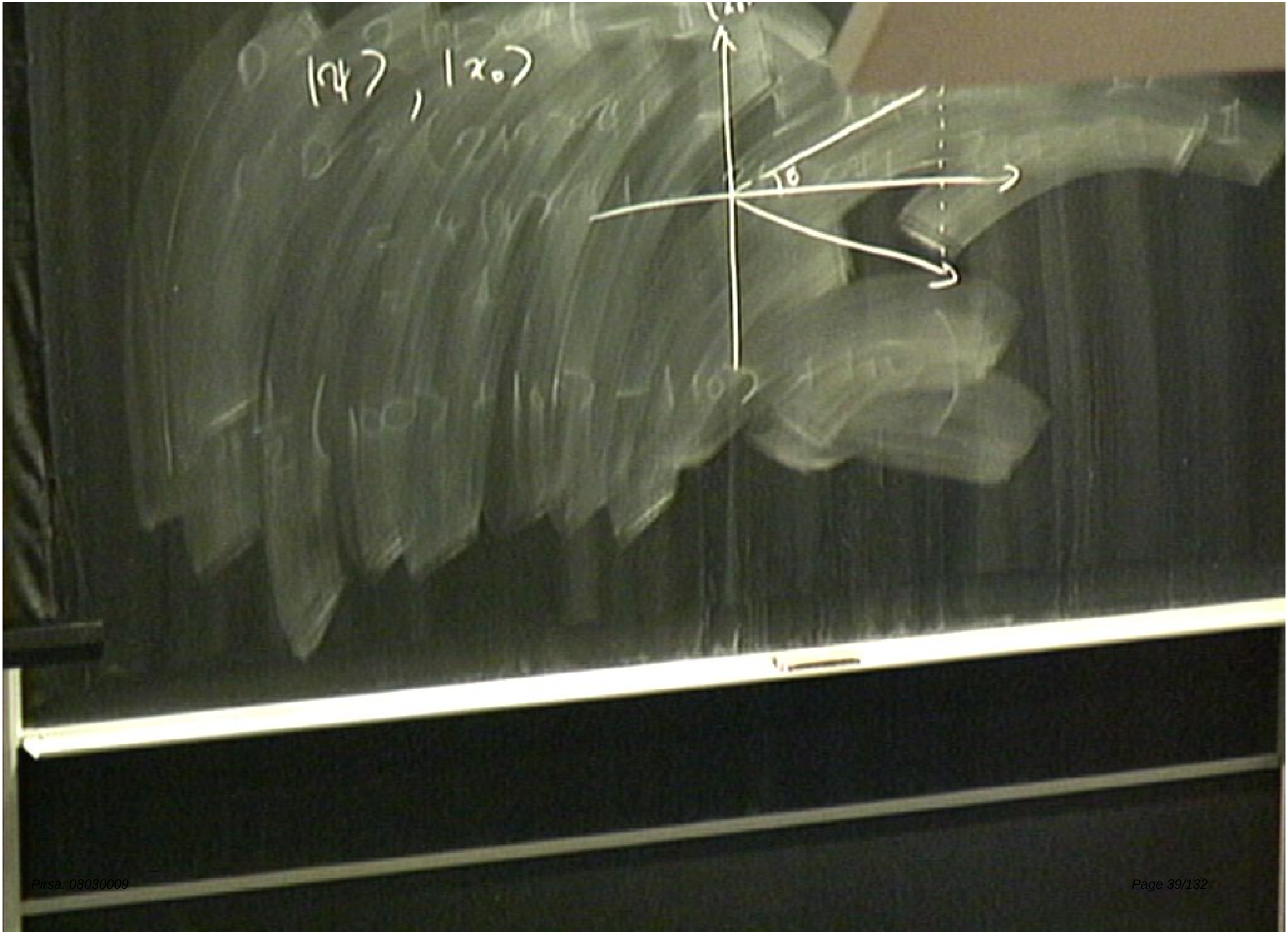
$$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$$

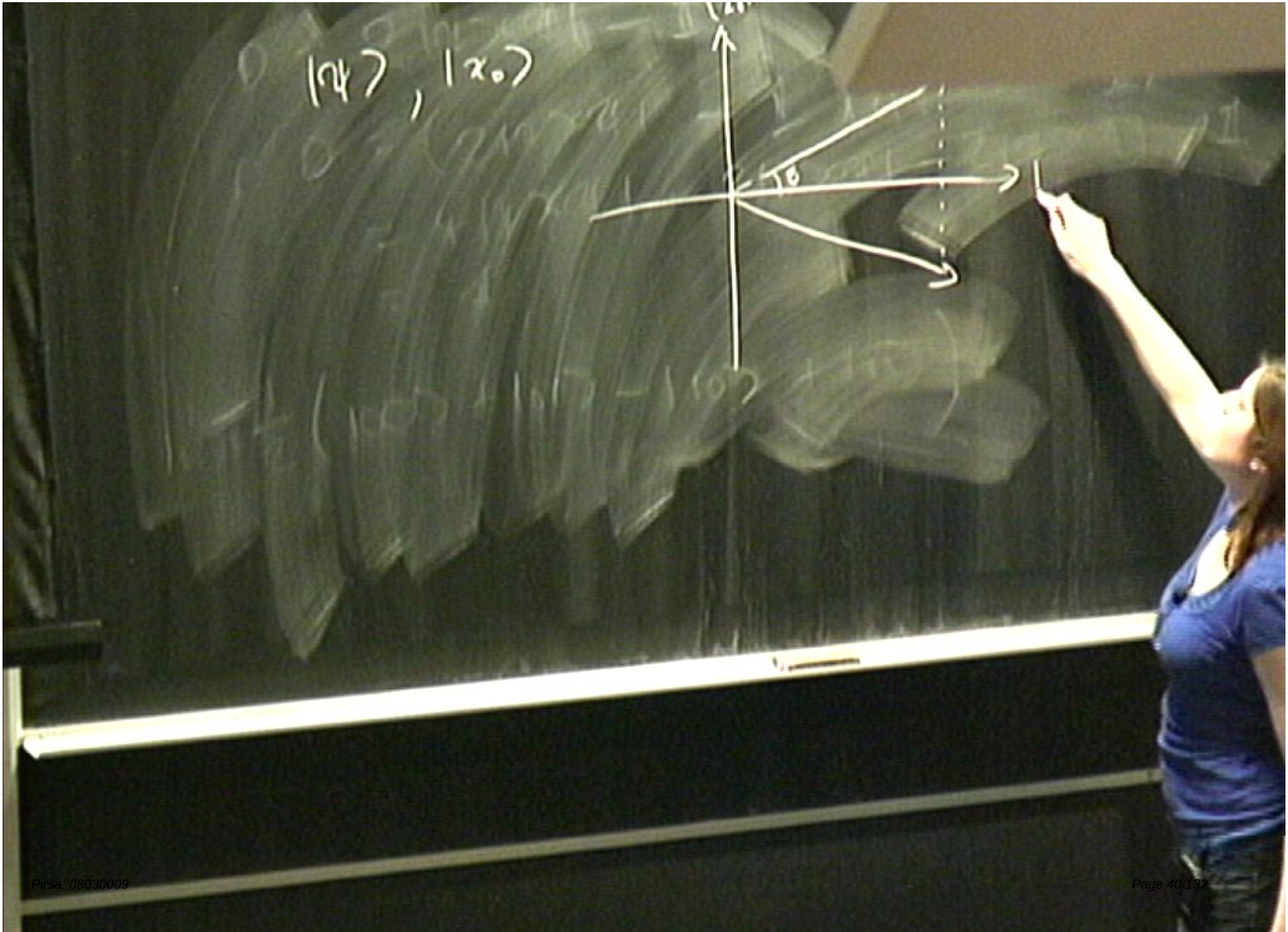

$|\psi\rangle$, $|x_0\rangle$

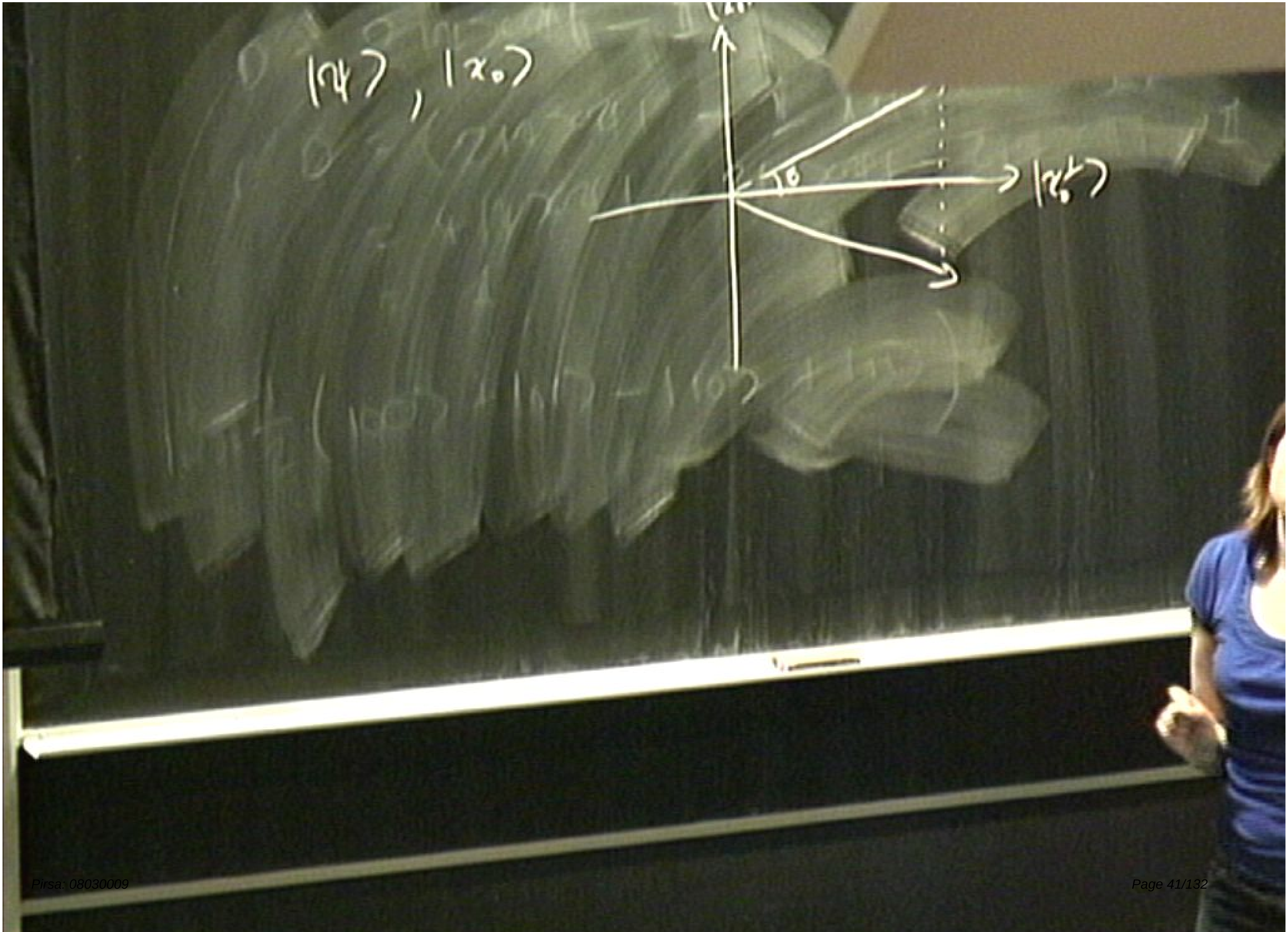

|ψ⟩ , |x₀⟩
|x₀⟩

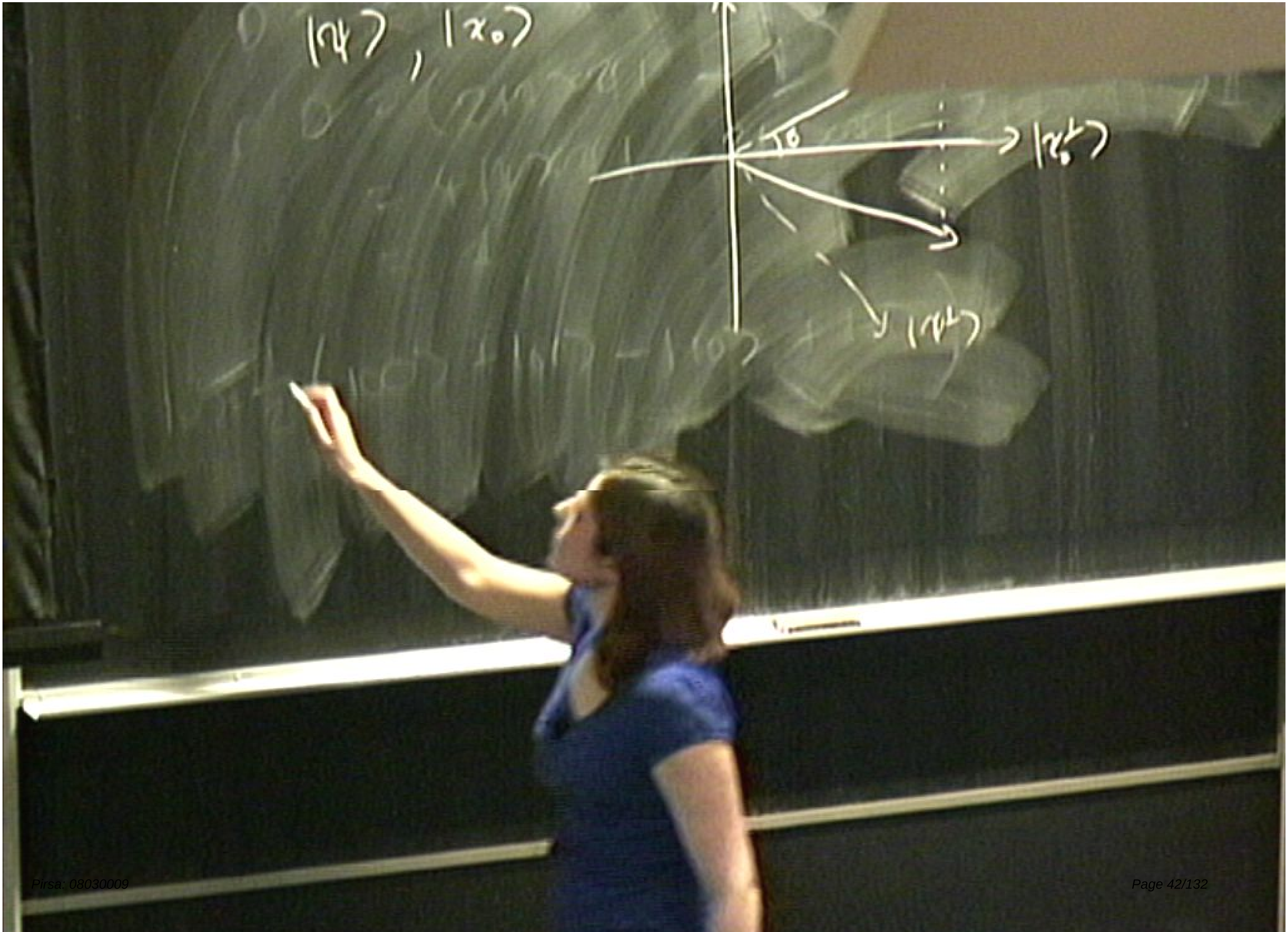

|ψ⟩ , |x₀⟩
|x₀⟩
|ψ⟩

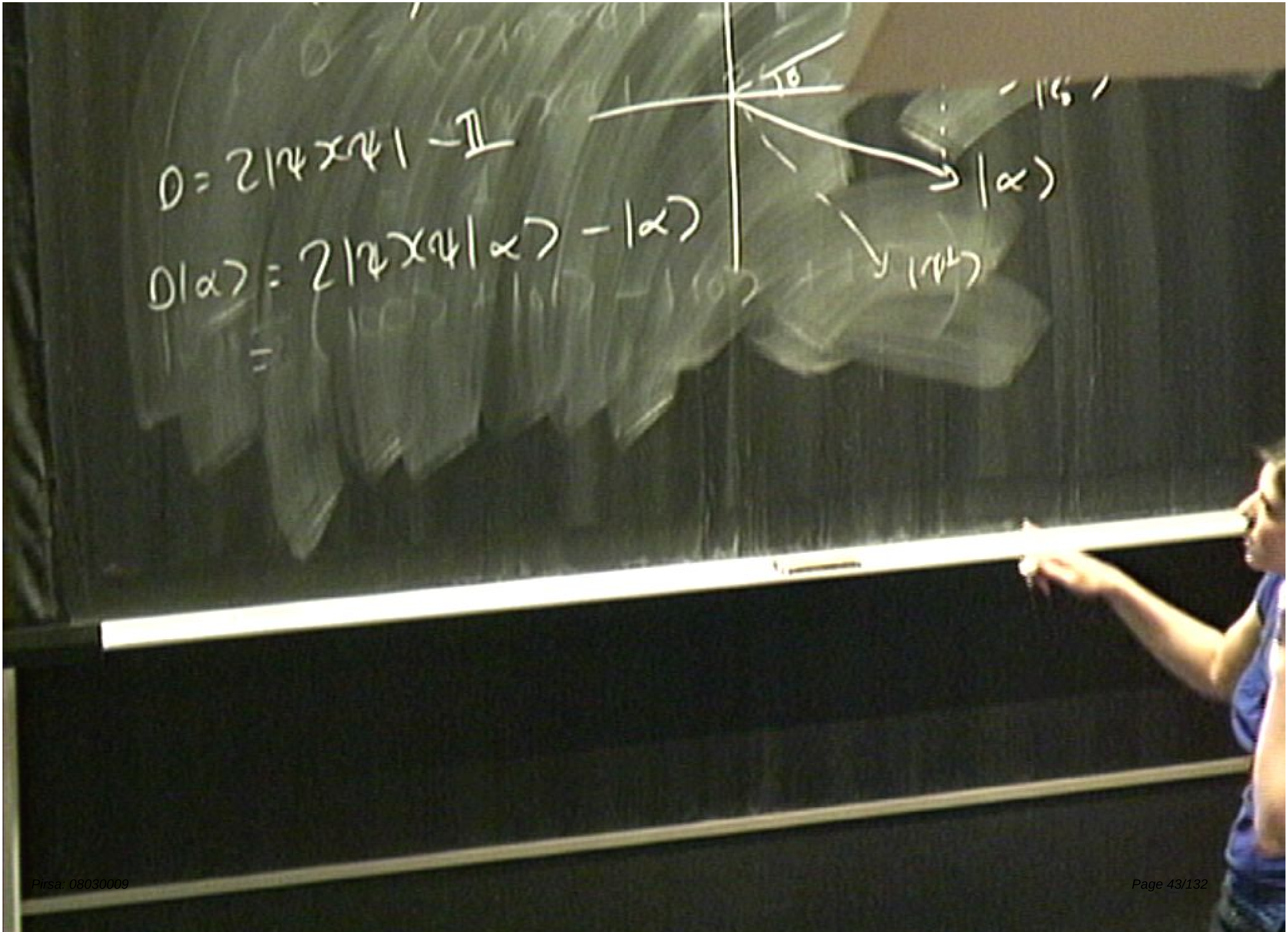

|ψ⟩ , |x₀⟩
|x₀⟩
|ψ⟩
θ

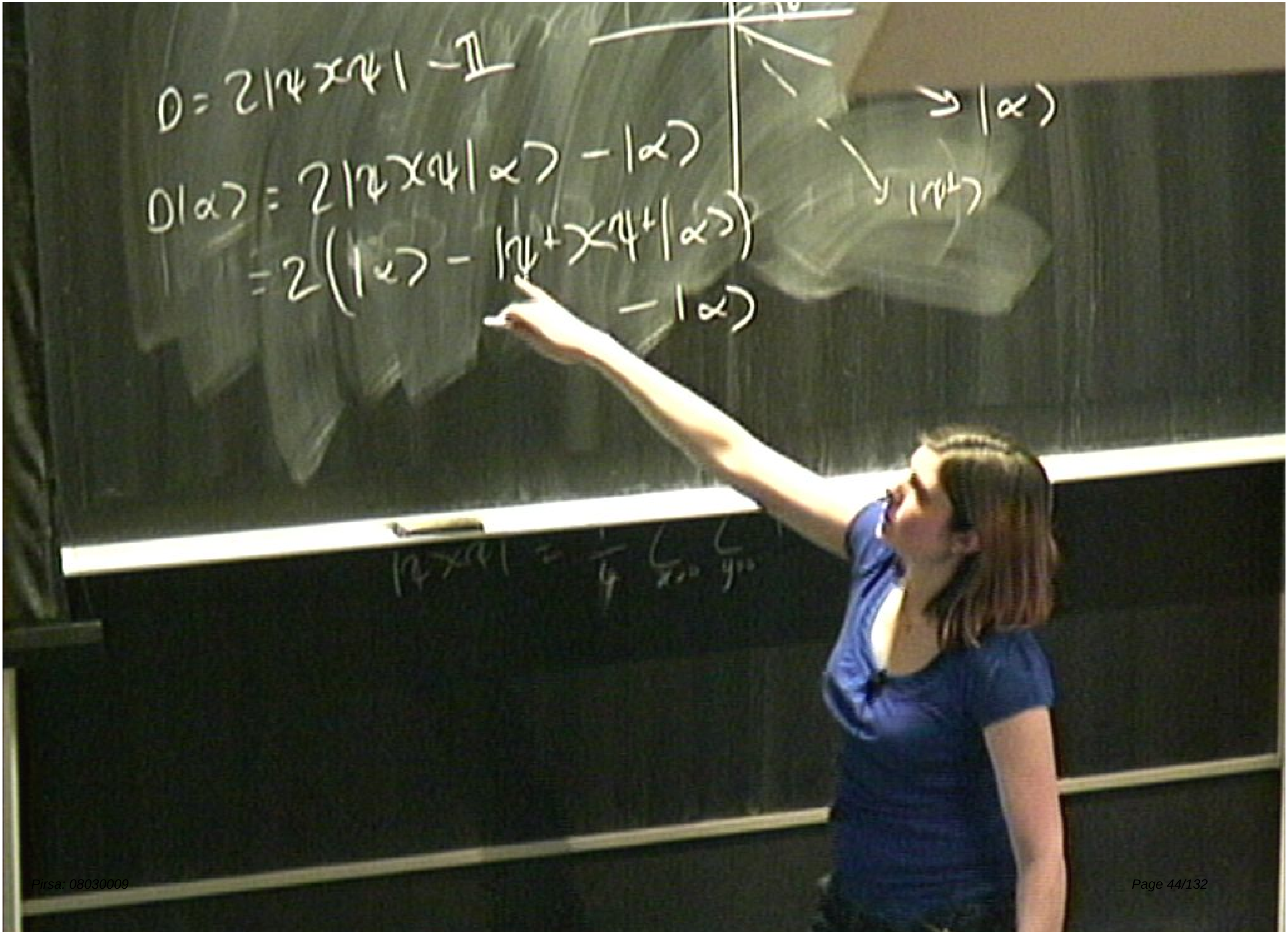


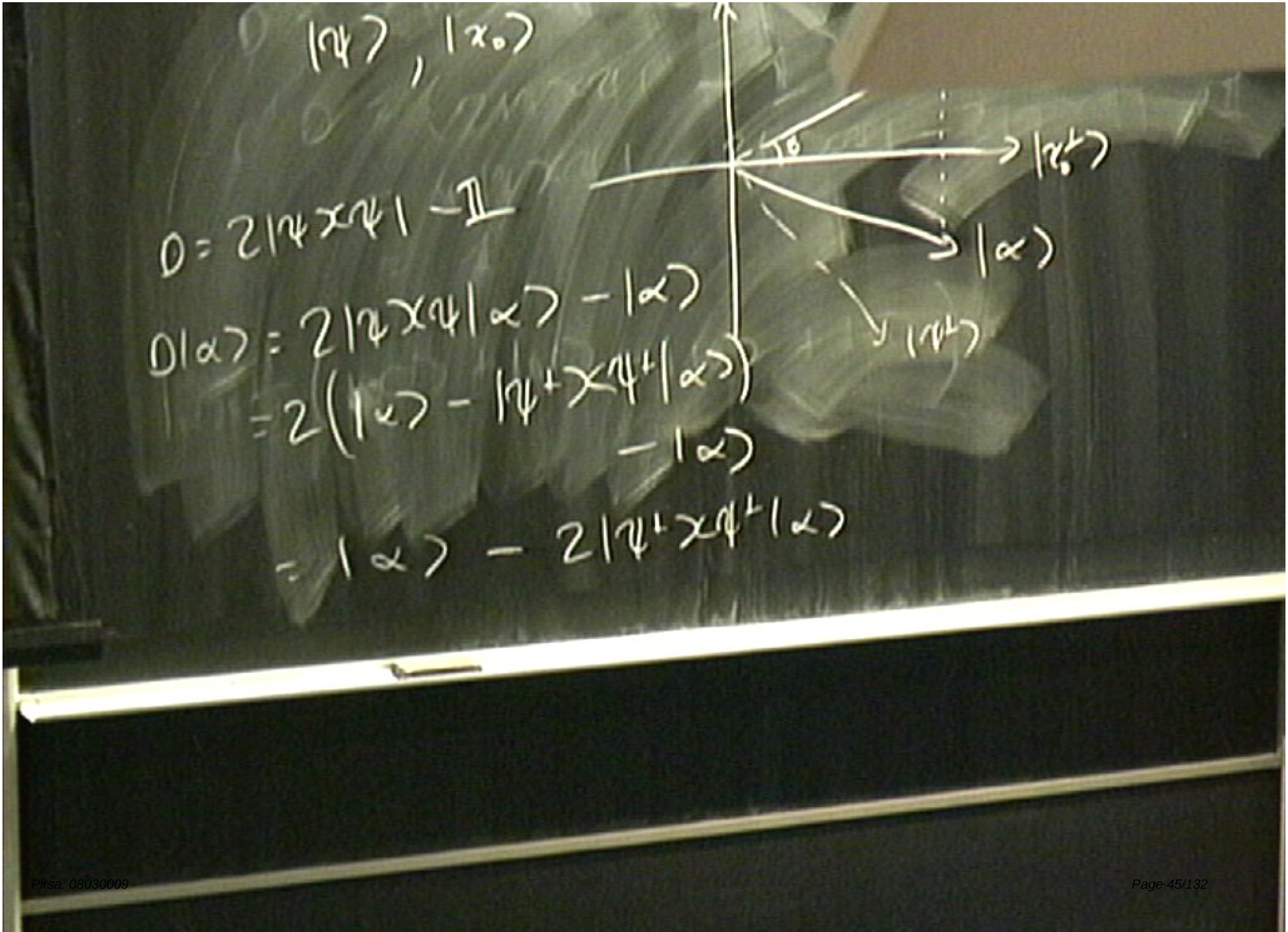

$|\psi\rangle$, $|x_0\rangle$


|ψ⟩ , |x₀⟩
θ




D = 2|ψ⟩⟨ψ| − 𝟙
D|α⟩ = 2|ψ⟩⟨ψ|α⟩ − |α⟩
|α⟩
|ψ⊥⟩


D = 2|ψ⟩⟨ψ| − 𝟙
D|α⟩ = 2|ψ⟩⟨ψ|α⟩ − |α⟩
= 2(|α⟩ − |ψ⊥⟩⟨ψ⊥|α⟩)
− |α⟩
→ |α⟩
→ |ψ⊥⟩


$|\psi\rangle, \; |x_0\rangle$
$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$
$D|\alpha\rangle = 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle$
$= 2\left(|\alpha\rangle - |\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle\right) - |\alpha\rangle$
$= |\alpha\rangle - 2|\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle$
θ
$|x_0^\perp\rangle$
$|\alpha\rangle$
$|\psi^\perp\rangle$

