Title: Quantum Information Theory #3

Date: Mar 18, 2008 06:30 PM

URL: http://pirsa.org/08030005

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

Quantum Information
Lecture 3: Quantum Computing

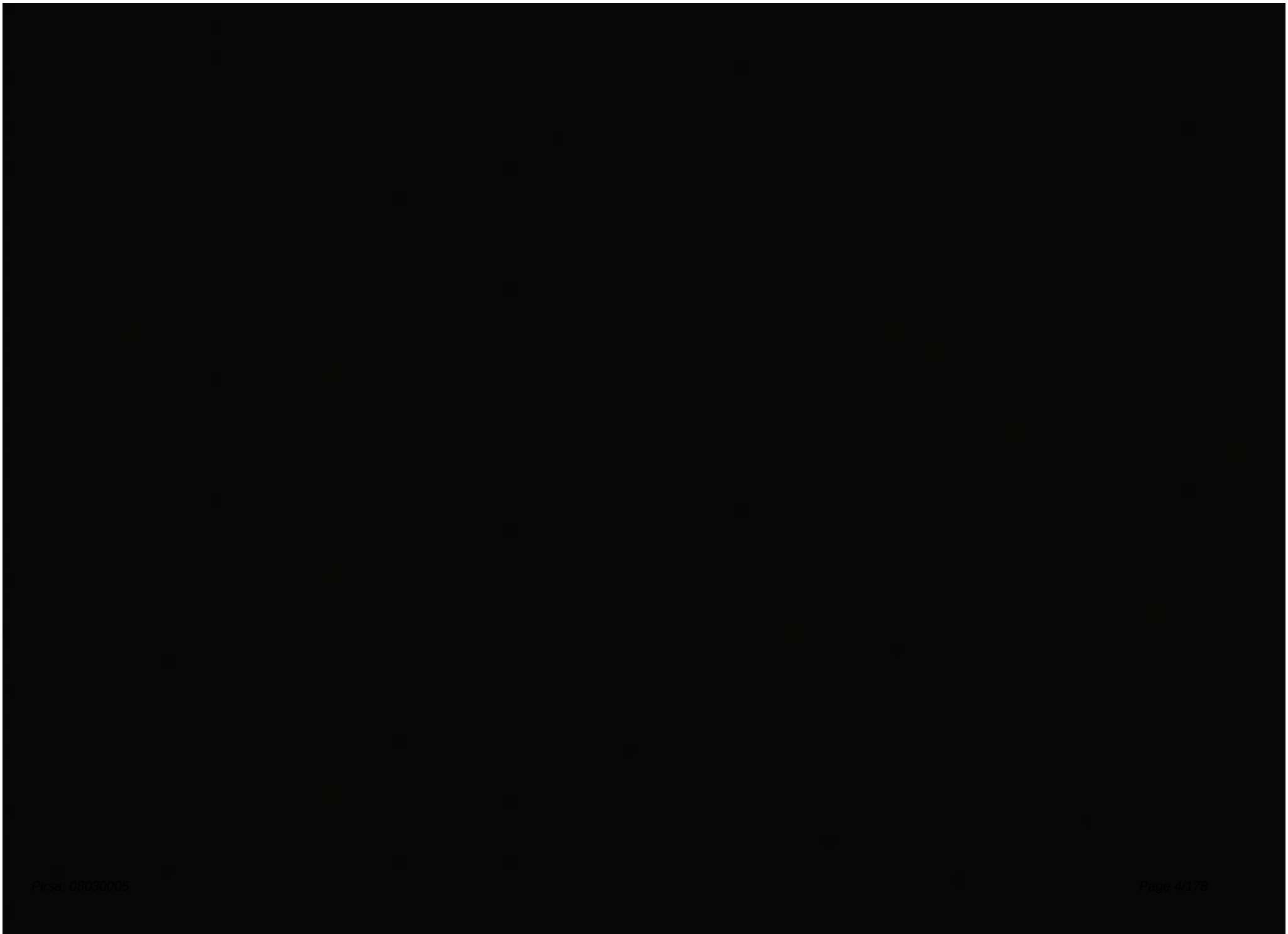
Sarah Croke

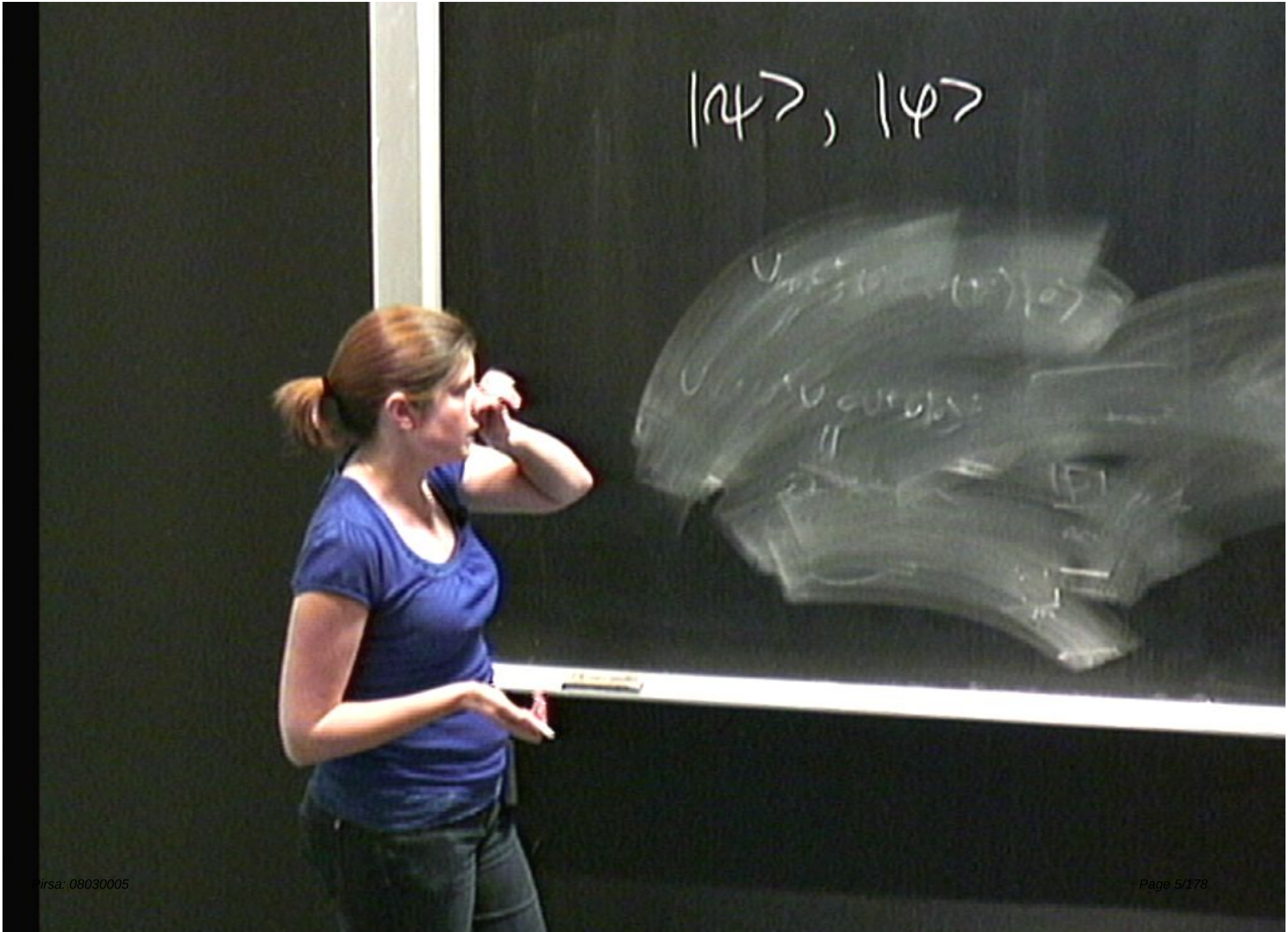
Perimeter Institute (Office: 252)

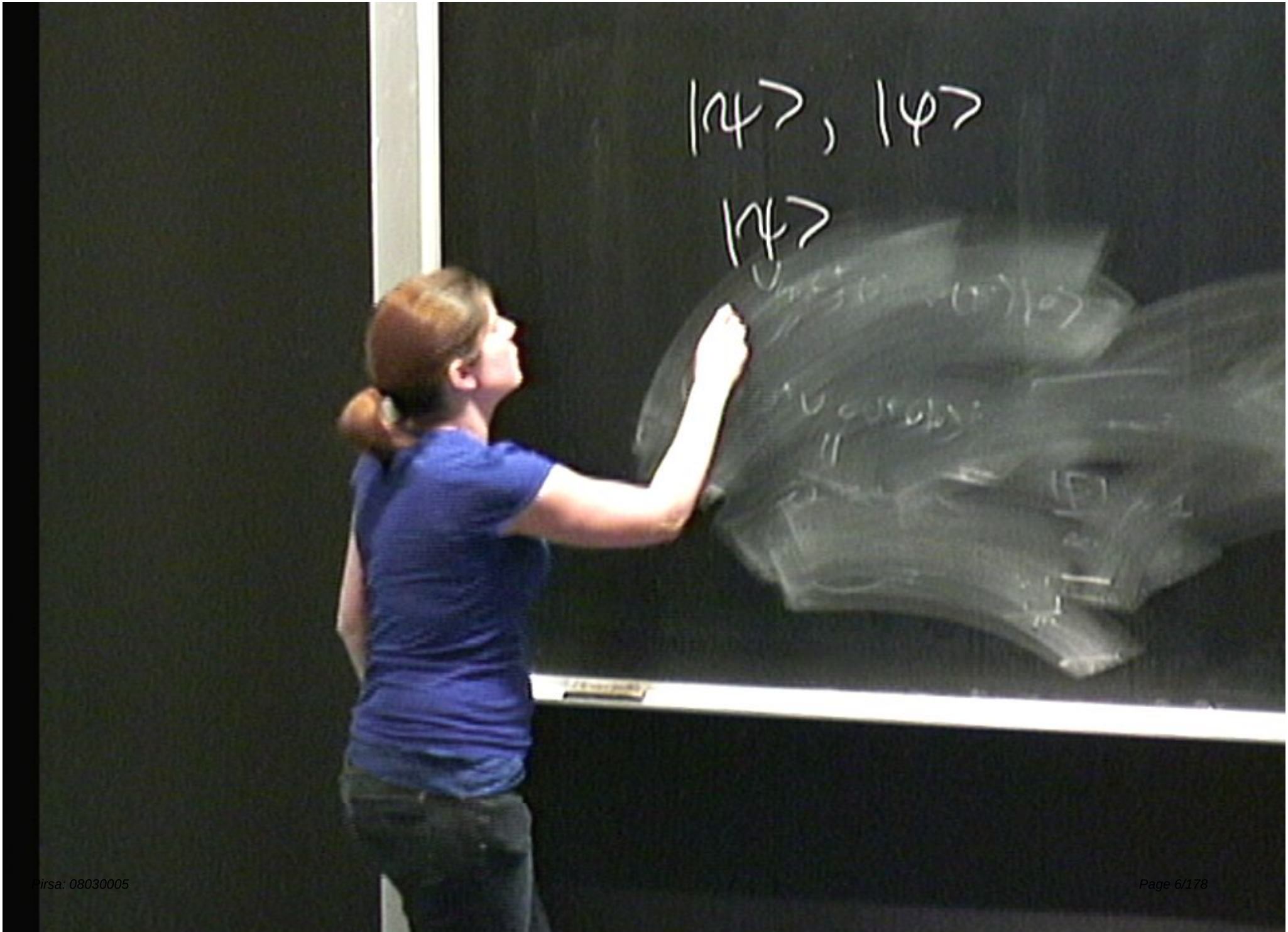
scroke@perimeterinstitute.ca

Quantum Key Distribution: BB84 Protocol

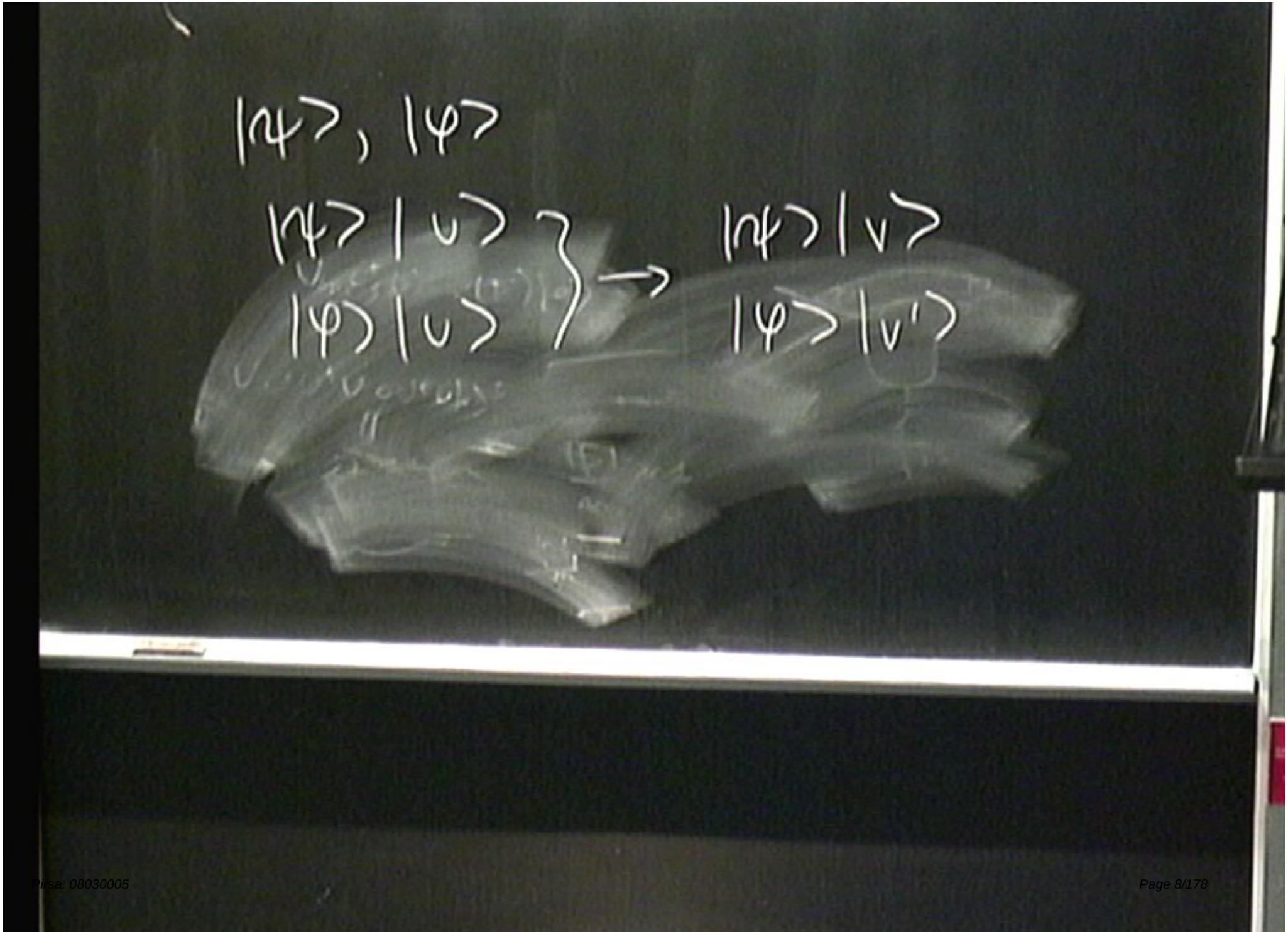
- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

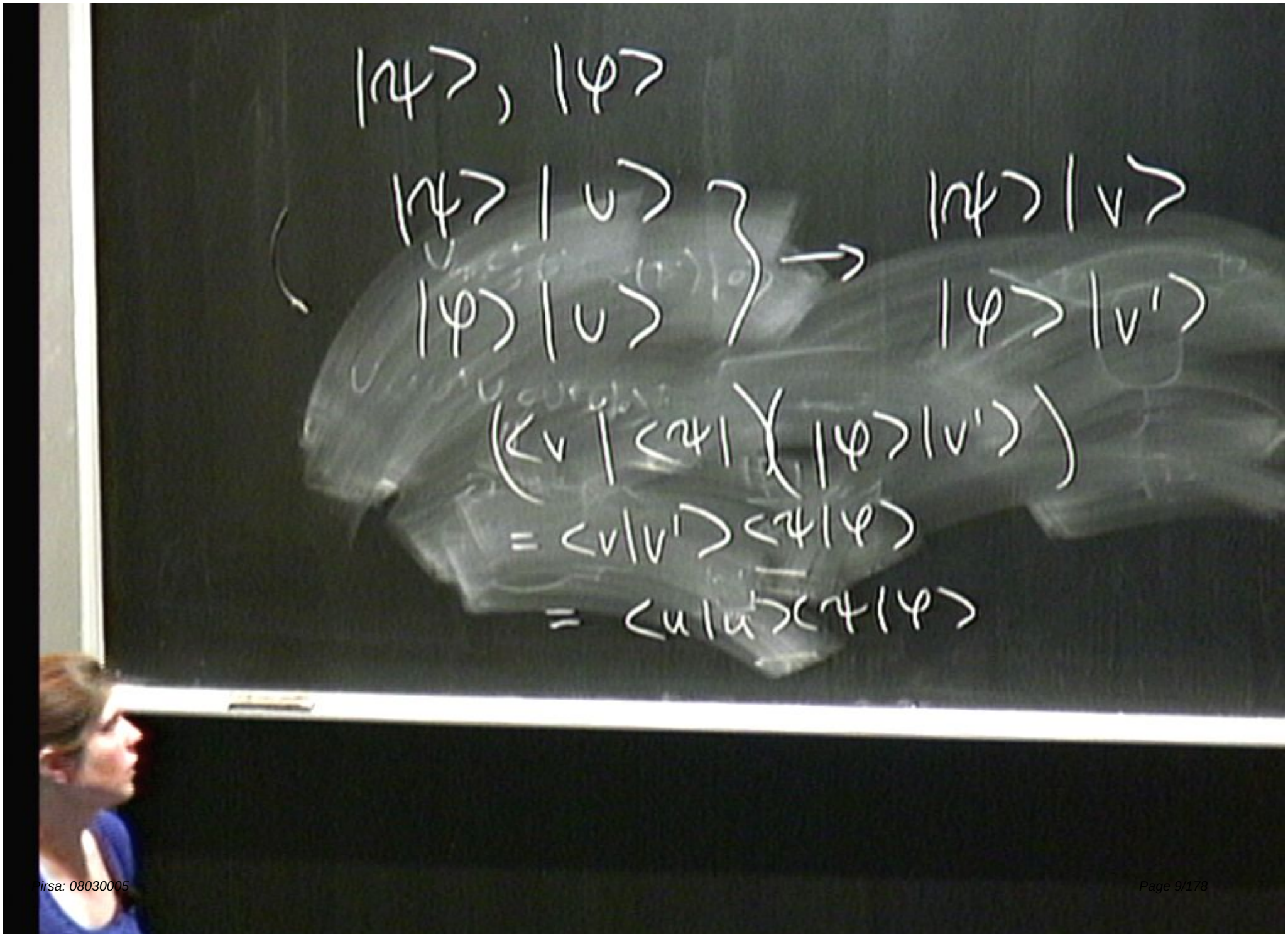



|4>, |4>

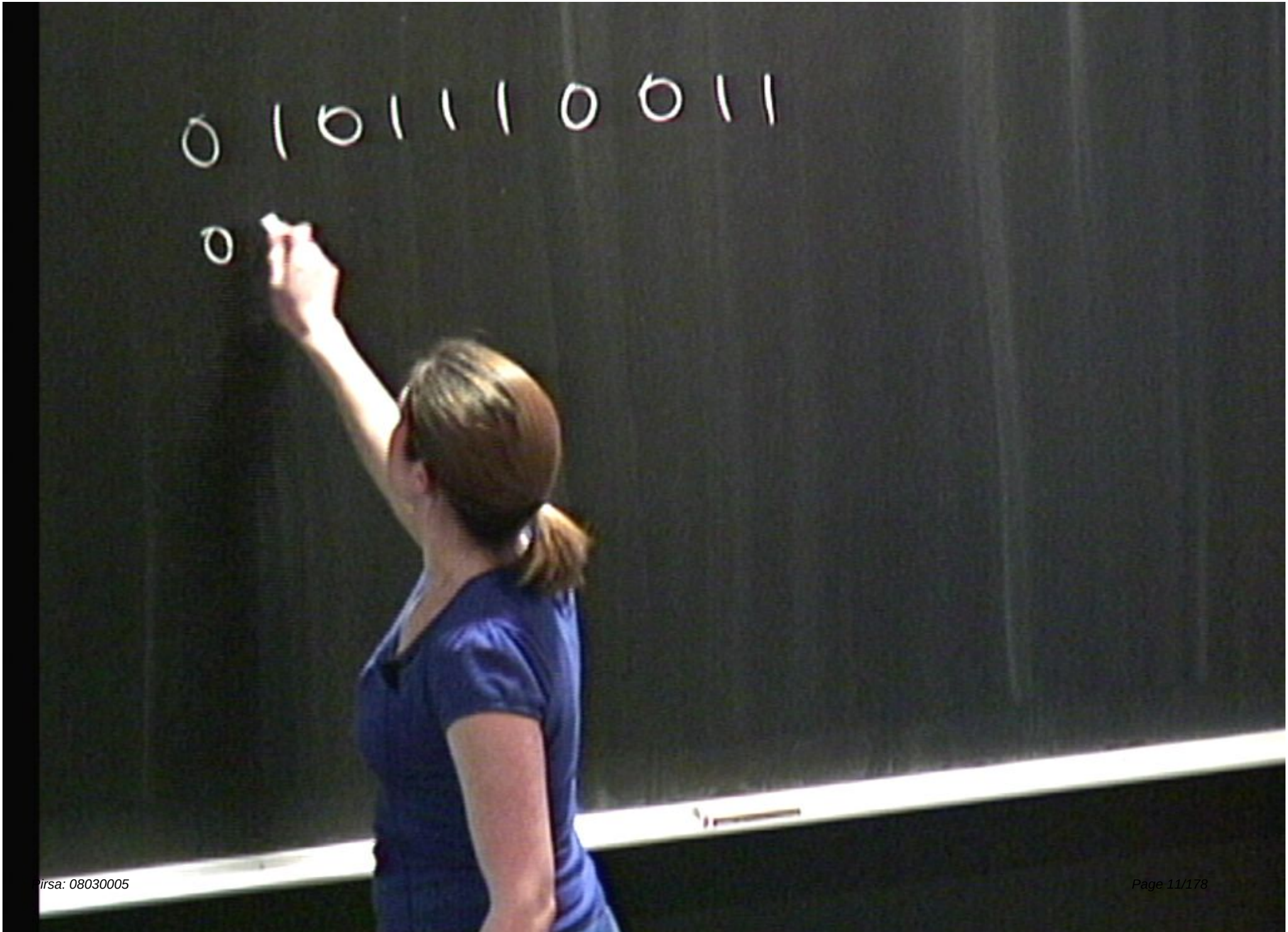

|ψ⟩, |φ⟩
|ψ⟩

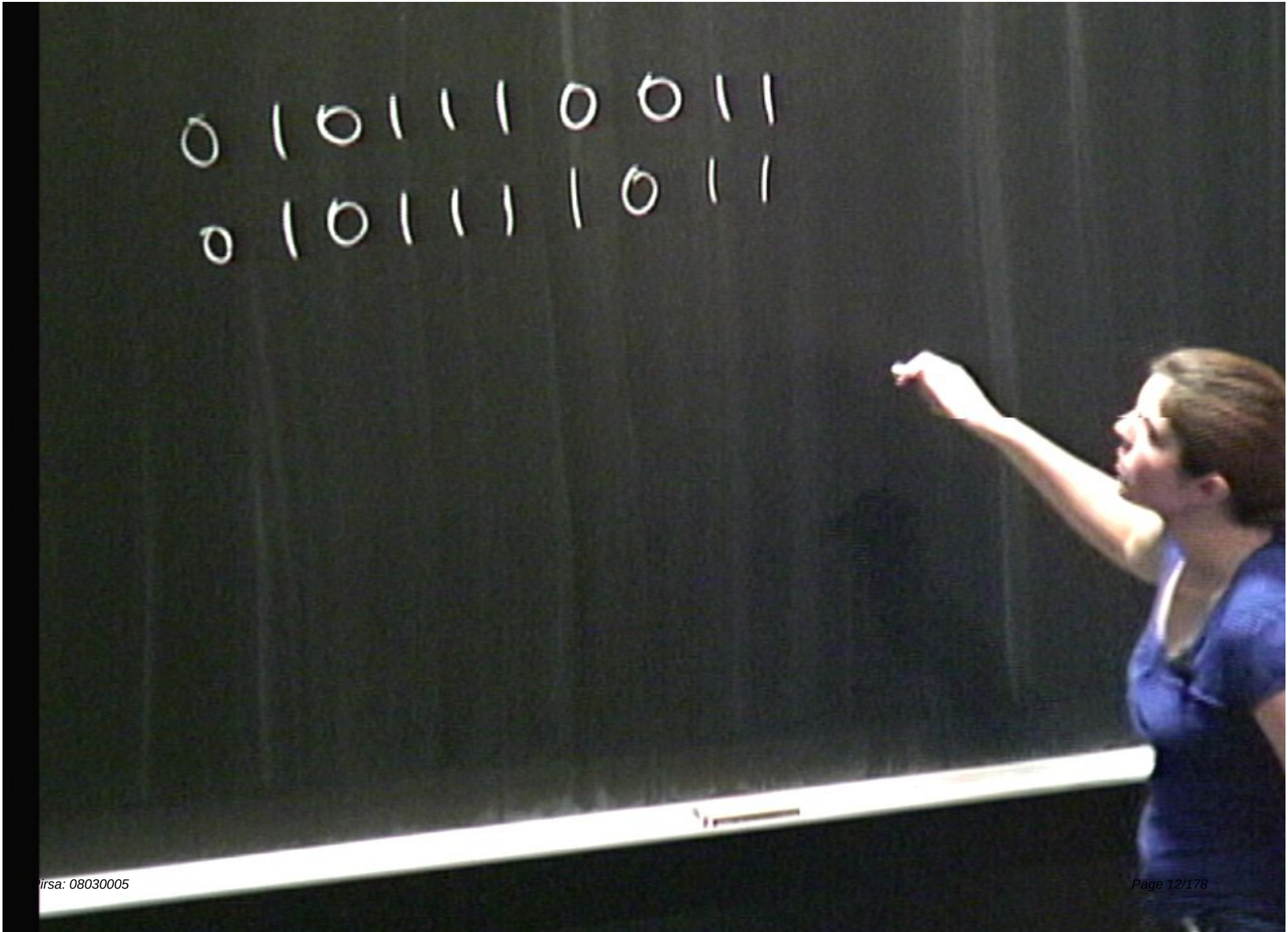

|ψ⟩, |φ⟩
|ψ⟩|υ⟩
|φ⟩|υ⟩


$|\psi\rangle, |\varphi\rangle$
$|\psi\rangle|v\rangle$
$|\varphi\rangle|v\rangle$
$\rightarrow$
$|\psi\rangle|v'\rangle$
$|\varphi\rangle|v'\rangle$


$|\psi\rangle, |\phi\rangle$
$\{|\psi\rangle|v\rangle, |\phi\rangle|v\rangle\} \to |\psi\rangle|v\rangle, |\phi\rangle|v'\rangle$
$(\langle v|\langle\psi|)(|\phi\rangle|v'\rangle)$
$= \langle v|v'\rangle\langle\psi|\phi\rangle$
$= \langle u|u'\rangle\langle\psi|\phi\rangle$


|ψ⟩, |φ⟩
{ |ψ⟩|v⟩ , |φ⟩|v⟩ } → |ψ⟩|v⟩ , |φ⟩|v'⟩
(⟨v|⟨ψ|)(|φ⟩|v'⟩)
= ⟨v|v'⟩⟨ψ|φ⟩
= |u'⟩⟨ψ|φ⟩

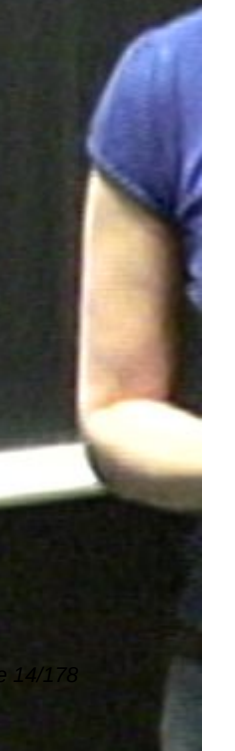

0 1 0 1 1 1 0 0 1 1
0

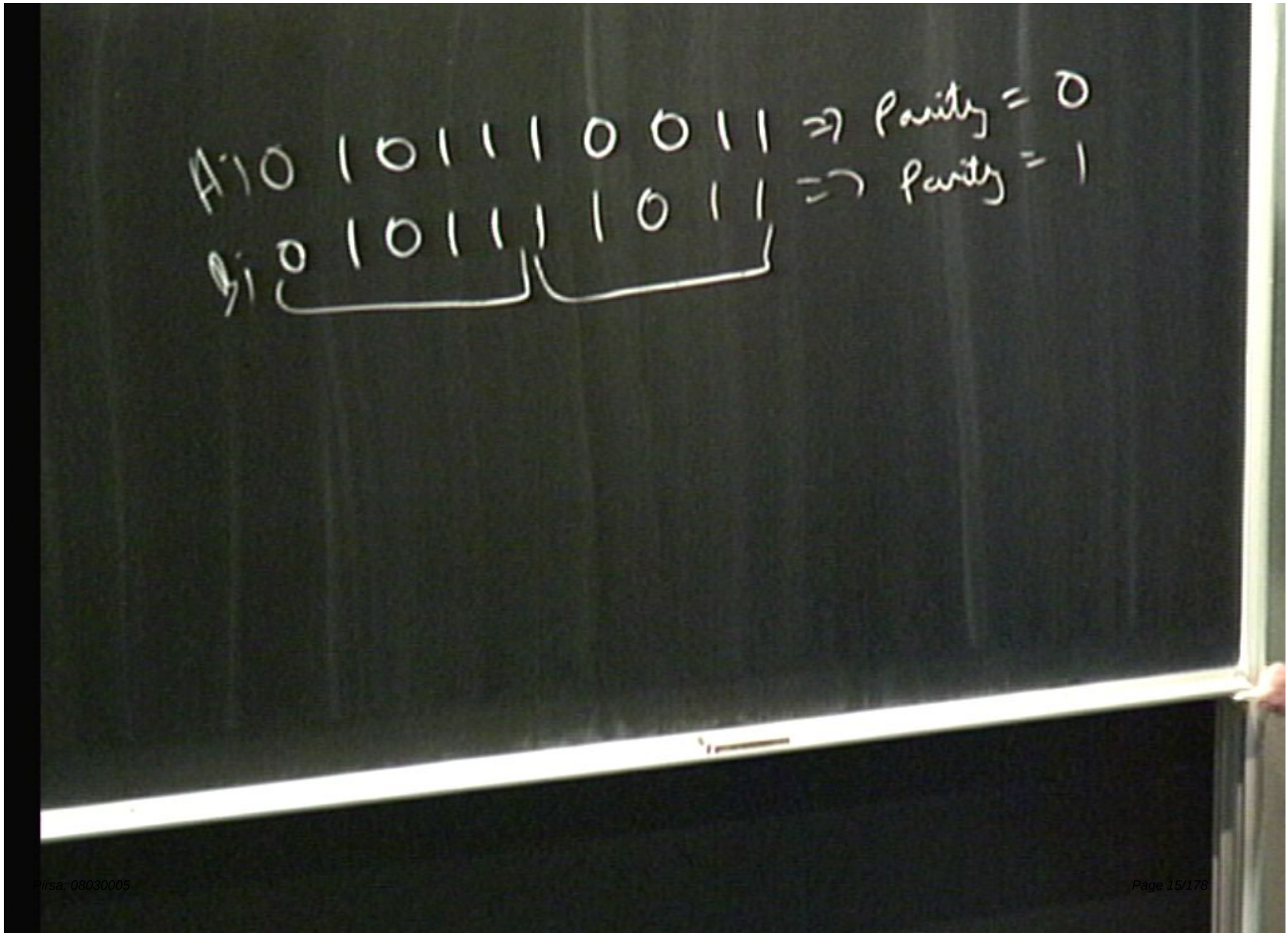

0 1 0 1 1 1 0 0 1 1
0 1 0 1 1 1 0 1 1


A:) 0 1 0 1 1 1 0 0 1 1
9; 0 1 0 1 1 1 0 1 1

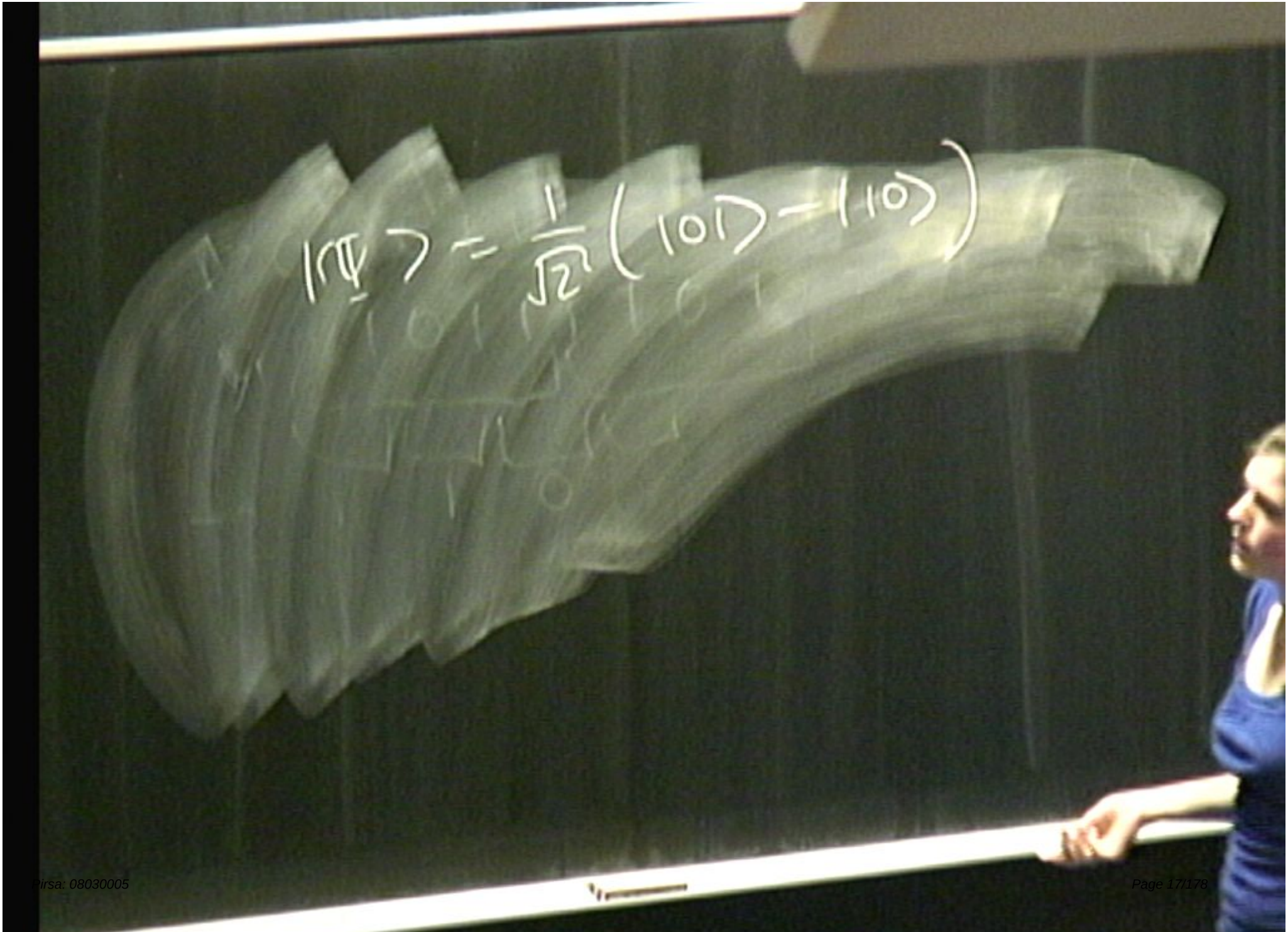
A: 1 0 1 0 1 1 1 1 0 0 1 1 ⇒ Parity = 0

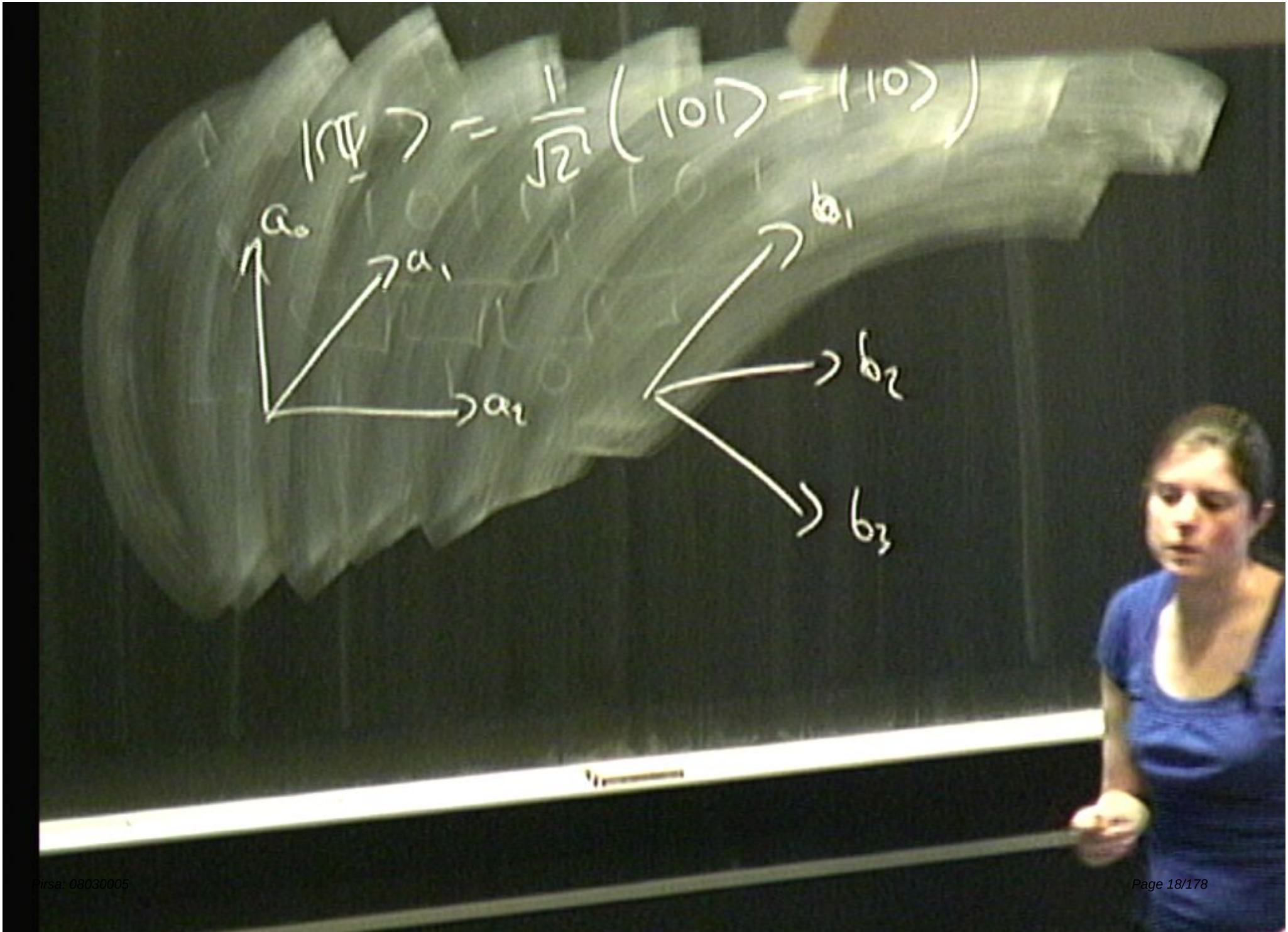
B: 0 1 0 1 1 1 1 0 1 1 ⇒ Parity = 1

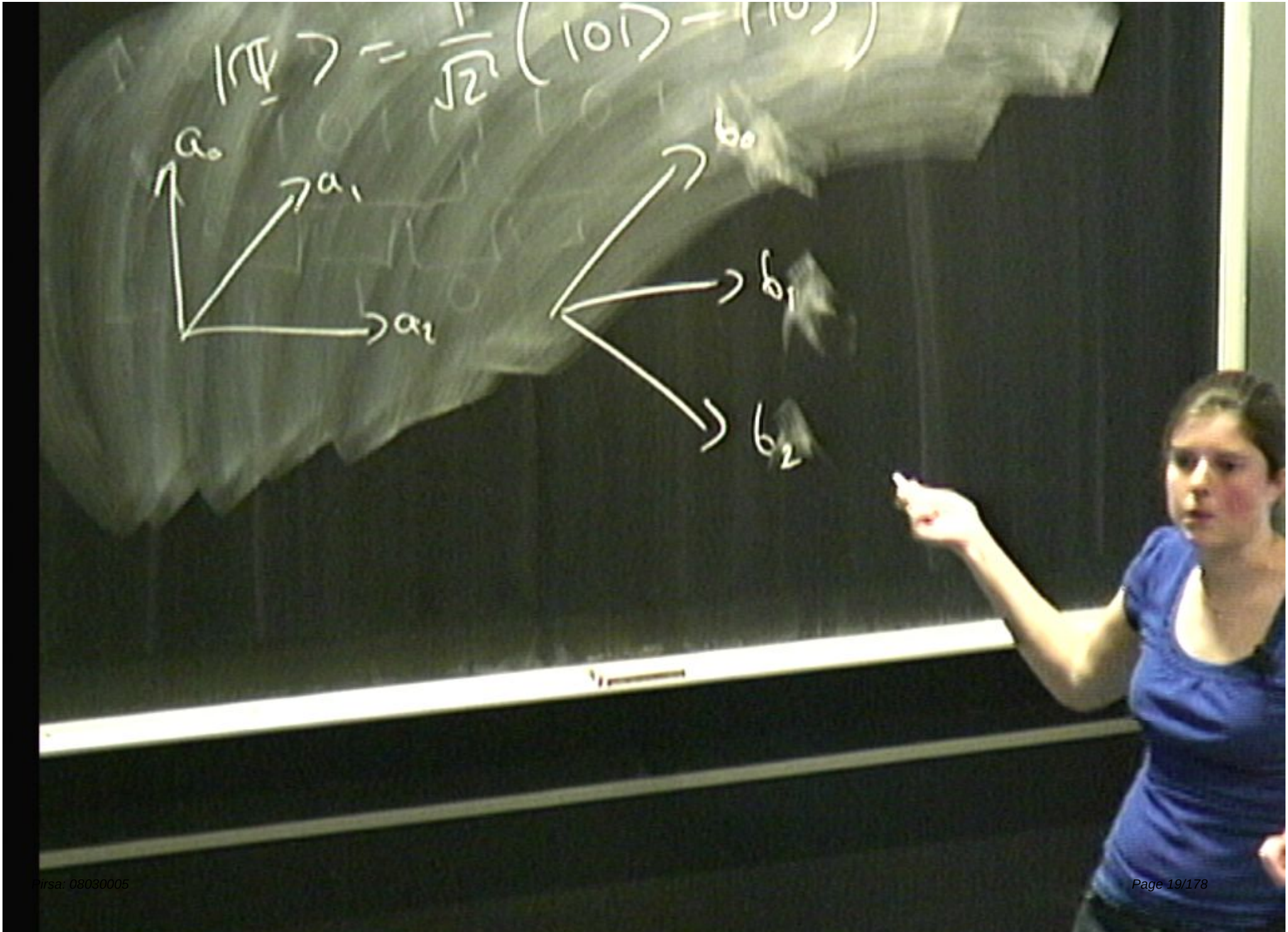



A: 1 0 1 0 1 1 1 1 0 0 1 1 => Parity = 0
B: 0 1 0 1 1 1 1 0 1 1 => Parity = 1


A: 10 1011100 11 ⇒ Parity = 0
B: 0 1011 1011 ⇒ Parity = 1
→ 1 1 0


$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$


$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
a_0
a_1
a_2
b_1
b_2
b_3


$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
a_0
a_1
a_2
b_0
b_1
b_2

Quantum key Distribution: E91 Protocol

- Alice and Bob share Bell states (from a common source, or e.g. Alice creates entangled states and sends one of each pair to Bob).
- Alice and Bob each choose at random in which of three possible bases to measure.
- Basis reconciliation; Alice and Bob announce the bases used, and divide their bits into two groups –those in which they used the same basis and those in which they used different bases.
- In the subset in which they used different bases they check that their results give maximum violation of Bell's inequality. If they do not they conclude there was some noise or eavesdropping on the channel.
- The remaining bits form the private shared key.
- This protocol may be useful in the future for key storage.

Quantum key Distribution: E91 Protocol

- Alice and Bob share Bell states (from a common source, or e.g. Alice creates entangled states and sends one of each pair to Bob).
- Alice and Bob each choose at random in which of three possible bases to measure.
- Basis reconciliation; Alice and Bob announce the bases used, and divide their bits into two groups –those in which they used the same basis and those in which they used different bases.
- In the subset in which they used different bases they check that their results give maximum violation of Bell's inequality. If they do not they conclude there was some noise or eavesdropping on the channel.
- The remaining bits form the private shared key.
- This protocol may be useful in the future for key storage.

Quantum Key Distribution: BB84 Protocol

- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

Quantum key Distribution: E91 Protocol

- Alice and Bob share Bell states (from a common source, or e.g. Alice creates entangled states and sends one of each pair to Bob).
- Alice and Bob each choose at random in which of three possible bases to measure.
- Basis reconciliation; Alice and Bob announce the bases used, and divide their bits into two groups –those in which they used the same basis and those in which they used different bases.
- In the subset in which they used different bases they check that their results give maximum violation of Bell's inequality. If they do not they conclude there was some noise or eavesdropping on the channel.
- The remaining bits form the private shared key.
- This protocol may be useful in the future for key storage.

Quantum Key Distribution: BB84 Protocol

- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

Quantum key Distribution: E91 Protocol

- Alice and Bob share Bell states (from a common source, or e.g. Alice creates entangled states and sends one of each pair to Bob).
- Alice and Bob each choose at random in which of three possible bases to measure.
- Basis reconciliation; Alice and Bob announce the bases used, and divide their bits into two groups –those in which they used the same basis and those in which they used different bases.
- In the subset in which they used different bases they check that their results give maximum violation of Bell's inequality. If they do not they conclude there was some noise or eavesdropping on the channel.
- The remaining bits form the private shared key.
- This protocol may be useful in the future for key storage.

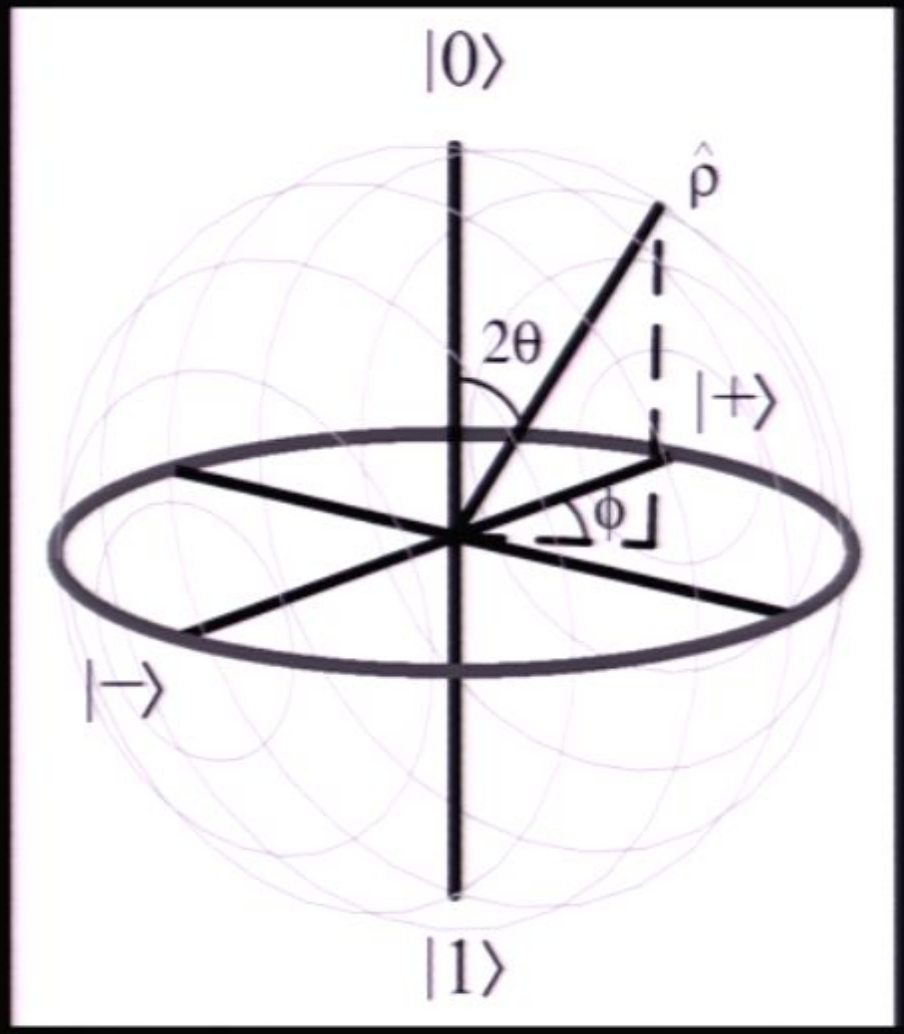
Quantum Key Distribution: BB84 Protocol

- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

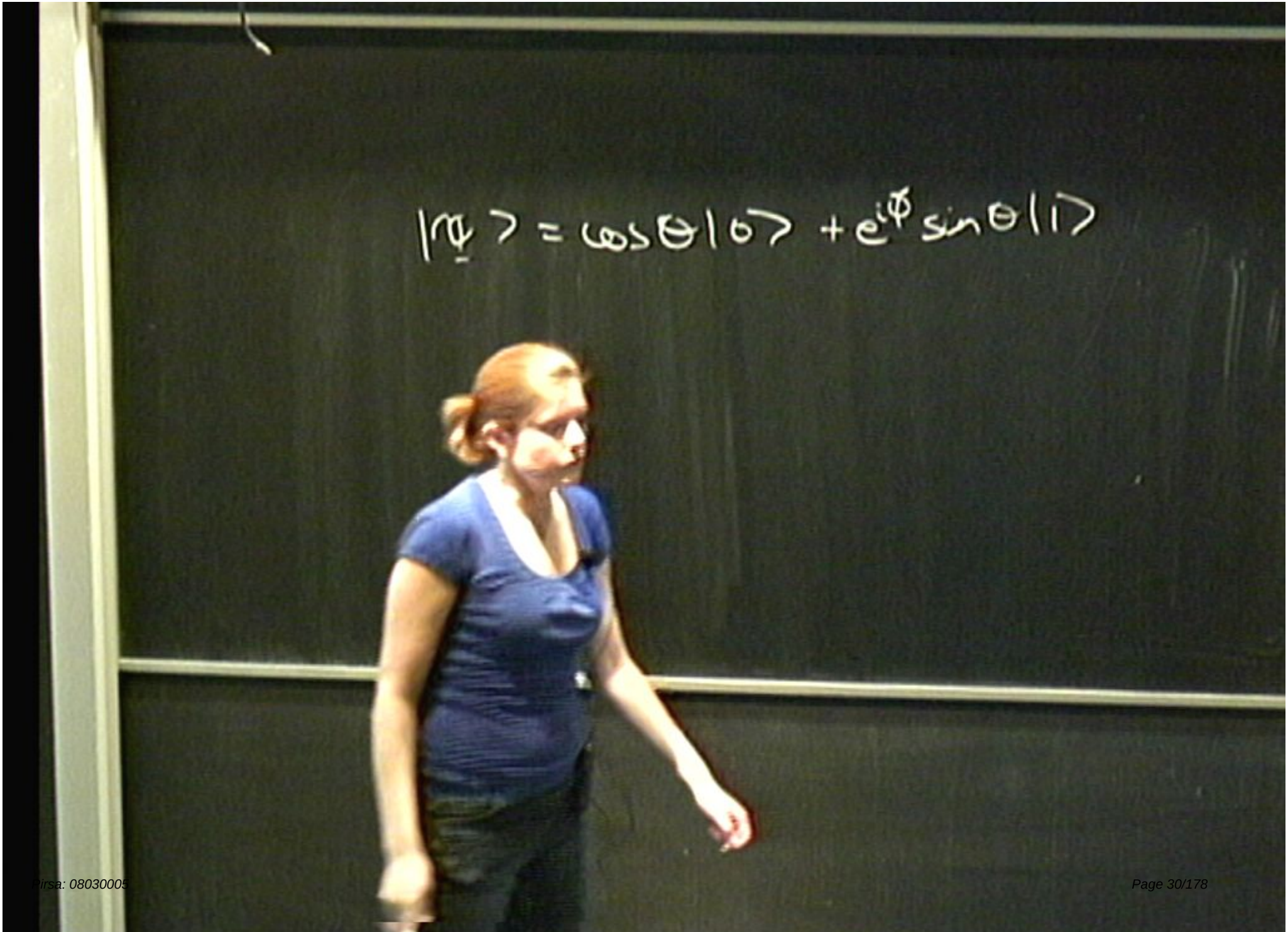
Error Correction and Privacy Amplification

- In any experimental implementation there will always be errors introduced in the channel.
- Assume that all errors are due to Eve.
- If the error rate is too high, abort the protocol and try again.
- If the error rate is acceptable, use error correction and privacy amplification to distill a secure key.

Density operators and the Bloch sphere representation of states.



