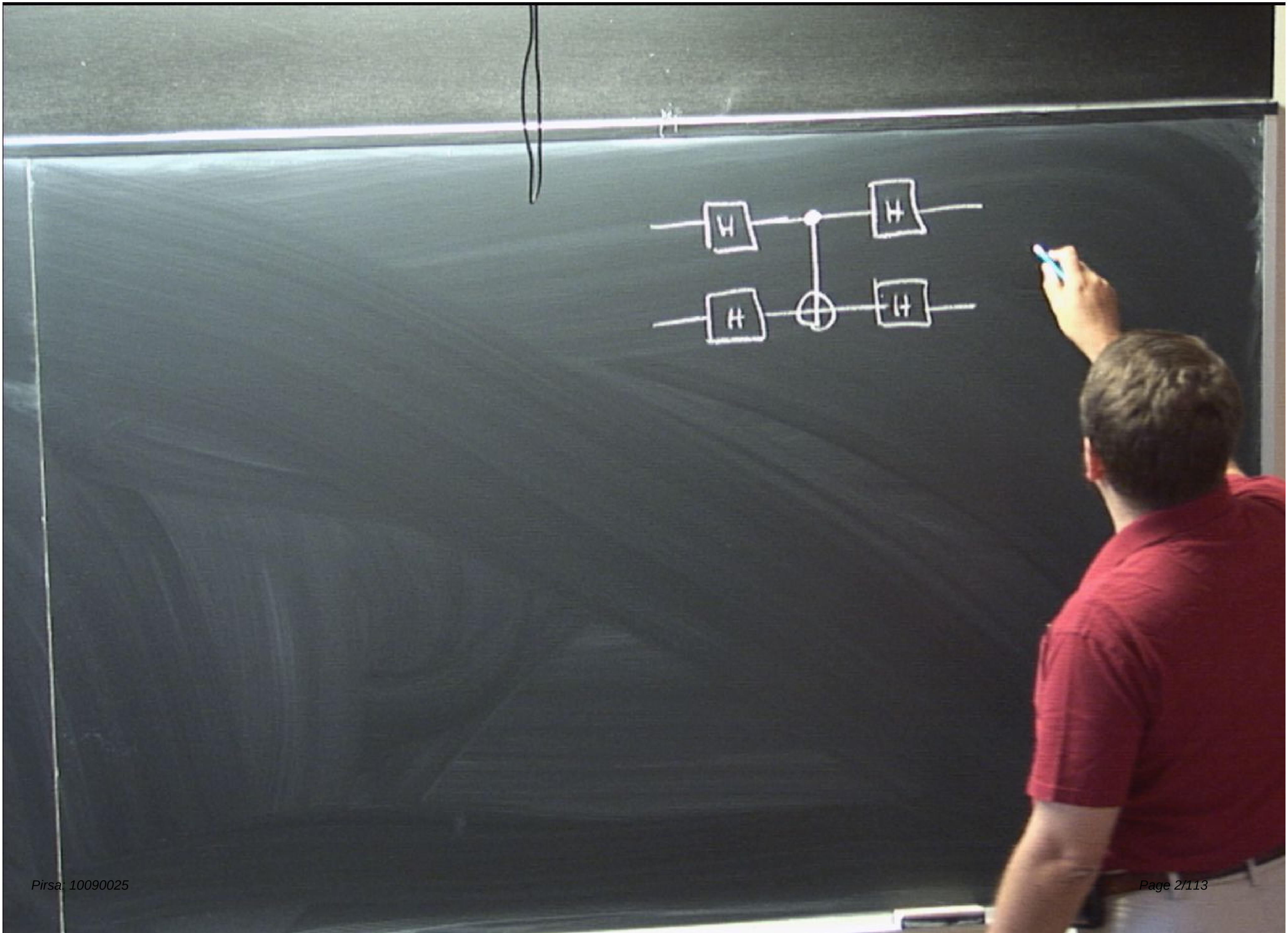
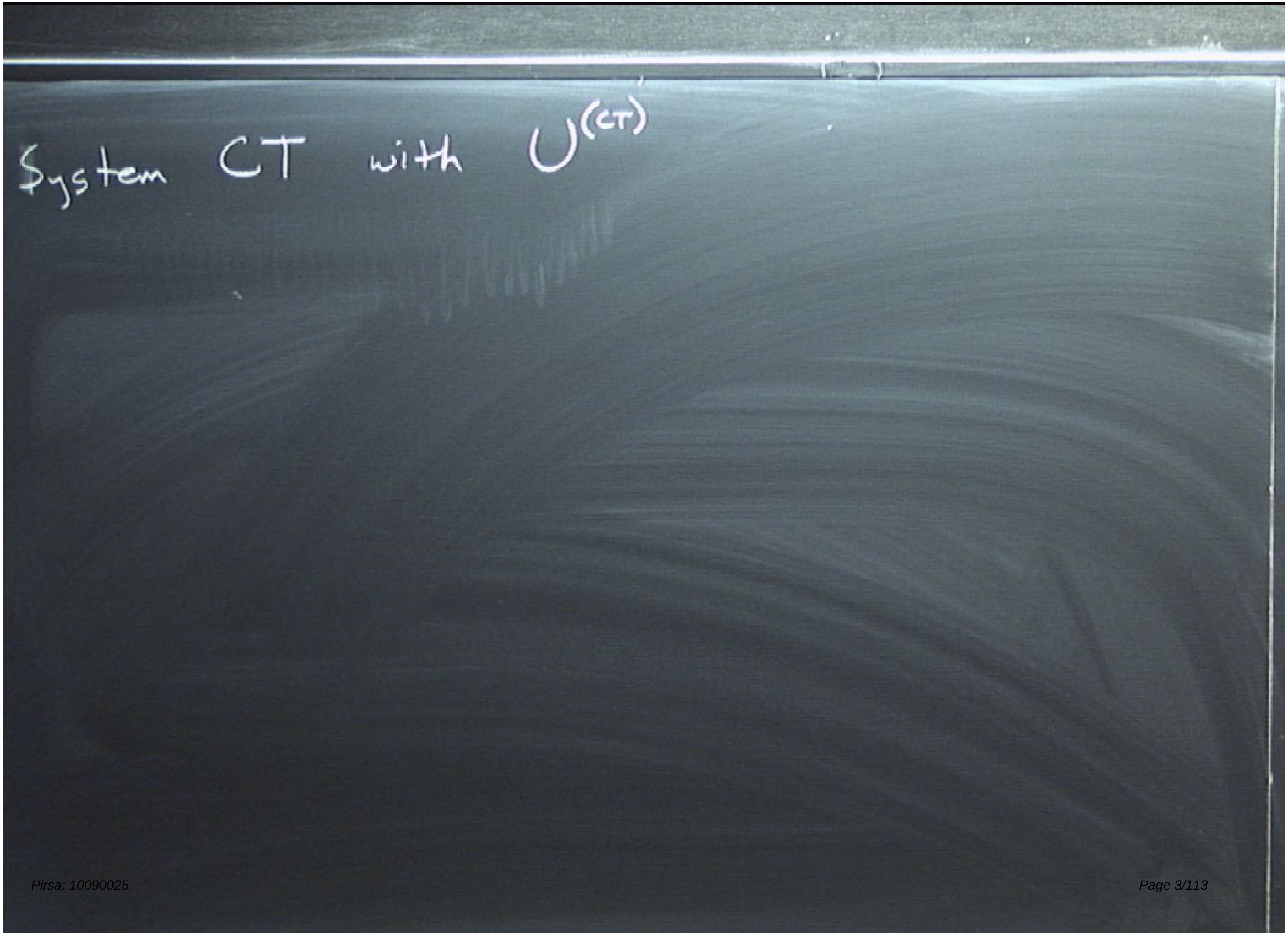
Title: Quantum Theory (PHYS 605) - Lecture 14

Date: Sep 30, 2010 09:00 AM

URL: http://pirsa.org/10090025

Abstract:


H
H
H
H

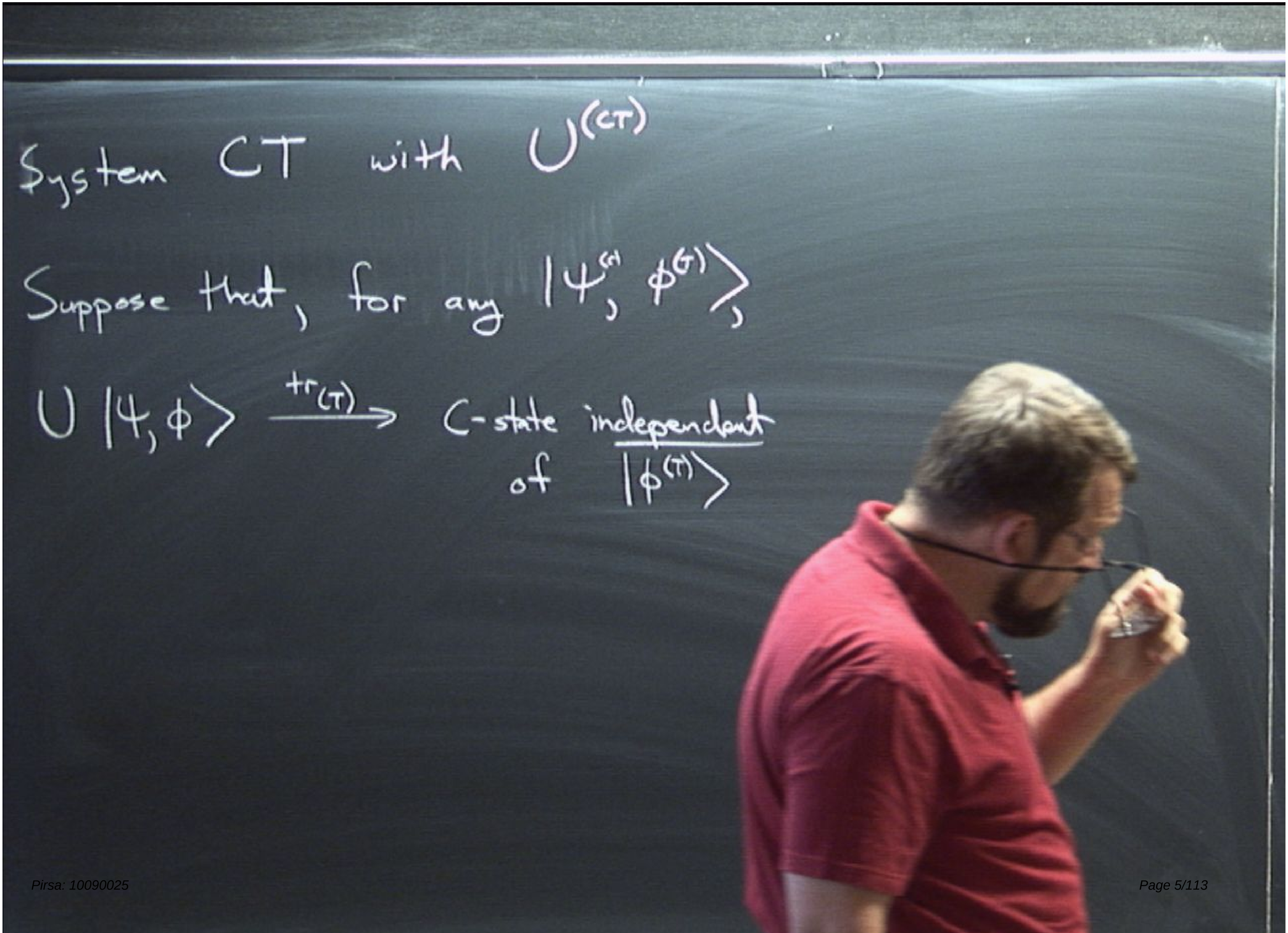


System CT with $U^{(CT)}$

System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

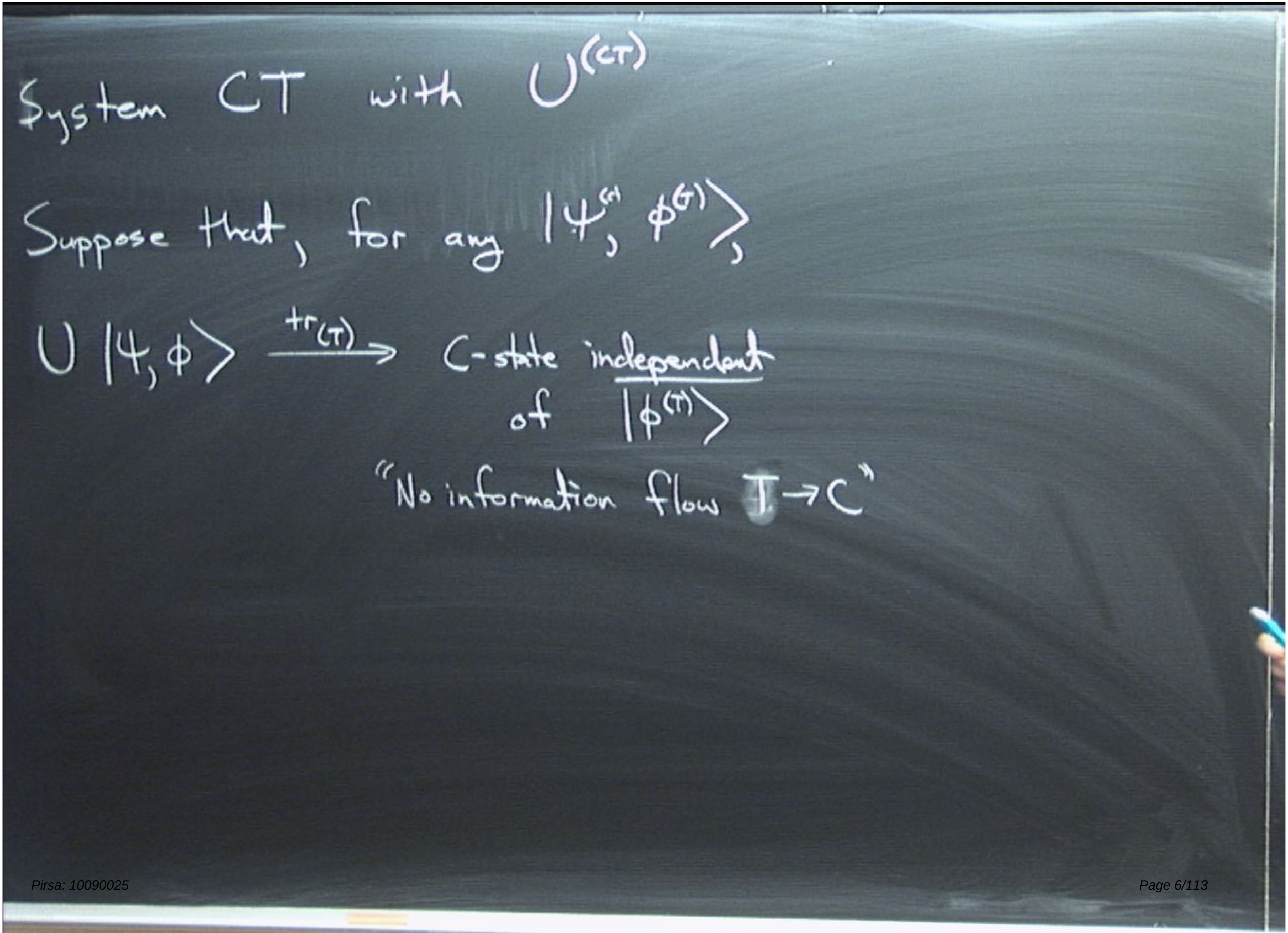
$U|\psi,\phi\rangle$



System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U|\psi,\phi\rangle \xrightarrow{tr_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