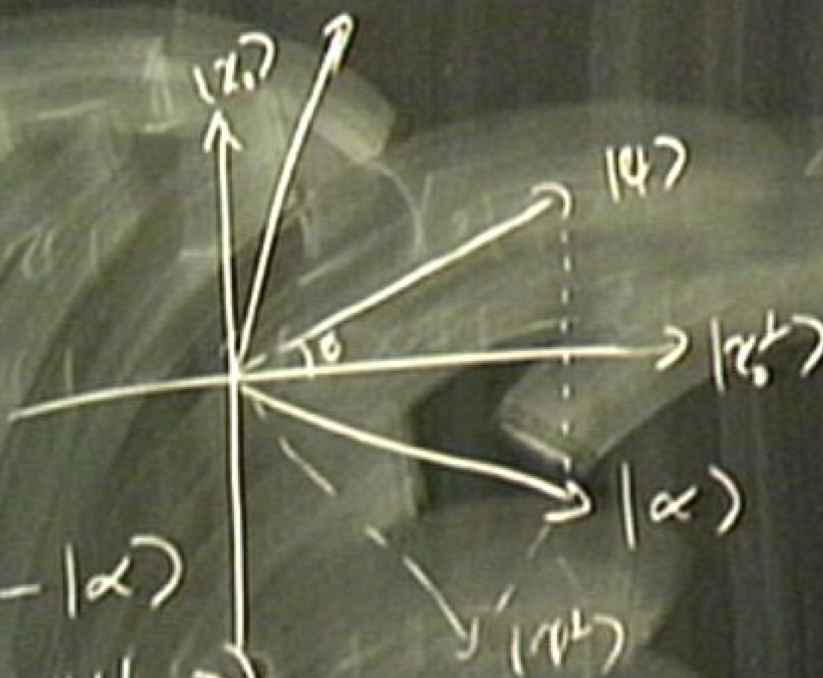
$$|\psi\rangle, \; |x_0\rangle$$

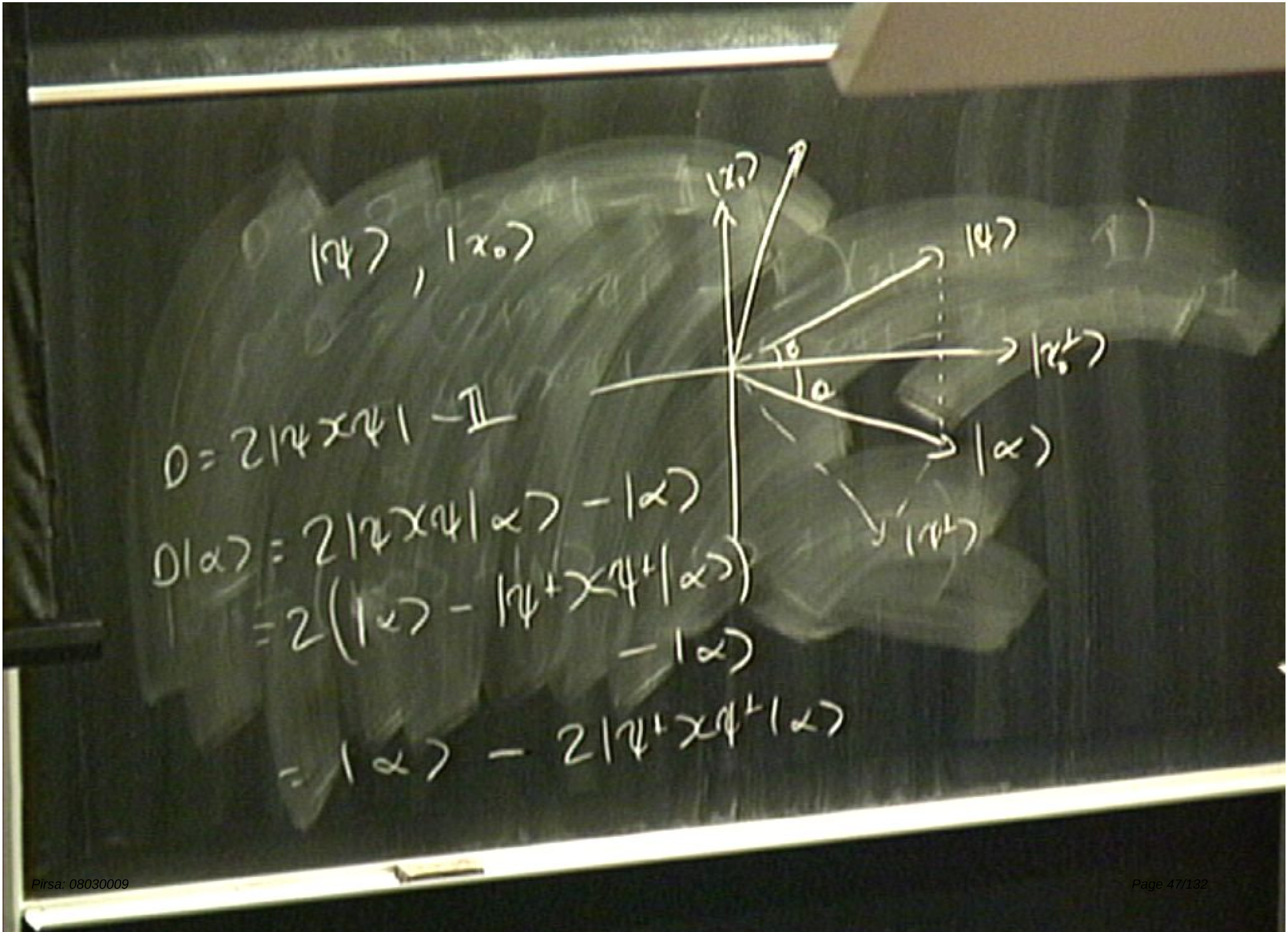
$$D = 2|\psi\rangle\langle\psi| - \mathbb{I}$$

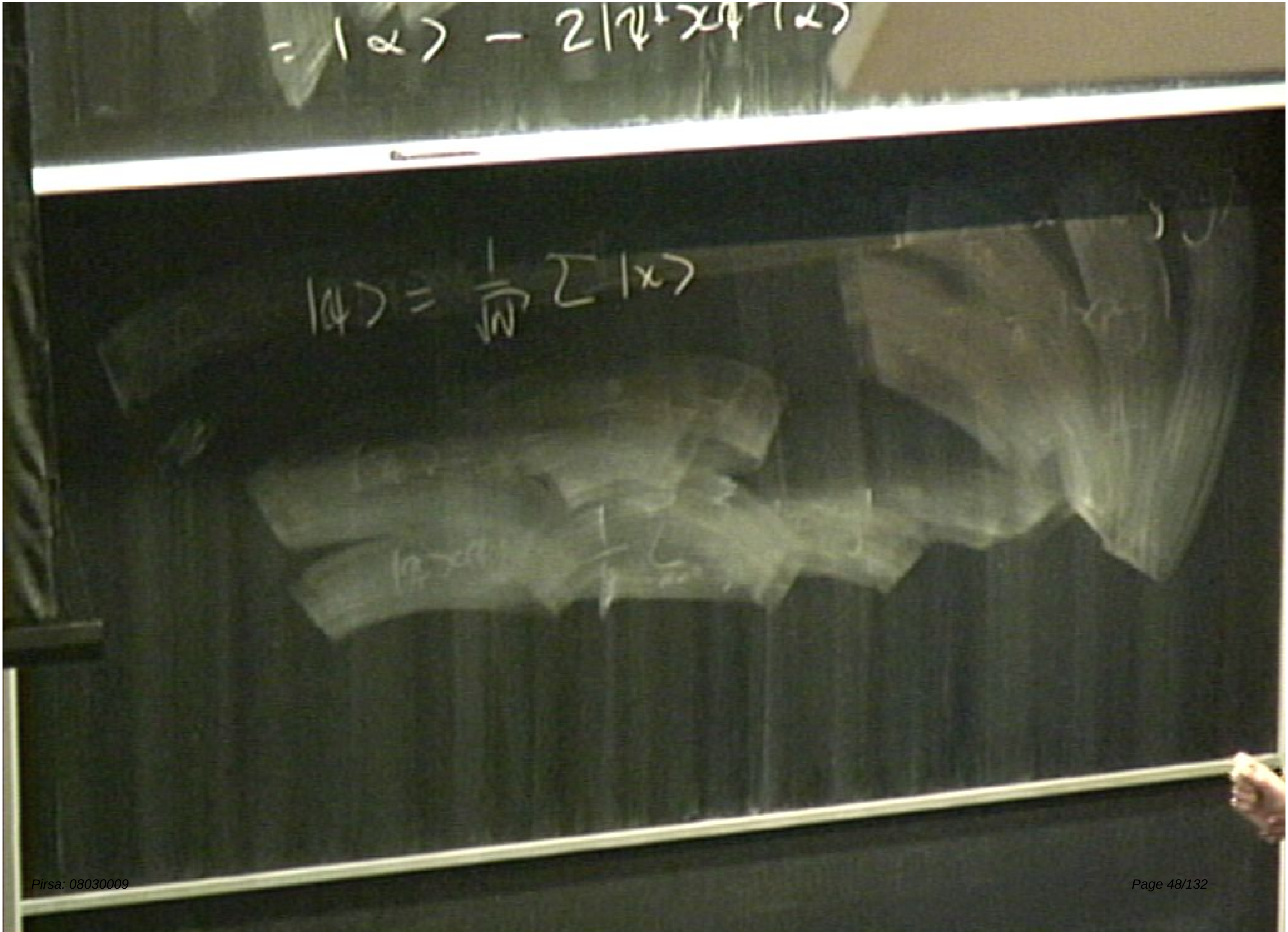
$$D|\alpha\rangle = 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle$$

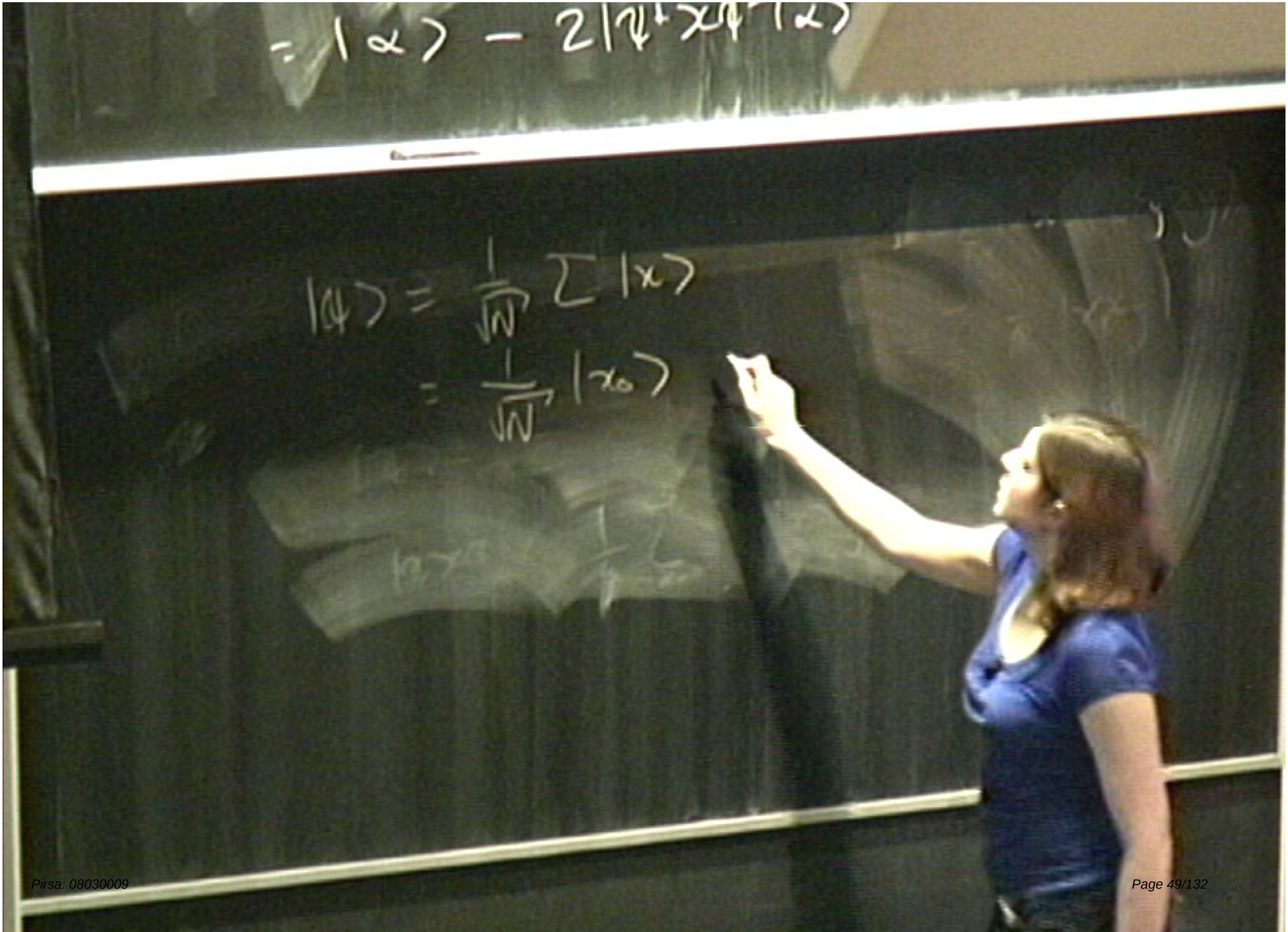
$$= 2\left(|\alpha\rangle - |\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle\right) - |\alpha\rangle$$

$$= |\alpha\rangle - 2|\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle$$




|ψ⟩ , |x₀⟩
D = 2|ψ⟩⟨ψ| − 𝟙
D|α⟩ = 2|ψ⟩⟨ψ|α⟩ − |α⟩
= 2(|α⟩ − |ψ⊥⟩⟨ψ⊥|α⟩)
− |α⟩
= |α⟩ − 2|ψ⊥⟩⟨ψ⊥|α⟩
|x₀⟩
|ψ⟩
|x₀⊥⟩
|α⟩
|ψ⊥⟩
θ
θ

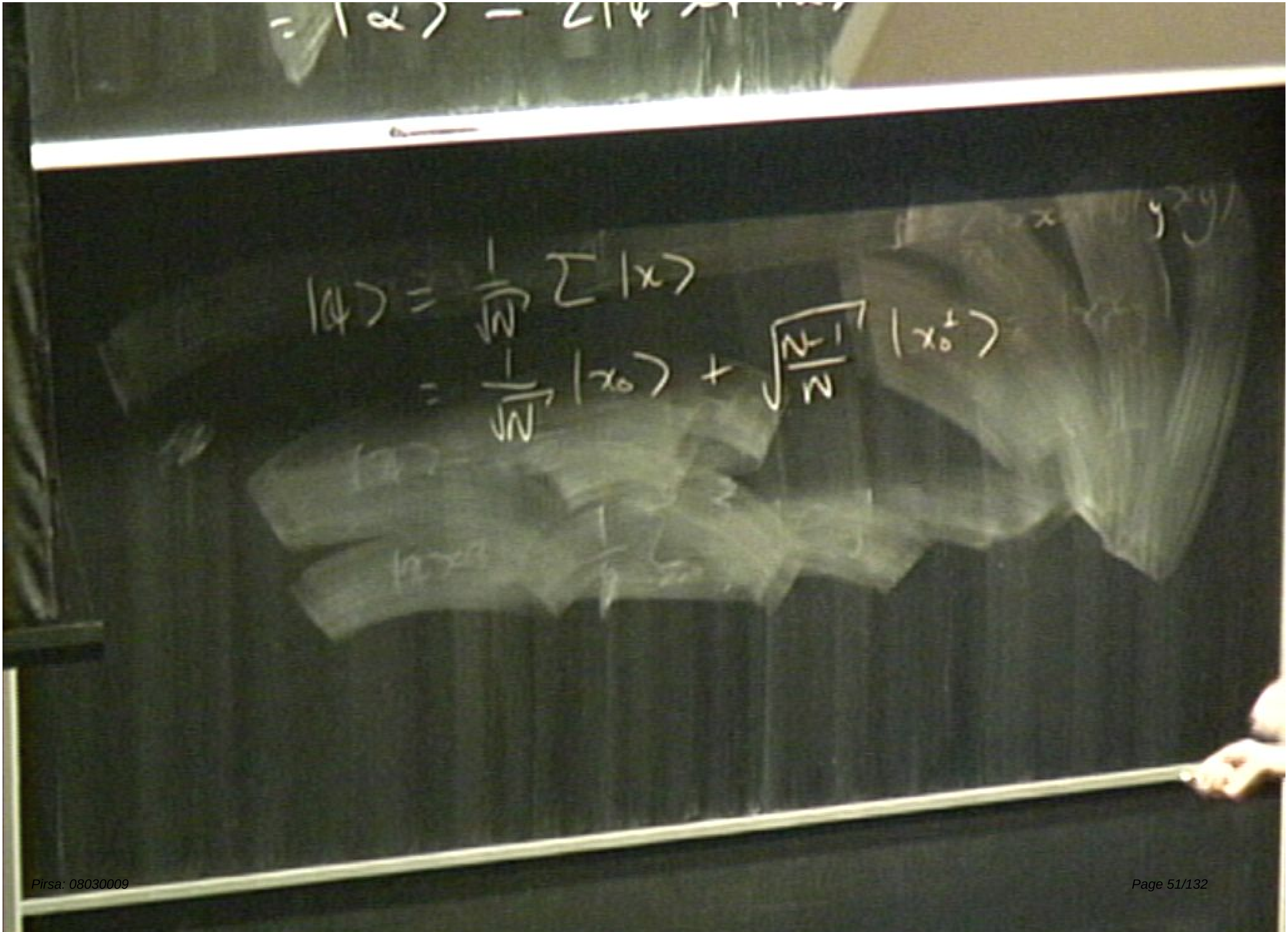

= |α⟩ − 2|ψ⟩⟨ψ|α⟩
|ψ⟩ = 1/√N Σ |x⟩


= |α> − 2|ψ><ψ|α>
|ψ> = 1/√N Σ |x>
= 1/√N |x₀>

$$= |\alpha\rangle - 2|\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^\perp\rangle$$


$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$
$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^\perp\rangle$

$$= |\alpha\rangle - 2\langle\psi \ldots$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}}\, |x_0^{\perp}\rangle$$

$$= \sin\theta\, |x_0\rangle + \cos\theta\, |x_0^{\perp}\rangle$$

$$= |\alpha\rangle - 2|\psi\rangle \ldots$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^{\perp}\rangle$$

$$= \sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$U^{f} |x\rangle = -\sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$= |\alpha\rangle - 2|\psi\rangle \ldots$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^\perp\rangle$$

$$= \sin\theta |x_0\rangle + \cos\theta |x_0^\perp\rangle$$

$$\sin\theta |x_0\rangle + \cos\theta |x_0^\perp\rangle$$

$$U_f |\alpha\rangle = -\sin\theta |x_0\rangle + \cos\theta |x_0^\perp\rangle$$

$$D U_f |\alpha\rangle =$$

$$= |\alpha\rangle - 2\langle\psi$$

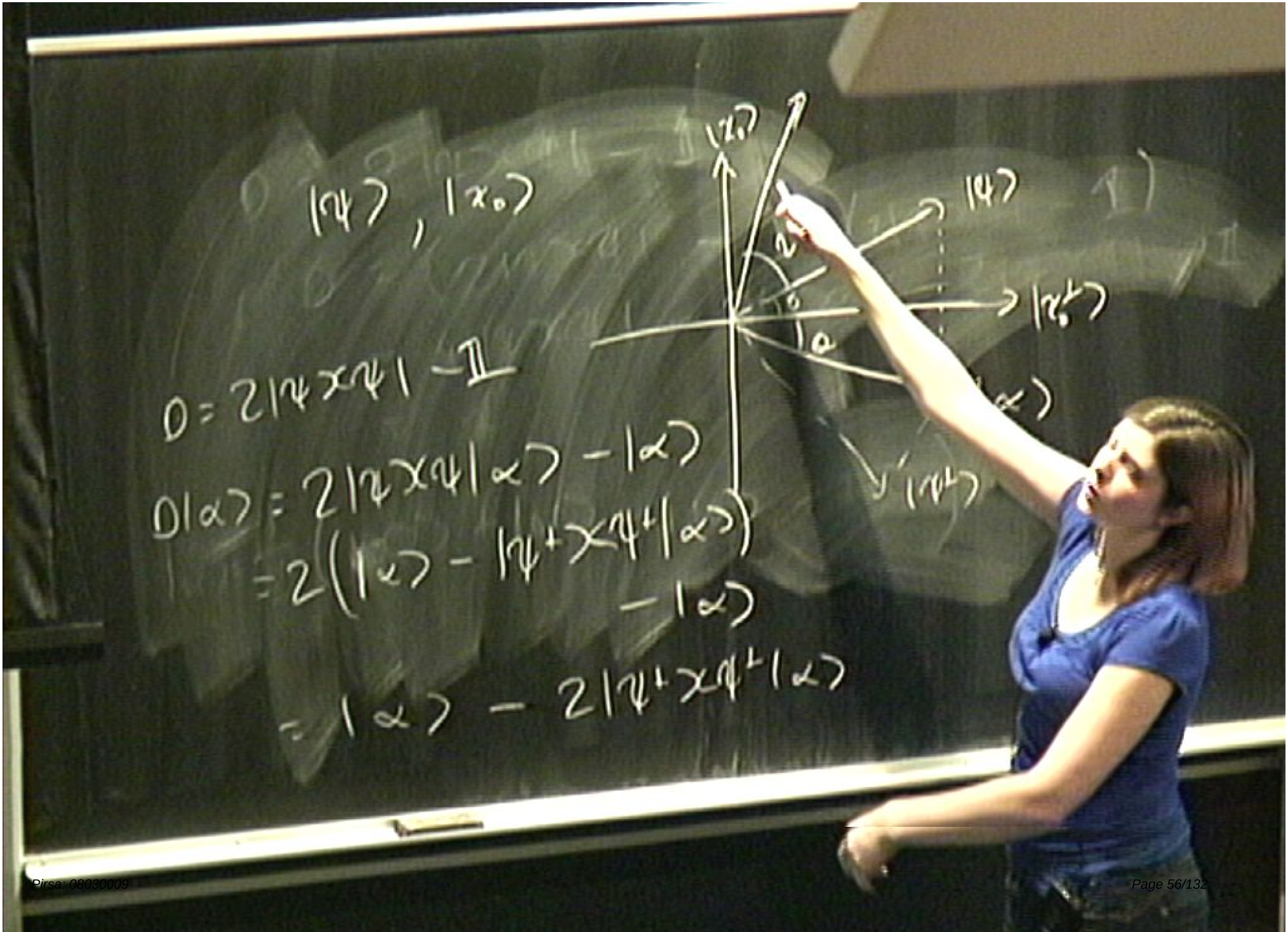
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^\perp\rangle$$

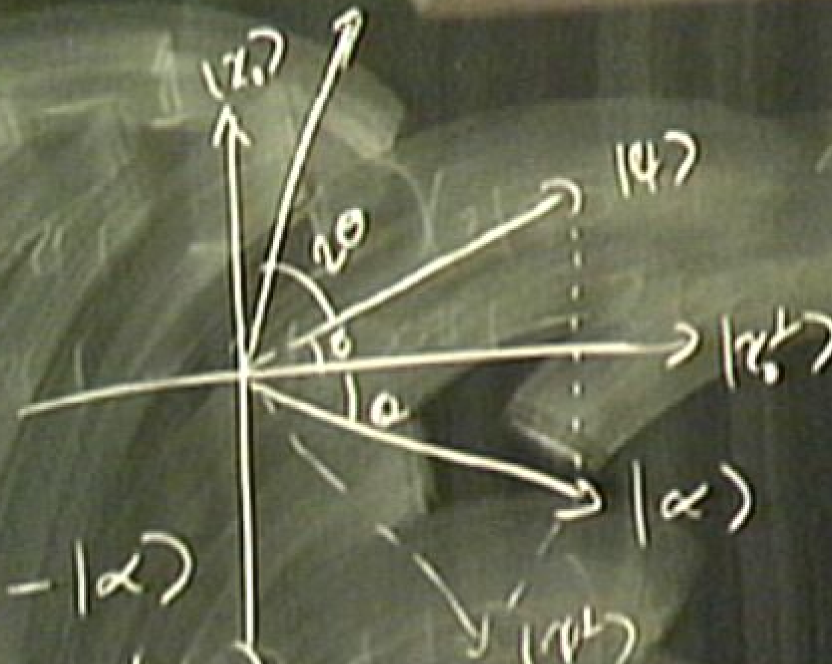
$$= \sin\theta |x_0\rangle + \cos\theta |x_0^\perp\rangle$$

$$U_f |\alpha\rangle = -\sin\theta |x_0\rangle + \cos\theta |x_0^\perp\rangle$$

$$D U_f |\alpha\rangle = \sin 3\theta |x_0\rangle + \cos 3\theta |x_0^\perp\rangle$$


$|\psi\rangle , |x_0\rangle$
$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$
$D|\alpha\rangle = 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle$
$= 2(|\alpha\rangle - |\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle)$
$- |\alpha\rangle$
$= |\alpha\rangle - 2|\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle$
$|x_0\rangle$
$|\psi\rangle$
$|x_0^\perp\rangle$
θ
θ
$|\alpha\rangle$
$|\psi^\perp\rangle$

$|\psi\rangle, \ |x_0\rangle$

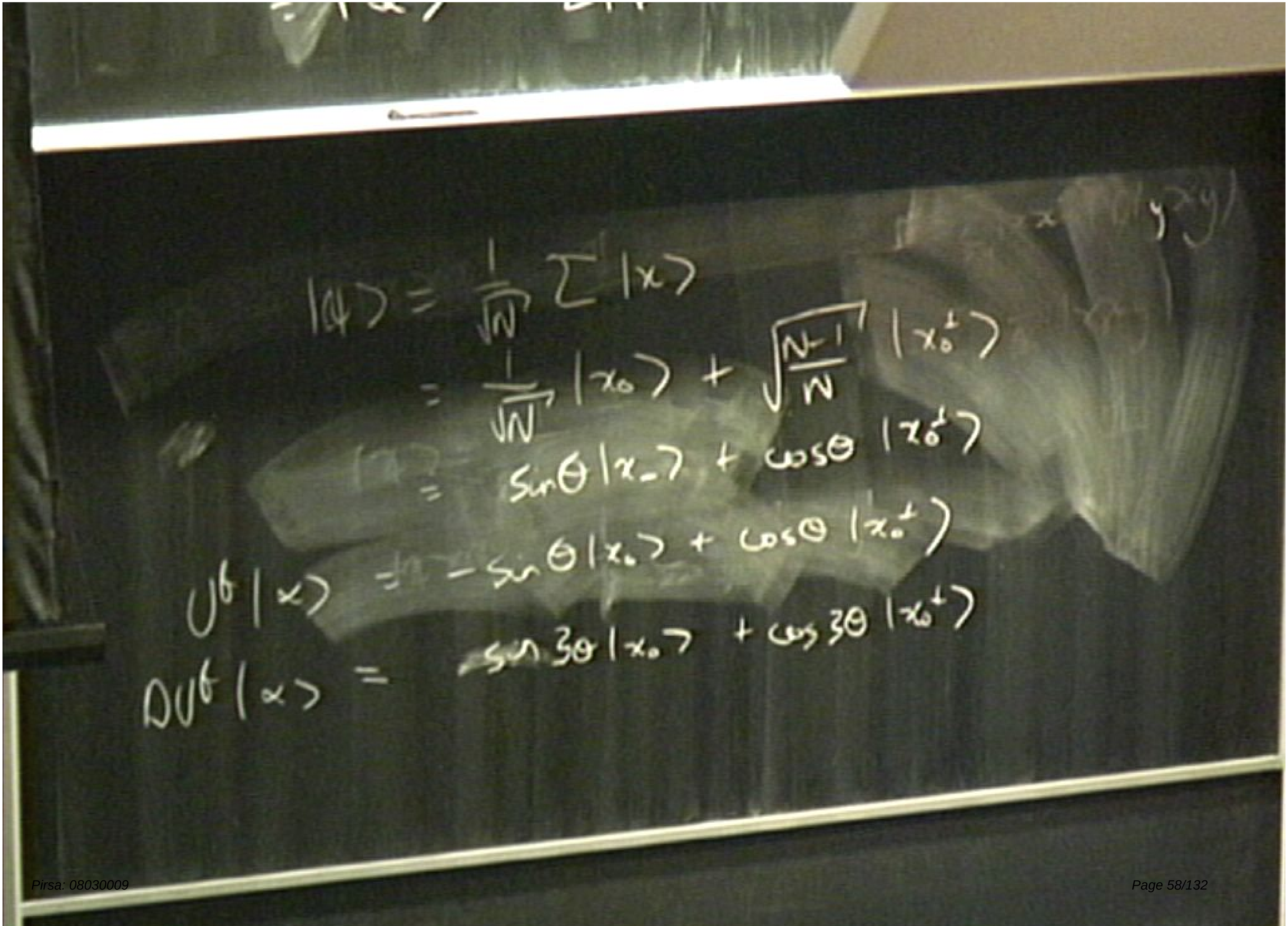


$$D = 2|\psi\rangle\langle\psi| - \mathbb{I}$$

$$D|\alpha\rangle = 2|\psi\rangle\langle\psi|\alpha\rangle - |\alpha\rangle$$

$$= 2\left(|\alpha\rangle - |\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle\right) - |\alpha\rangle$$

$$= |\alpha\rangle - 2|\psi^\perp\rangle\langle\psi^\perp|\alpha\rangle$$


|ψ> = 1/√N Σ|x>
= 1/√N |x₀> + √((N-1)/N) |x₀⊥>
= sinθ |x₀> + cosθ |x₀⊥>
U^f |ψ> = -sinθ |x₀> + cosθ |x₀⊥>
DU^f |ψ> = sin3θ |x₀> + cos3θ |x₀⊥>