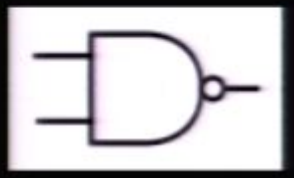
$$|\hat{n}\rangle = \cos\theta|0\rangle + e^{i\phi}$$


$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$

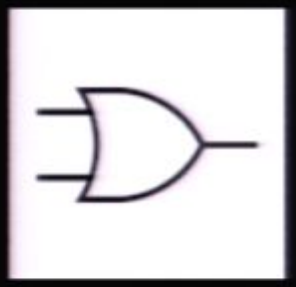
Classical Logic Gates

- AND

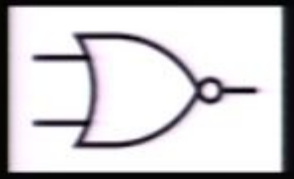
- NAND



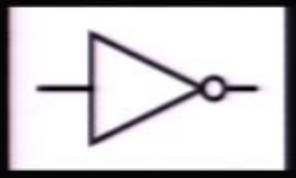
- OR



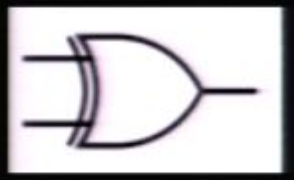
- NOR



- NOT



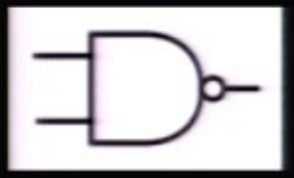
- XOR



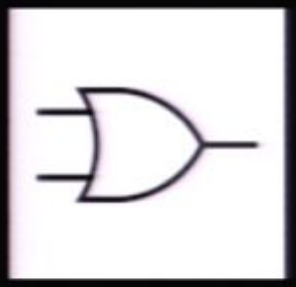
Classical Logic Gates

- AND

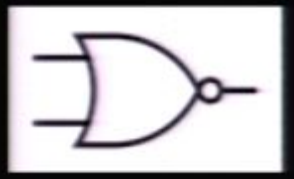
- NAND



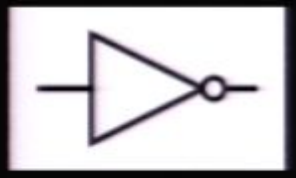
- OR



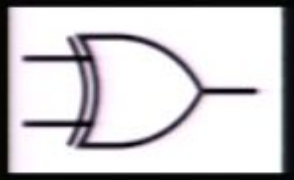
- NOR

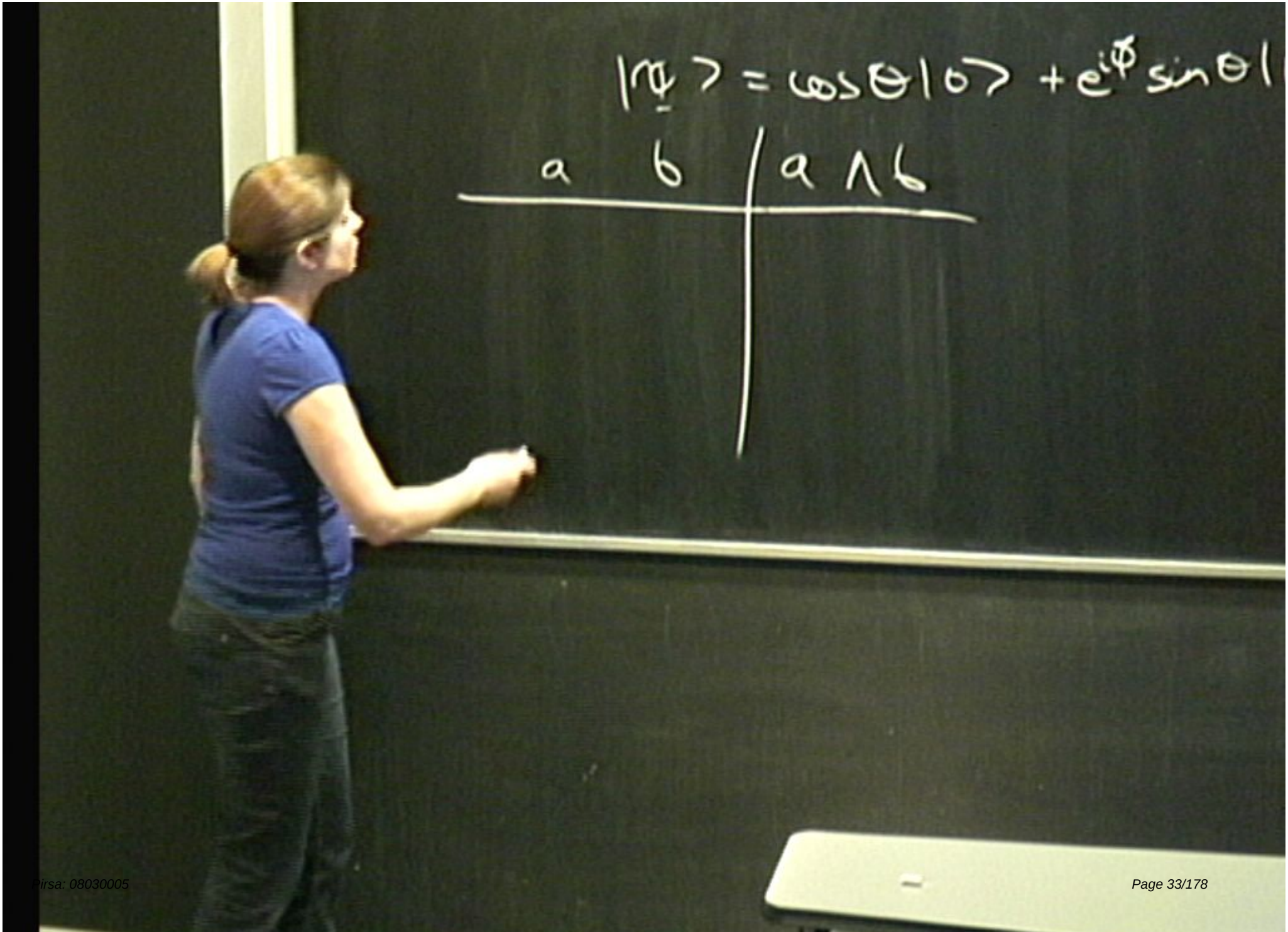


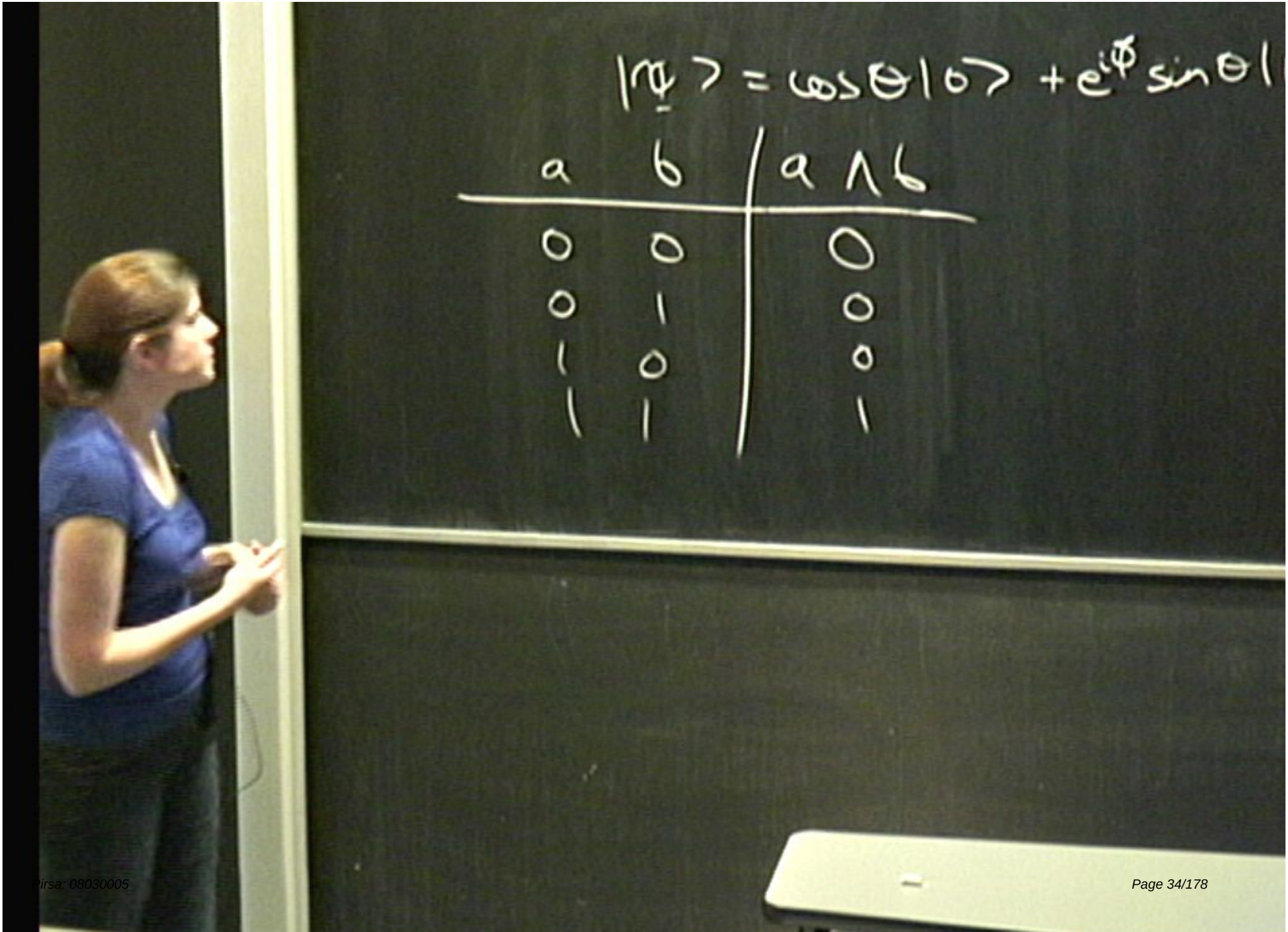
- NOT

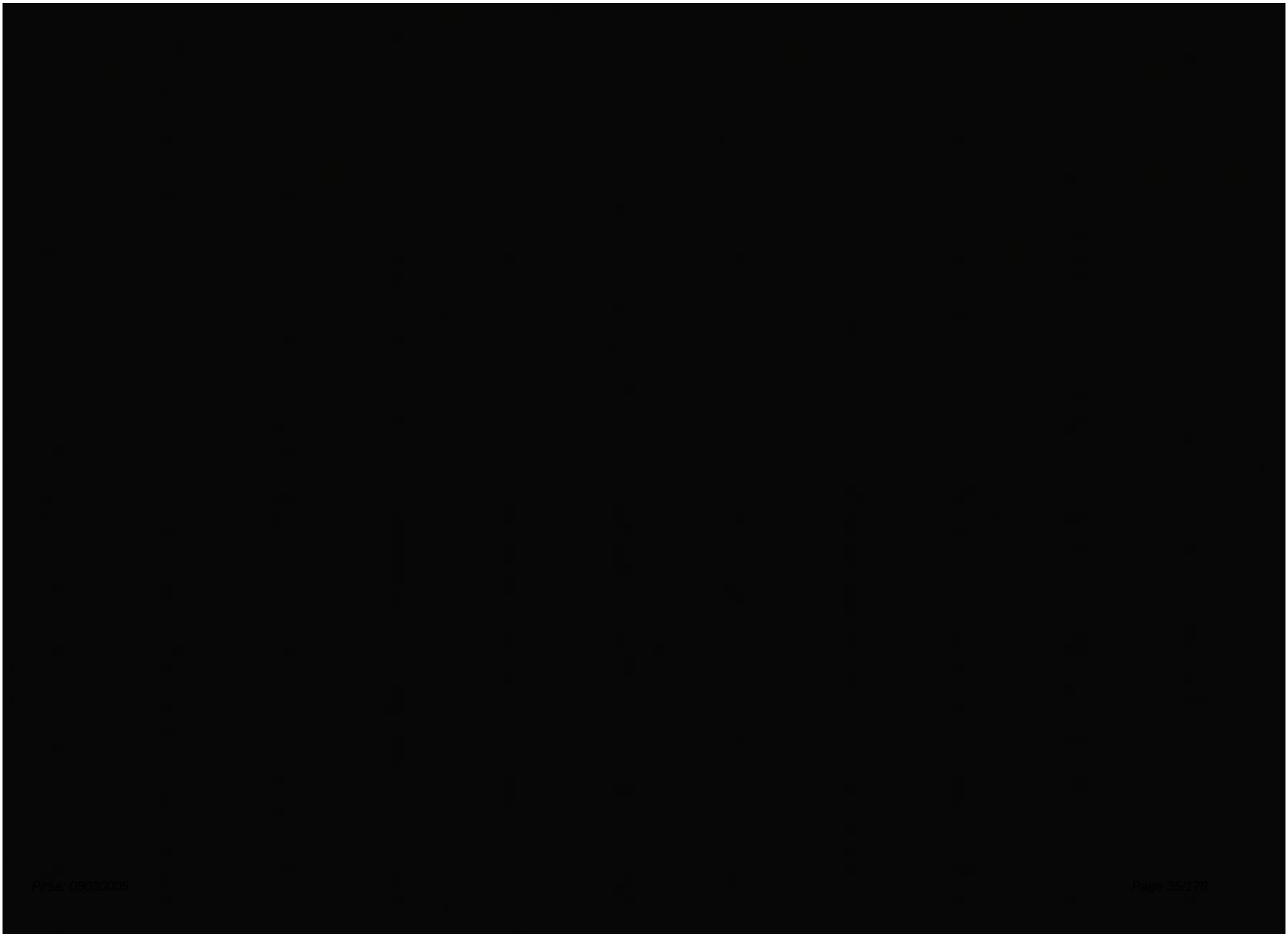


- XOR




$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|$
a b | a ∧ b

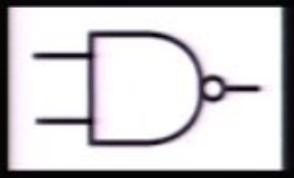

$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|$
a b | a ∧ b
0 0 | 0
0 1 | 0
1 0 | 0
1 1 | 1



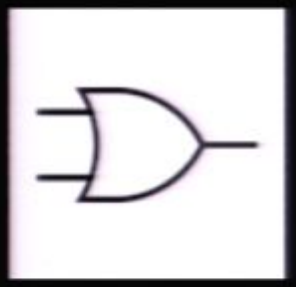
Classical Logic Gates

- AND

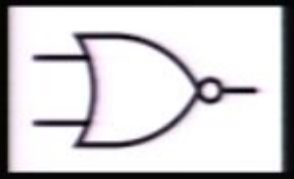
- NAND



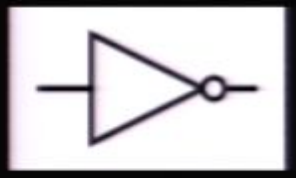
- OR



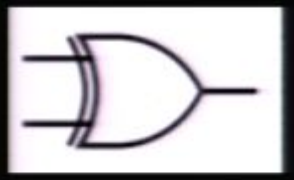
- NOR

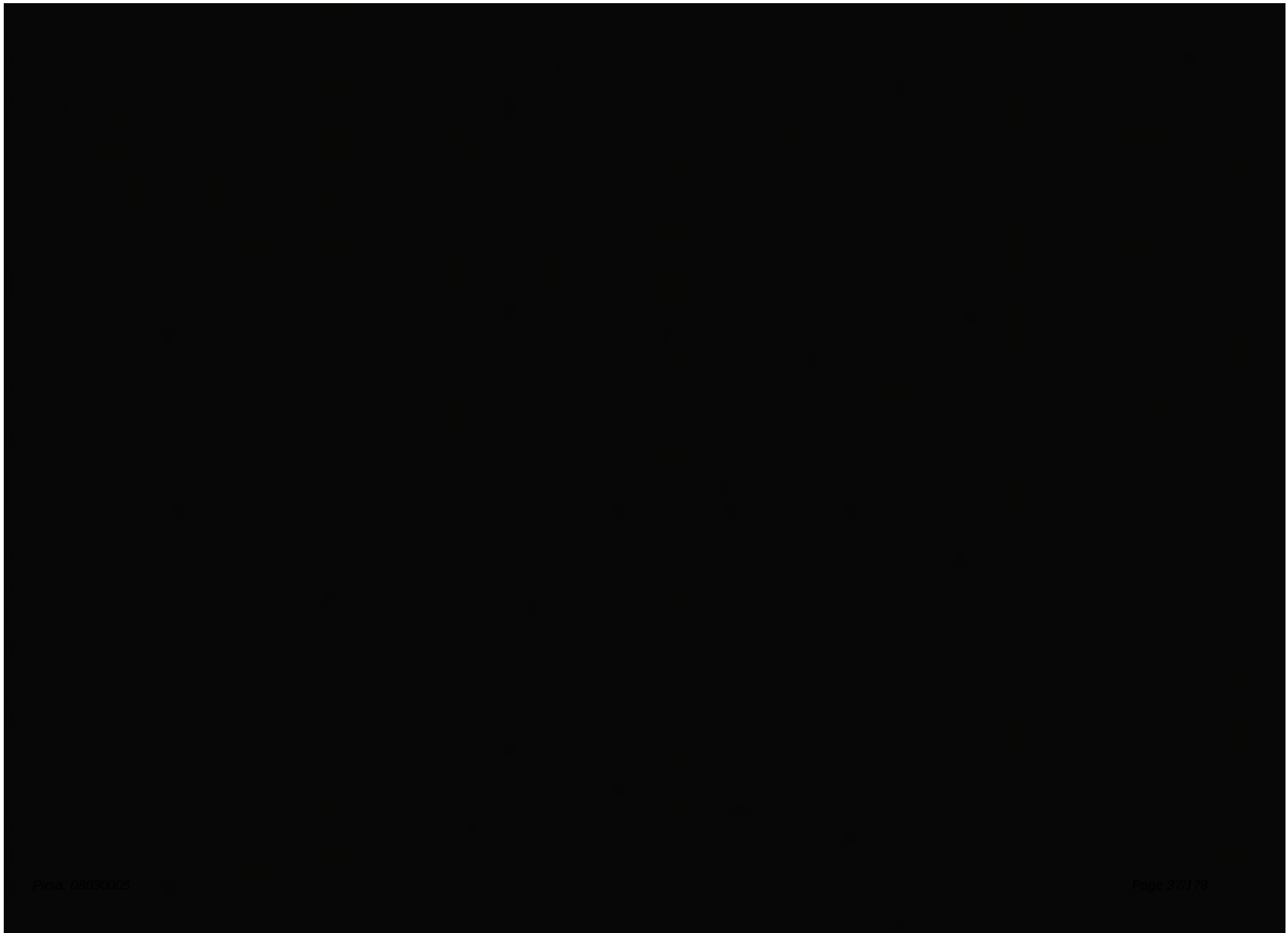


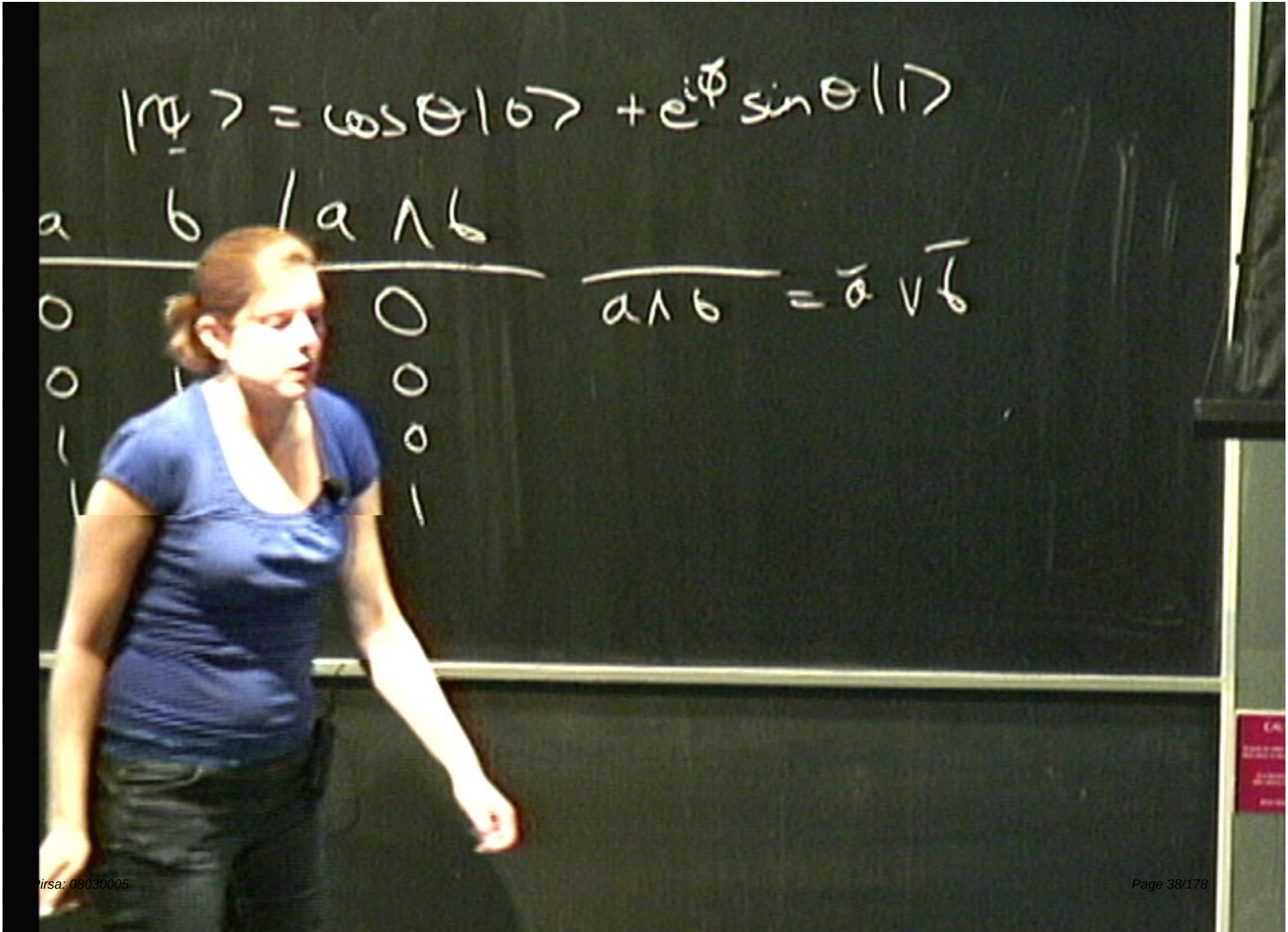
- NOT



- XOR

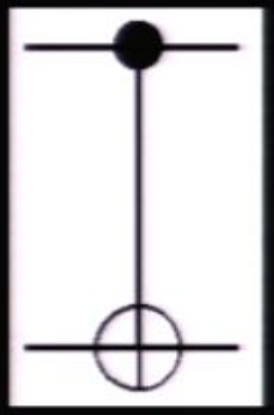





$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$
a b | a ∧ b
0 0 0
0 1 0
1 0 0
1 1 1
$\overline{a \wedge b} = \bar{a} \vee \bar{b}$

Controlled Logic Gates

- CNOT



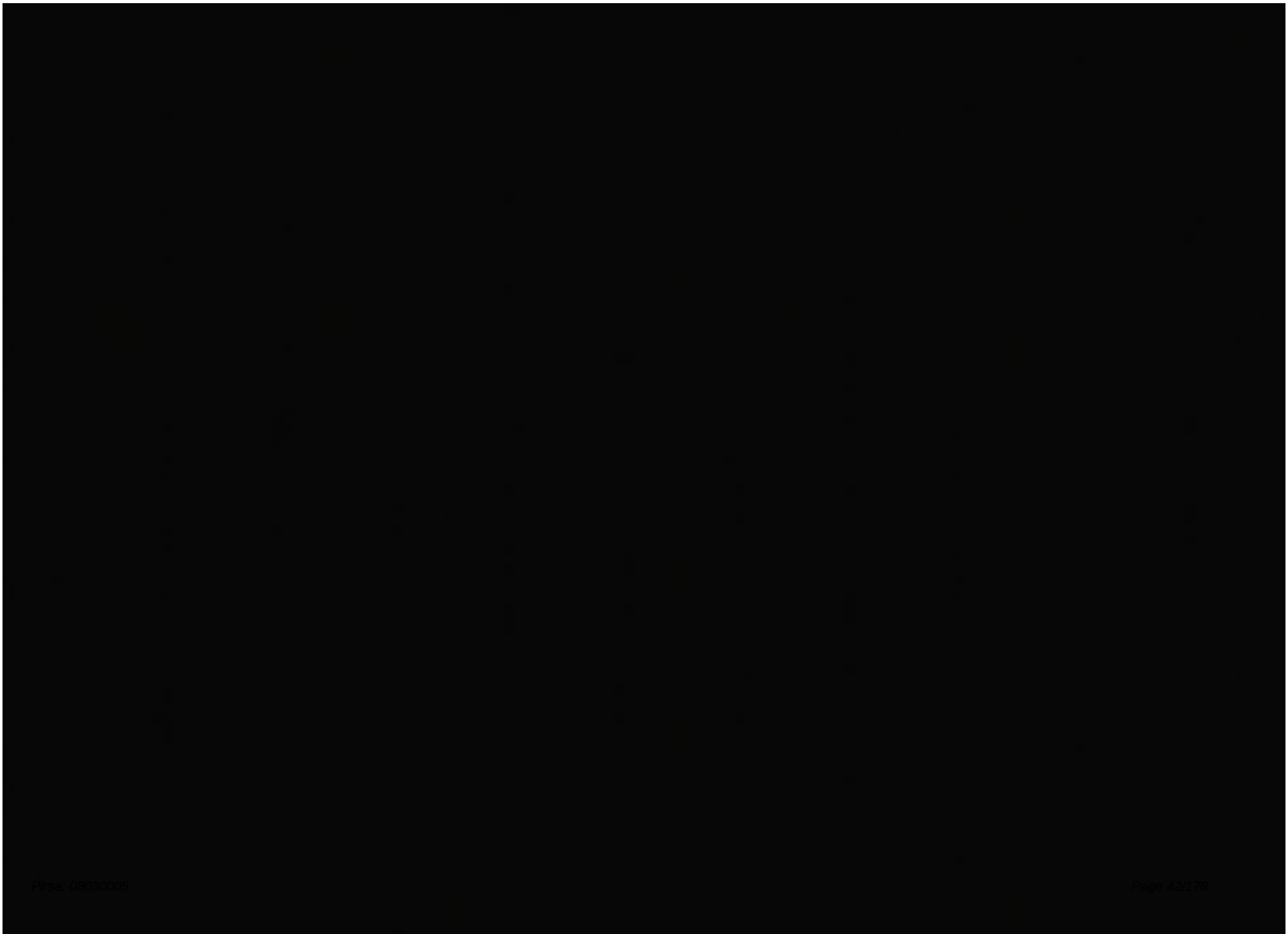
- Toffoli

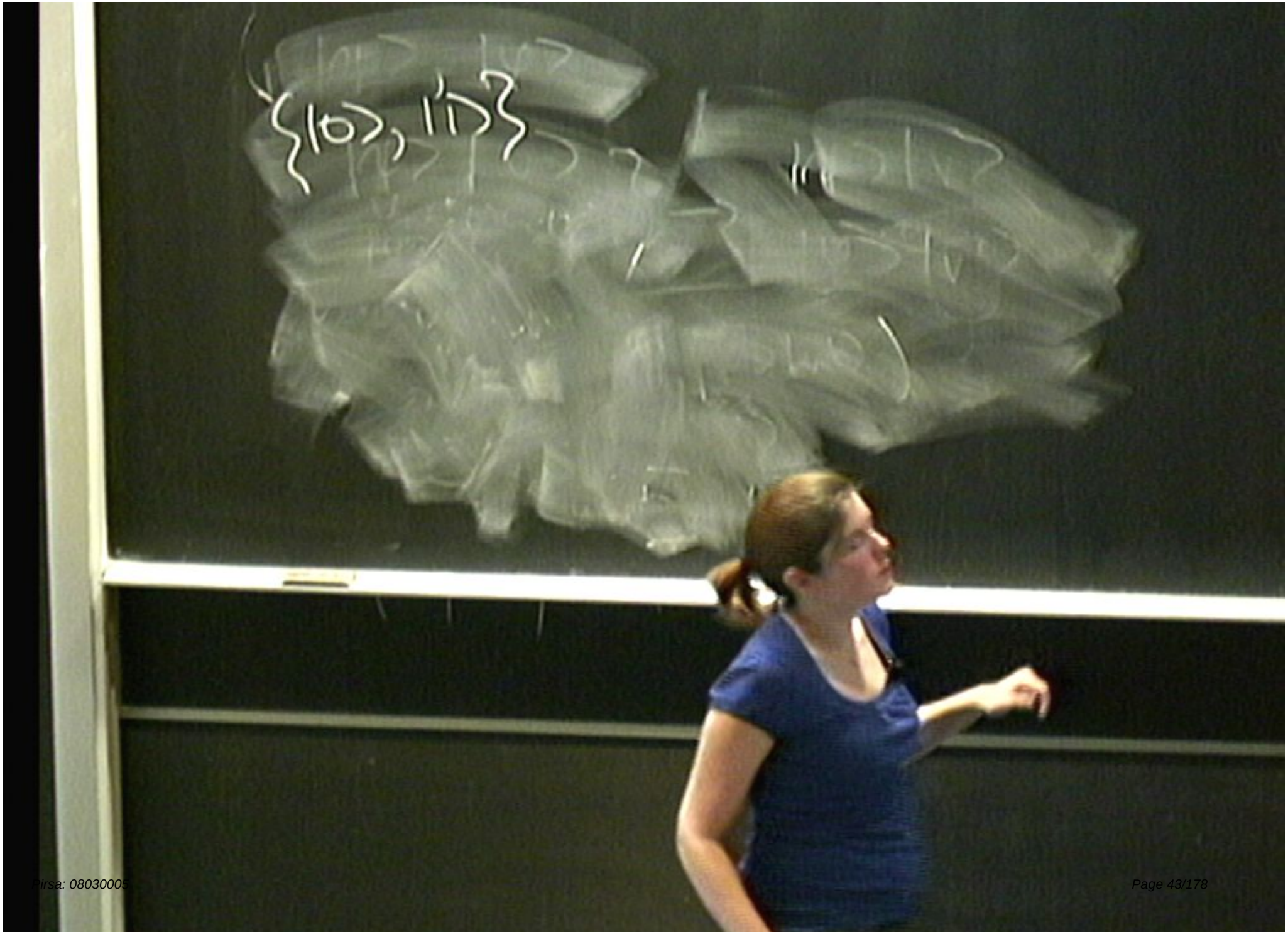
Quantum Computing

- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.

Quantum Computing

- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.



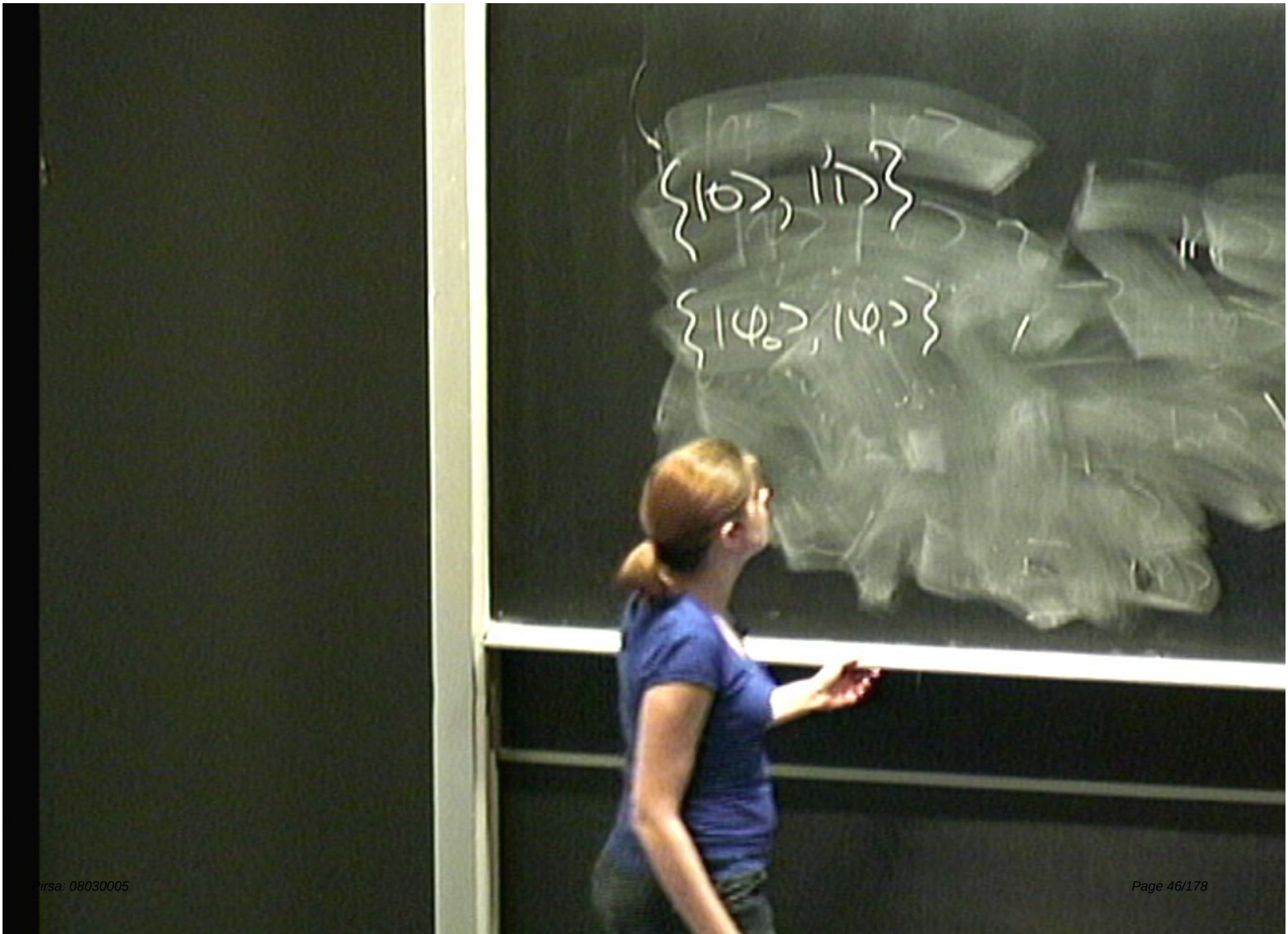


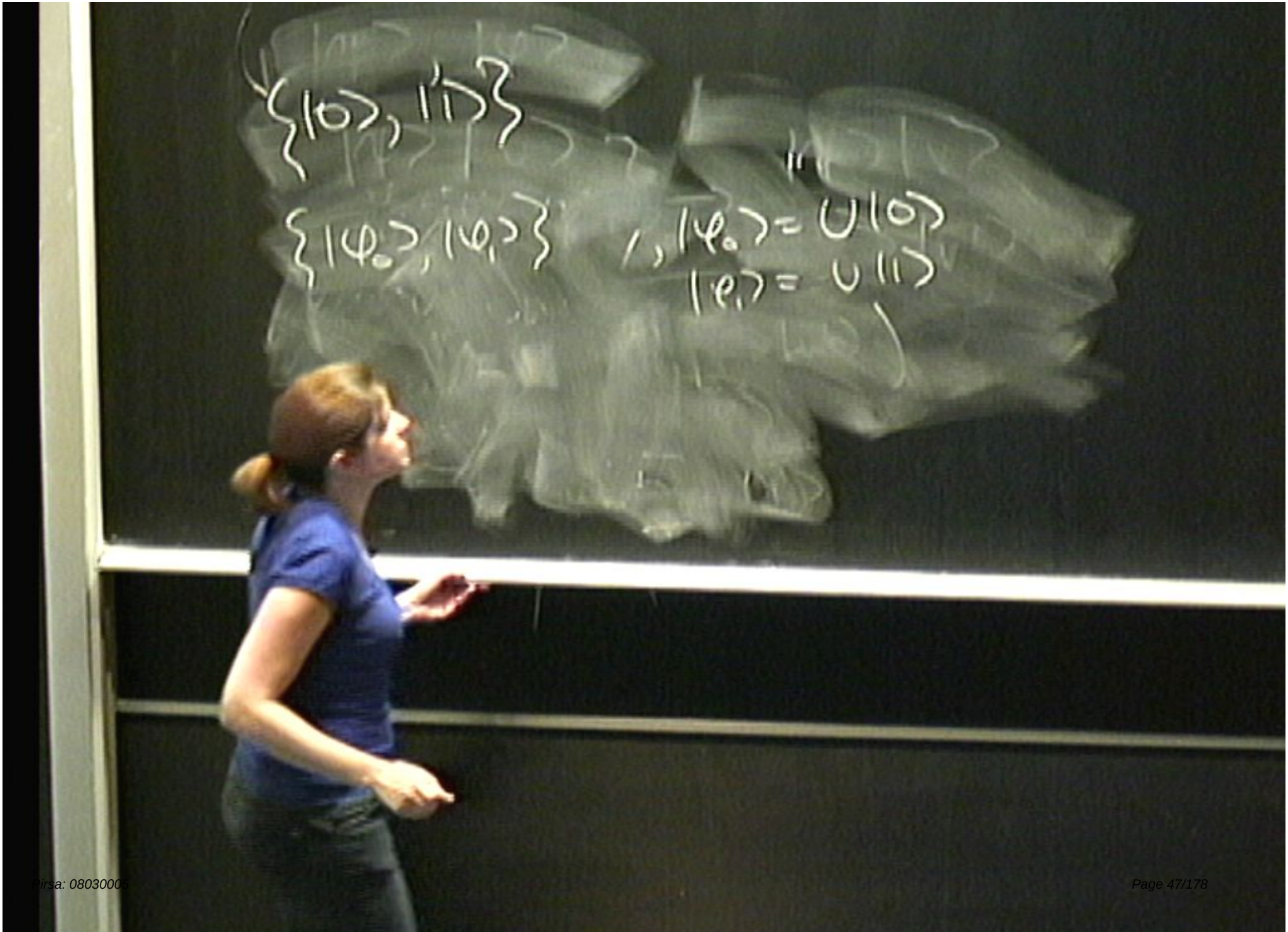
Quantum Computing

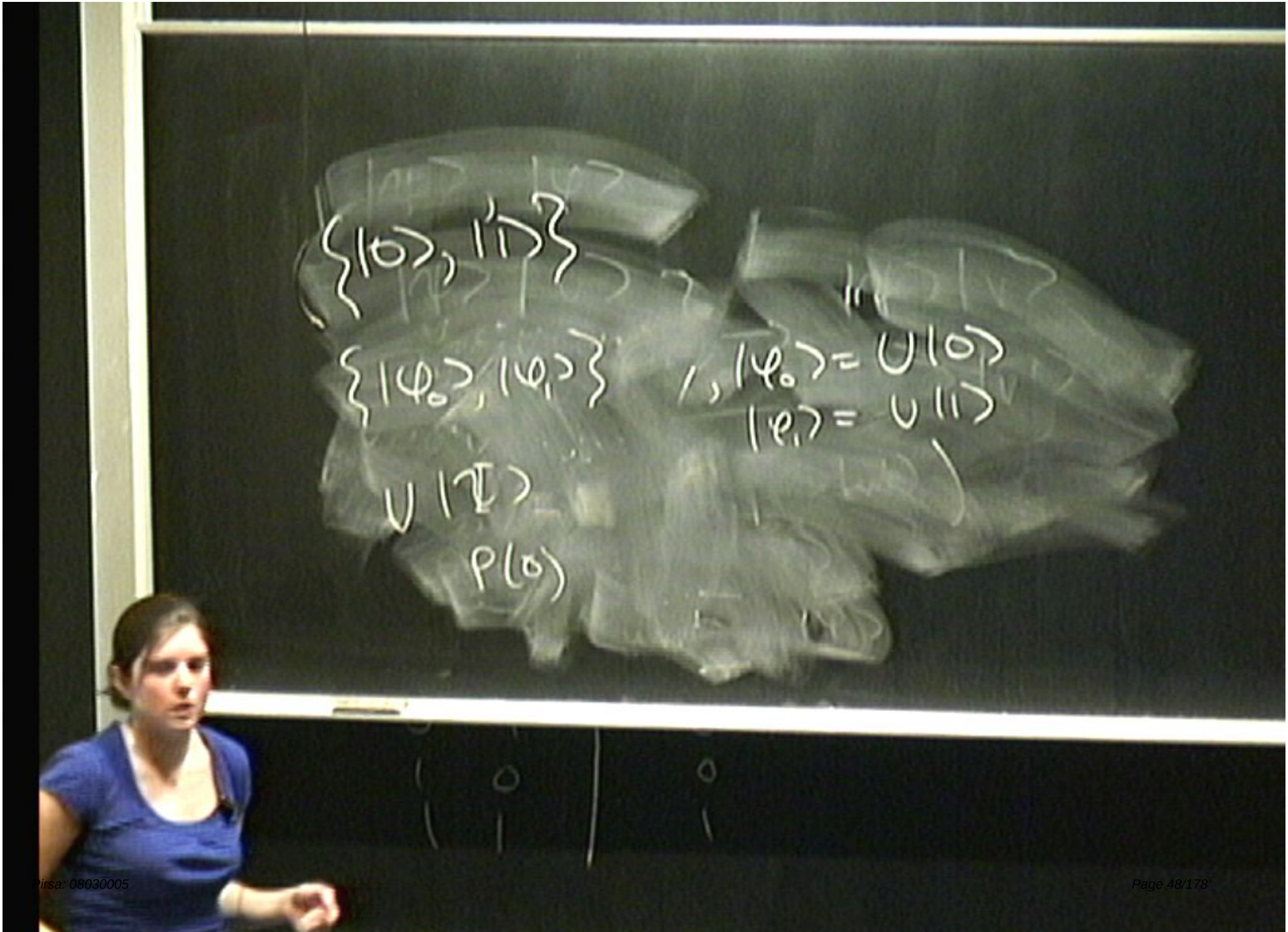
- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.

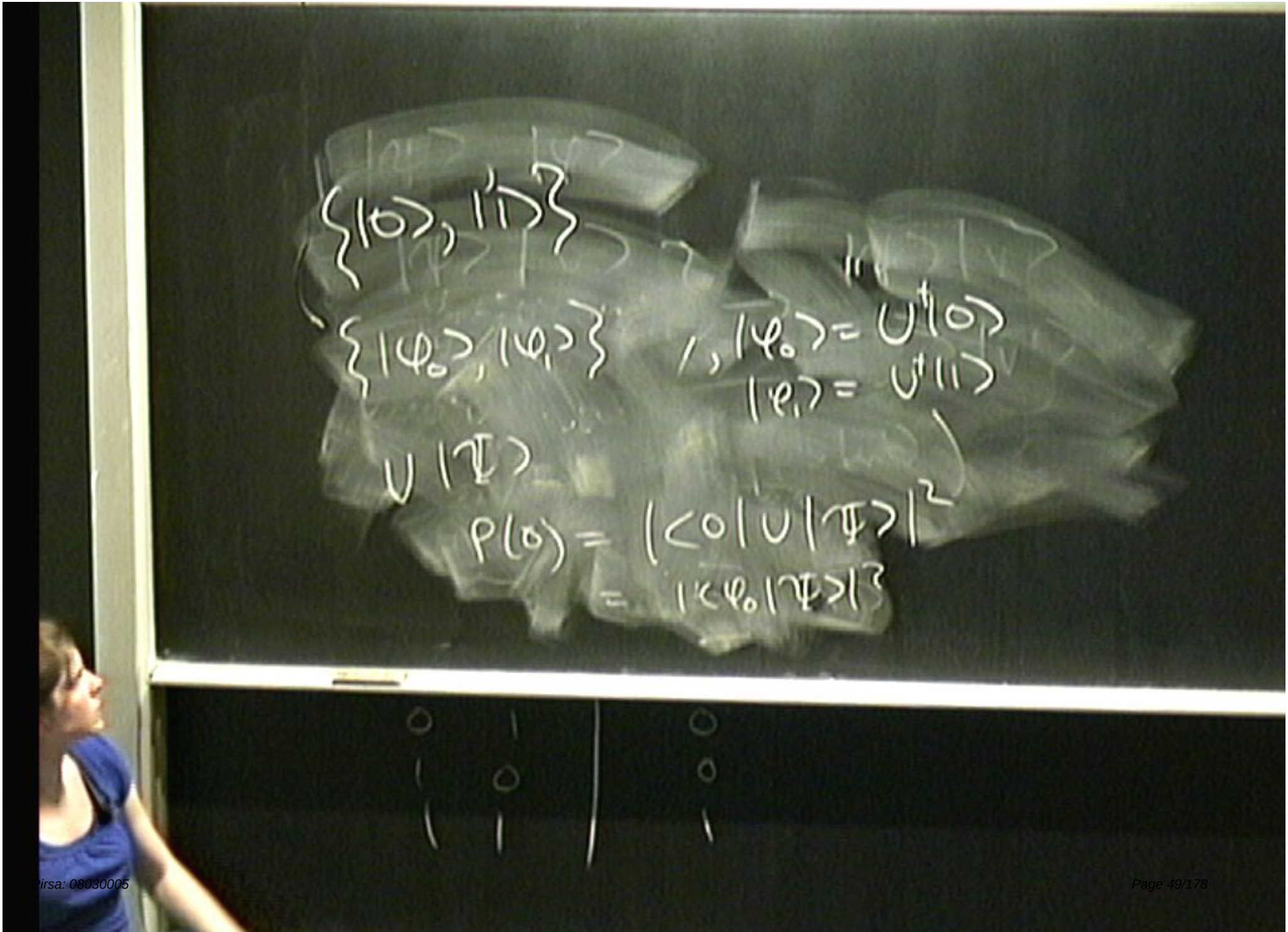
Quantum Computing

- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.


{|0⟩, |1⟩}
{|φ0⟩, |φ1⟩}


{|0⟩, |1⟩}
{|φ0⟩, |φ1⟩}
, |φ0⟩ = U|0⟩
|φ1⟩ = U|1⟩


{|0⟩, |1⟩}
{|φ0⟩, |φ1⟩}
U|ψ⟩
P(0)
|φ0⟩ = U|0⟩
|φ1⟩ = U|1⟩


{|0>, |1>}
{|φ0>, |φ1>}
|φ0> = U†|0>
|φ1> = U†|1>
U|Ψ>
P(0) = |<0|U|Ψ>|²
= |<φ0|Ψ>|²

Quantum Computing

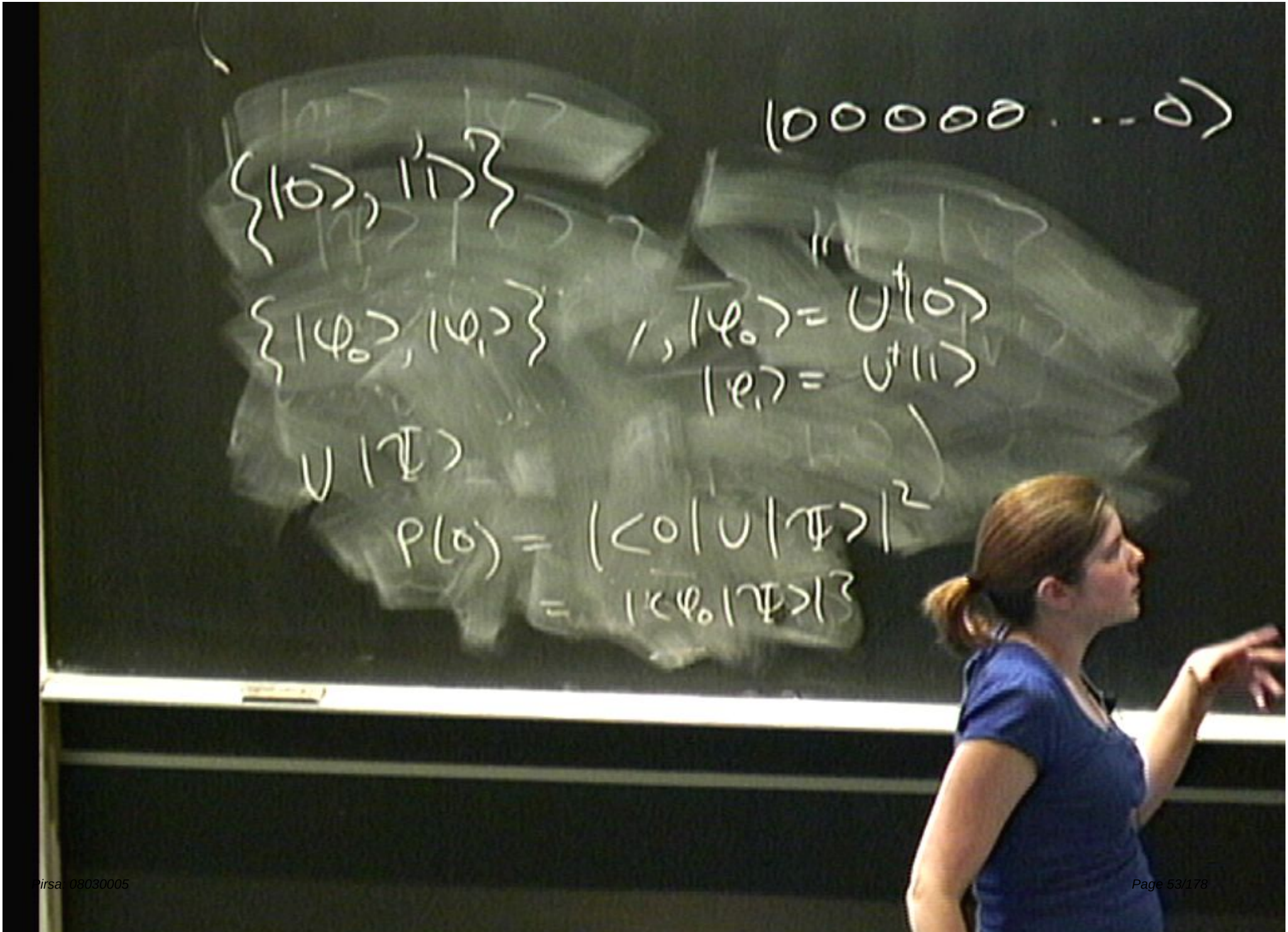
- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.

Quantum Computing

- A two-level system can be used as a qubit if:
  - It can be prepared in some well-defined state, the *fiducial* state of the qubit;
  - Any state can be transformed into any other state (unitary transformations);
  - The qubit state can be measured in the computational basis.

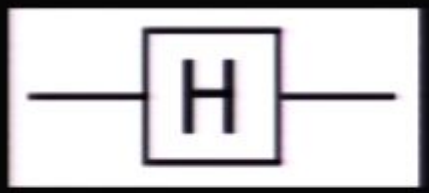
Quantum Computing

- In order to perform a quantum computation, should be able to:
  - Prepare the computer in a well-defined initial state, the *fiducial* state of the computer;
  - Perform any given unitary transformation;
  - Perform, at the end of the algorithm, a measurement in the computational basis.


|00000...0⟩
{|0⟩, |1⟩}
{|φ0⟩, |φ1⟩}
|φ0⟩ = U†|0⟩
|φ1⟩ = U†|1⟩
U|ψ⟩
P(0) = |⟨0|U|ψ⟩|²
= |⟨φ0|ψ⟩|²

Quantum logic gates

- Hadamard gate

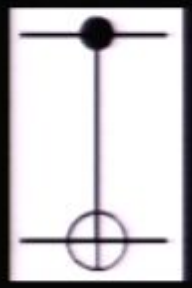


- Single qubit Unitary

- Phase-shift gate

$$R(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

- Controlled-NOT gate



Quantum logic gates

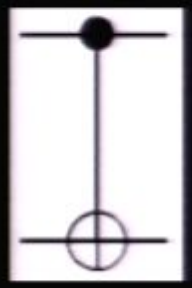
- Hadamard gate

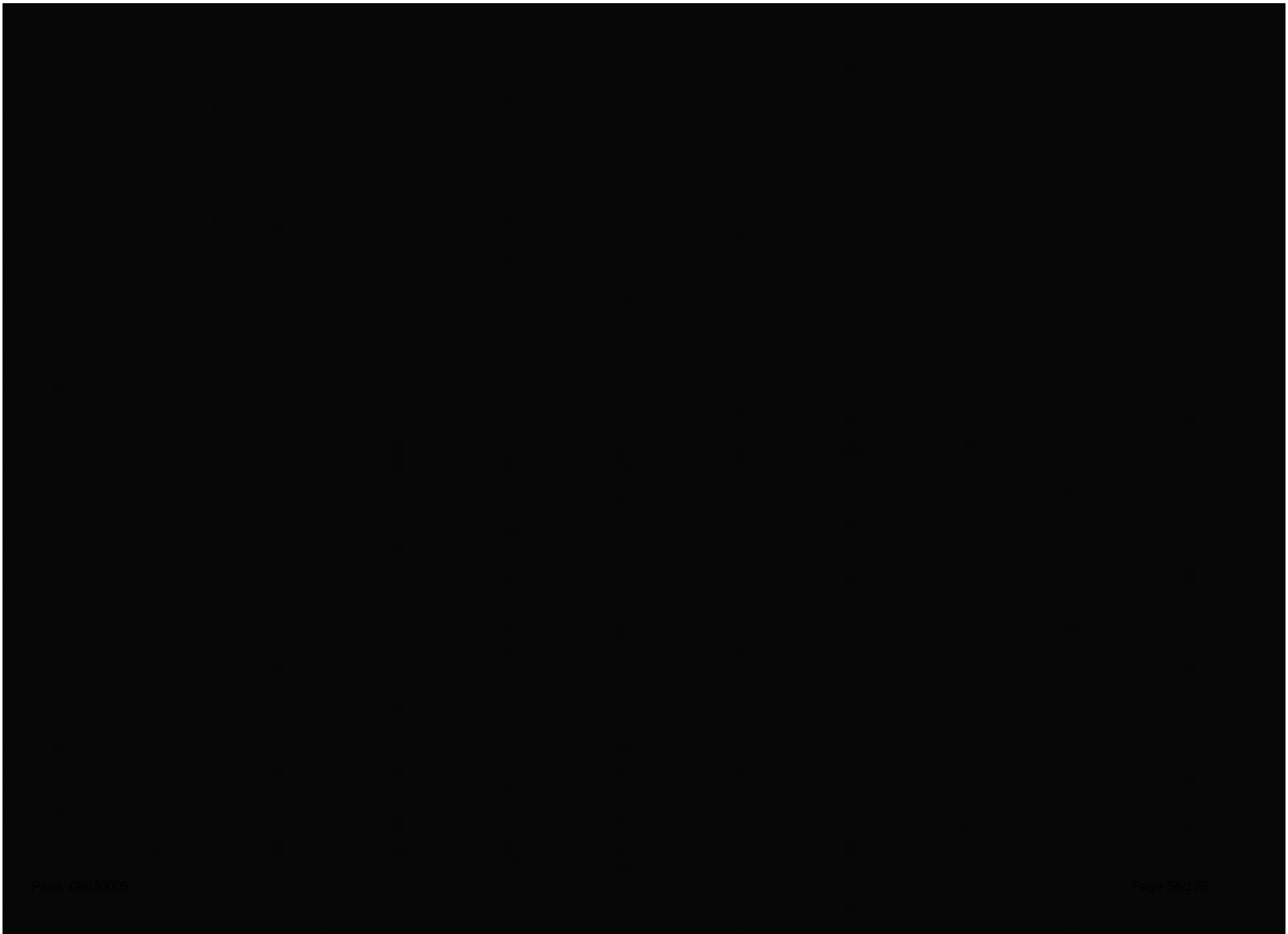
- Single qubit Unitary

- Phase-shift gate

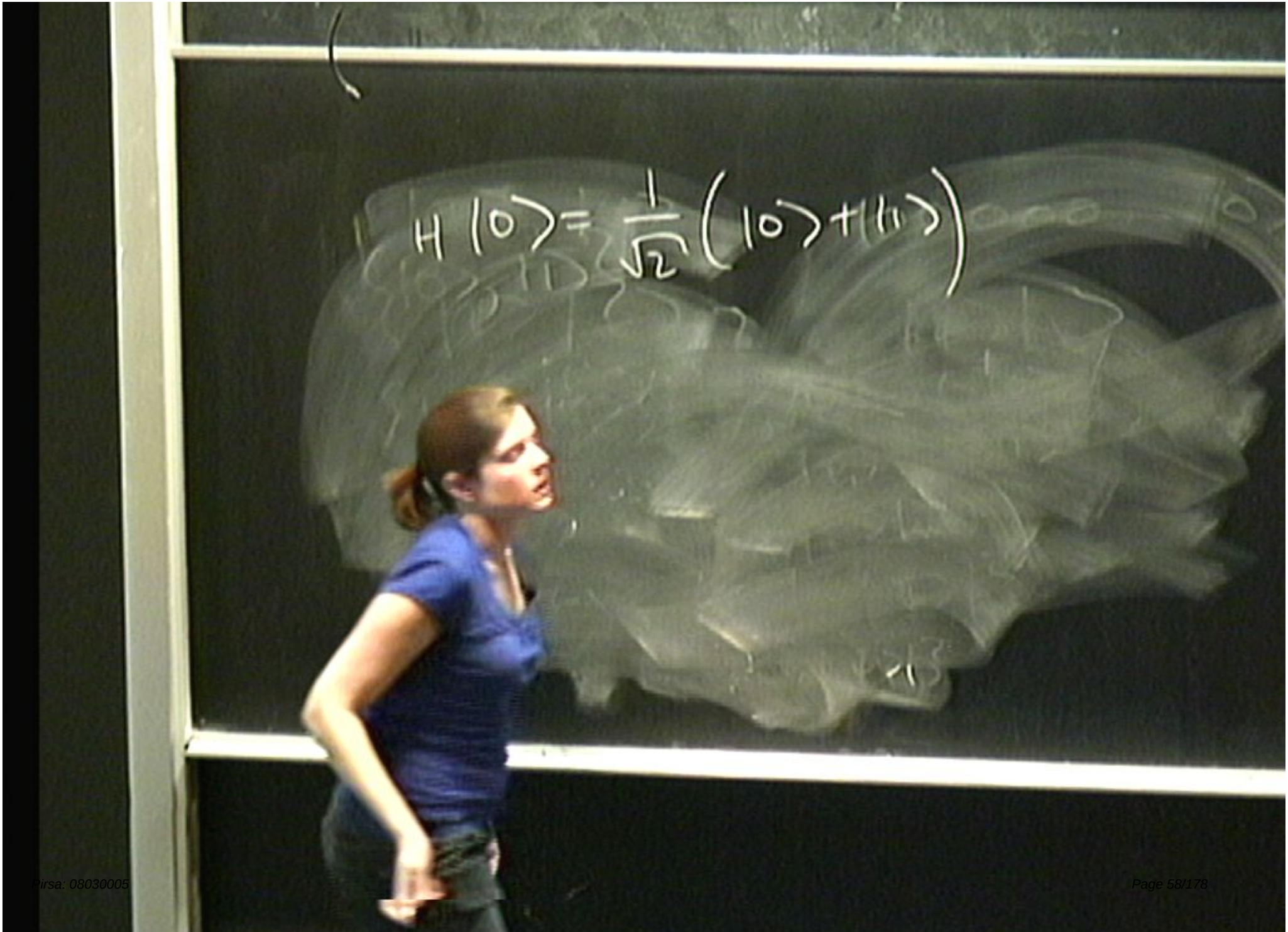
$$R(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

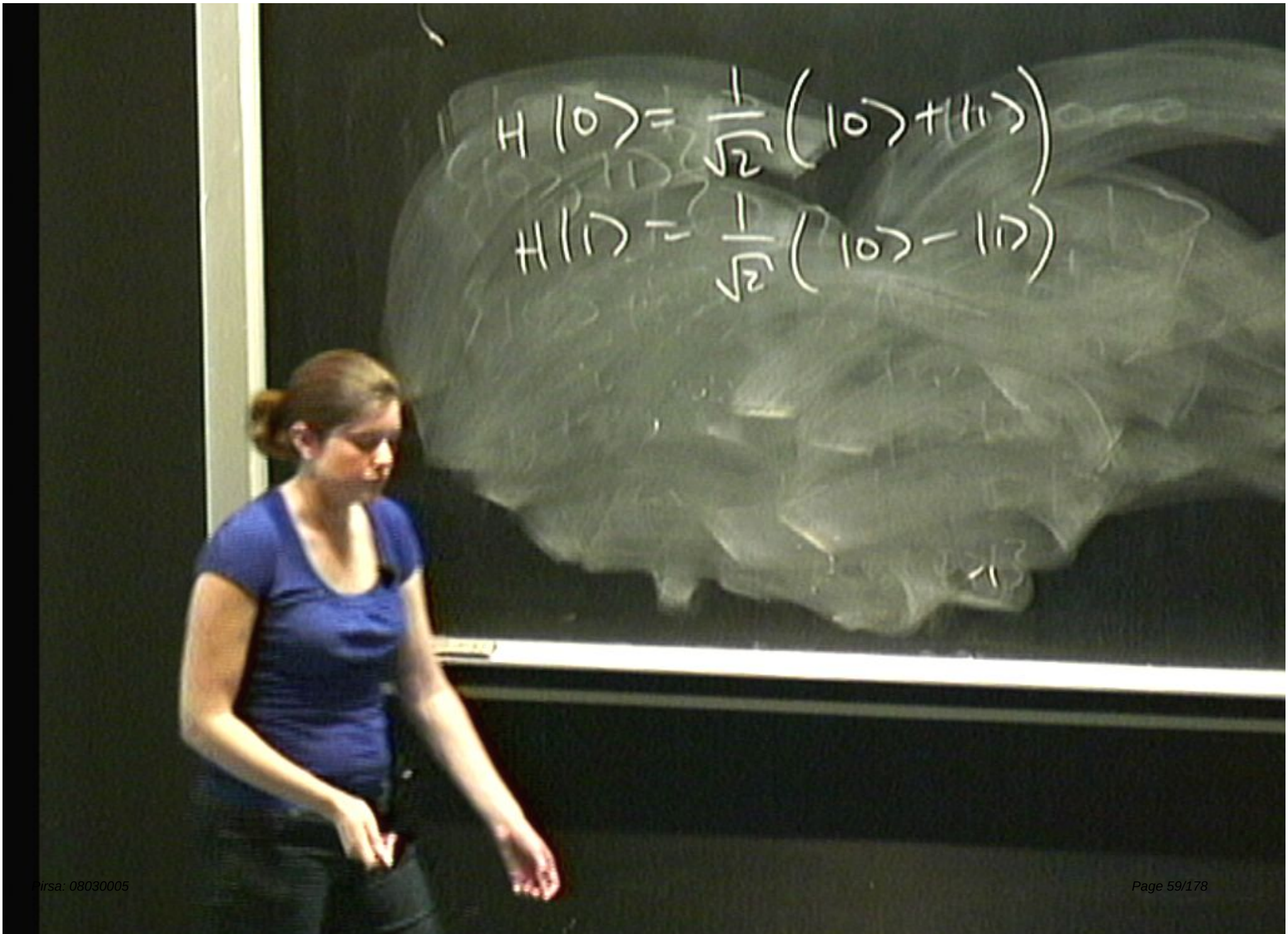
- Controlled-NOT gate



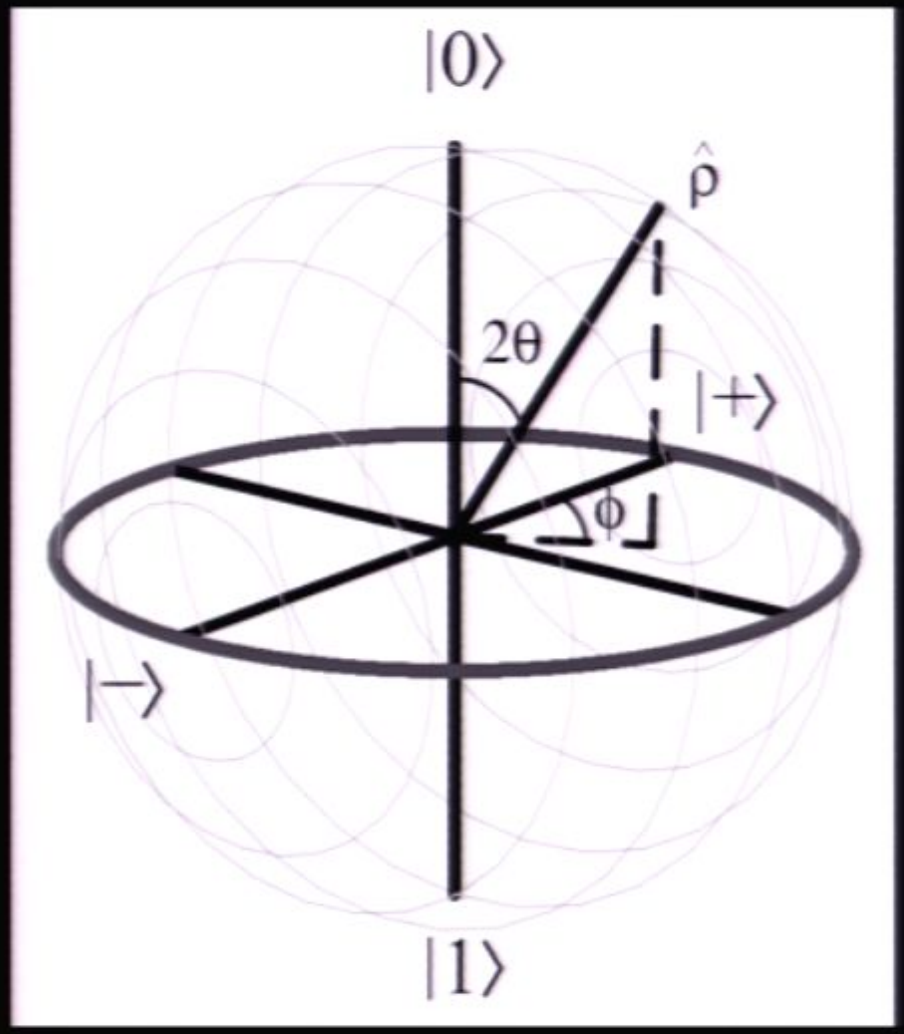


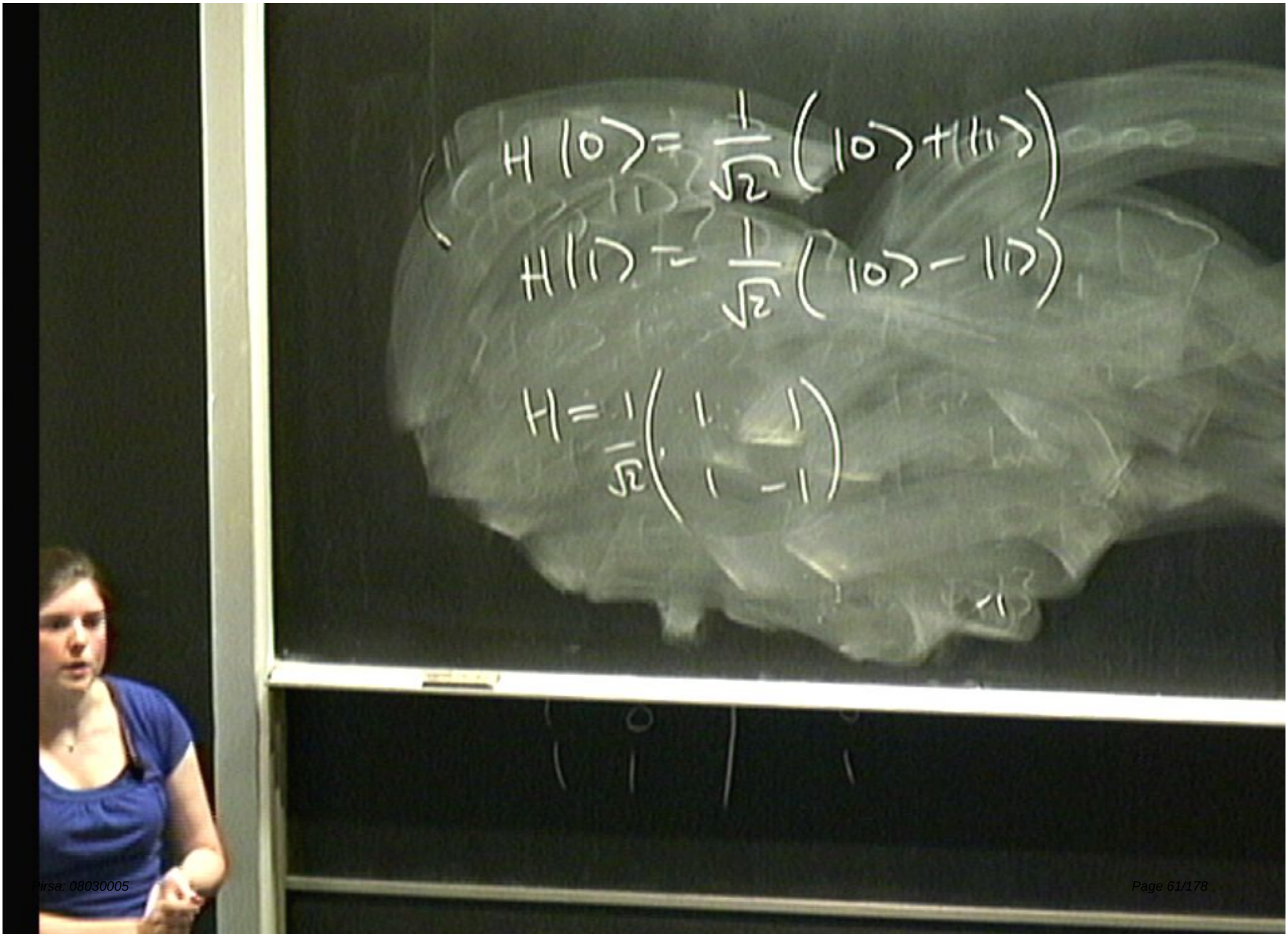

H(0)

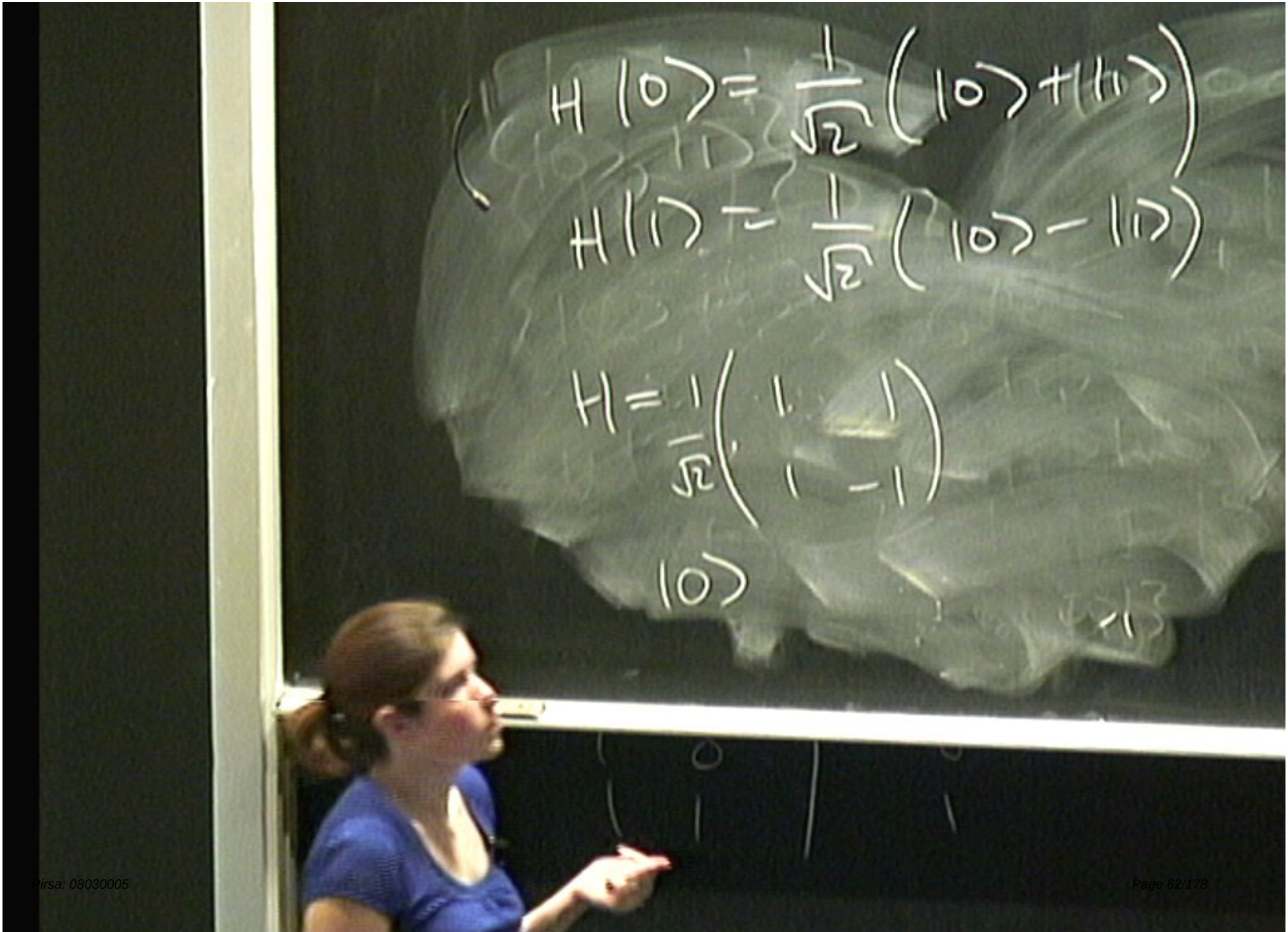

H|0⟩ = 1/√2 (|0⟩ + |1⟩)

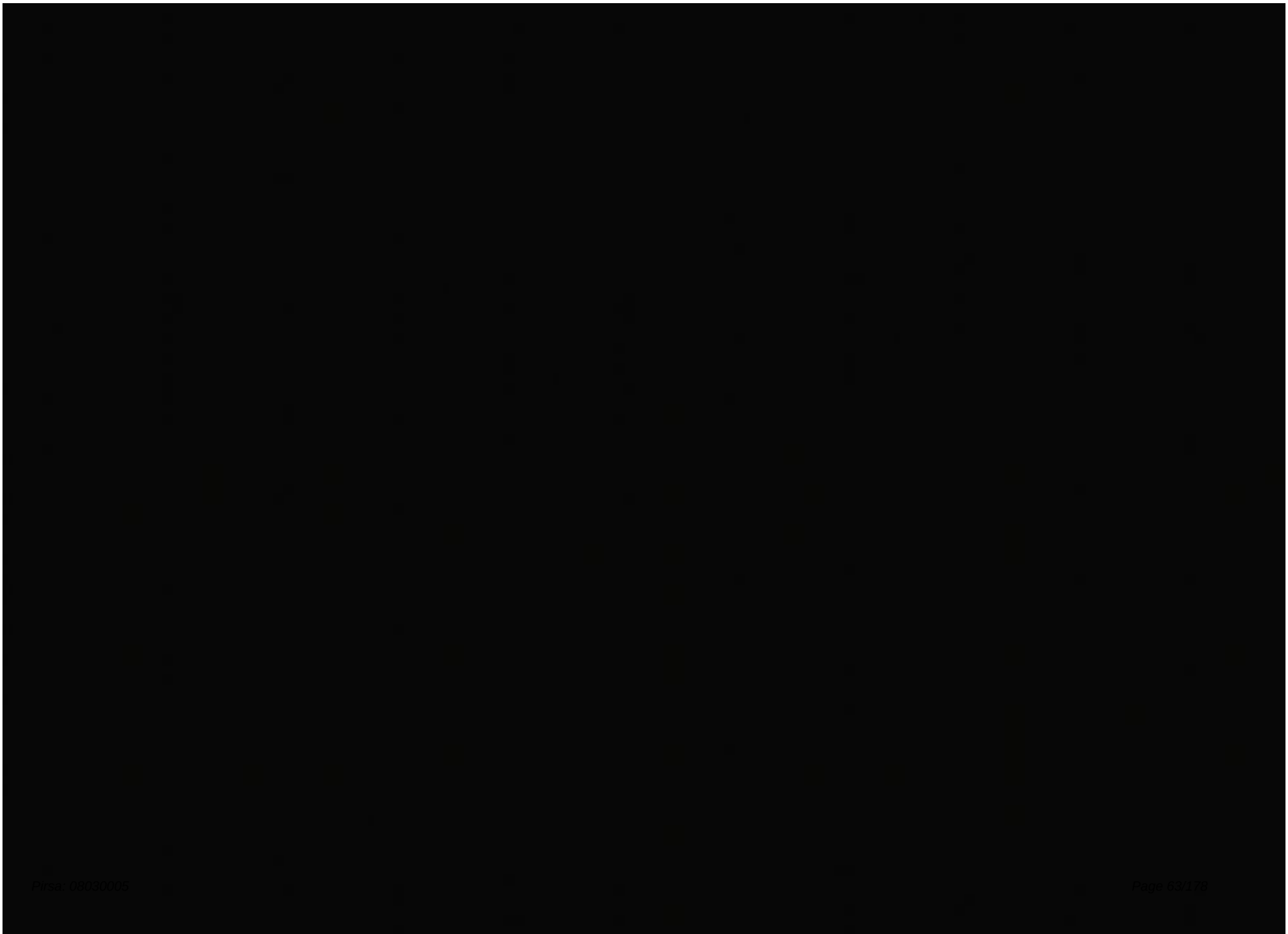

H|0⟩ = 1/√2 (|0⟩ + |1⟩)
H|1⟩ = 1/√2 (|0⟩ − |1⟩)

Density operators and the Bloch sphere representation of states.