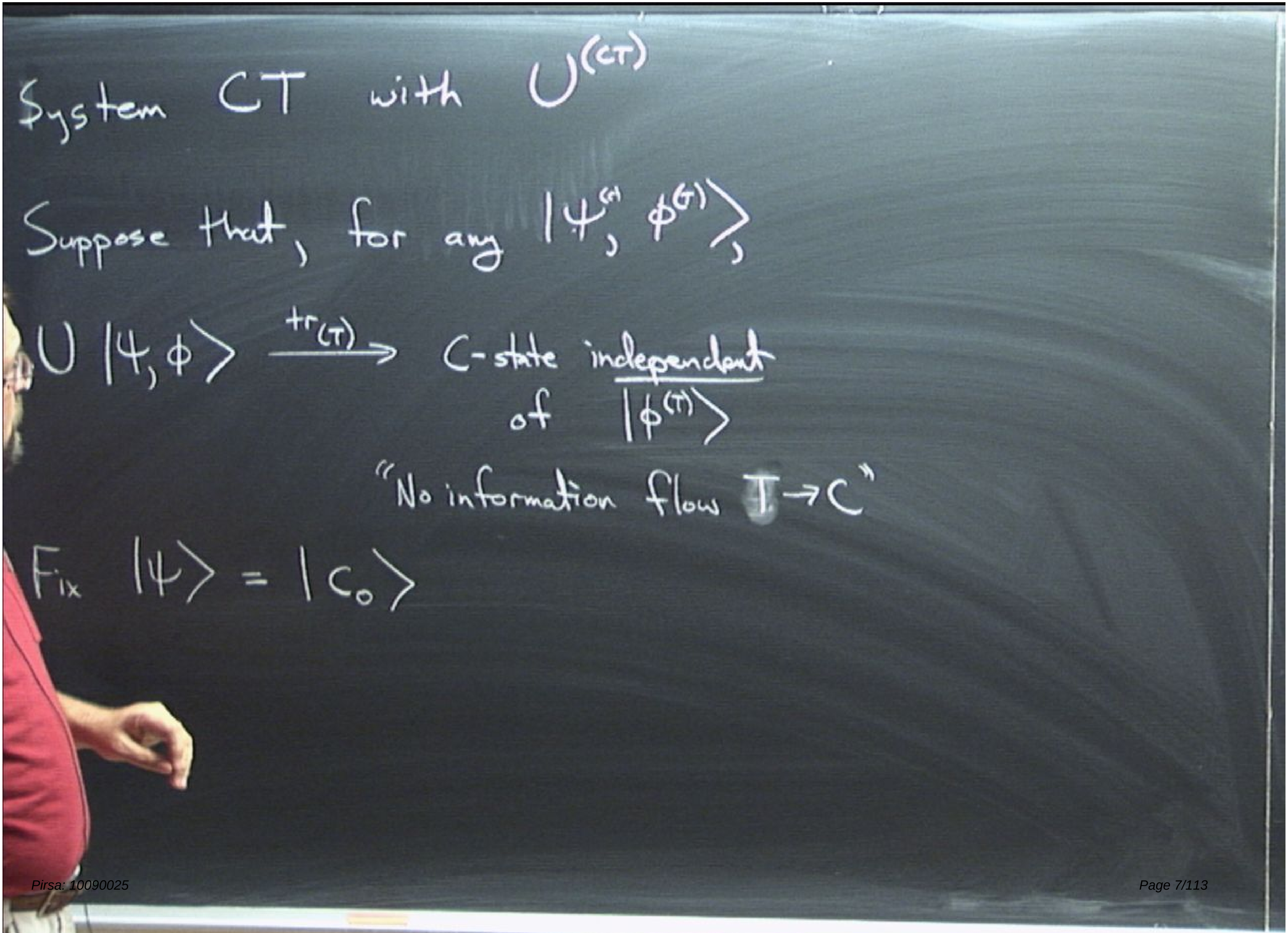


System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U|\psi,\phi\rangle \xrightarrow{\mathrm{tr}_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

"No information flow T → C"



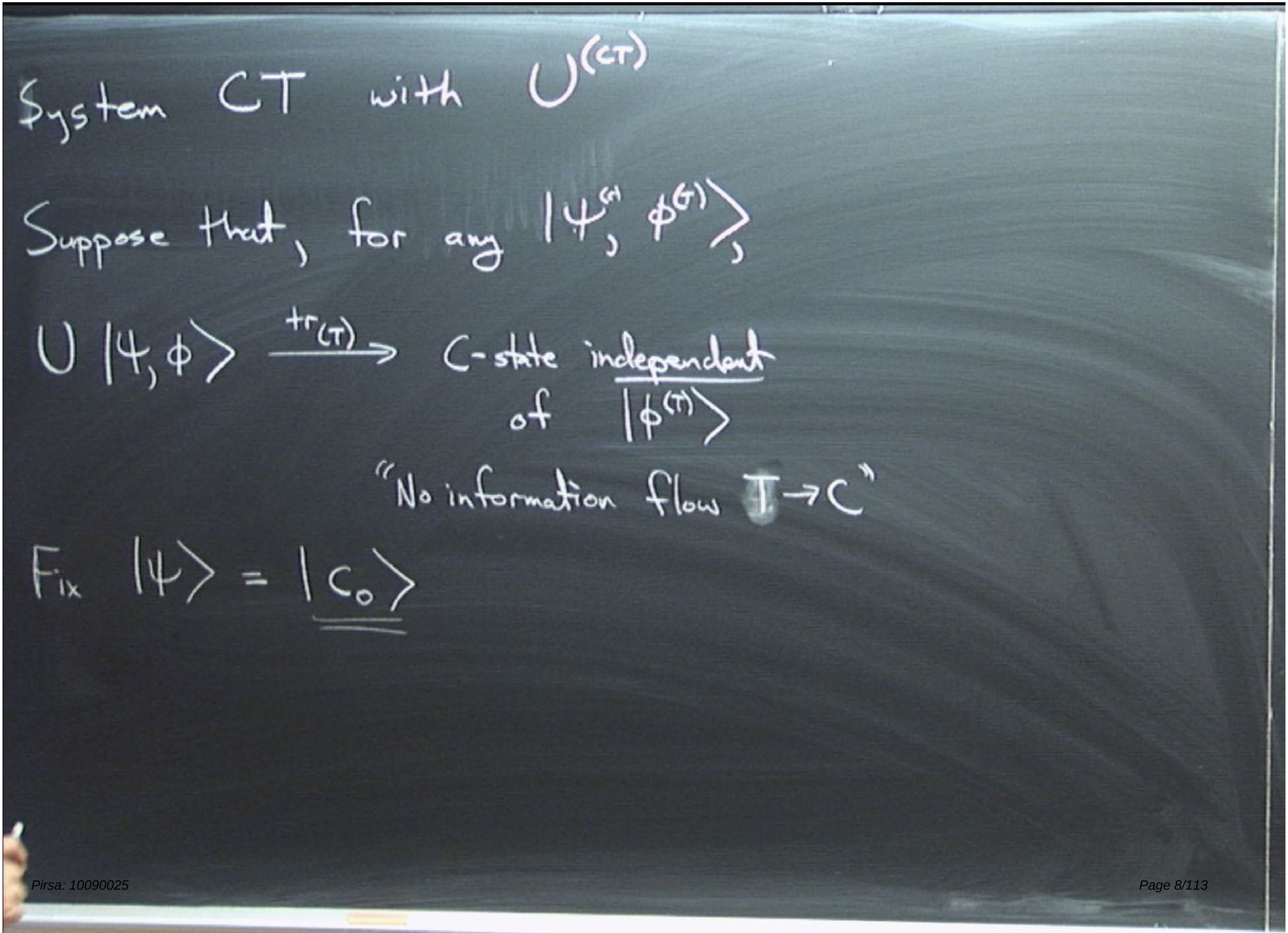
System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U|\psi,\phi\rangle \xrightarrow{tr_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

"No information flow T → C"

Fix $|\psi\rangle = |c_0\rangle$



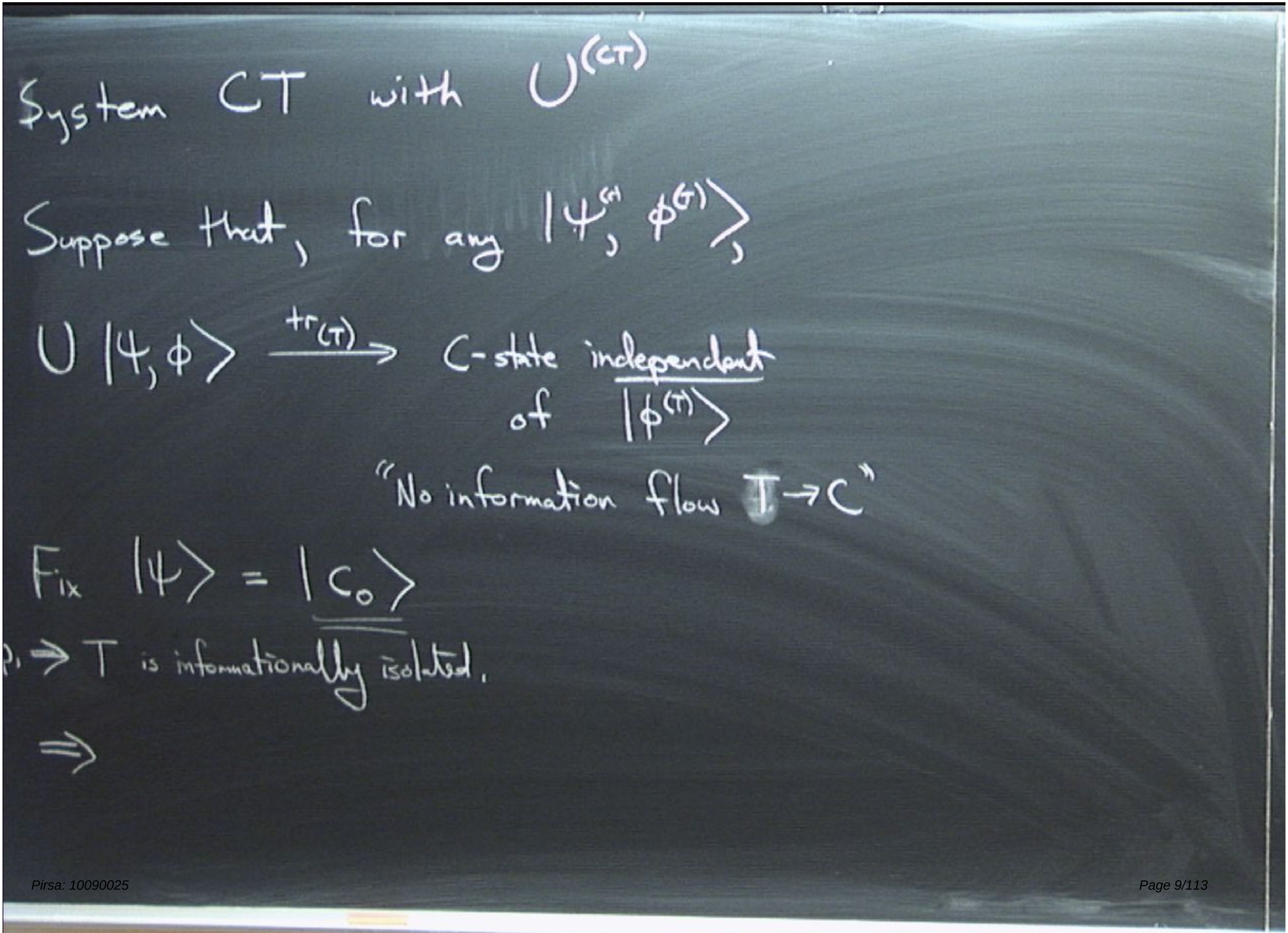
System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U\,|\psi,\phi\rangle \xrightarrow{tr_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

"No information flow T $\rightarrow$ C"

Fix $|\psi\rangle = |\underline{\underline{c_0}}\rangle$



System CT with $U^{(CT)}$

Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

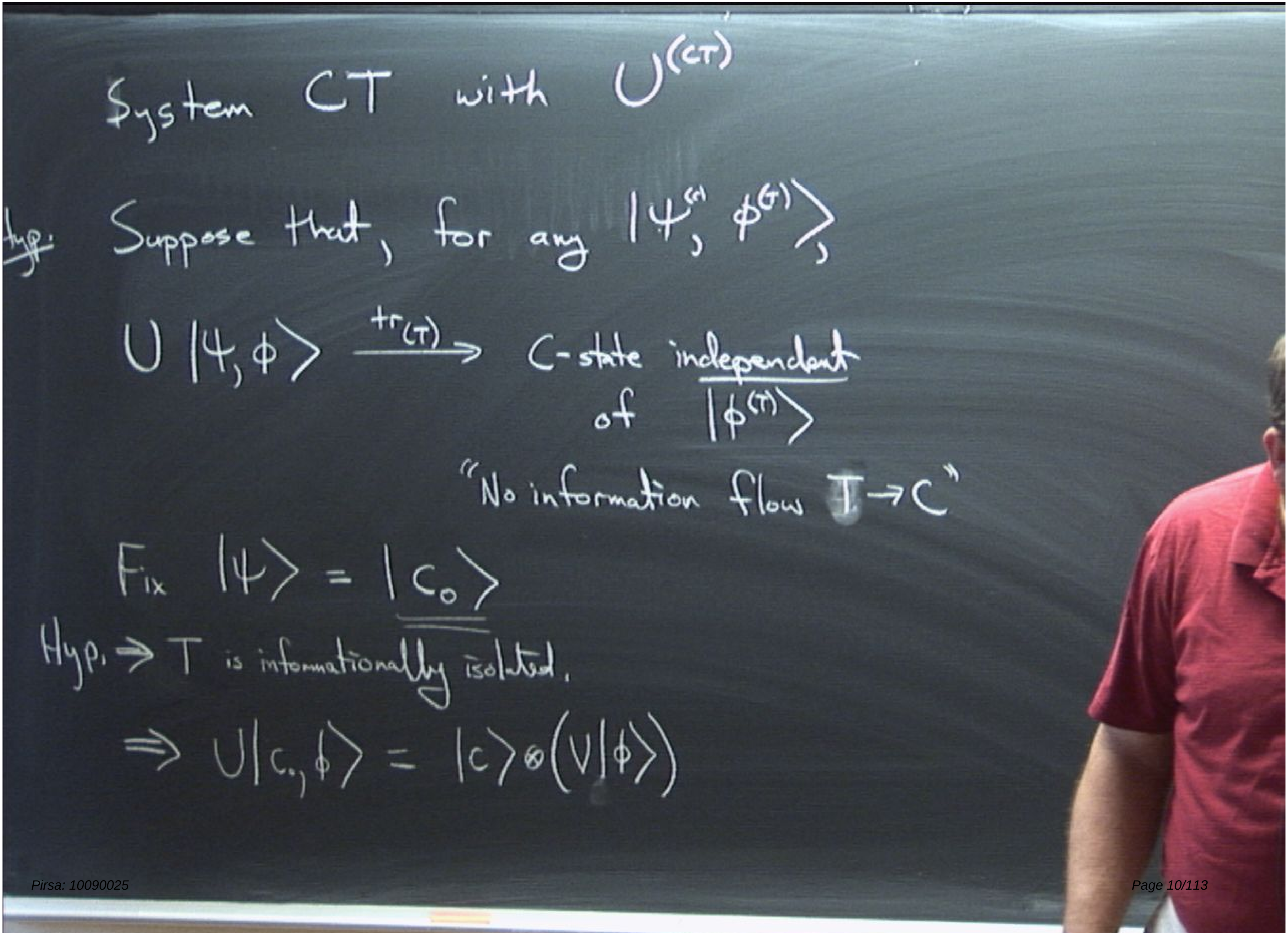
$U|\psi,\phi\rangle \xrightarrow{\mathrm{tr}_{(T)}}$ C-state $\underline{\text{independent}}$ of $|\phi^{(T)}\rangle$

"No information flow T → C"

Fix $|\psi\rangle = |\underline{\underline{c_0}}\rangle$

$\Rightarrow$ T is informationally isolated.

$\Rightarrow$



System CT with $U^{(CT)}$

Hyp: Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

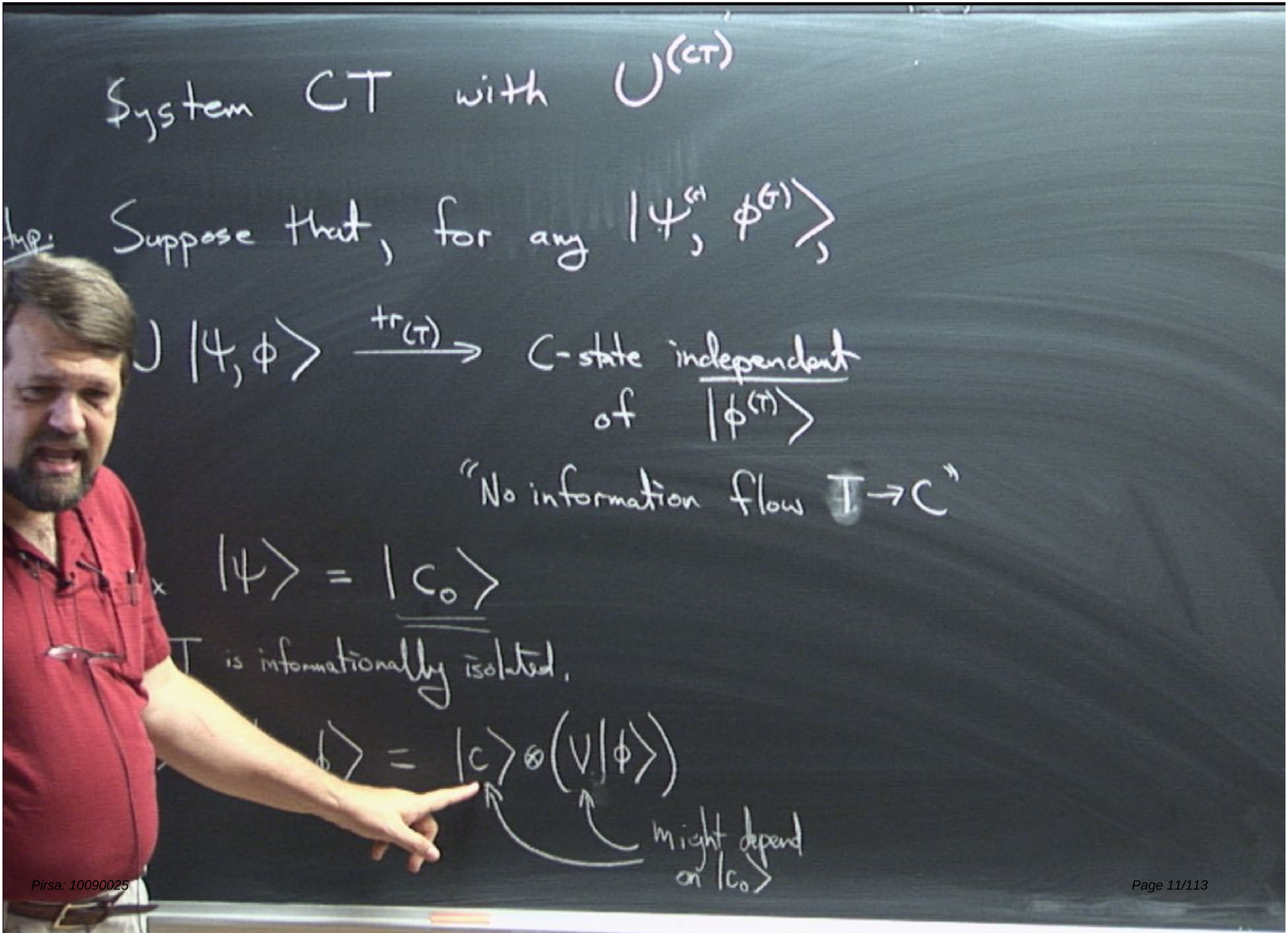
$U|\psi,\phi\rangle \xrightarrow{tr_{(T)}}$ C-state <u>independent</u> of $|\phi^{(T)}\rangle$

"No information flow T→C"

Fix $|\psi\rangle = |\underline{c_0}\rangle$

Hyp. ⇒ T is informationally isolated.