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^{\perp}\rangle$$

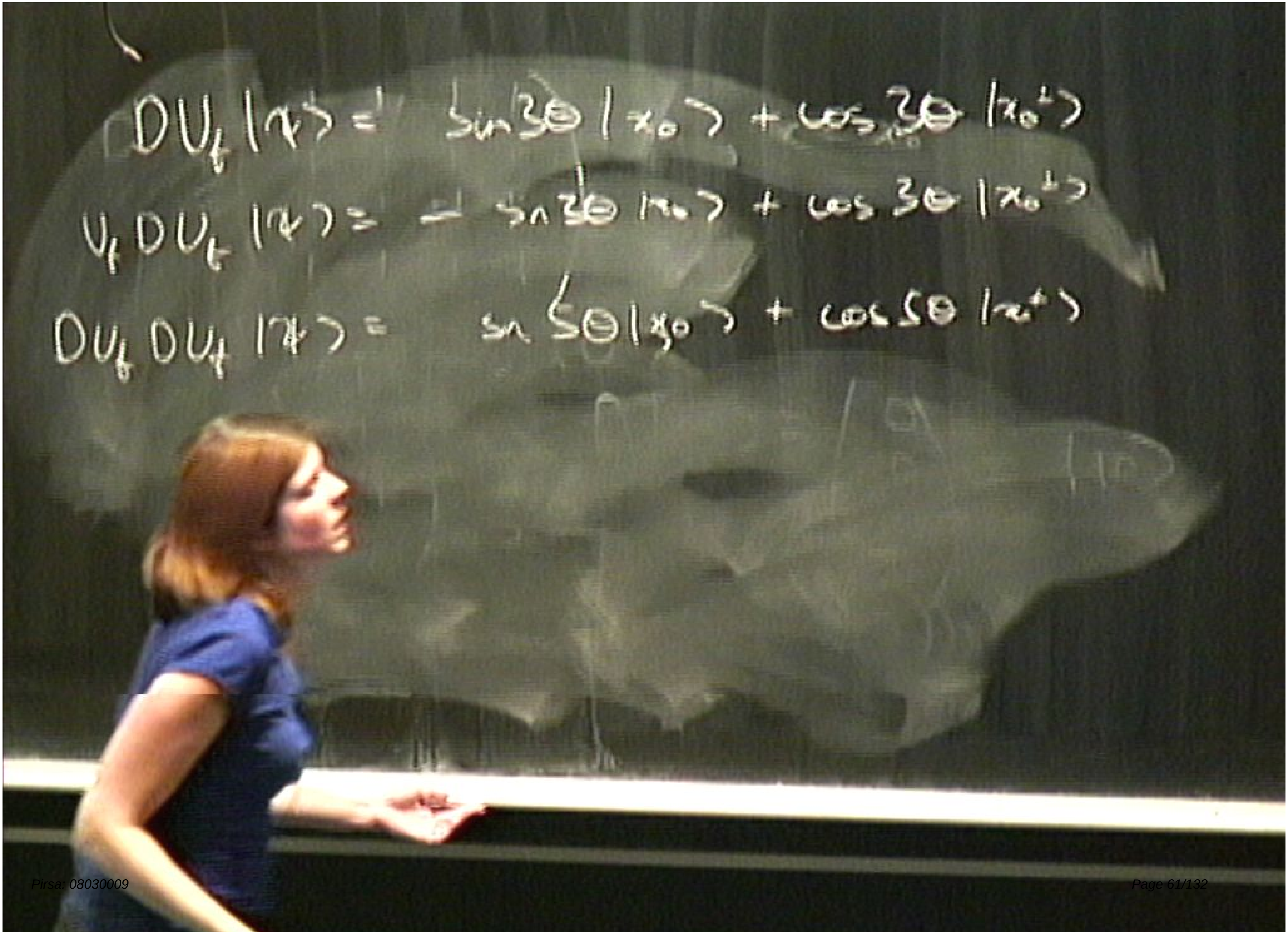
$$= \sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$U^f |\alpha\rangle = -\sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$DU^f |\alpha\rangle = \sin 3\theta |x_0\rangle + \cos 3\theta |x_0^{\perp}\rangle$$

$D U_t |\psi\rangle = \sin 3\theta \, |x_0\rangle + \cos 3\theta \, |x_0^\perp\rangle$

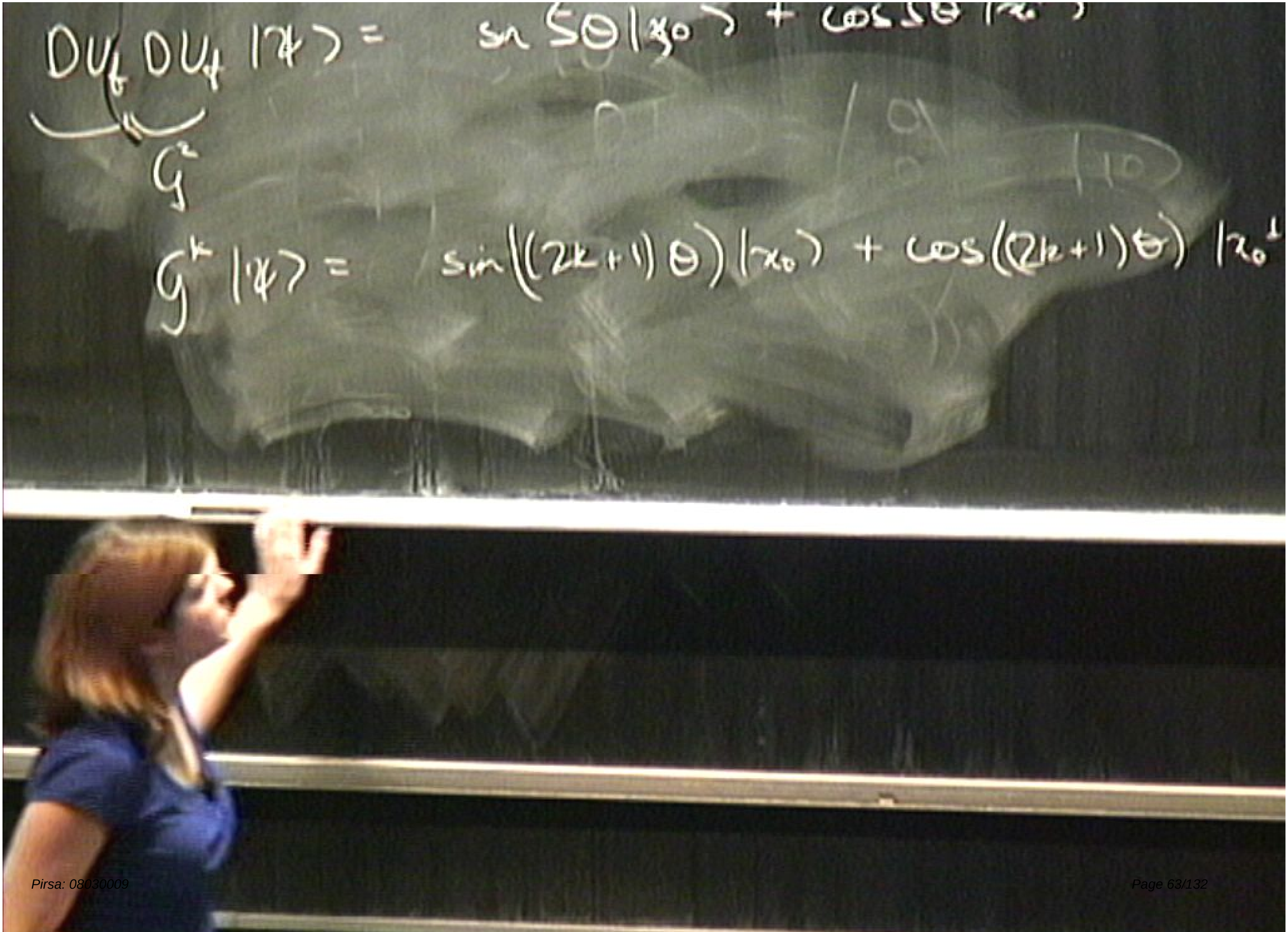
$U_t D U_t |\psi\rangle$


DU_t |ψ> = sin3θ |x_0> + cos3θ |x_0^⊥>
U_t DU_t |ψ> = sin3θ |x_0> + cos3θ |x_0^⊥>
DU_t DU_t |ψ> = sin5θ |x_0> + cos5θ |x_0^⊥>

$$D U_t |\psi\rangle = \sin 3\theta \, |x_0\rangle + \cos 3\theta \, |x_0^\perp\rangle$$

$$U_t D U_t |\psi\rangle = -\sin 3\theta \, |x_0\rangle + \cos 3\theta \, |x_0^\perp\rangle$$

$$\underbrace{D U_t}\underbrace{D U_t}_{G} |\psi\rangle = \sin 5\theta \, |x_0\rangle + \cos 5\theta \, |x_0^\perp\rangle$$


$DU_f DU_f |\psi\rangle = \sin 5\theta |x_0\rangle + \cos 5\theta |x_0'\rangle$
G^2
$G^k |\psi\rangle = \sin((2k+1)\theta) |x_0\rangle + \cos((2k+1)\theta) |x_0'\rangle$

$$DU_f\, DU_f\, |\psi\rangle = \sin 5\theta\, |x_0\rangle + \cos 5\theta\, |x_0^{\perp}\rangle$$

$$G^2$$

$$G^k |\psi\rangle = \sin\big((2k+1)\theta\big)\, |x_0\rangle + \cos\big((2k+1)\theta\big)\, |x_0^{\perp}\rangle$$

$DU_f\, DU_f\, |\psi\rangle$

G^2

$$G^k|\psi\rangle = \sin((2k+1)\theta)\,|x_0\rangle + \cos((2k+1)\theta)\,|x_0^\perp\rangle$$

$$P(x_0) = |\langle x_0|G^k|\psi\rangle|^2 = \sin^2((2k+1)\theta)$$

$$D = 2|\psi\rangle\langle\psi| - \mathbb{1}$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$= \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^{\perp}\rangle$$

$$= \sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$U_f |\psi\rangle = -\sin\theta |x_0\rangle + \cos\theta |x_0^{\perp}\rangle$$

$$D U_f |\psi\rangle = \sin 3\theta |x_0\rangle + \cos 3\theta |x_0^{\perp}\rangle$$

$$|\alpha\rangle = U^b|\alpha\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$$

$$= \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}\,|x_0^\perp\rangle$$

$$= \sin\theta\,|x_0\rangle + \cos\theta\,|x_0^\perp\rangle$$

$$U^b|\psi\rangle = -\sin\theta\,|x_0\rangle + \cos\theta\,|x_0^\perp\rangle$$

$$DU^b|\psi\rangle = \sin 3\theta\,|x_0\rangle + \cos 3\theta\,|x_0^\perp\rangle$$

$$\sin^2((2k+1)\theta) \simeq 1$$

$$\Rightarrow (2k+1)\theta \simeq \pi/2$$

$$\sin^2((2k+1)\theta) \simeq 1$$

$$\Rightarrow (2k+1)\theta \simeq \pi/2$$

$$k = \pi/4\theta - \frac{1}{2}$$

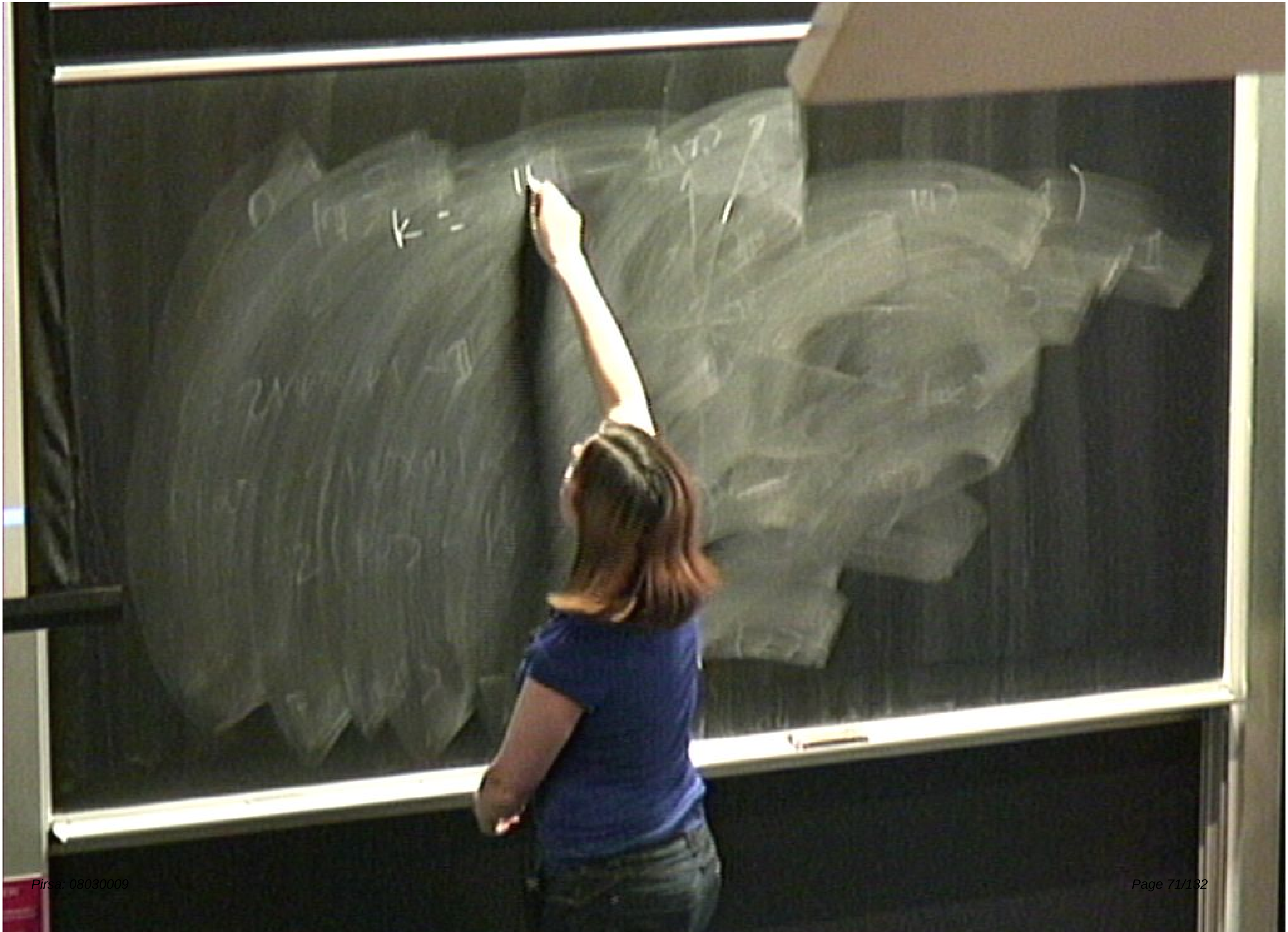
$$\sin^2((2k+1)\theta) \simeq 1$$

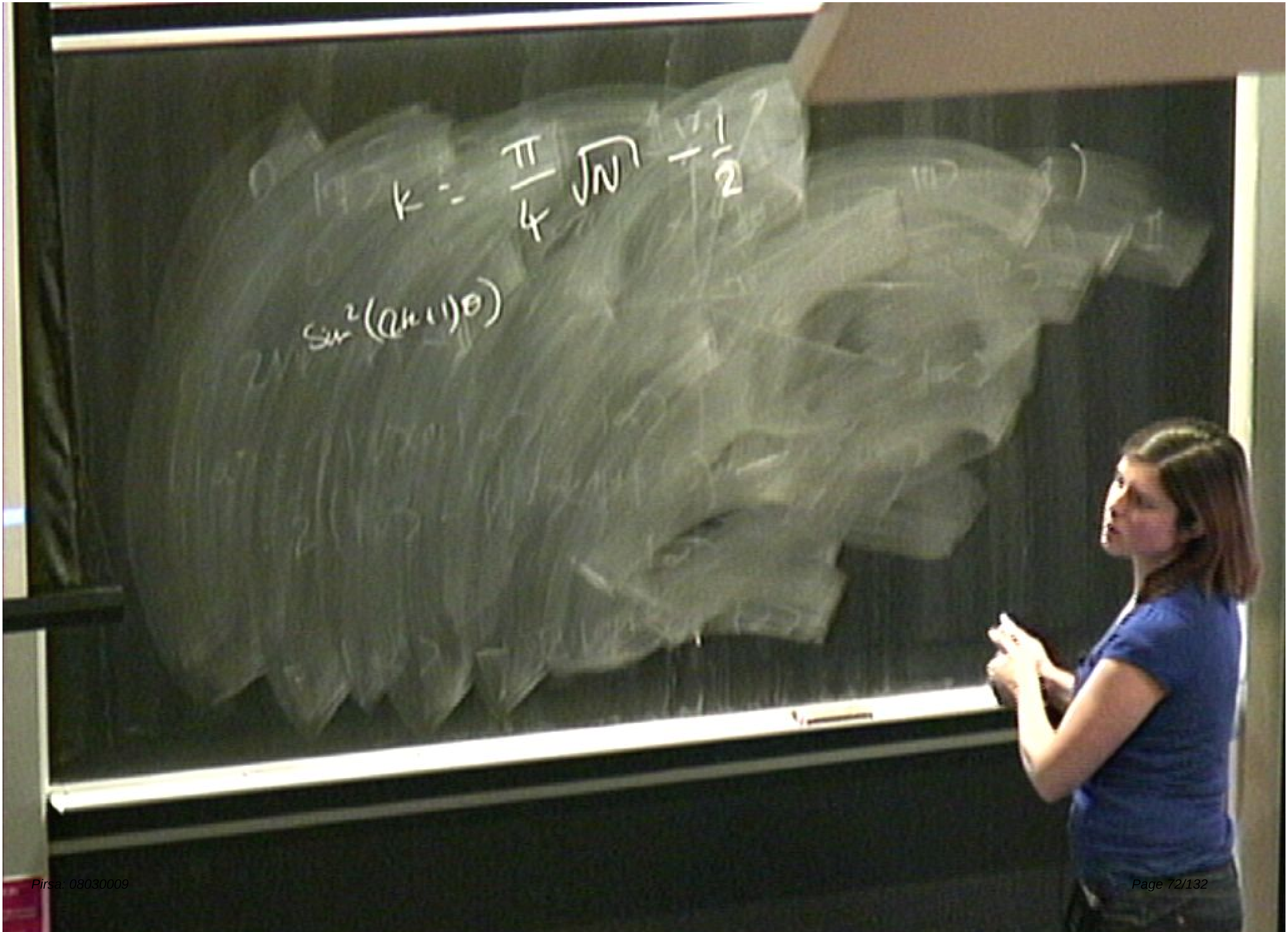
$$\Rightarrow (2k+1)\theta \simeq \pi/2$$

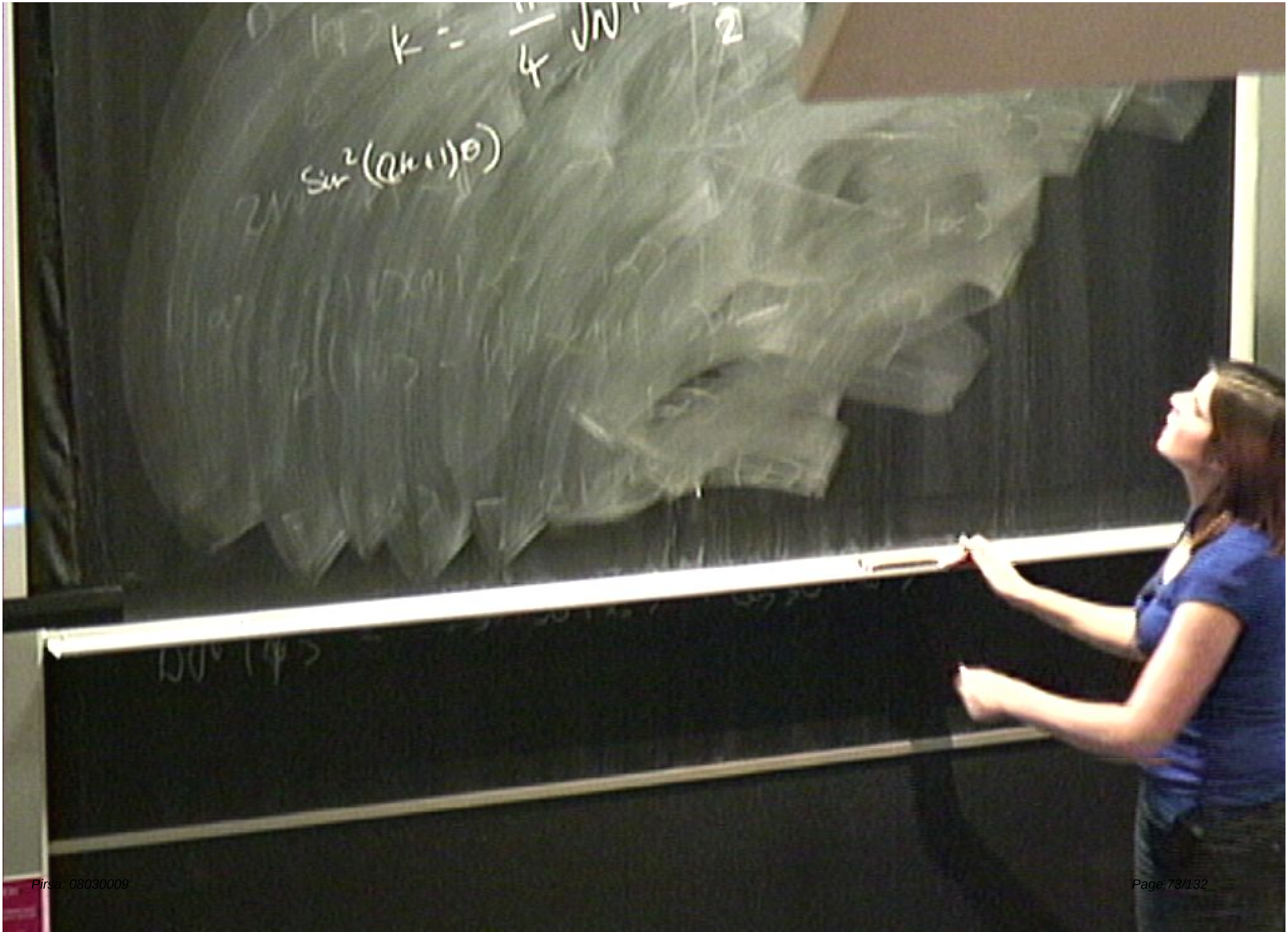
$$k = \pi/4\theta - \frac{1}{2}$$

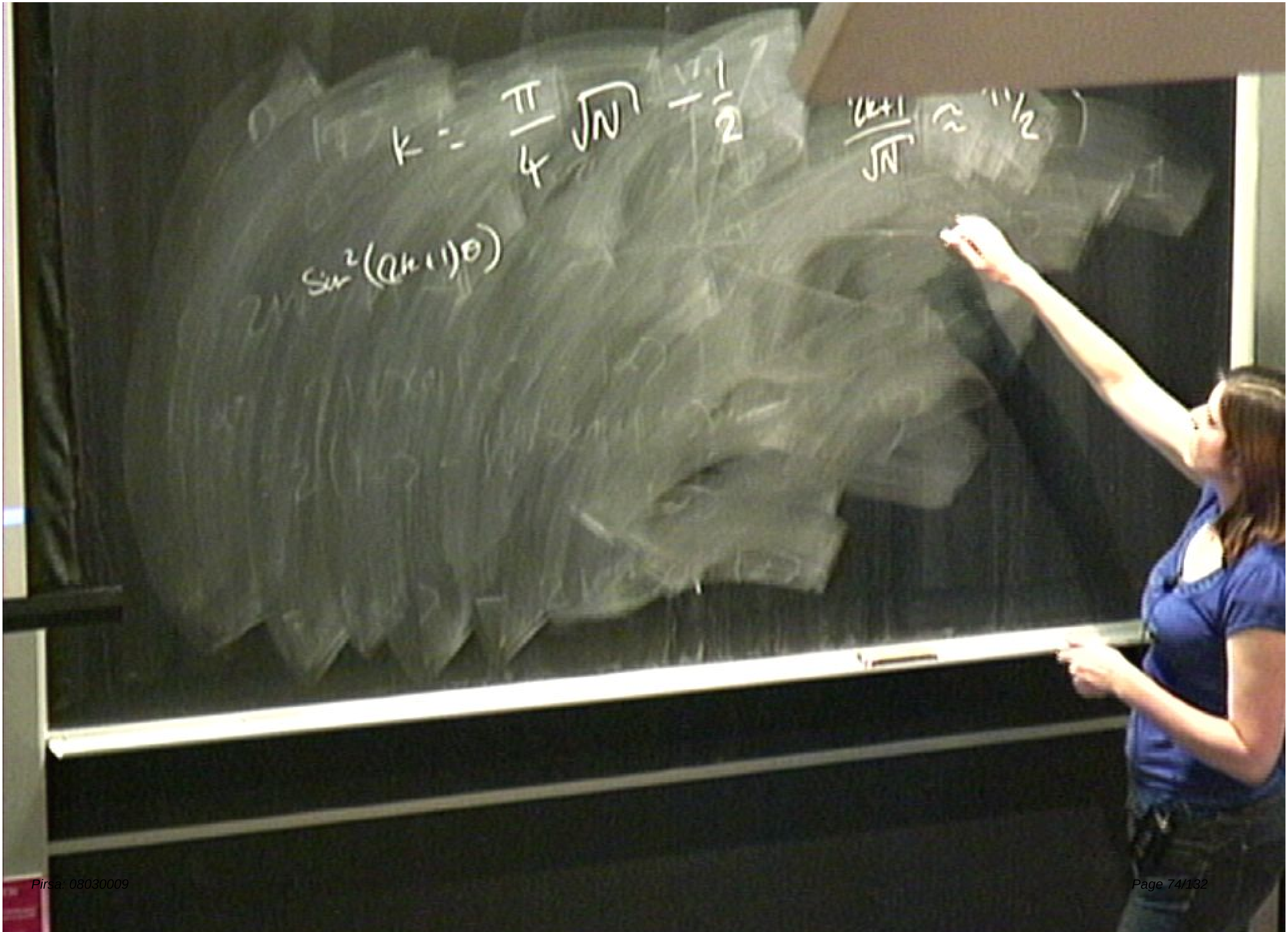
$$\sin\theta = 1/\sqrt{N}, \quad \theta \simeq 1/\sqrt{N}$$