H|0⟩ = 1/√2 (|0⟩ + |1⟩)
H|1⟩ = 1/√2 (|0⟩ − |1⟩)
H = 1/√2 (1 1)
         (1 −1)


H|0⟩ = 1/√2 (|0⟩ + |1⟩)
H|1⟩ = 1/√2 (|0⟩ − |1⟩)
H = 1/√2 (1 1)
         (1 −1)
|0⟩



Quantum logic gates

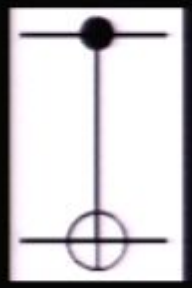
- Hadamard gate

- Single qubit Unitary

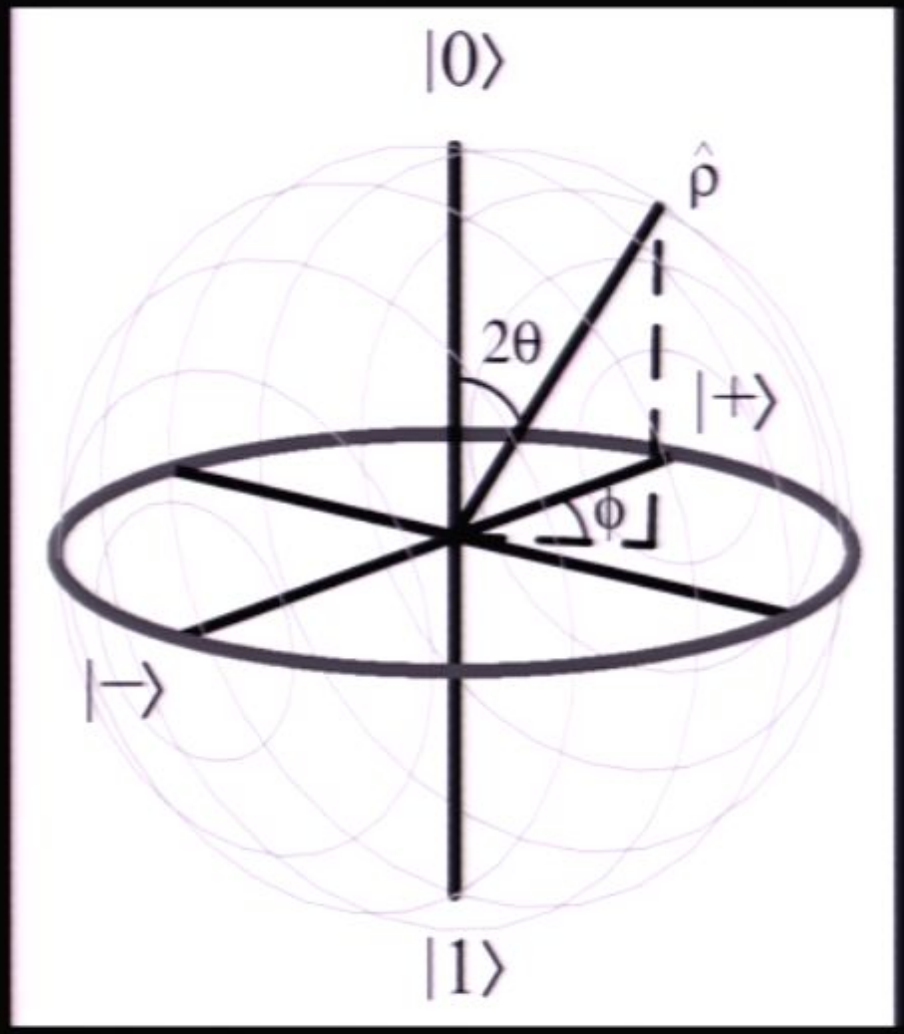
- Phase-shift gate

$$R(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

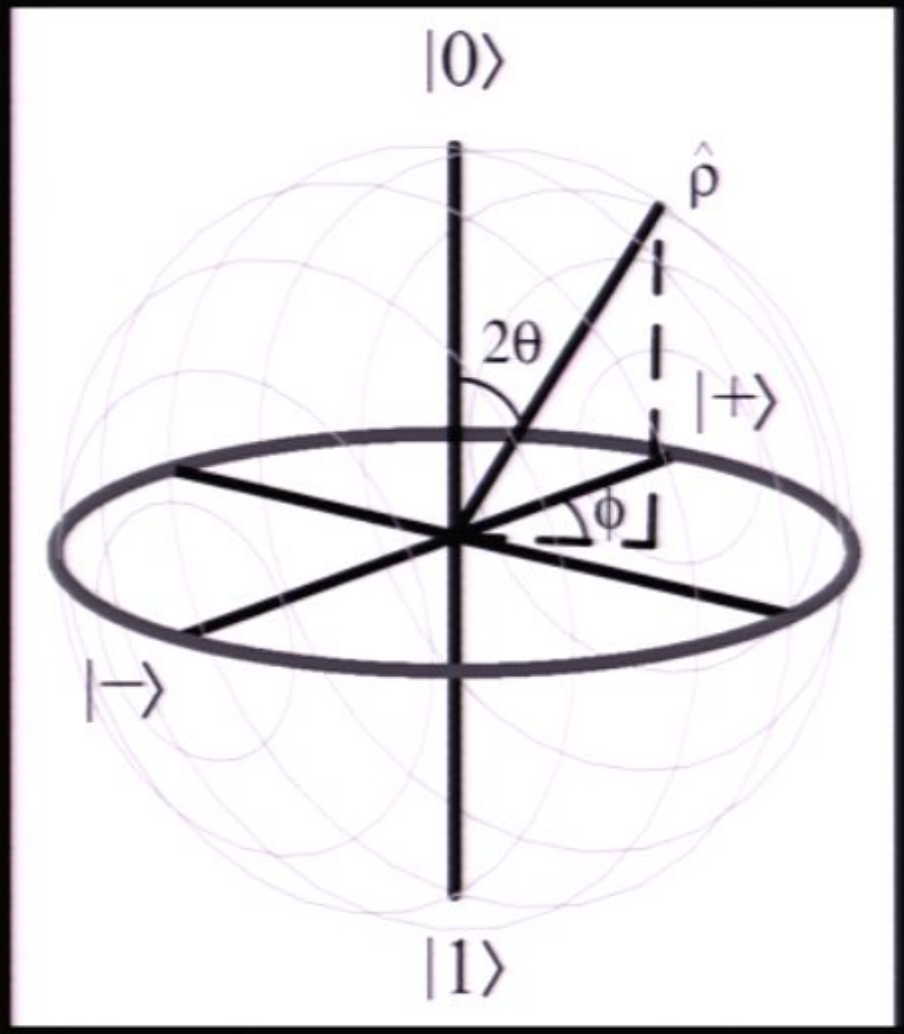
- Controlled-NOT gate

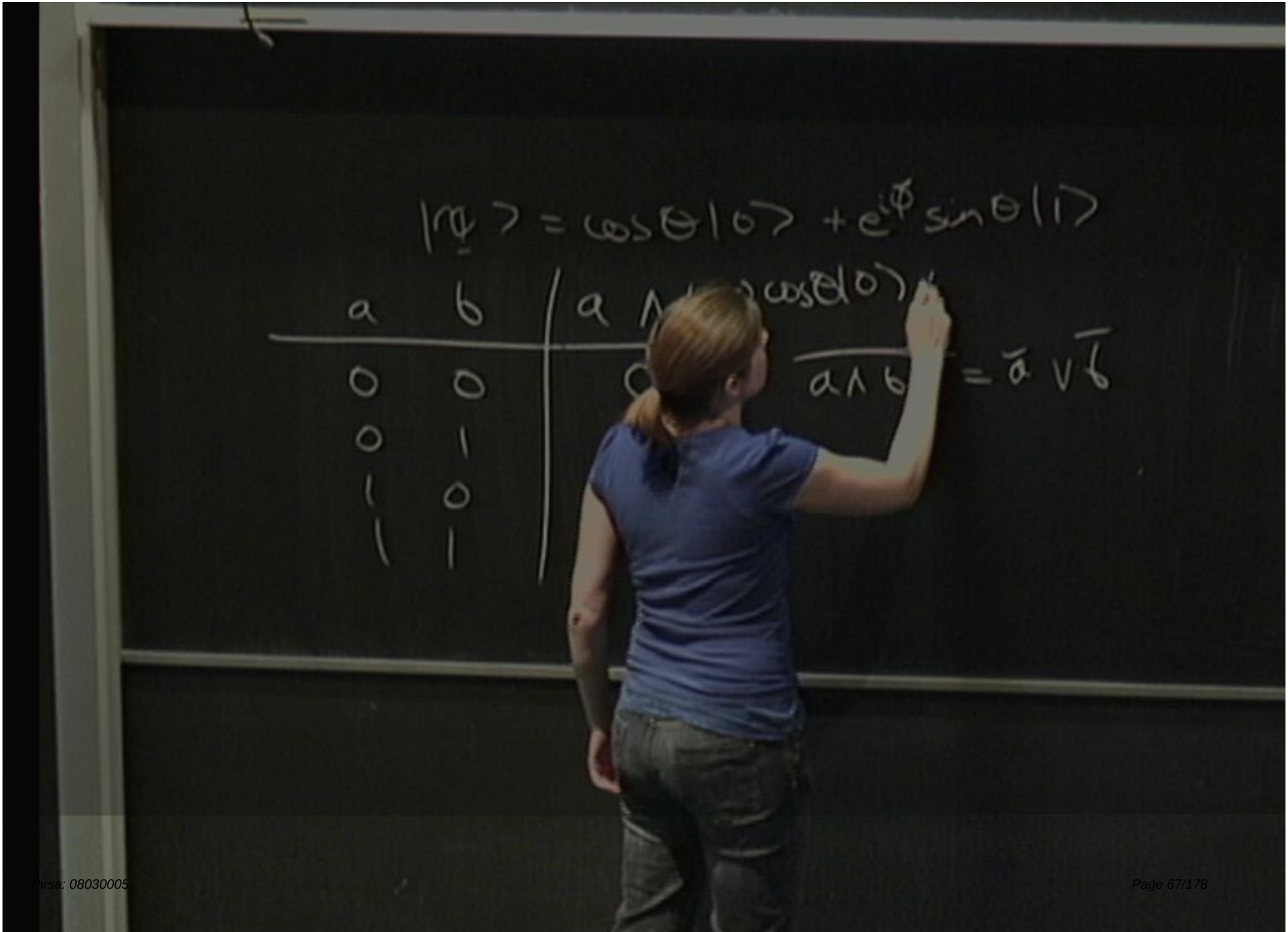


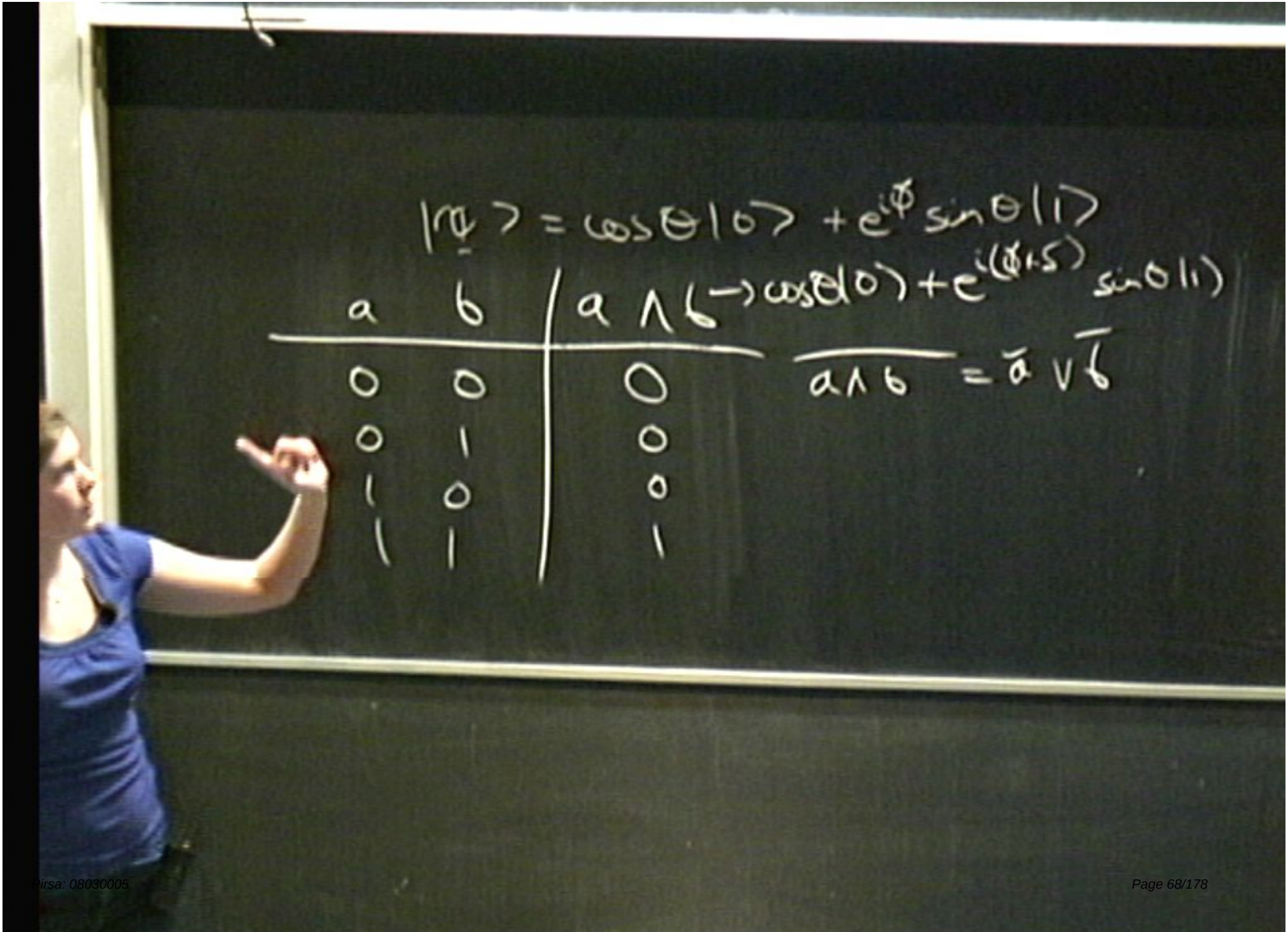
Density operators and the Bloch sphere representation of states.



Density operators and the Bloch sphere representation of states.




$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$
a b
0 0
0 1
1 0
1 1
$\overline{a \wedge b} = \bar{a} \vee \bar{b}$


$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$
$\rightarrow \cos\theta|0\rangle + e^{i(\phi+\delta)}\sin\theta|1\rangle$
a b | a ∧ b
0 0 | 0
0 1 | 0
1 0 | 0
1 1 | 1
$\overline{a \wedge b} = \bar{a} \vee \bar{b}$

Quantum logic gates

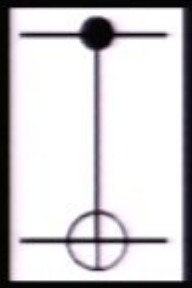
- Hadamard gate

- Single qubit Unitary

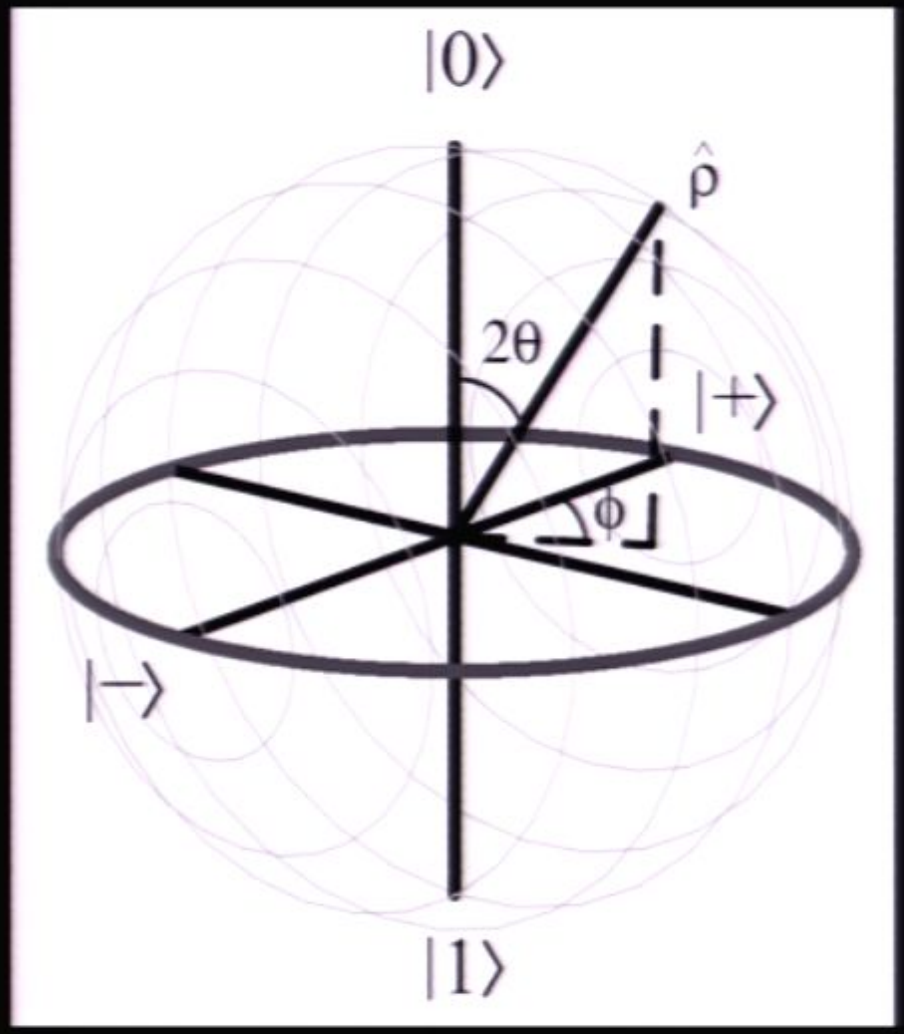
- Phase-shift gate

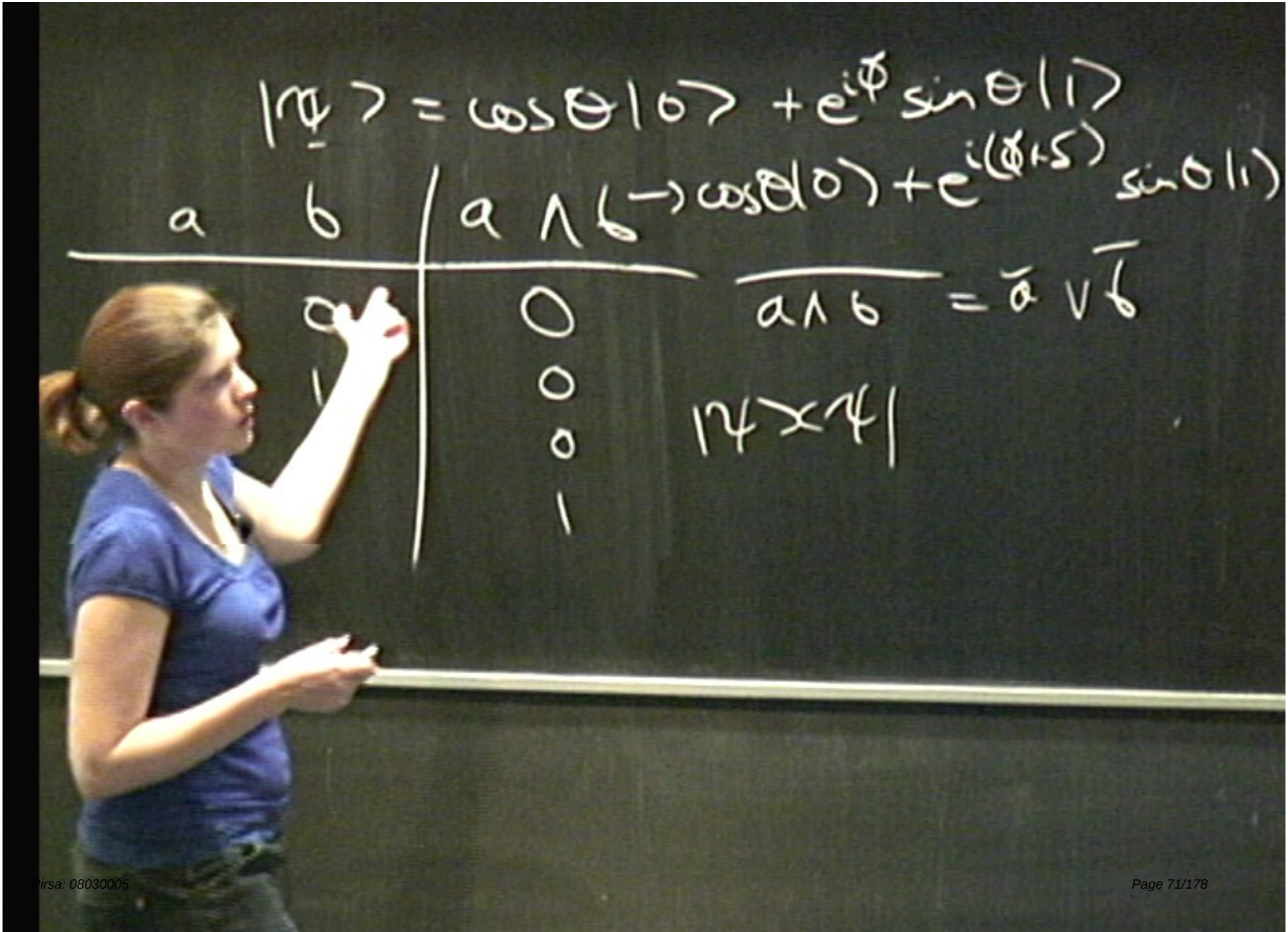
$$R(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

- Controlled-NOT gate

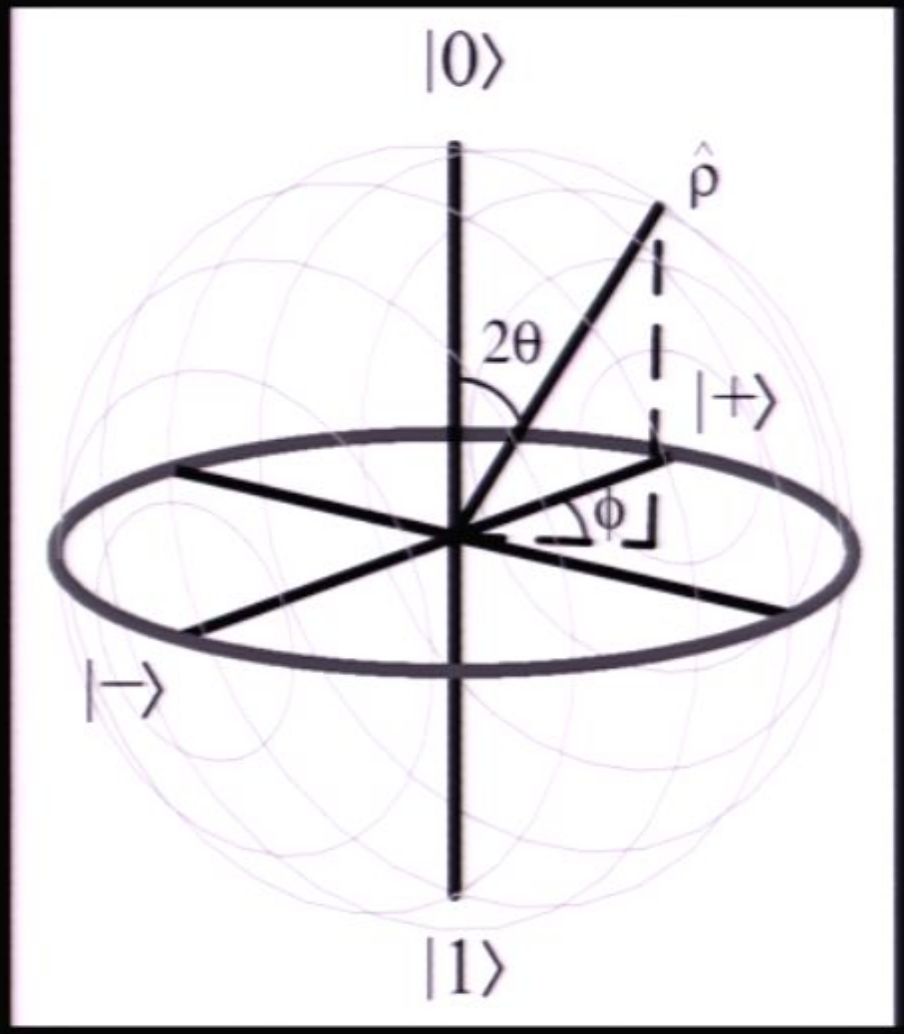


Density operators and the Bloch sphere representation of states.



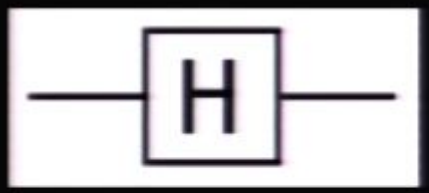

$|\Psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$
$= \cos\theta|0\rangle + e^{i(\phi+\delta)}\sin\theta|1\rangle$
a b | a ∧ b
0 0 0
0 1 0
1 0 0
1 1 1
$\overline{a \wedge b} = \bar{a} \vee \bar{b}$
$|\psi\rangle\langle\psi|$

Density operators and the Bloch sphere representation of states.



Quantum logic gates

- Hadamard gate

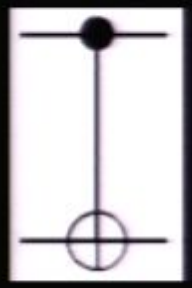


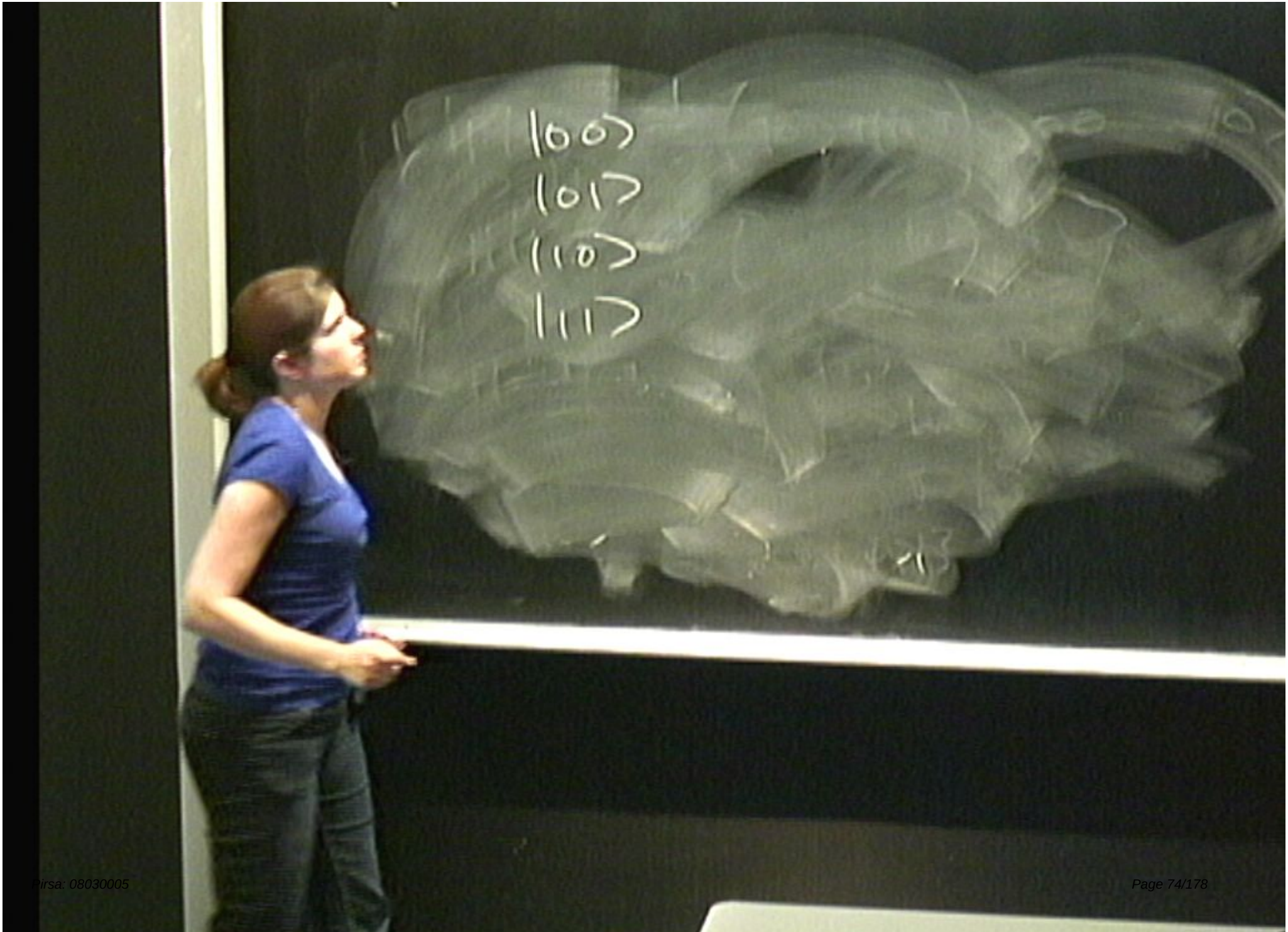
- Single qubit Unitary

- Phase-shift gate

$$R(\delta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix}$$

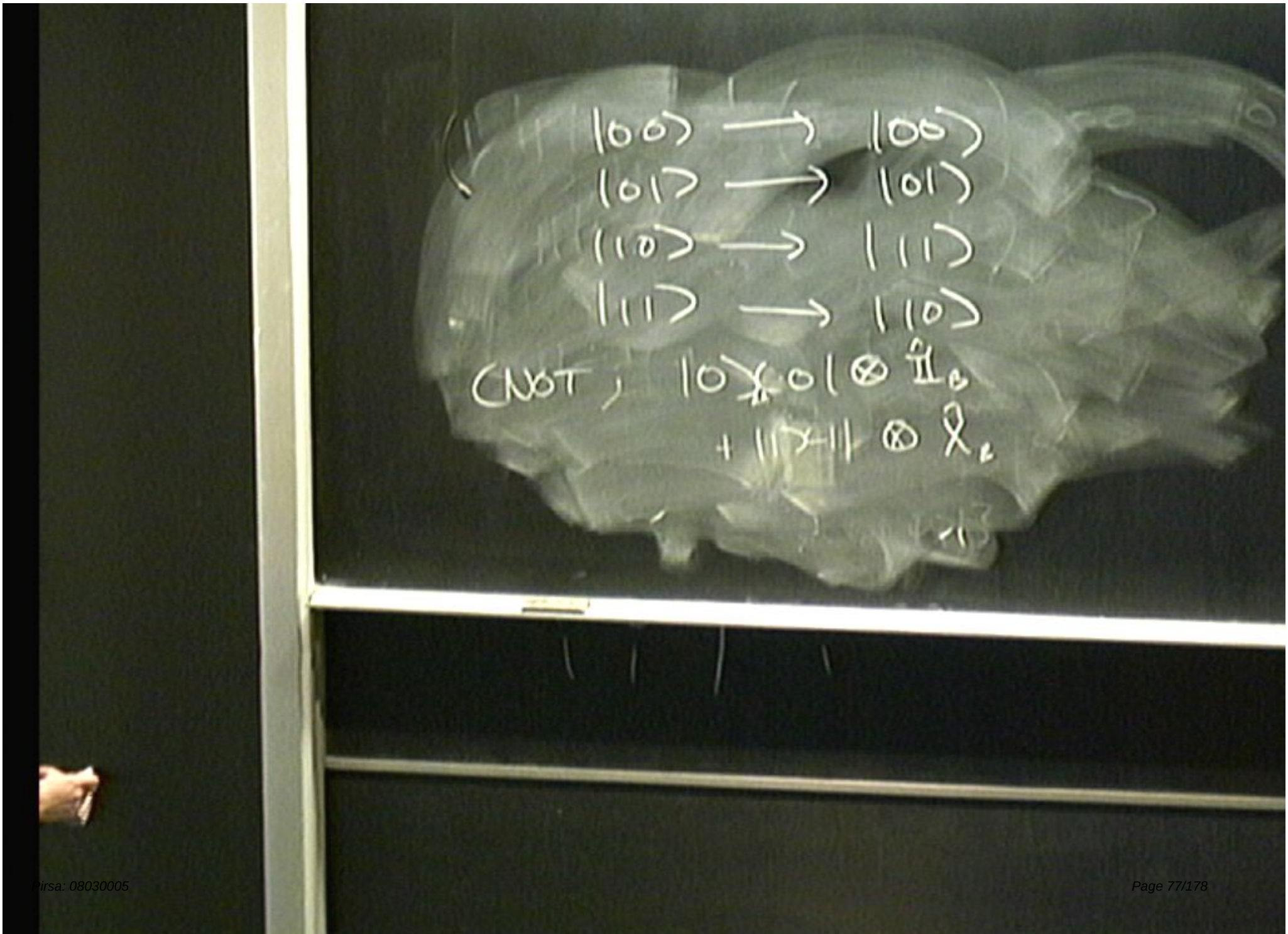
- Controlled-NOT gate

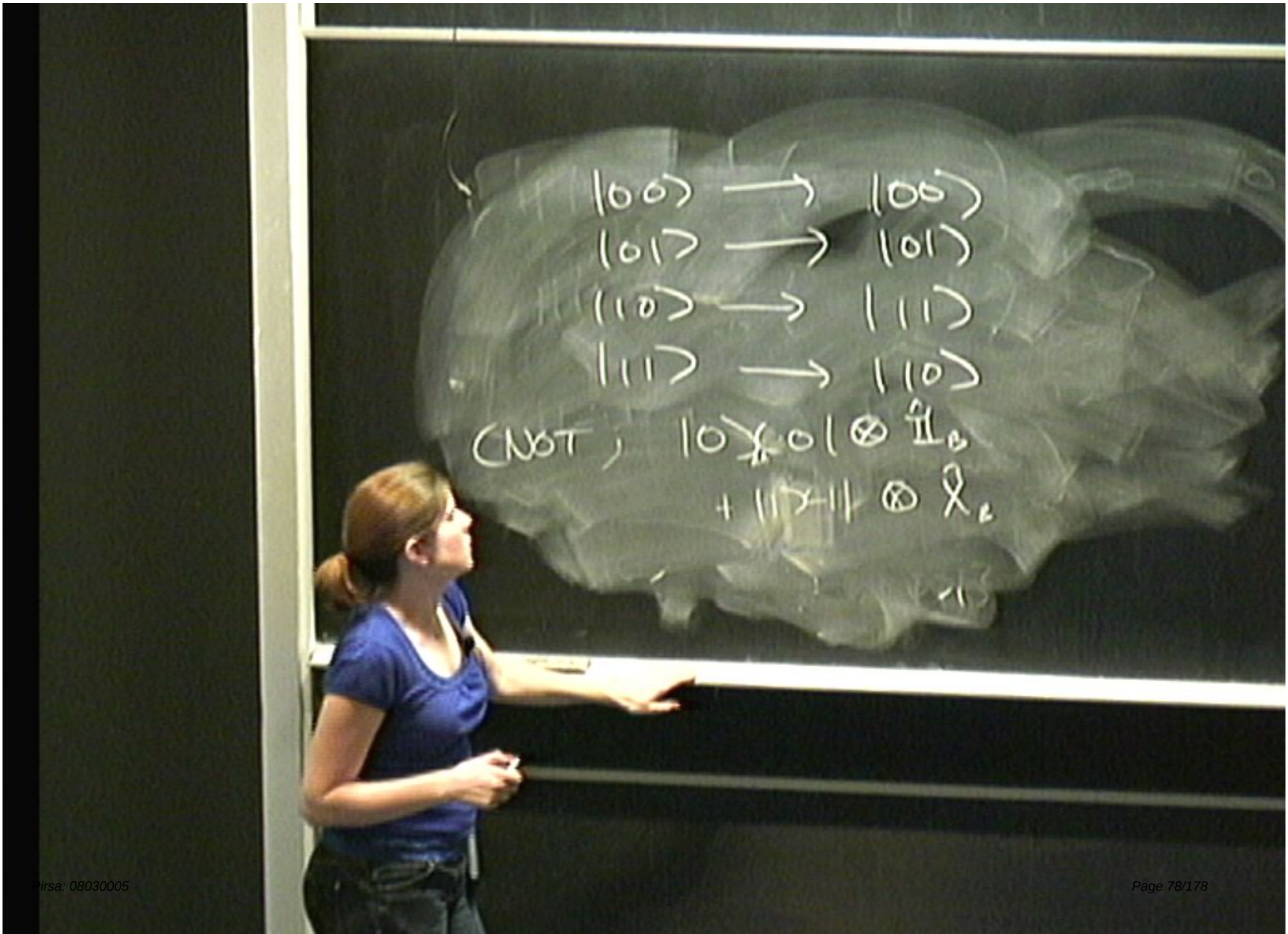


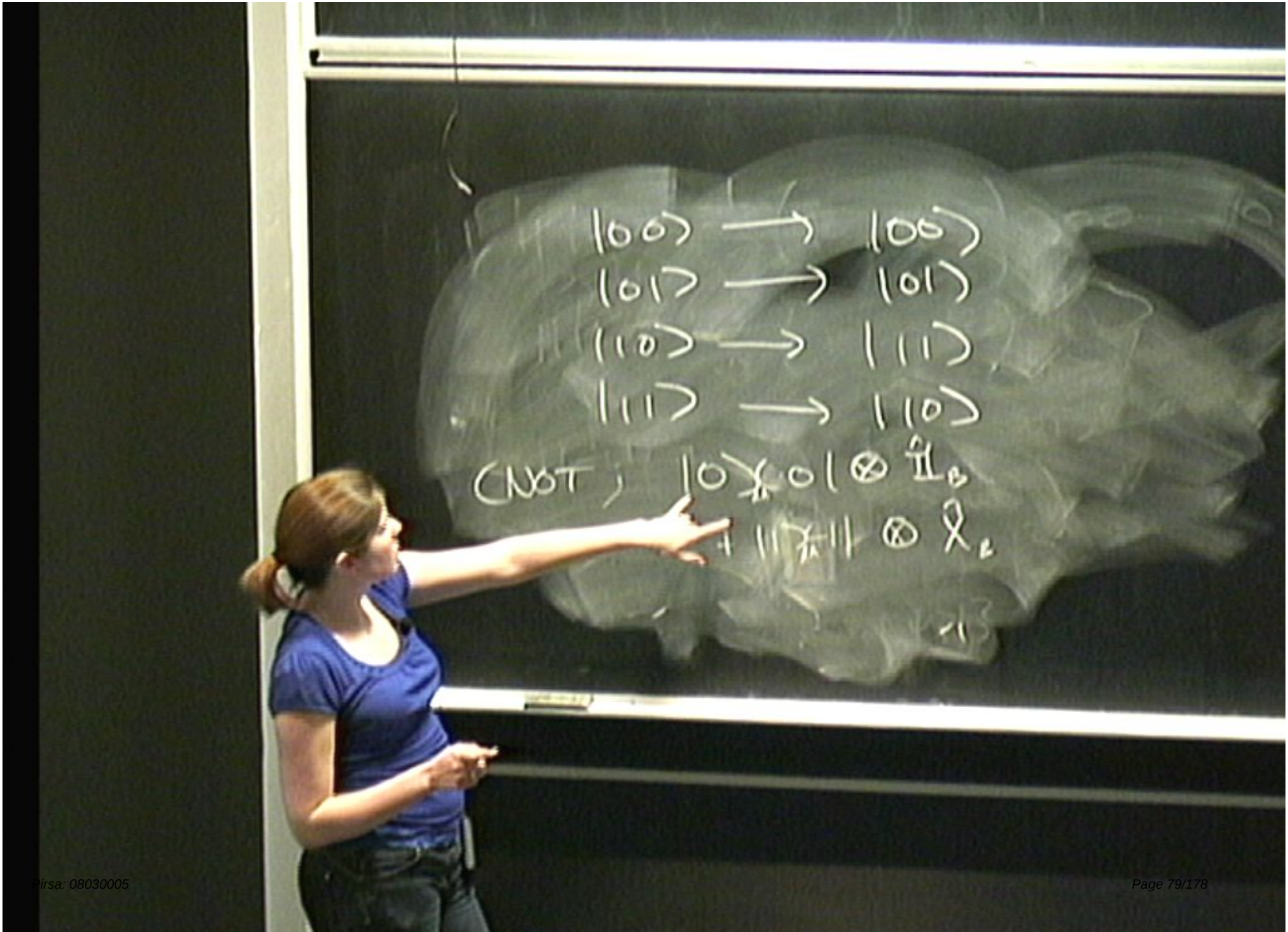

|00⟩
|01⟩
|10⟩
|11⟩

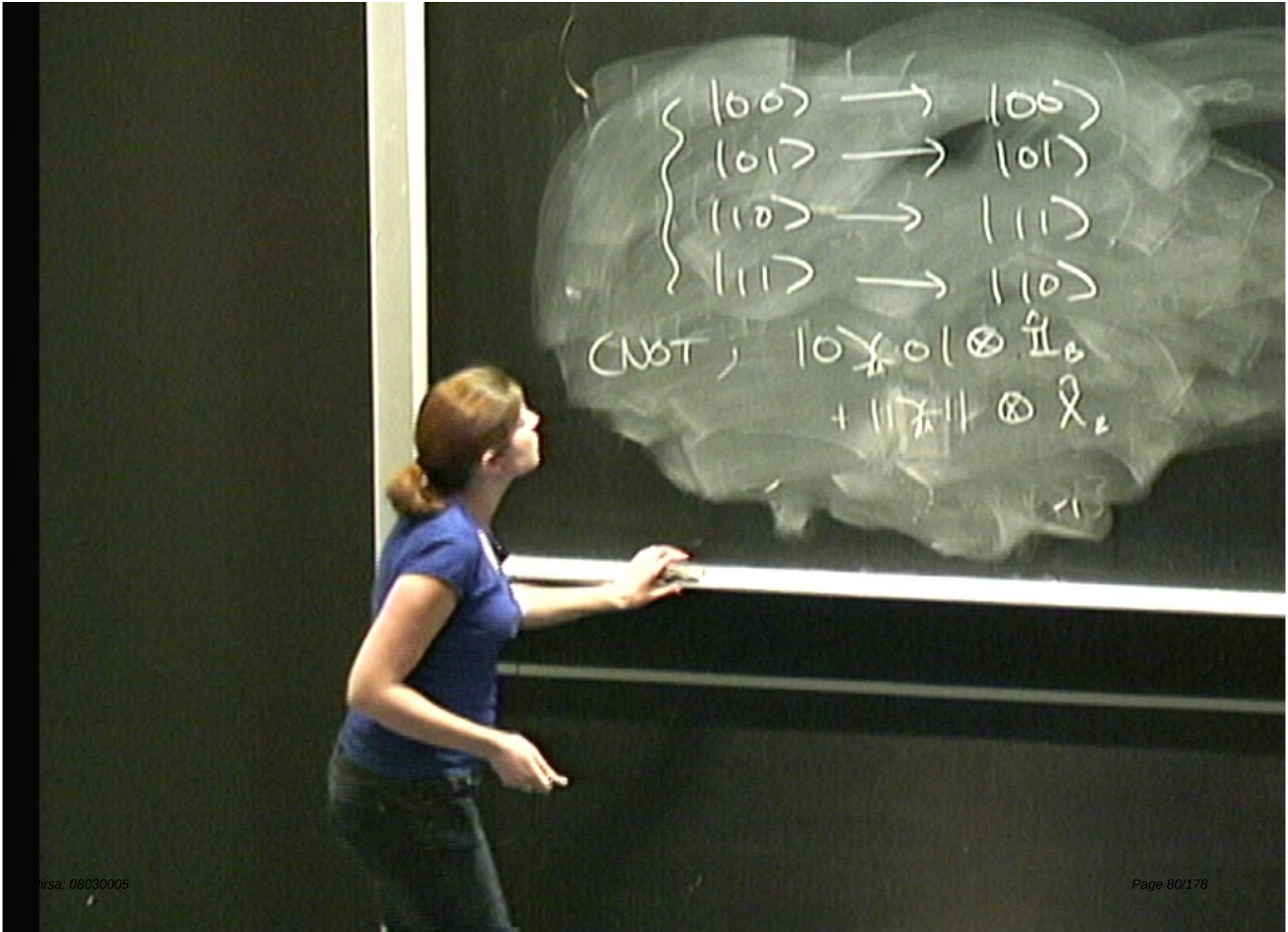

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩
|11⟩

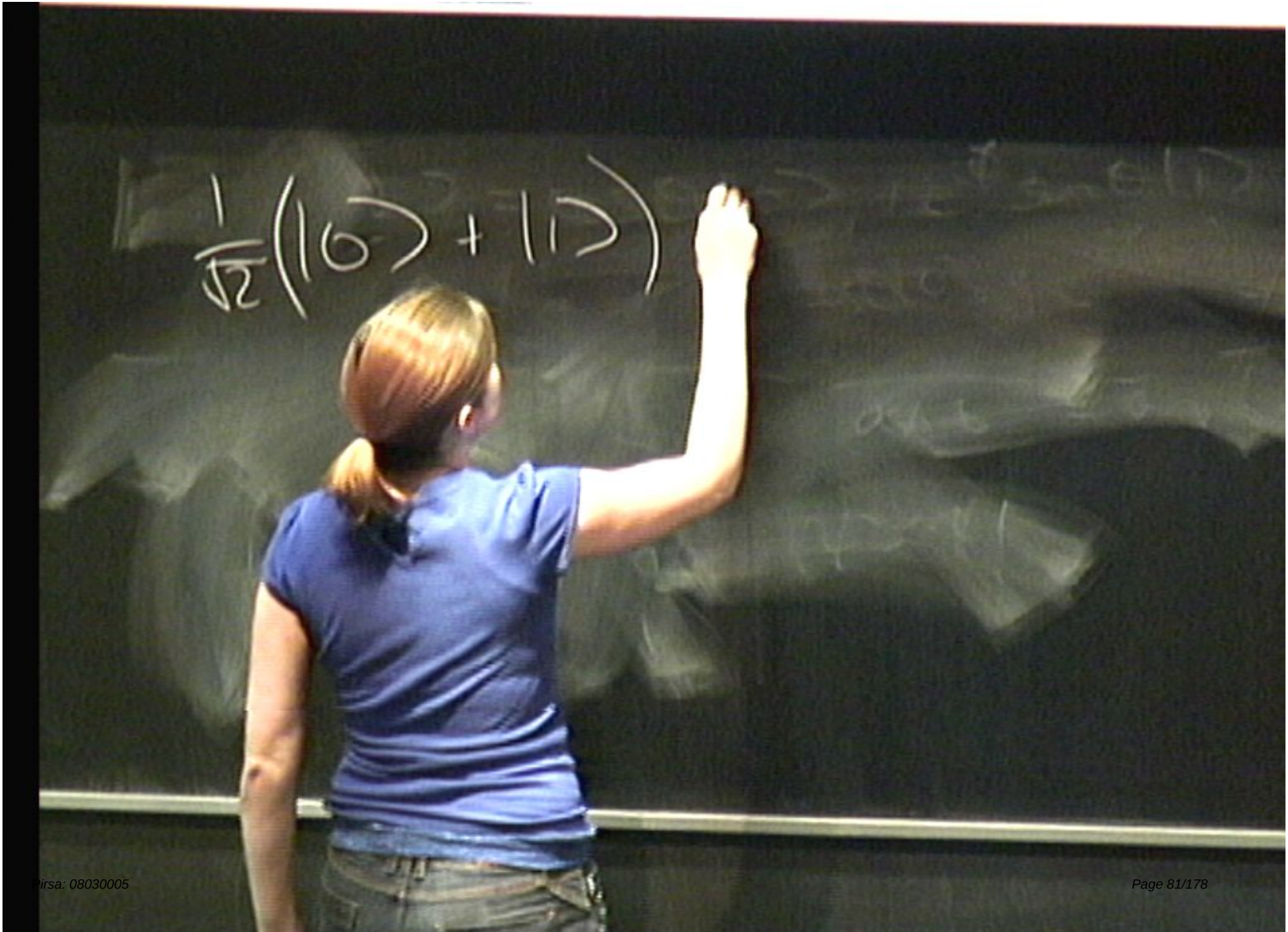

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
→ |10⟩

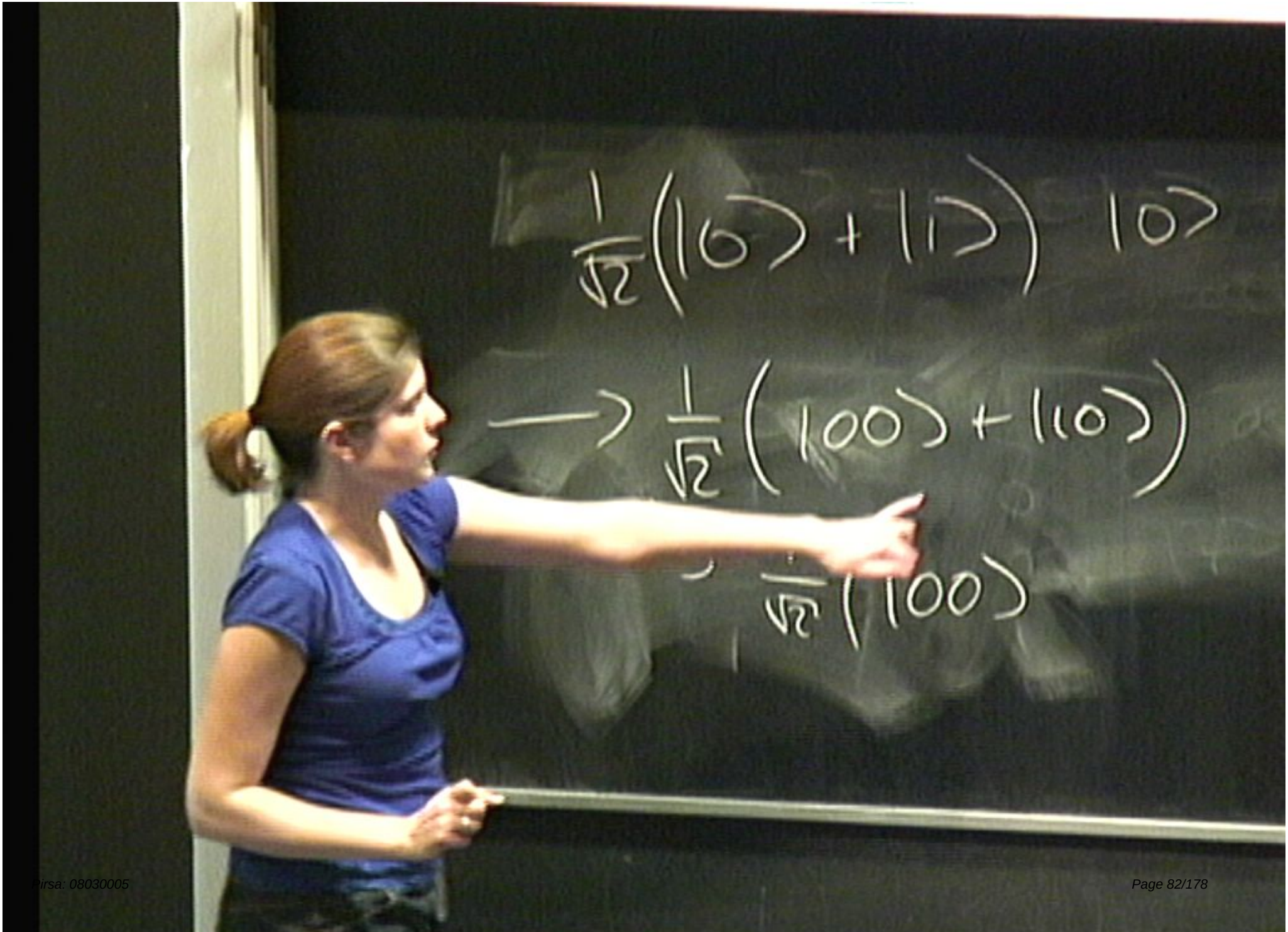

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
|11⟩ → |10⟩
CNOT; |0⟩⟨0| ⊗ Î +
|1⟩⟨1| ⊗ σ̂x