$\Rightarrow U|c_0,\phi\rangle = |c\rangle\otimes\left(V|\phi\rangle\right)$



System CT with $U^{(CT)}$

Hyp: Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$U|\psi,\phi\rangle \xrightarrow{\text{tr}_{(T)}}$ C-state <u>independent</u> of $|\phi^{(T)}\rangle$

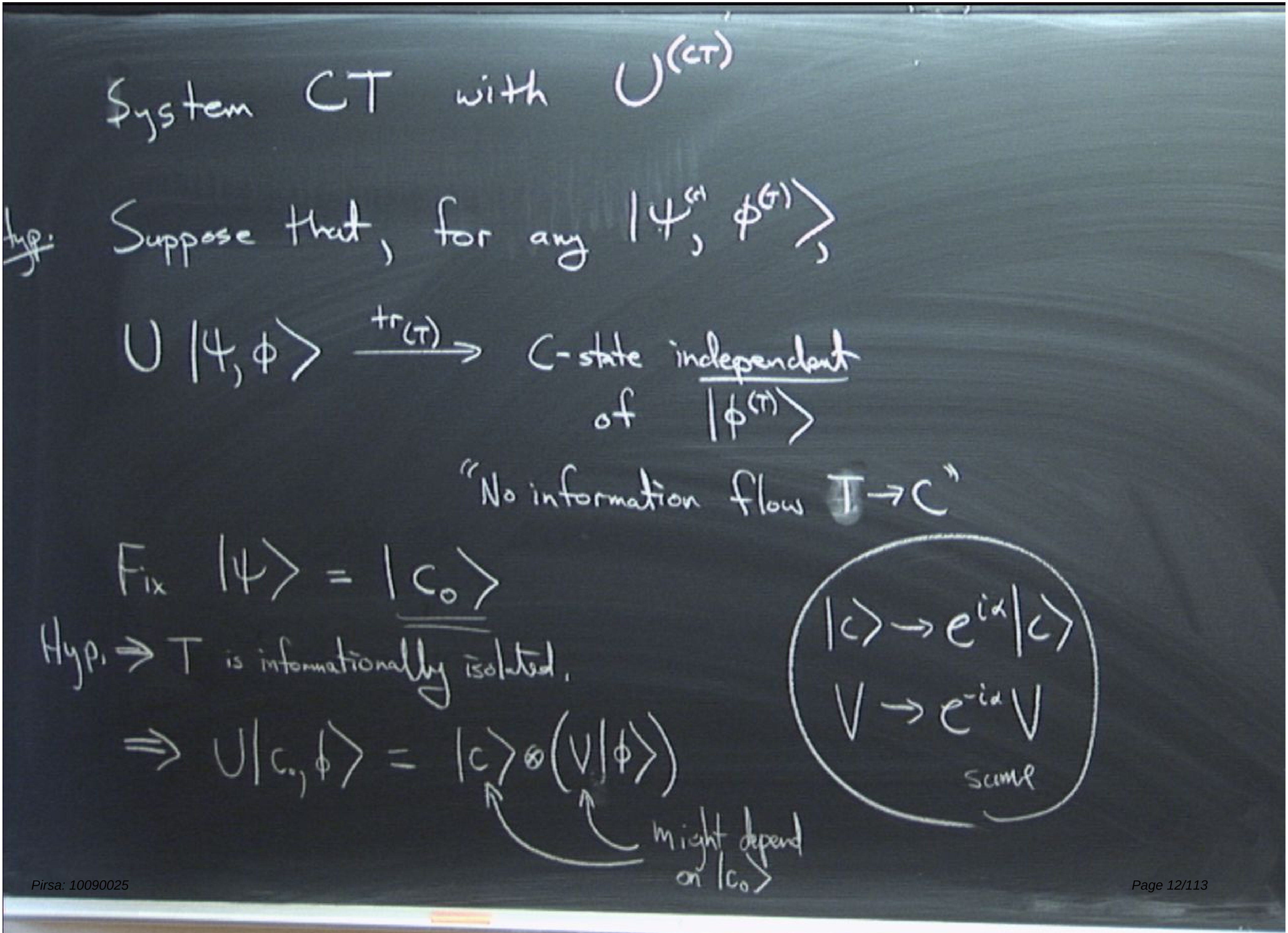
"No information flow T→C"

x $|\psi\rangle = |\underline{\underline{c_0}}\rangle$

T is informationally isolated.

$\phi\rangle = |c\rangle \otimes (V|\phi\rangle)$

might depend on $|c_0\rangle$



System CT with $U^{(CT)}$

Hyp: Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U|\psi,\phi\rangle \xrightarrow{tr_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

"No information flow T → C"

Fix $|\psi\rangle = |\underline{\underline{c_0}}\rangle$

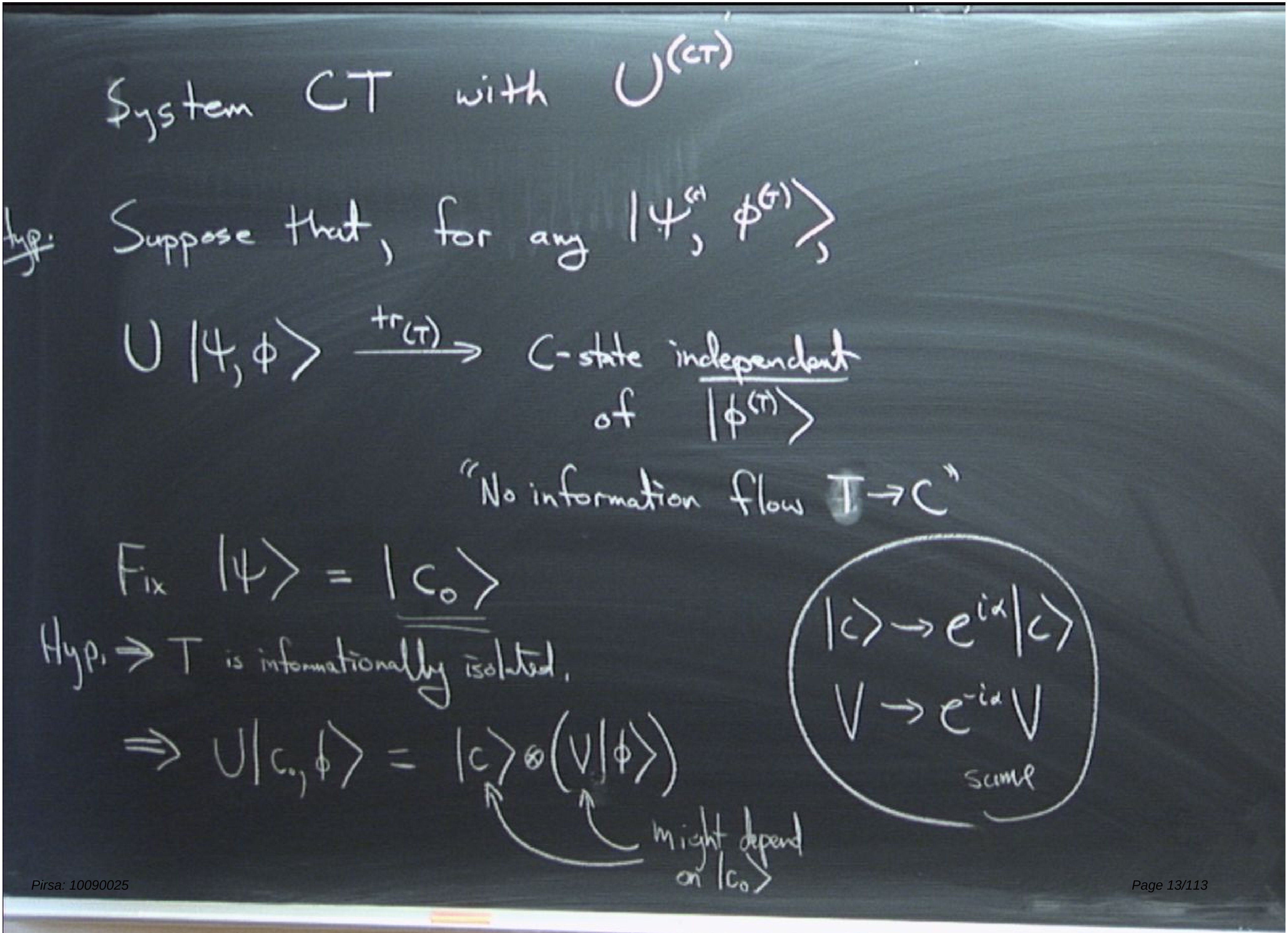
Hyp. ⇒ T is informationally isolated.

$$\Rightarrow U|c_0,\phi\rangle = |c\rangle \otimes (V|\phi\rangle)$$

might depend on $|c_0\rangle$

$$|c\rangle \to e^{i\alpha}|c\rangle$$
$$V \to e^{-i\alpha}V$$

same



System CT with $U^{(CT)}$

Hyp: Suppose that, for any $|\psi^{(C)}, \phi^{(T)}\rangle$,

$$U|\psi,\phi\rangle \xrightarrow{\mathrm{tr}_{(T)}} \text{C-state } \underline{\text{independent}} \text{ of } |\phi^{(T)}\rangle$$

"No information flow T → C"

Fix $|\psi\rangle = |\underline{\underline{c_0}}\rangle$

Hyp. ⇒ T is informationally isolated.

$$\Rightarrow U|c_0,\phi\rangle = |c\rangle \otimes \left(V|\phi\rangle\right)$$

might depend on $|c_0\rangle$

$|c\rangle \to e^{i\alpha}|c\rangle$

$V \to e^{-i\alpha}V$

same

$J \to C$"

$$|c\rangle \to e^{i\alpha}|c\rangle$$

$$V \to e^{-i\alpha} V$$

same

Pick another $|\psi\rangle = |c_0'\rangle$

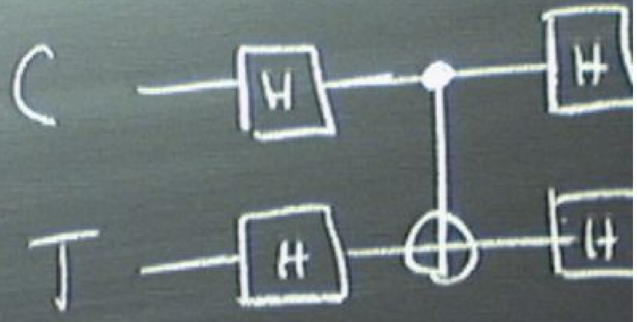
s.t. $\langle c_0|c_0'\rangle \neq 0$

C —

J —

Pick another $|\psi\rangle = |c_0'\rangle$

$\{$ s.t. $\langle c_0|c_0'\rangle \neq 0$

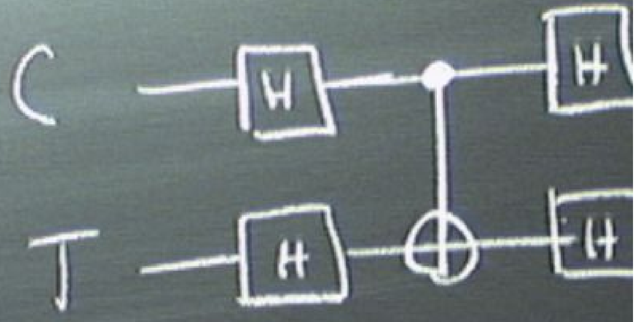


Hyp. $\Longrightarrow$ T is info. iso.

$$\Longrightarrow U|c_0',\phi\rangle = |c'\rangle \otimes \left(V'|\phi\rangle\right)$$

Pick another $|\psi\rangle = |c_0'\rangle$

s.t. $\langle c_0|c_0'\rangle \neq 0$



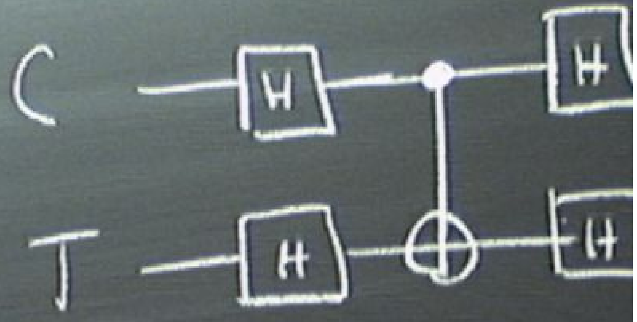
$\Rightarrow$ T is info. iso.

$\Rightarrow U|c_0',\phi\rangle = |c'\rangle\otimes\left(V'|\phi\rangle\right)$

$\phi|U^{\dagger}U|c_0',\phi\rangle$

Pick another $|\psi\rangle = |c_0'\rangle$

s.t. $\langle c_0|c_0'\rangle \neq 0$



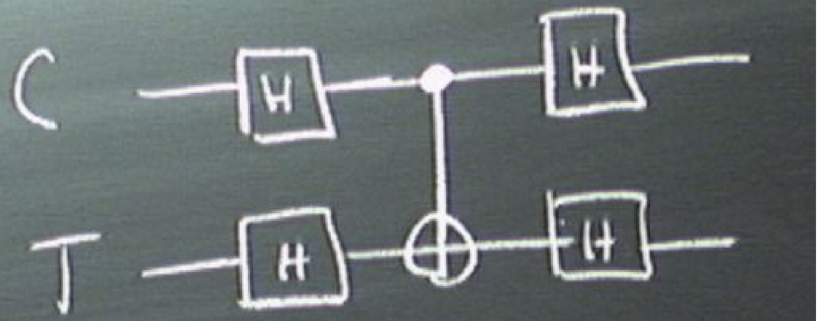
Hyp. $\Longrightarrow$ T is info. iso.

$$\Longrightarrow \boxed{U|c_0',\phi\rangle = |c'\rangle \otimes (V'|\phi\rangle)}$$

$$\begin{array}{l} \langle c_0,\phi|U^\dagger U|c_0',\phi\rangle = \langle c|c'\rangle\langle\phi|V^\dagger V'|\phi\rangle \\ \quad\quad \| \\ \quad \langle c_0|c_0'\rangle \end{array}$$

ick another $|\psi\rangle = |c_0'\rangle$

s.t. $\langle c_0|c_0'\rangle \neq 0$



Hyp. $\Rightarrow$ T is info. iso.