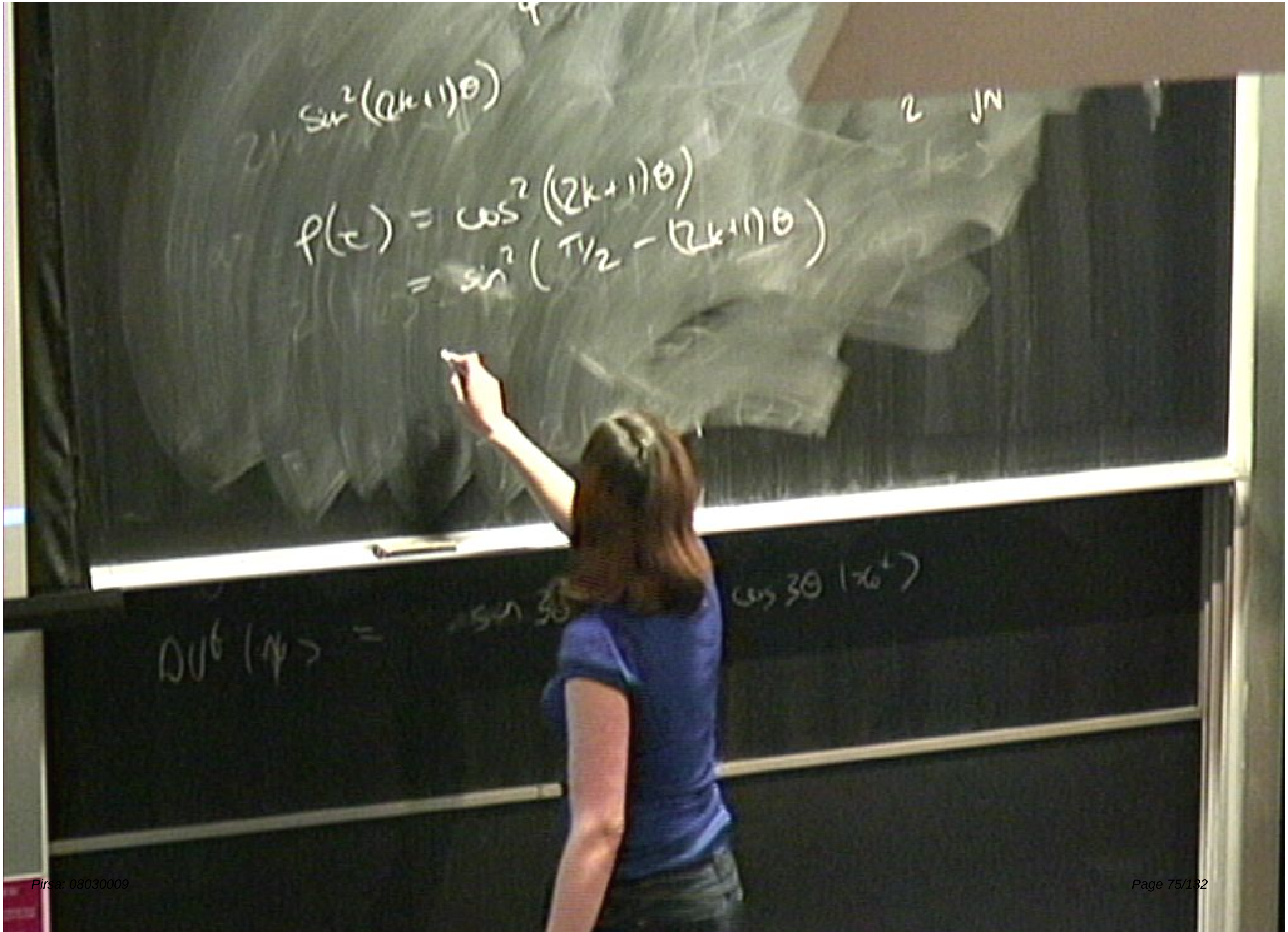
$$\Rightarrow k = \pi/4\sqrt{N} - 1/2 = O(\sqrt{N})$$

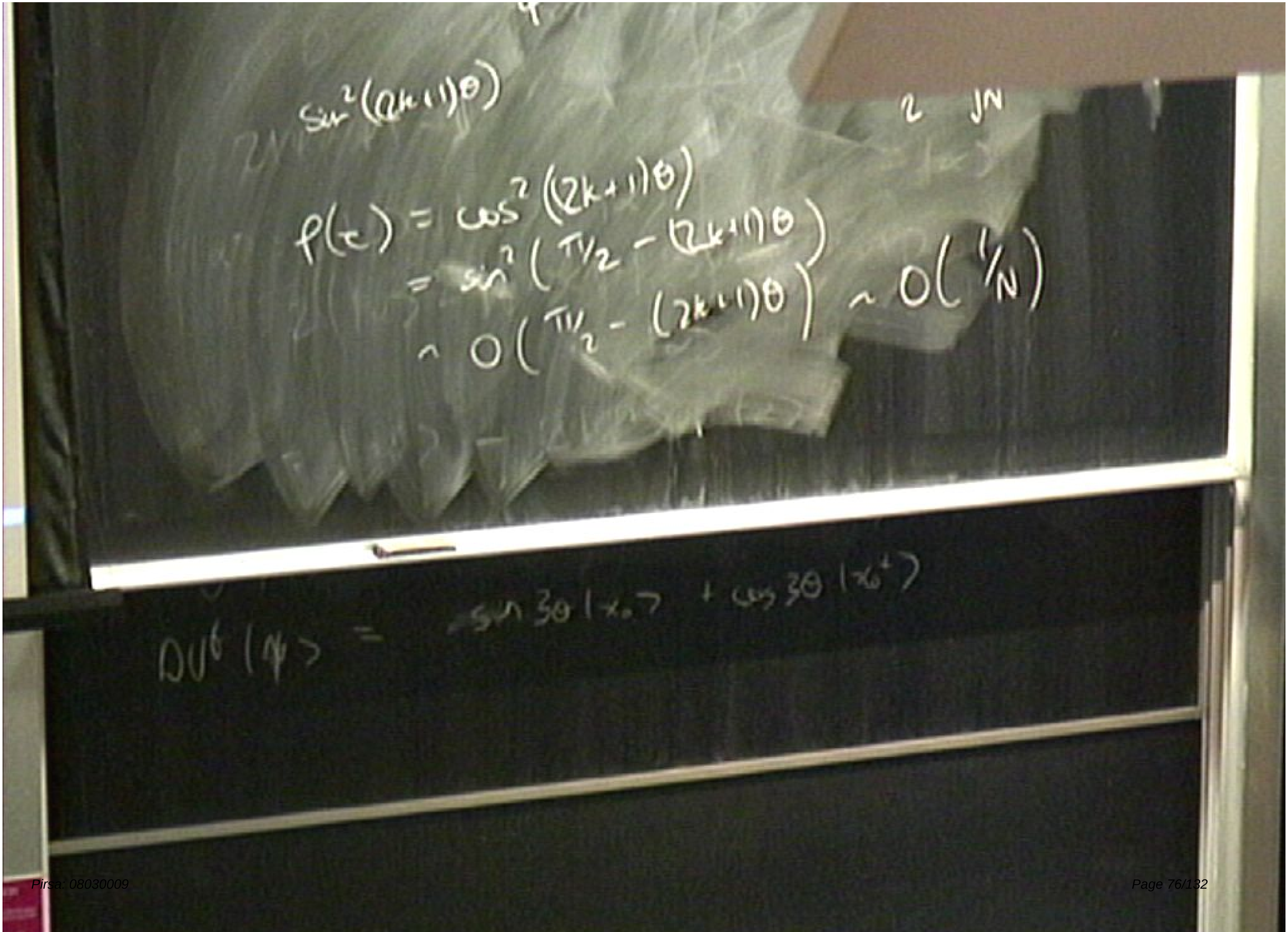



$k = \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$
$\sin^2((2k+1)\theta)$


sin^2((2k+1)θ)


k = π/4 √N − 1/2
sin²((2k+1)θ)


sin²((2k+1)θ)
2 √N
ρ(t) = cos²((2k+1)θ)
= sin²(π/2 − (2k+1)θ)
cos 3θ |ψ⁺⟩


sin²((2k+1)θ)
2 √N
P(c) = cos²((2k+1)θ)
= sin²(π/2 − (2k+1)θ)
~ O(π/2 − (2k+1)θ) ~ O(1/N)
DU⁶ |ψ> = sin 3θ |x₀> + cos 3θ |x₀⊥>

$$U_f |x\rangle|0\rangle \to |x\rangle|f(x)\rangle$$

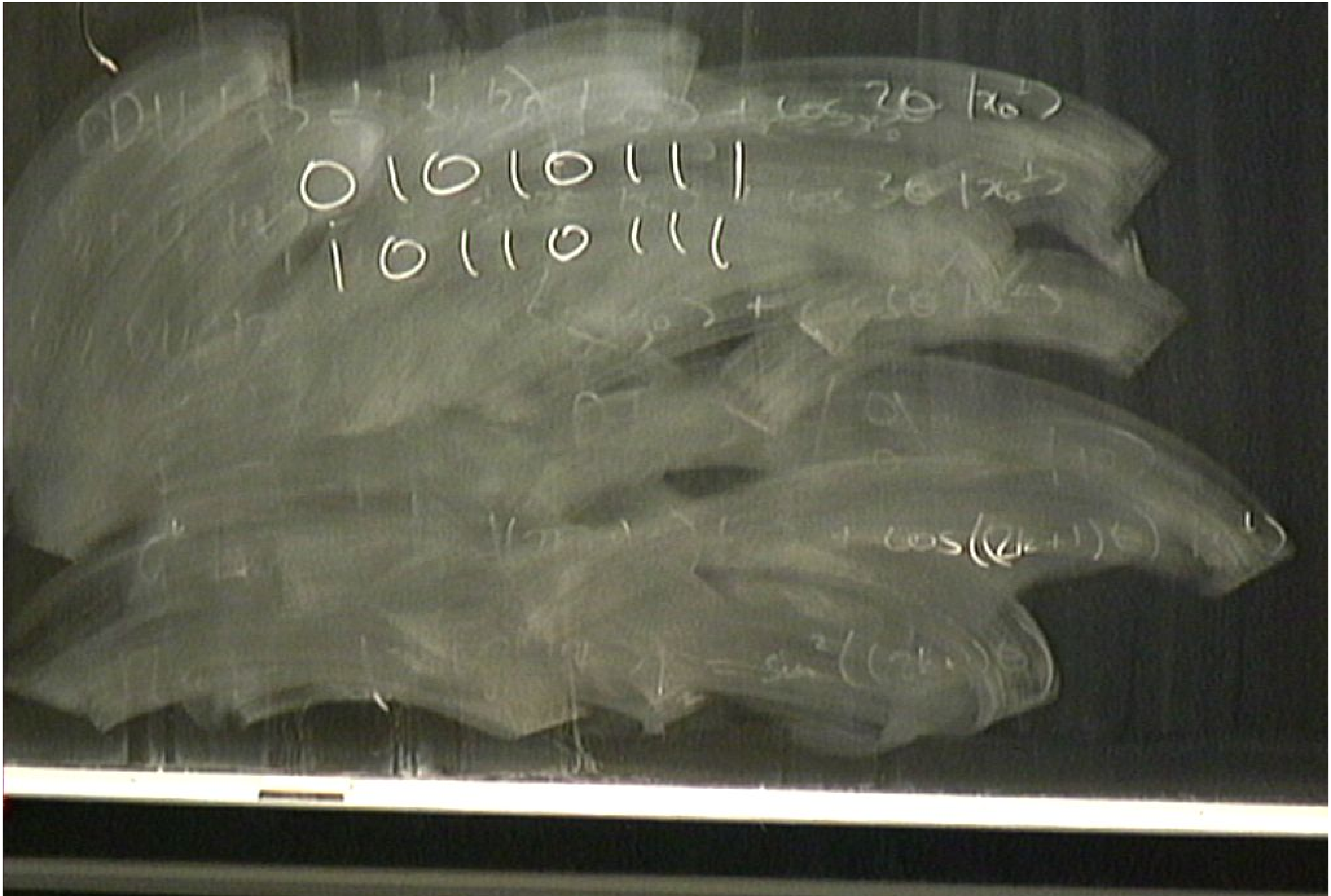
$$D = 2|\psi\rangle\langle\psi| - \mathbb{I}$$

Computational Complexity

- Problems which can be solved in a time polynomial in the size of the input (i.e. the number of bits needed to store the input) are in the complexity class P, e.g. multiplication.
- (Classical) Strong Church-Turing thesis: A probabilistic Turing machine can efficiently simulate any realistic model of computation.
- Problems whose solution can be verified in polynomial time are in the complexity class NP e.g. factorisation.
- Not known if P=NP. (It is conjectured, but not proven, that this is not the case).
- NP-complete problems, e.g. travelling salesman.

Computational Complexity

- Problems which can be solved in a time polynomial in the size of the input (i.e. the number of bits needed to store the input) are in the complexity class P, e.g. multiplication.
- (Classical) Strong Church-Turing thesis: A probabilistic Turing machine can efficiently simulate any realistic model of computation.
- Problems whose solution can be verified in polynomial time are in the complexity class NP e.g. factorisation.
- Not known if P=NP. (It is conjectured, but not proven, that this is not the case).
- NP-complete problems, e.g. travelling salesman.


01010111
10110111

Computational Complexity

- Problems which can be solved in a time polynomial in the size of the input (i.e. the number of bits needed to store the input) are in the complexity class P, e.g. multiplication.
- (Classical) Strong Church-Turing thesis: A probabilistic Turing machine can efficiently simulate any realistic model of computation.
- Problems whose solution can be verified in polynomial time are in the complexity class NP e.g. factorisation.
- Not known if P=NP. (It is conjectured, but not proven, that this is not the case).
- NP-complete problems, e.g. travelling salesman.

Shor's Algorithm

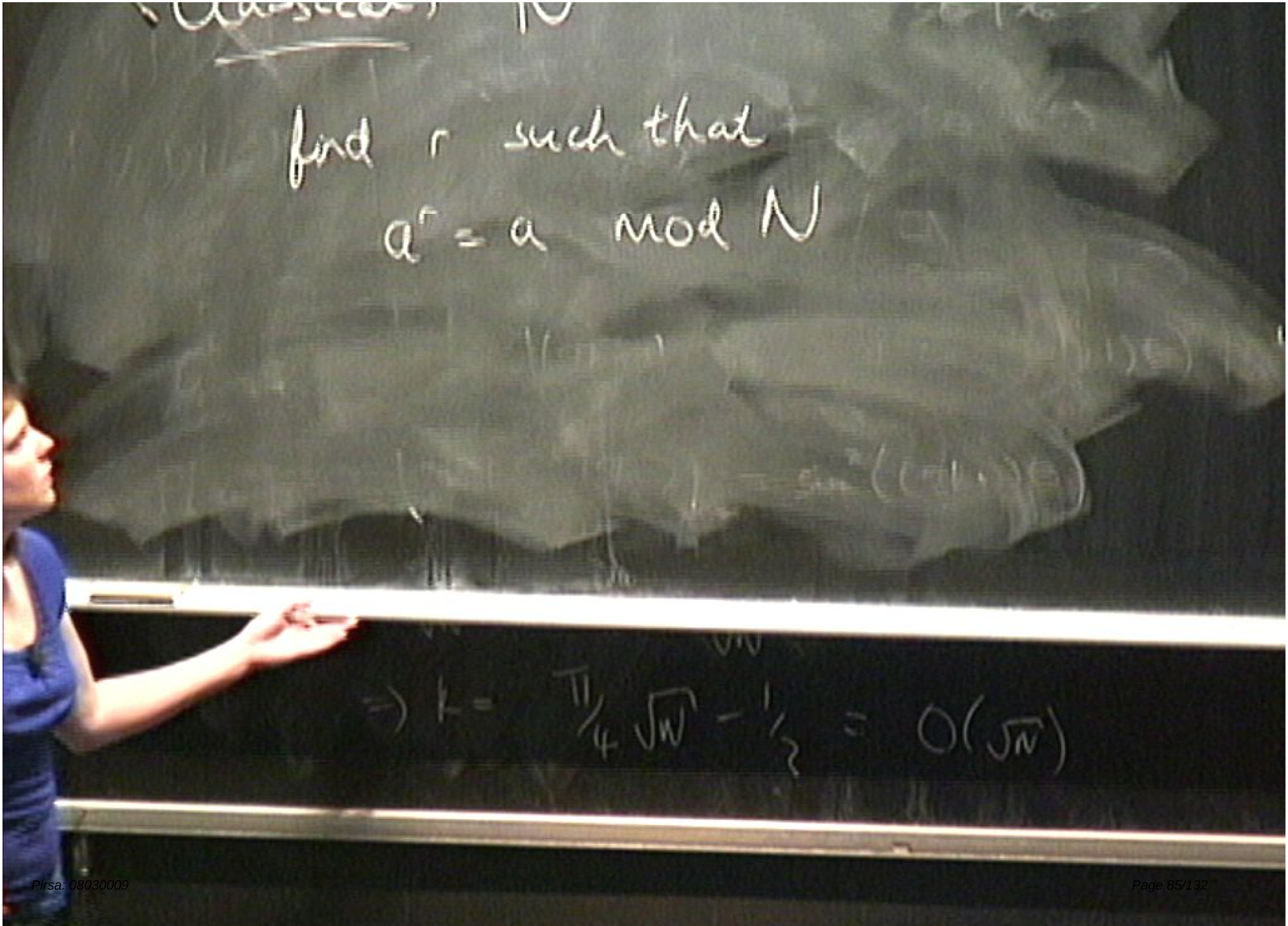
- Integer factorization algorithm. Believed to be computationally hard classically, which is important for security of RSA public key cryptography.
- Best known classical algorithm requires $\exp(O((\log N)^{1/3}(\log \log N)^{2/3}$ gates.
- Shor's algorithm requires a number of gates which is polynomial in input size (polynomial in log N).
- Shor's algorithm is probabilistic.

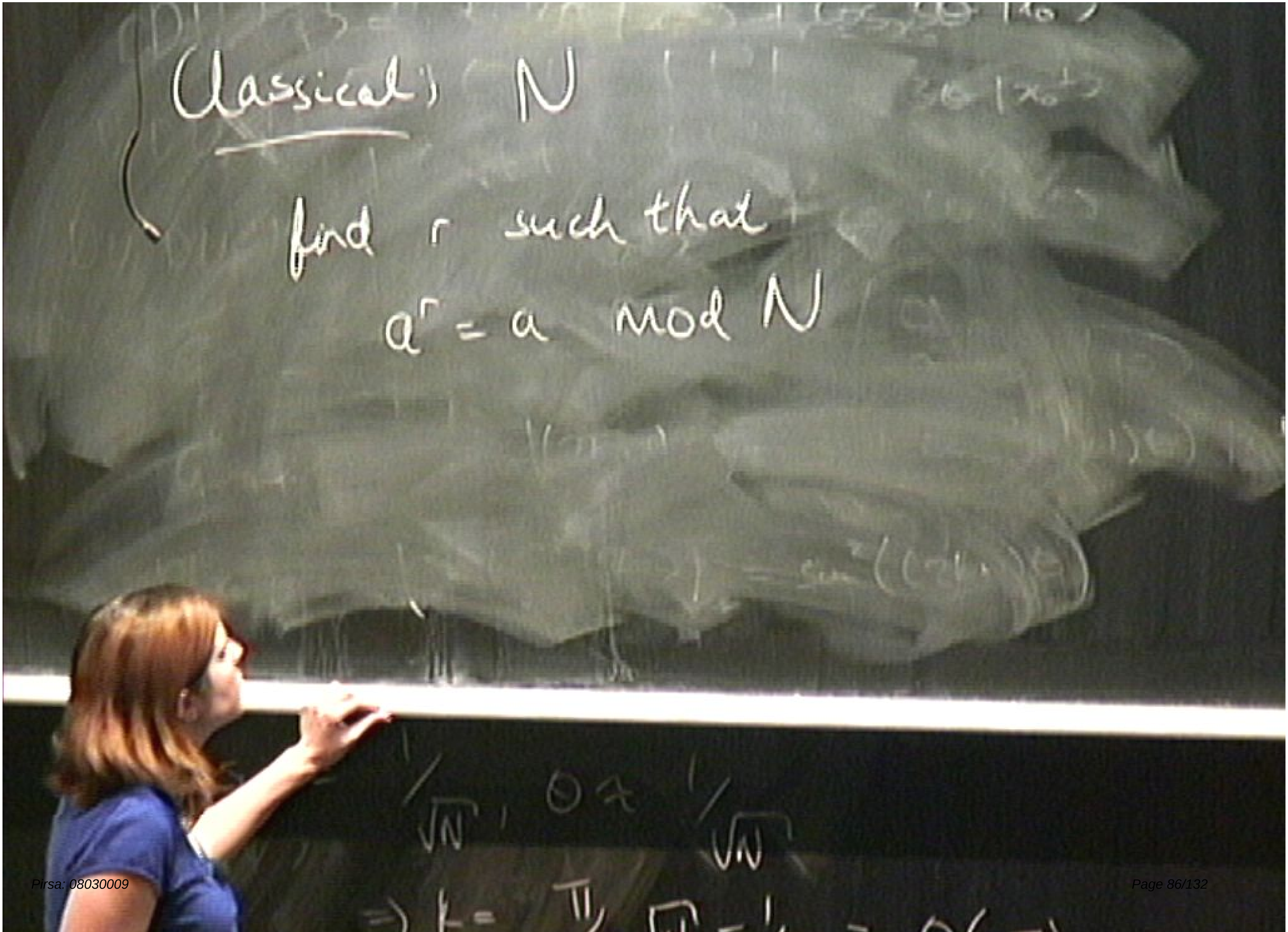
Decoherence and Scalability

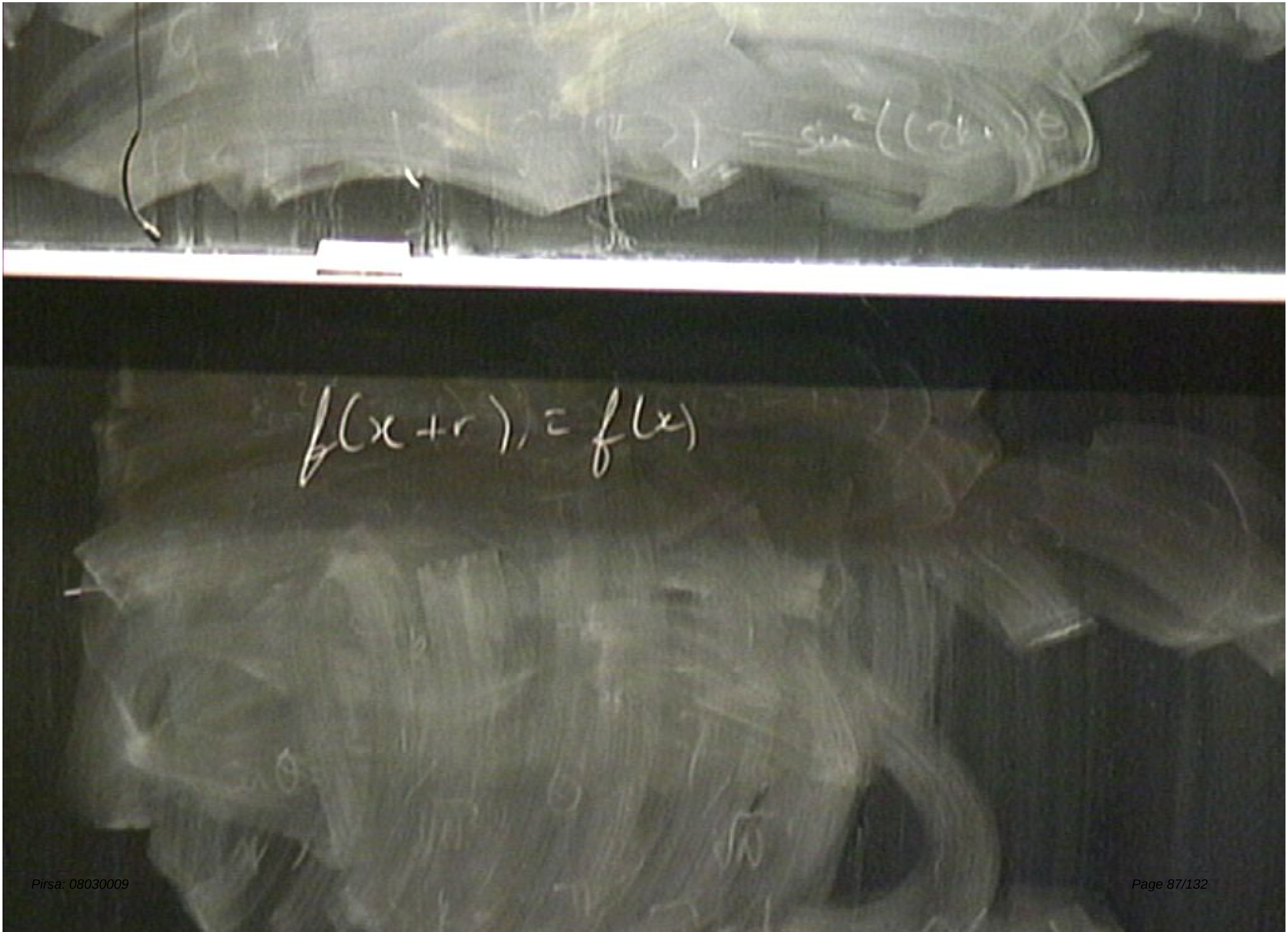
- Have assumed unitary transformations, in the presence of an environment this is not the case.
- Interactions with an environment partially corrupt the information encoded in quantum states.
- Fault-tolerant quantum computation possible if probability of single gate error is below a certain threshold level.
- Is there a scale at which the world stops behaving quantum mechanically?

Shor's Algorithm

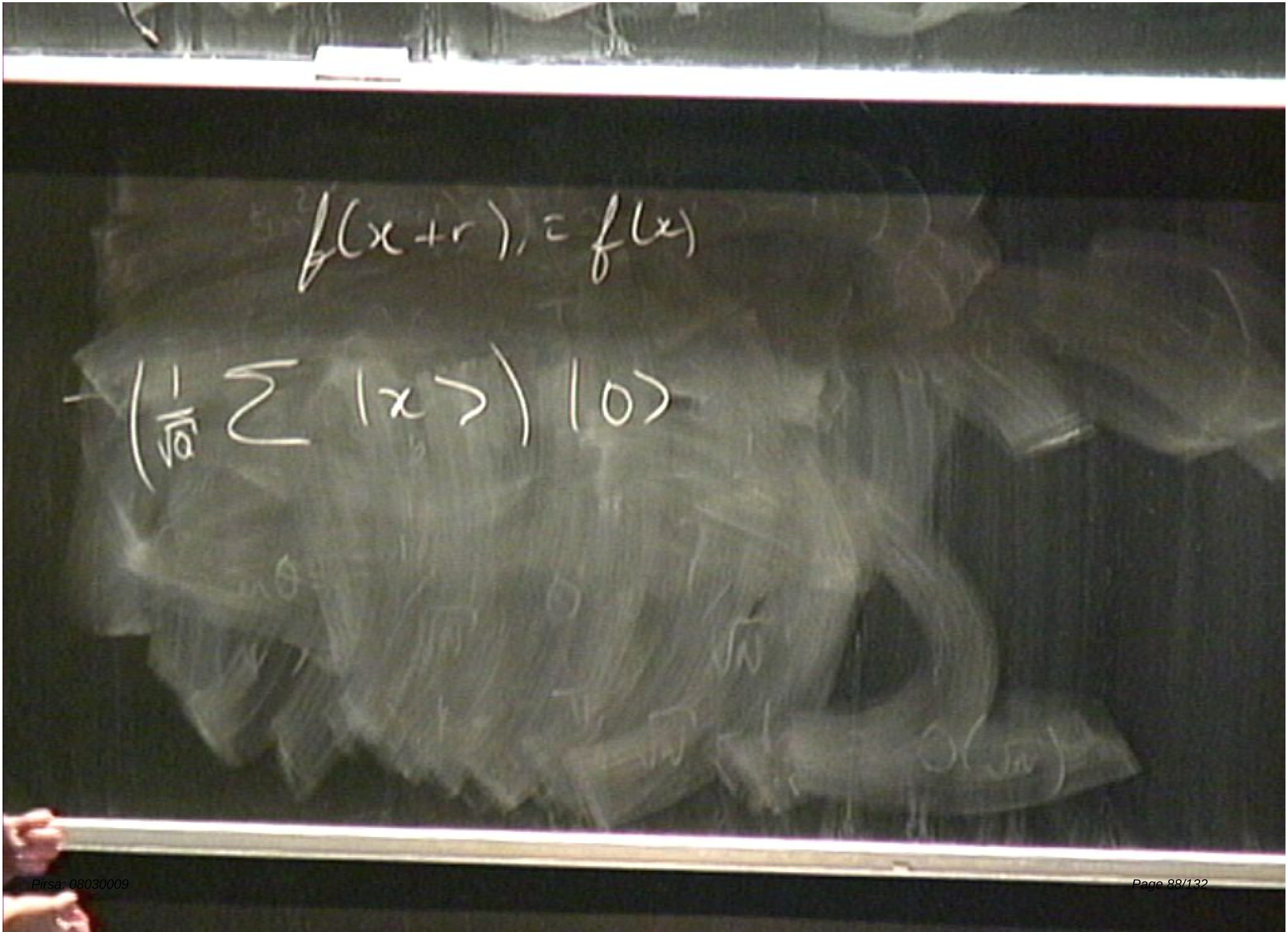
- Integer factorization algorithm. Believed to be computationally hard classically, which is important for security of RSA public key cryptography.
- Best known classical algorithm requires $\exp(O((\log N)^{1/3}(\log \log N)^{2/3}$ gates.
- Shor's algorithm requires a number of gates which is polynomial in input size (polynomial in log N).
- Shor's algorithm is probabilistic.