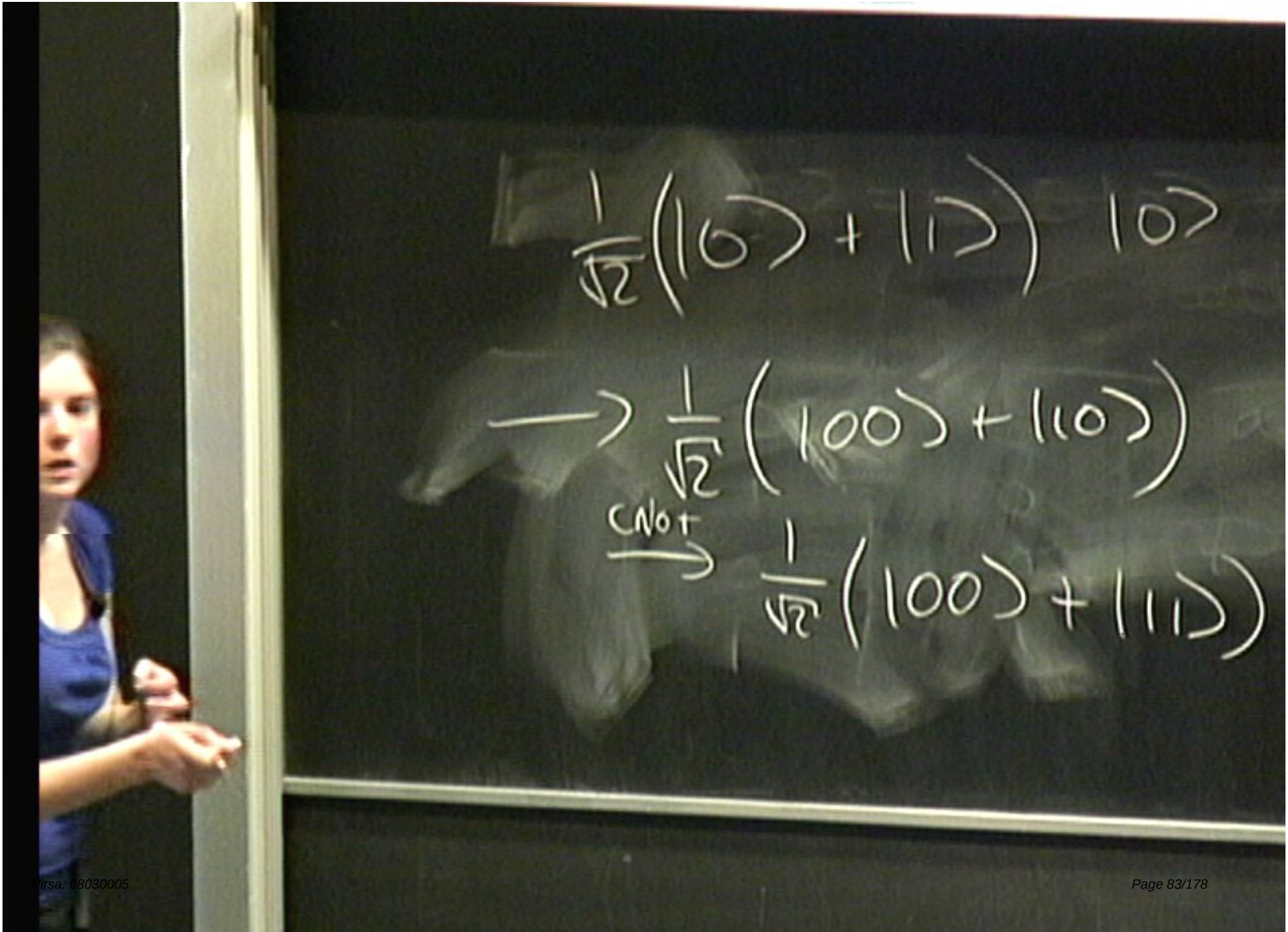

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
|11⟩ → |10⟩
CNOT; |0⟩⟨0| ⊗ 𝟙
+ |1⟩⟨1| ⊗ X

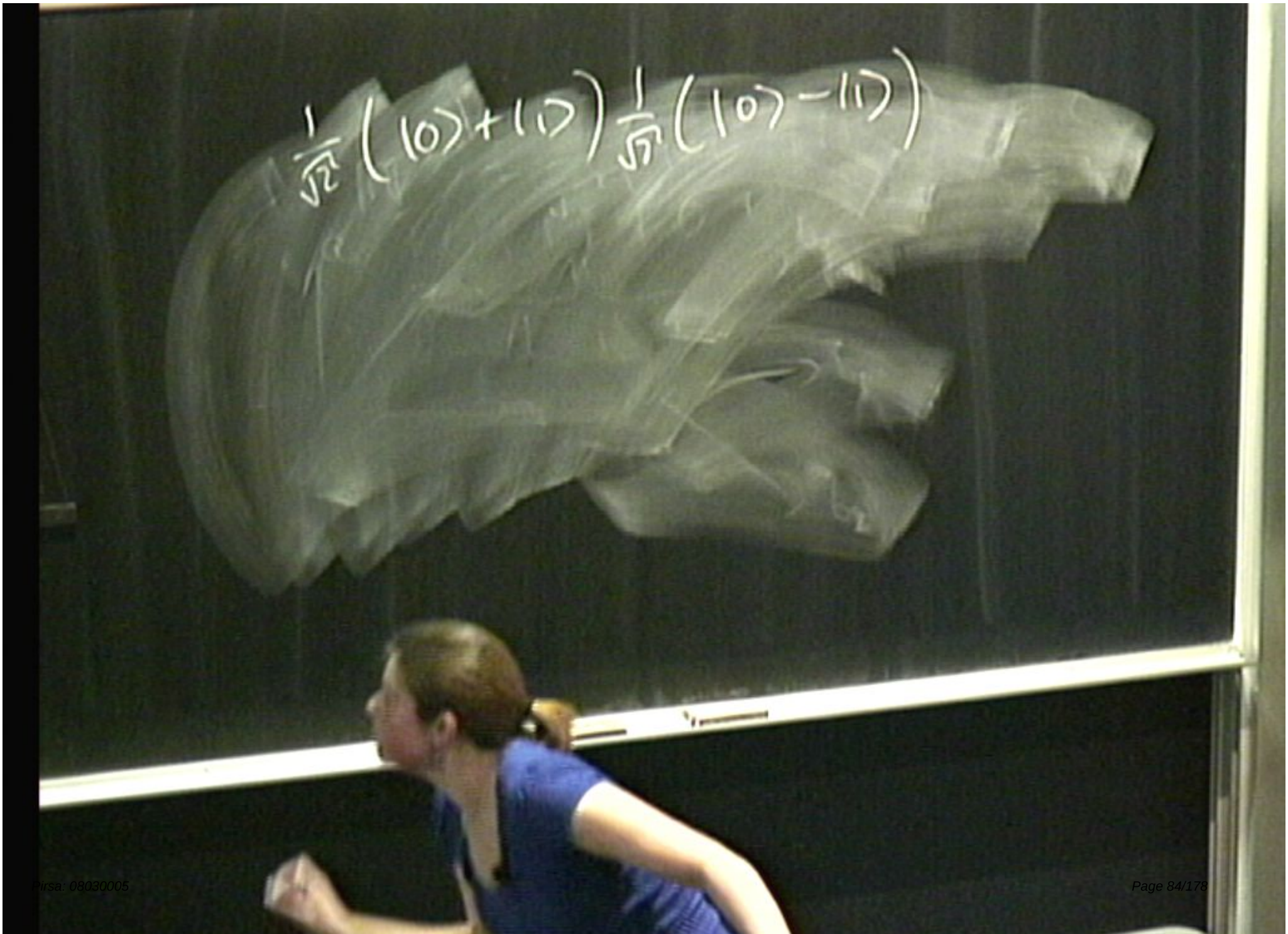

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
|11⟩ → |10⟩
CNOT

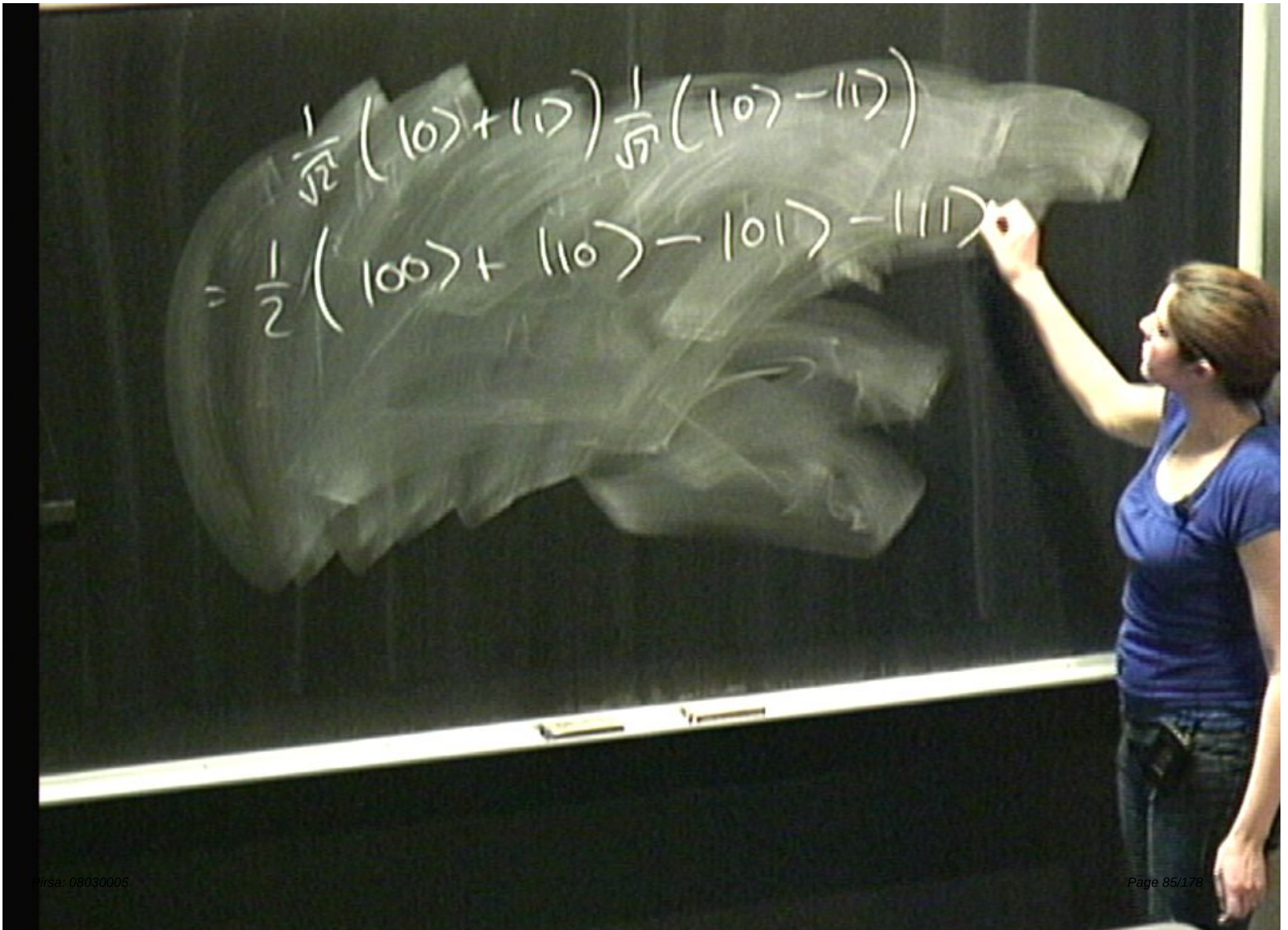

|00⟩ → |00⟩
|01⟩ → |01⟩
|10⟩ → |11⟩
|11⟩ → |10⟩
CNOT ; |0⟩⟨0| ⊗ 𝟙
+ |1⟩⟨1| ⊗ X

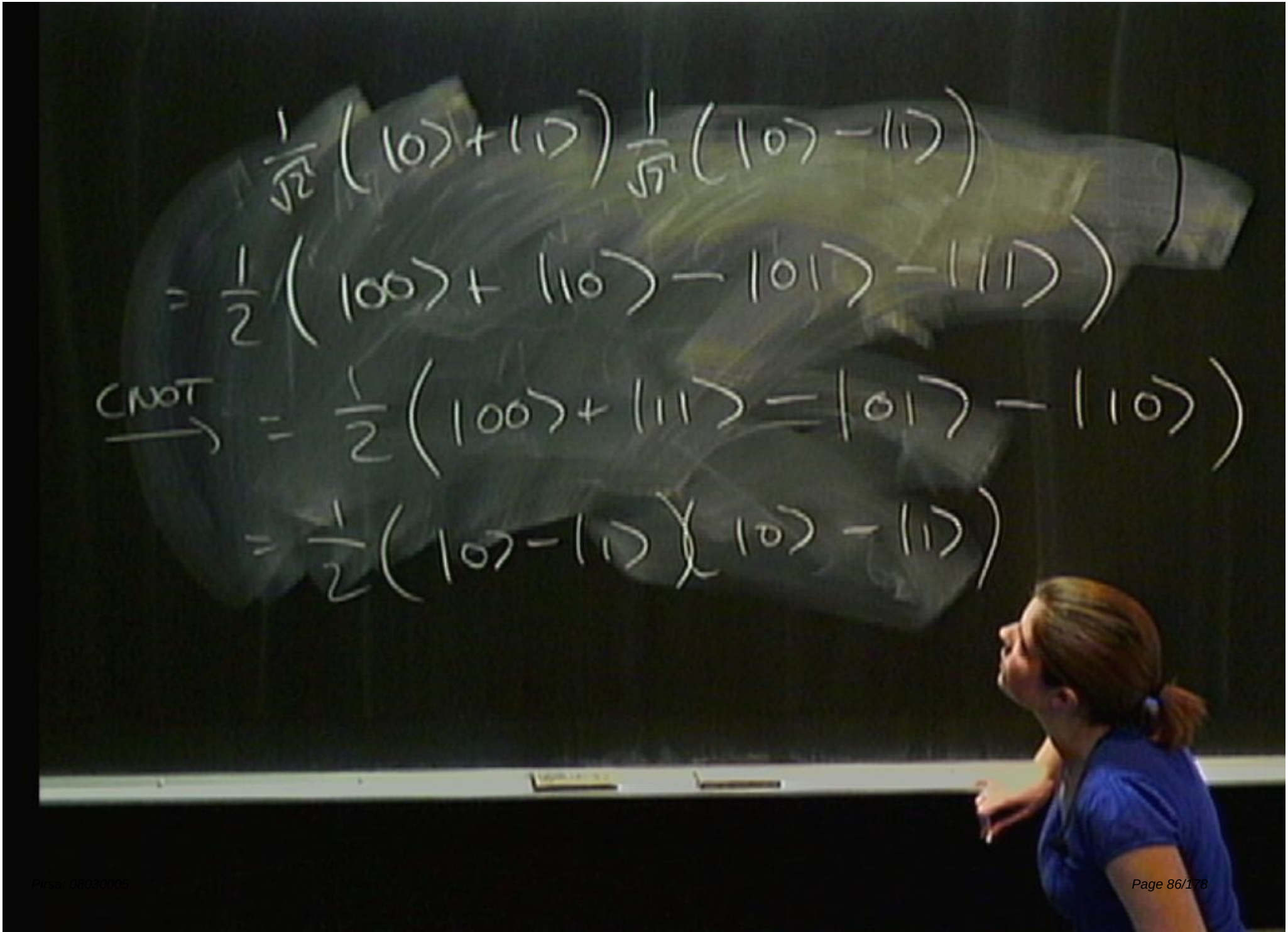

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

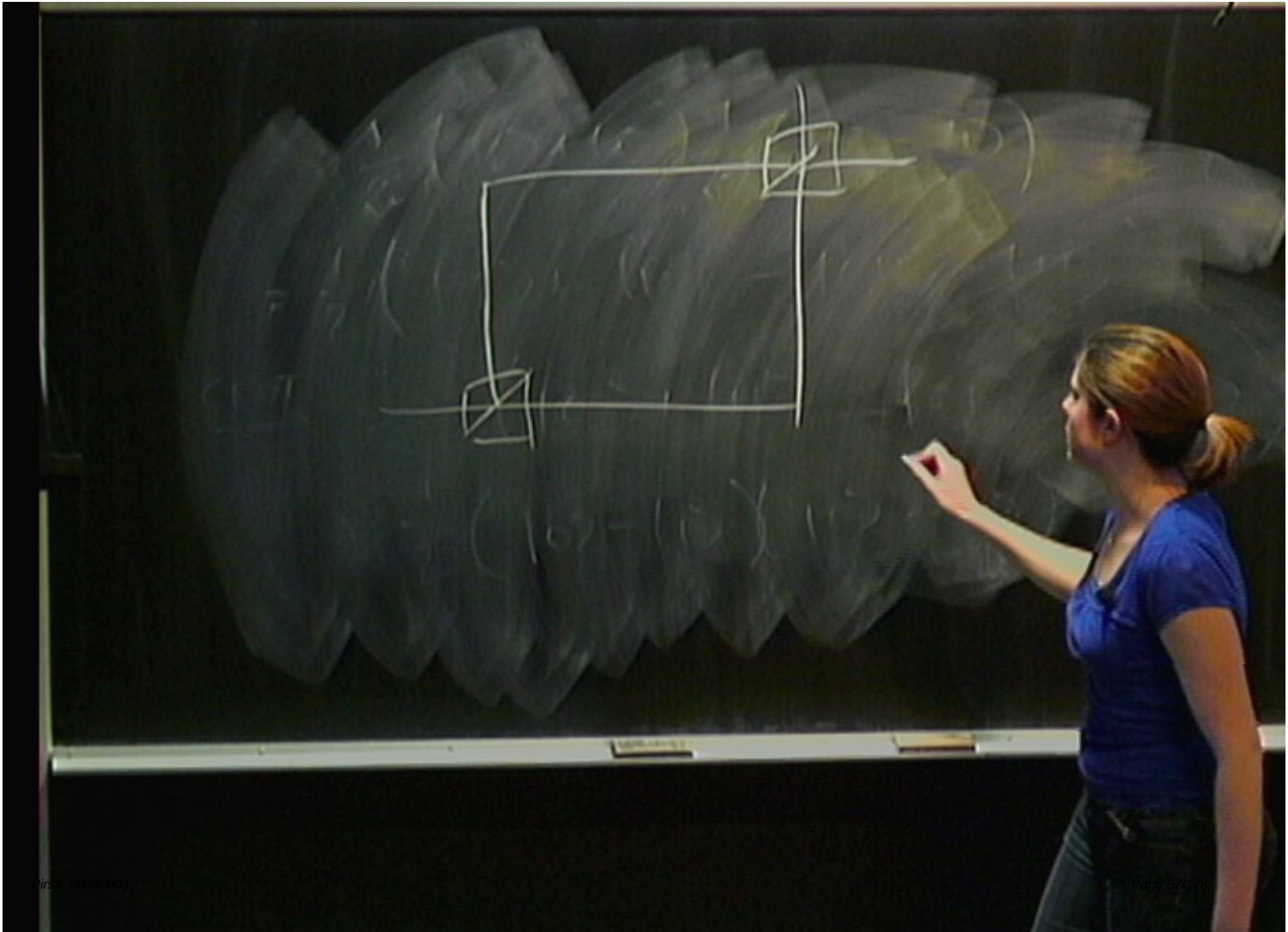

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |0\rangle$
$\longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
$\frac{1}{\sqrt{2}}(|00\rangle$

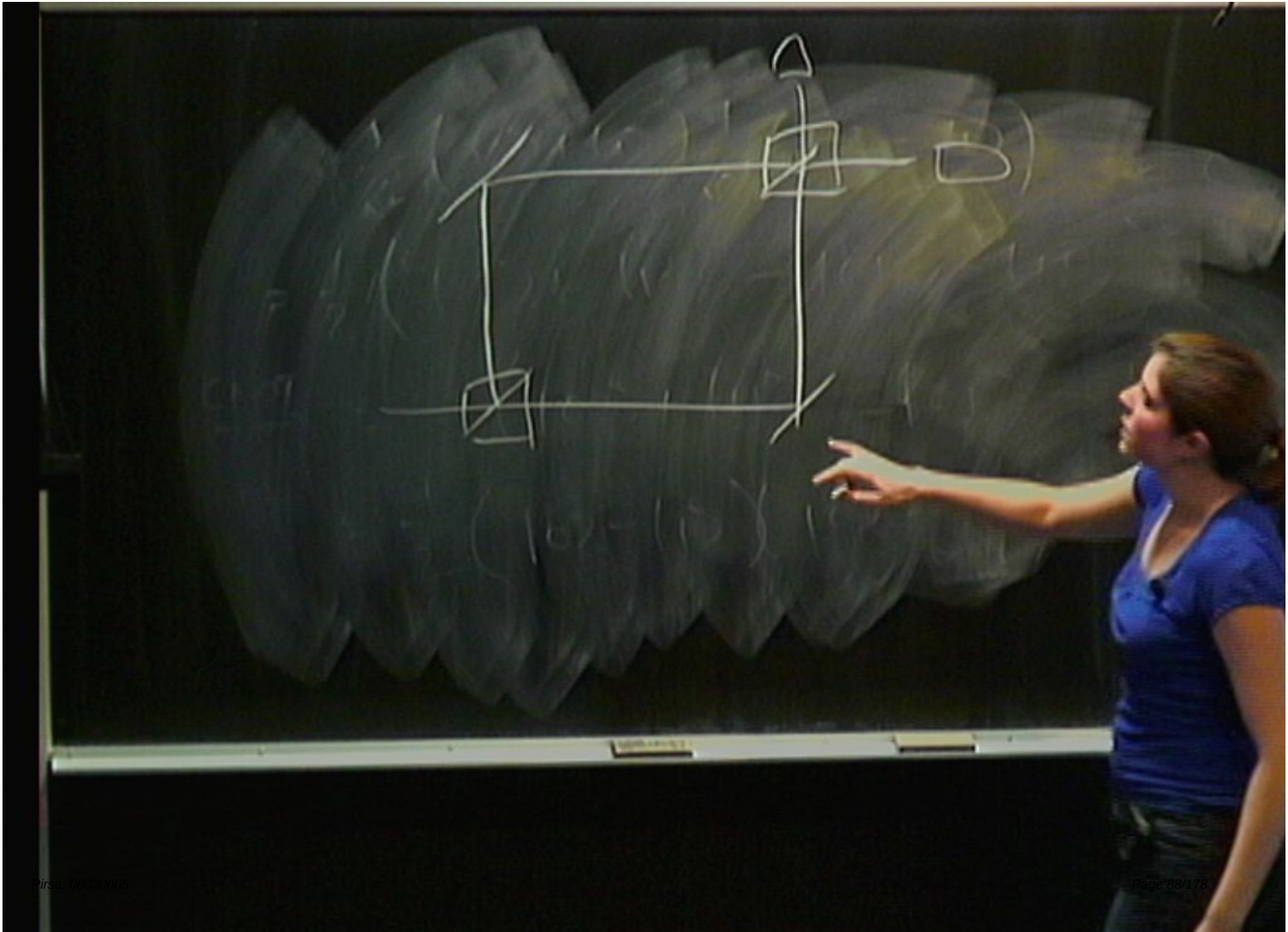

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |0\rangle$
$\longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
CNot
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

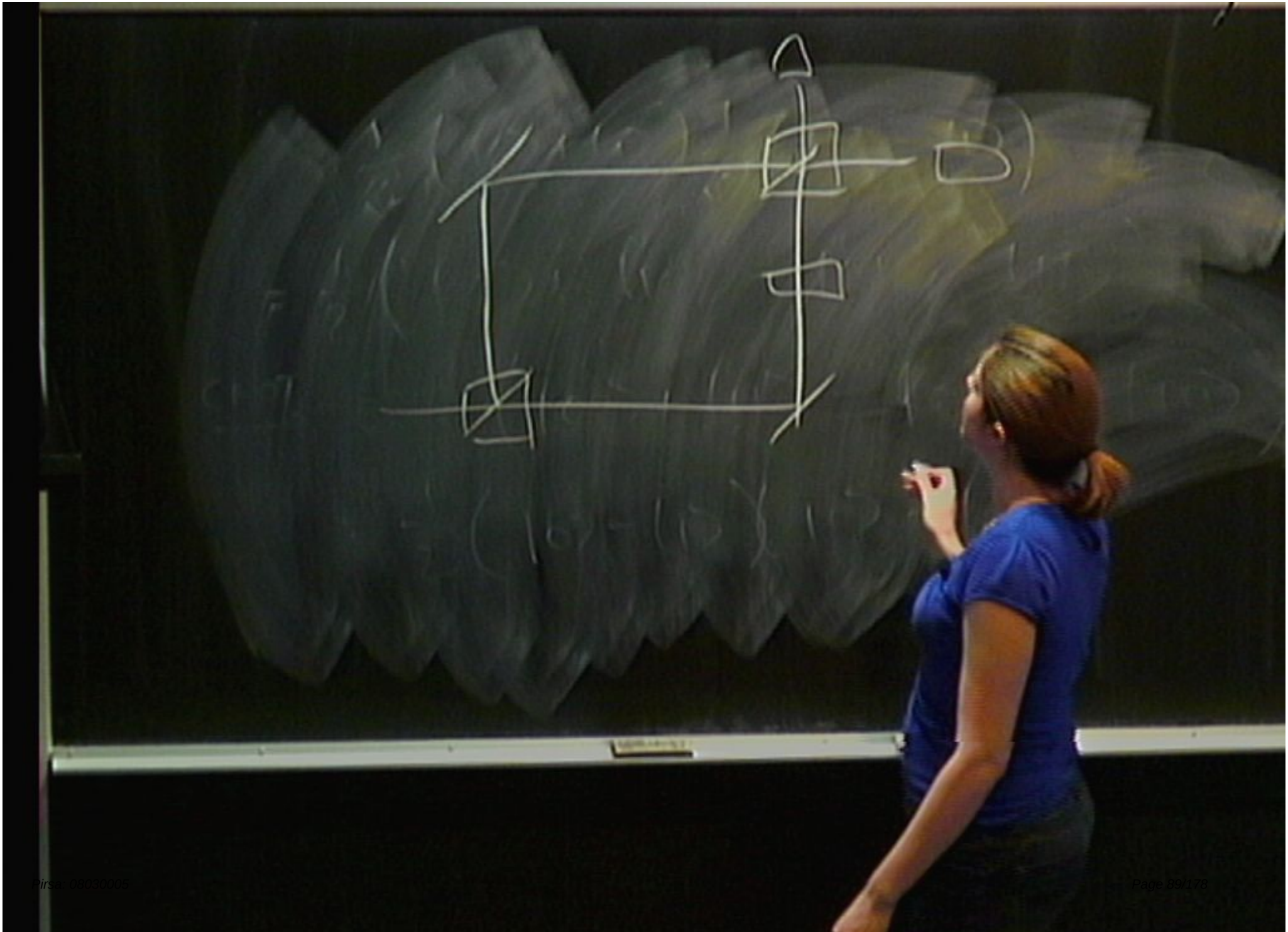

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

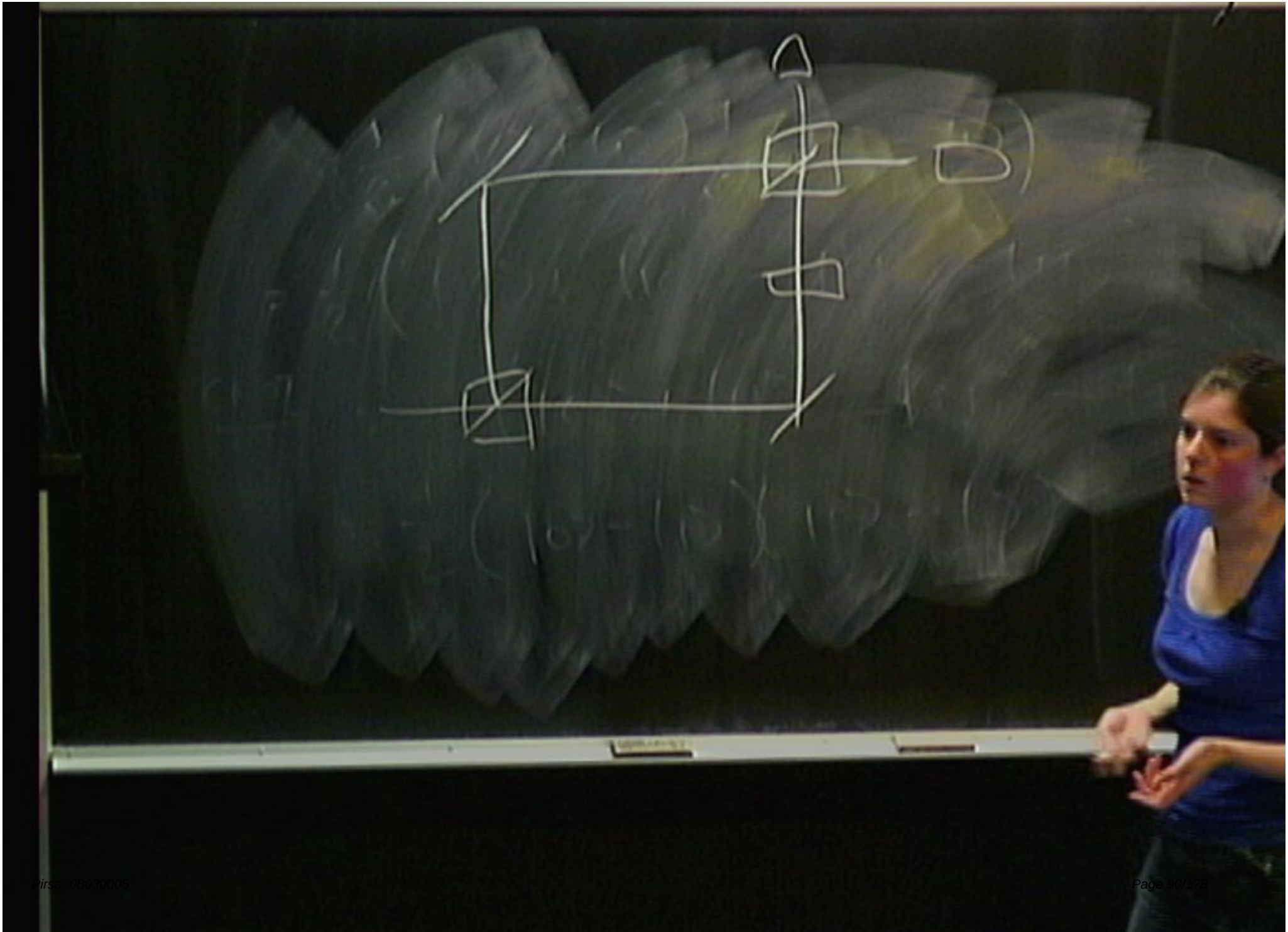

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$=\frac{1}{2}(|00\rangle+|10\rangle-|01\rangle-|11\rangle)$

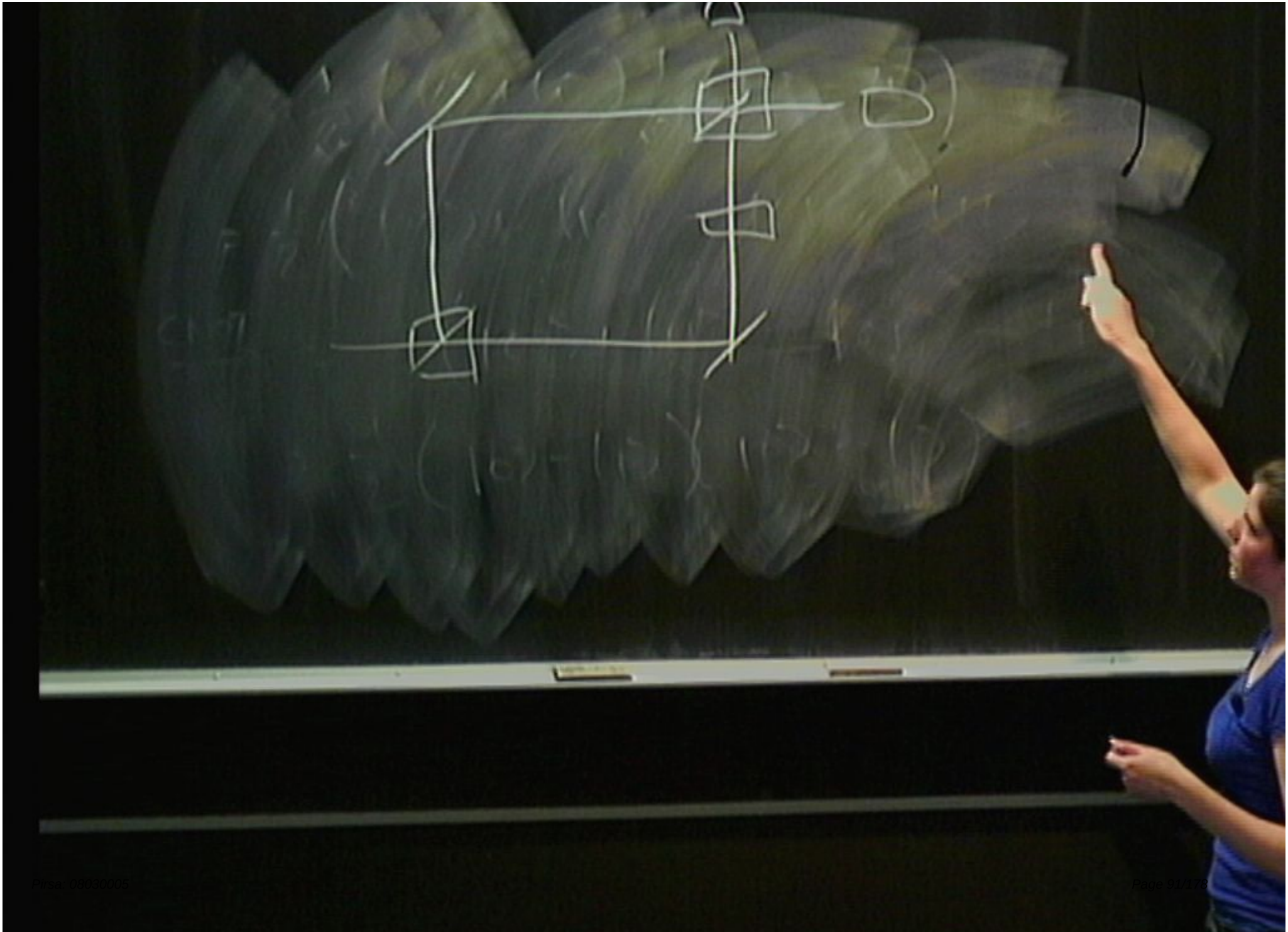

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$=\frac{1}{2}(|00\rangle+|10\rangle-|01\rangle-|11\rangle)$
CNOT
$=\frac{1}{2}(|00\rangle+|11\rangle-|01\rangle-|10\rangle)$
$=\frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)$

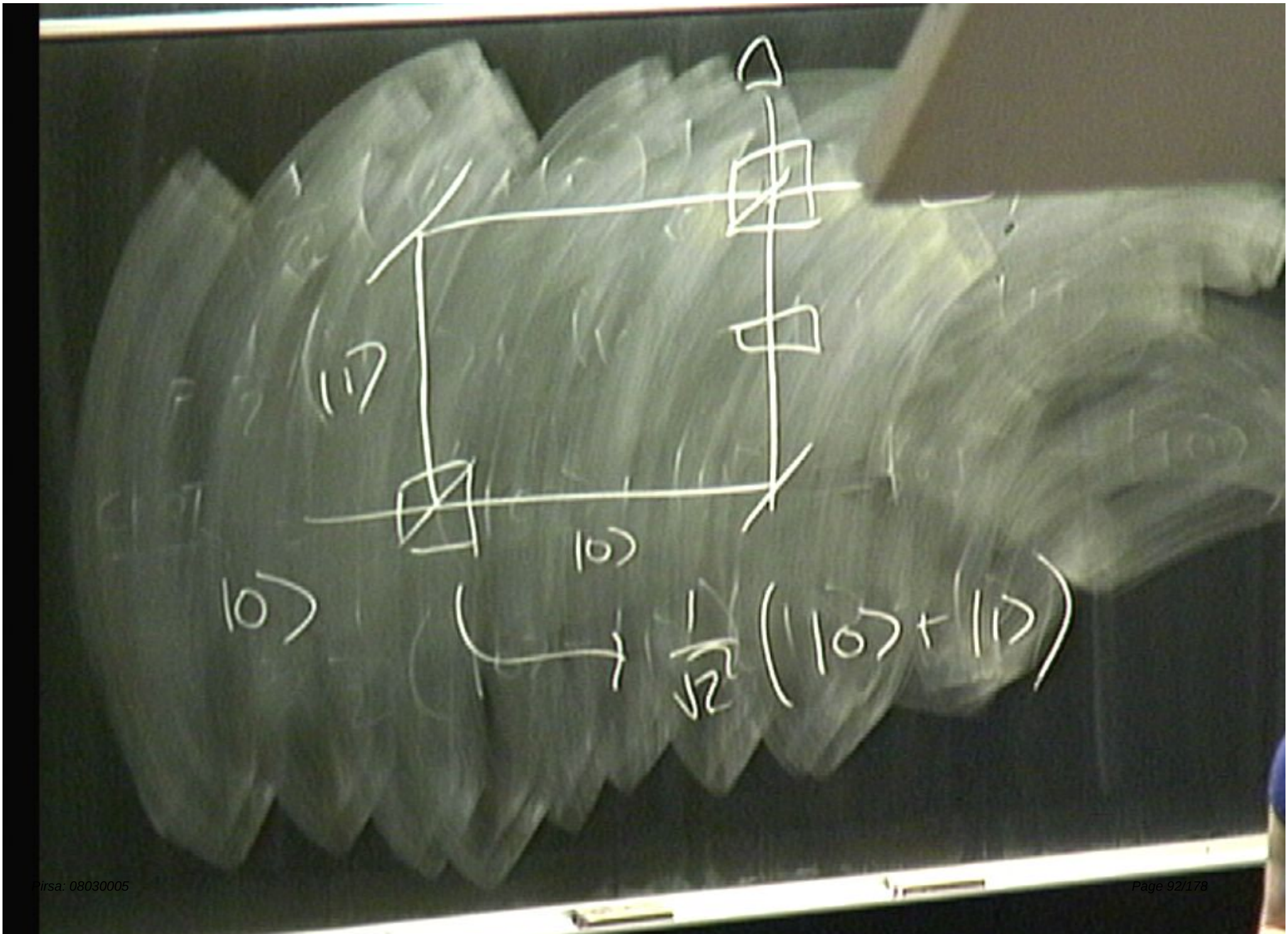


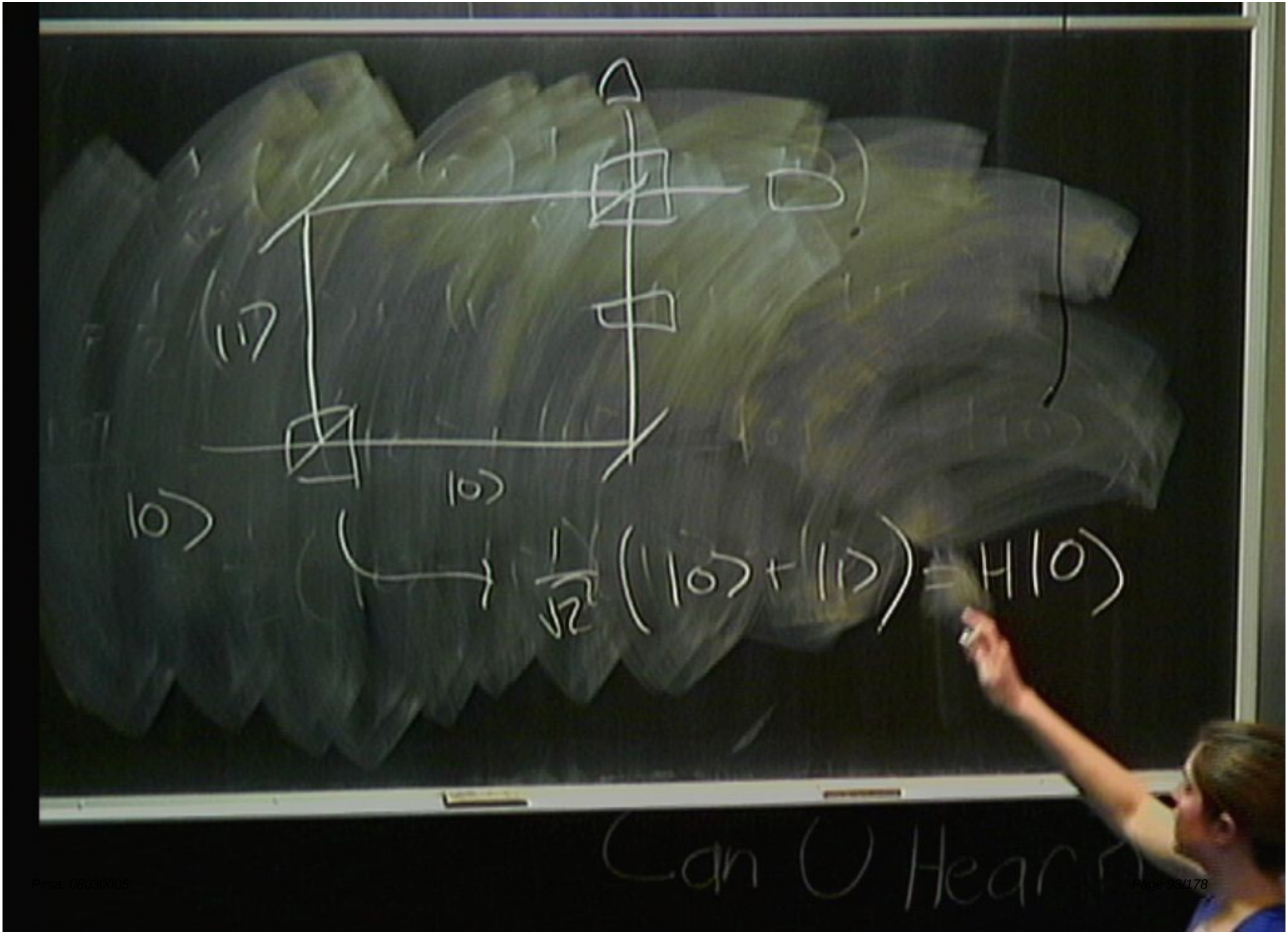


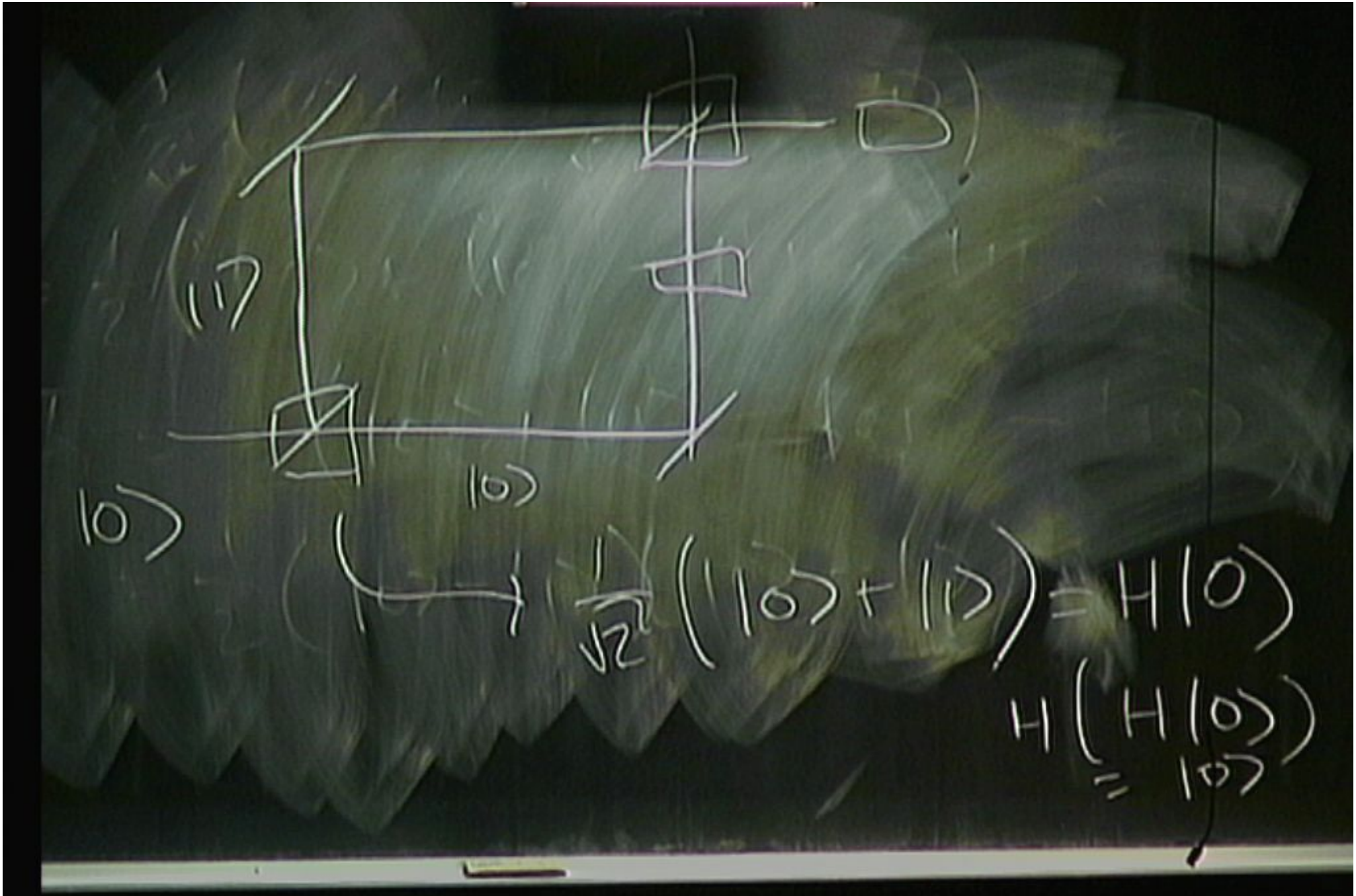


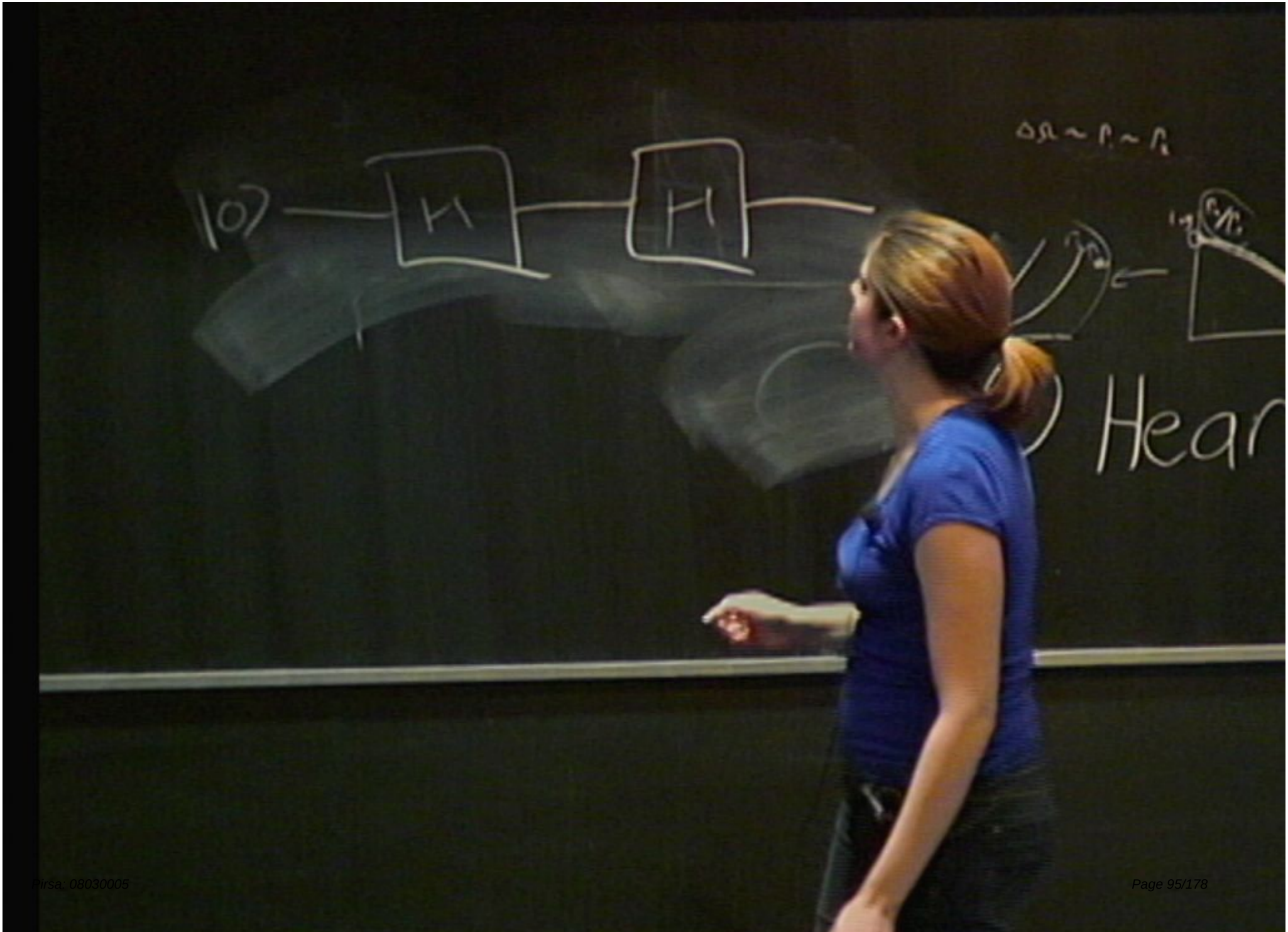





|1⟩
|0⟩
|0⟩ ⟶ 1/√2 (|0⟩ + |1⟩)

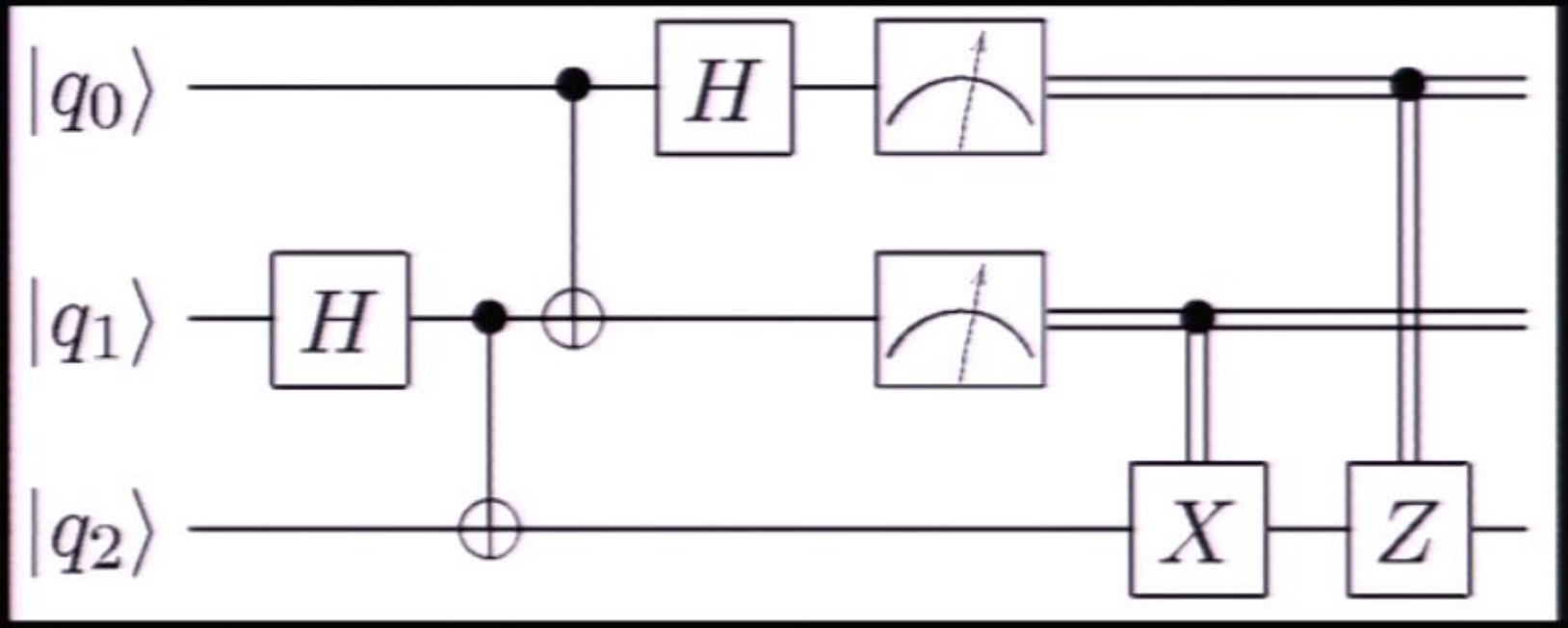

|1⟩
|0⟩
|0⟩
⟶ 1/√2 (|0⟩+|1⟩) = H|0⟩
Can U Hear D


|1⟩
|0⟩
|1⟩
|0⟩
H|0⟩ = 1/√2 (|0⟩ + |1⟩)
H(H|0⟩) = |0⟩

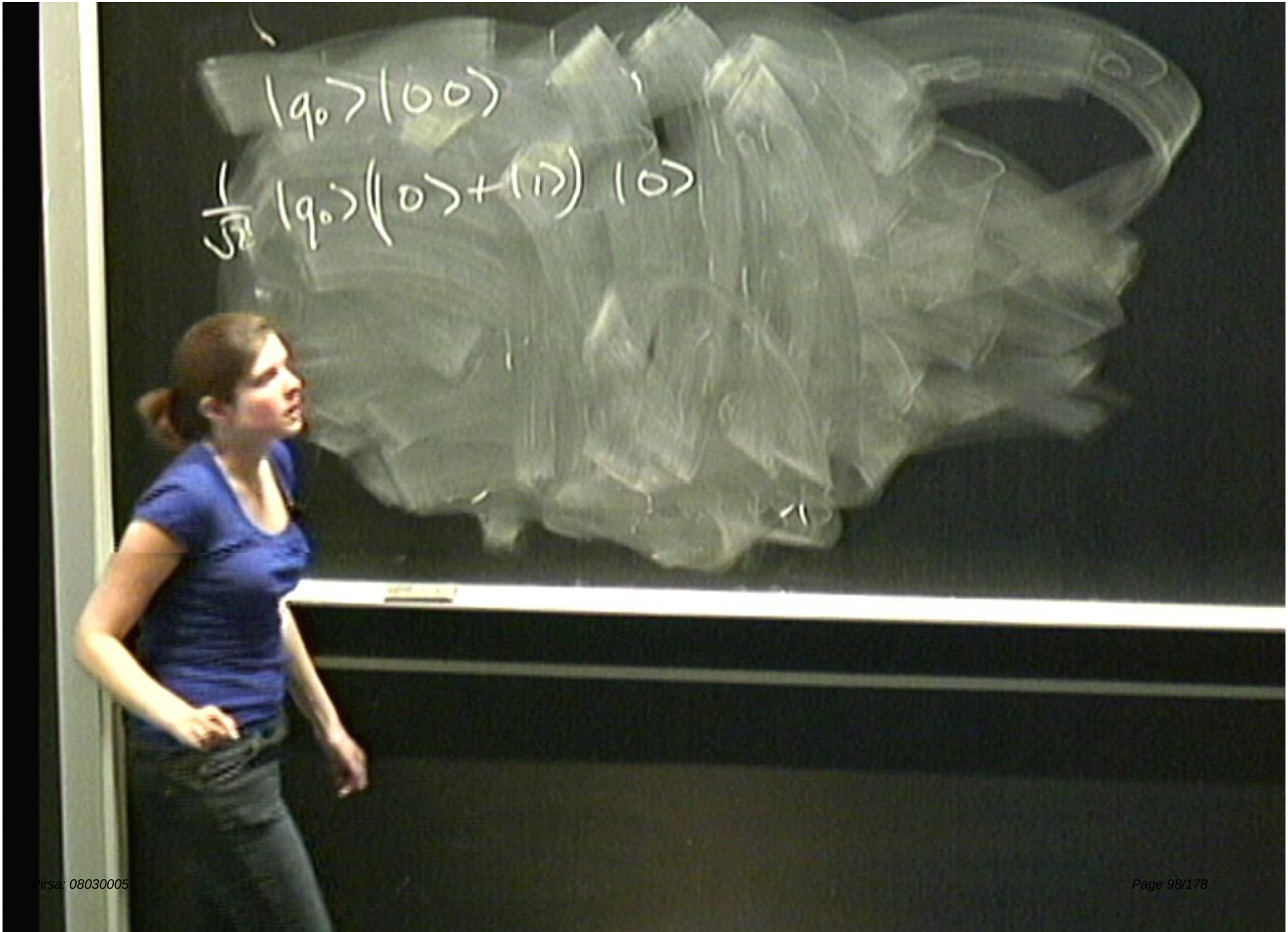

Hear

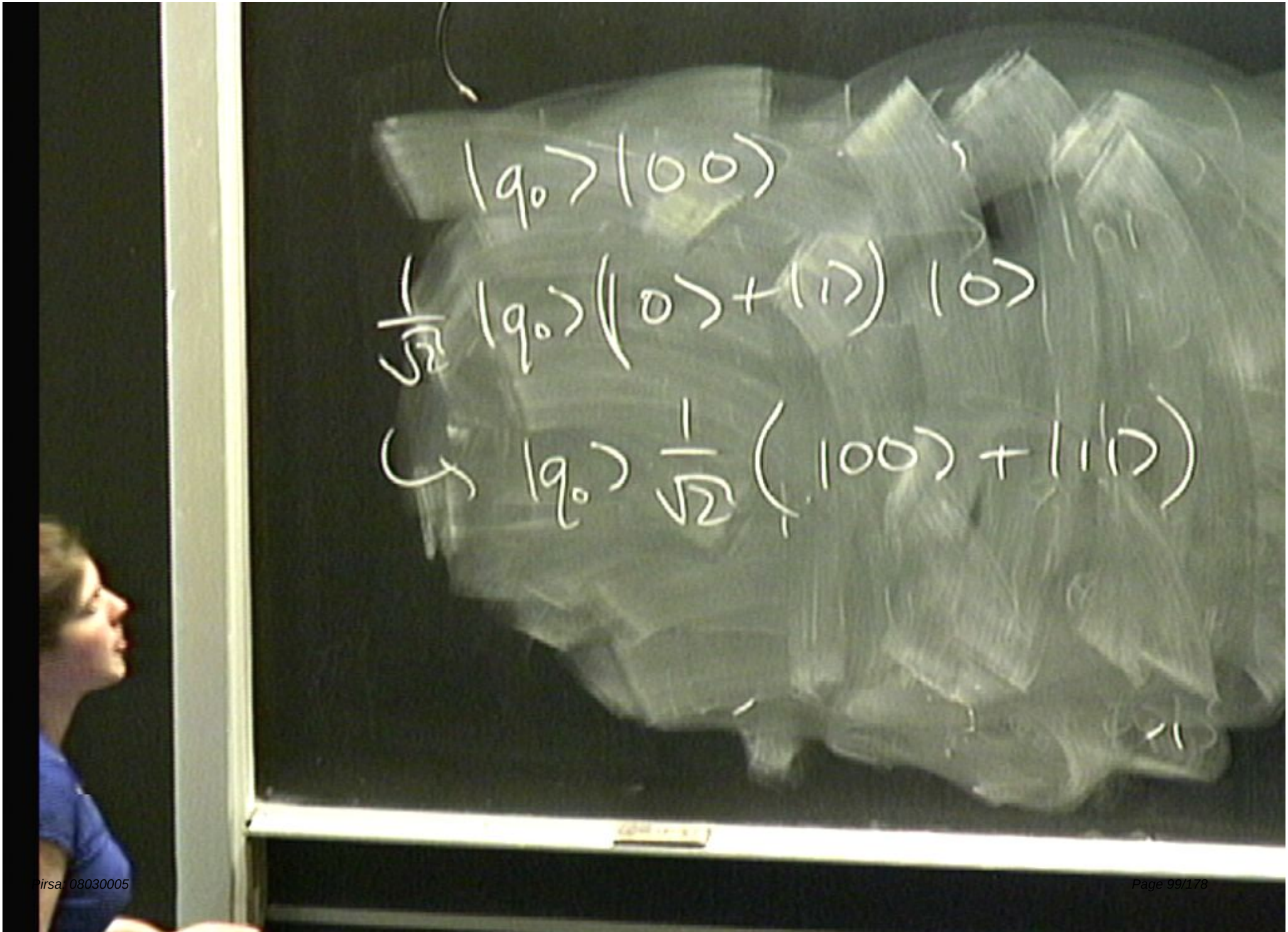
Quantum Circuit Diagrams

- e.g. teleportation




|q0>|00>


$|q_0\rangle|00\rangle$
$\frac{1}{\sqrt{2}}|q_0\rangle(|0\rangle+|1\rangle)|0\rangle$