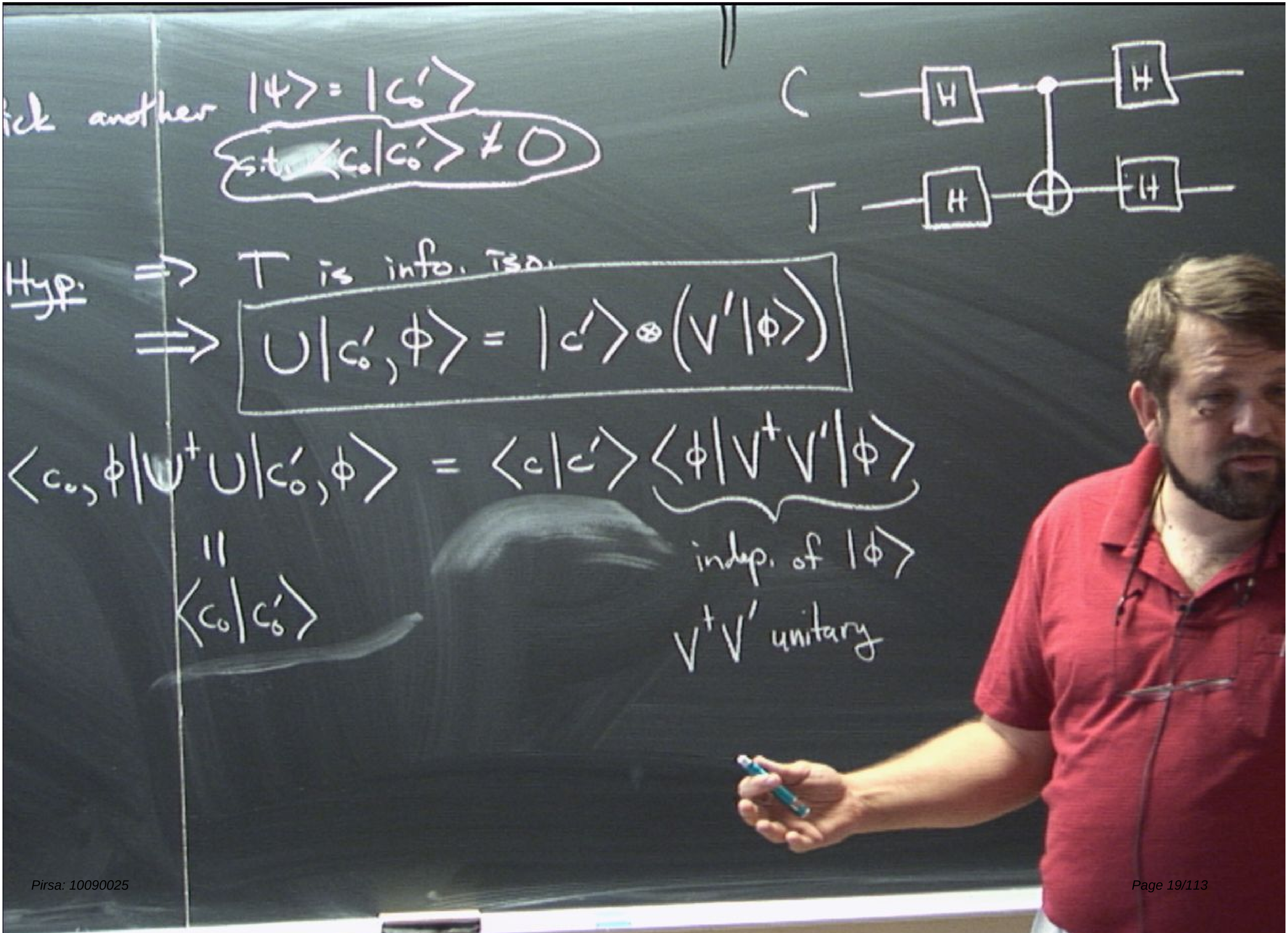
$$\Rightarrow \boxed{U|c_0',\phi\rangle = |c'\rangle \otimes (V'|\phi\rangle)}$$

$$\langle c_0,\phi|U^\dagger U|c_0',\phi\rangle = \langle c|c'\rangle \underbrace{\langle\phi|V^\dagger V'|\phi\rangle}_{\text{indep. of } |\phi\rangle}$$

$$\| $$

$$\langle c_0|c_0'\rangle$$

$V^\dagger V'$ unitary



ick another $|\psi\rangle = |c_0'\rangle$

$\{$s.t. $\langle c_0|c_0'\rangle \neq 0$

Hyp. $\Rightarrow$ T is info. iso.

$$\Rightarrow \boxed{U|c_0', \phi\rangle = |c'\rangle \otimes \left(V'|\phi\rangle\right)}$$

$$\langle c_0, \phi|U^{\dagger}U|c_0', \phi\rangle = \langle c|c'\rangle \underbrace{\langle \phi|V^{\dagger}V'|\phi\rangle}_{\text{indep. of } |\phi\rangle}$$

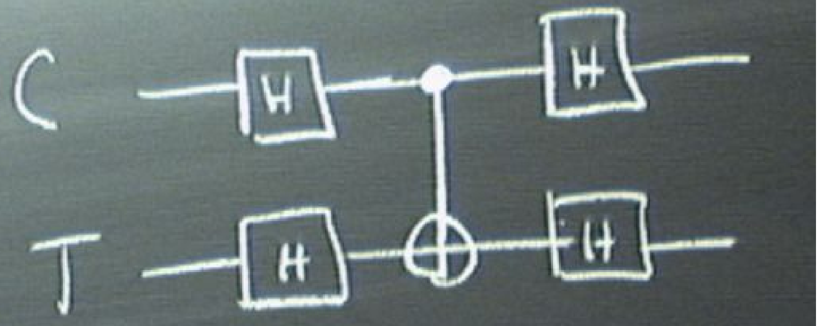
$$\| $$

$$\langle c_0|c_0'\rangle$$

$V^{\dagger}V'$ unitary

ick another $|\psi\rangle = |c_0'\rangle$

s.t. $\langle c_0|c_0'\rangle \neq 0$



Hyp. $\Longrightarrow$ T is info. iso.

$$\Longrightarrow \boxed{U|c_0',\phi\rangle = |c'\rangle \otimes \left(V'|\phi\rangle\right)}$$

$V' \to e^{-i}$

$|c'\rangle$

$$\langle c_0,\phi|U^\dagger U|c_0',\phi\rangle = \langle c|c'\rangle \underbrace{\langle\phi|V^\dagger V'|\phi\rangle}_{\text{indep. of } |\phi\rangle}$$

$$\|$$

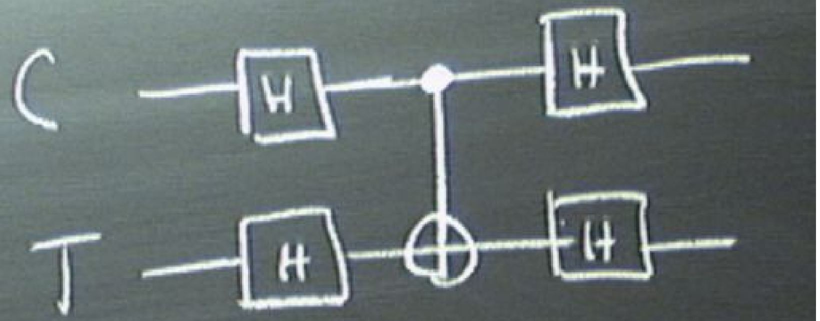
$$\langle c_0|c_0'\rangle$$

$V^\dagger V'$ unitary

$e^{i\alpha}$

ick another $|\psi\rangle = |c_0'\rangle$

s.t. $\langle c_0|c_0'\rangle \neq 0$



Hyp. $\Rightarrow$ T is info. iso.

$\Rightarrow$ $\boxed{U|c_0',\phi\rangle = |c'\rangle \otimes (V'|\phi\rangle)}$

$V' \longrightarrow e$

$|c'\rangle \longrightarrow e$

$$\langle c_0,\phi|U^\dagger U|c_0',\phi\rangle = \langle c|c'\rangle \underbrace{\langle\phi|V^\dagger V'|\phi\rangle}_{\text{indep. of } |\phi\rangle}$$