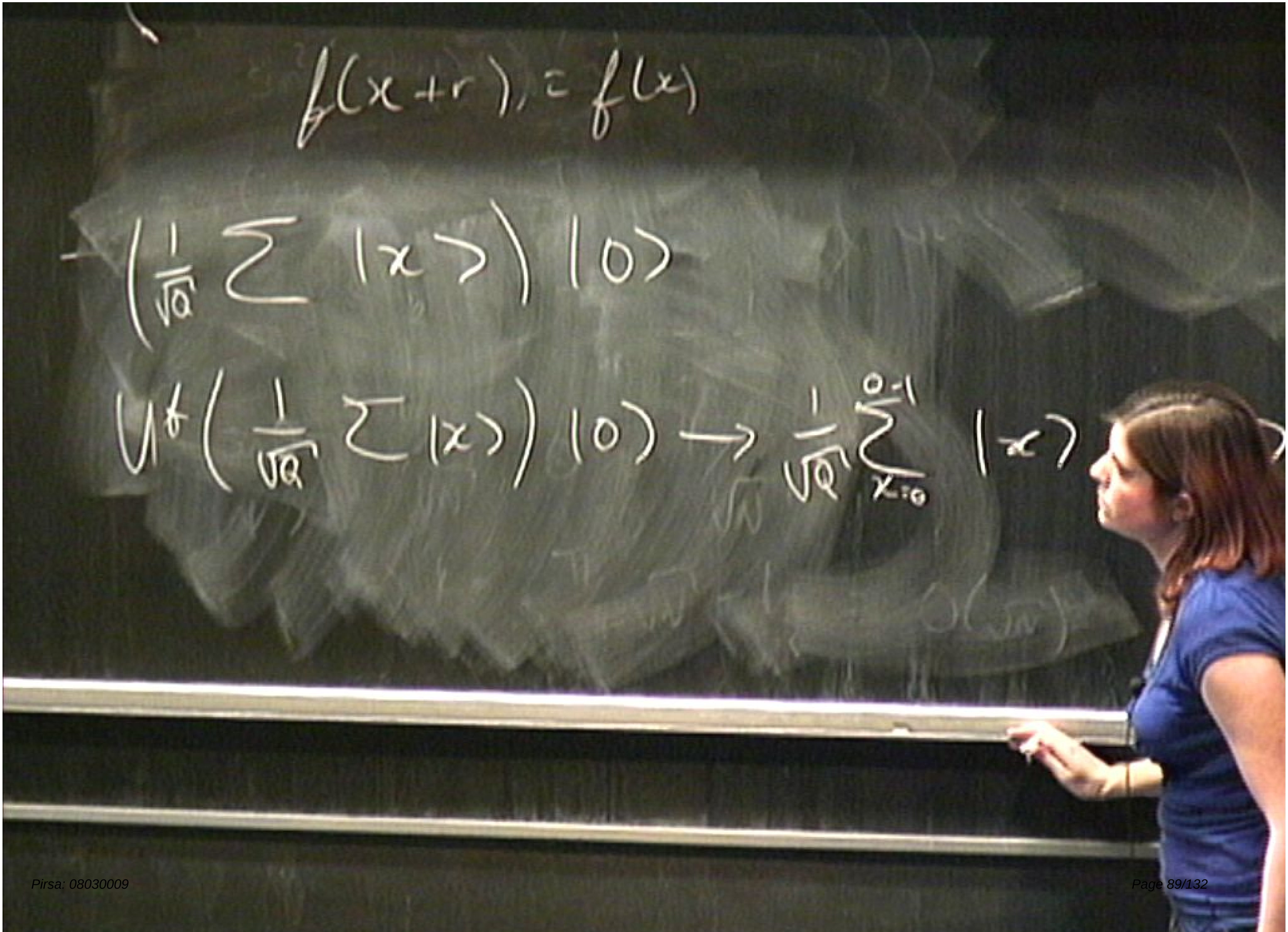

find r such that
a^r = a mod N
=> k = π/4 √N - 1/2 = O(√N)

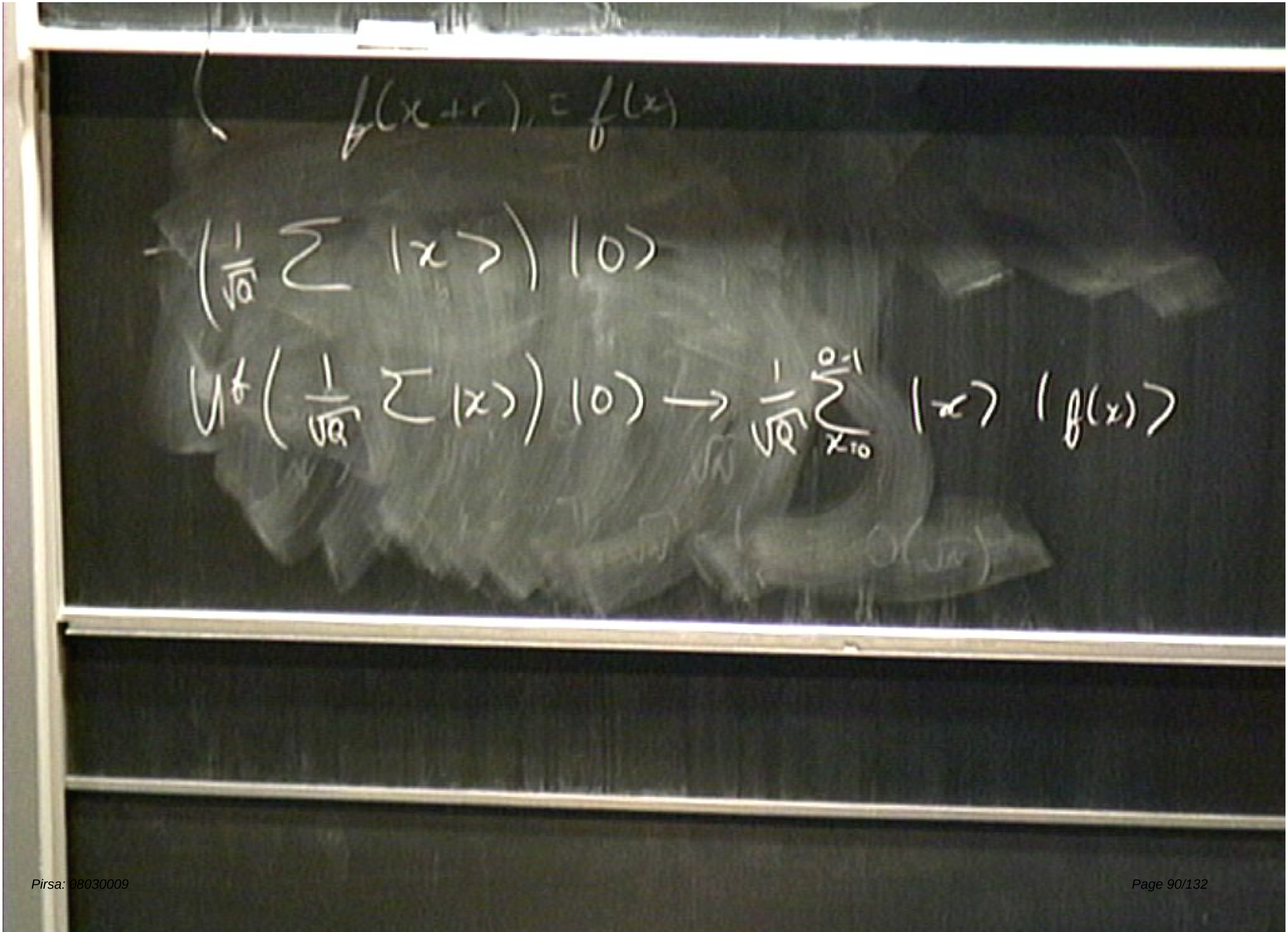

Classical: N
find r such that
a^r = a mod N
1/√N , θ ≈ 1/√N

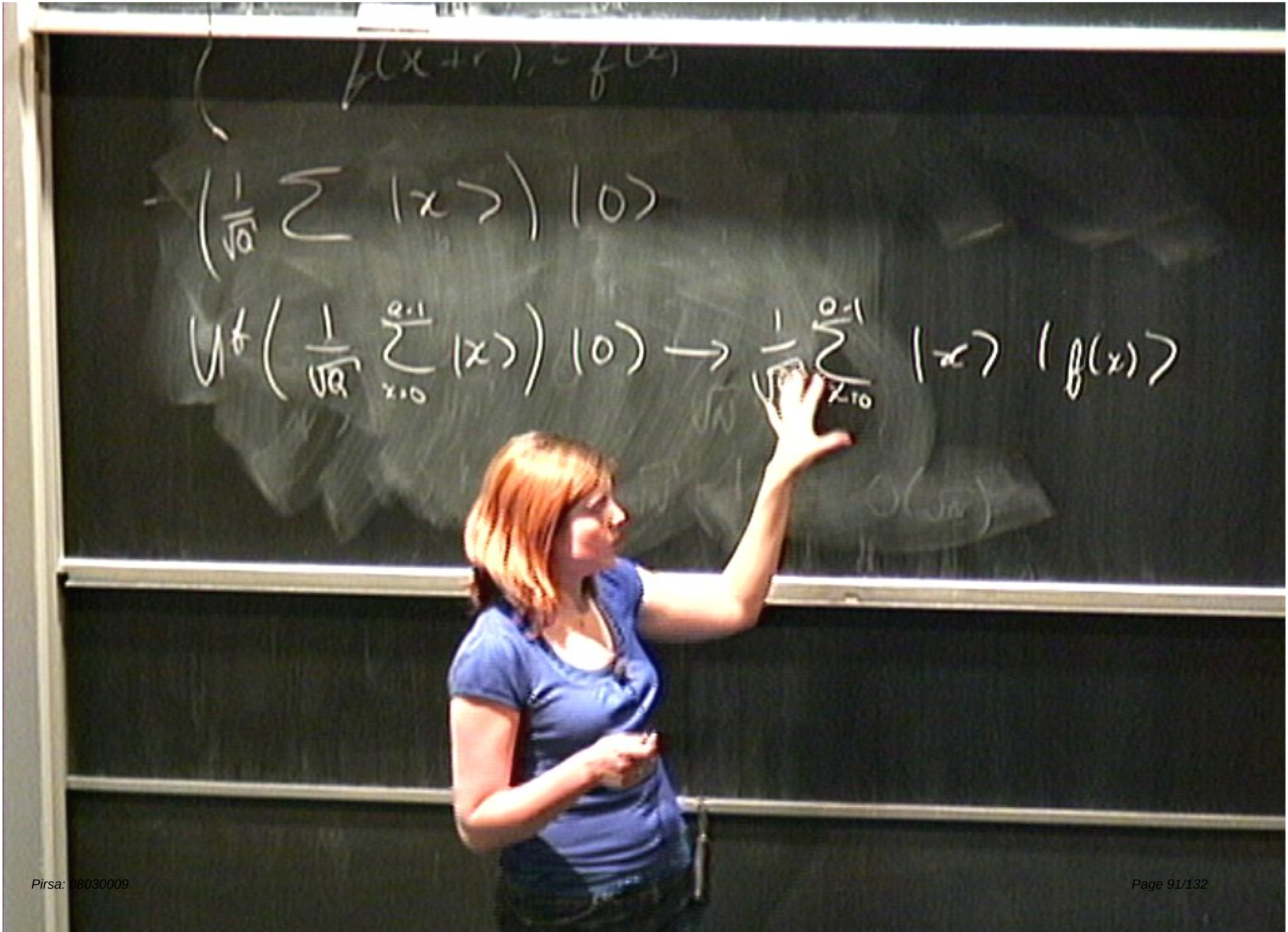


f(x+r) = f(x)


$f(x+r) = f(x)$
$\left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right) |0\rangle$


$f(x+r) = f(x)$
$\left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right)|0\rangle$
$U_f\left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right)|0\rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle$

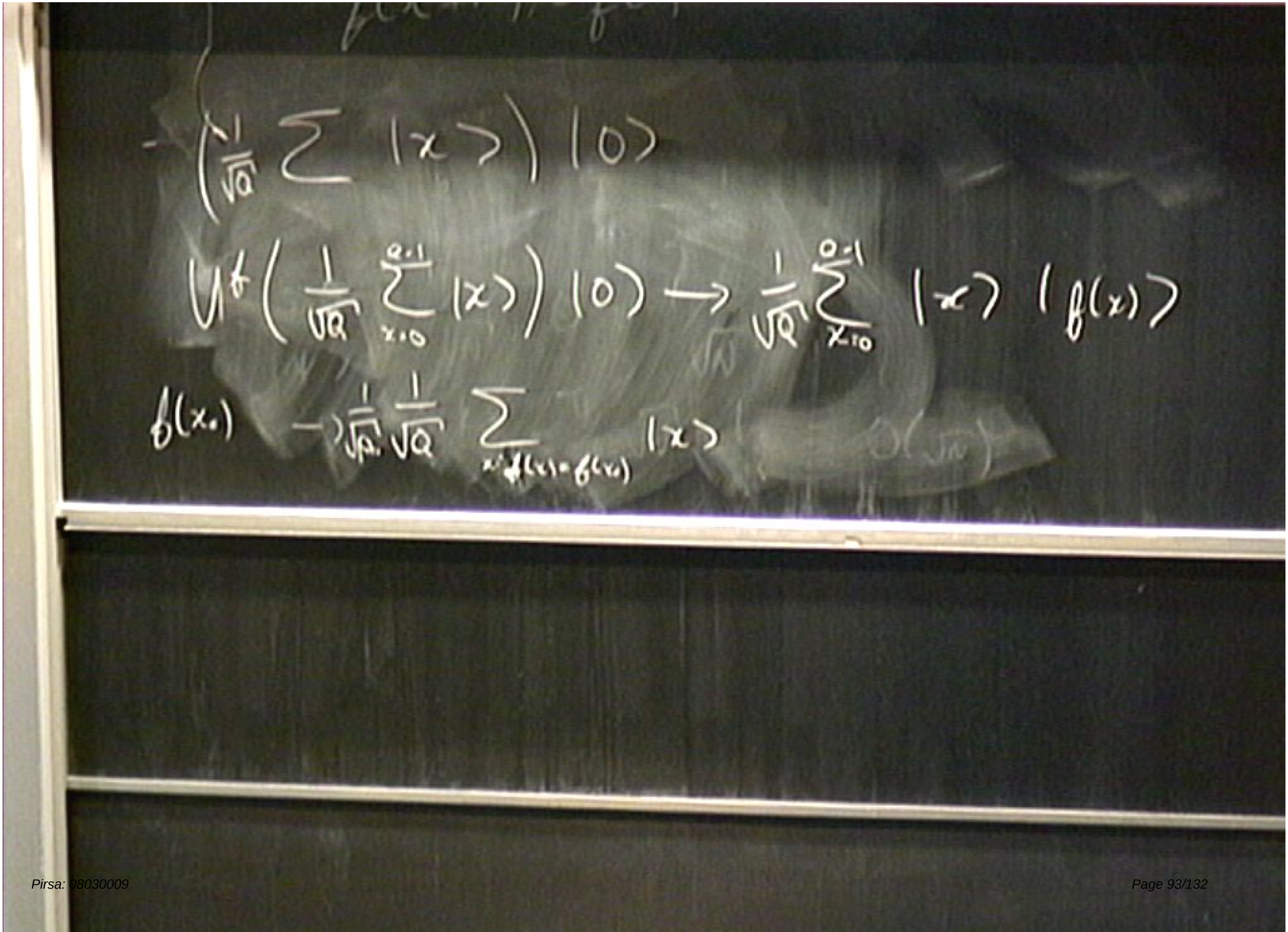

$f(x+r) = f(x)$
$\left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right) |0\rangle$
$U_f \left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right) |0\rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$

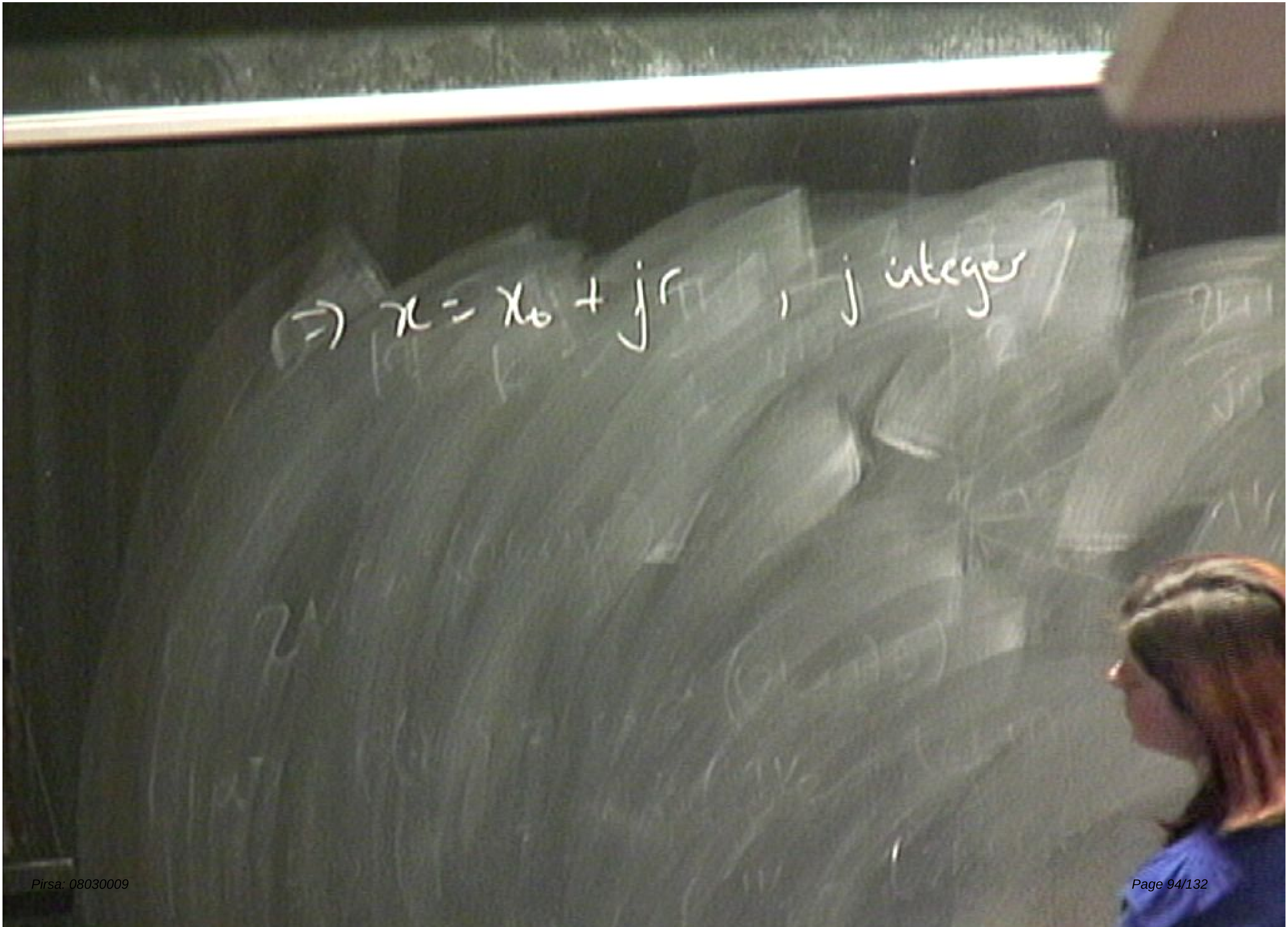

$\left(\frac{1}{\sqrt{Q}} \sum |x\rangle\right)|0\rangle$
$U_f\left(\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle\right)|0\rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|f(x)\rangle$

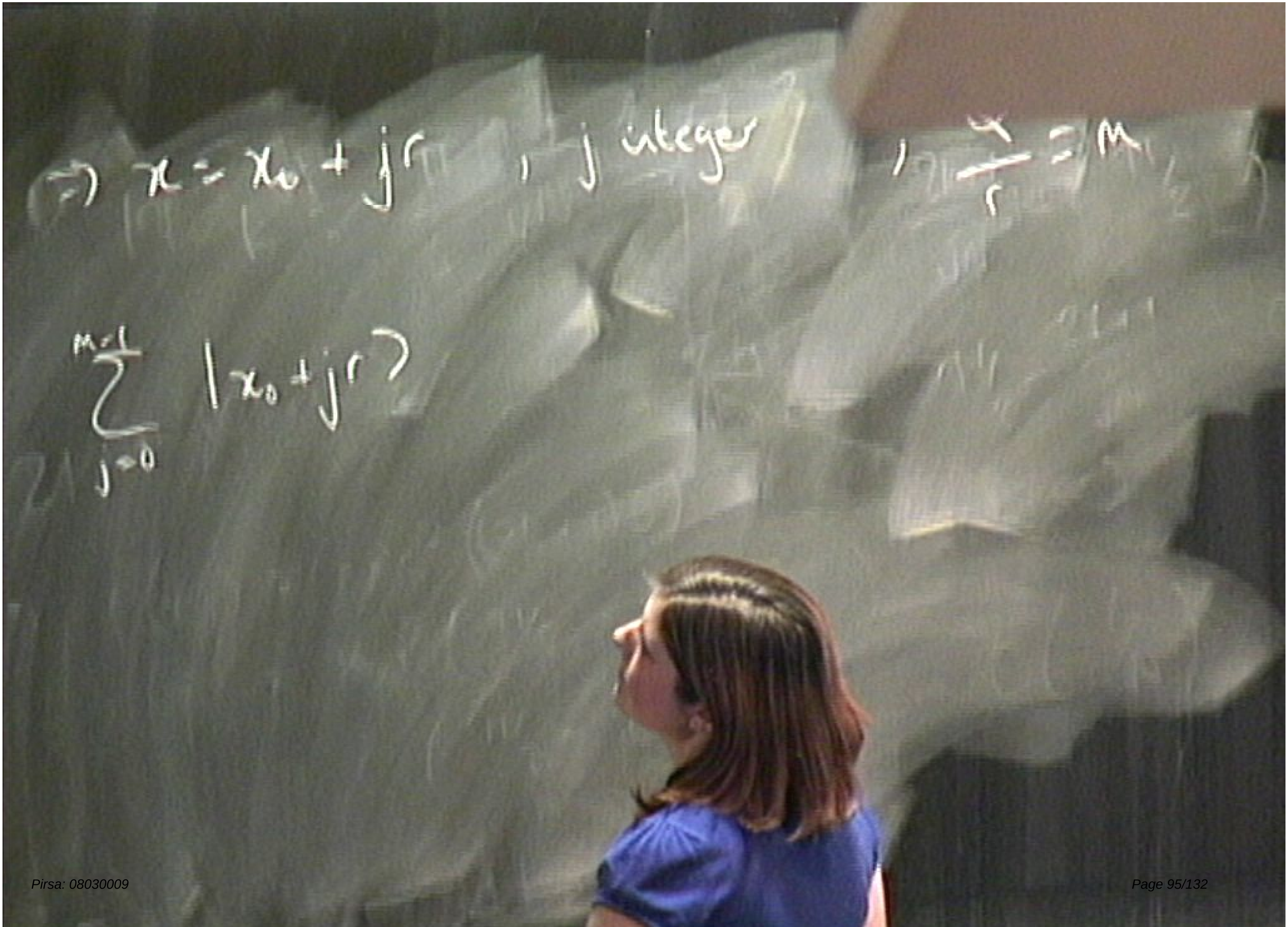
$$\left(\frac{1}{\sqrt{Q}}\sum |x\rangle\right)|0\rangle$$

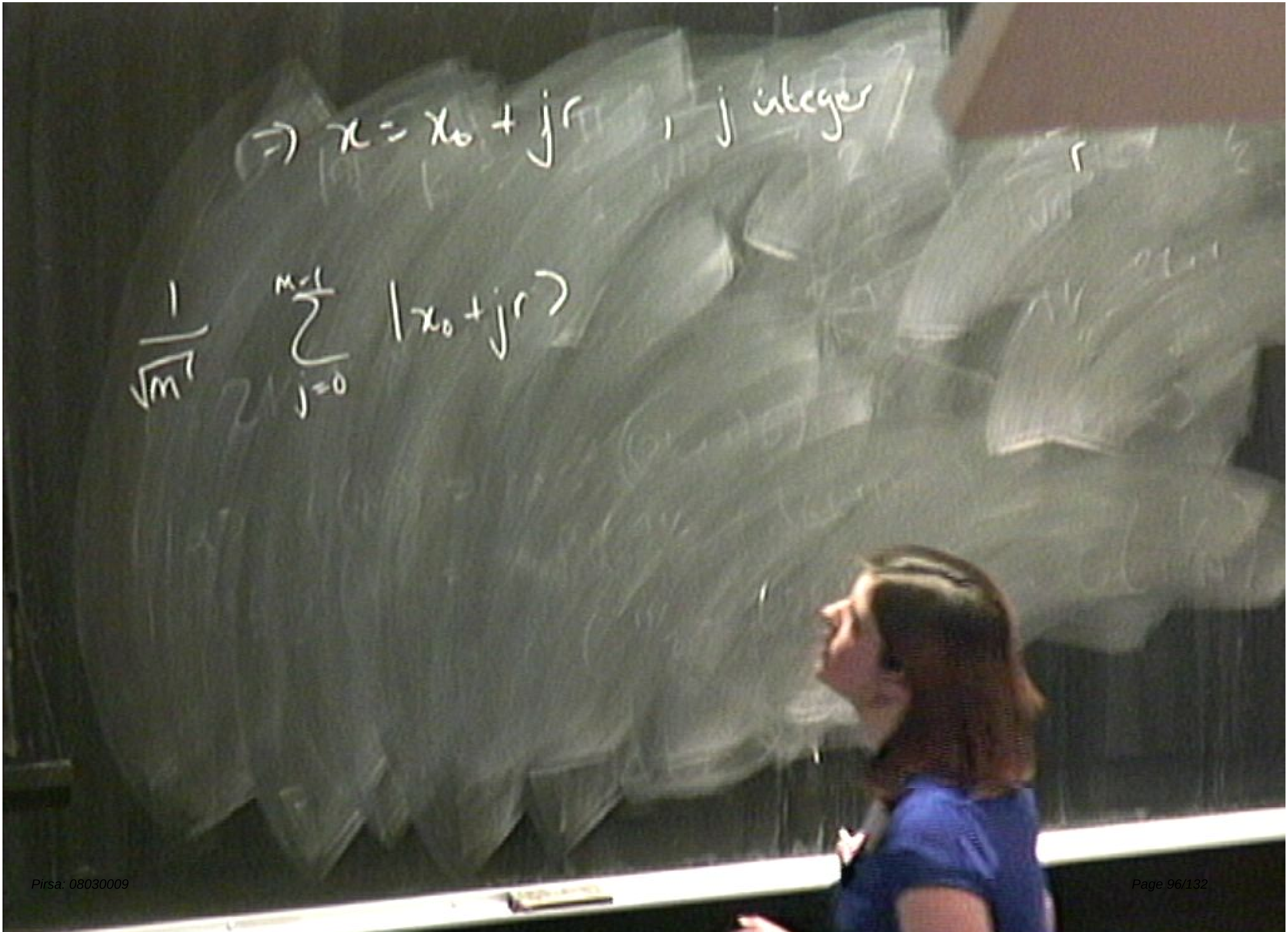
$$U_f\left(\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\right)|0\rangle \rightarrow \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|f(x)\rangle$$