$|q_0\rangle|00\rangle$
$\frac{1}{\sqrt{2}}|q_0\rangle(|0\rangle+|1\rangle)|0\rangle$
$\hookrightarrow |q_0\rangle\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$

$$|q_0\rangle|00\rangle$$

$$\frac{1}{\sqrt{2}}|q_0\rangle(|0\rangle+|1\rangle)|0\rangle$$

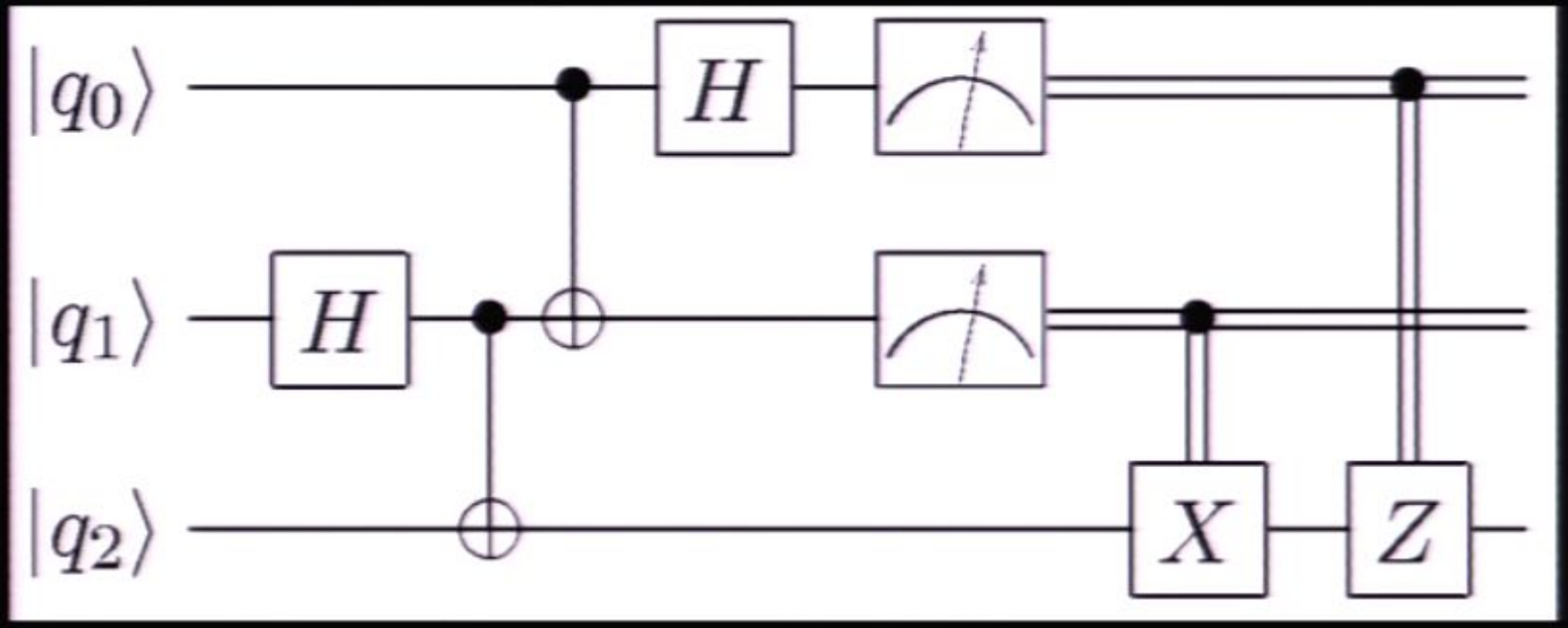
$$\rightarrow |q_0\rangle\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$$

$$\frac{1}{\sqrt{2}}(|q_0\rangle|00\rangle+|q_0\rangle|11\rangle)$$

$$\rightarrow \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$$

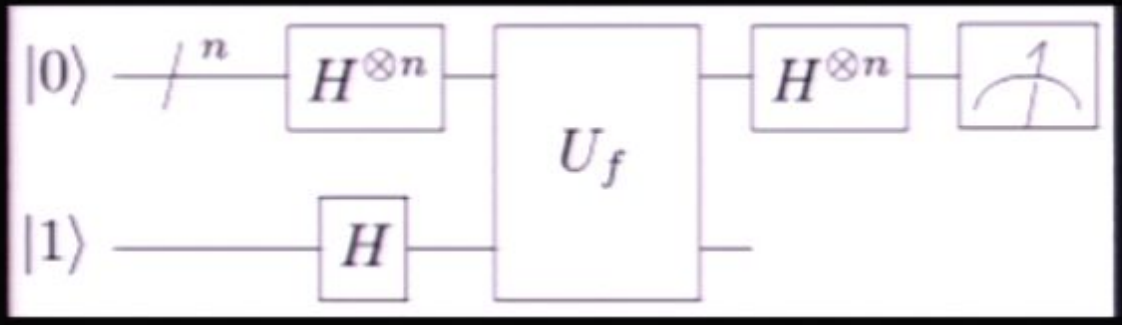
Quantum Circuit Diagrams

- e.g. teleportation

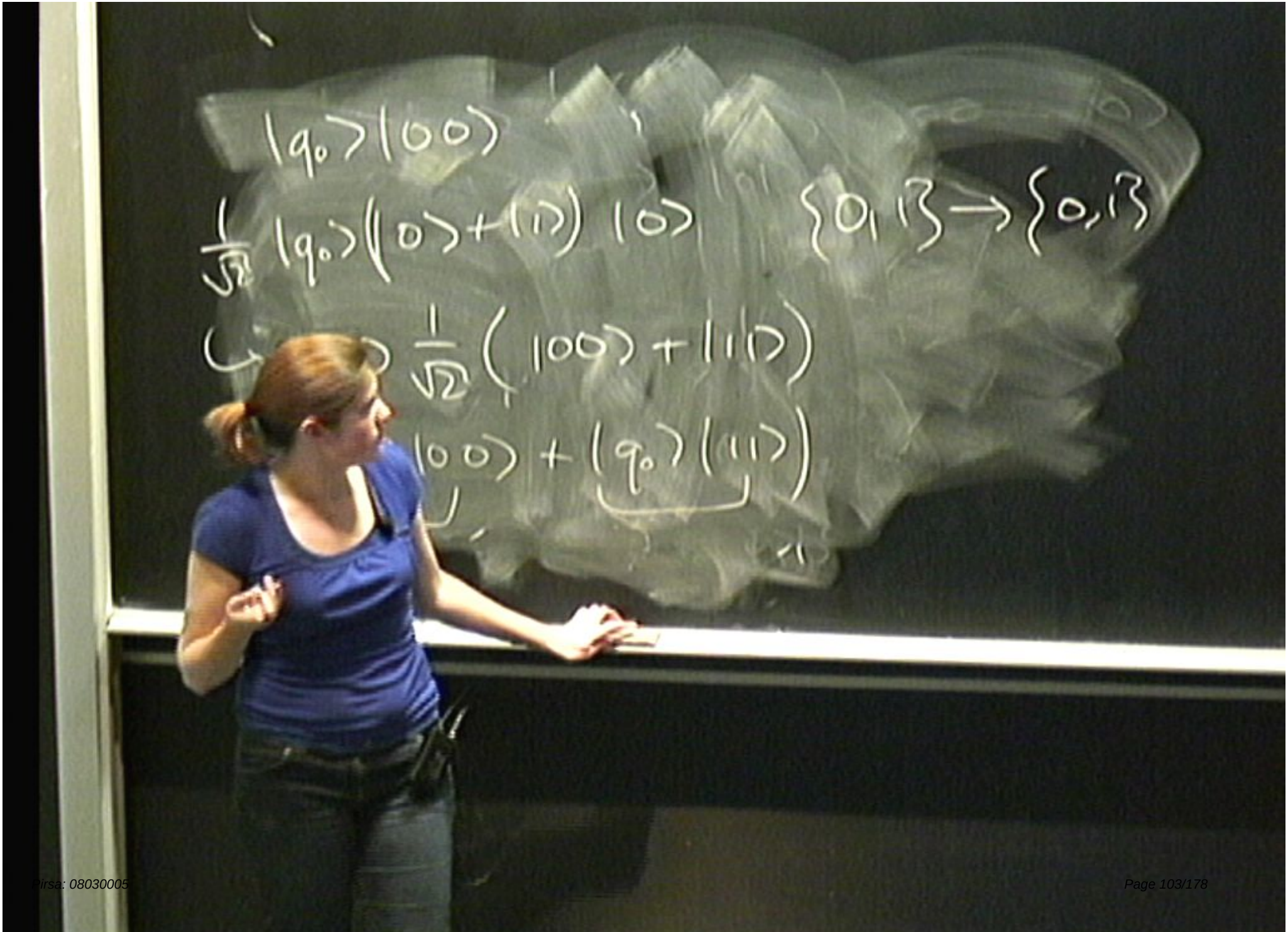


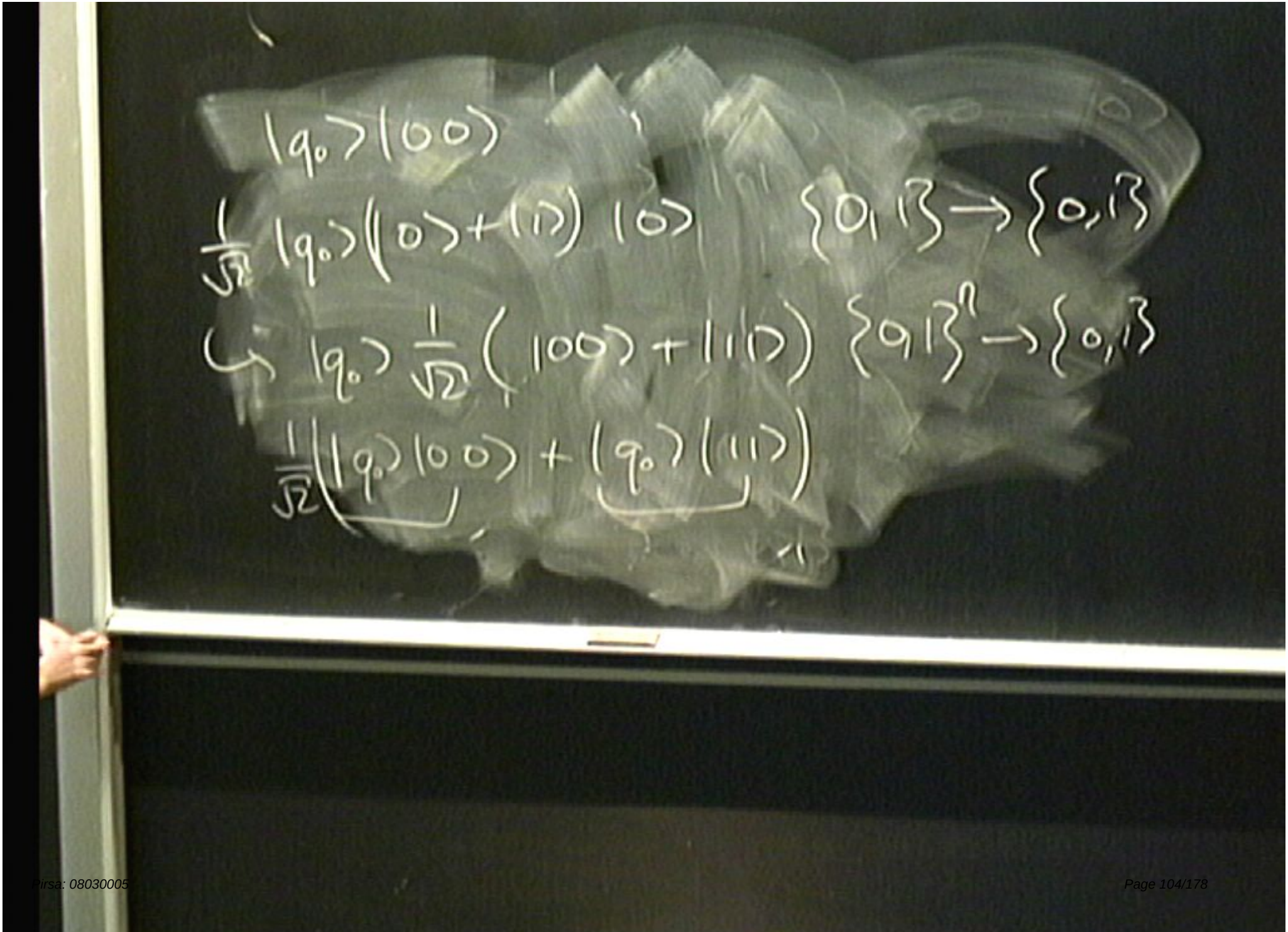
Deutsch-Josza Algorithm

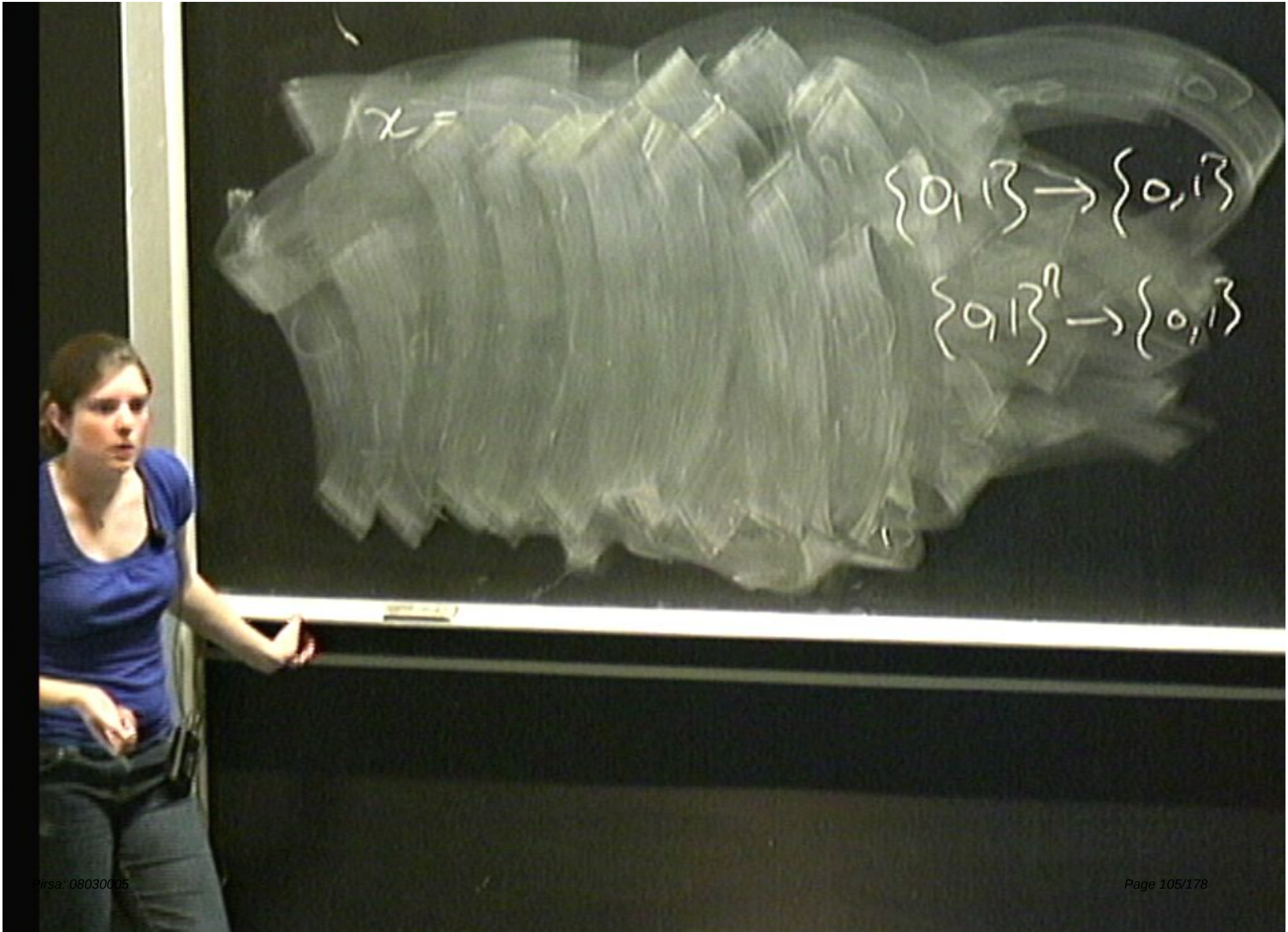
- Extension of Deutsch algorithm
- Quantum circuit diagram

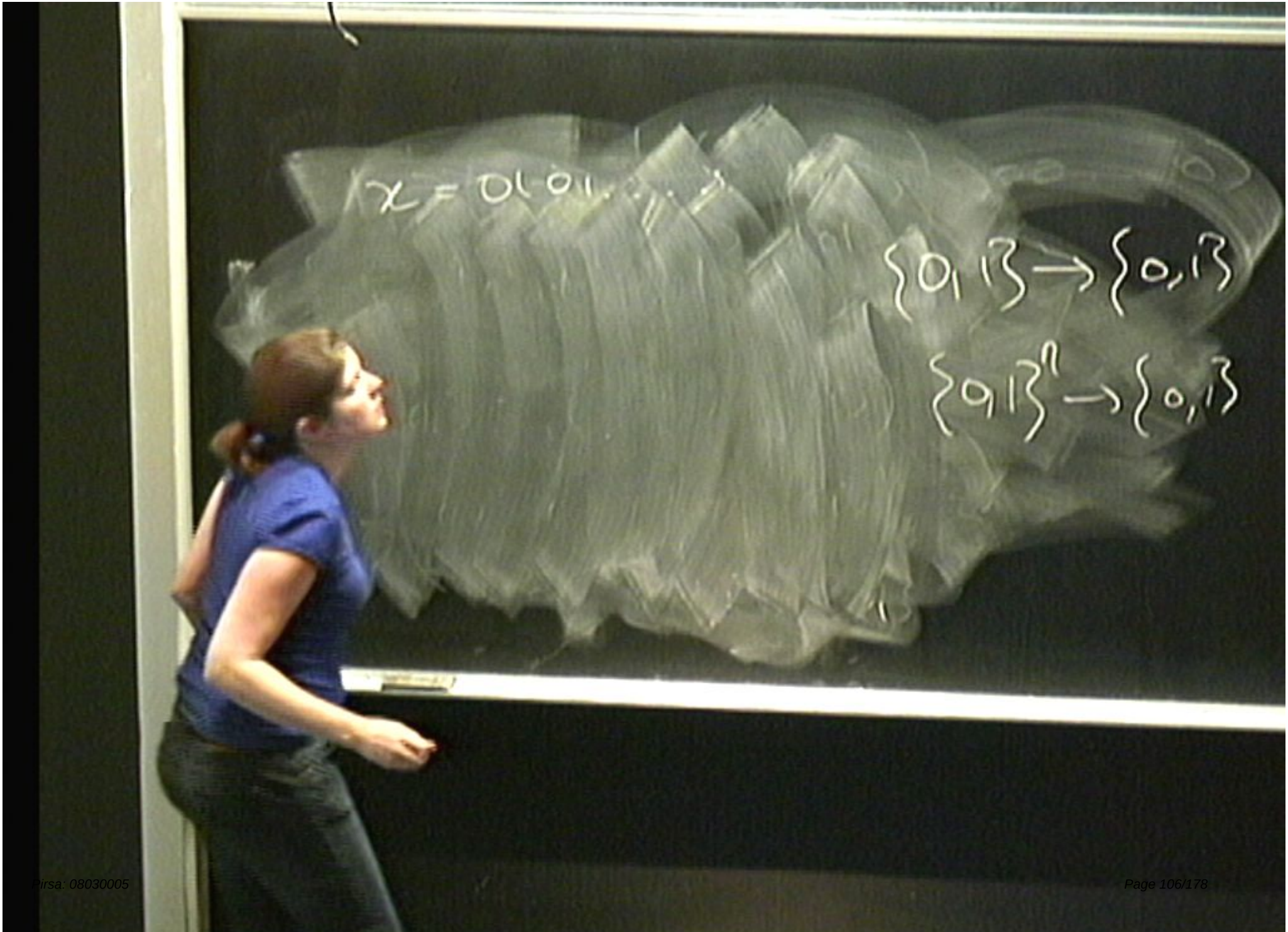


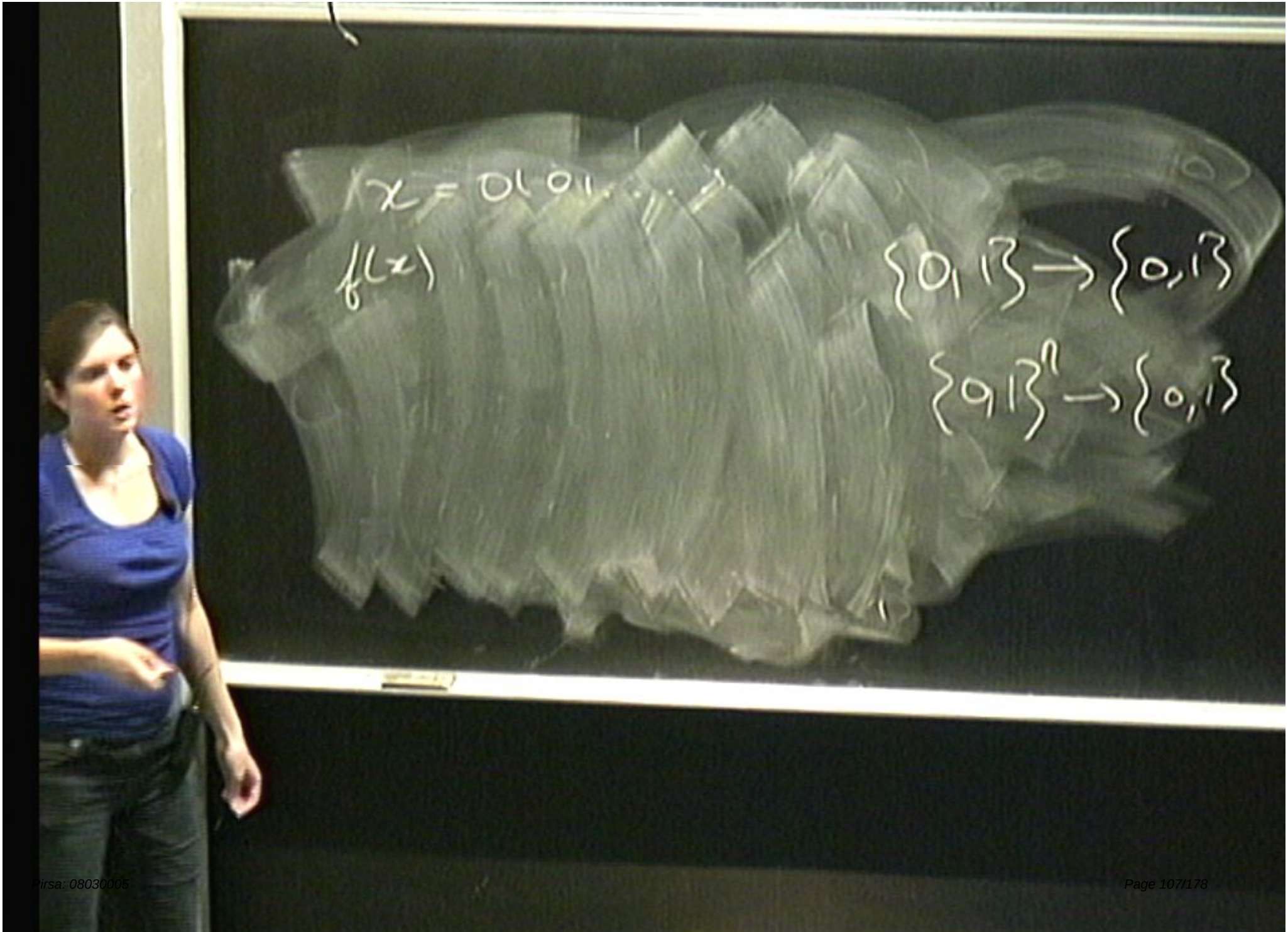
- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.


$|q_0\rangle|00\rangle$
$\frac{1}{\sqrt{2}}|q_0\rangle(|0\rangle+|1\rangle)|0\rangle$
$\{0,1\}\rightarrow\{0,1\}$
$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$
$|00\rangle+|q_0\rangle|11\rangle$

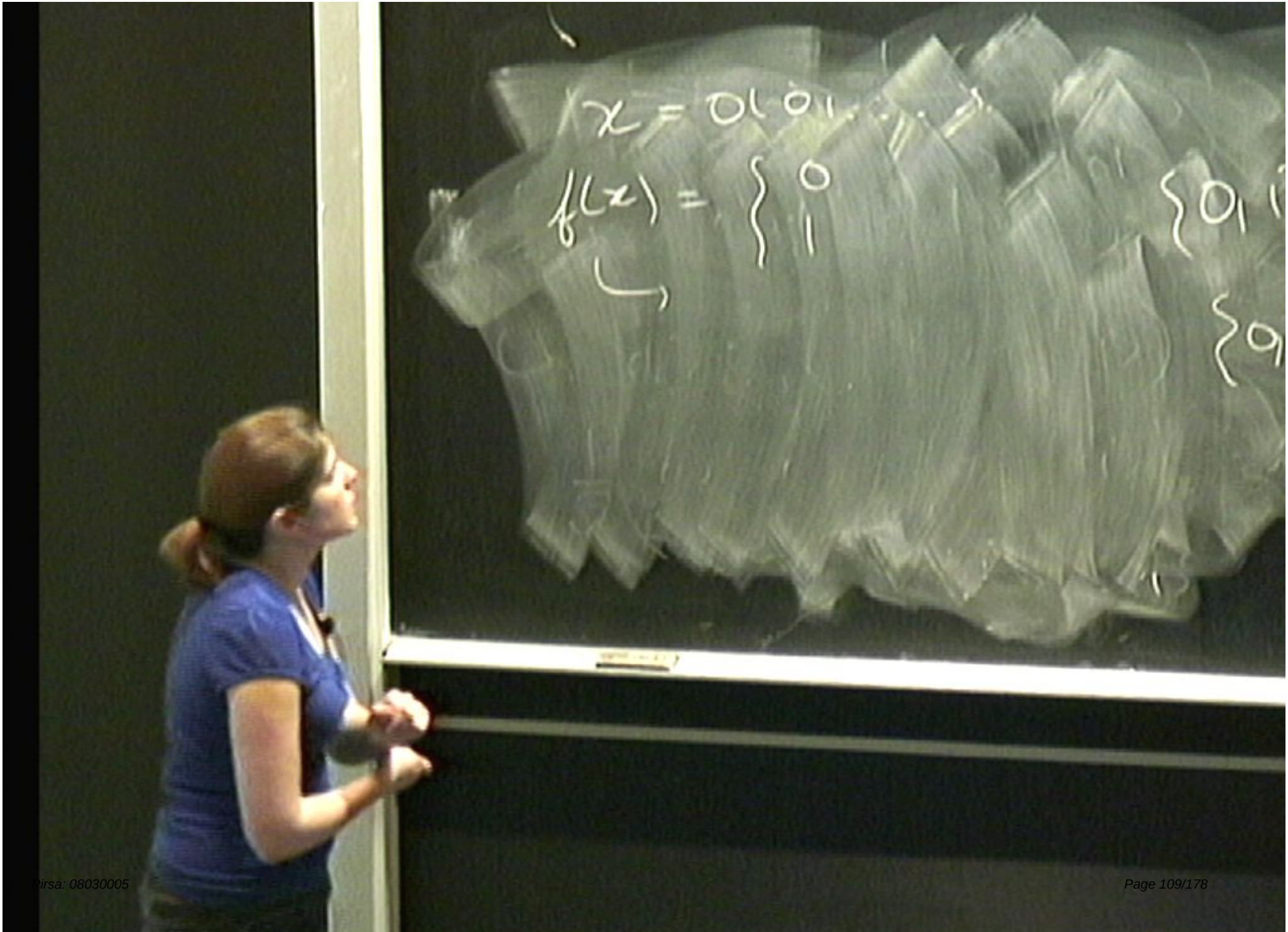

$|q_0\rangle|00\rangle$
$\frac{1}{\sqrt{2}}|q_0\rangle(|0\rangle+|1\rangle)|0\rangle$ $\{0,1\}\to\{0,1\}$
$\hookrightarrow |q_0\rangle\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ $\{0,1\}^n\to\{0,1\}$
$\frac{1}{\sqrt{2}}(|q_0\rangle|00\rangle+|q_0\rangle|11\rangle)$

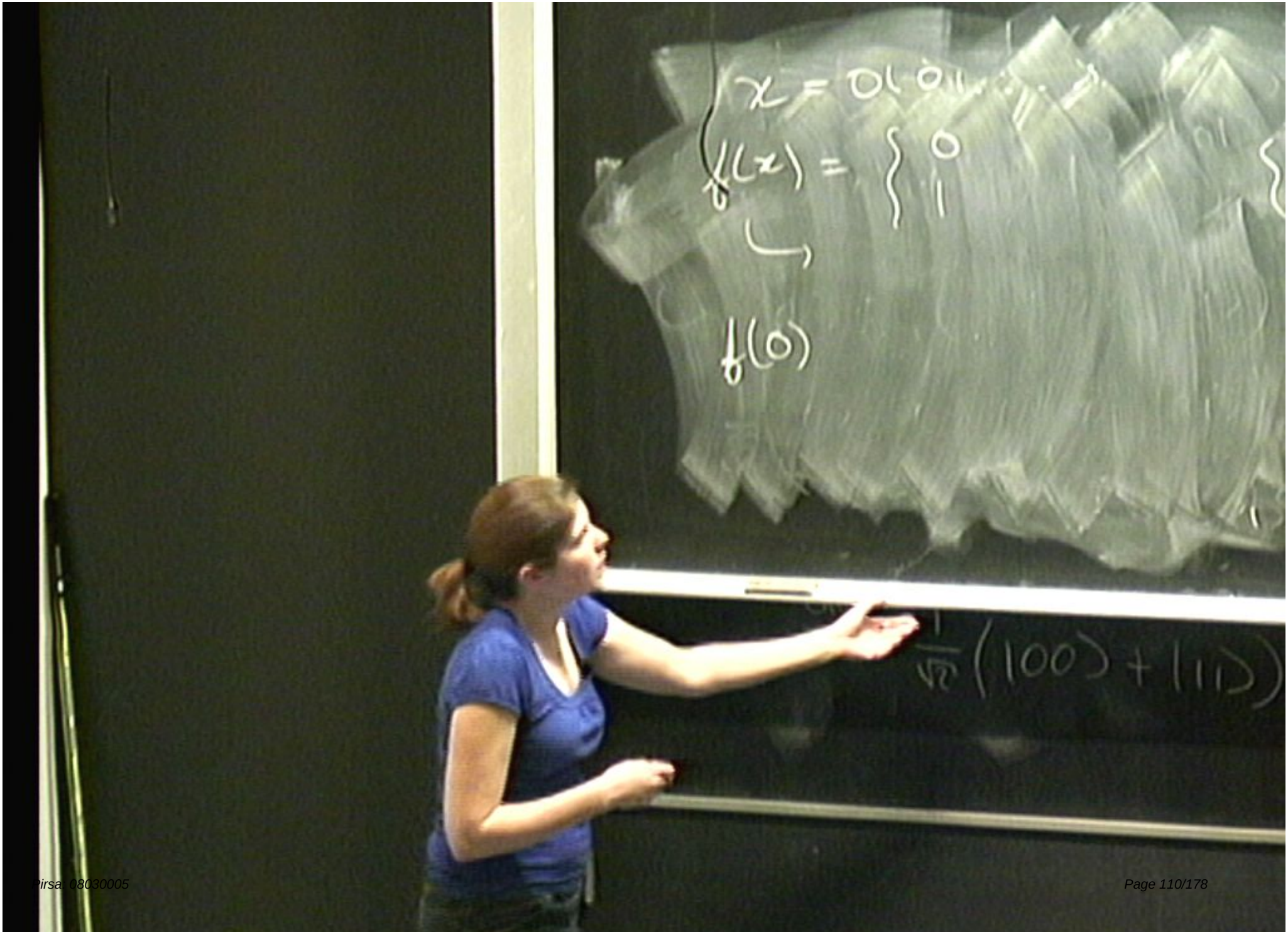

$\chi =$
$\{0,1\} \to \{0,1\}$
$\{0,1\}^n \to \{0,1\}$


$\{0,1\}^3 \to \{0,1\}$
$\{0,1\}^n \to \{0,1\}$

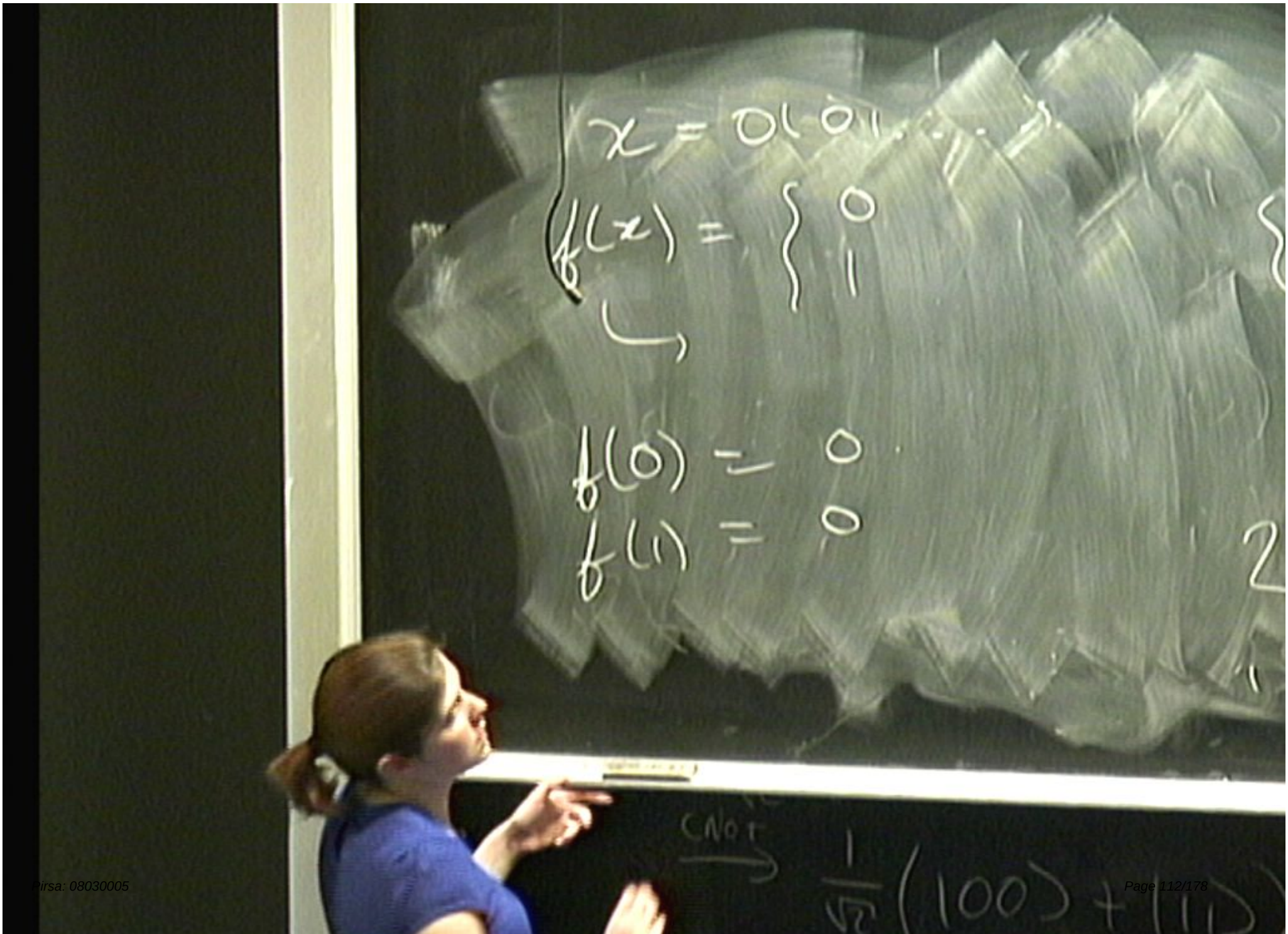

$x = 0101\ldots$
$f(x)$
$\{0,1\} \to \{0,1\}$
$\{0,1\}^n \to \{0,1\}$

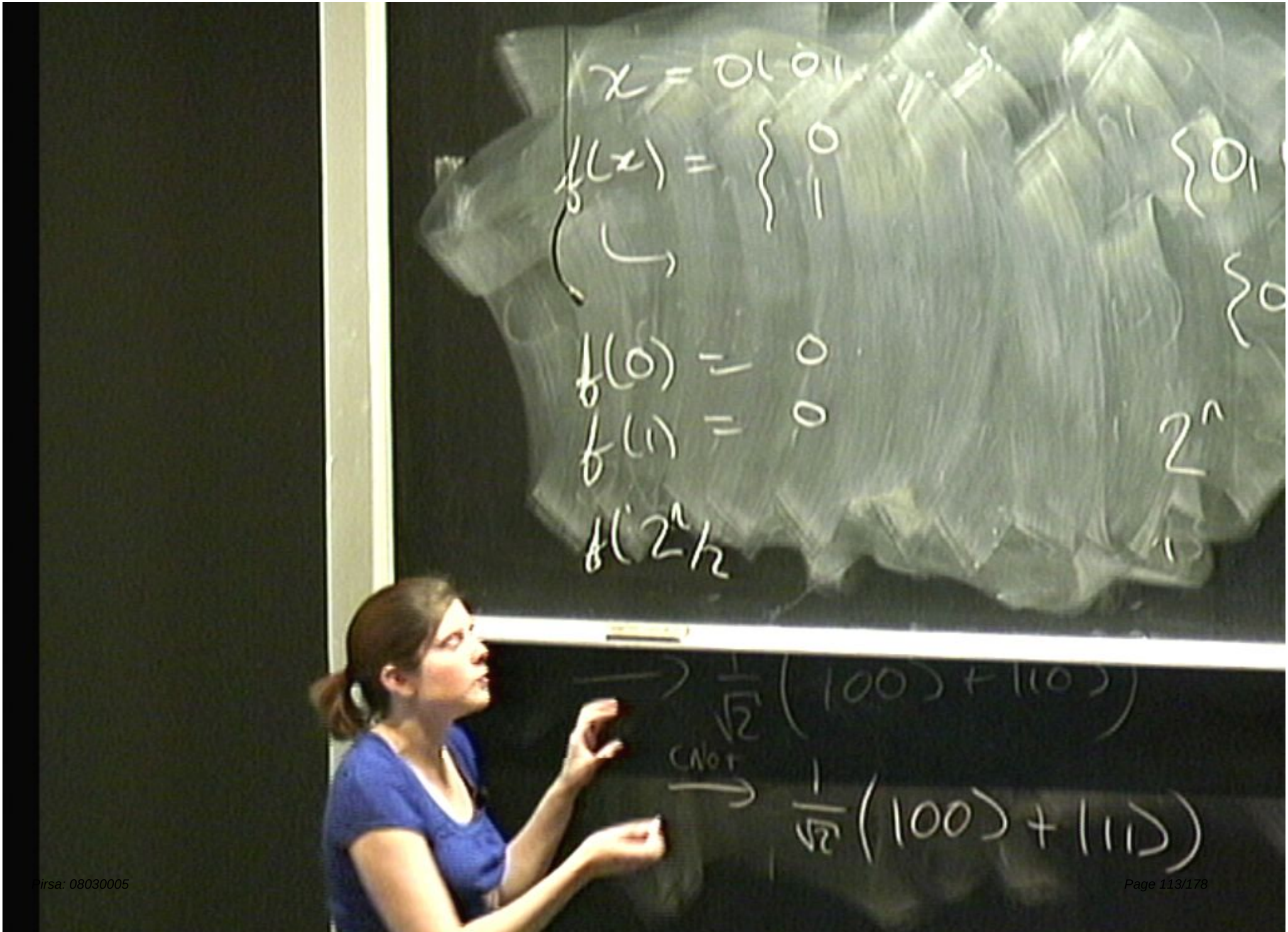

x = 0(01...
f(x) = { 0
1

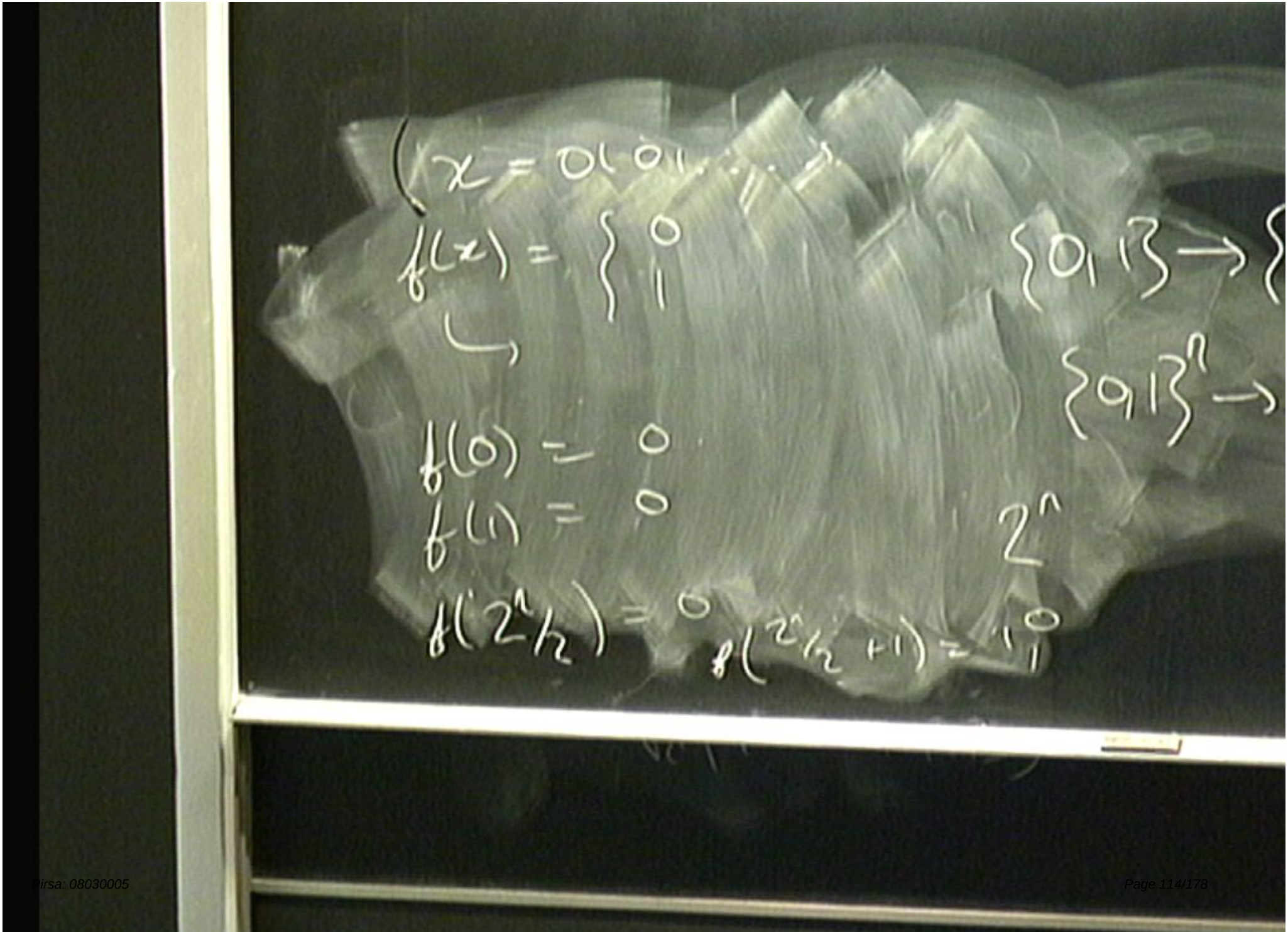

$x = 0101\ldots$
$f(x) = \begin{cases} 0 \\ 1 \end{cases}$
$\{0,1$
$\{0$


f(x) = { 0
1
f(0)
1/√2 (|00⟩ + |11⟩)


f(x) = { 0
1
f(0) = 0
CNOT
1/√2 (|00⟩ + |11⟩)

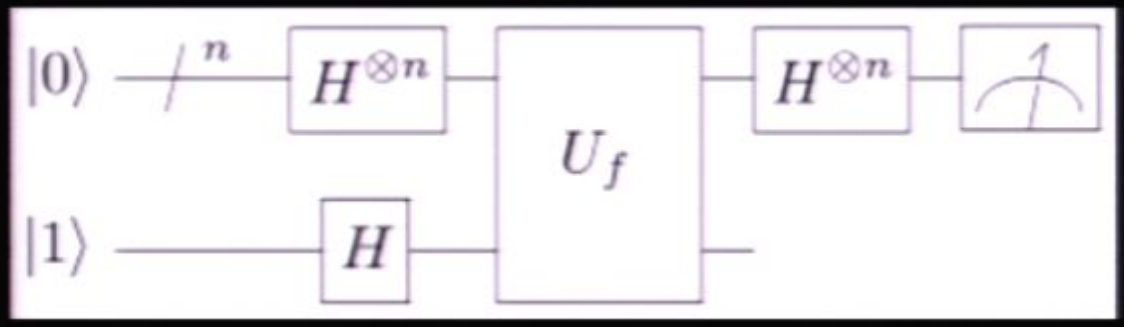

x = 0(01...)
f(x) = { 0
1
f(0) = 0
f(1) = 0
CNOT


f(x) = { 0
1
f(0) = 0
f(1) = 0
f(2^k
2^
1/√2 (|00⟩ + |10⟩)
CNOT
1/√2 (|00⟩ + |11⟩)


$x = 0101\ldots$
$f(x) = \begin{cases} 0 \\ 1 \end{cases}$
$\{0,1\} \to \{$
$\hookrightarrow$
$\{0,1\}^n \to$
$f(0) = 0$
$f(1) = 0$
2^n
$f(2^n k) = 0$
$f(2^n k + 1) = 1$

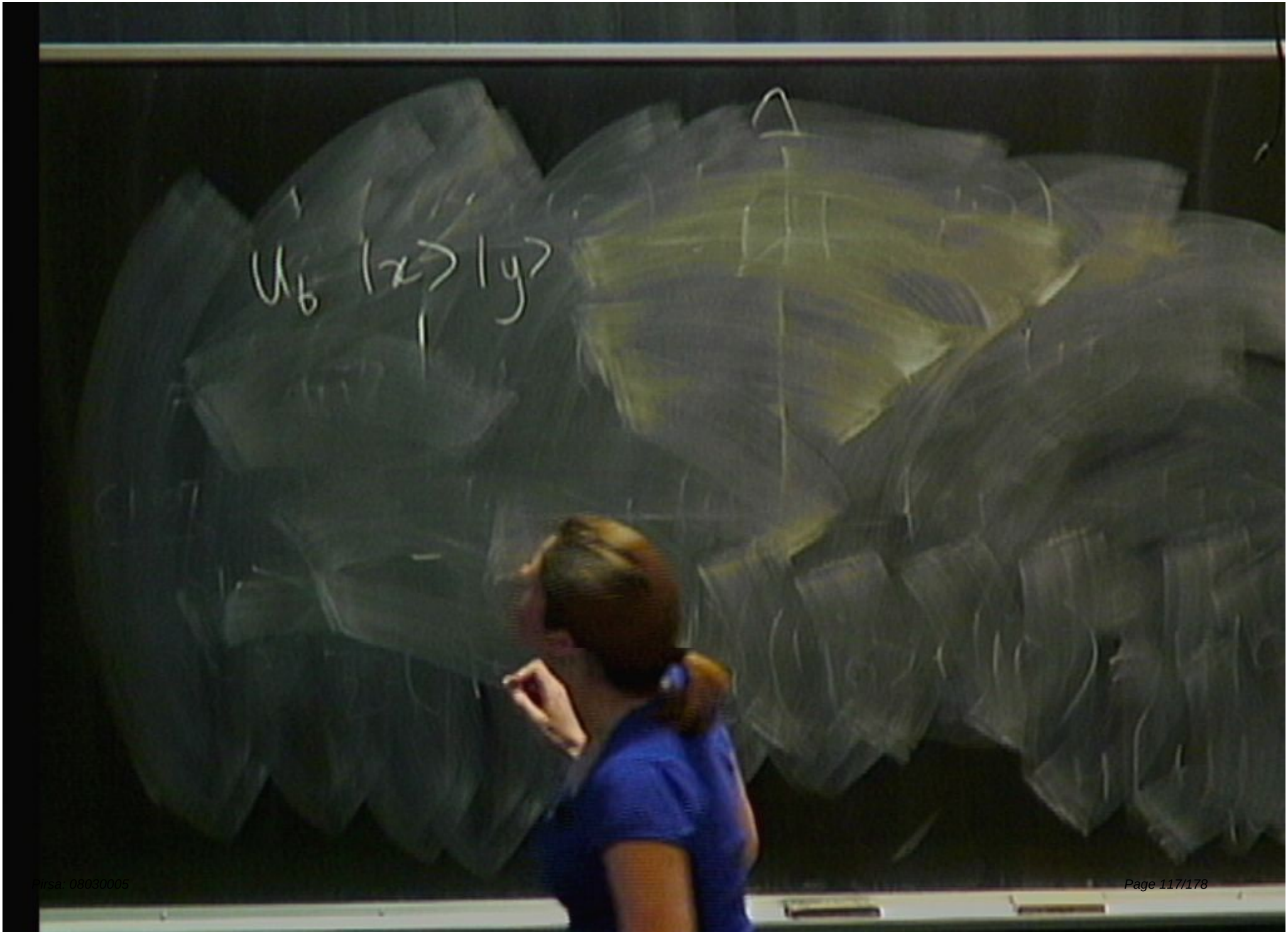
Deutsch-Josza Algorithm

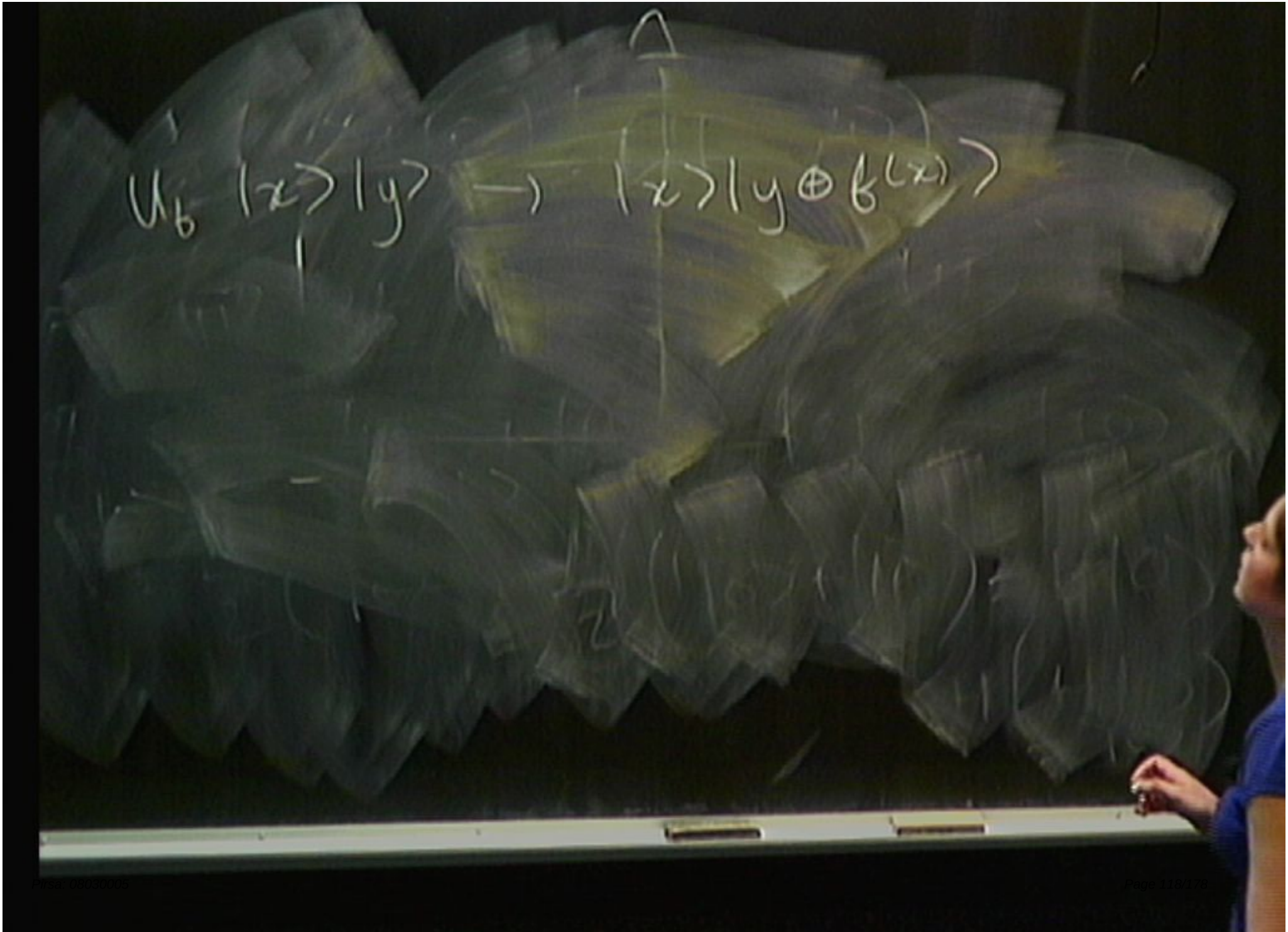
- Extension of Deutsch algorithm
- Quantum circuit diagram

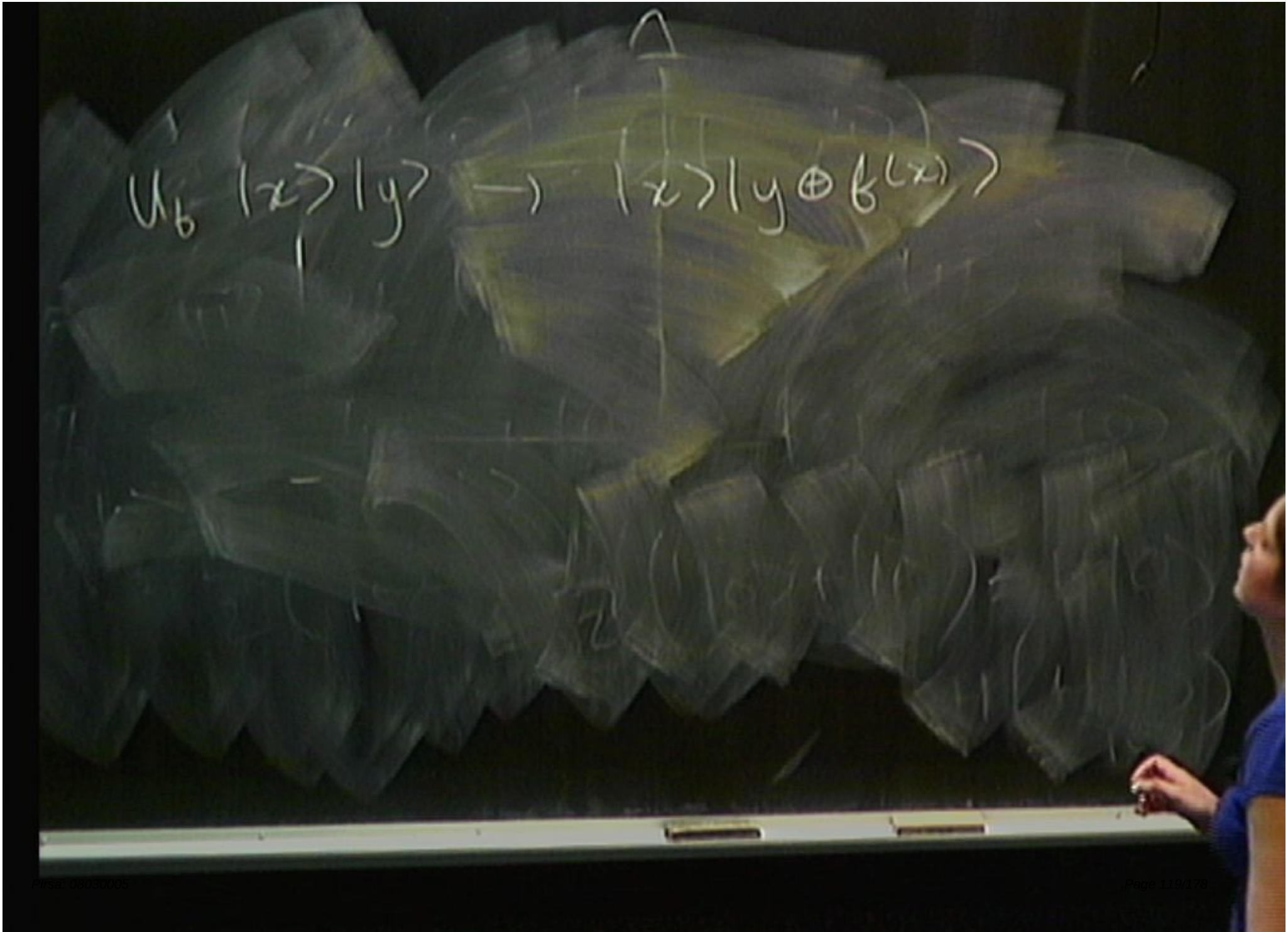


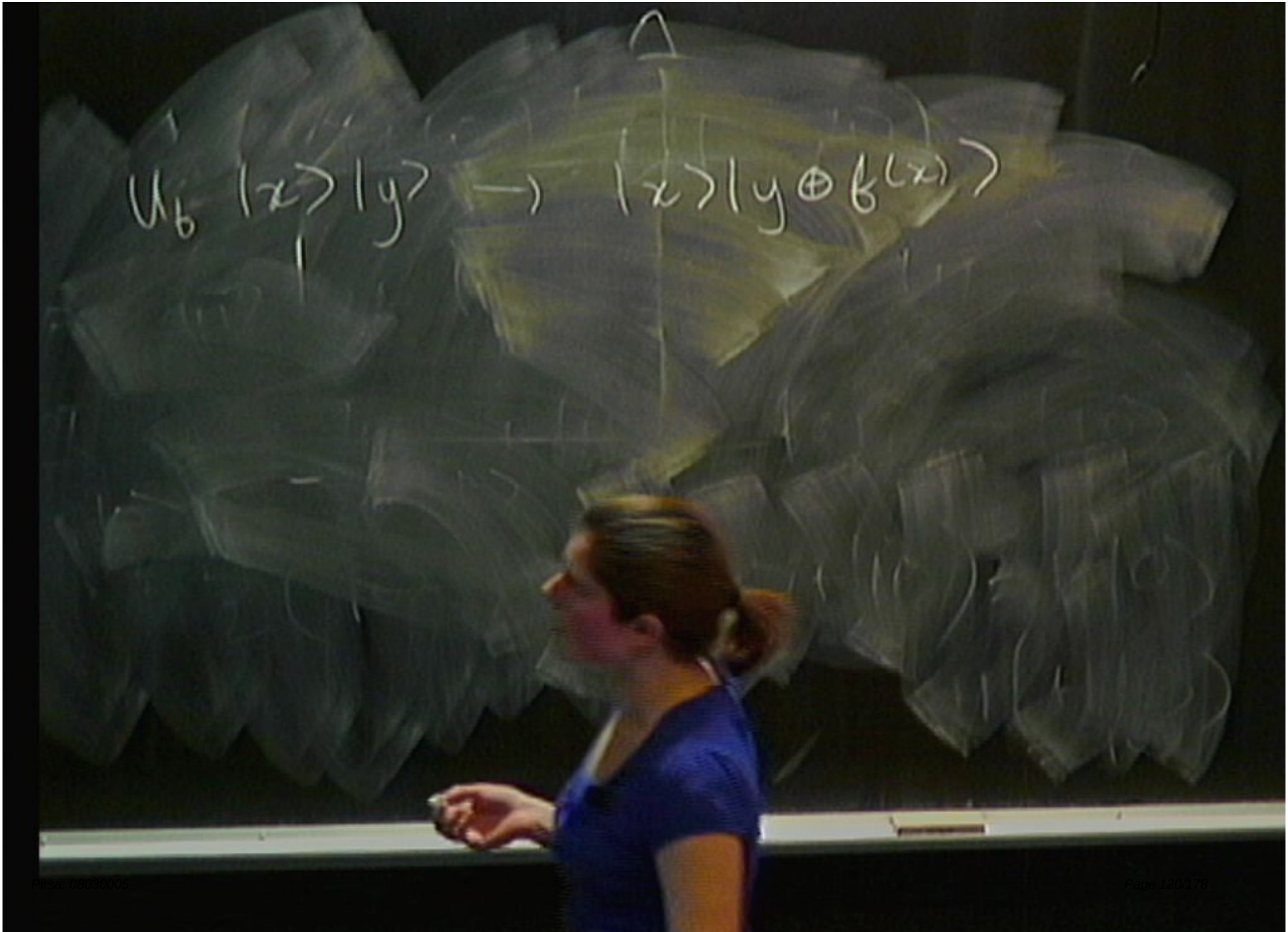
- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.