$\|$

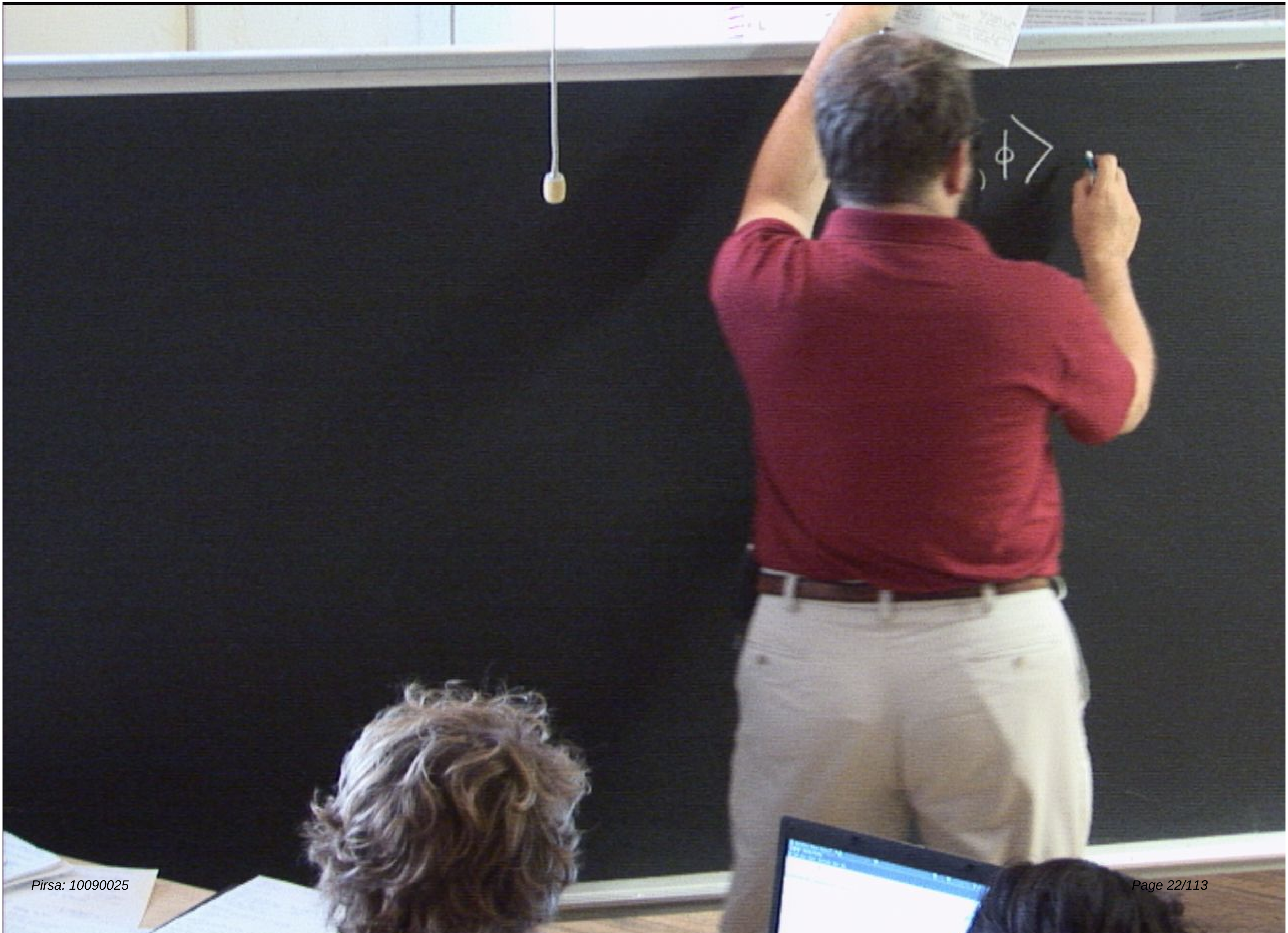
$\langle c_0|c_0'\rangle$

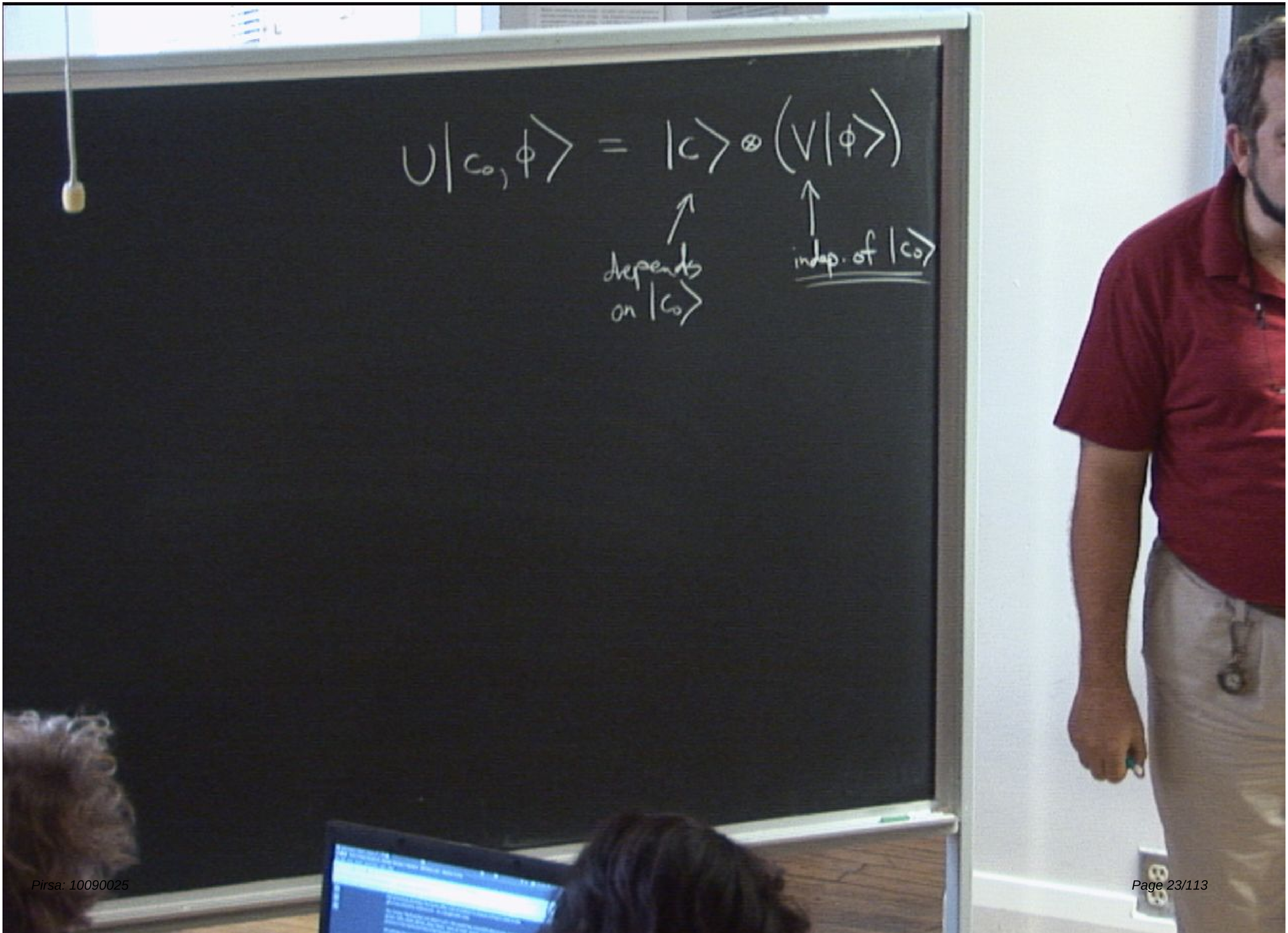
$V^\dagger V'$ unitary

$e^{i\alpha}$

Now: $\langle\phi|V^\dagger V'$

$V^\dagger$

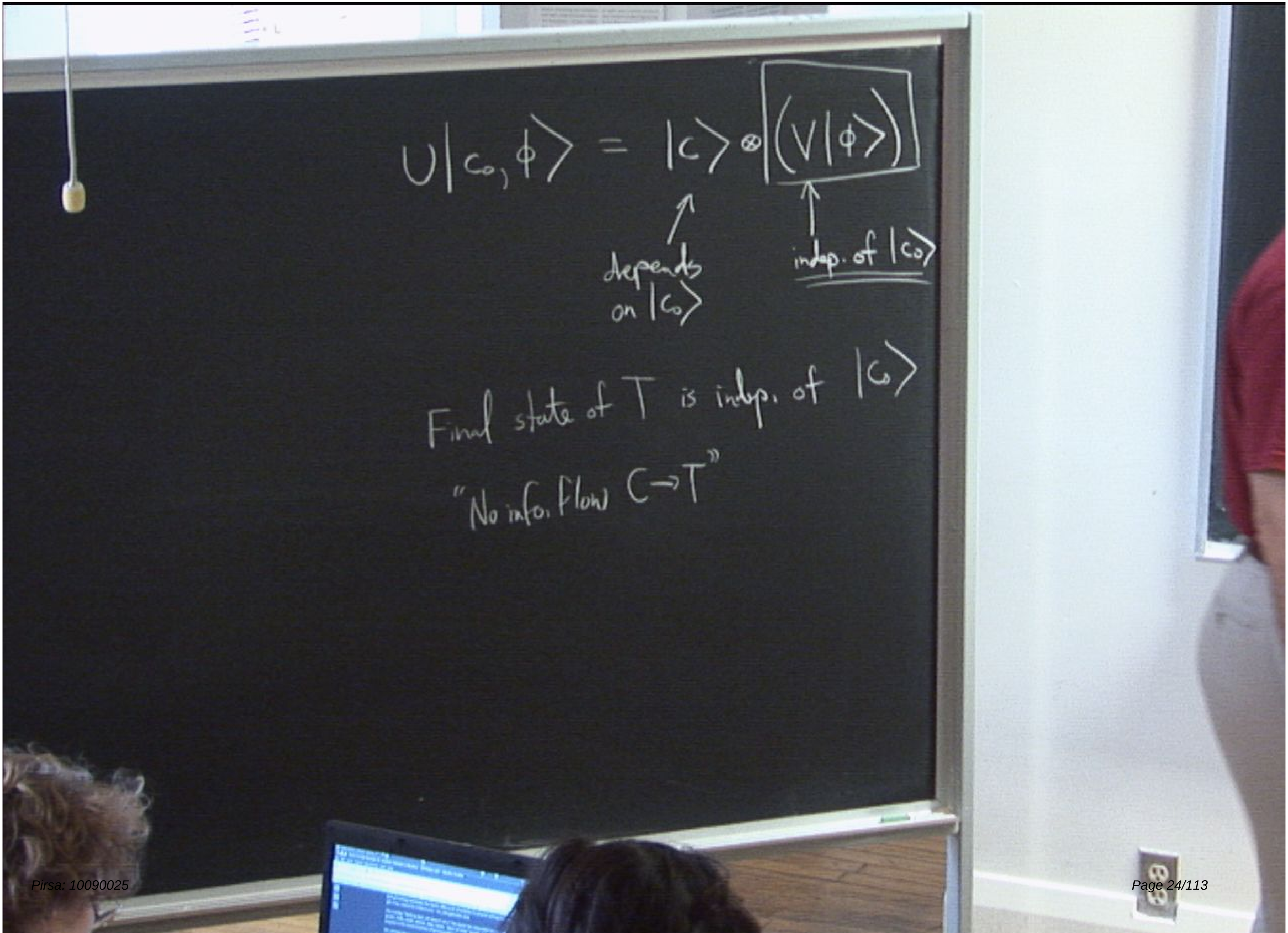

, ϕ⟩



$$U|c_0,\phi\rangle = |c\rangle \otimes \left(V|\phi\rangle\right)$$

depends on $|c_0\rangle$

indep. of $|c_0\rangle$



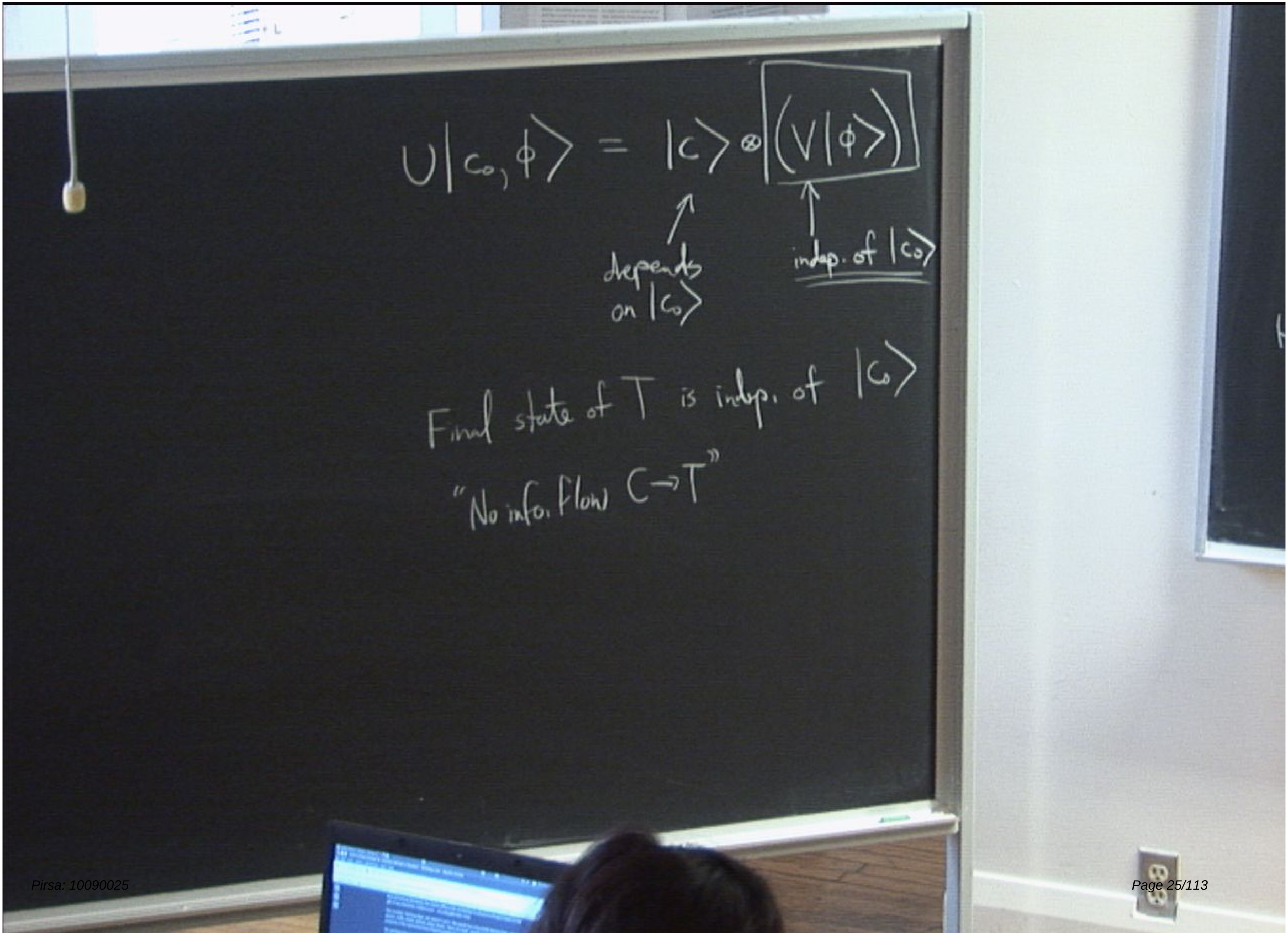
$$U|c_0,\phi\rangle = |c\rangle \otimes \boxed{(V|\phi\rangle)}$$

depends on $|c_0\rangle$

indep. of $|c_0\rangle$

Final state of T is indep. of $|c_0\rangle$

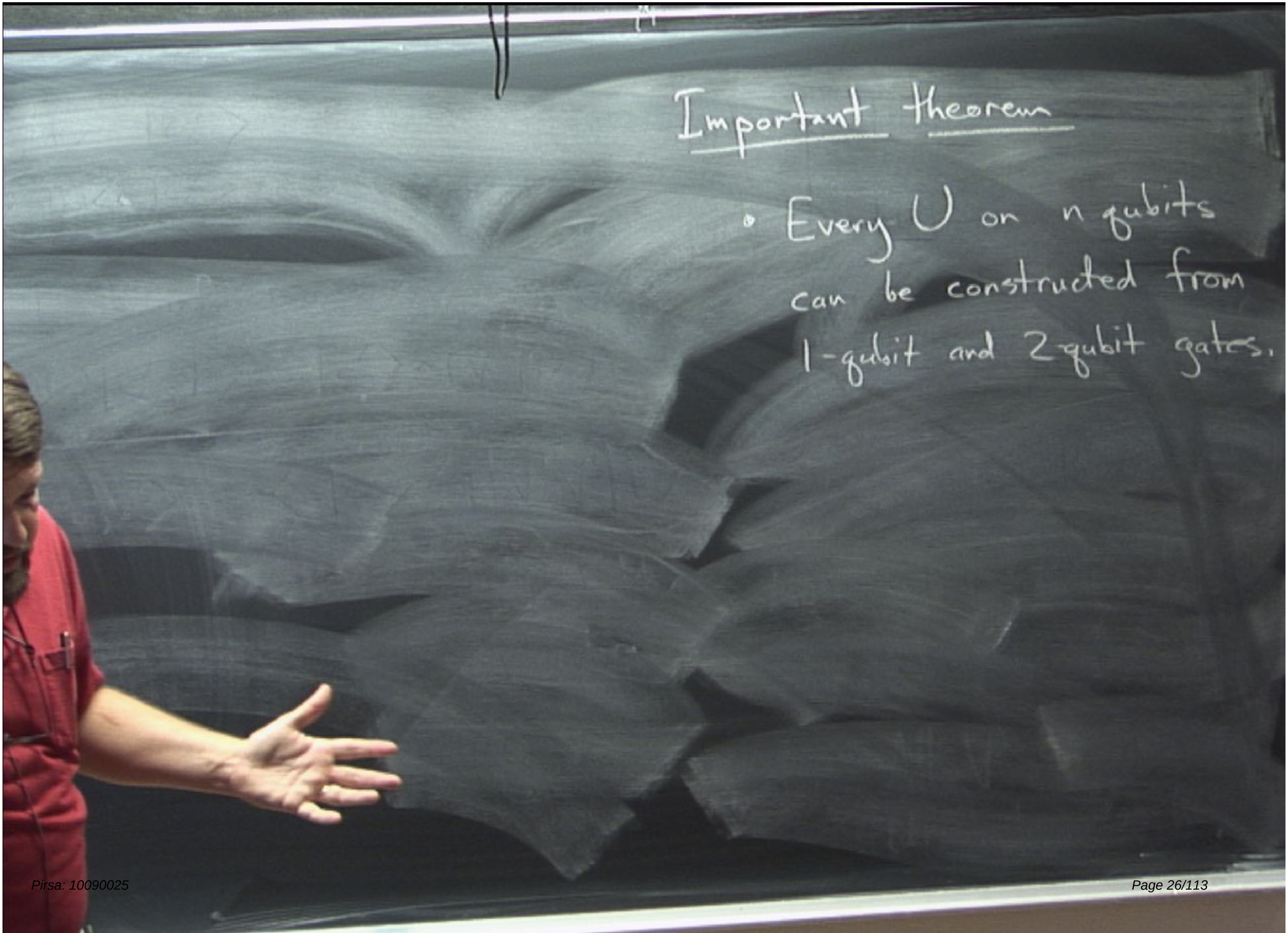
"No info. flow C → T"



$$U|c_0,\phi\rangle = \underset{\substack{\uparrow \\ \text{depends} \\ \text{on } |c_0\rangle}}{|c\rangle} \otimes \underset{\substack{\uparrow \\ \text{indep. of } |c_0\rangle}}{\boxed{(V|\phi\rangle)}}$$

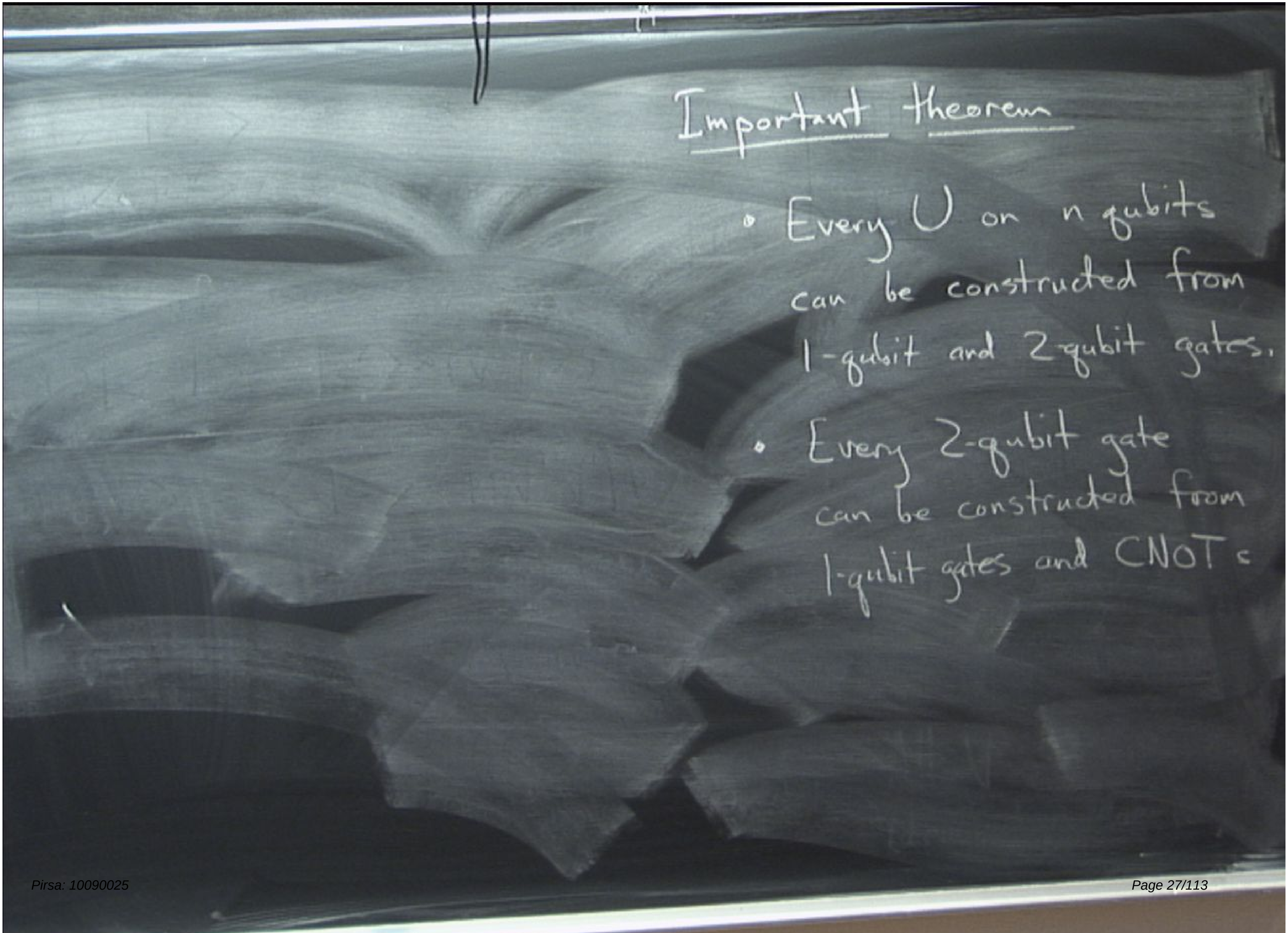
Final state of T is indp. of $|c_0\rangle$

"No info. flow $C \to T$"



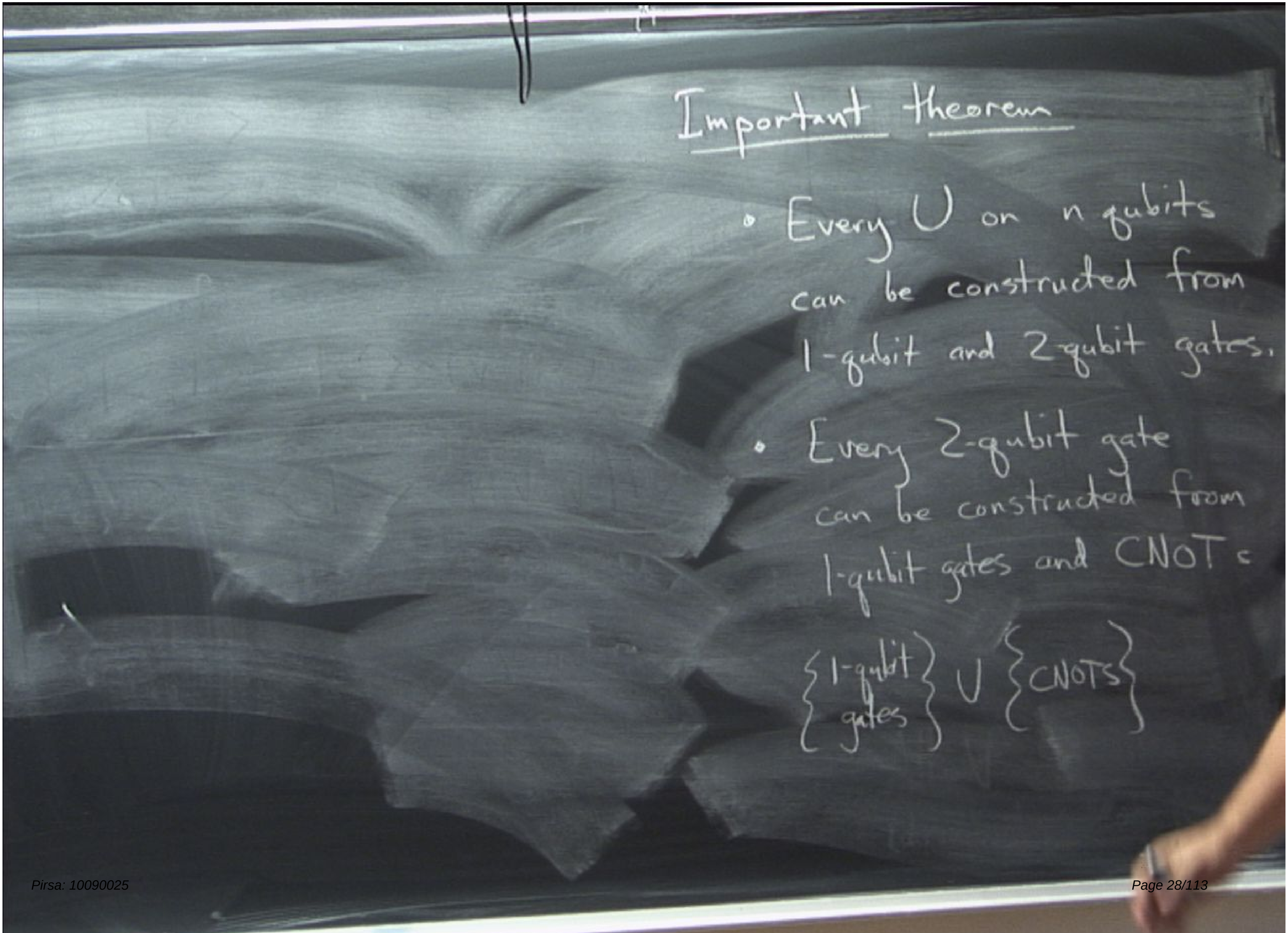
Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.