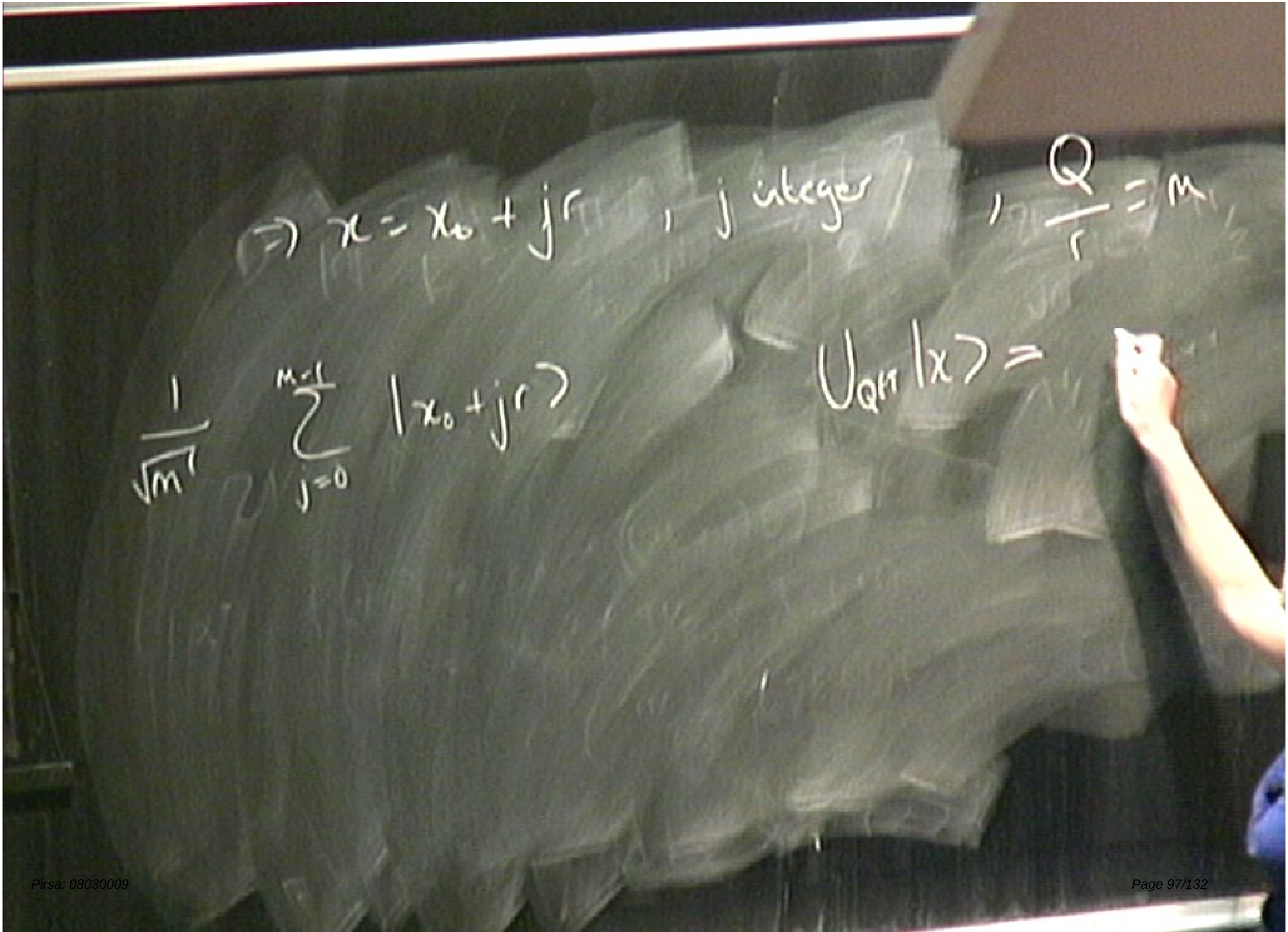
$$f(x_0) \rightarrow \frac{1}{\sqrt{Q}}\sum_{x:f(x)=f(x_0)}|x\rangle$$


$\left(\frac{1}{\sqrt{Q}}\sum |x\rangle\right)|0\rangle$
$U_f\left(\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\right)|0\rangle \to \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle$
$f(x_0) \to \frac{1}{\sqrt{p}}\frac{1}{\sqrt{Q}}\sum_{x: f(x)=f(x_0)}|x\rangle$


⇒ x = x0 + jr , j integer


⇒ x = x0 + jr , j integer , x/r = m
Σ_{j=0}^{m-1} |x0 + jr⟩


⇒ x = x0 + jr , j integer
r
1/√m Σ_{j=0}^{m-1} |x0 + jr⟩


⇒ x = x₀ + jr , j integer , Q/r = m
1/√m Σ_{j=0}^{m-1} |x₀ + jr⟩
U_QFT |x⟩ =

$\Rightarrow x = x_0 + jr$, j integer , $\frac{Q}{r} = m$

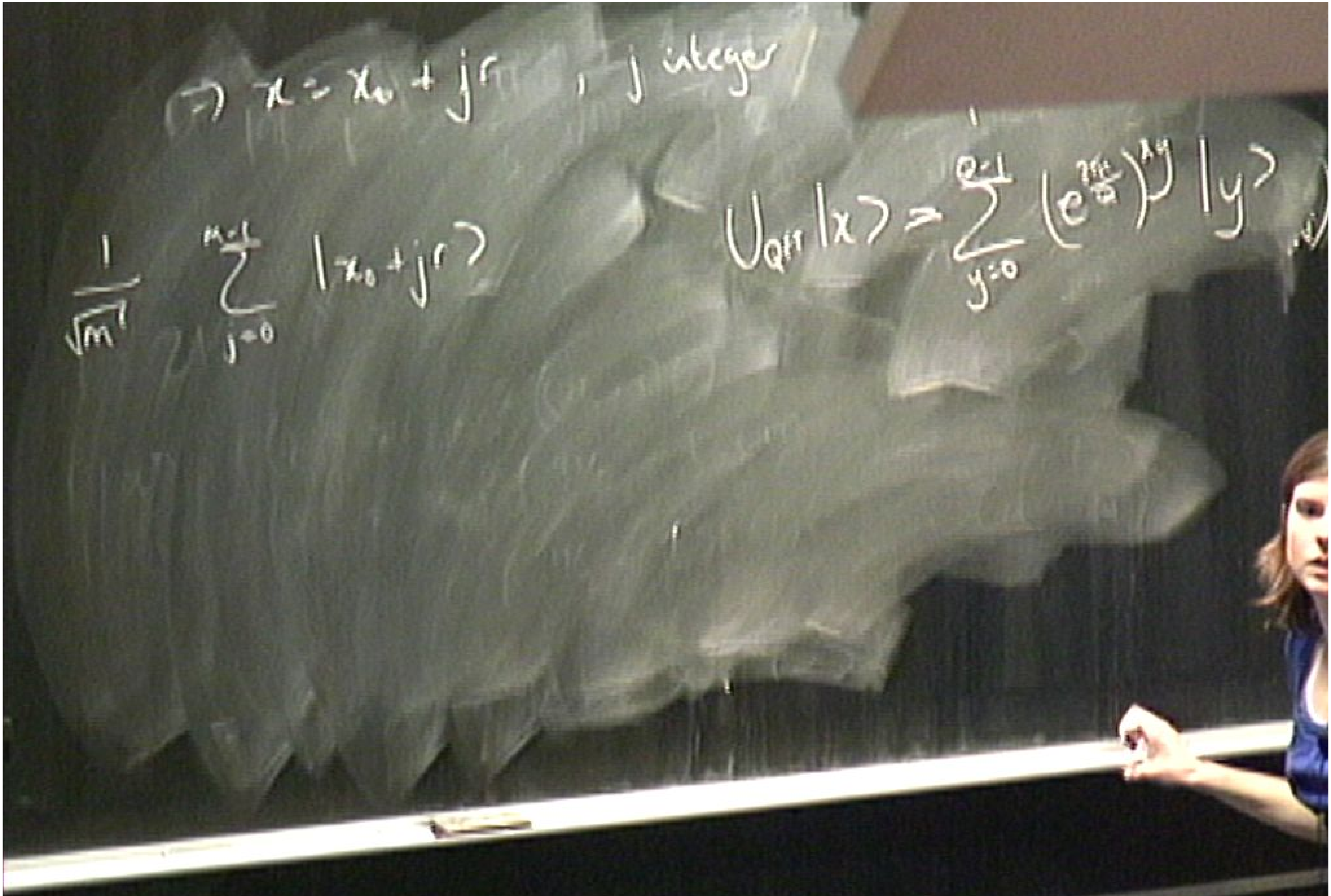
$U_{QFT} |x\rangle = \sum$

$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$

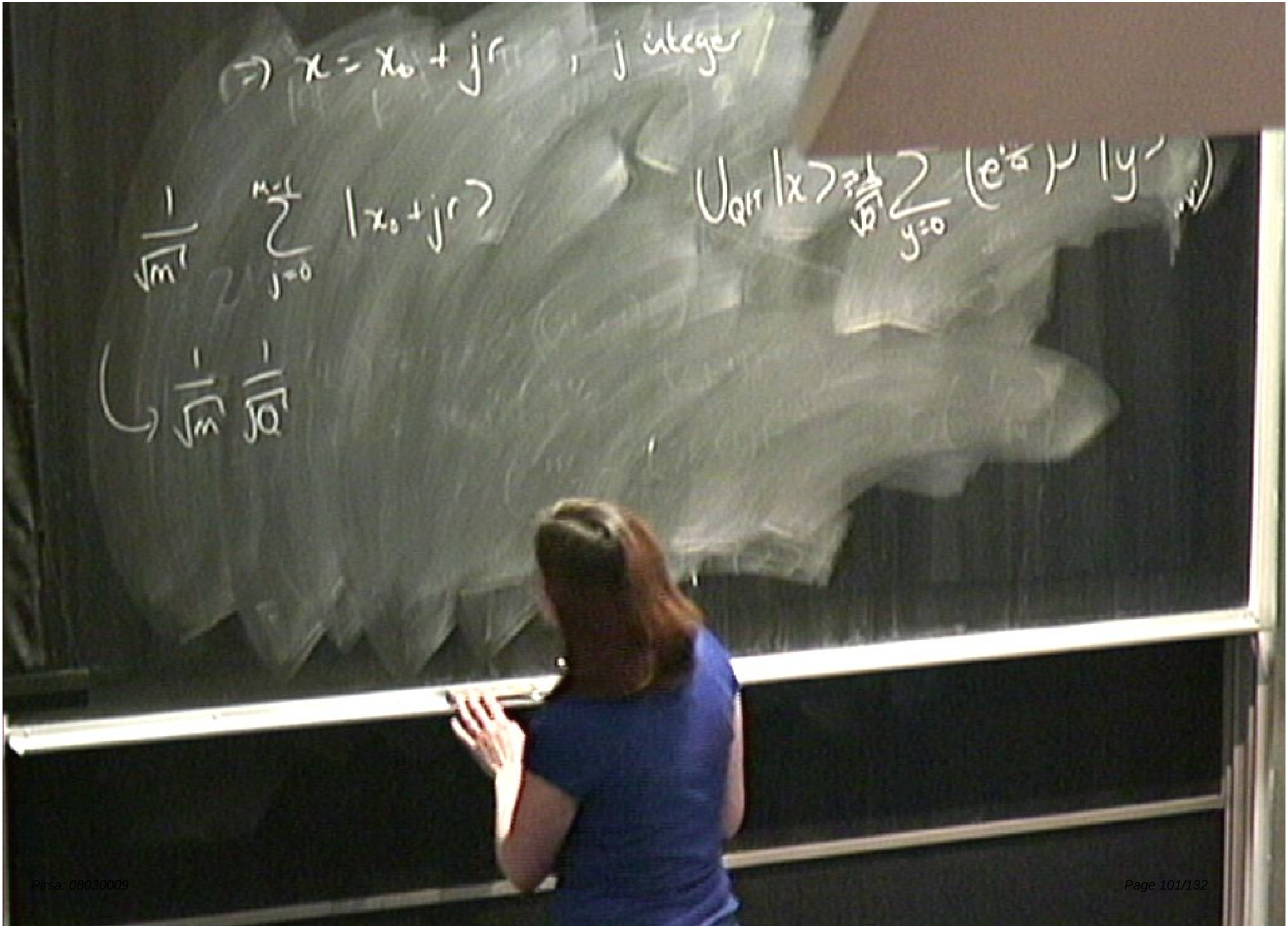
$\Rightarrow x = x_0 + jr$, j integer

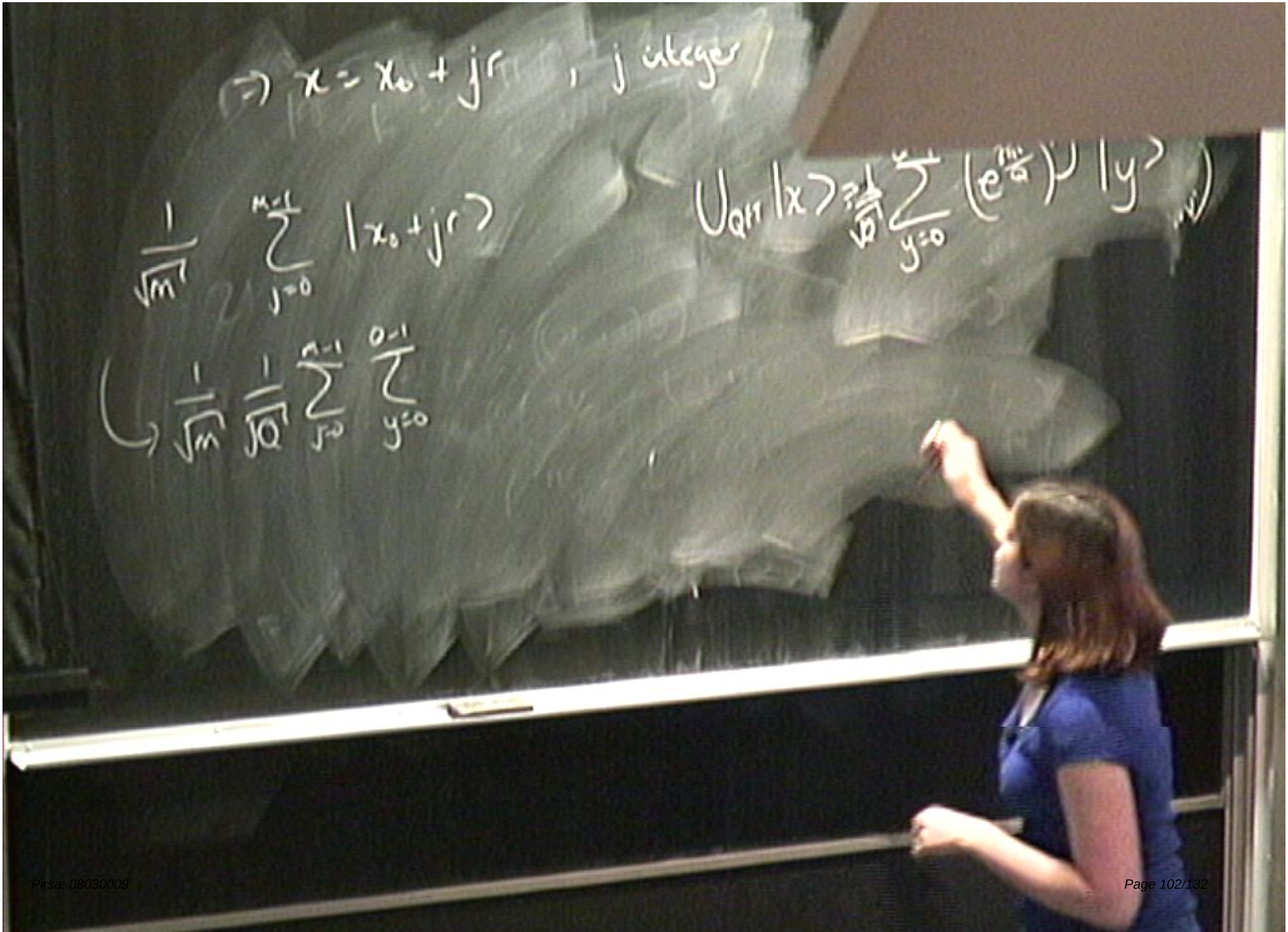
$$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$$

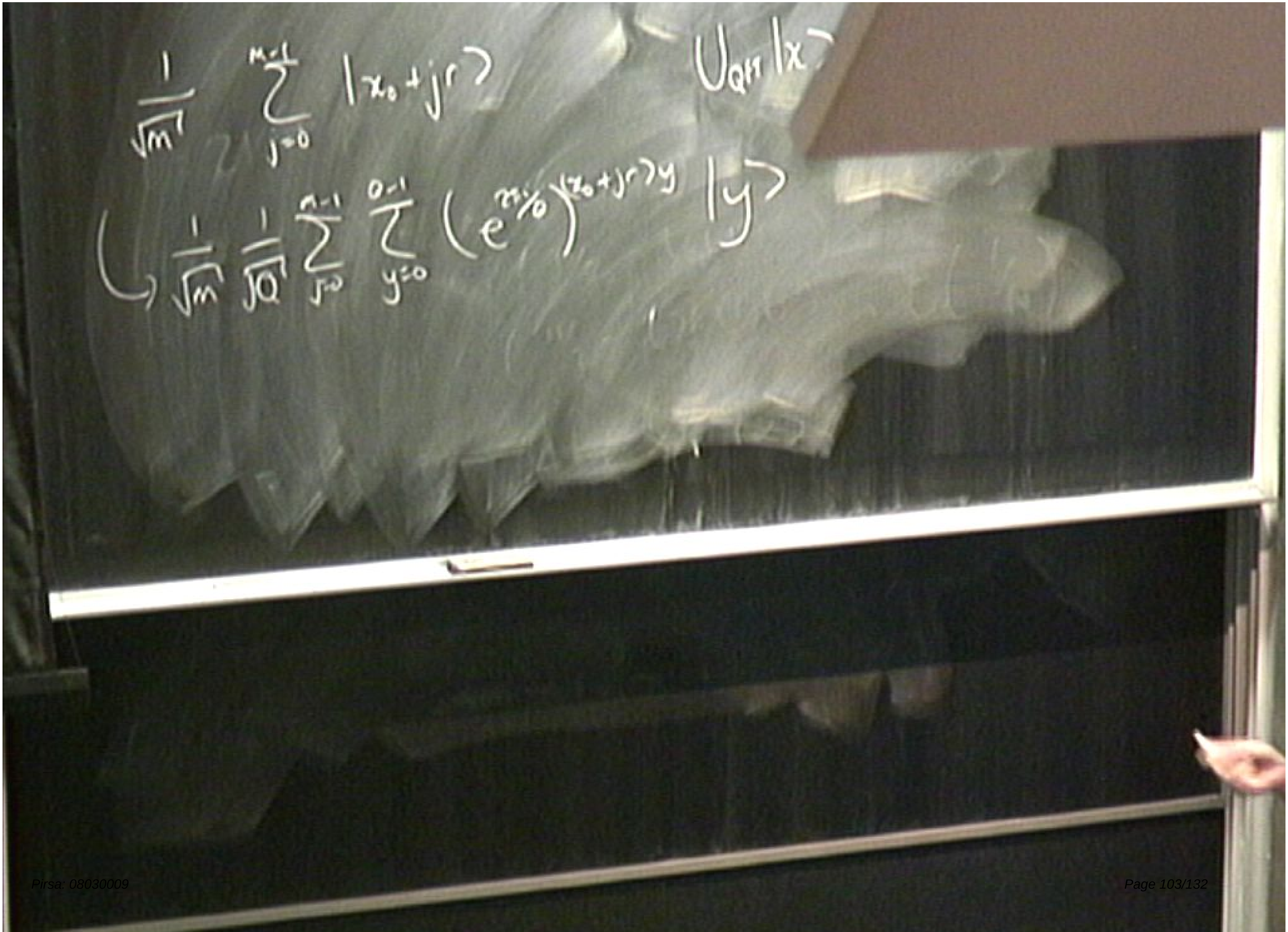
$$U_{QFT} |x\rangle = \sum_{y=0}^{Q-1} e^{2\pi i \cdots}$$

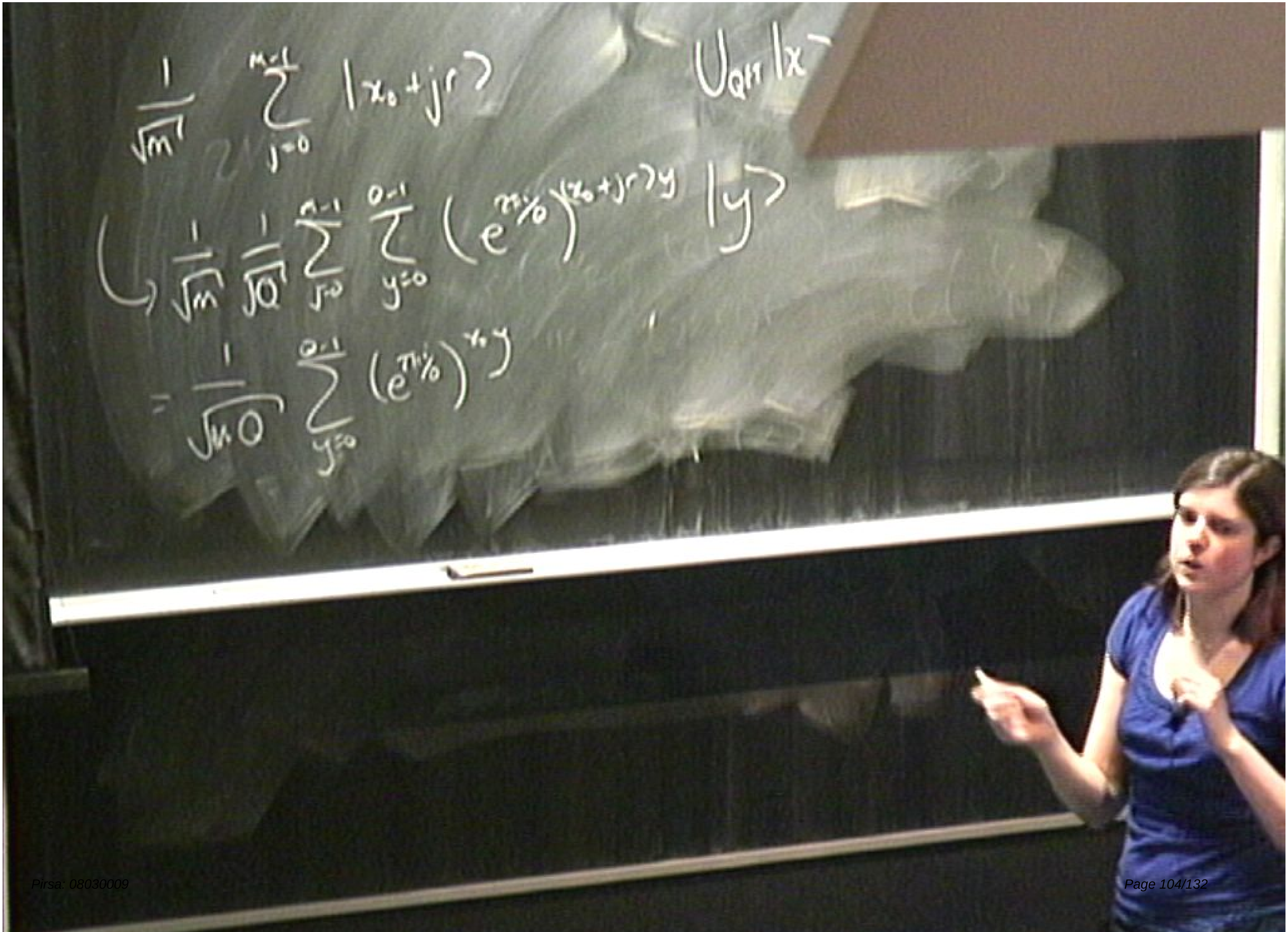


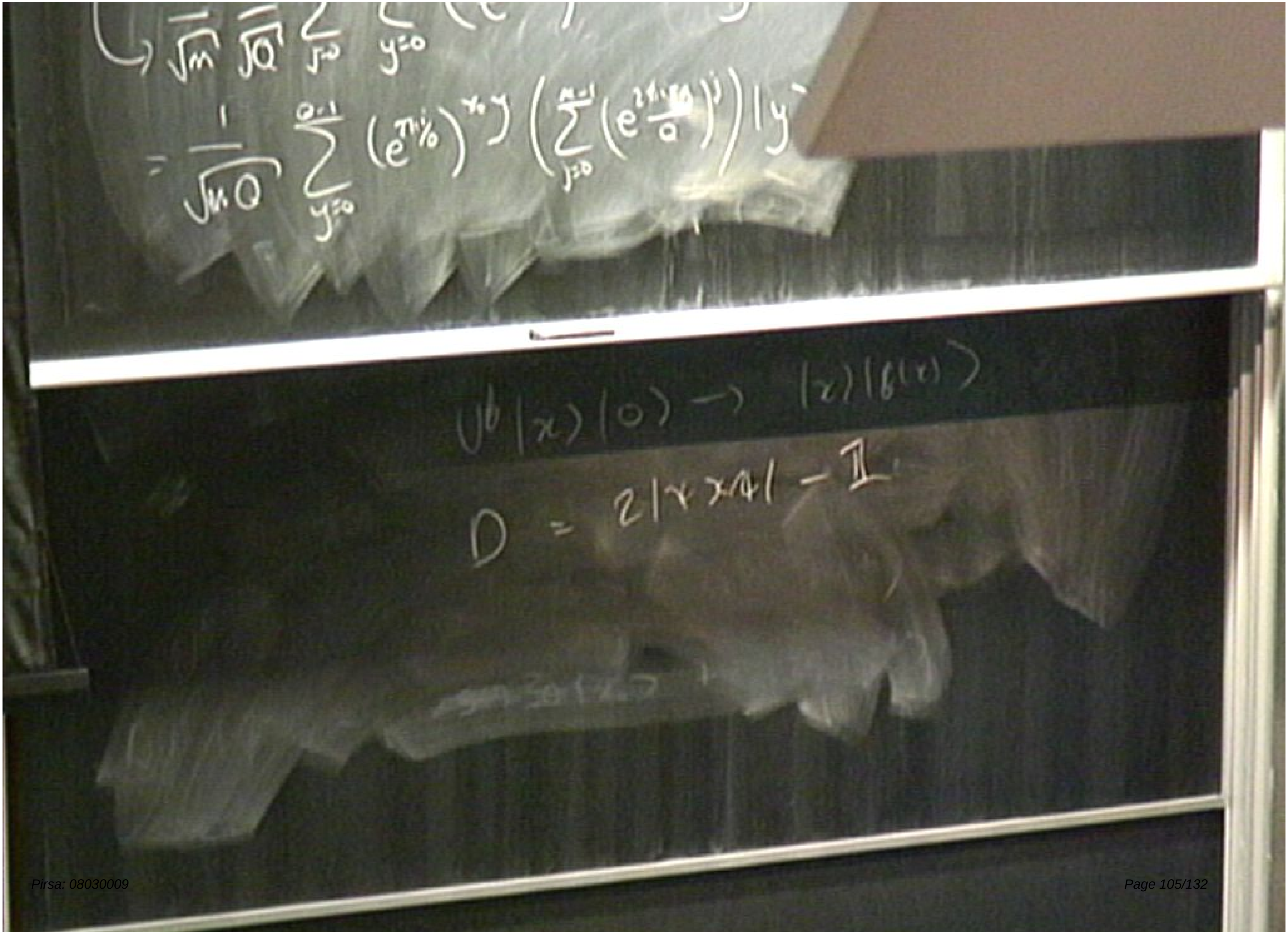
$\Rightarrow x = x_0 + jr$, j integer
$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$
$U_{QFT}|x\rangle = \sum_{y=0}^{Q-1} (e^{\frac{2\pi i}{Q}})^{xy} |y\rangle$