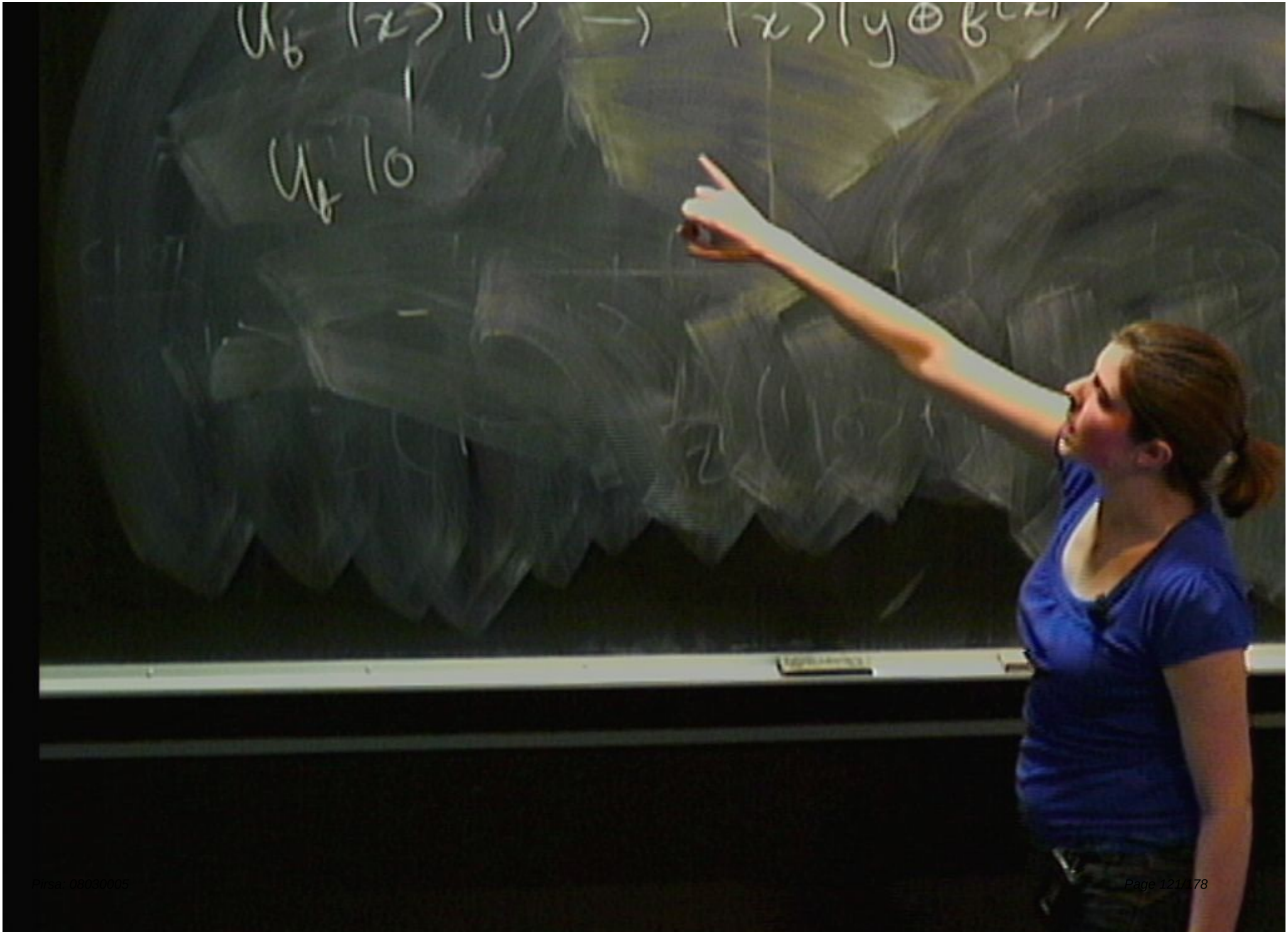

|x>|y>

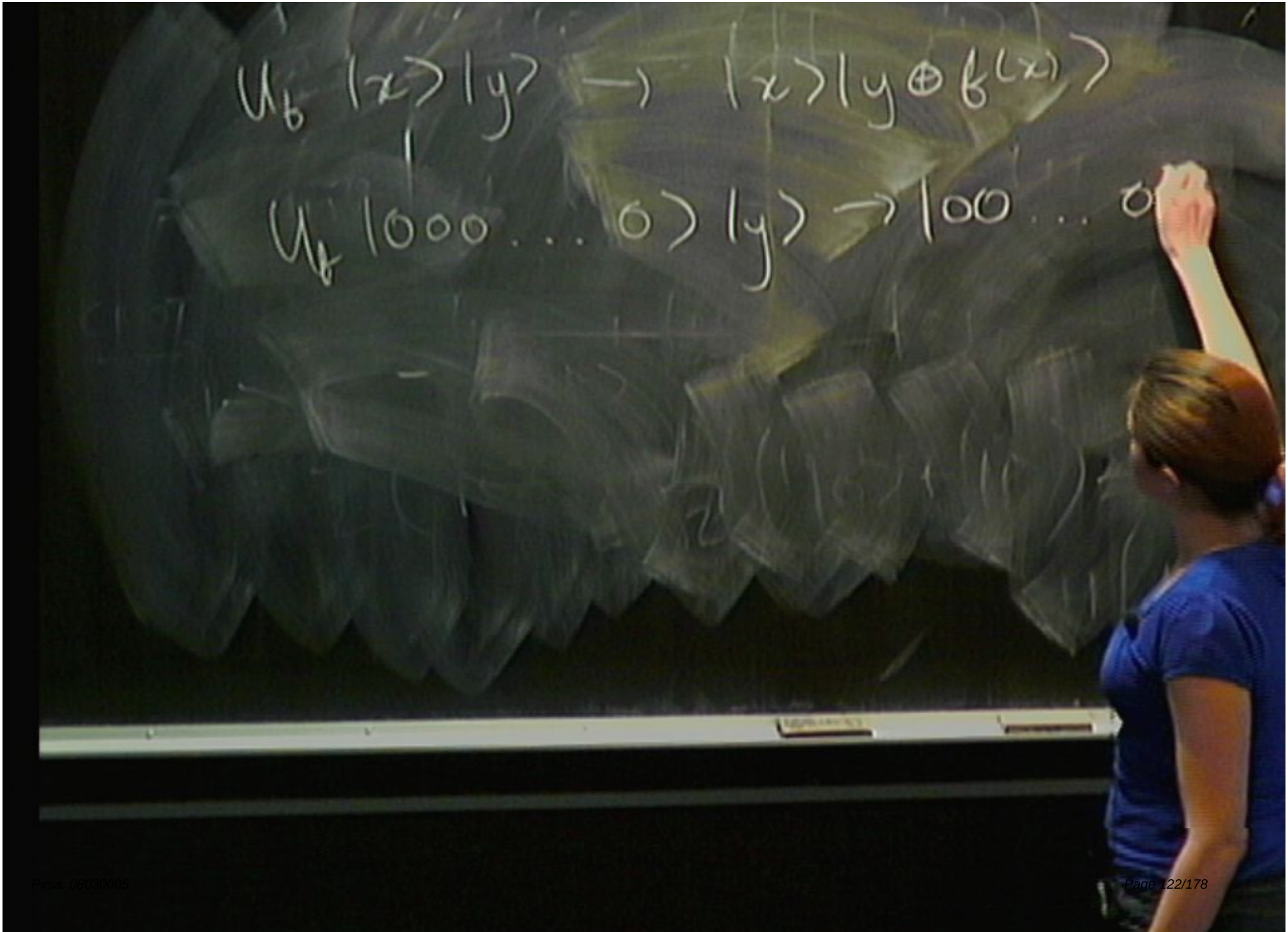

$U_b |x\rangle |y\rangle$

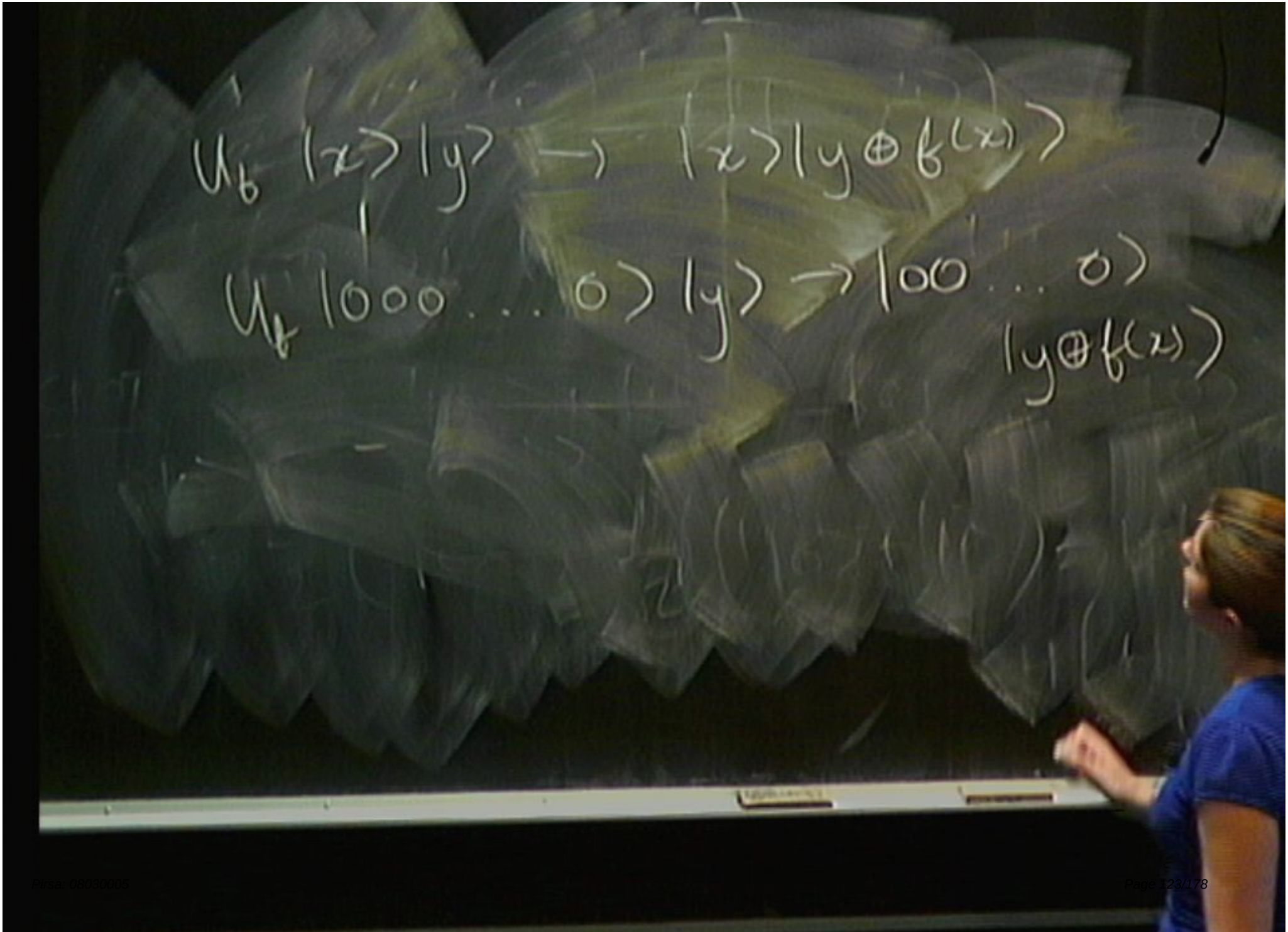

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$

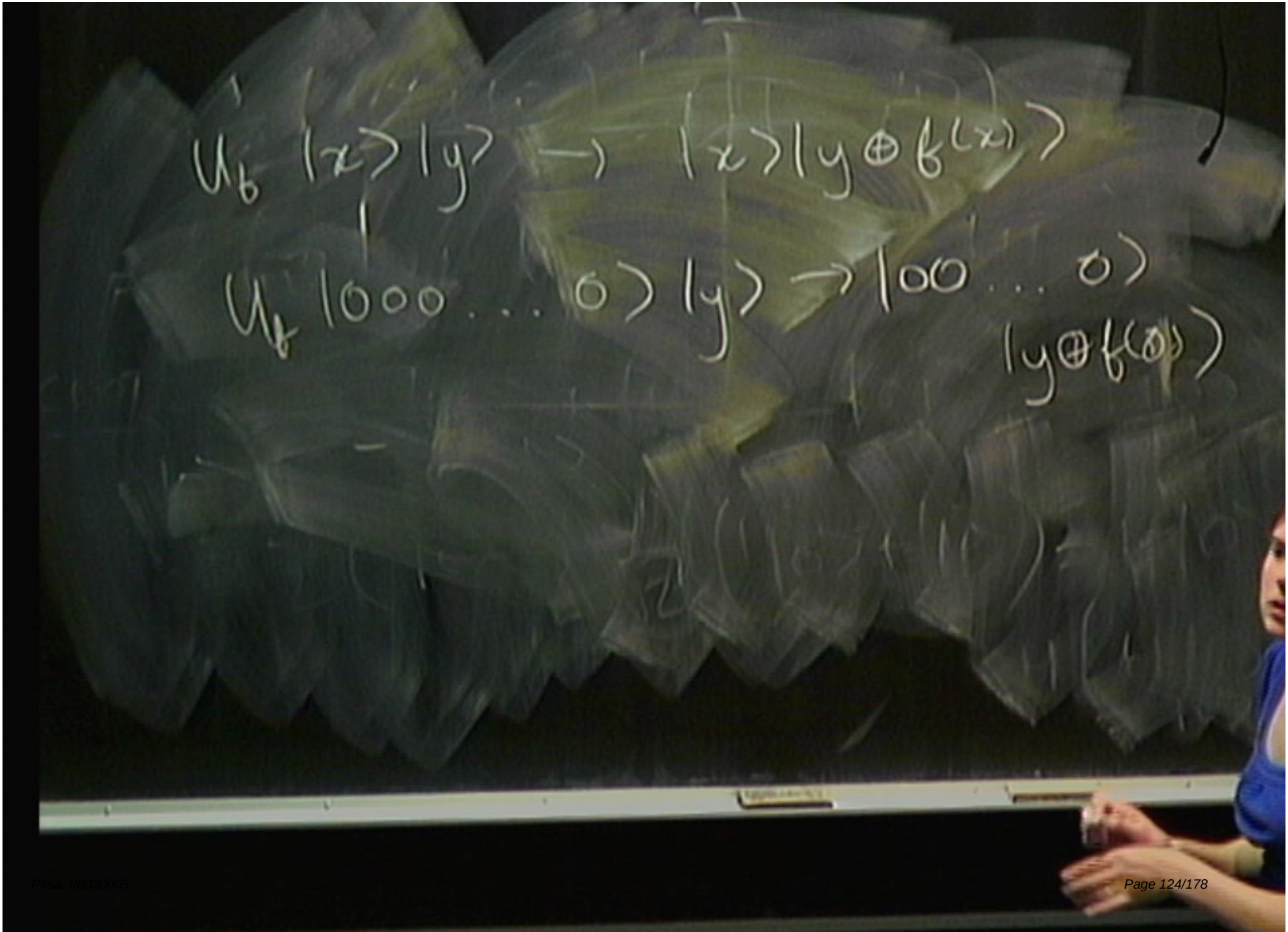

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$

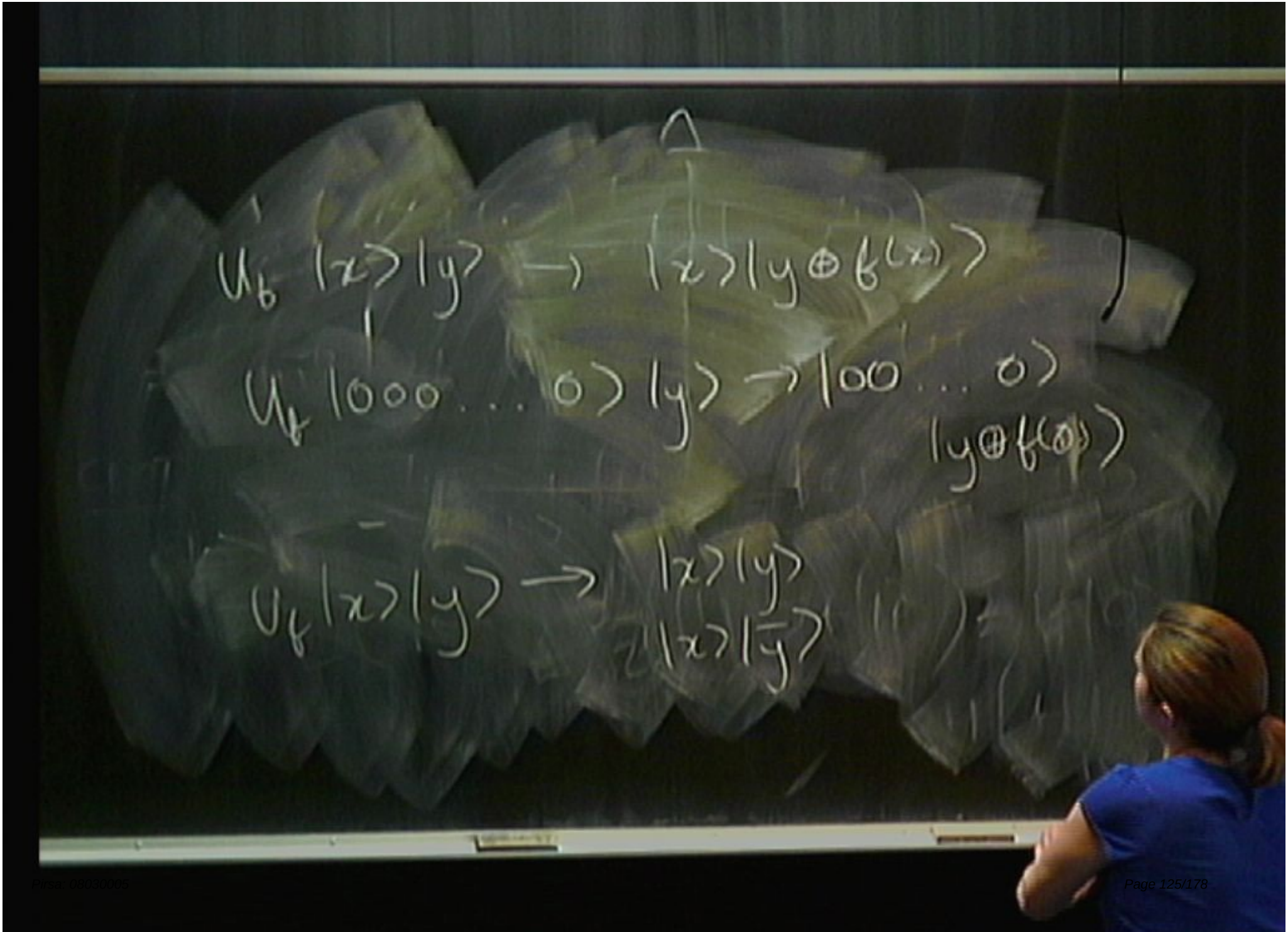

$U_b |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus b(x)\rangle$

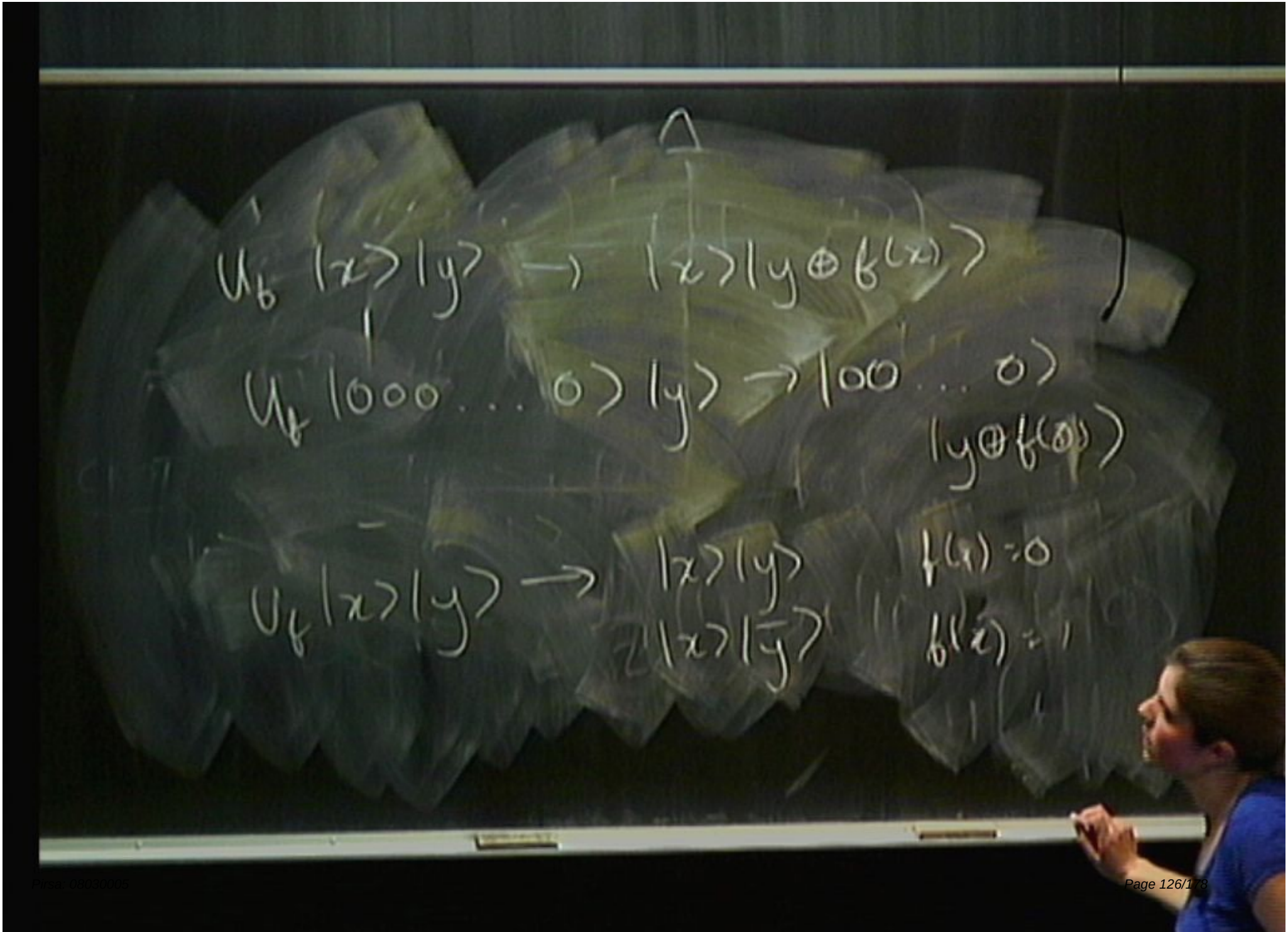

$U_b |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus b(x)\rangle$
$U_b |0$

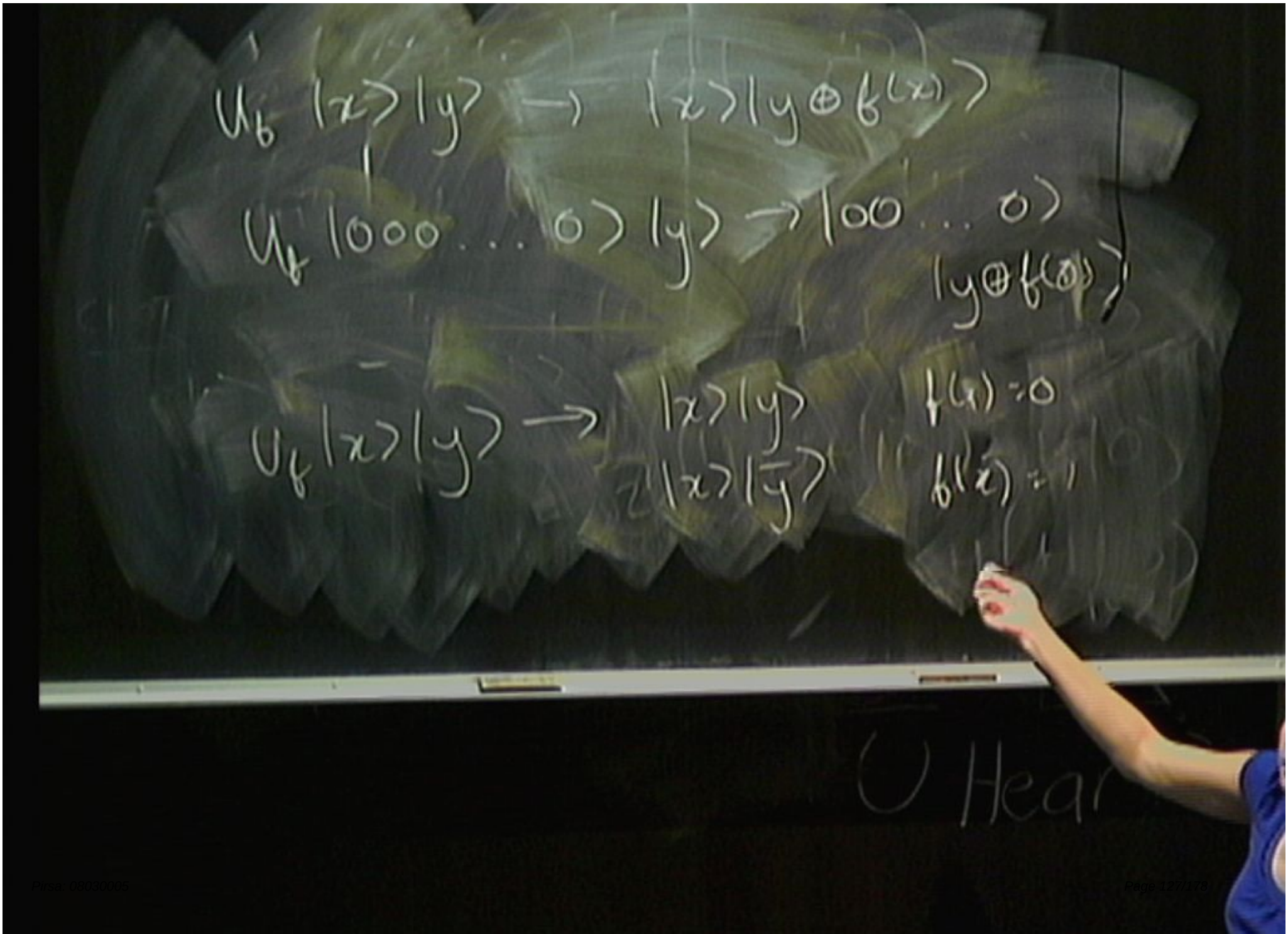

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0$

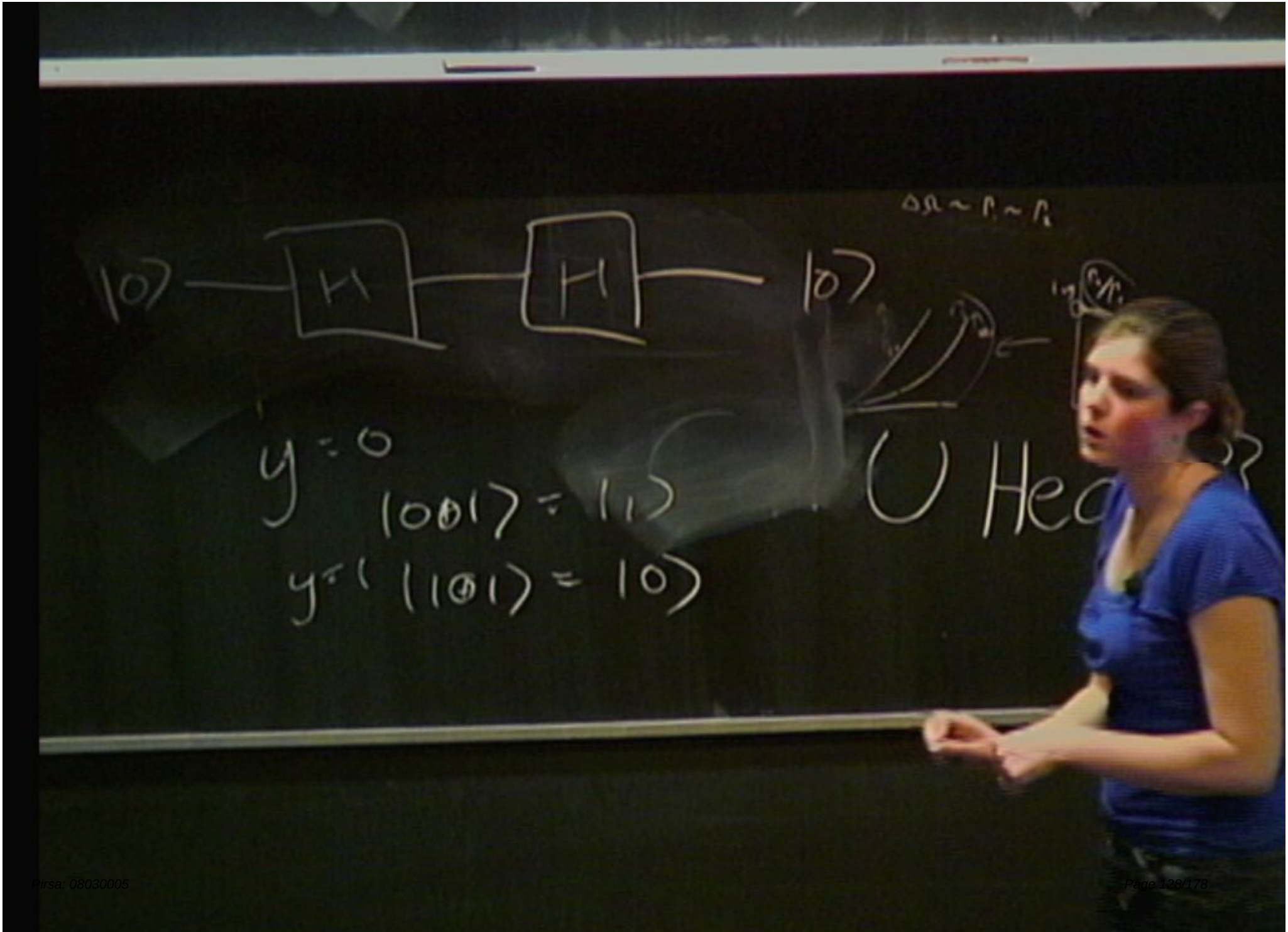

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0\rangle |y \oplus f(x)\rangle$

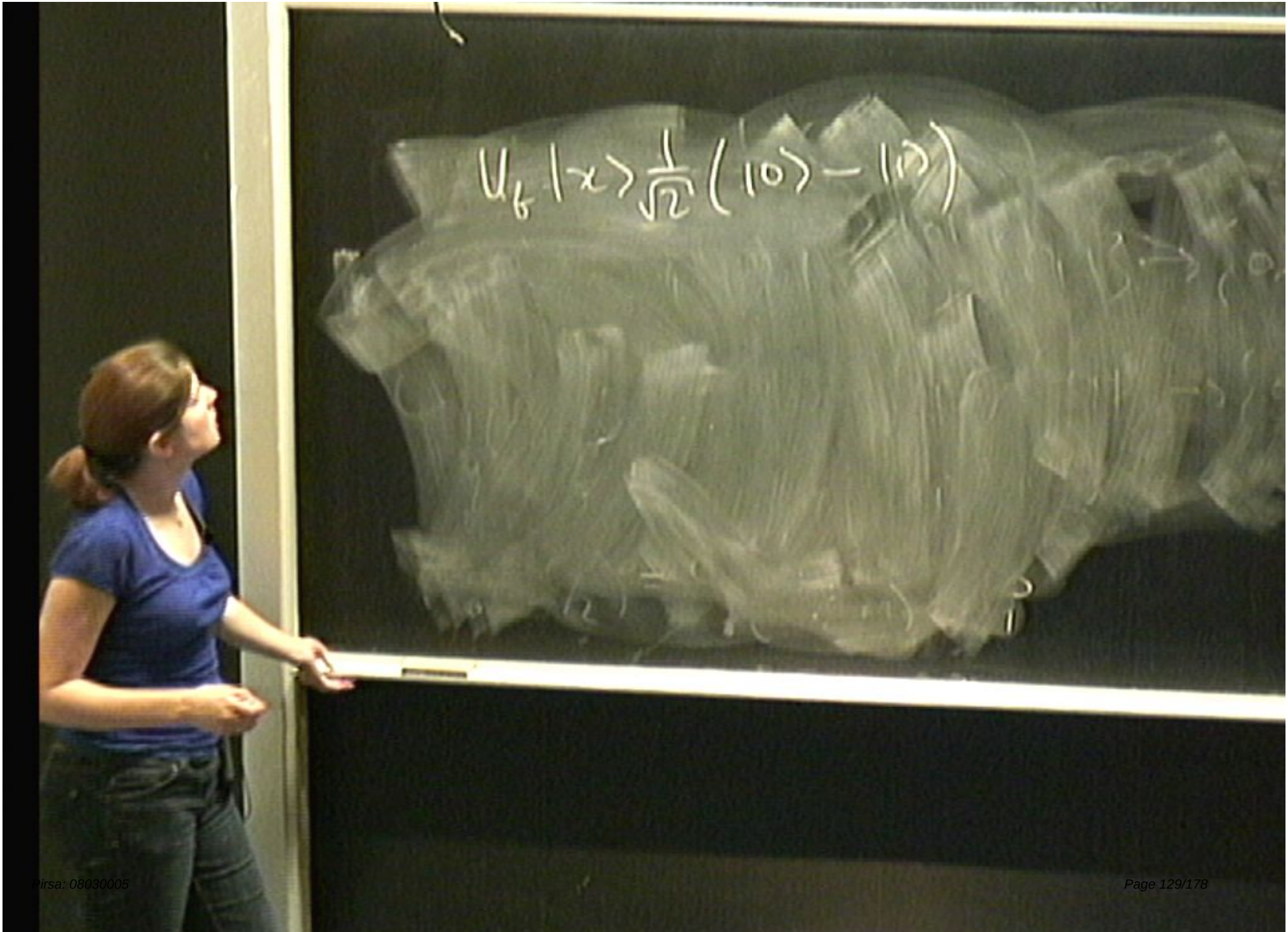

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0\rangle$
$|y \oplus f(0)\rangle$

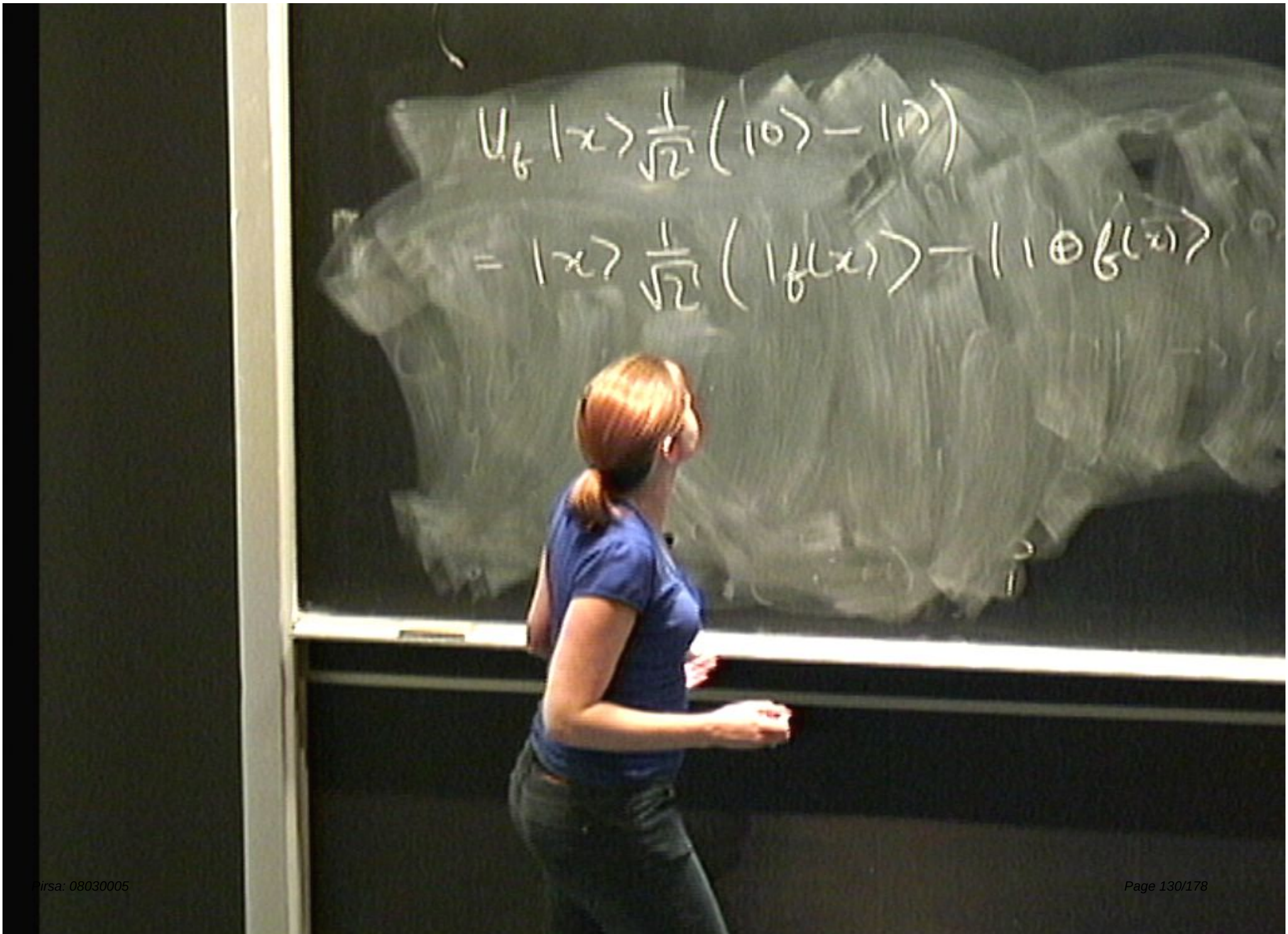

$U_b |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus b(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0\rangle$
$|y \oplus f(0)\rangle$
$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y\rangle$
$|x\rangle|\bar{y}\rangle$

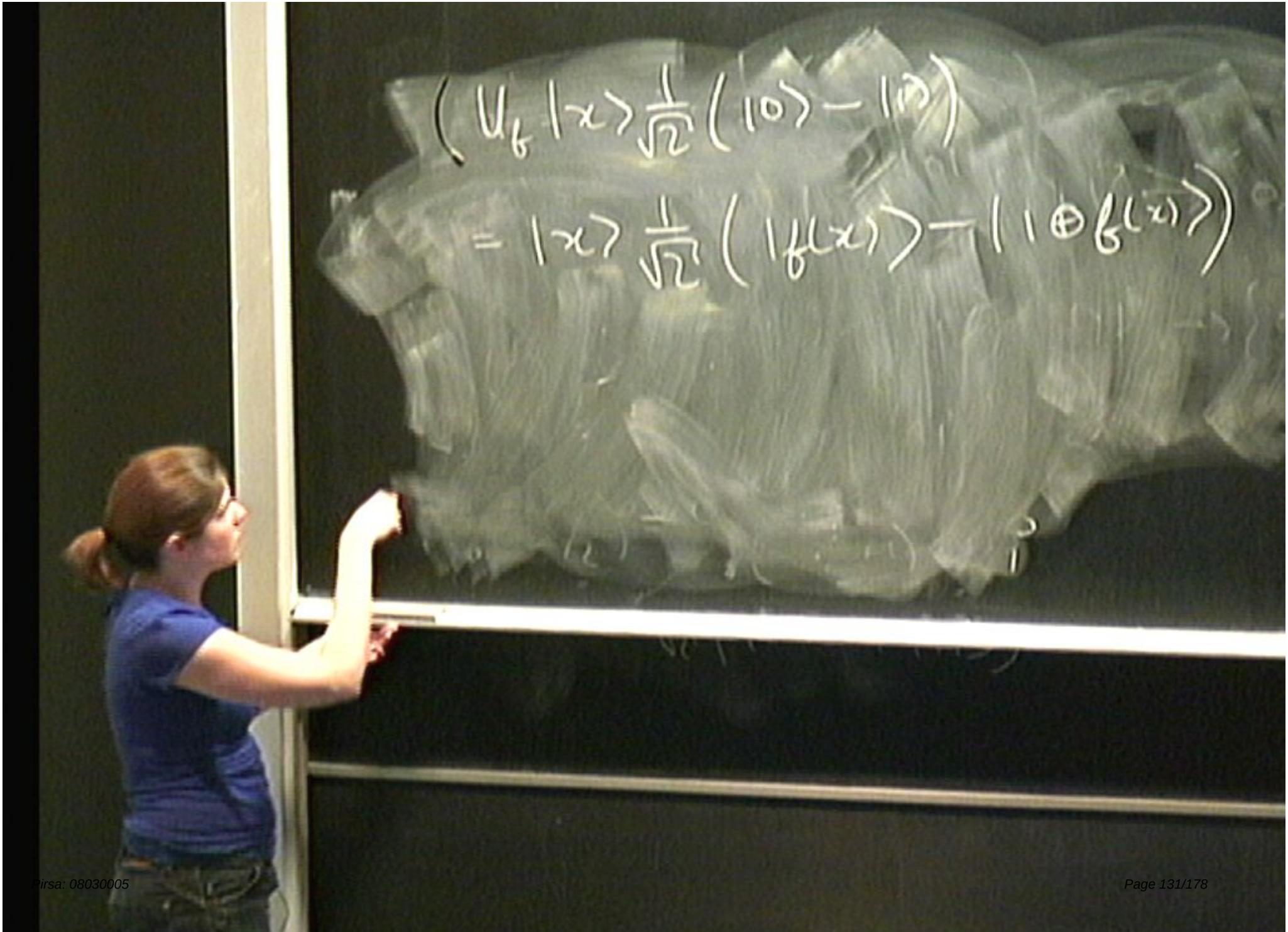

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0\rangle$
$|y \oplus f(0)\rangle$
$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y\rangle \quad f(x)=0$
$|x\rangle|\bar{y}\rangle \quad f(x)=1$

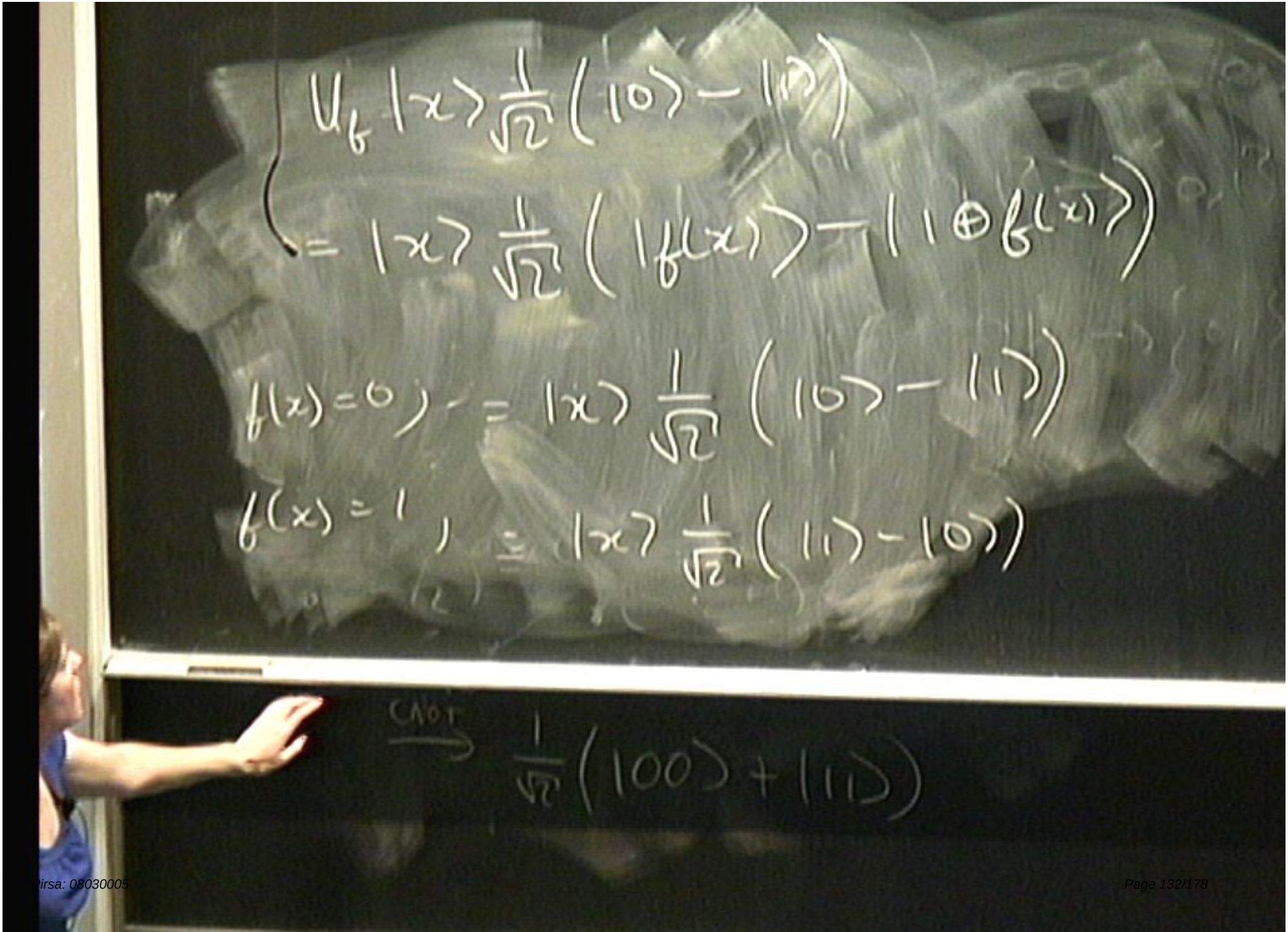

$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
$U_f |000\ldots0\rangle|y\rangle \rightarrow |00\ldots0\rangle |y \oplus f(0)\rangle$
$U_f |x\rangle|y\rangle \rightarrow |x\rangle|y\rangle \quad f(x)=0$
$|x\rangle|\bar{y}\rangle \quad f(x)=1$


|0⟩
H
H
|0⟩
y=0
|001⟩ = |1⟩
y=1 |101⟩ = |0⟩


$U_6|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$


$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$=|x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle$


$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$=|x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle)$


$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$=|x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle)$
$f(x)=0$ $=|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$f(x)=1$ $=|x\rangle\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle)$
CNOT
$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$

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

$$= |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

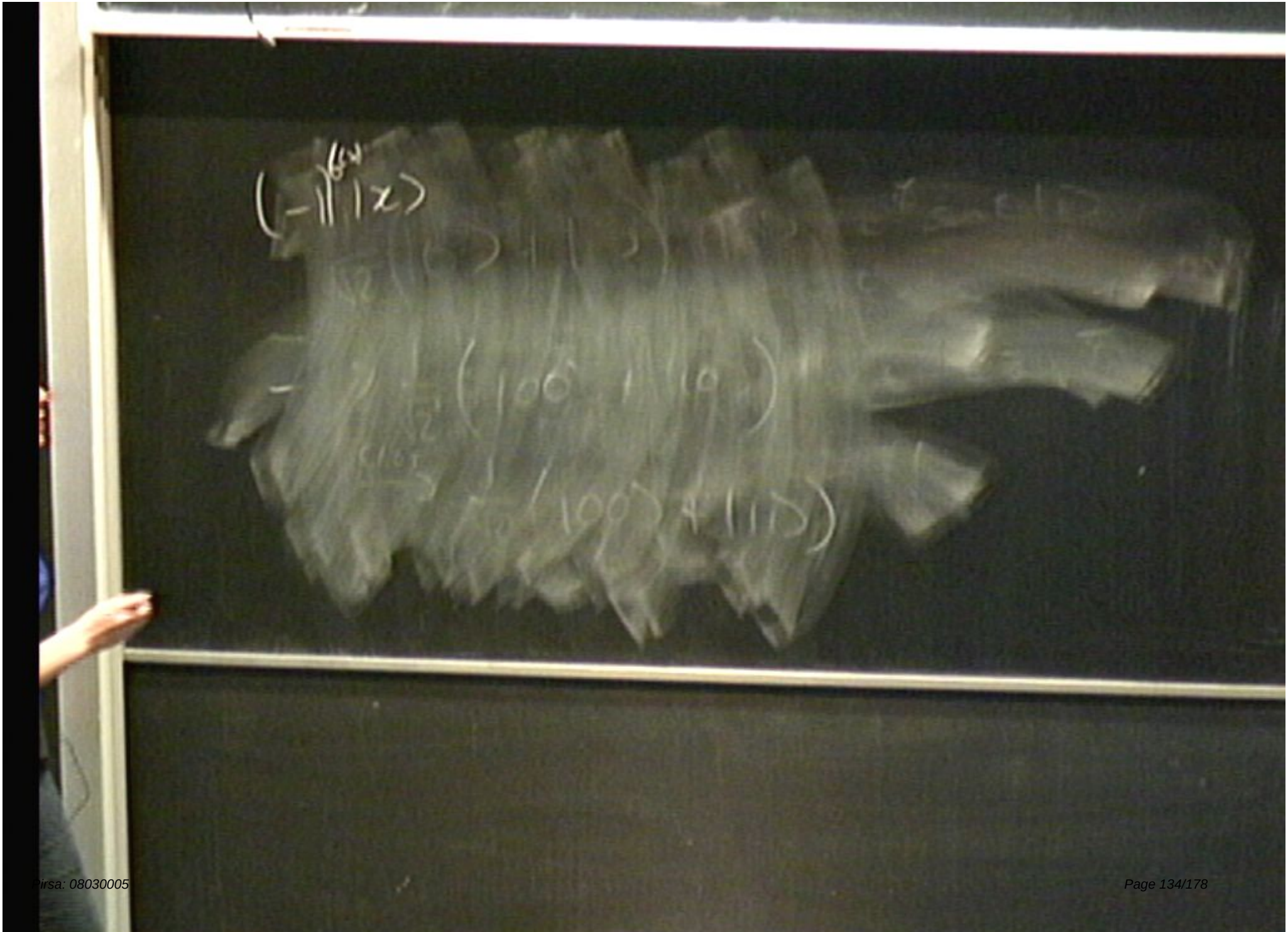
$$f(x)=0) = |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

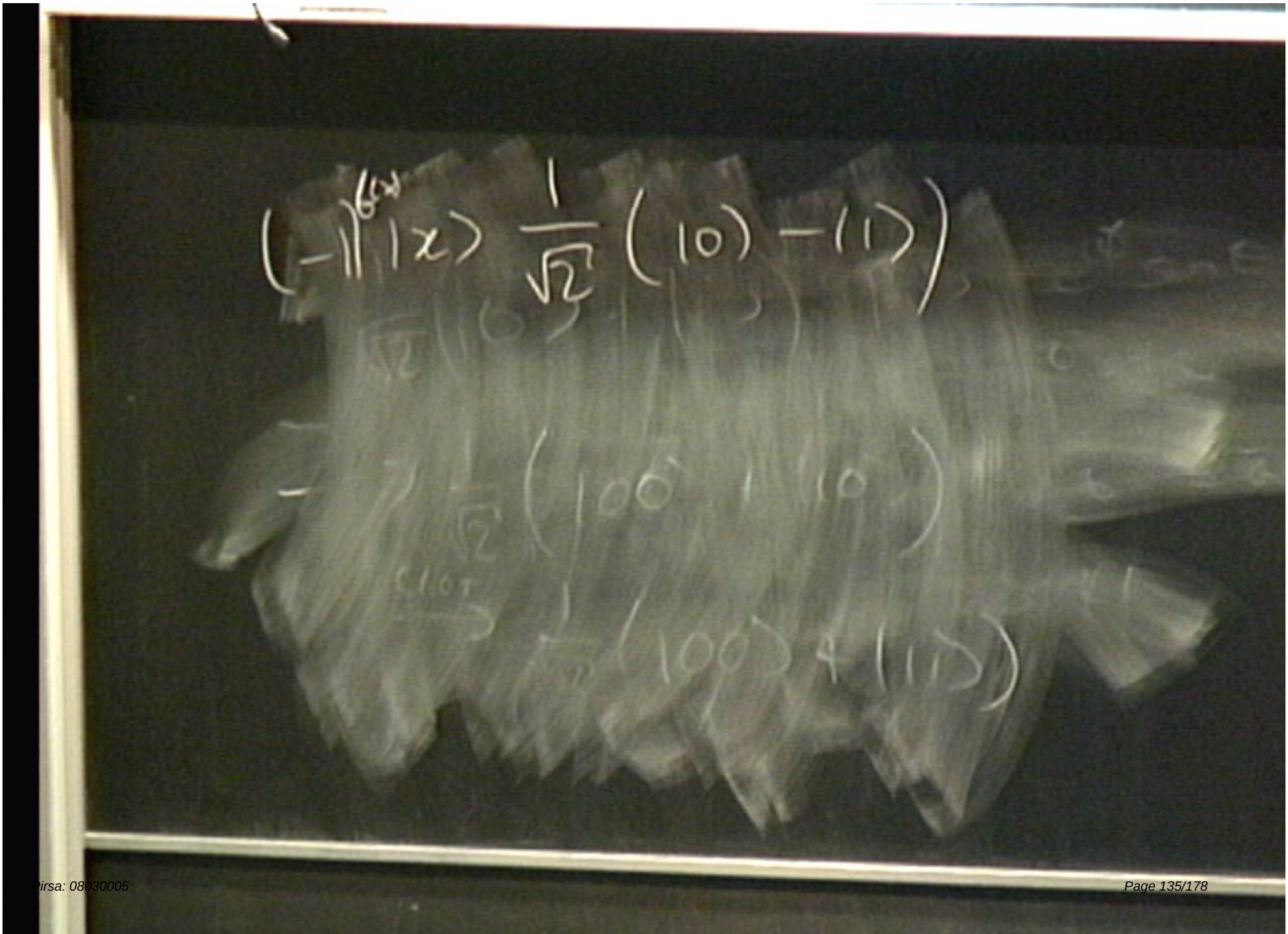
$$f(x)=1) = |x\rangle \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$$

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

$$\rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

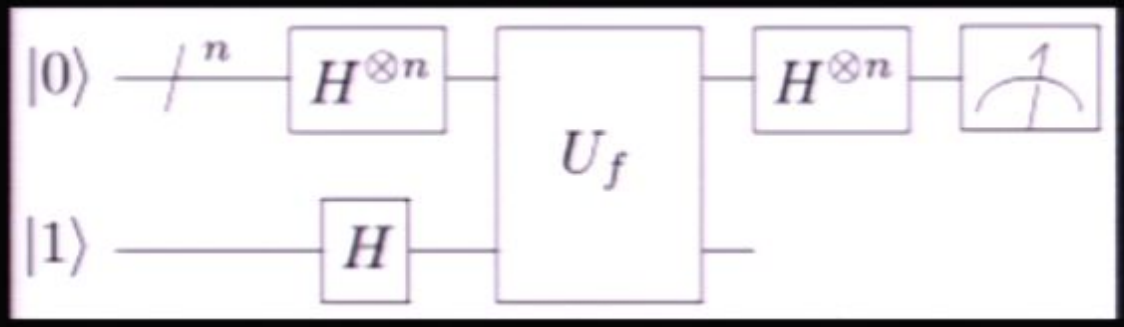
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



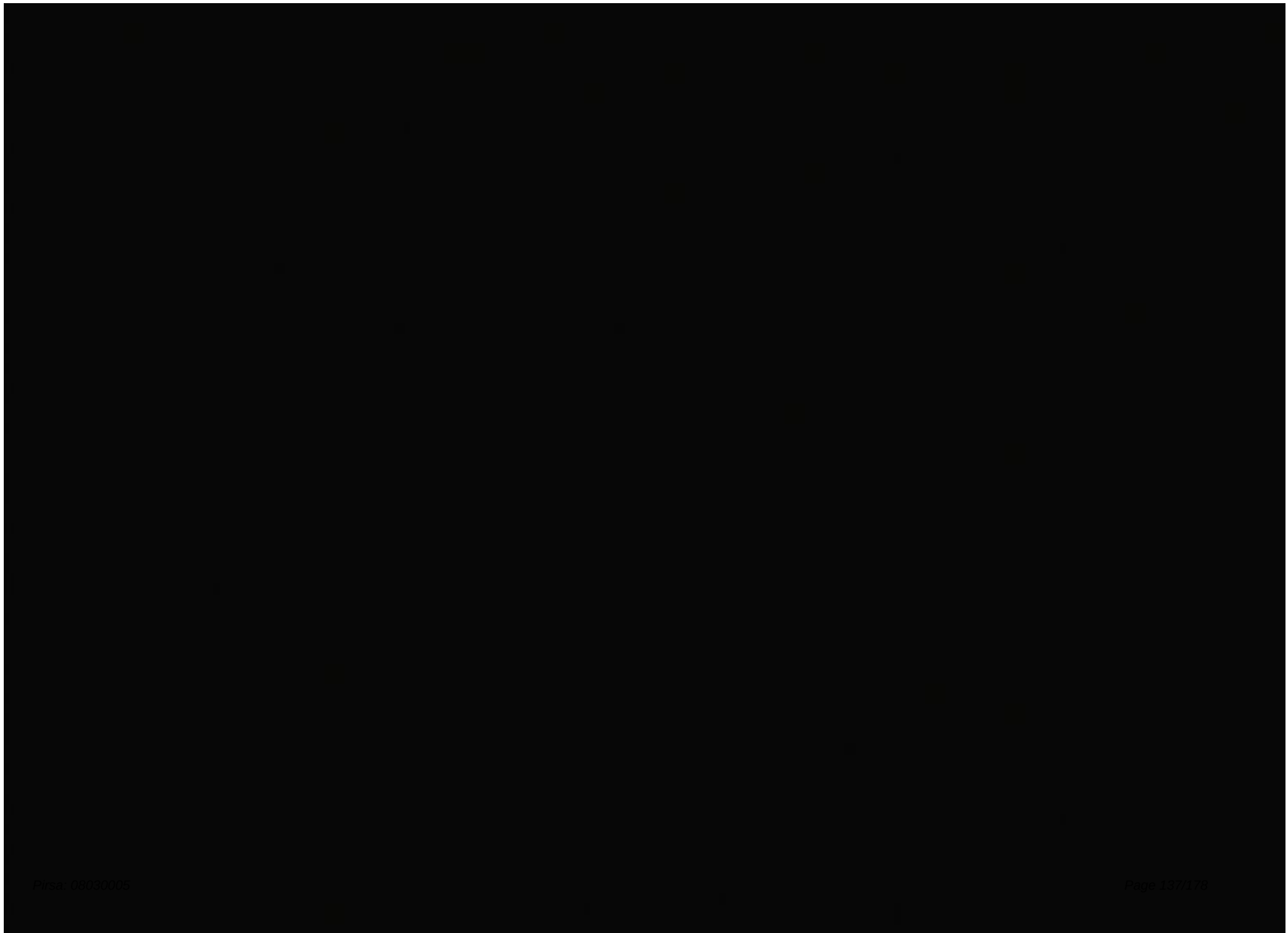

$(-1)^{G(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$

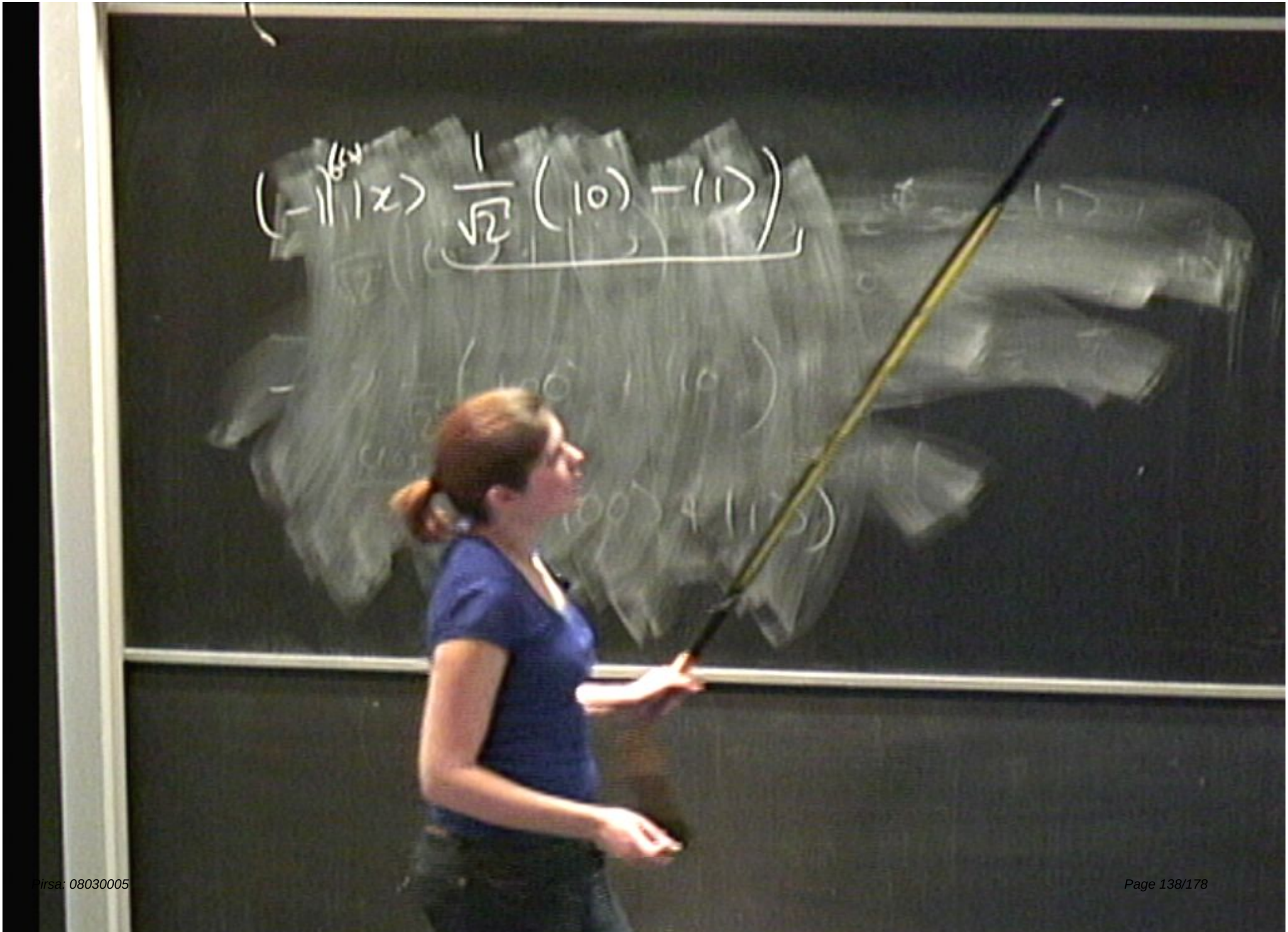
Deutsch-Josza Algorithm

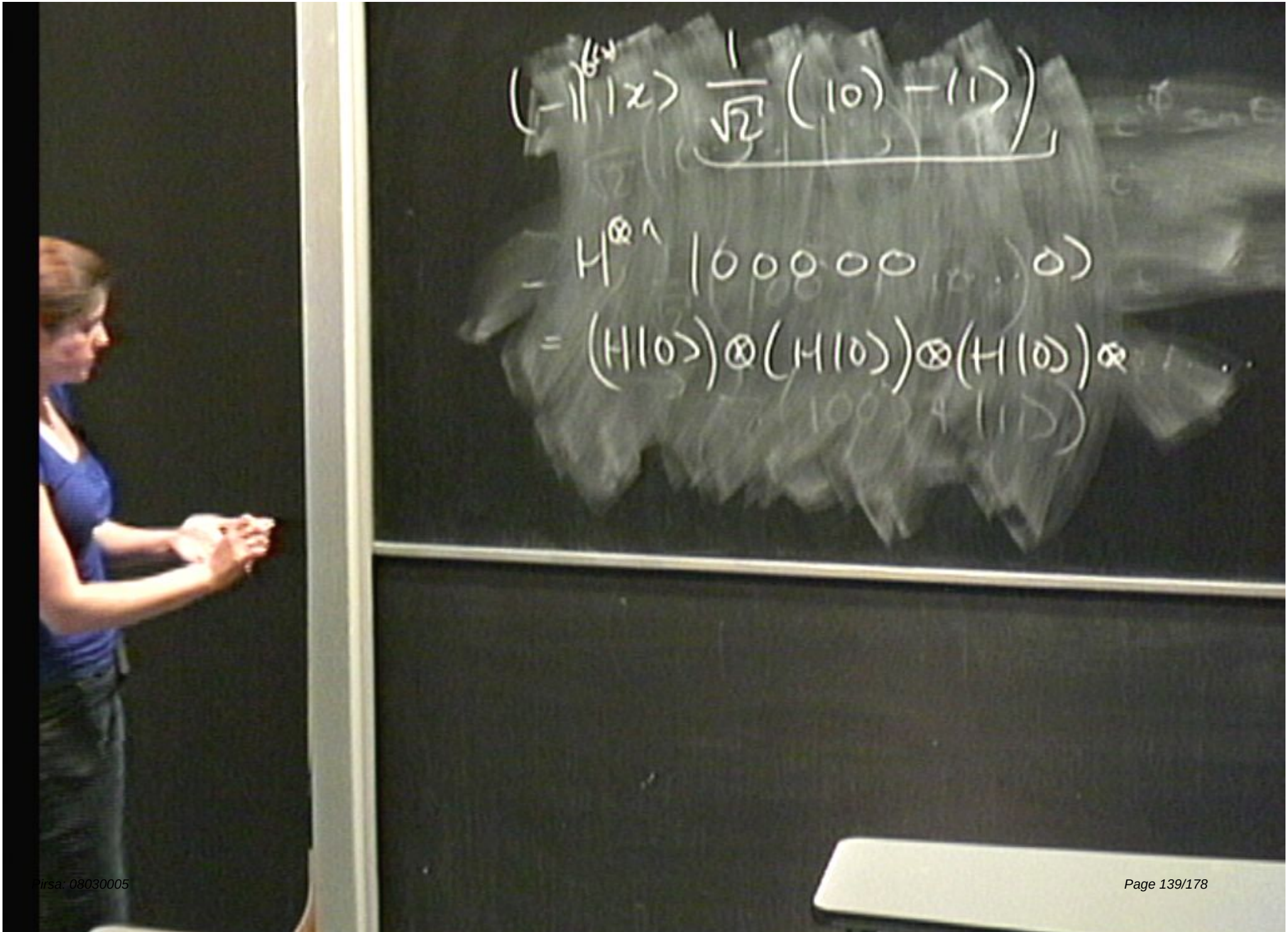
- Extension of Deutsch algorithm
- Quantum circuit diagram

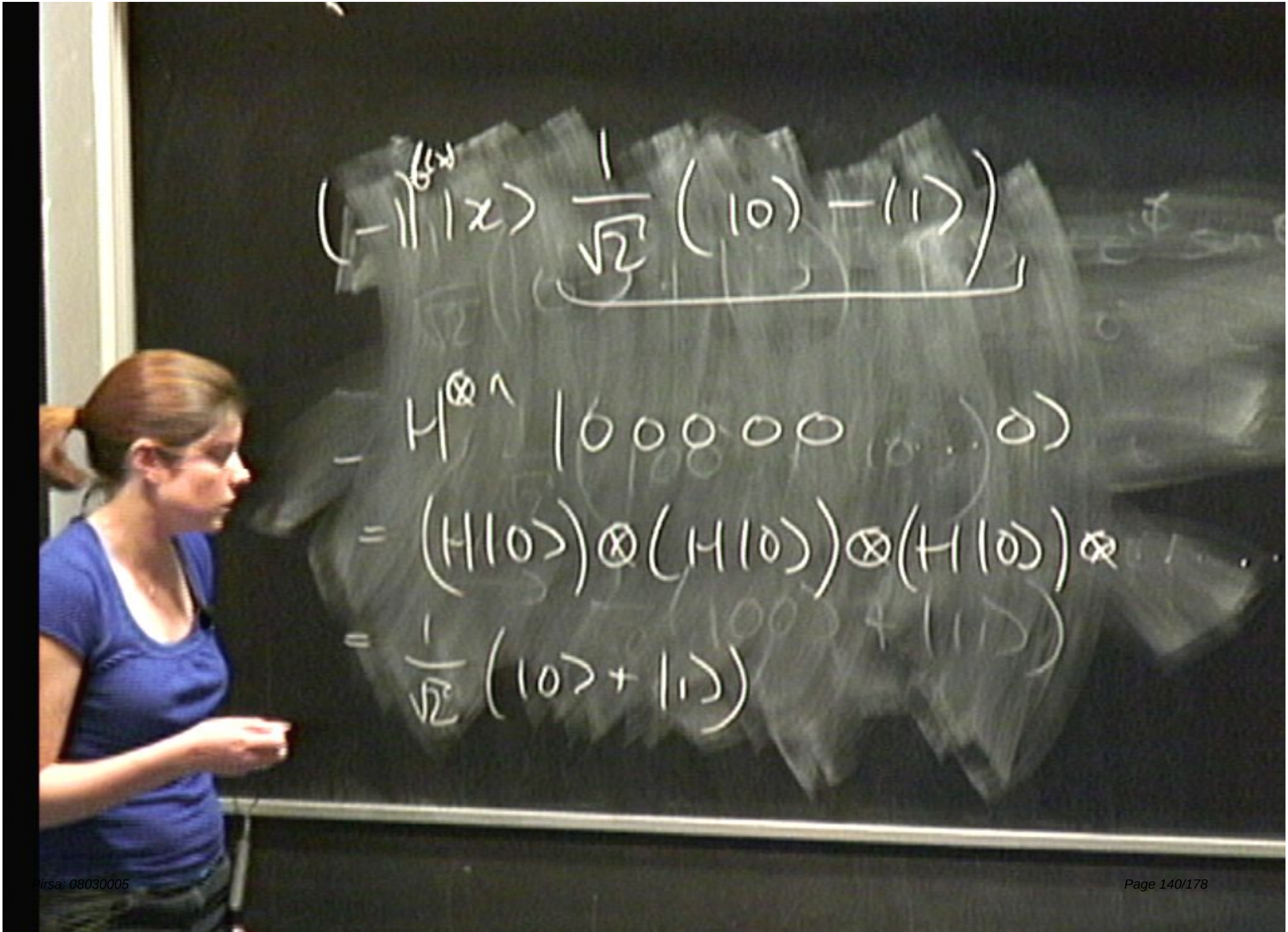


- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.