Important theorem

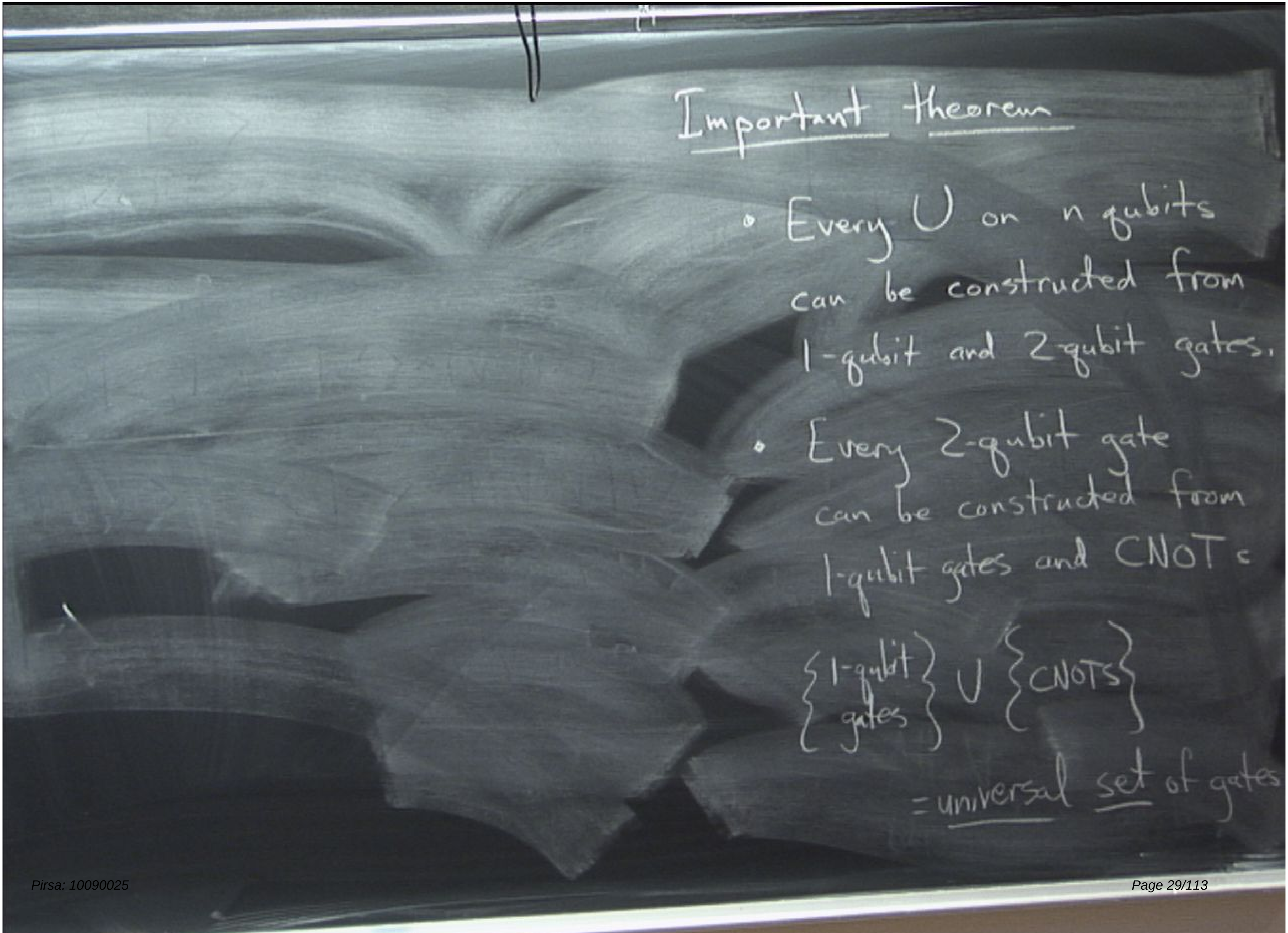
- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$$\left\{\begin{matrix}\text{1-qubit} \\ \text{gates}\end{matrix}\right\} \cup \left\{\text{CNOTs}\right\}$$

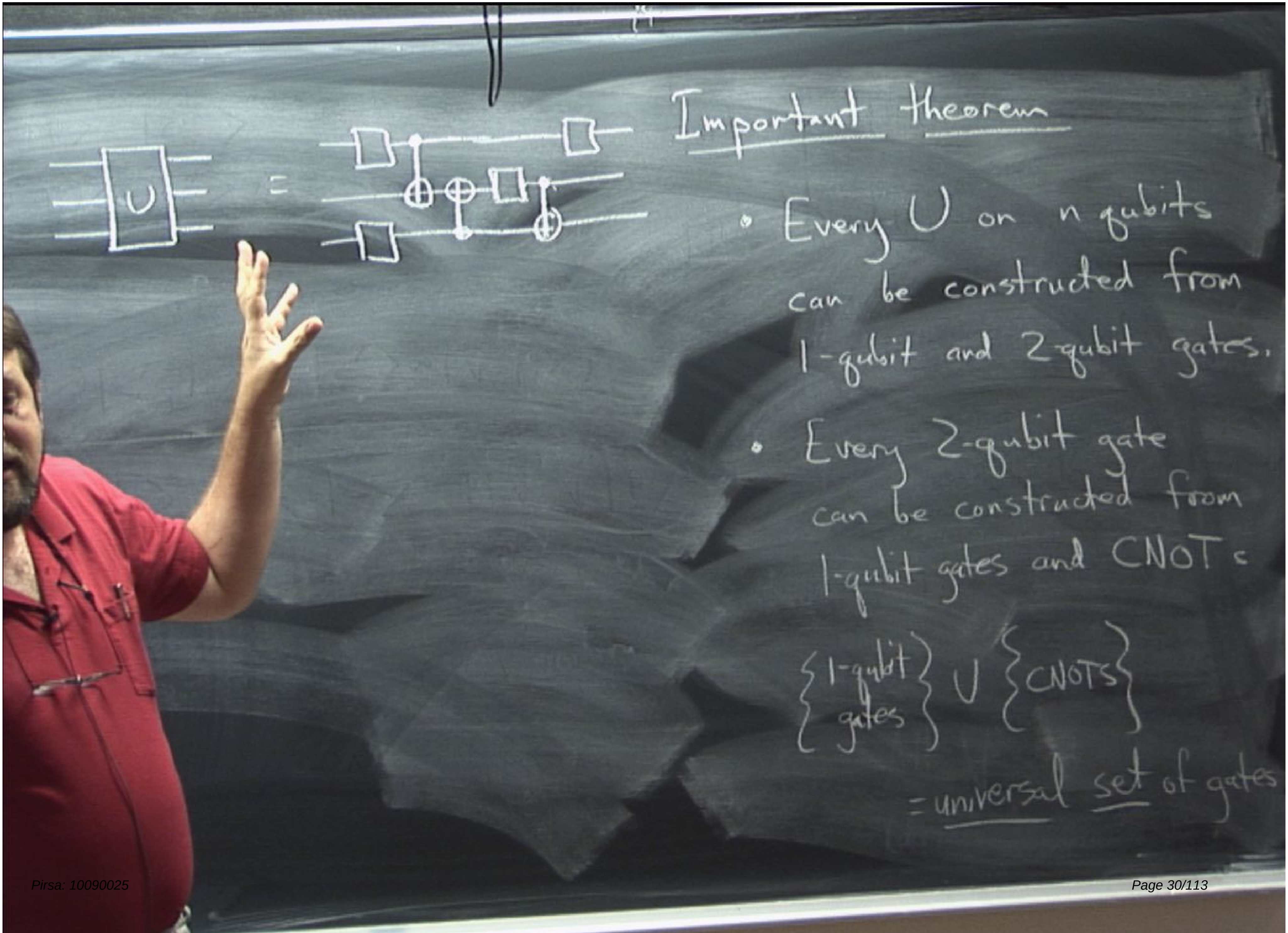


Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$$\begin{Bmatrix}\text{1-qubit}\\ \text{gates}\end{Bmatrix} \cup \begin{Bmatrix}\text{CNOTS}\end{Bmatrix}$$

= universal set of gates

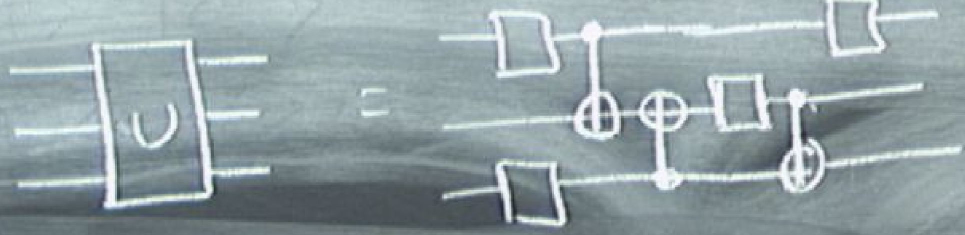


Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$\left\{\begin{matrix}\text{1-qubit} \\ \text{gates}\end{matrix}\right\} \cup \left\{\text{CNOTS}\right\}$

= universal set of gates

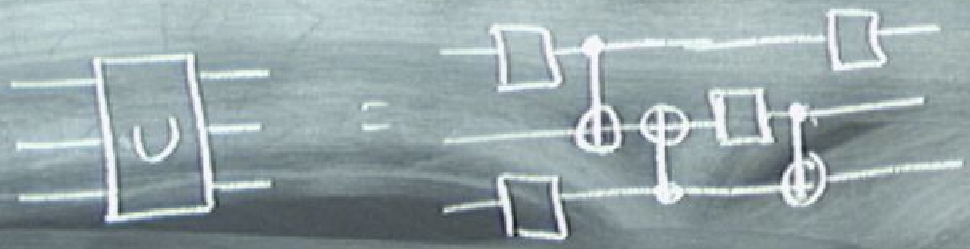


Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$$\left\{\begin{matrix}\text{1-qubit}\\ \text{gates}\end{matrix}\right\} \cup \left\{\text{CNOTS}\right\}$$

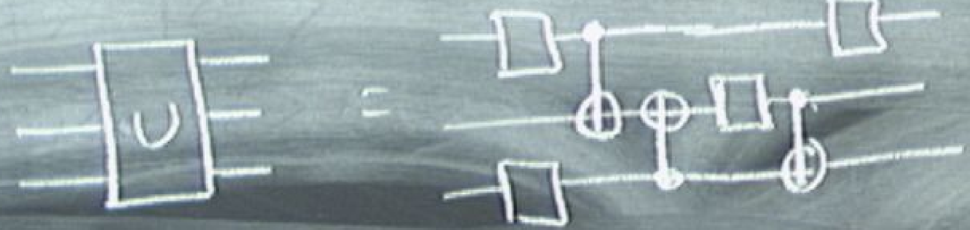
$=$ <u>universal</u> <u>set</u> of gates



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

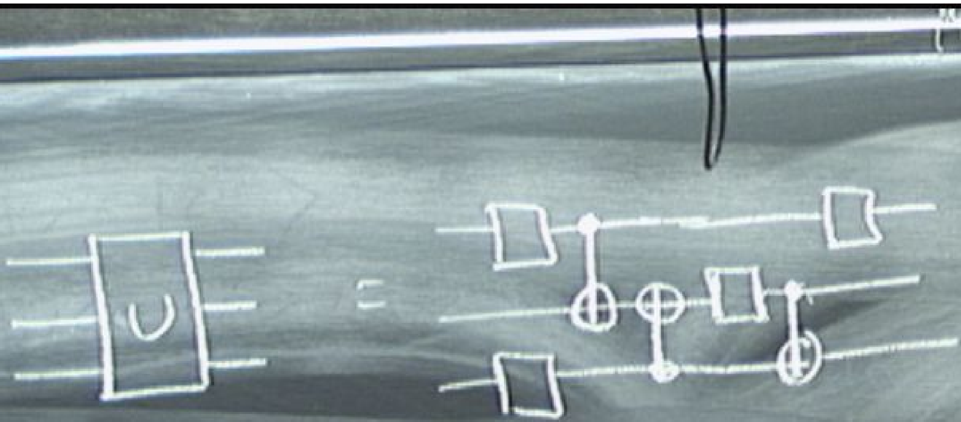
$$\boxed{\begin{gathered}\left\{\begin{matrix}\text{1-qubit}\\ \text{gates}\end{matrix}\right\} \cup \left\{\text{CNOT}\right\}\\ = \underline{\text{universal}}\ \underline{\text{set}}\ \text{of gates}\end{gathered}}$$



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

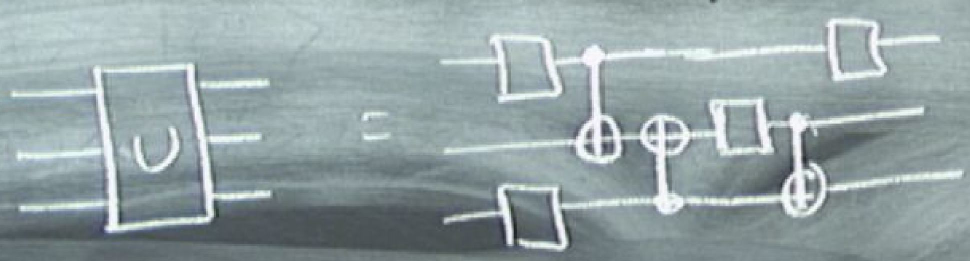
$$\boxed{\begin{array}{c}\left\{\begin{array}{c}\text{1-qubit}\\ \text{gates}\end{array}\right\} \cup \{\text{CNOTS}\}\\ = \underline{\text{universal}}\ \underline{\text{set}}\ \text{of gates}\end{array}}$$



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$$\boxed{\left\{\begin{matrix}\text{1-qubit}\\ \text{gates}\end{matrix}\right\} \cup \left\{\text{CNOTS}\right\} = \underline{\text{universal}}\ \underline{\text{set}}\ \text{of gates}}$$

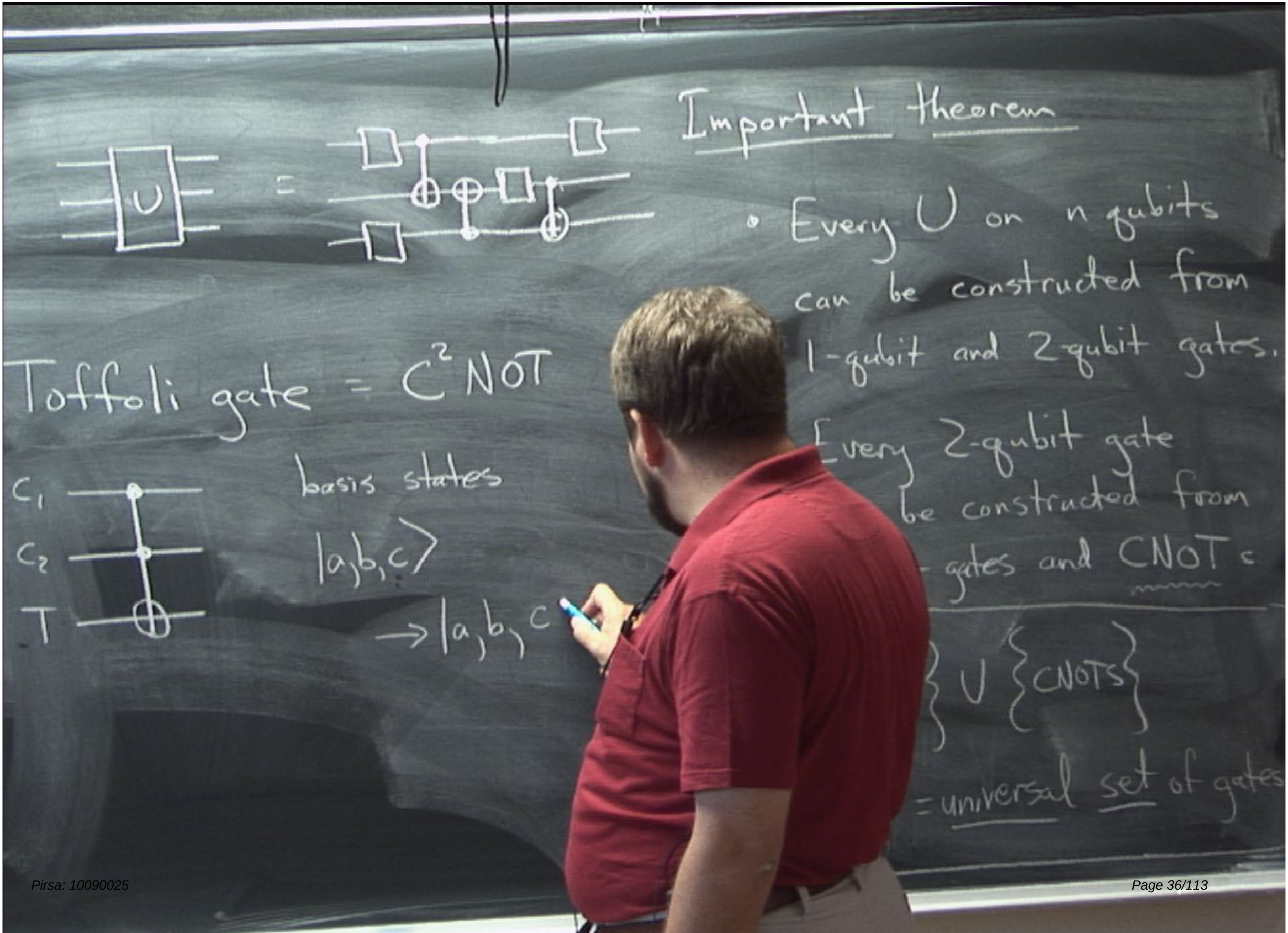


Toffoli gate = C^2NOT

Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

$$\boxed{\begin{Bmatrix}\text{1-qubit}\\ \text{gates}\end{Bmatrix} \cup \{\text{CNOTS}\} = \underline{\text{universal}}\ \underline{\text{set}} \text{ of gates}}$$



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.