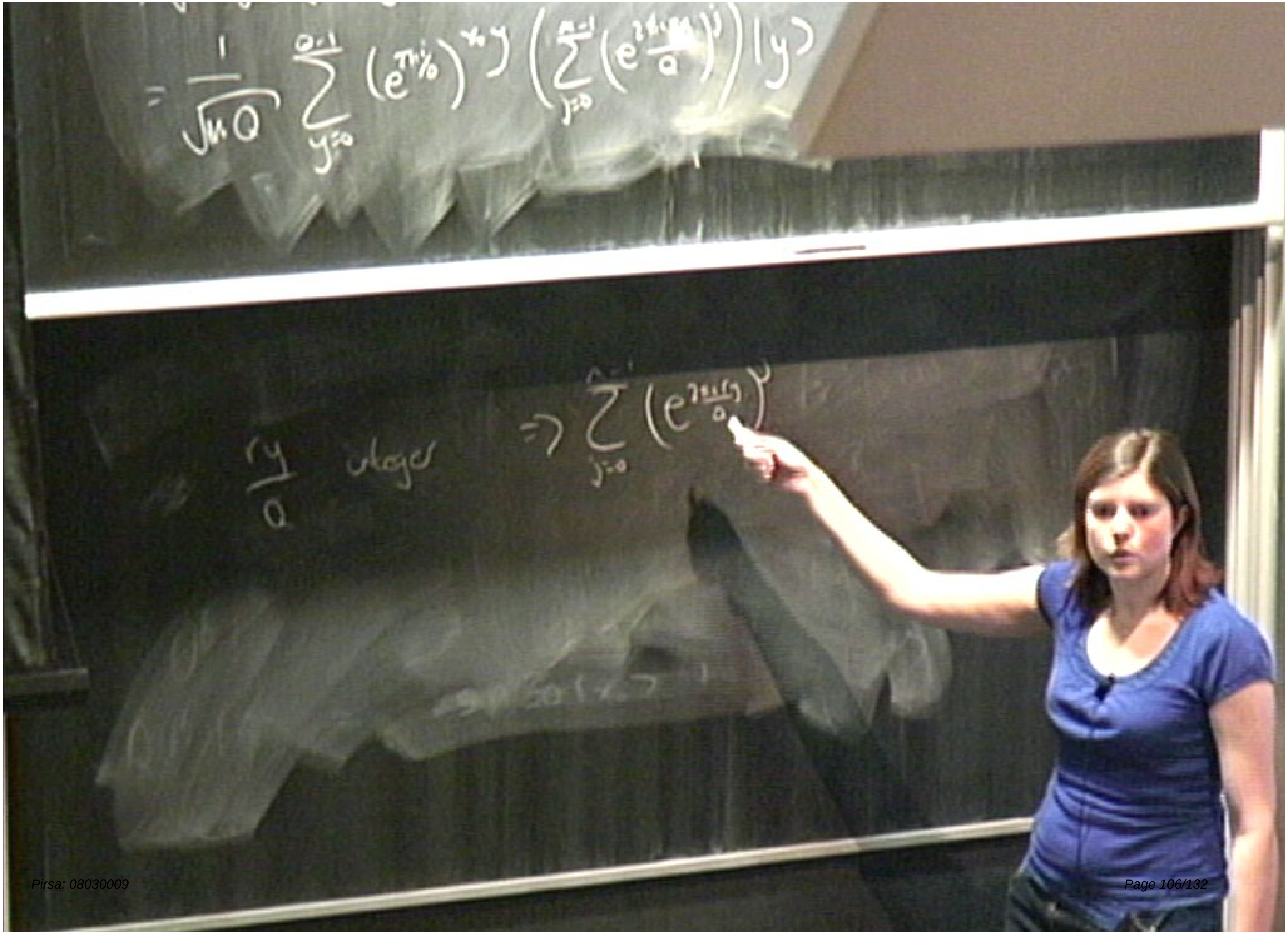

⇒ x = x0 + jr , j integer
1/√m Σ_{j=0}^{m-1} |x0 + jr⟩
U_QFT |x⟩ = 1/√Q Σ_{y=0} |y⟩
1/√m 1/√Q

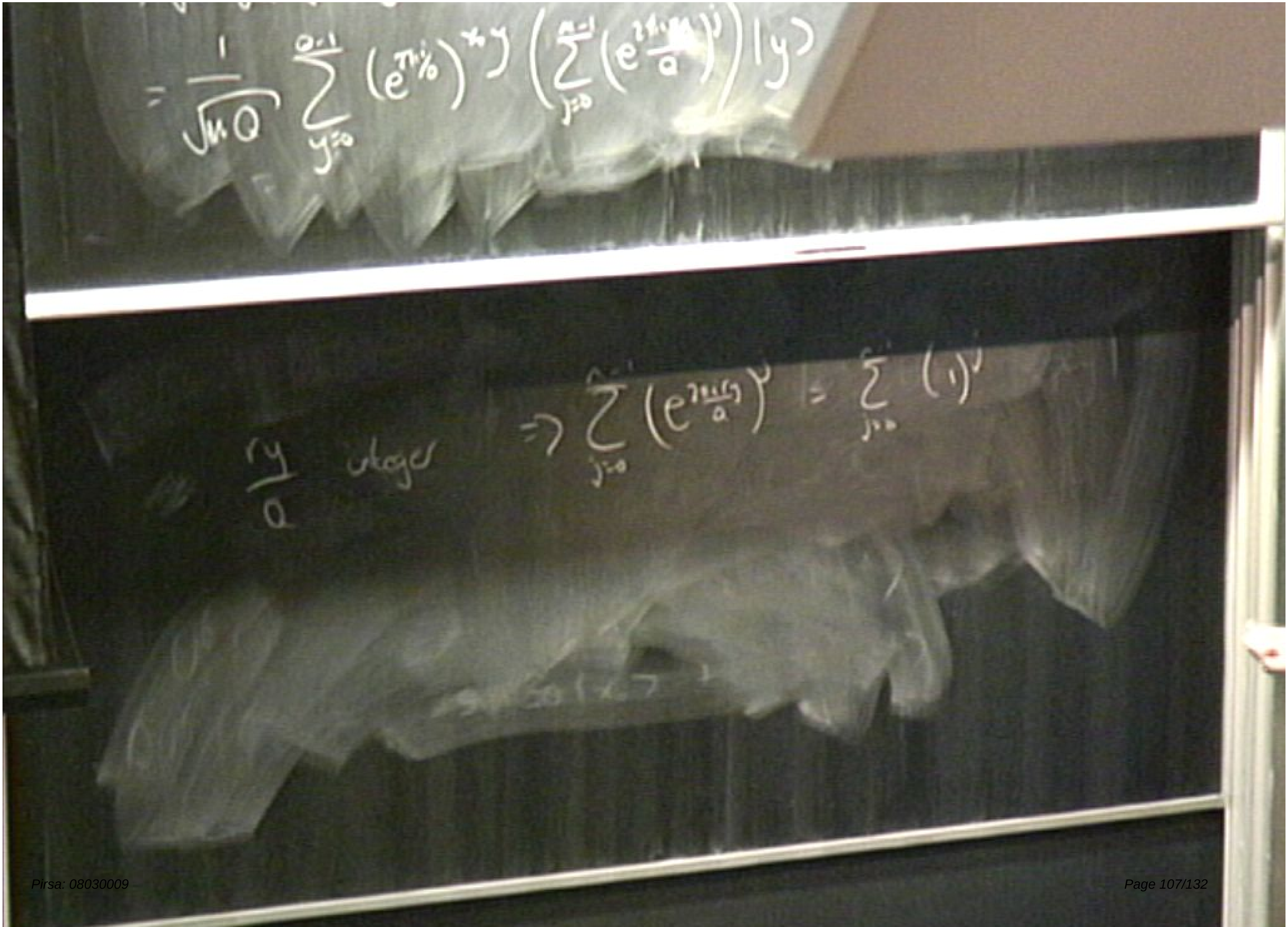

⇒ x = x0 + jr , j integer
1/√m Σ_{j=0}^{m-1} |x0 + jr⟩
U_QFT |x⟩ = 1/√Q Σ_{y=0} (e^{2πi/Q})^{xy} |y⟩
1/√m 1/√Q Σ_{j=0}^{m-1} Σ_{y=0}^{Q-1}


$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$
$U_{QFT} |x\rangle$
$\hookrightarrow \frac{1}{\sqrt{m}} \frac{1}{\sqrt{Q}} \sum_{j=0}^{m-1} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{(x_0+jr)y} |y\rangle$


$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$
$U_{QFT} |x$
$\frac{1}{\sqrt{m}} \frac{1}{\sqrt{Q}} \sum_{j=0}^{m-1} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{(x_0+jr)y} |y\rangle$
$= \frac{1}{\sqrt{mQ}} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{x_0 y}$

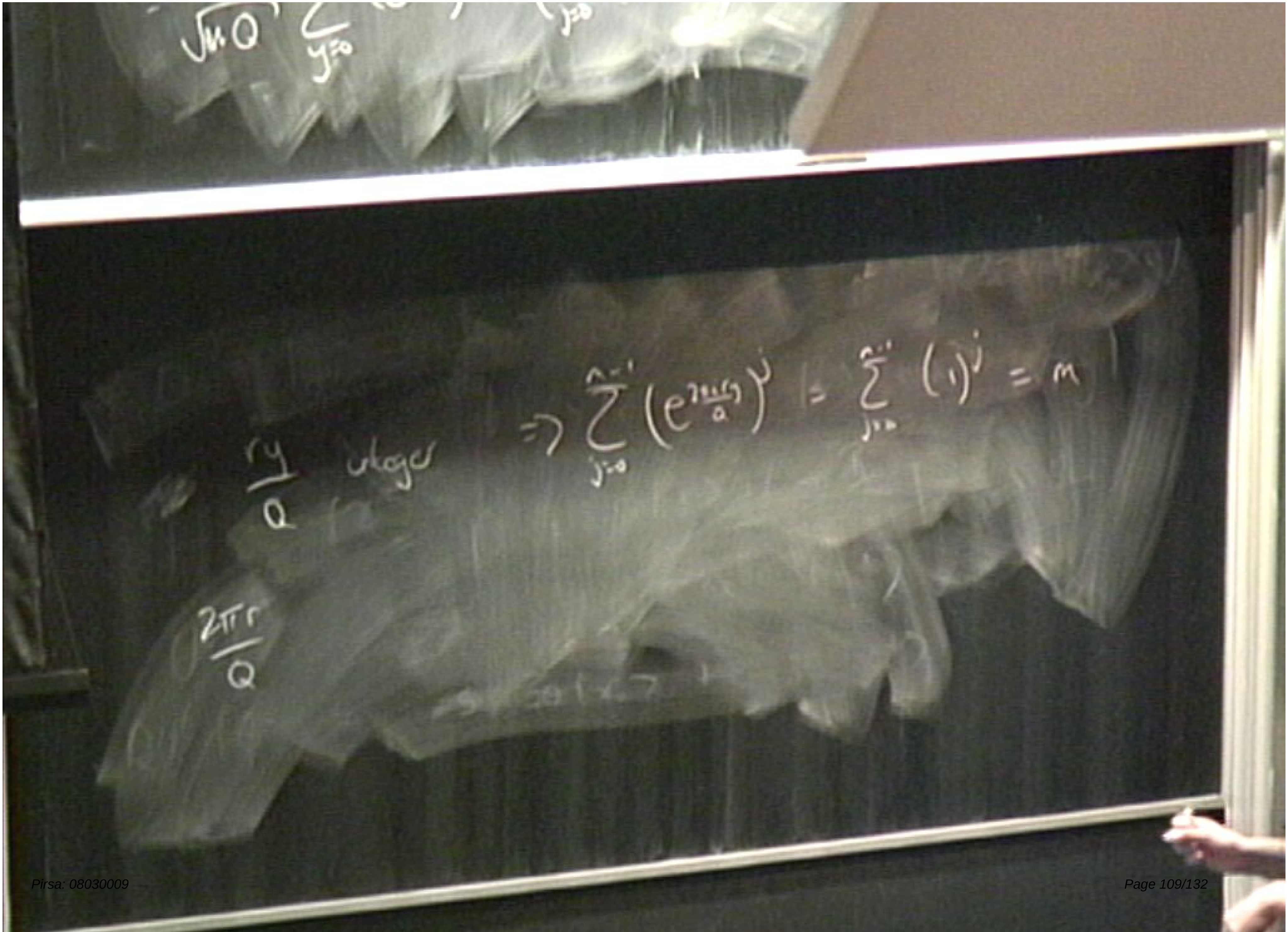

U_f |x⟩|0⟩ → |x⟩|f(x)⟩
D = 2|ψ⟩⟨ψ| − I




$= \frac{1}{\sqrt{mQ}} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{x_0 y} \left(\sum_{j=0}^{m-1} (e^{\frac{2\pi i r y}{Q}})^j \right) |y\rangle$
$\frac{ry}{Q}$ integer
$\Rightarrow \sum_{j=0}^{m-1} (e^{\frac{2\pi i r y}{Q}})^j = \sum_{j=0}^{m-1} (1)^j$

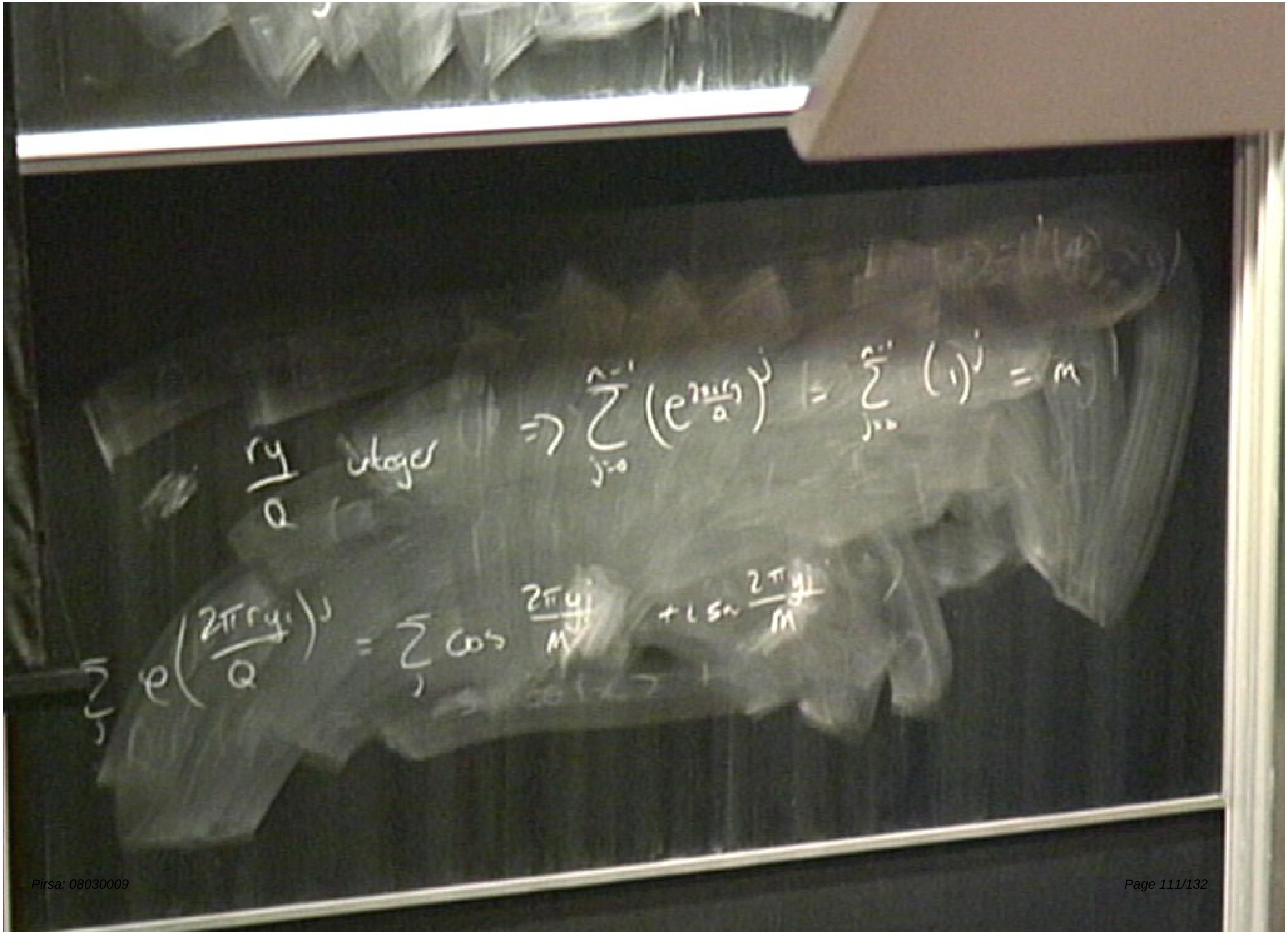
$$= \frac{1}{\sqrt{mQ}} \sum_{y=0} \left(e^{\pi i/Q}\right) \ldots \left(\sum_{j=0} \left(e^{\frac{\ldots}{Q}}\right) \ldots \right)$$

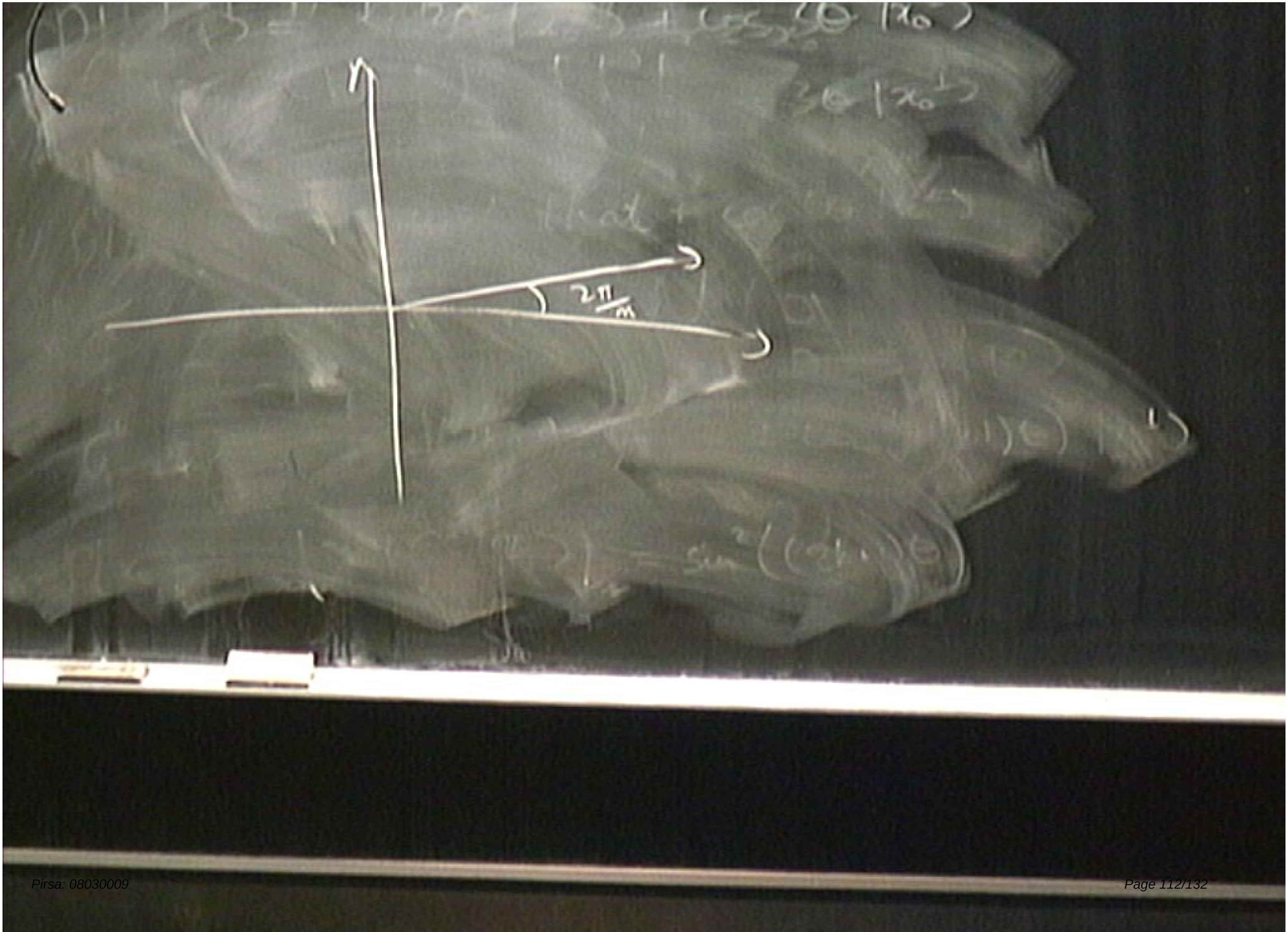
$\frac{ry}{Q}$ integer $\Rightarrow \sum_{j=0}^{m-1} \left(e^{\frac{2\pi i r y}{Q}}\right)^j = \sum_{j=0}^{m-1} (1)^j = m$

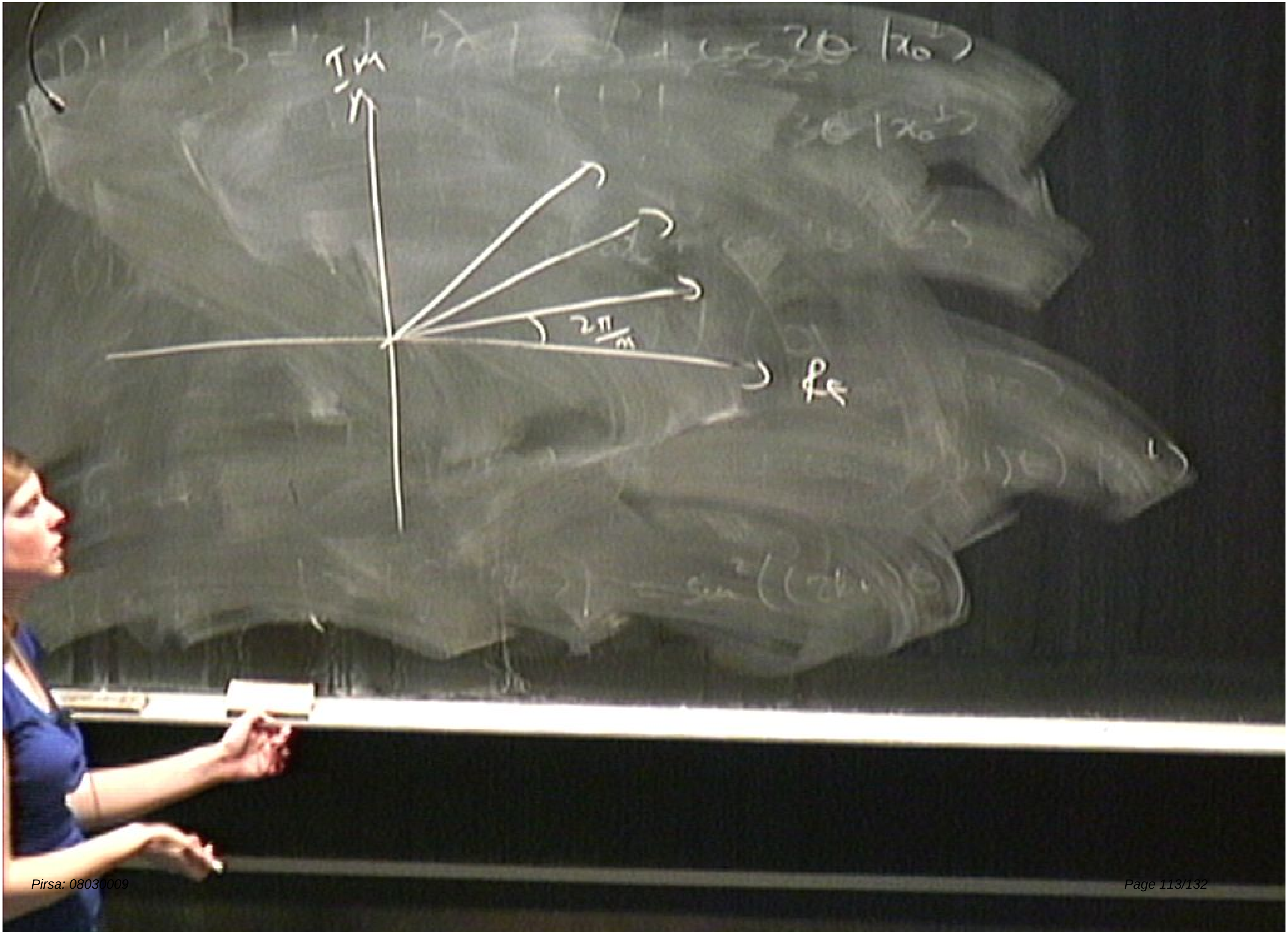

ry/Q integer
⇒ Σ_{j=0}^{m-1} (e^{2πi r y/Q})^j = Σ_{j=0}^{m-1} (1)^j = m
2πr/Q

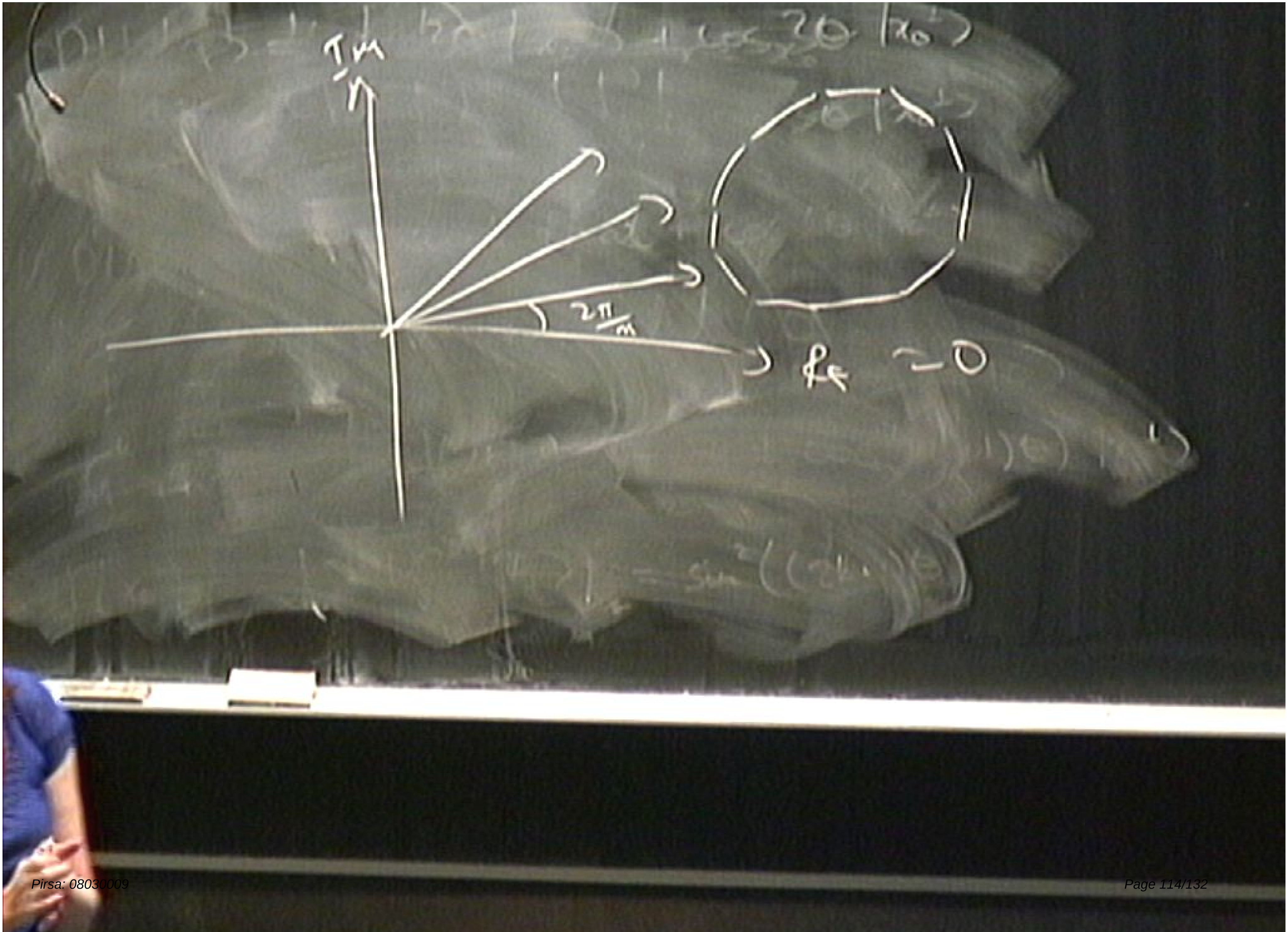
$\frac{ry}{Q}$ integer $\Rightarrow \sum_{j=0}^{m-1} \left(e^{\frac{2\pi i r y}{Q}}\right)^j = \sum_{j=0}^{m-1} (1)^j = m$