$(-1)^{\delta w} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$


$(-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$H^{\otimes n}|000\ldots0\rangle$
$= (H|0\rangle) \otimes (H|0\rangle) \otimes (H|0\rangle) \otimes \ldots$

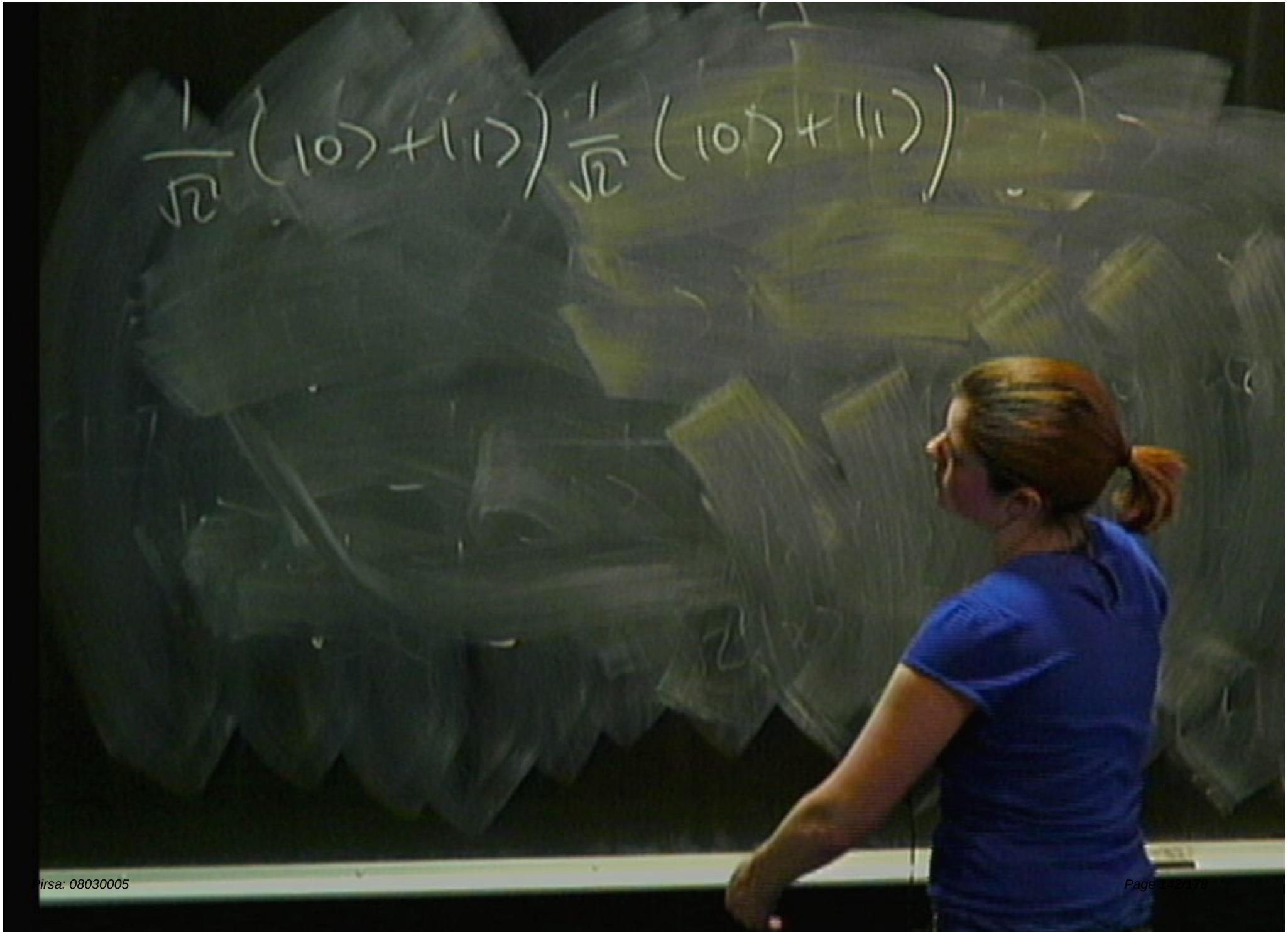

$(-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$H^{\otimes n} |000\ldots0\rangle$
$= (H|0\rangle) \otimes (H|0\rangle) \otimes (H|0\rangle) \otimes \ldots$
$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

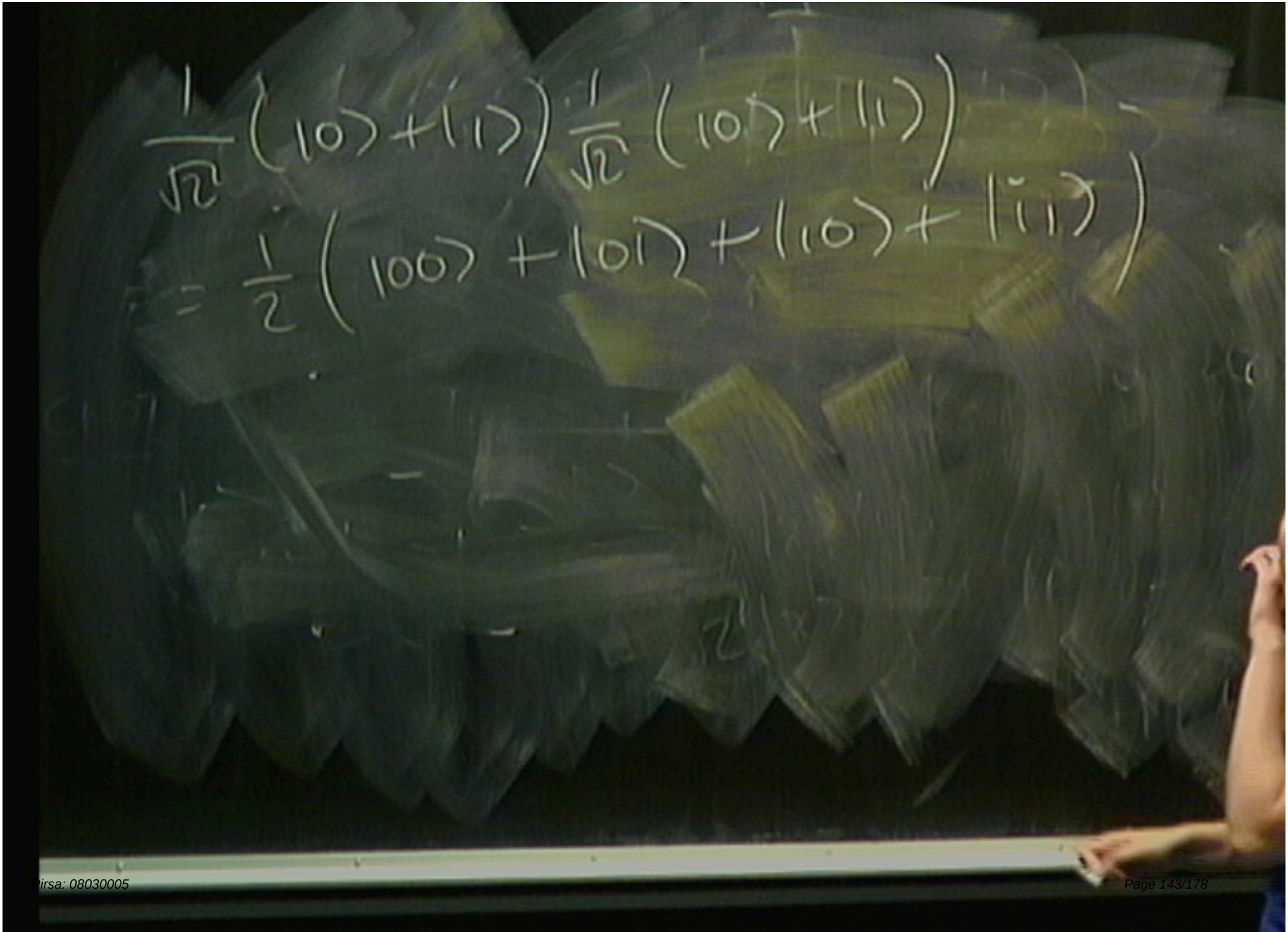
$$(-1)^{f(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

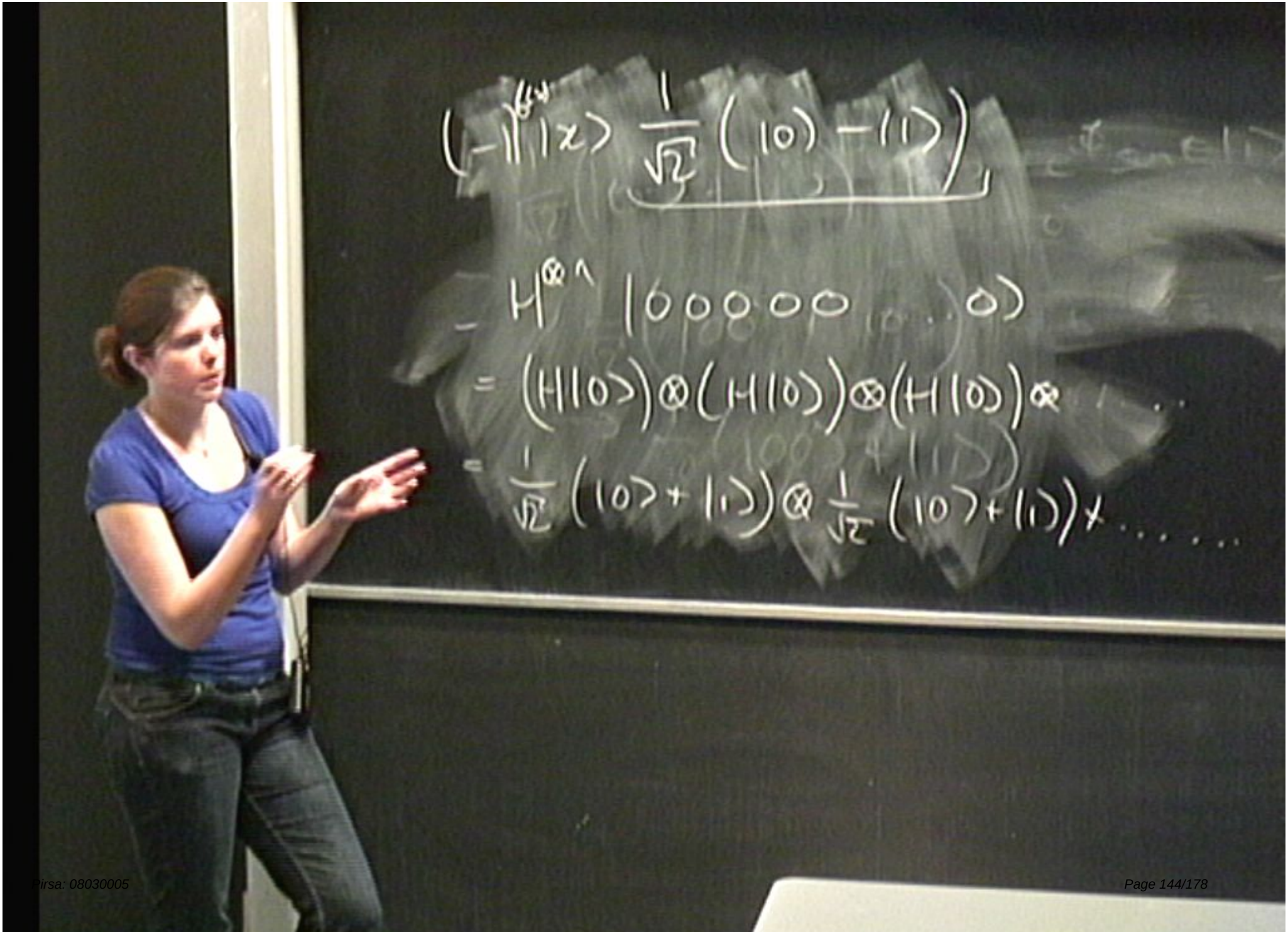
$$= H^{\otimes n}|000000\ldots0\rangle$$

$$= (H|0\rangle)\otimes(H|0\rangle)\otimes(H|0\rangle)\otimes\ldots$$

$$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\ldots\ldots$$


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


$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$


$(-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$H^{\otimes n}|000\ldots0\rangle$
$= (H|0\rangle)\otimes(H|0\rangle)\otimes(H|0\rangle)\otimes\ldots$
$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\ldots$

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

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

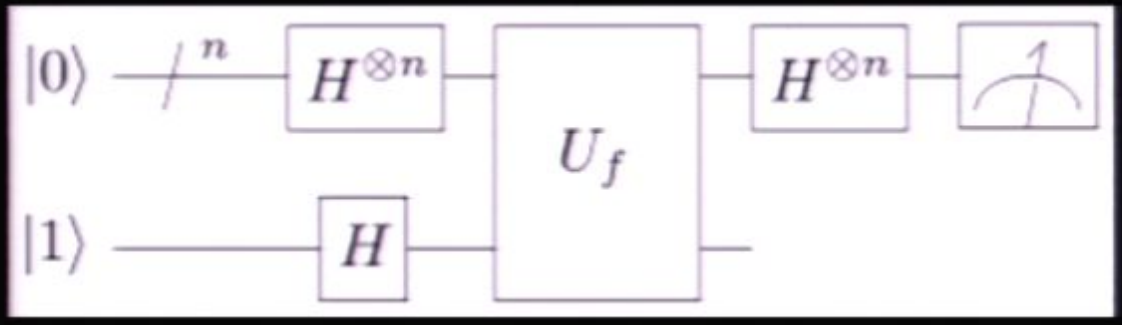
$$H^{\otimes n}|0\dots 0\rangle$$

$$=\frac{1}{\sqrt{2^n}}\left(\sum_{x\in\{0,1\}^n}|x\rangle\right)$$

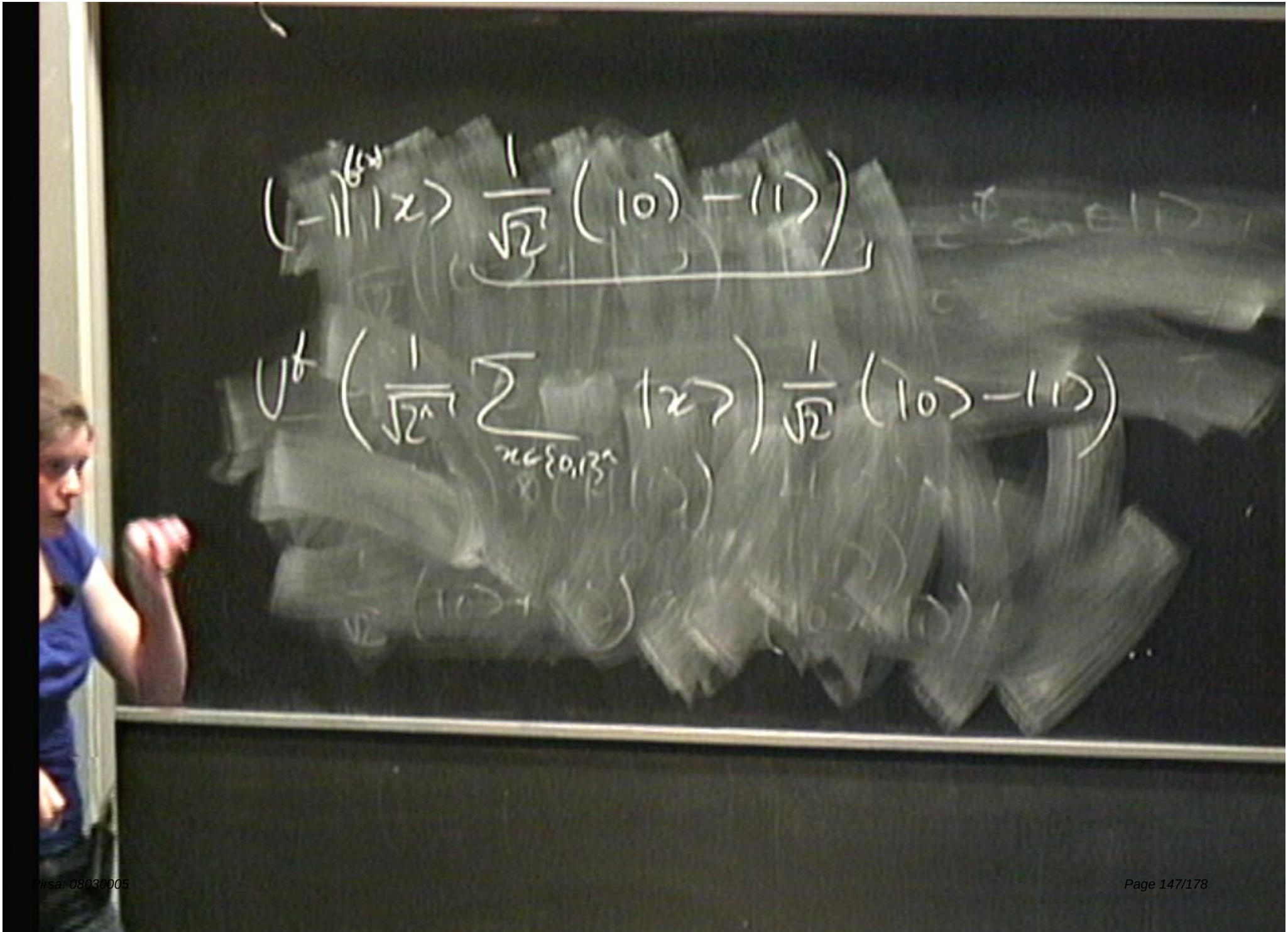
Pirsa: 08030005

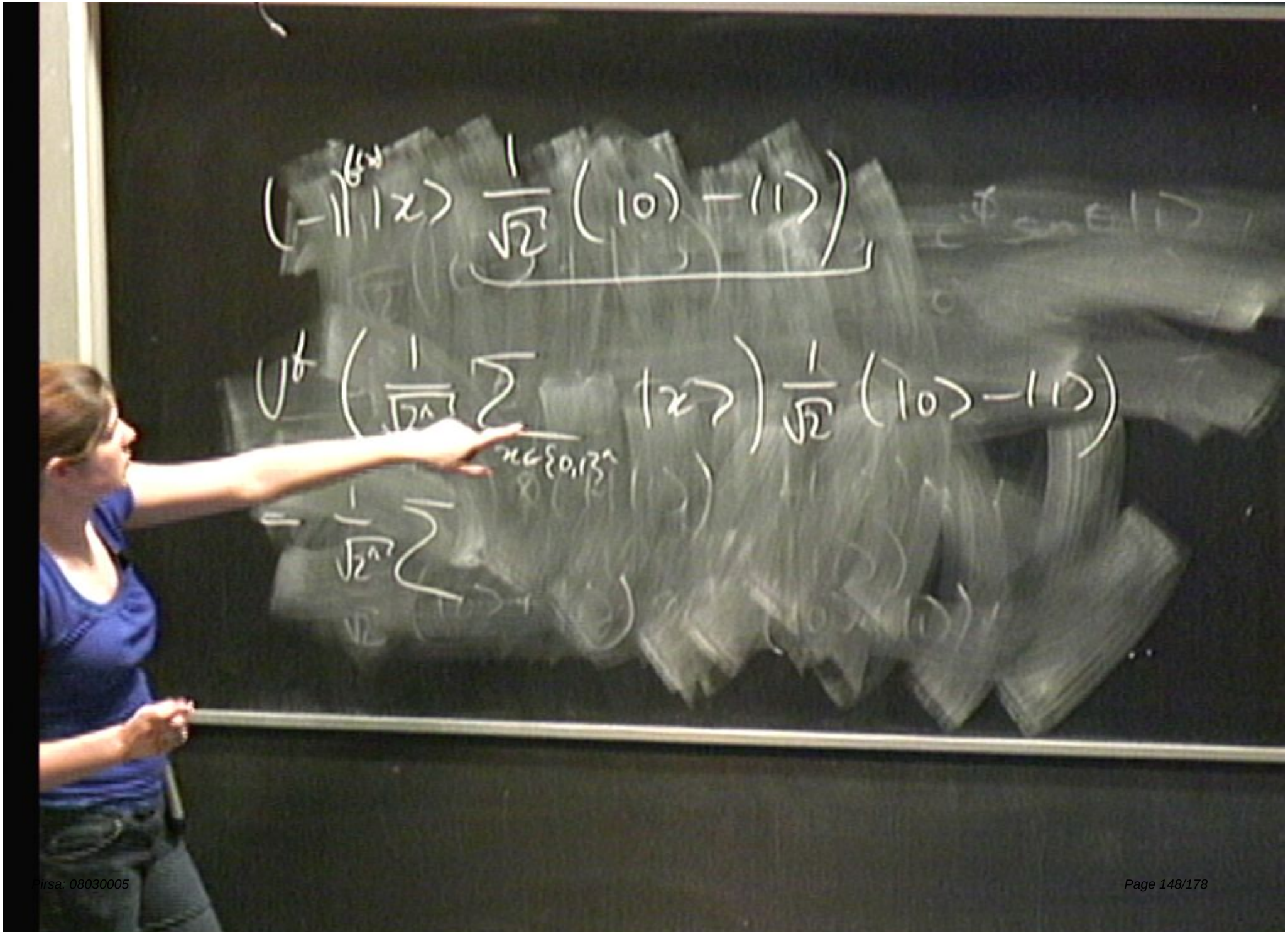
Deutsch-Josza Algorithm

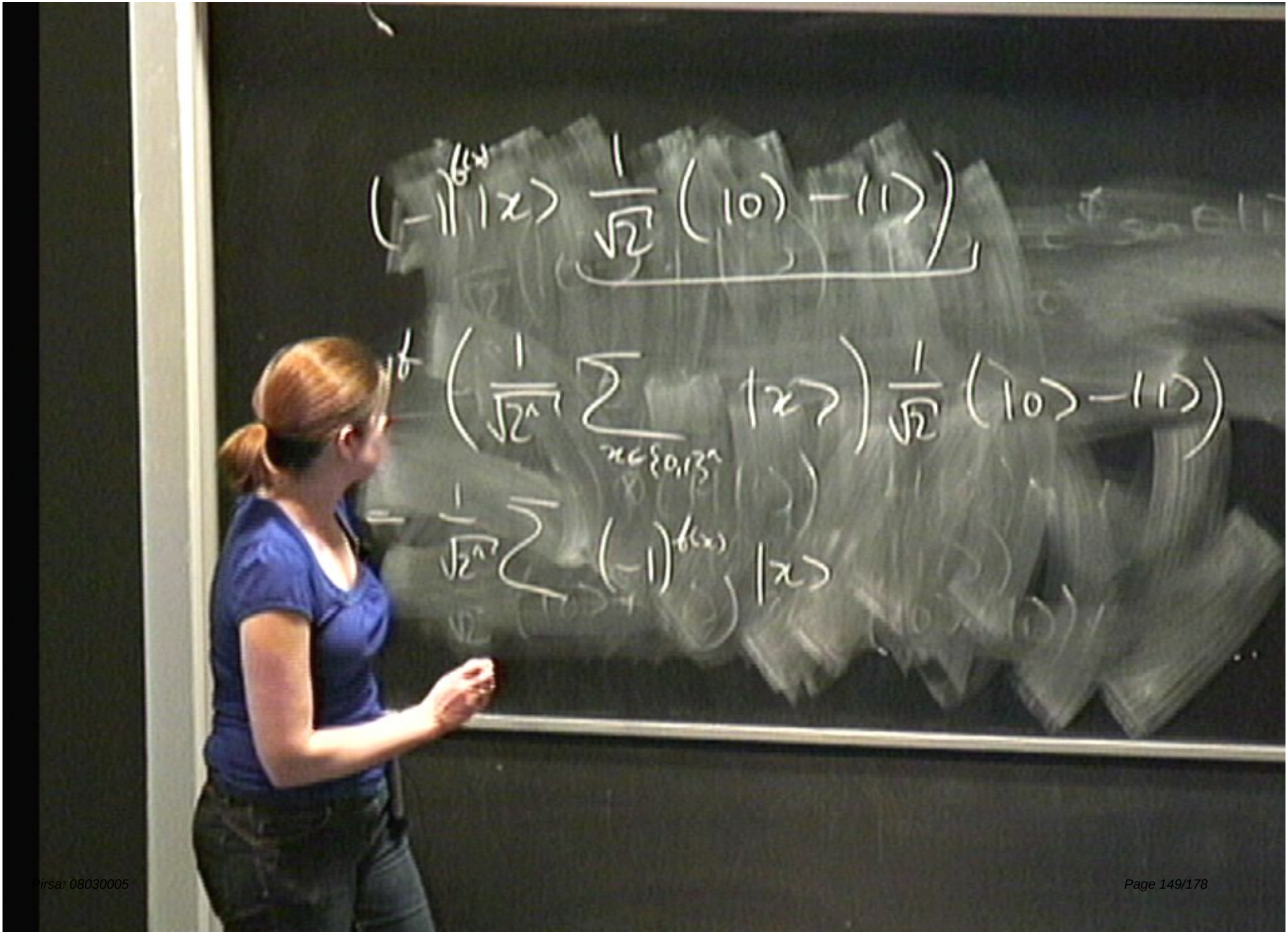
- Extension of Deutsch algorithm
- Quantum circuit diagram

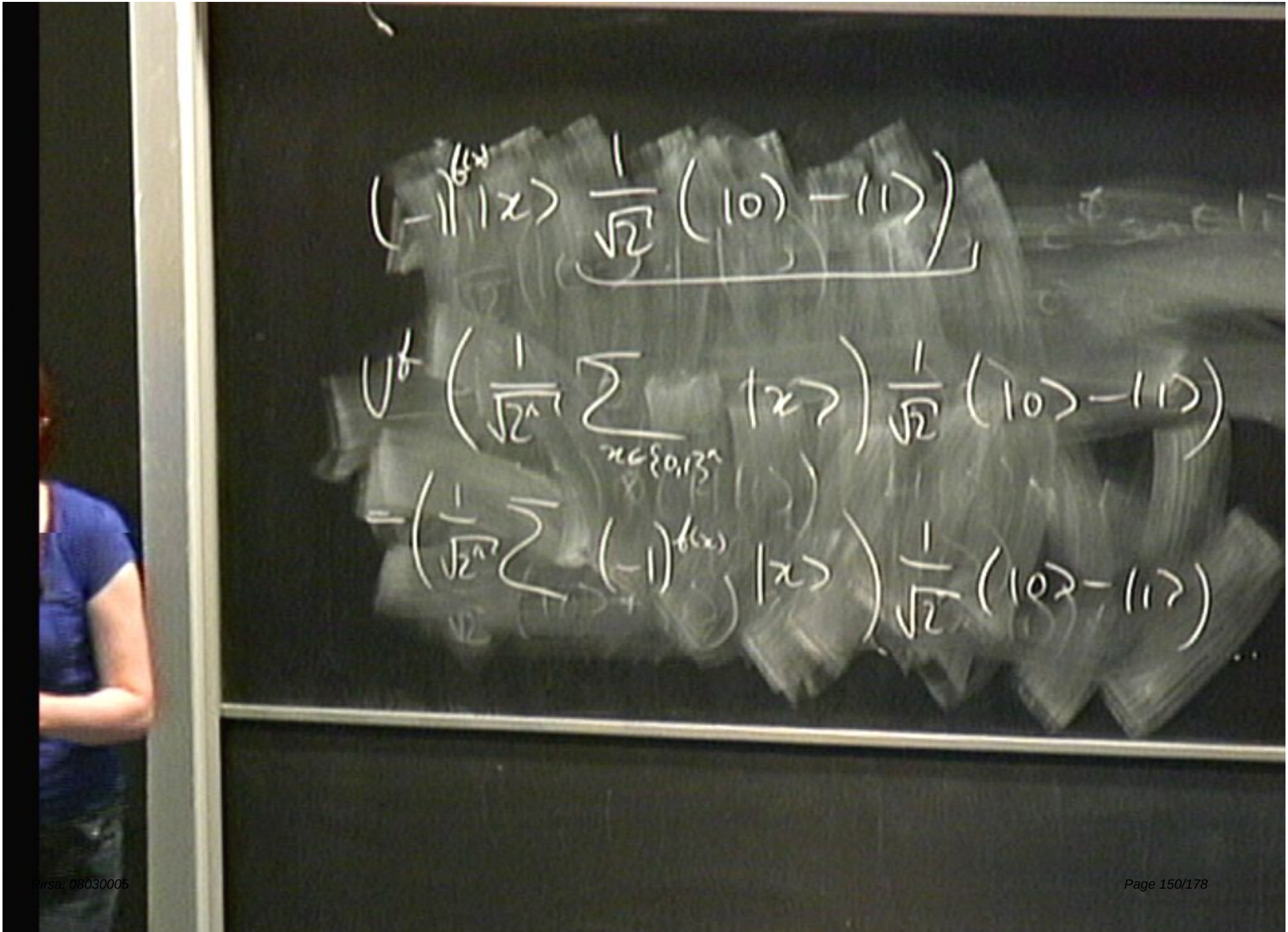


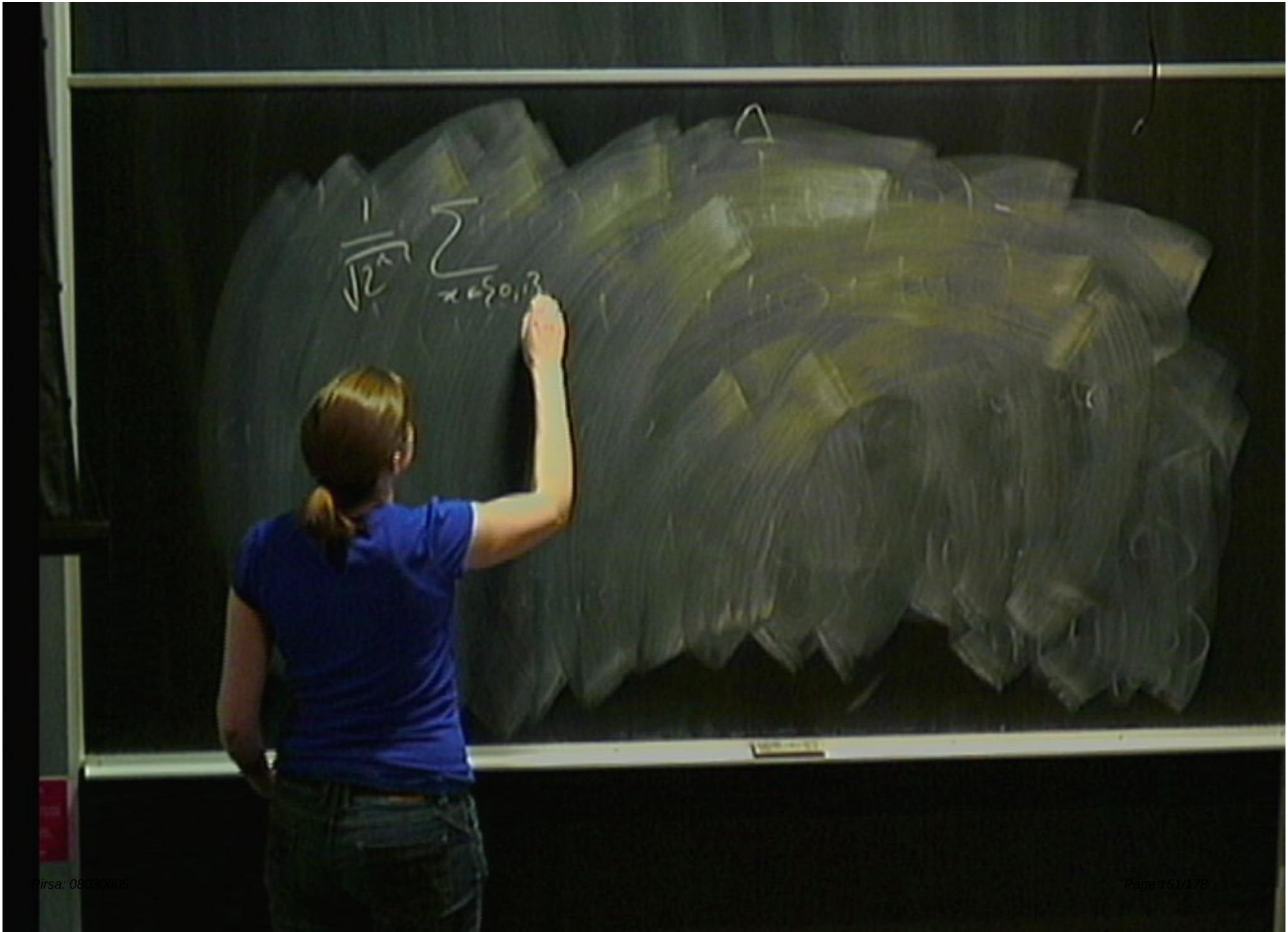
- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.

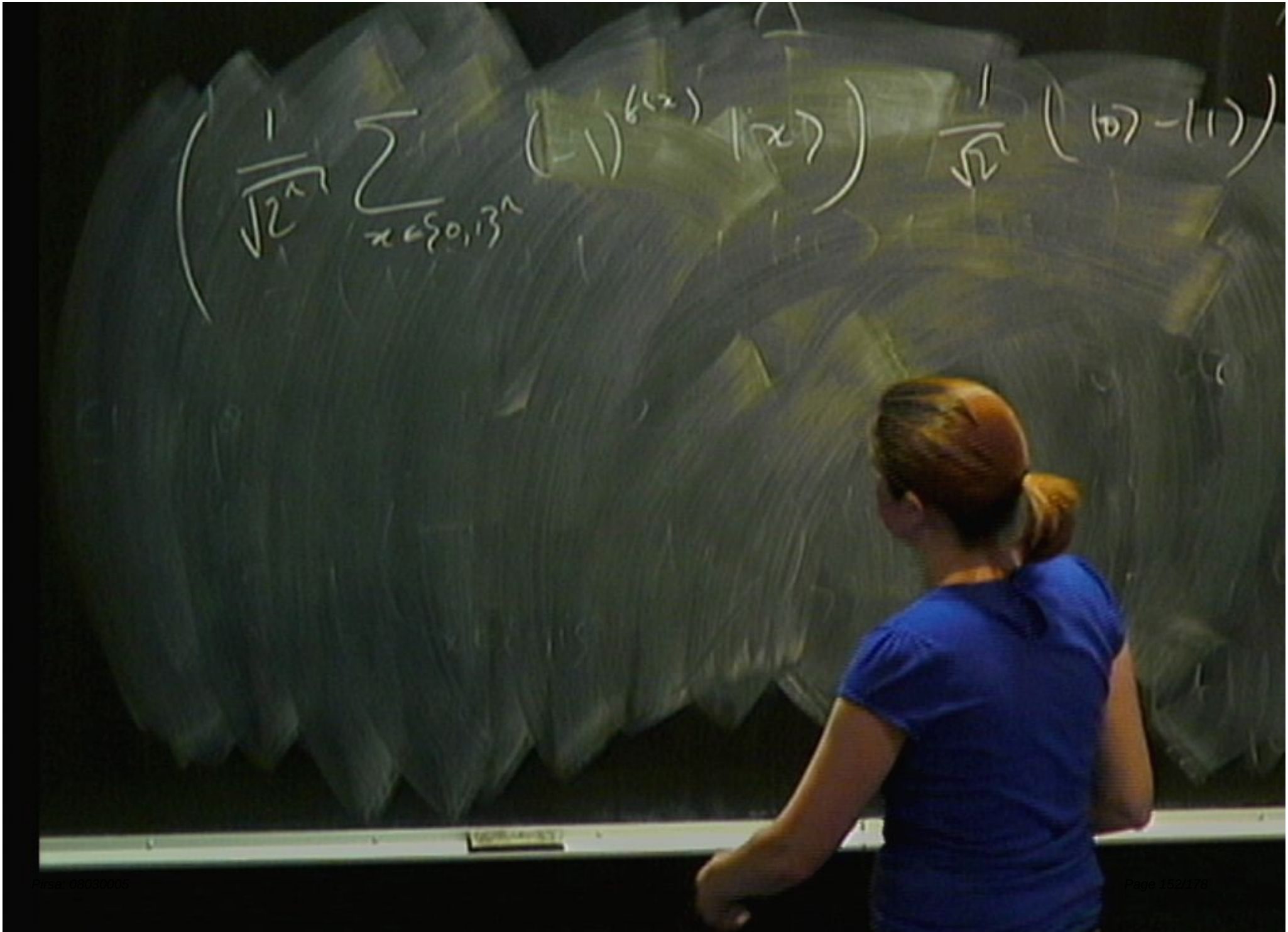

$(-1)^{f(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

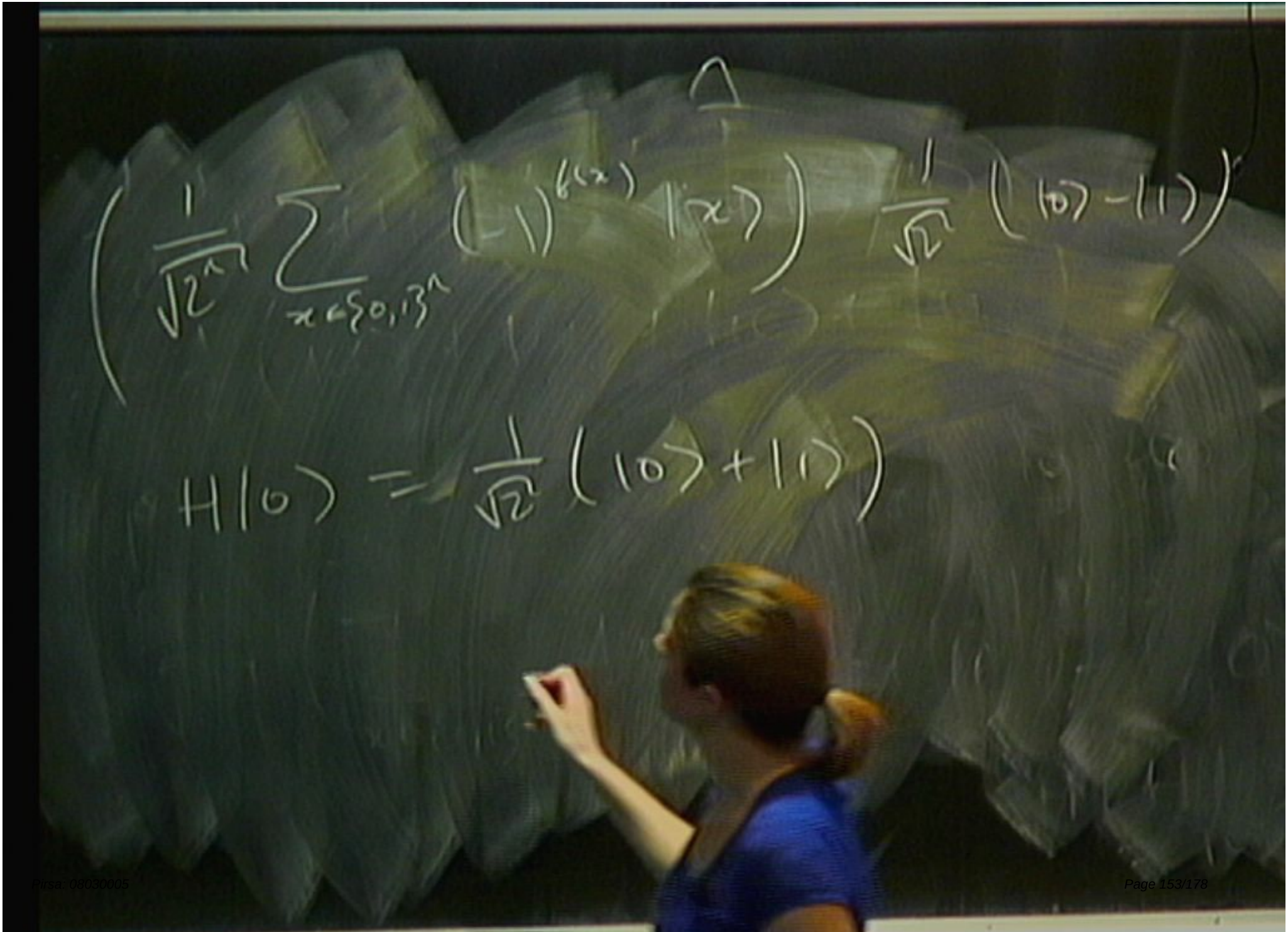

$(-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$= \frac{1}{\sqrt{2^n}} \sum$

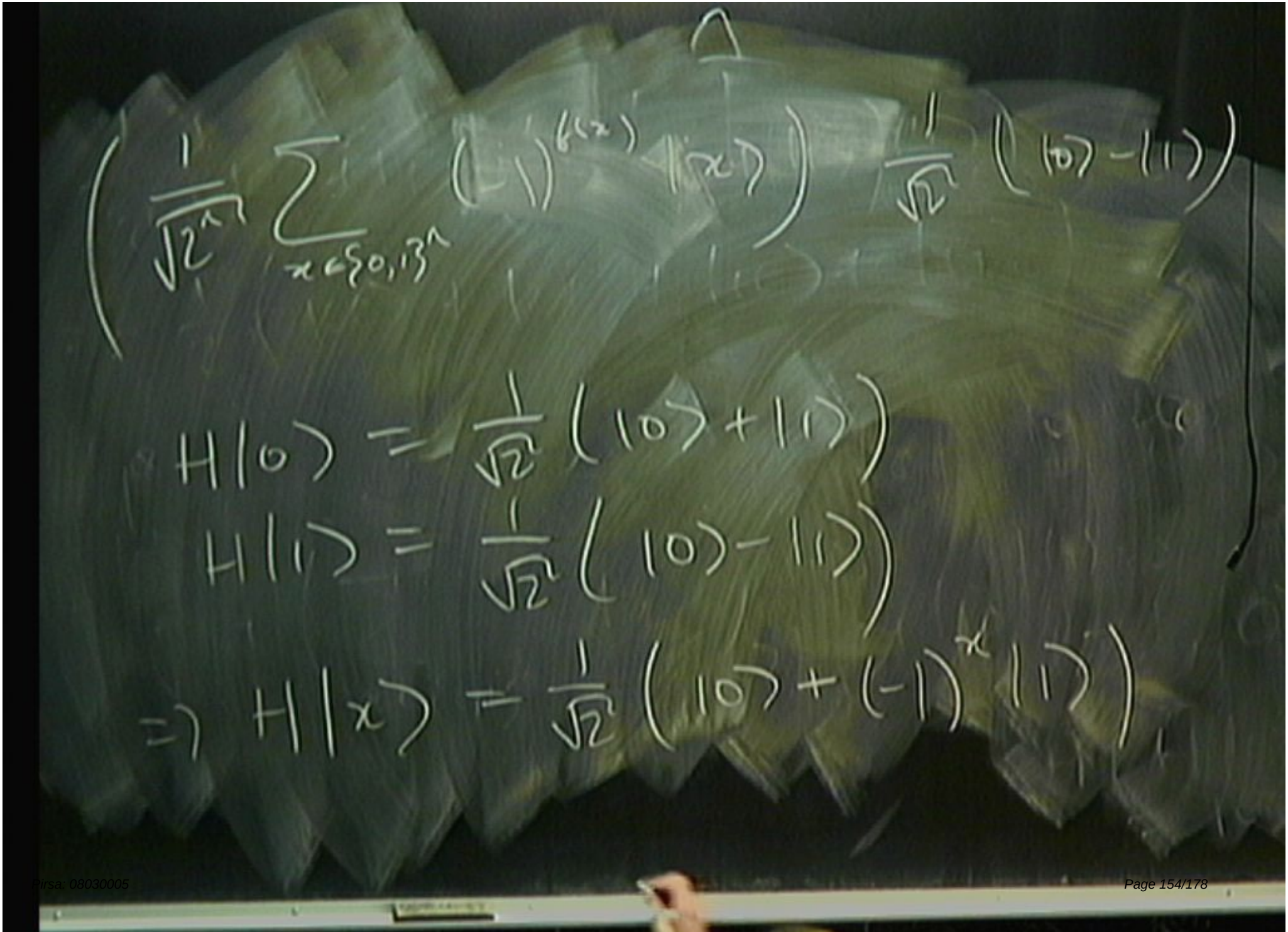

$(-1)^{f(x)}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$= \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle$


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




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


$\left(\frac{1}{\sqrt{2}^n}\sum_{x\in\{0,1\}^n}(-1)^{\delta(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$


$\left(\frac{1}{\sqrt{2}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$
$H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$\Rightarrow H|x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+(-1)^x|1\rangle)$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

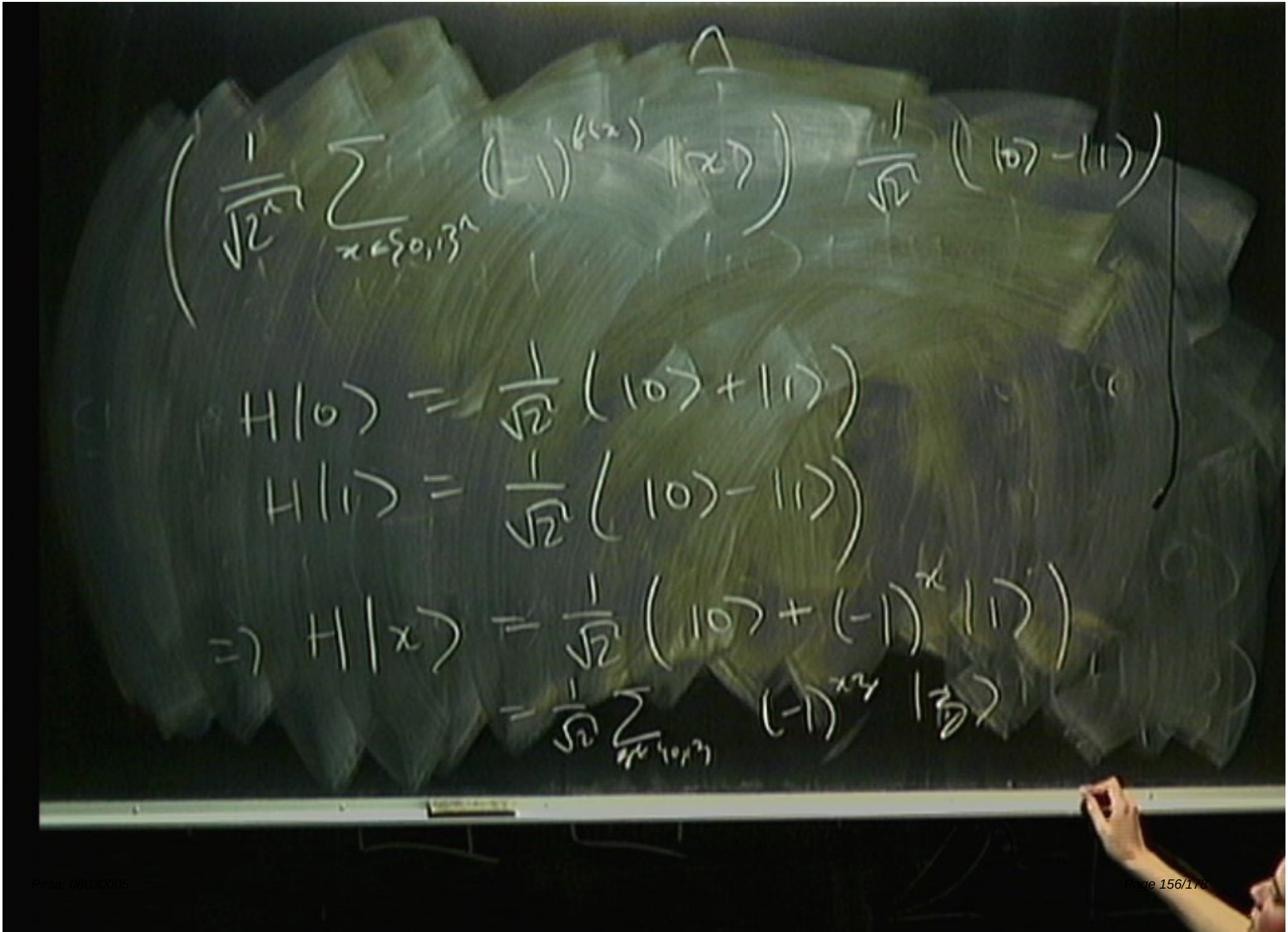
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\Rightarrow H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

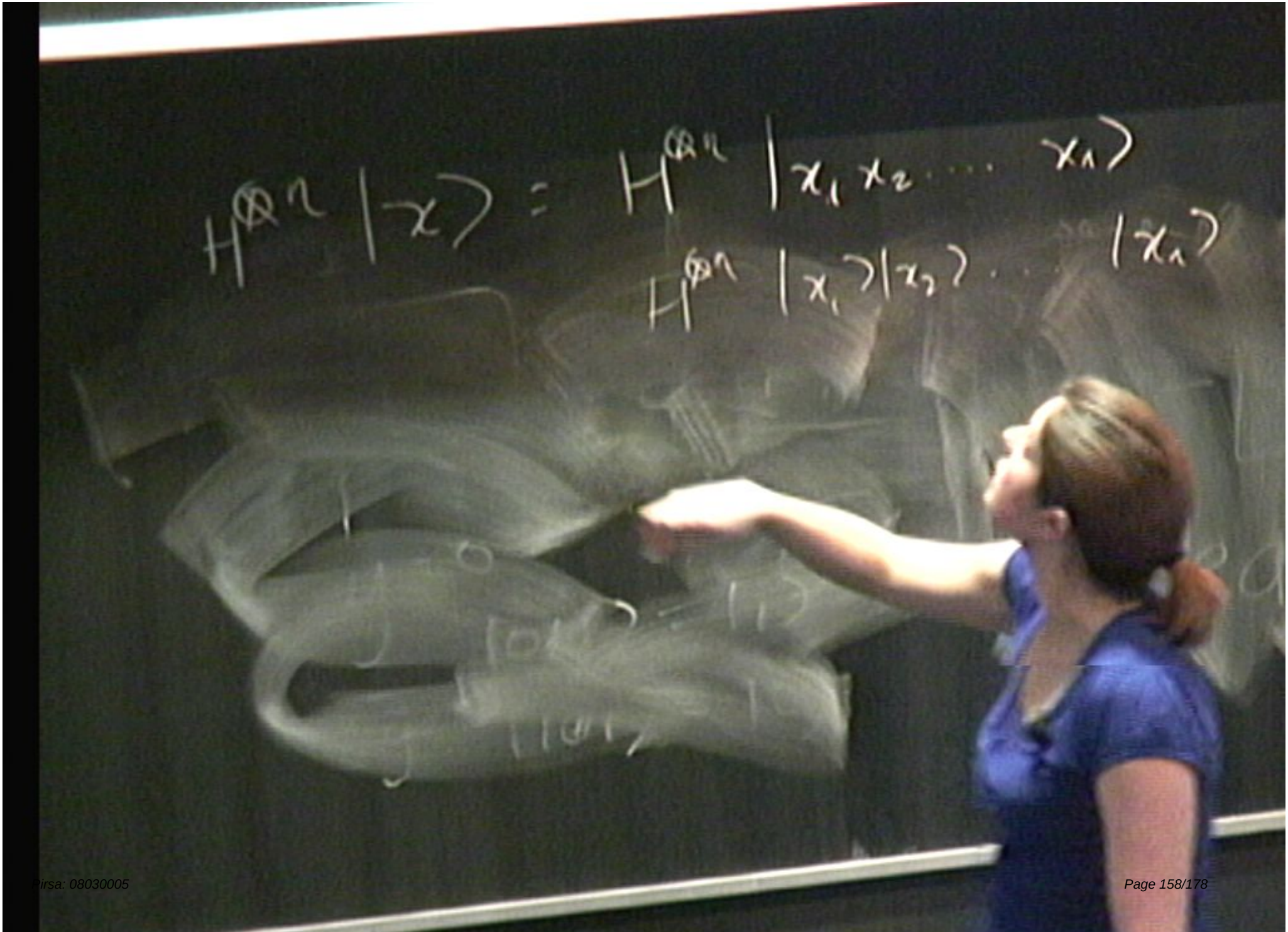
$$= \frac{1}{\sqrt{2}} \sum_{y=0,1} (-1)^{xy} |y\rangle$$