Every 2-qubit gate
be constructed from
gates and CNOTs

$\} U \{ CNOTS \}$

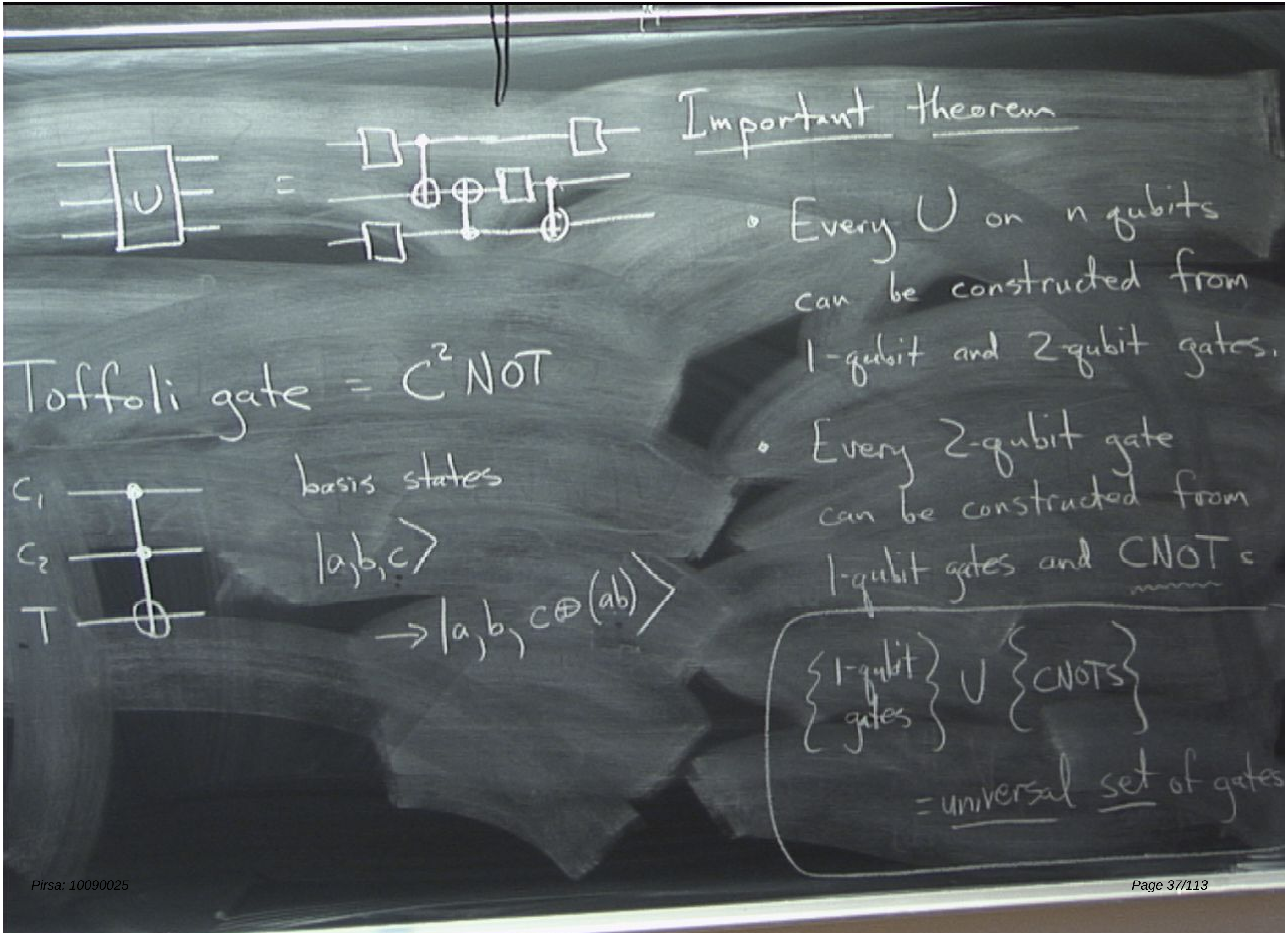
= universal set of gates

Toffoli gate = C^2NOT

basis states

$|a,b,c\rangle$

$\rightarrow |a,b,c$



Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

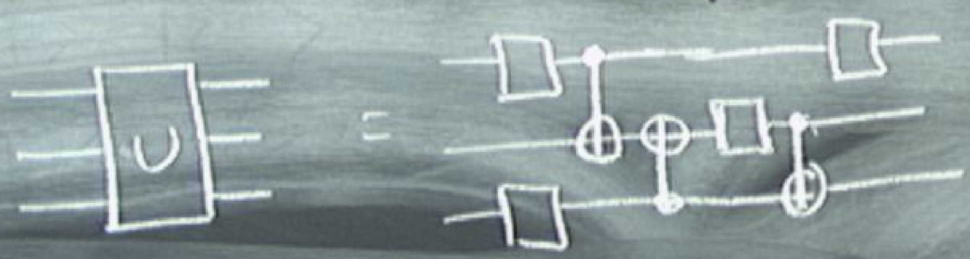
$\{\text{1-qubit gates}\} \cup \{\text{CNOTS}\}$ = universal set of gates

Toffoli gate = C^2NOT

basis states

$|a,b,c\rangle$

$\rightarrow |a,b,c\oplus(ab)\rangle$

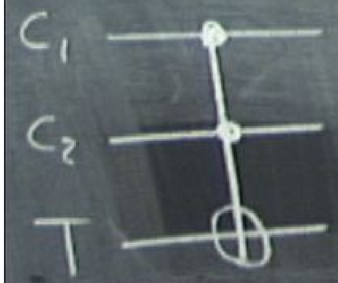


Important theorem

- Every U on n qubits can be constructed from 1-qubit and 2-qubit gates.
- Every 2-qubit gate can be constructed from 1-qubit gates and CNOTs

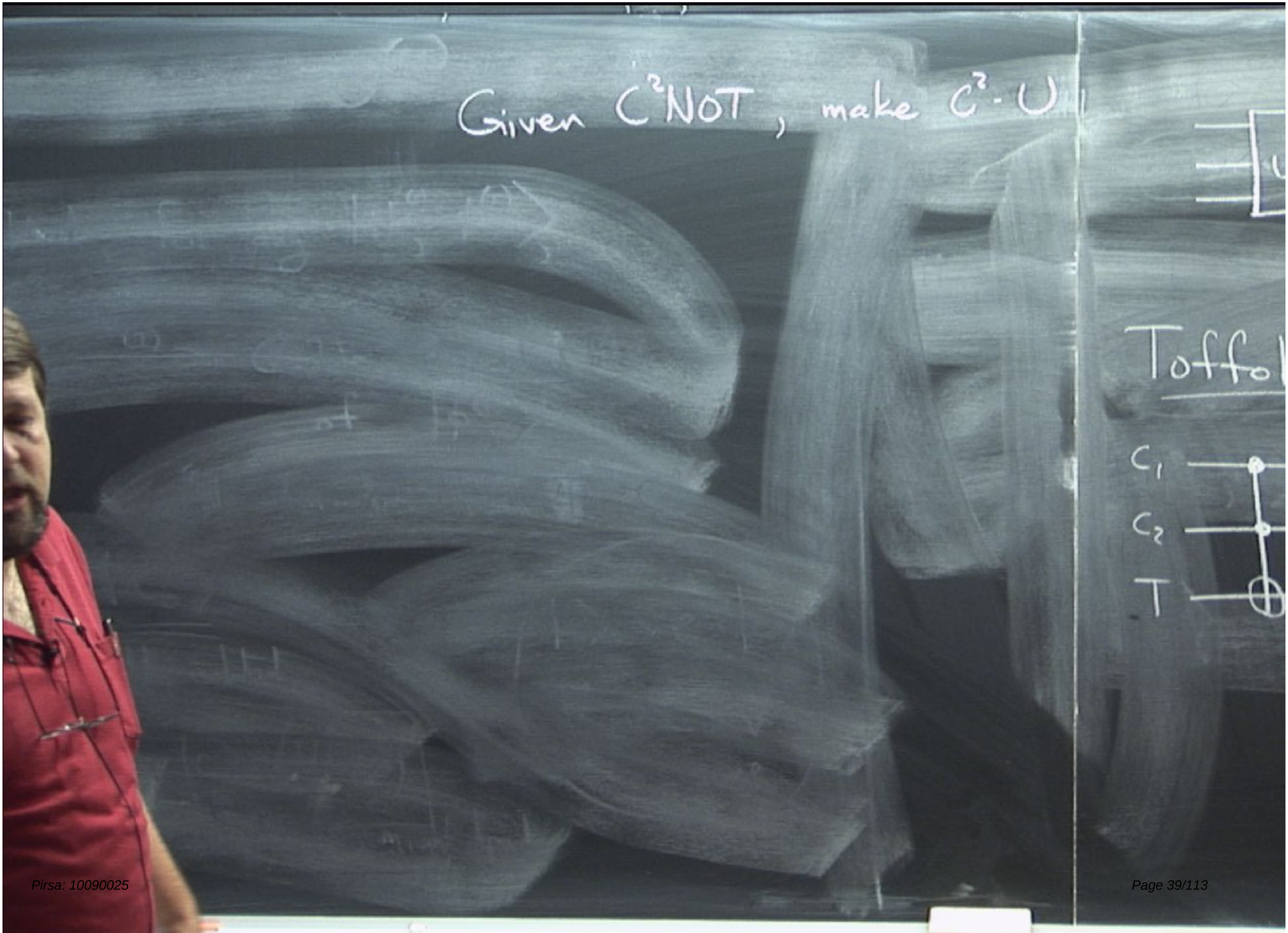
$$\boxed{\begin{Bmatrix}\text{1-qubit}\\ \text{gates}\end{Bmatrix} \cup \{\text{CNOTs}\} = \underline{\text{universal}}\ \underline{\text{set}} \text{ of gates}}$$

Toffoli gate = C^2NOT



basis states

$$|a,b,c\rangle \rightarrow |a,b,c\oplus(ab)\rangle$$

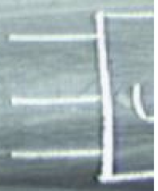


Given C^2NOT, make $C^2 \cdot U$

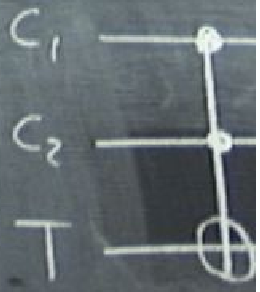
Toffol

Given C^2NOT, make C^2-U

(assume we have C-U)



Toffo

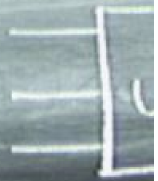


Given C^2NOT, make $C^2\text{-}U$

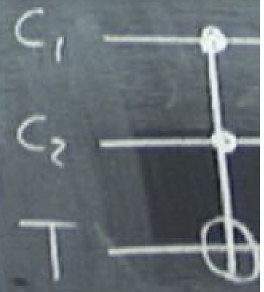
(assume we have $C\text{-}U$)

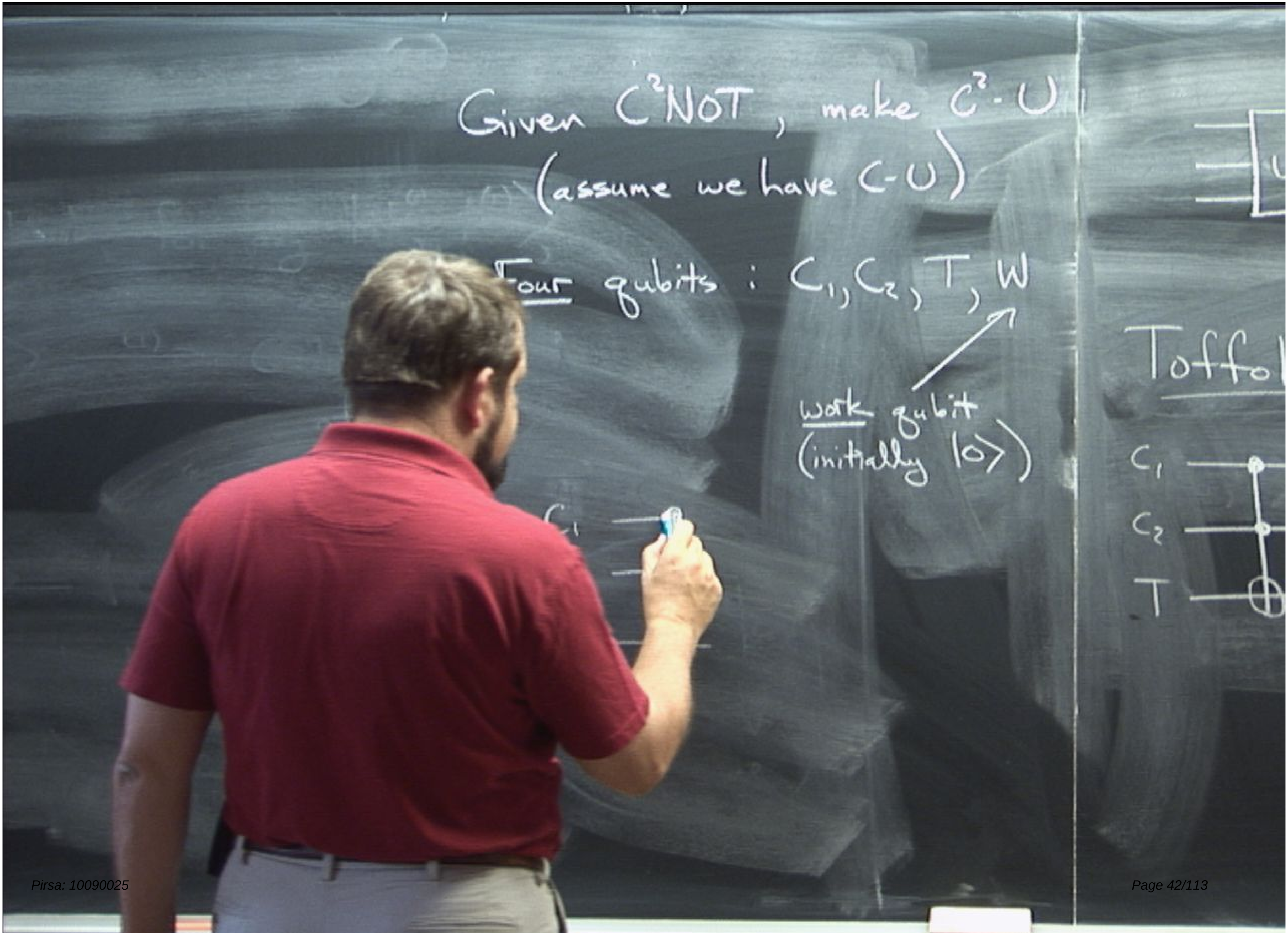
Four qubits : C_1, C_2, T, W

work qubit
(initially $|0\rangle$)



Toffol





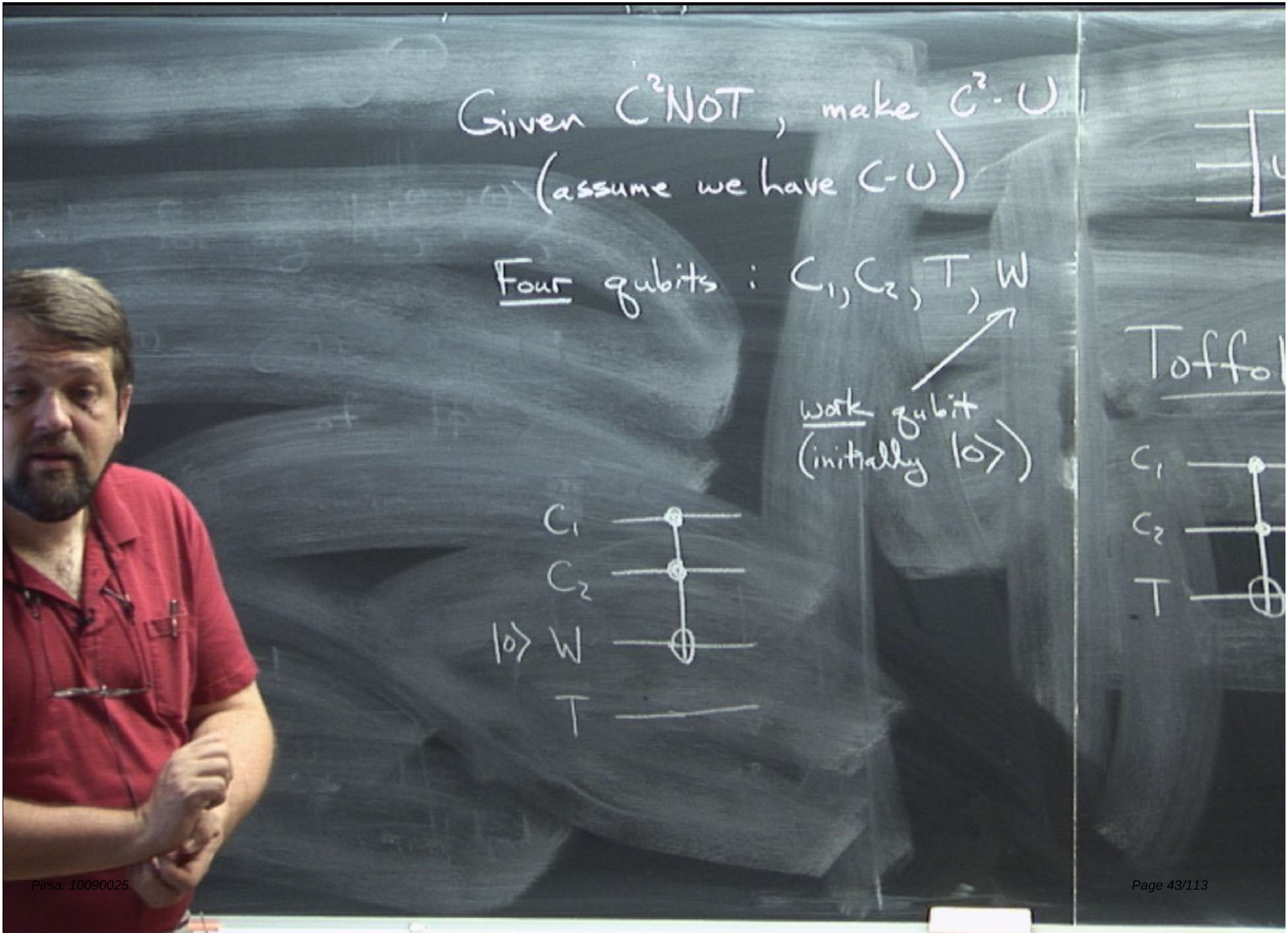
Given C^2NOT, make $C^2\text{-}U$

(assume we have $C\text{-}U$)

Four qubits : C_1, C_2, T, W

work qubit

(initially $|0\rangle$)