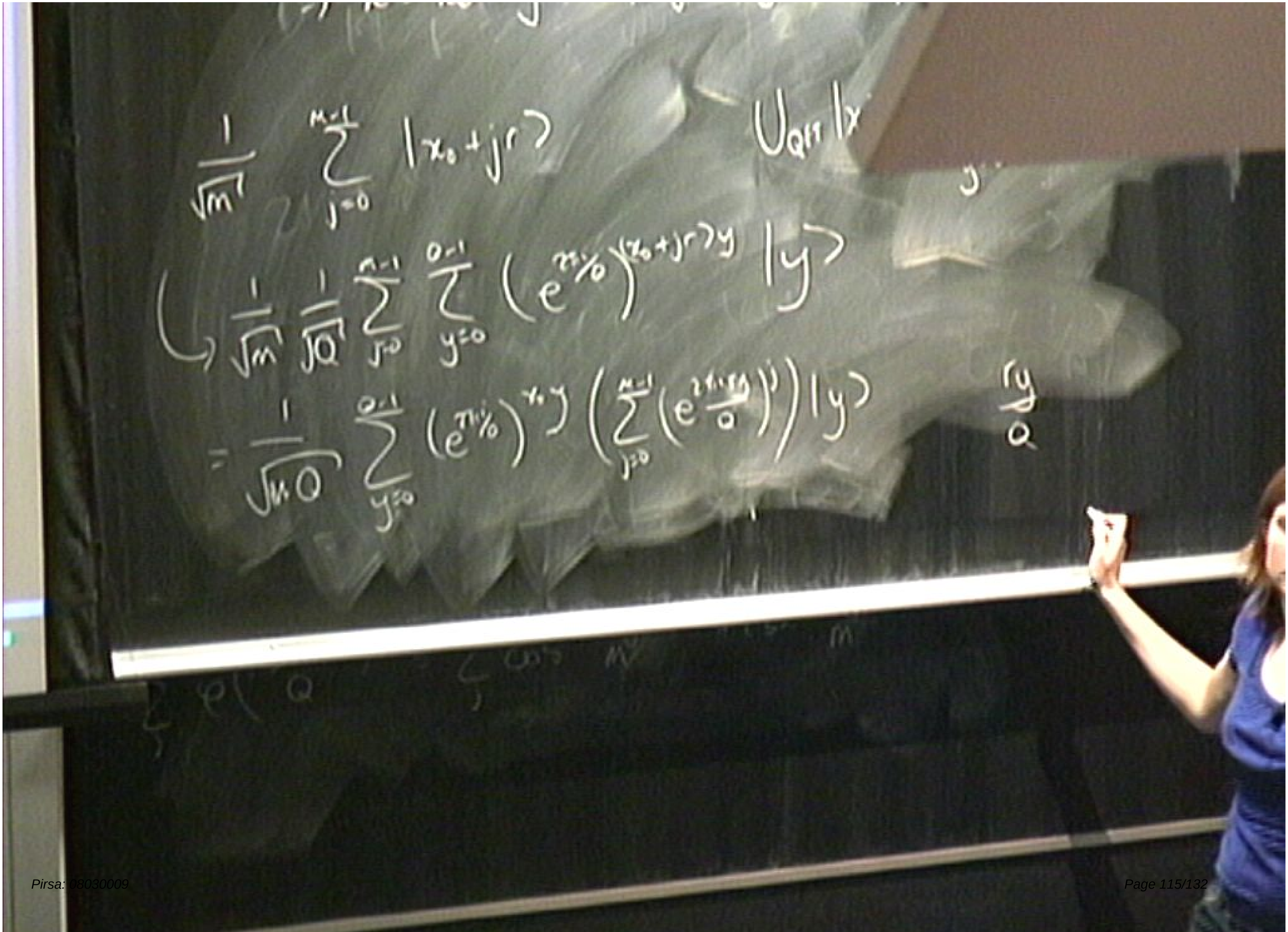
$$\sum_j e\left(\frac{2\pi r y i}{Q}\right)^j = \sum_j \cos\frac{2\pi r y j}{Q} + i\sin\frac{2\pi r y j}{Q}$$

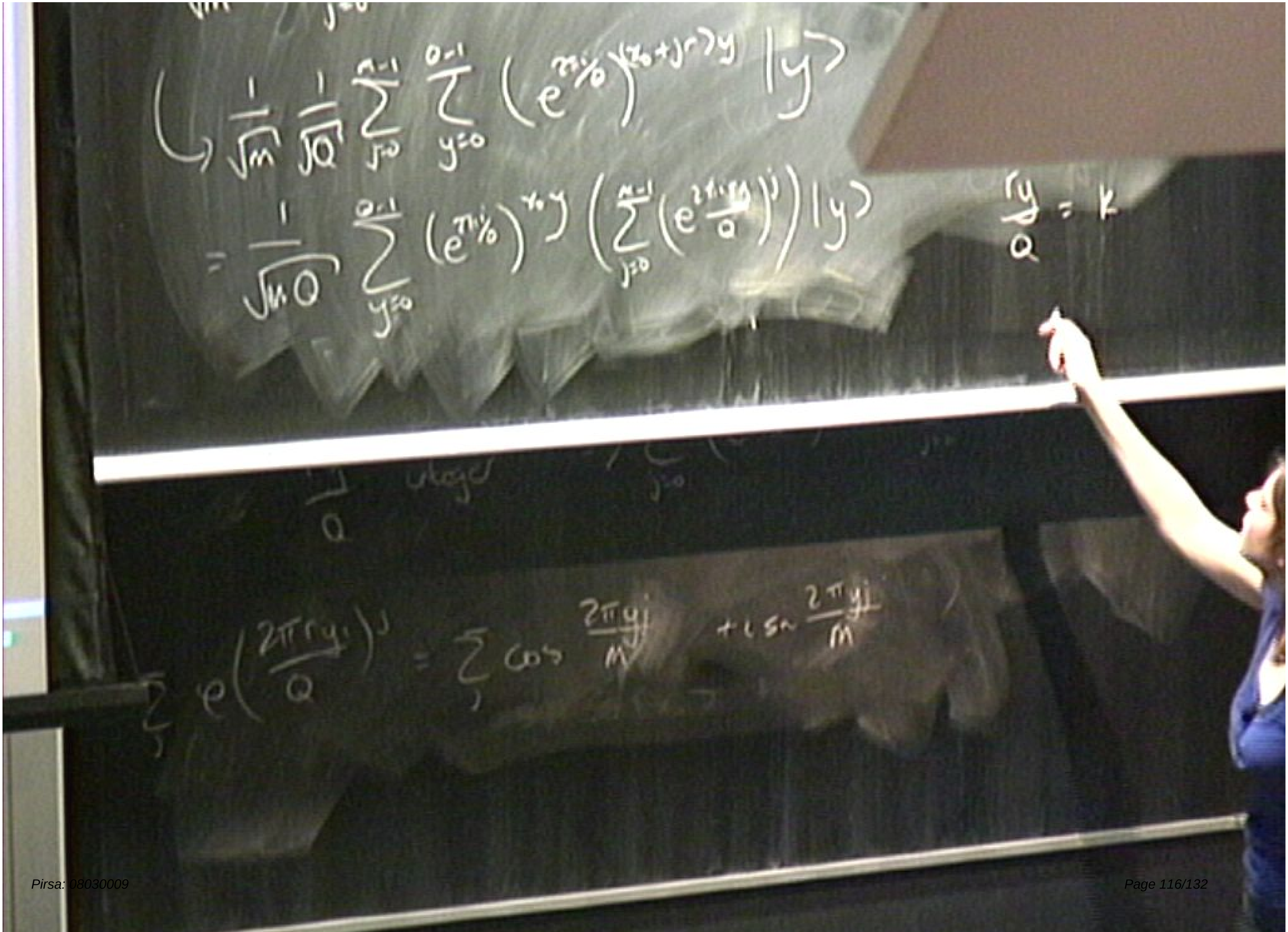

$\frac{ry}{Q}$ integer $\Rightarrow \sum_{j=0}^{m-1} \left(e^{\frac{2\pi i r y}{Q}}\right)^j = \sum_{j=0}^{m-1} (1)^j = m$
$\sum_j e\left(\frac{2\pi i r y j}{Q}\right)^j = \sum_j \cos \frac{2\pi y j}{M} + i \sin \frac{2\pi y j}{M}$

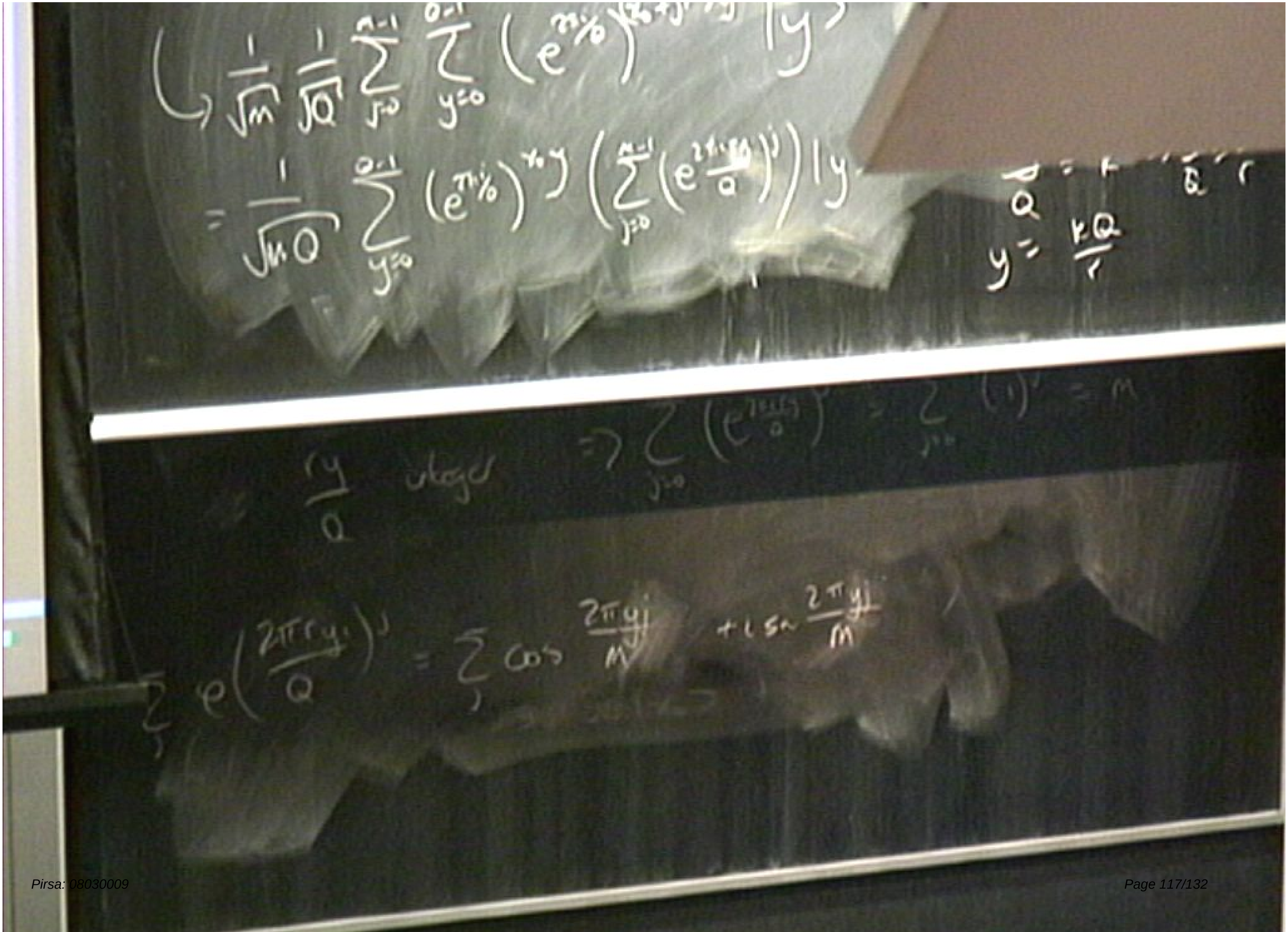

2π/m

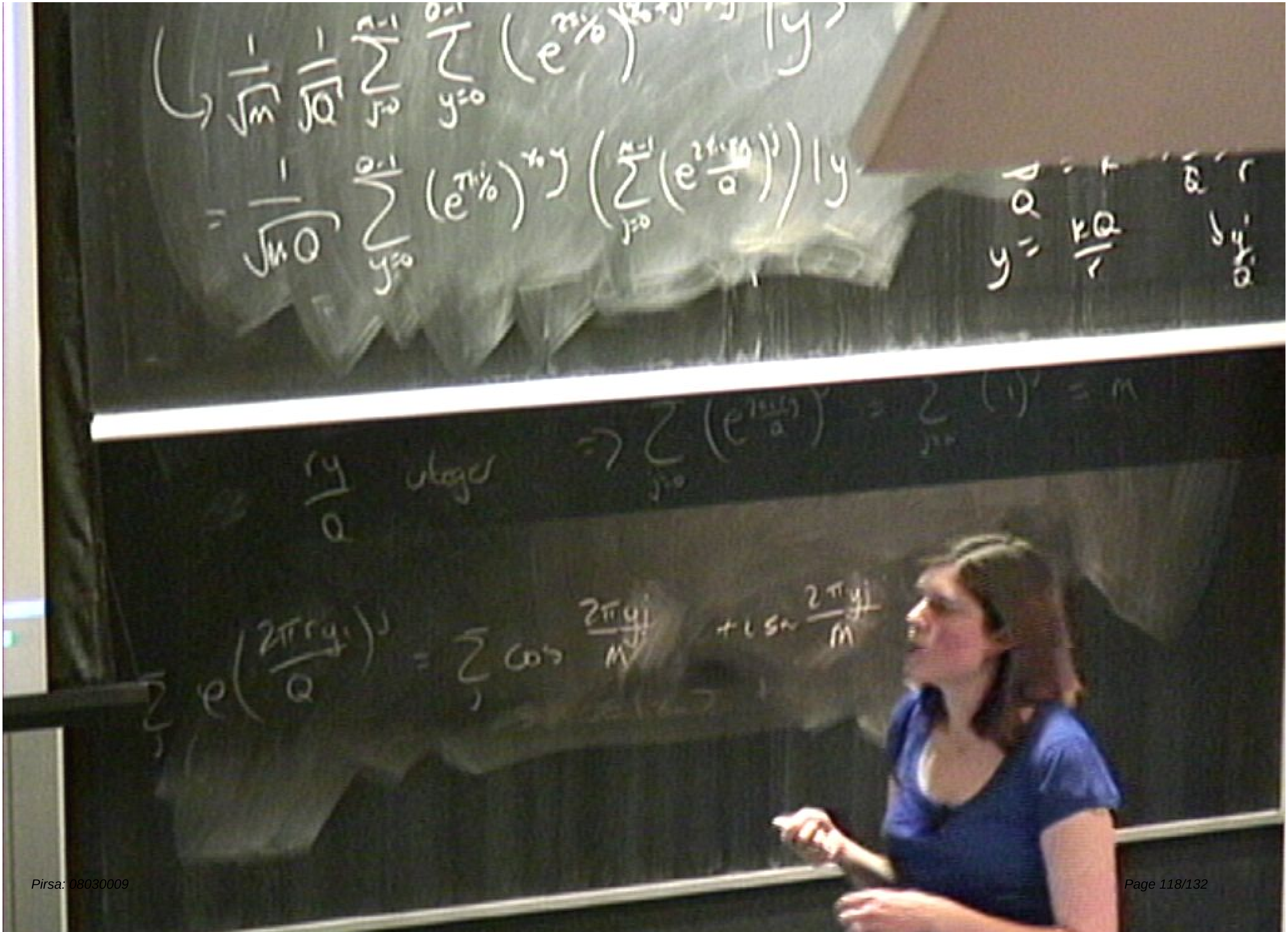

Im
2π/m
Re

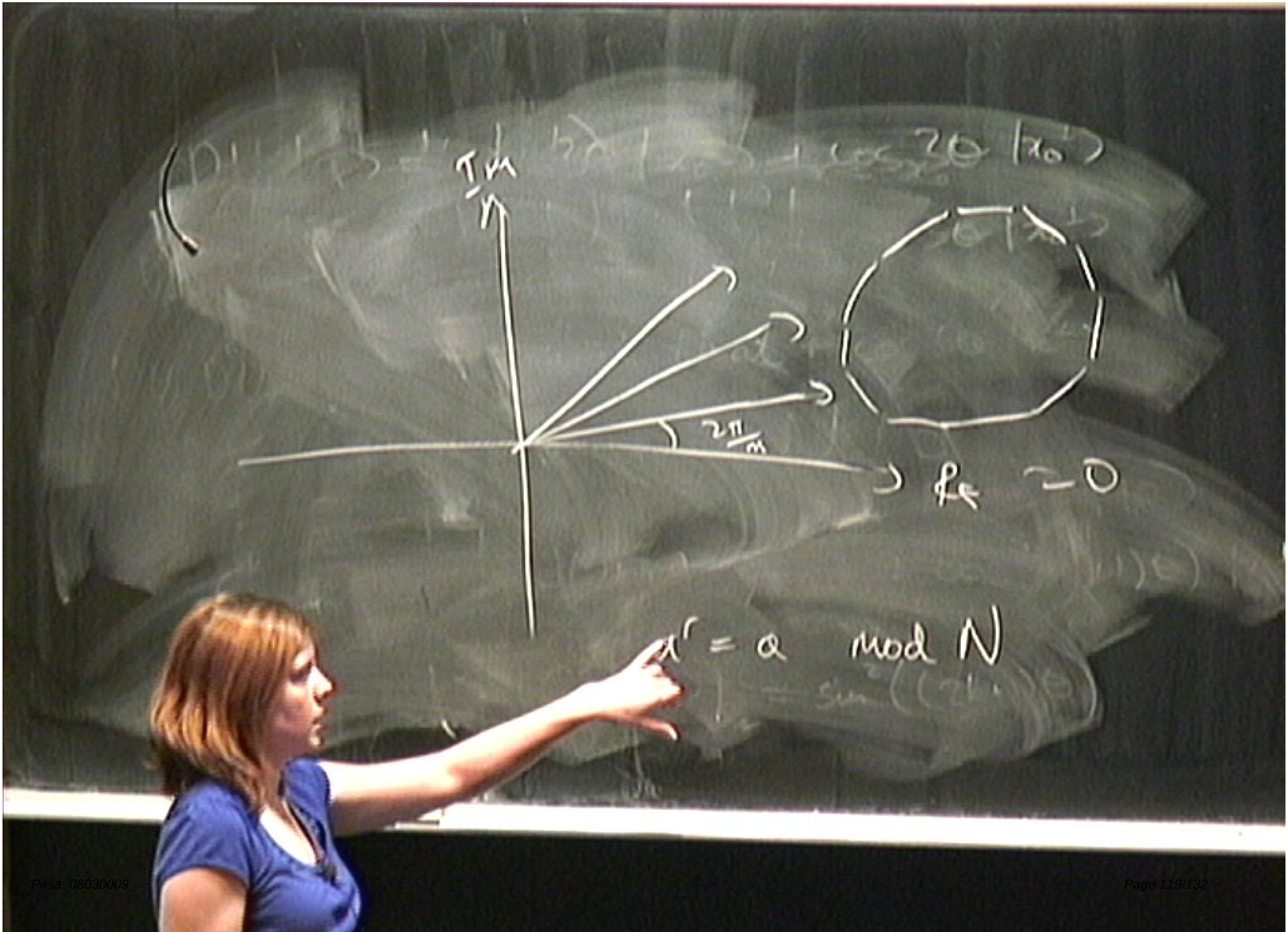

Im
2π/m

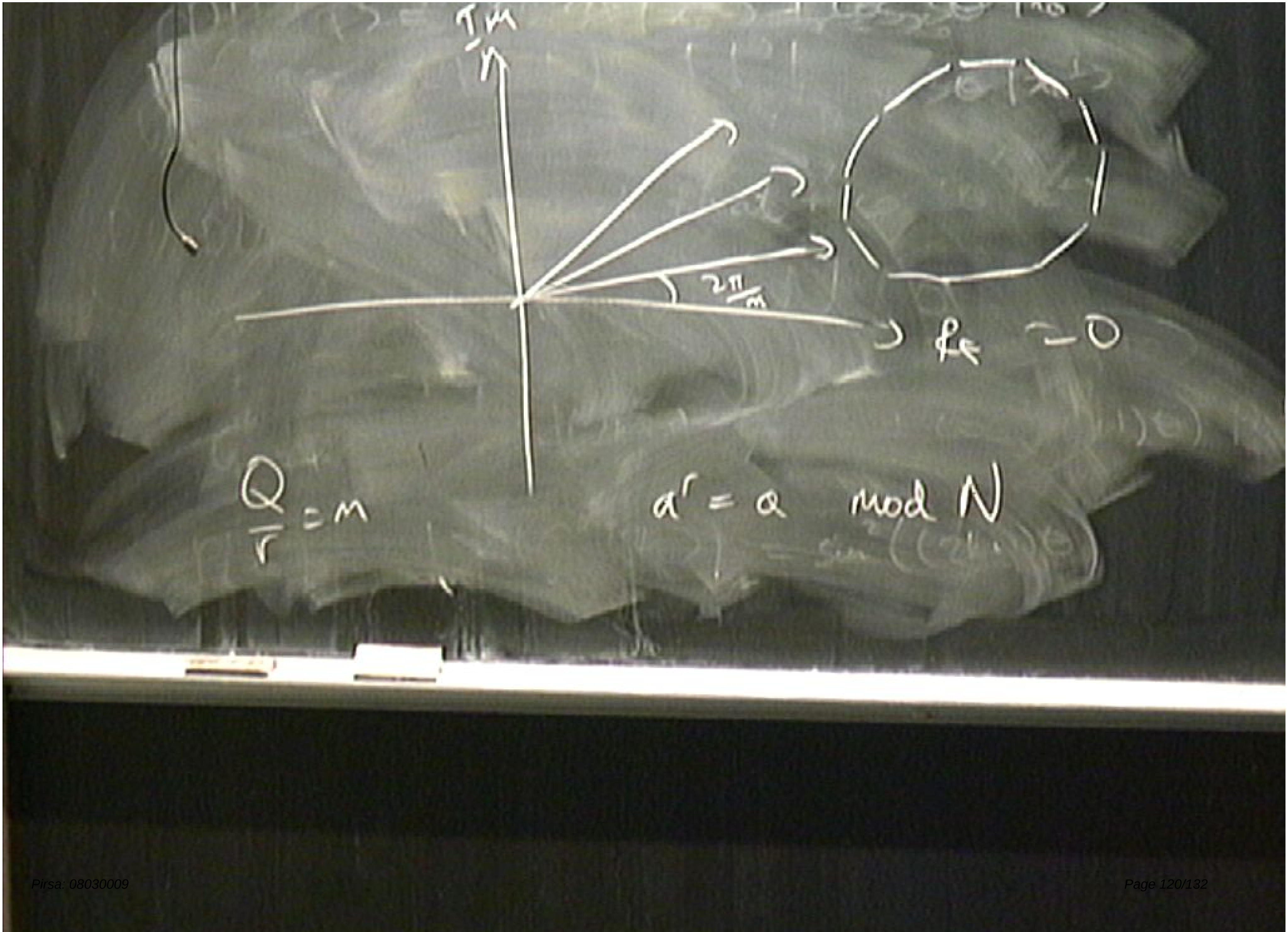

$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle$
$U_{QFT} |x\rangle$
$\frac{1}{\sqrt{m}} \frac{1}{\sqrt{Q}} \sum_{j=0}^{m-1} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{(x_0+jr)y} |y\rangle$
$= \frac{1}{\sqrt{mQ}} \sum_{y=0}^{Q-1} (e^{2\pi i/Q})^{x_0 y} \left(\sum_{j=0}^{m-1} (e^{2\pi i \frac{ry}{Q}})^j \right) |y\rangle$
$\frac{ry}{Q}$




$\frac{1}{\sqrt{m}}\frac{1}{\sqrt{Q}}\sum_{j=0}^{m-1}\sum_{y=0}^{Q-1}(e^{2\pi i/Q})^{\ldots}|y\rangle$
$=\frac{1}{\sqrt{mQ}}\sum_{y=0}^{Q-1}(e^{2\pi i/Q})^{x_0 y}\left(\sum_{j=0}^{m-1}(e^{\frac{2\pi i r y}{Q}})^j\right)|y\rangle$
$y = \frac{kQ}{r}$
$\frac{ry}{Q}$ integer
$\Rightarrow \sum_{j=0}(e^{\frac{2\pi i r y}{Q}})^j = \sum_{j=0}(1)^j = m$
$\sum e(\frac{2\pi r y_1}{Q})^j = \sum_j \cos\frac{2\pi y j}{m} + i\sin\frac{2\pi y j}{m}$




2π/m
= a mod N


Im
2π/m
Q/r = m
a^r = a mod N


integer

$\frac{ry}{Q}$ integer $\Rightarrow \sum_{j=0}^{m-1} \left(e^{\frac{2\pi i r y}{Q}}\right)^j = \sum_{j=0}^{m-1} (1)^j = m$

$\sum_j e\left(\frac{2\pi i r y_i}{Q}\right)^j = \sum_j \cos \frac{2\pi y j}{M} + i \sin \frac{2\pi y j}{M}$

Decoherence and Scalability

- Have assumed unitary transformations, in the presence of an environment this is not the case.
- Interactions with an environment partially corrupt the information encoded in quantum states.
- Fault-tolerant quantum computation possible if probability of single gate error is below a certain threshold level.
- Is there a scale at which the world stops behaving quantum mechanically?

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right) \quad |\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right) \quad |\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle \right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right) \; |\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right) \; |\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle \right) \Rightarrow \rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \quad |\psi\rangle$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \quad |\psi\rangle$$

000
010

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle\right) \Rightarrow \rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Summary

- By taking advantage of the laws of quantum mechanics, we can perform some information processing and communication tasks that are not possible classically.
  - Dense coding, teleportation, QKD
  - Quantum algorithms
- It is not possible to do EVERYTHING faster with a quantum computer! But by carefully using quantum parallelism and interference, it is possible to design some algorithms which are more powerful than any known classical ones.

Open questions

- What are the class of problems for which a quantum computer can provide an improvement over classical computing?
  - Note that, in principle, a quantum computer can do anything a classical one can (without speed-up).
- What is it that makes a quantum computer more powerful? (Entanglement is not the full story…)
- Is quantum computing scalable?

References

- Quantum Cryptography: N. Gisin, G. C. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography", *Reviews of Modern Physics* **74**, 145 (2002)
- Quantum Information Processing: T. P. Spiller, W. J. Munro, S. D. Barrett and P. Kok, "An introduction to quantum information processing: applications and realizations", *Contemporary Physics* **46**, 407 (2005)
- Shor's algorithm for the man on the street: http://scottaaronson.com/blog/?p=208