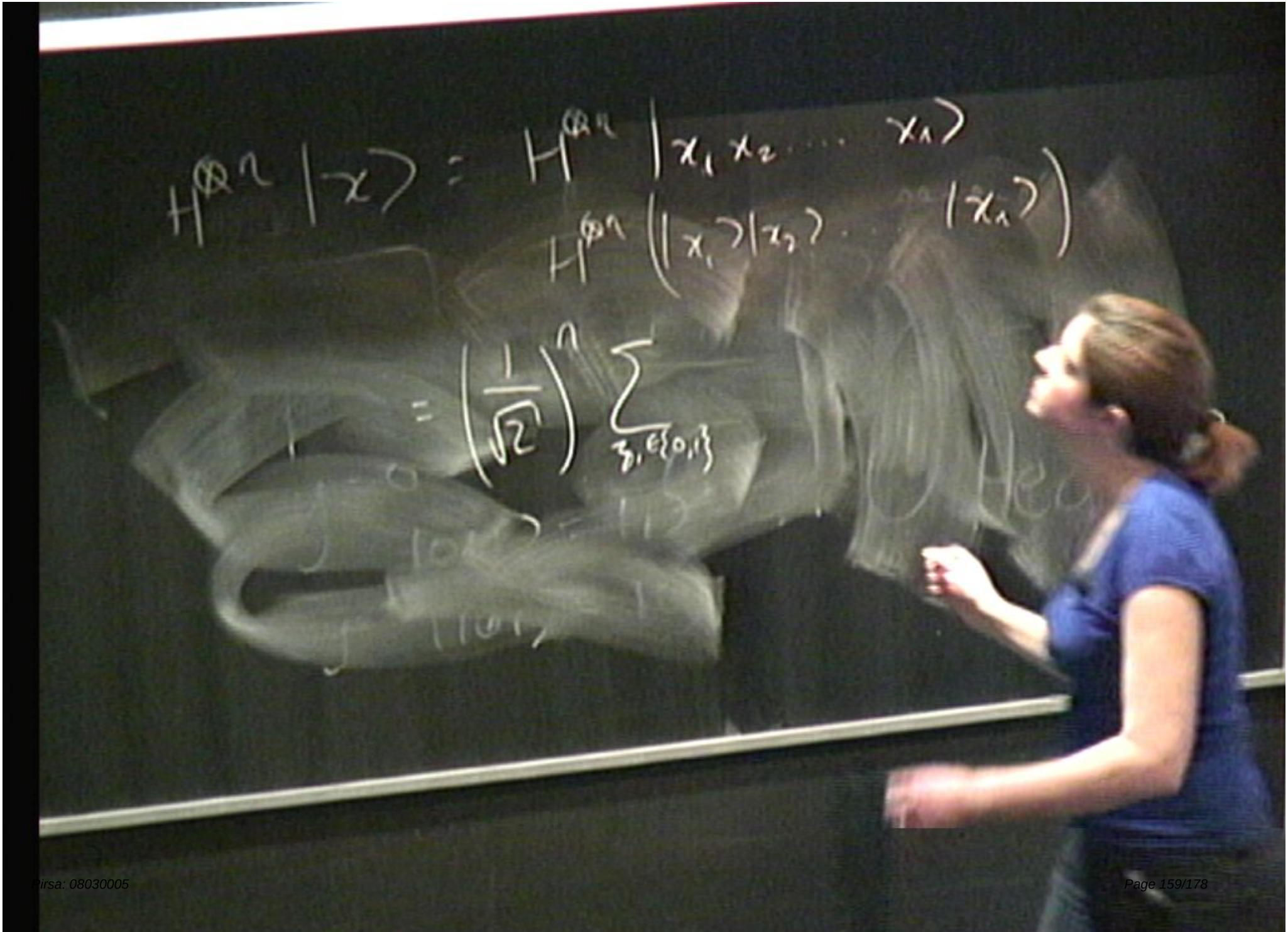
$y = 0$

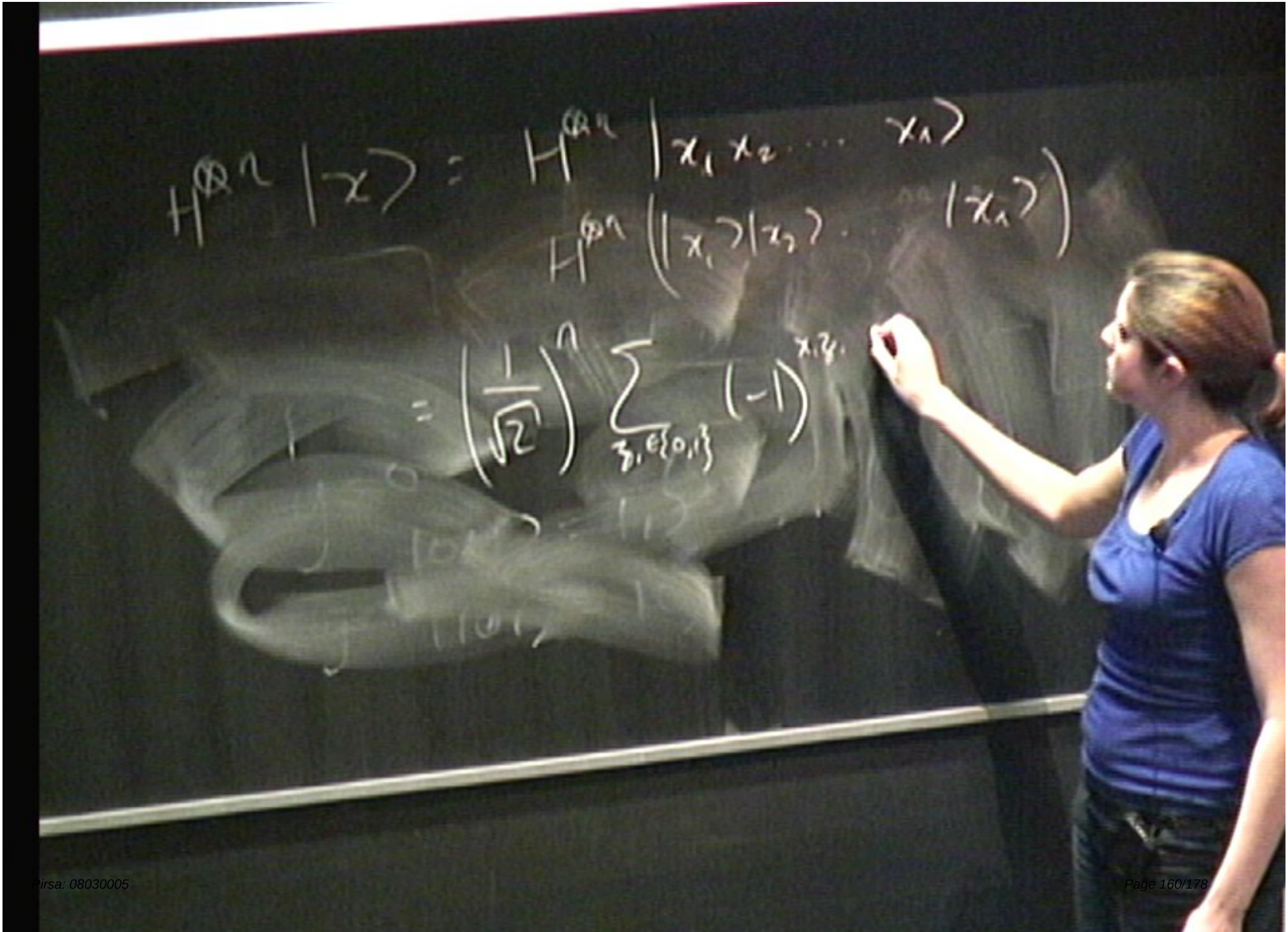
$|001\rangle = |1\rangle$

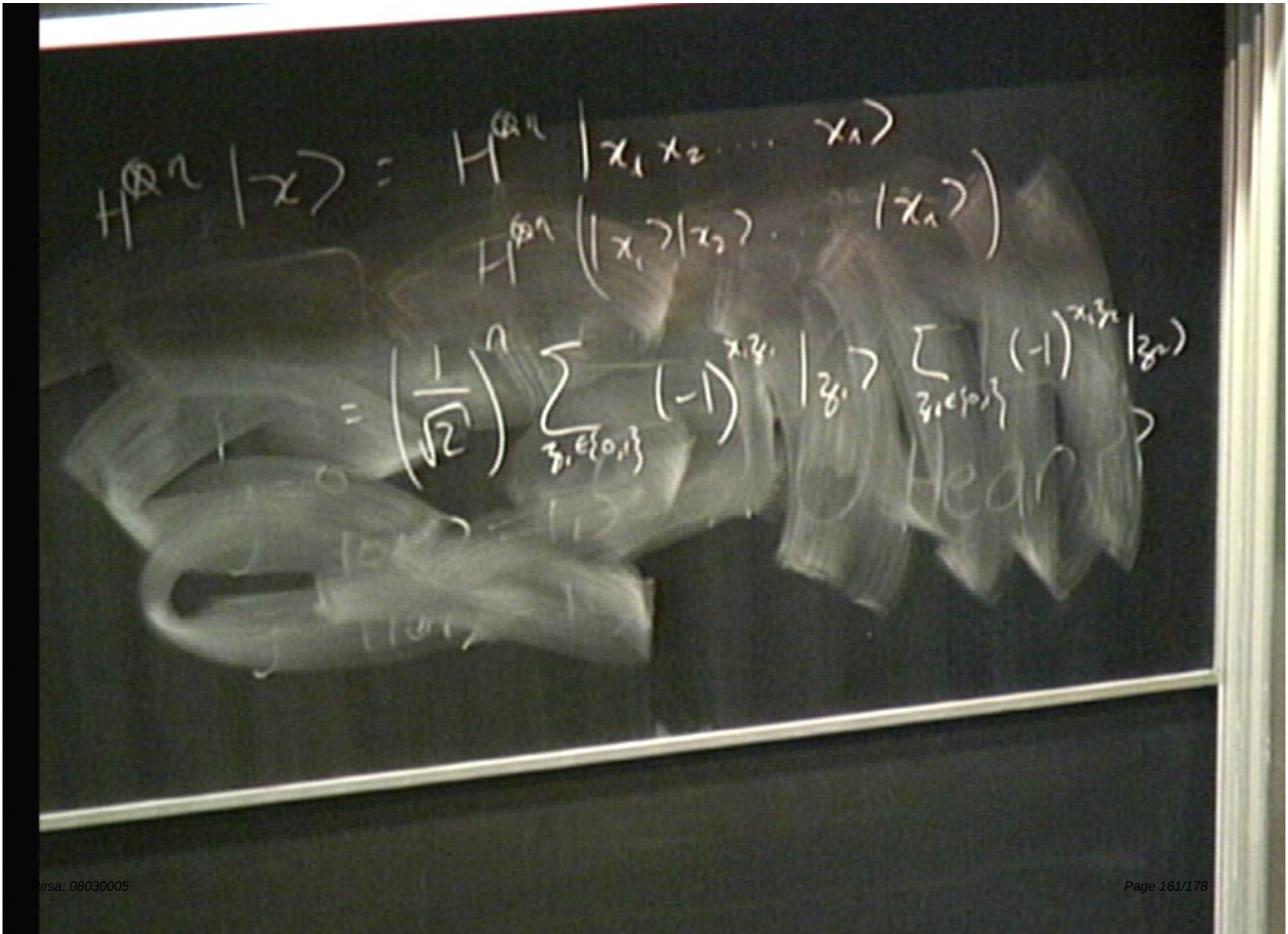

$\left(\frac{1}{\sqrt{2}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$
$H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$
$\Rightarrow H|x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+(-1)^x|1\rangle)$
$=\frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle$

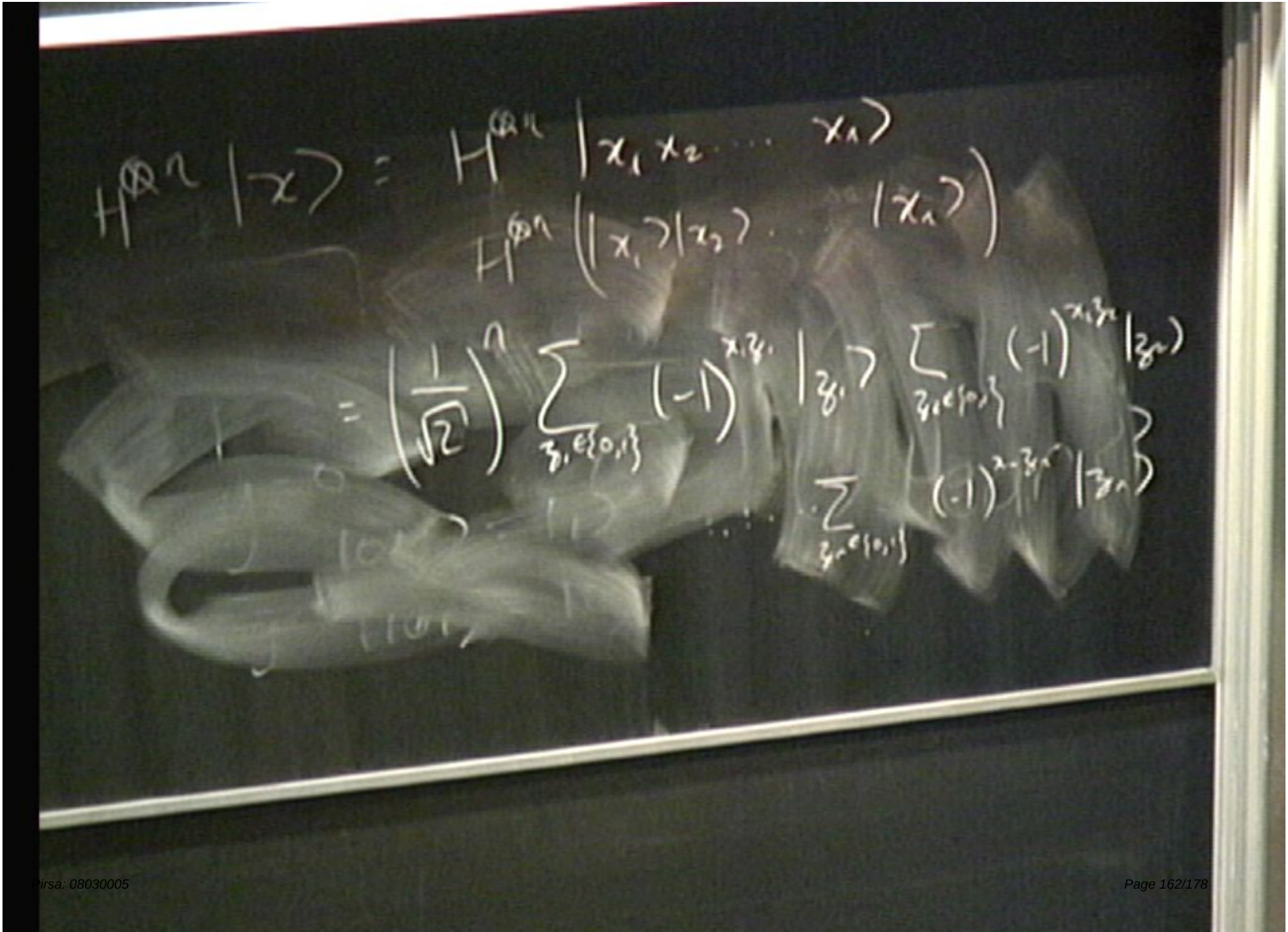

H⊗n |x⟩

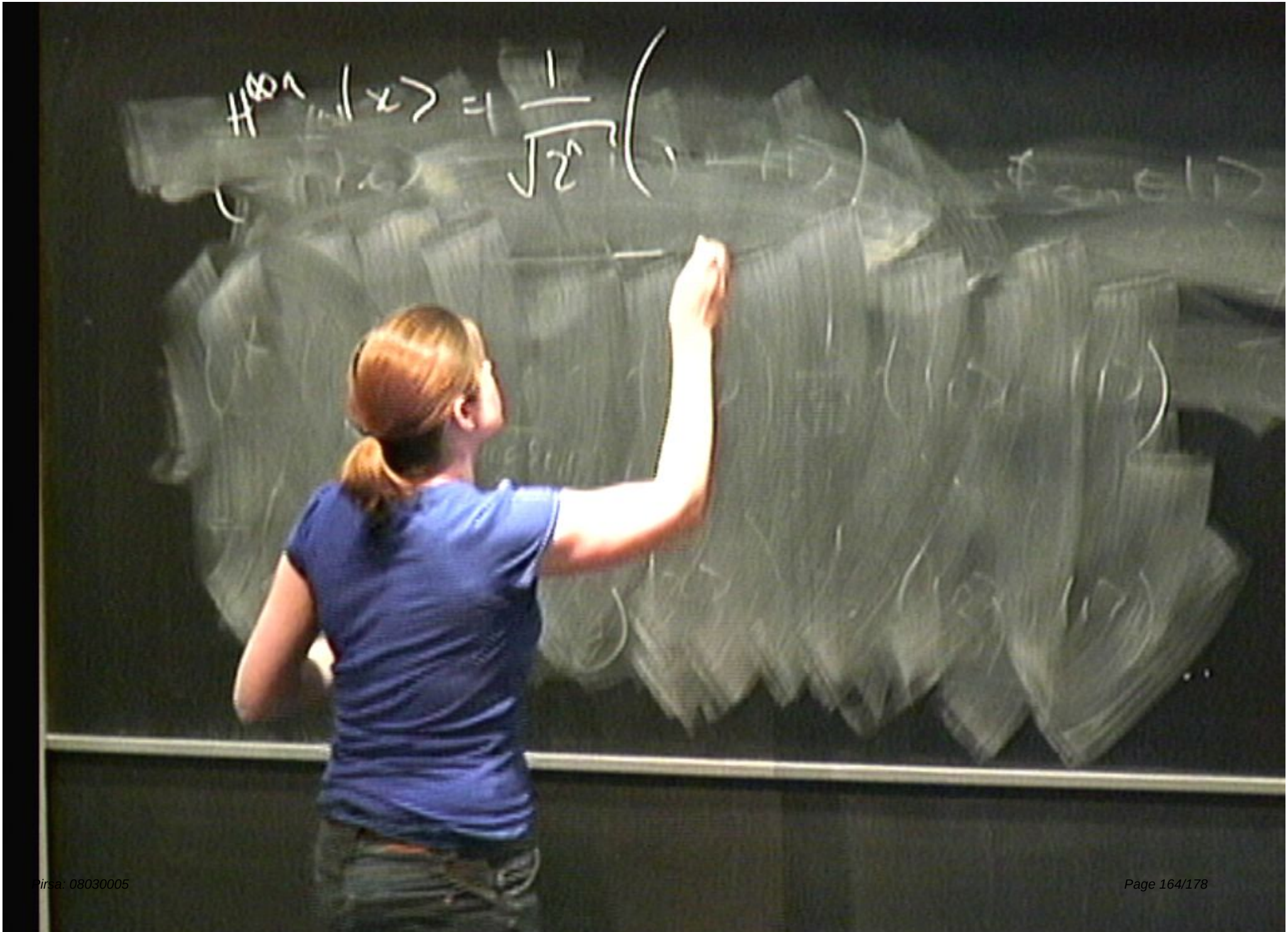

$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1 x_2 \cdots x_n\rangle$
$H^{\otimes n}|x_1\rangle|x_2\rangle \cdots |x_n\rangle$

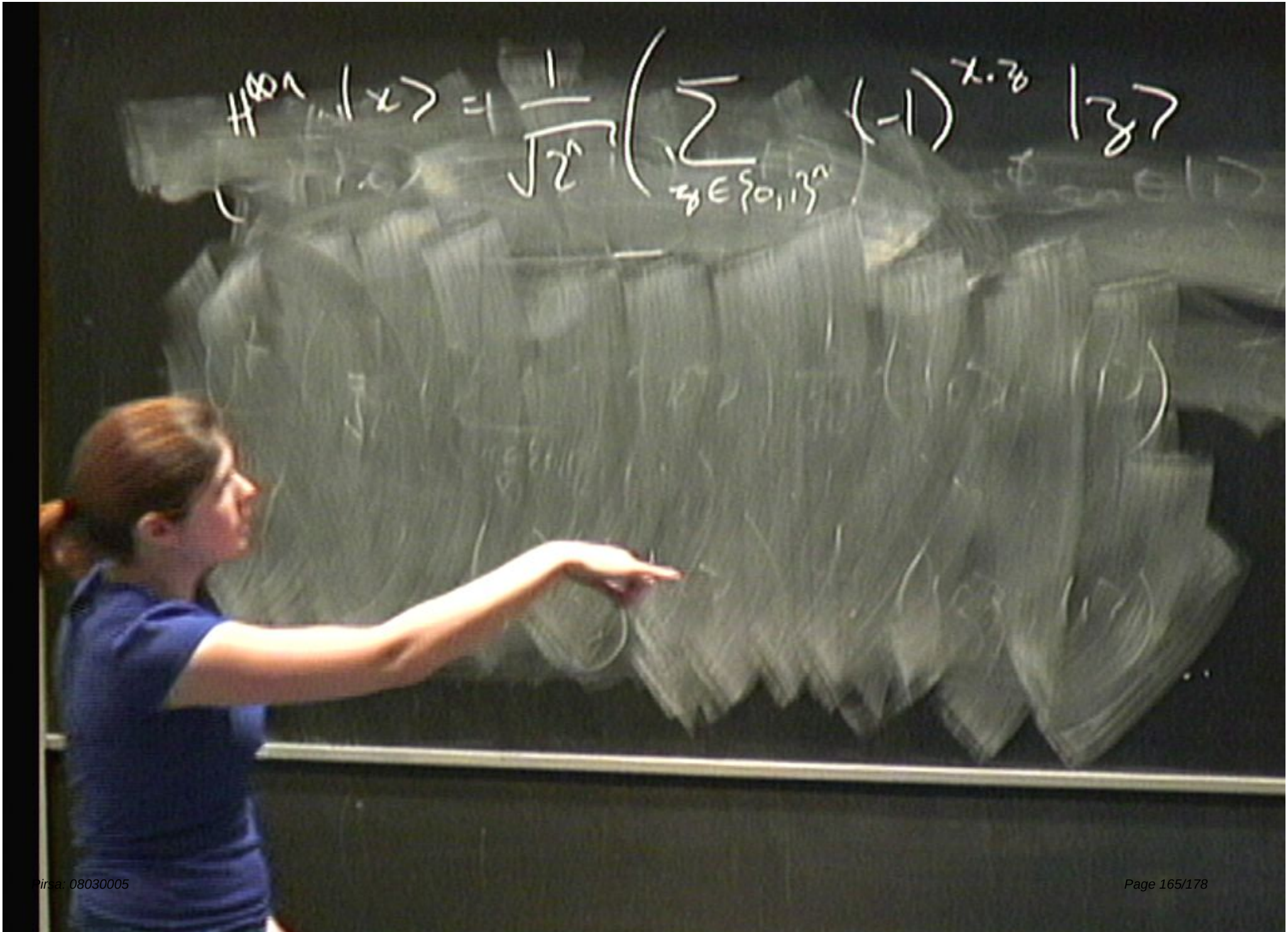

$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1 x_2 \ldots x_n\rangle$
$H^{\otimes n}(|x_1\rangle|x_2\rangle \ldots |x_n\rangle)$
$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z_i \in \{0,1\}}$

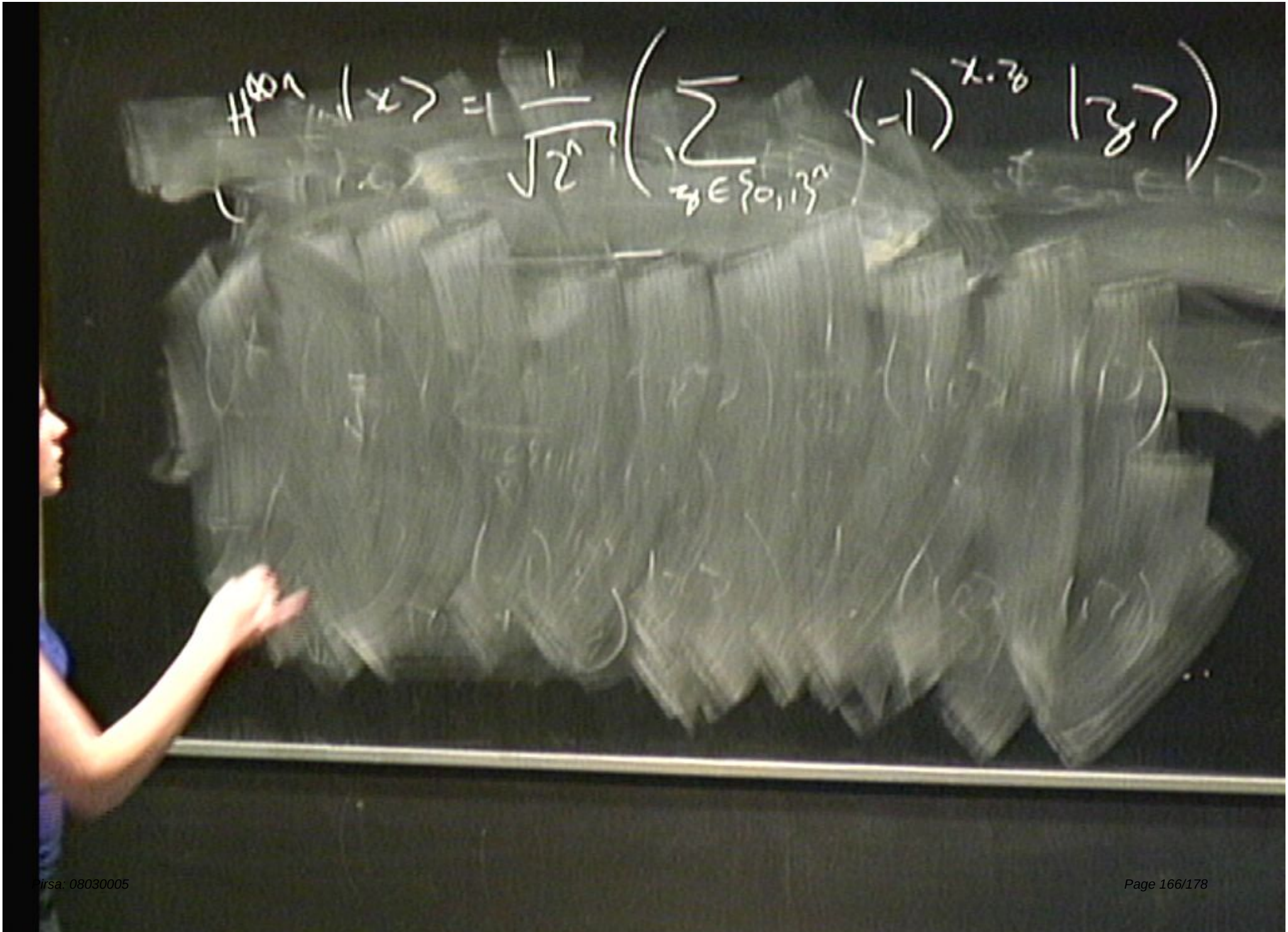

$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1 x_2 \ldots x_n\rangle$
$H^{\otimes n}(|x_1\rangle|x_2\rangle \ldots |x_n\rangle)$
$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z_i \in \{0,1\}} (-1)^{x_i z_i}$


$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1 x_2 \ldots x_n\rangle$
$H^{\otimes n}(|x_1\rangle|x_2\rangle \ldots |x_n\rangle)$
$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |z_1\rangle \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_n} |z_n\rangle$


$H^{\otimes n}|x\rangle = H^{\otimes n}|x_1 x_2 \cdots x_n\rangle$
$H^{\otimes n}(|x_1\rangle|x_2\rangle \cdots |x_n\rangle)$
$= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |z_1\rangle \sum_{z_2 \in \{0,1\}} (-1)^{x_2 z_2} |z_2\rangle$
$\cdots \sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} |z_n\rangle$




$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right)$

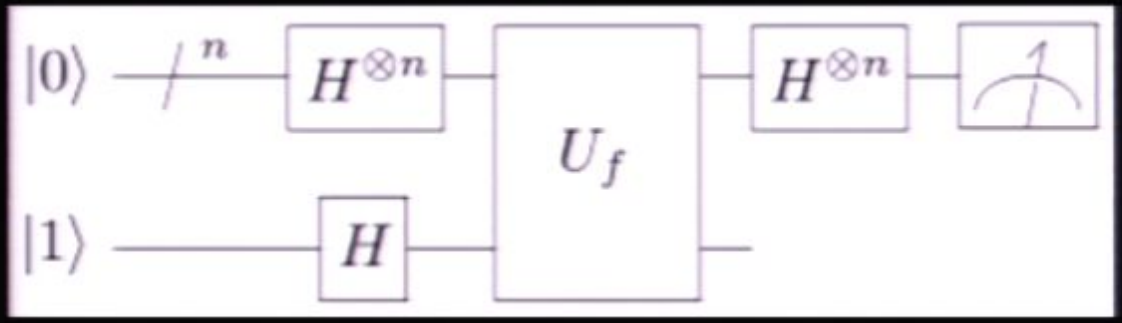

$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right)$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right)$$

$$x \cdot z = x_1 z_1 + x_2 z_2 \ldots$$

Deutsch-Josza Algorithm

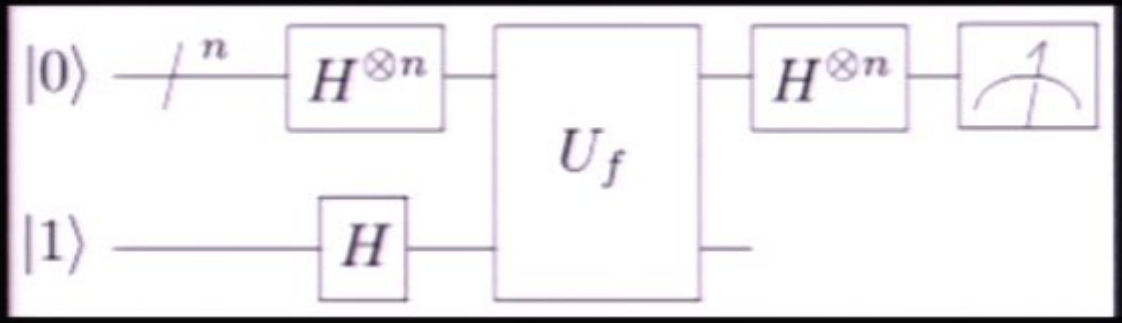
- Extension of Deutsch algorithm
- Quantum circuit diagram



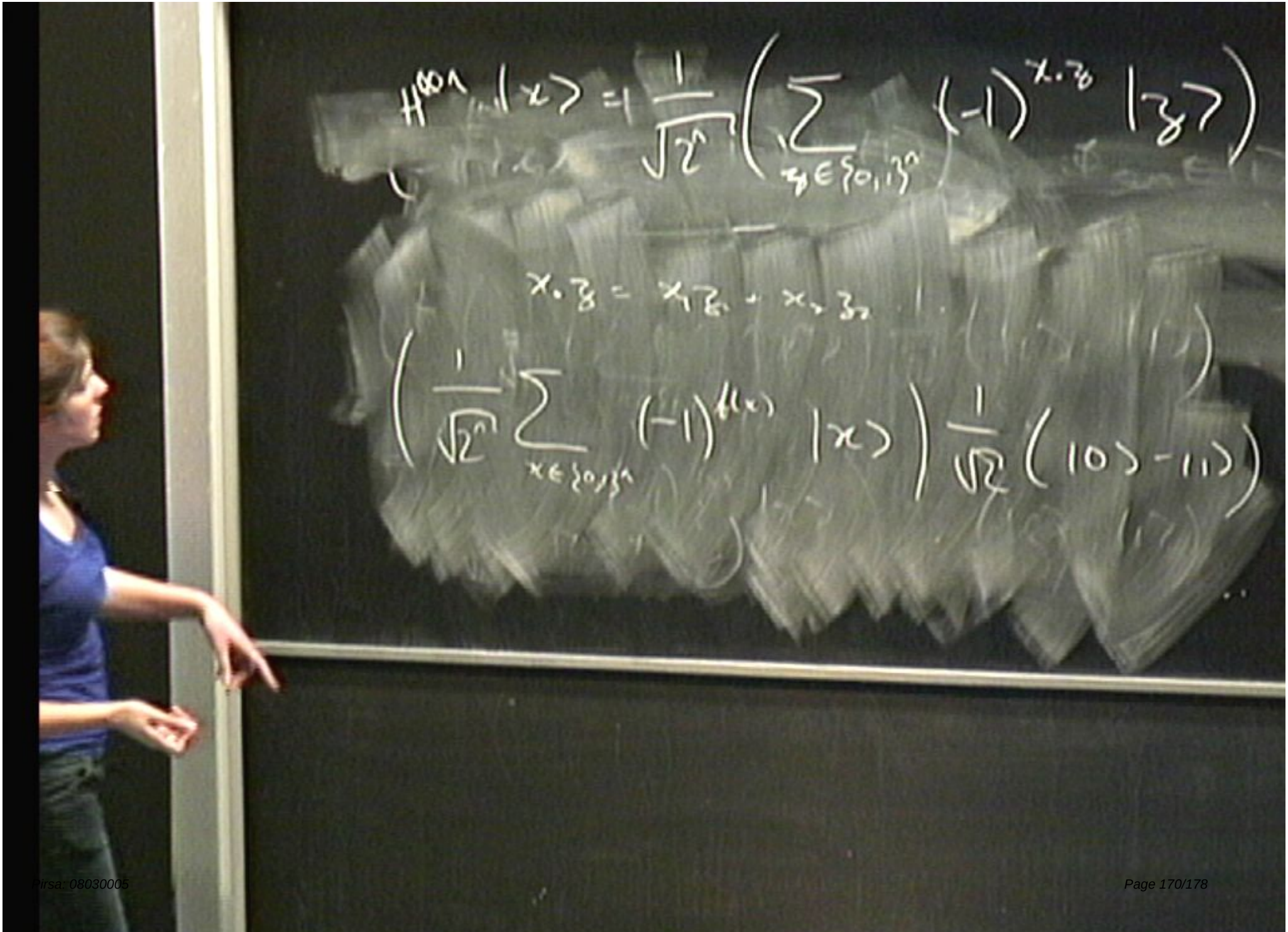
- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.

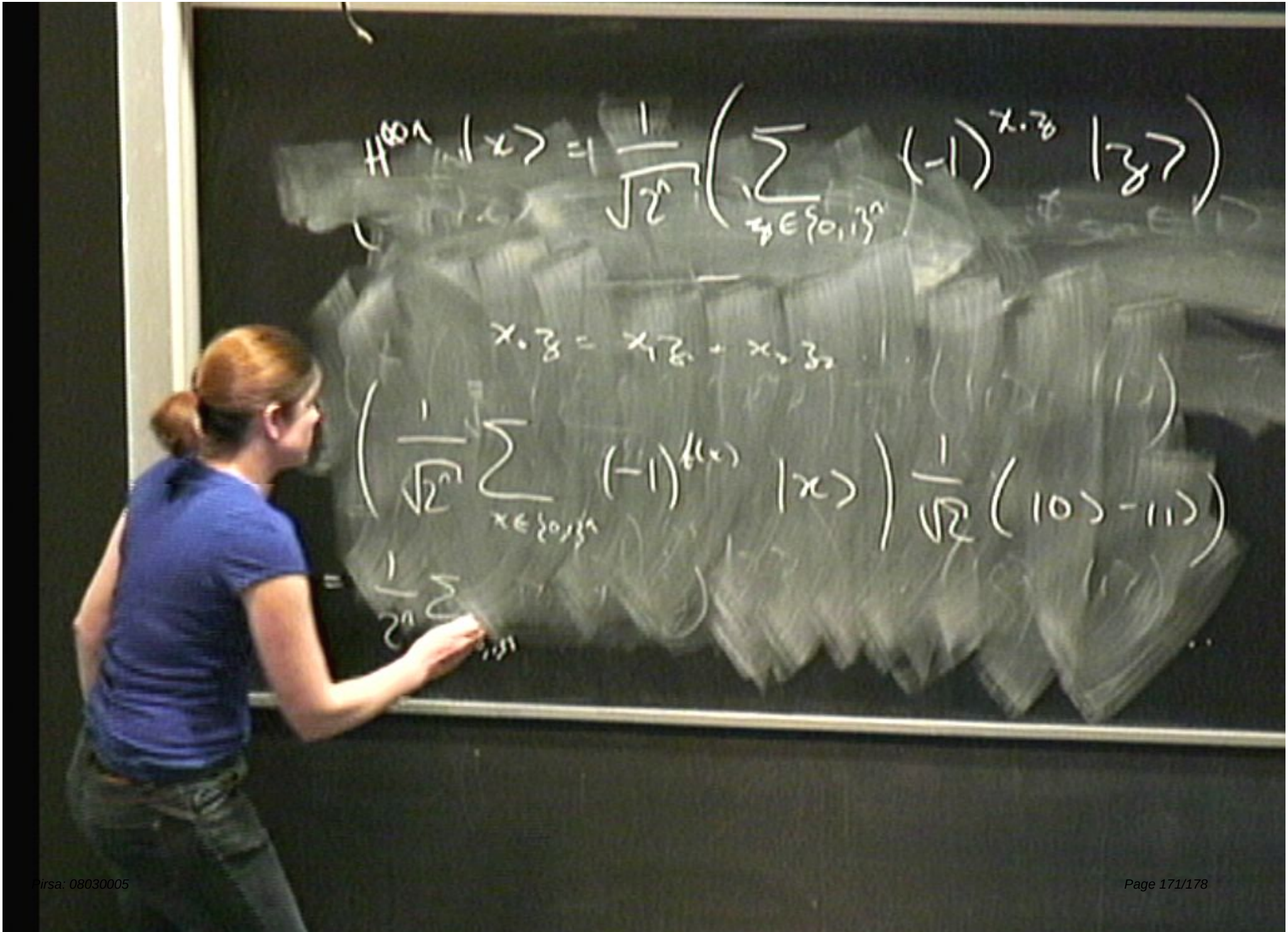
Deutsch-Josza Algorithm

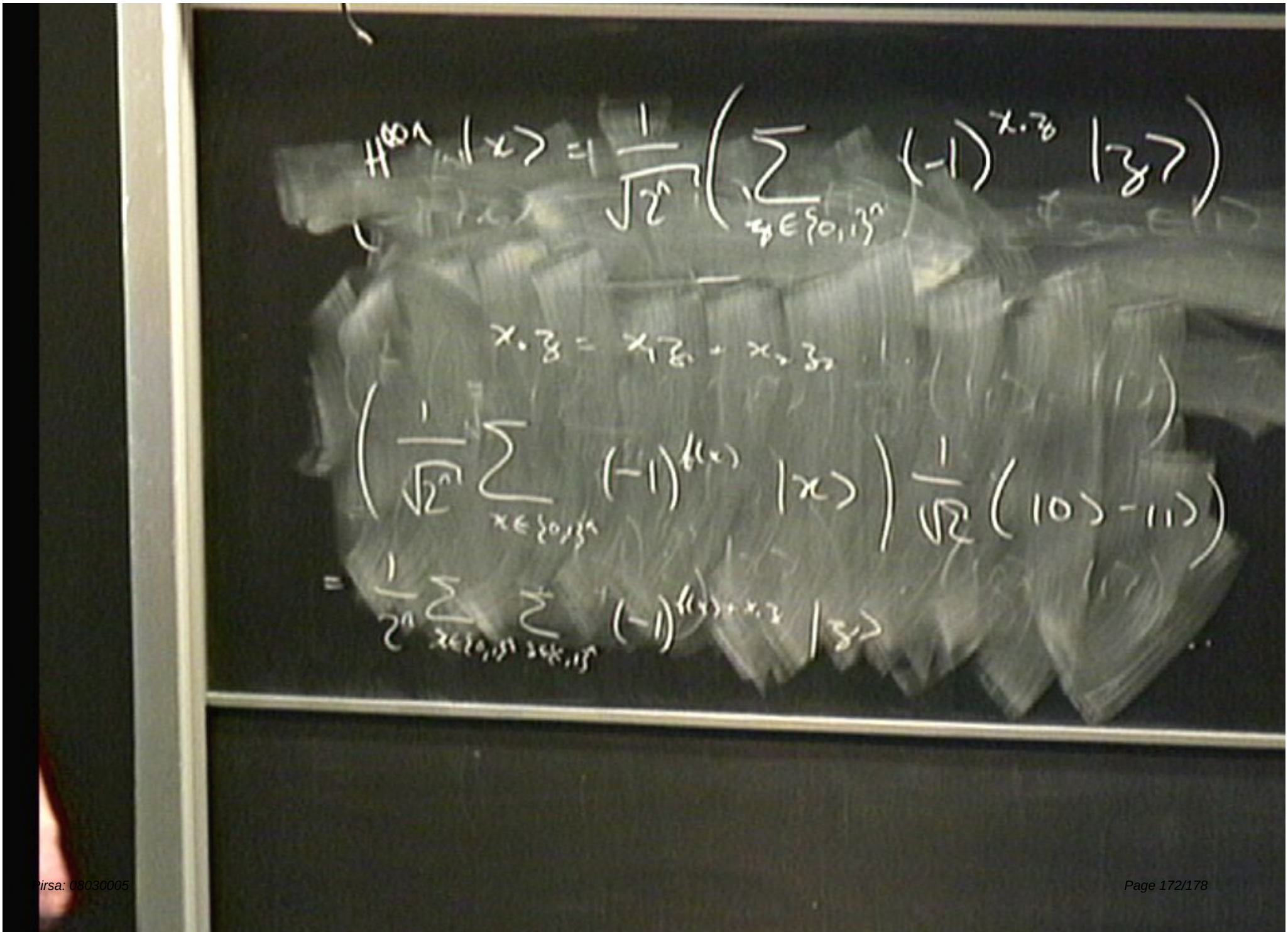
- Extension of Deutsch algorithm
- Quantum circuit diagram

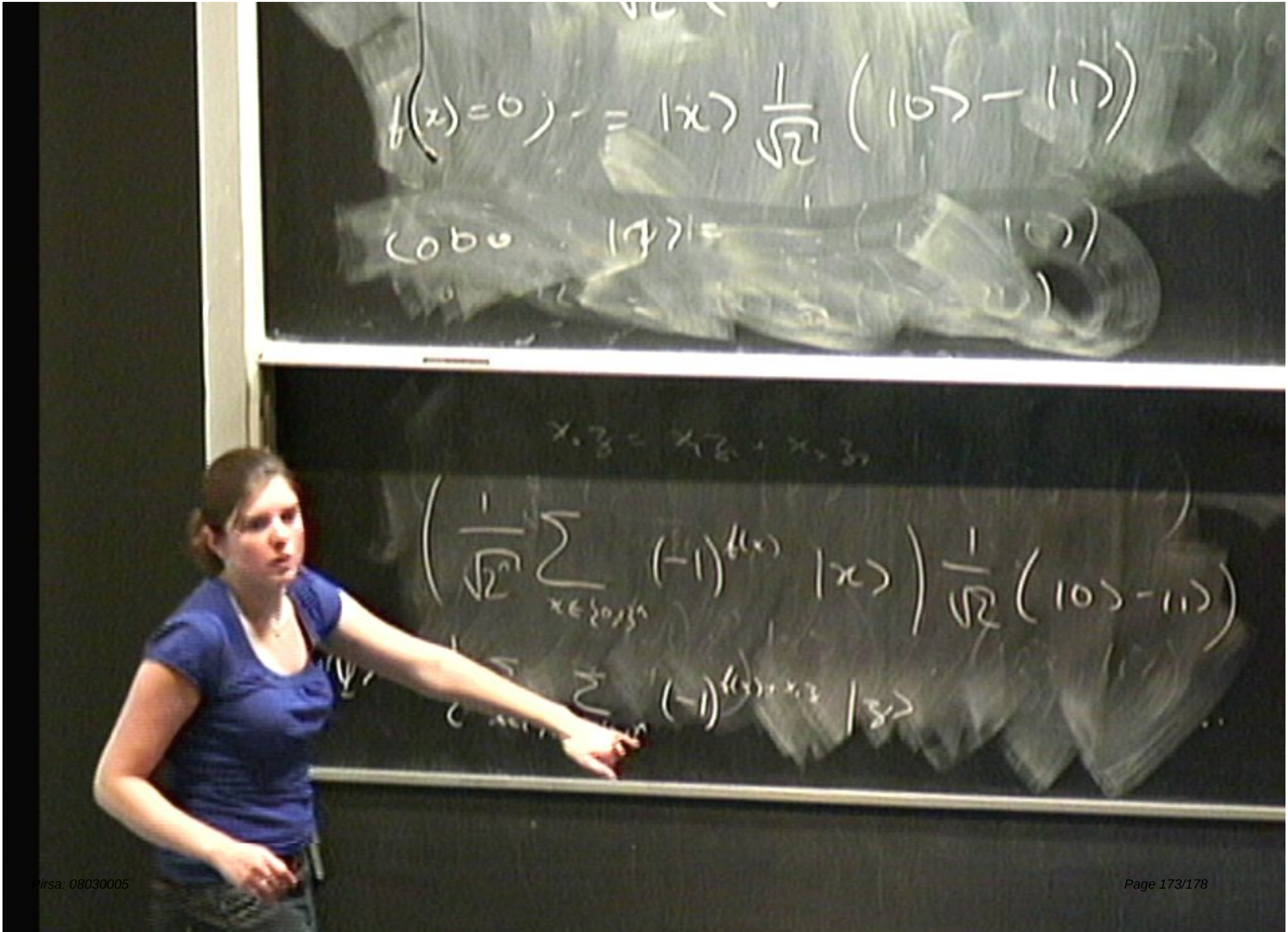


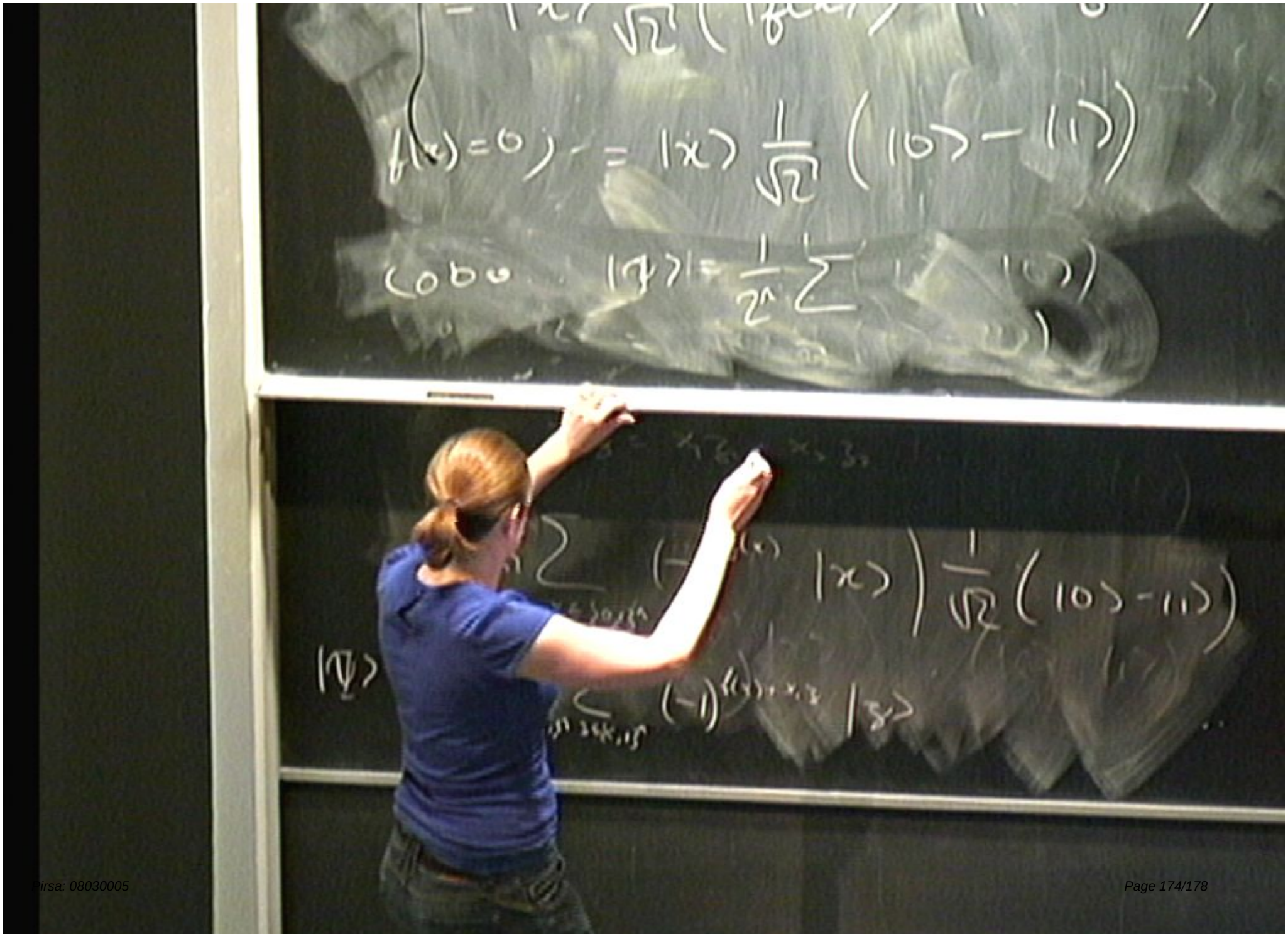
- Allows us to determine whether a function is constant or balanced with one query.
- Classically, need $2^n/2+1$ queries to say with certainty.

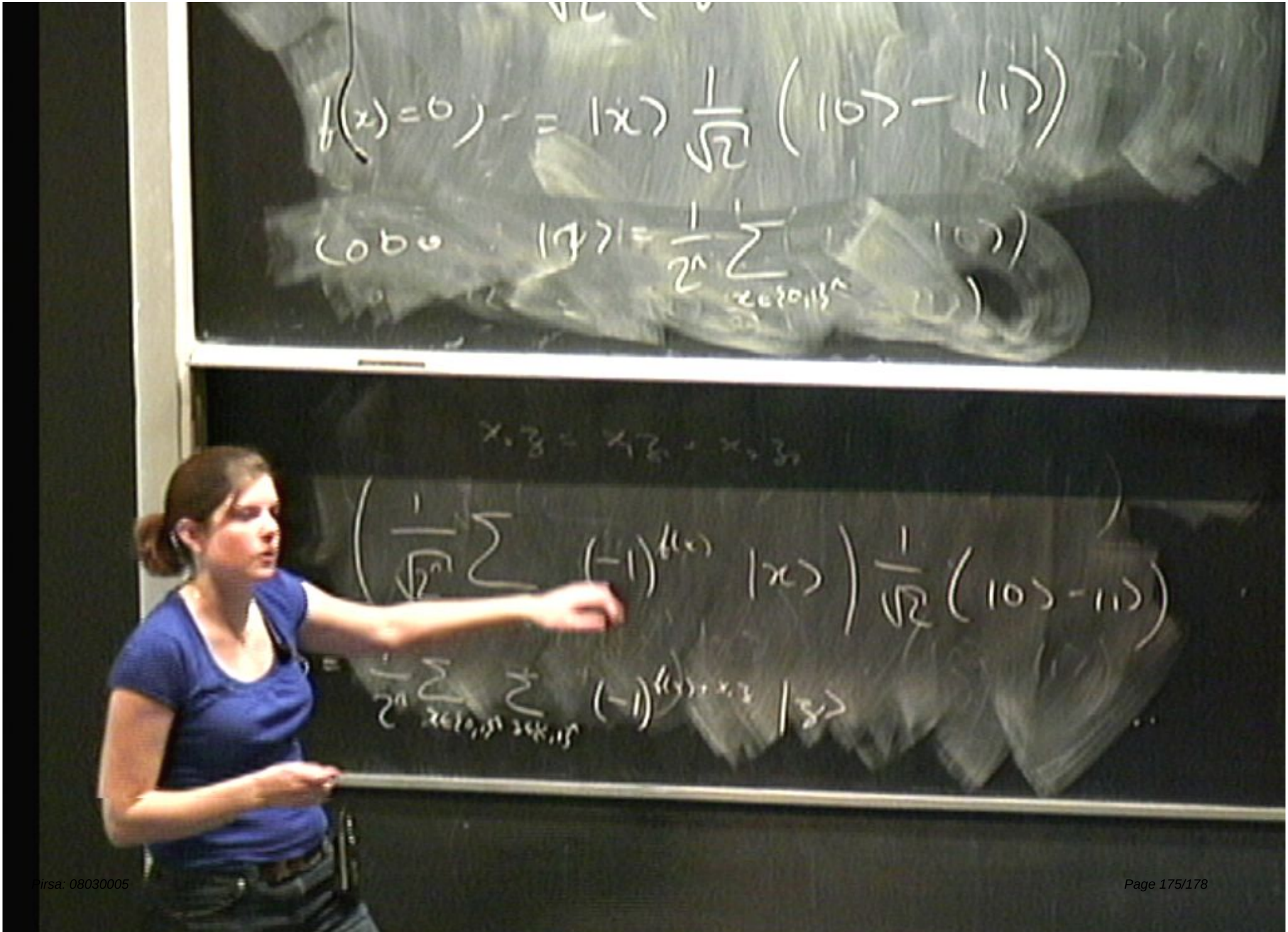

$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right)$
$x \cdot z = x_1 z_1 + x_2 z_2$
$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$

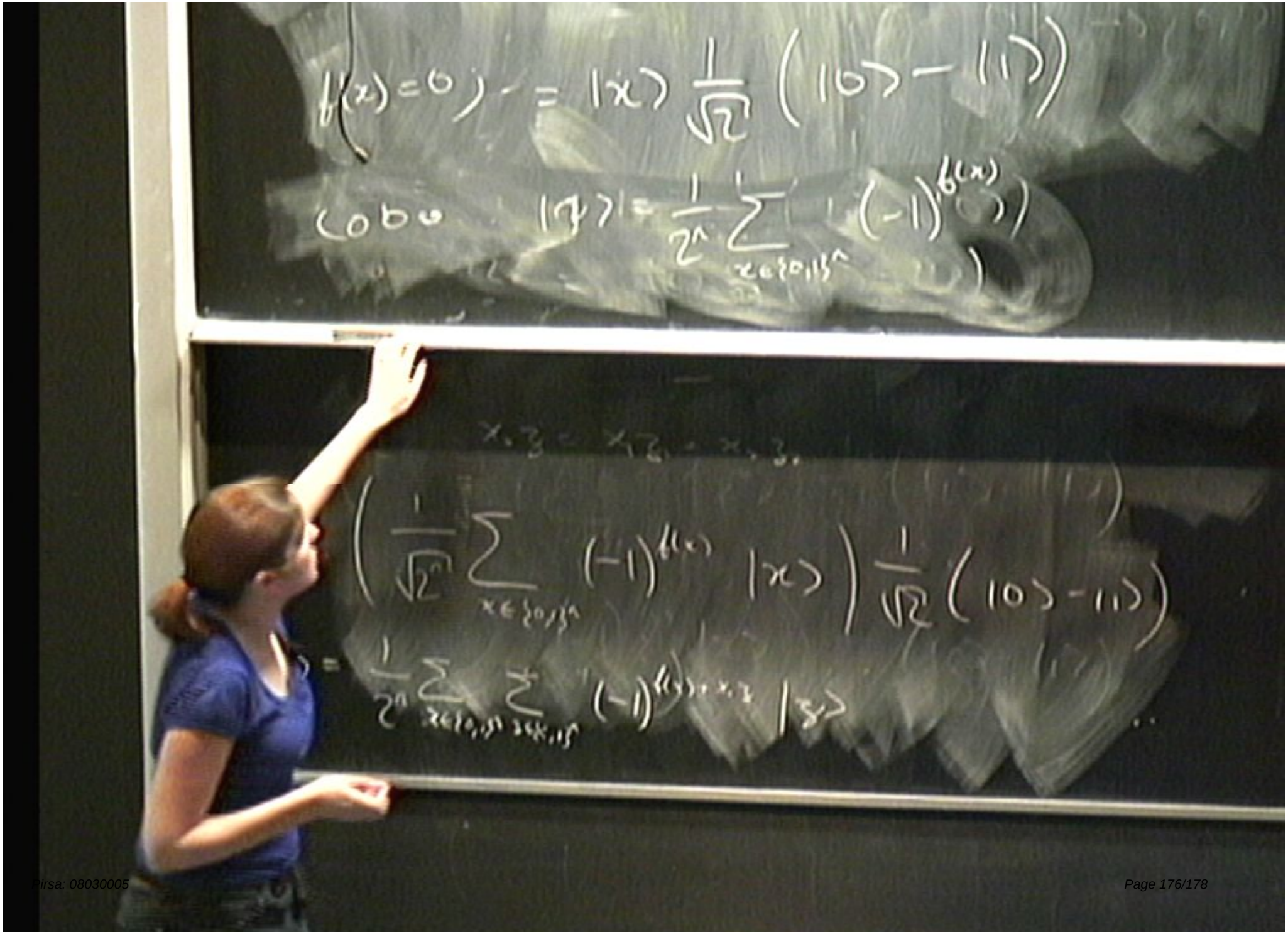

$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right)$
$x \cdot z = x_1 z_1 + \cdots + x_n z_n$
$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
$= \frac{1}{2^n} \sum$

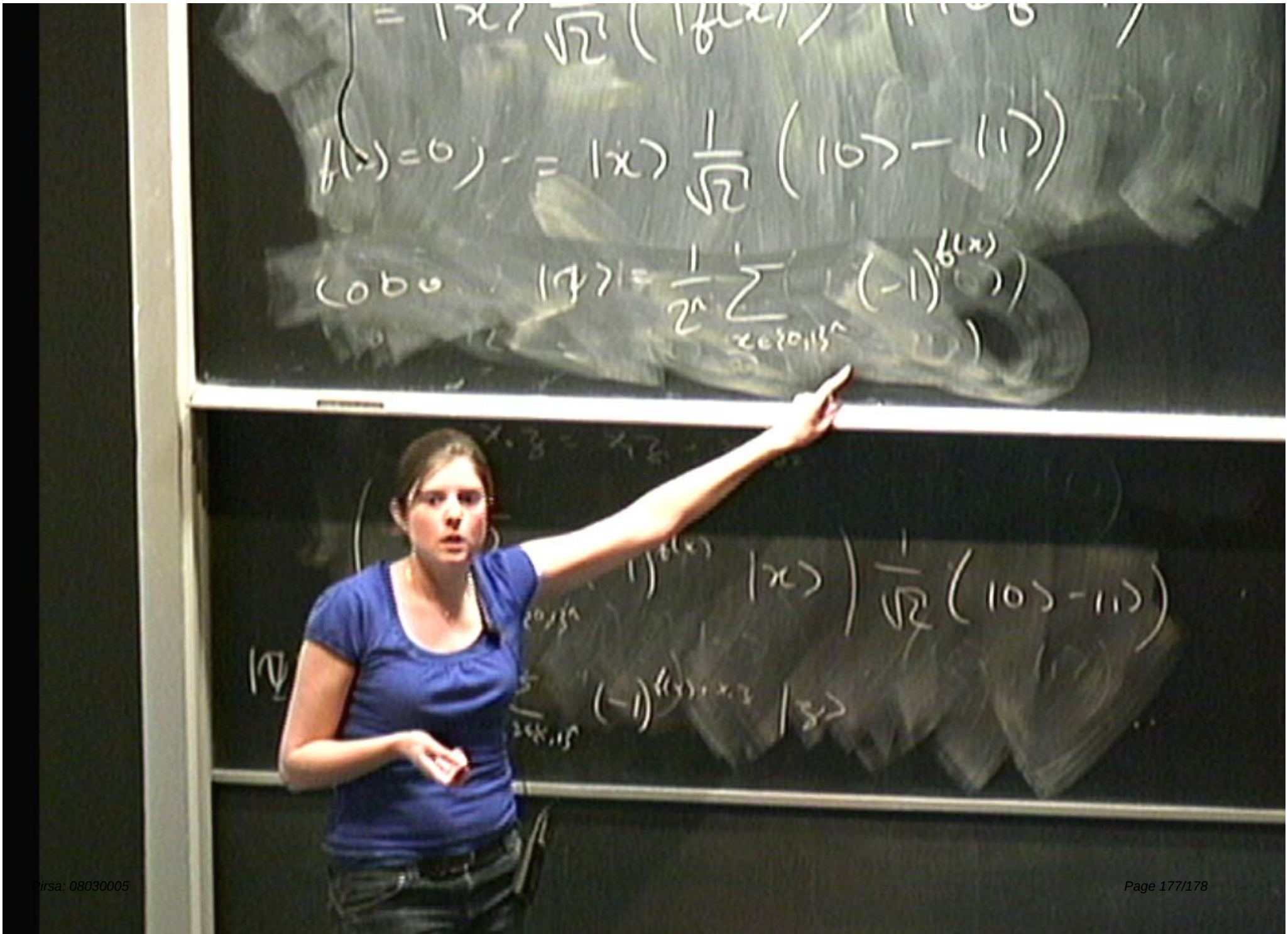

$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right)$
$x \cdot z = x_1 z_1 + \cdots + x_n z_n$
$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right)$
$= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{f(x) + x \cdot z} |z\rangle$

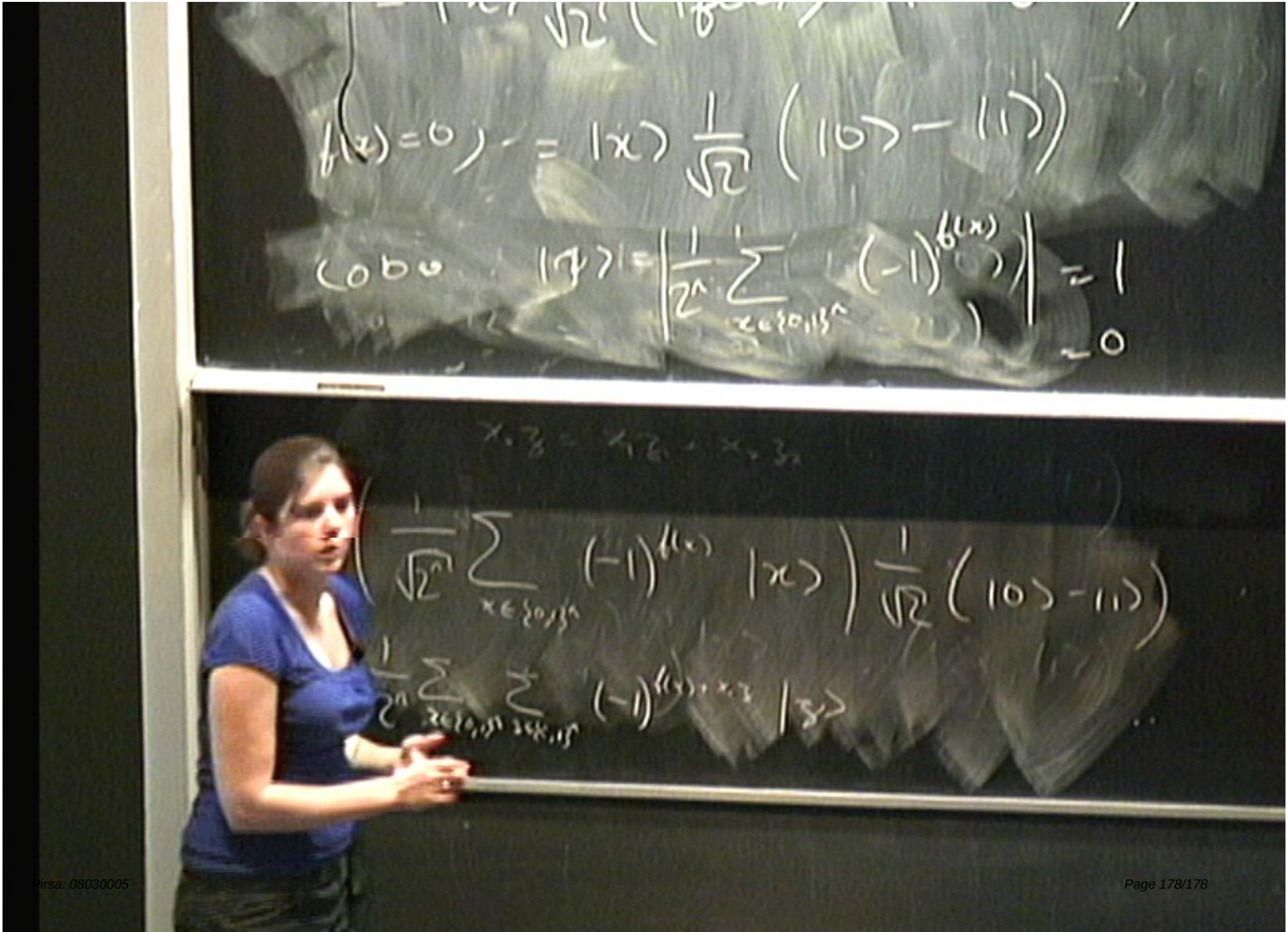

$f(x)=0) = |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$










$|f(x)=0\rangle = |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$