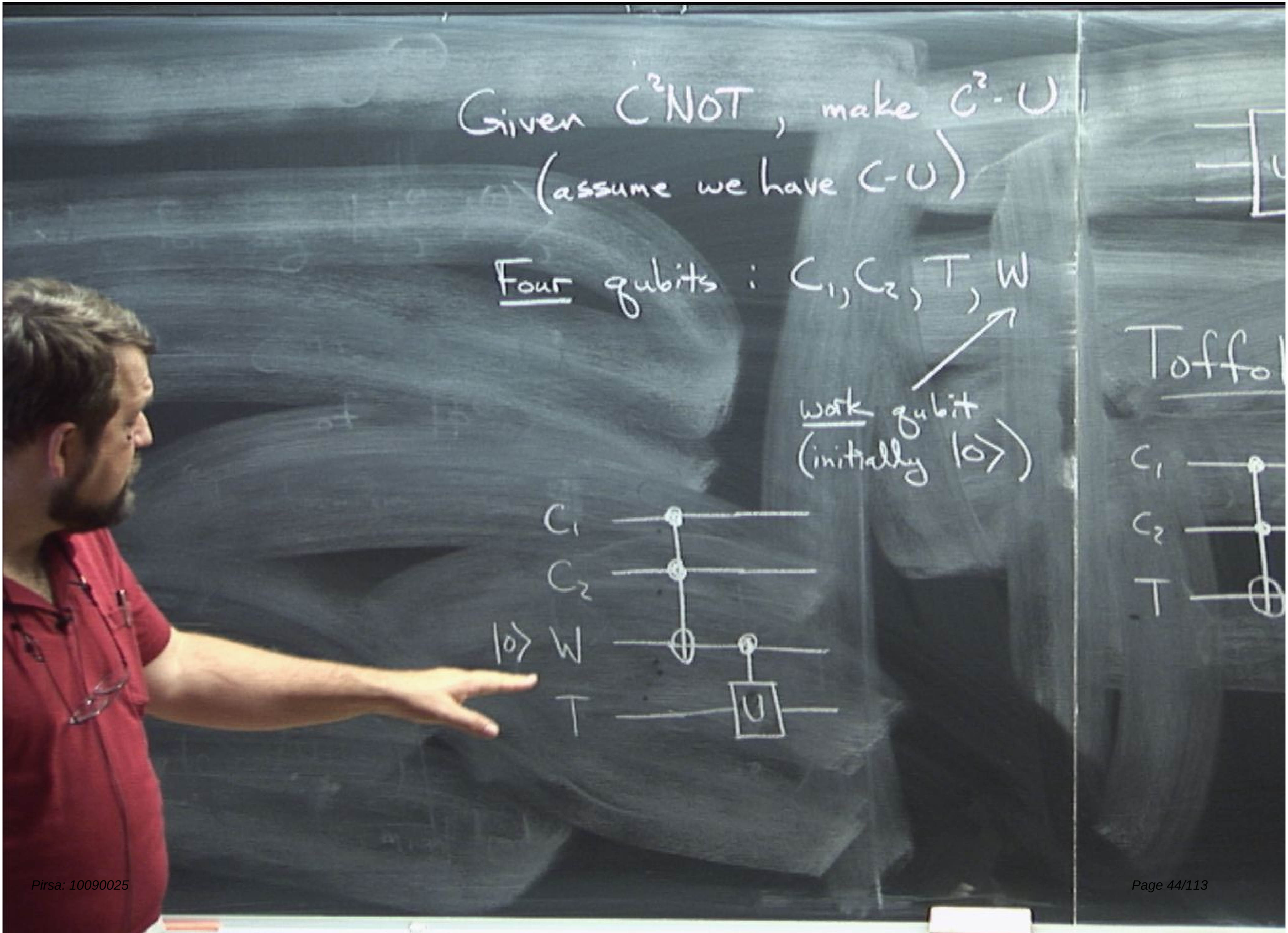


Given C^2NOT, make $C^2\text{-}U$

(assume we have $C\text{-}U$)

__Four__ qubits : C_1, C_2, T, W

__work__ qubit
(initially $|0\rangle$)



Given C^2NOT, make C^2-U

(assume we have C-U)

Four qubits : C_1, C_2, T, W

work qubit

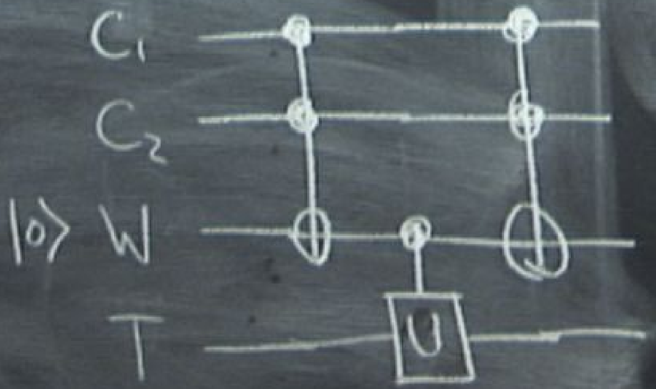
(initially $|0\rangle$)

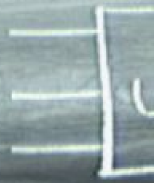
Given C^2NOT, make C^2-U

(assume we have C-U)

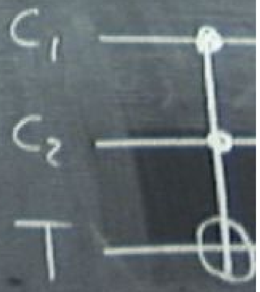
Four qubits : C_1, C_2, T, W

work qubit
(initially $|0\rangle$)





Toffo



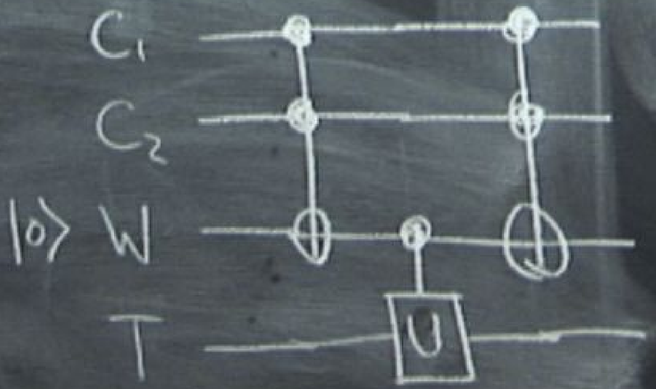
Given C^2NOT, make C^2-U

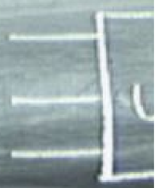
(assume we have C-U)

<u>Four</u> qubits : C_1, C_2, T, W

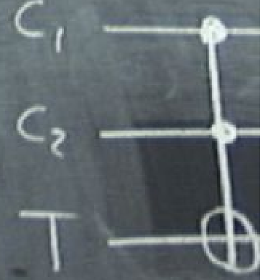
work qubit

(initially $|0\rangle$)





Toffol



initial states

$|a,b,c\rangle \otimes |\phi\rangle$

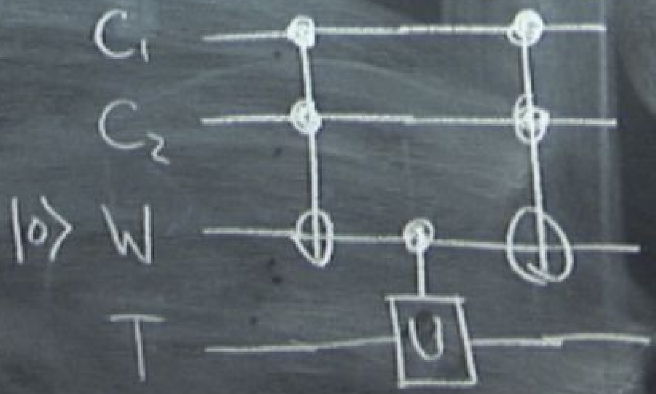
$C_1 \; C_2 \; W \quad T$

Given C^2NOT, make C^2-U

(assume we have C-U)

Four qubits : C_1, C_2, T, W

work qubit
(initially $|0\rangle$)



initial states

$$|a,b,0\rangle \otimes |\phi\rangle$$

$$C_1 \; C_2 \; W \qquad T$$

$$a,b,0\rangle \otimes |\phi\rangle \rightarrow |a,b,ab\rangle \otimes |\phi\rangle$$

$$\rightarrow$$

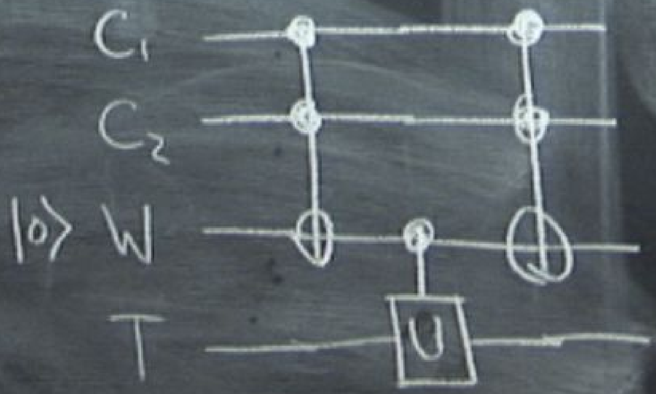
Given C^2NOT, make C^2-U

(assume we have C-U)

Four qubits : C_1, C_2, T, W

work qubit

(initially $|0\rangle$)



initial states

$$|a, b, 0\rangle \otimes |\phi\rangle$$

$C_1 \; C_2 \; W \qquad T$

$$|a,b,0\rangle \otimes |\phi\rangle \rightarrow |a,b,ab\rangle \otimes |\phi\rangle$$

$$\rightarrow |a,b,ab\rangle \otimes U$$

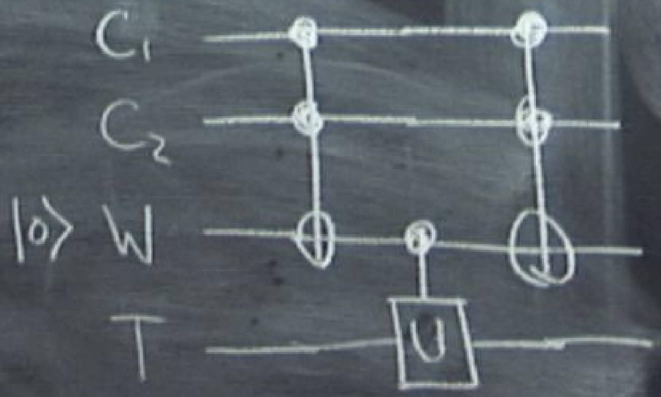
Given C^2NOT, make C^2

(assume we have C-U)

Four qubits : $C_1, C_2, T,$

work qubit

(initially $|0\rangle$



initial states

$$|a,b,0\rangle \otimes |\phi\rangle$$

C_1 C_2 W T

$$a,b,0\rangle \otimes |\phi\rangle \to |a,b,ab\rangle \otimes |\phi\rangle$$

$$\to |a,b,ab\rangle \otimes U^{ab}|\phi\rangle$$

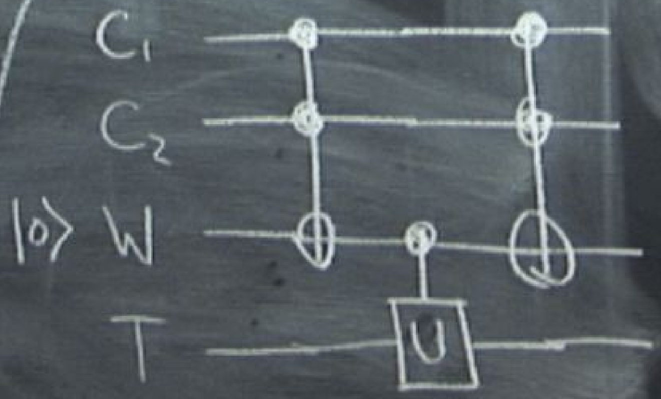
Given C^2NOT, make C^2

(assume we have C-U)

Four qubits: $C_1, C_2, T,$

work qubit

(initially $|0\rangle$



initial states

$|a,b,0\rangle \otimes |\phi\rangle$

$C_1 \ C_2 \ W \qquad T$

$|a,b,0\rangle \otimes |\phi\rangle \rightarrow |a,b,ab\rangle \otimes |\phi\rangle$

$\rightarrow |a,b,ab\rangle \otimes U^{ab}|\phi\rangle$

$\rightarrow |a,b,\underline{ab \oplus ab}\rangle \otimes U^{ab}|\phi\rangle$

$= |a,b,0\rangle \otimes U^{ab}|\phi\rangle$

✓

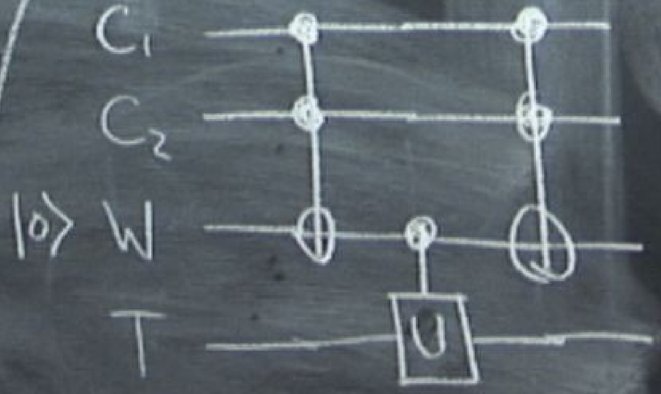
Given C^2NOT, make C^2

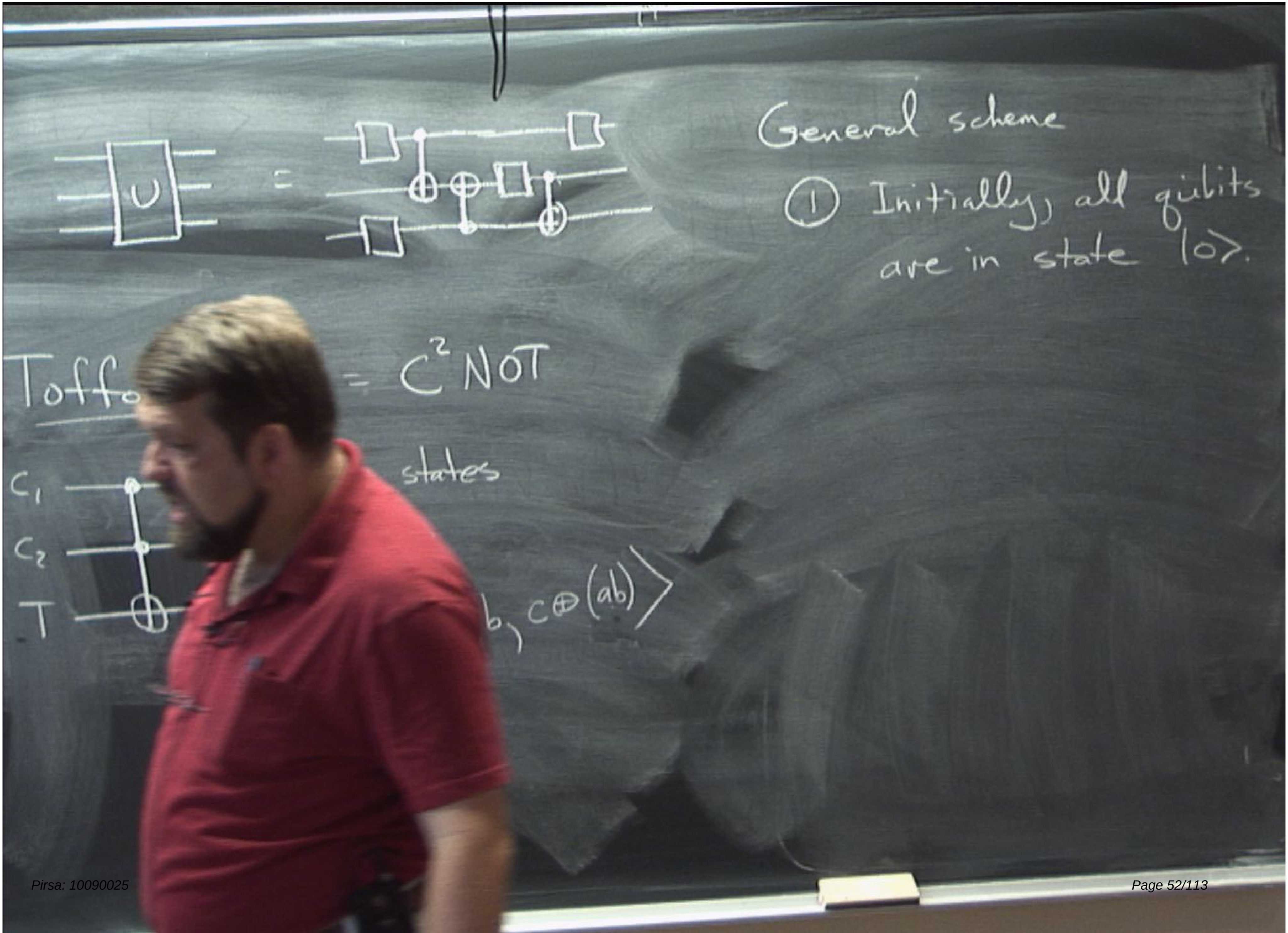
(assume we have C-U)

Four qubits : $C_1, C_2, T,$

work qubit

(initially $|0\rangle$





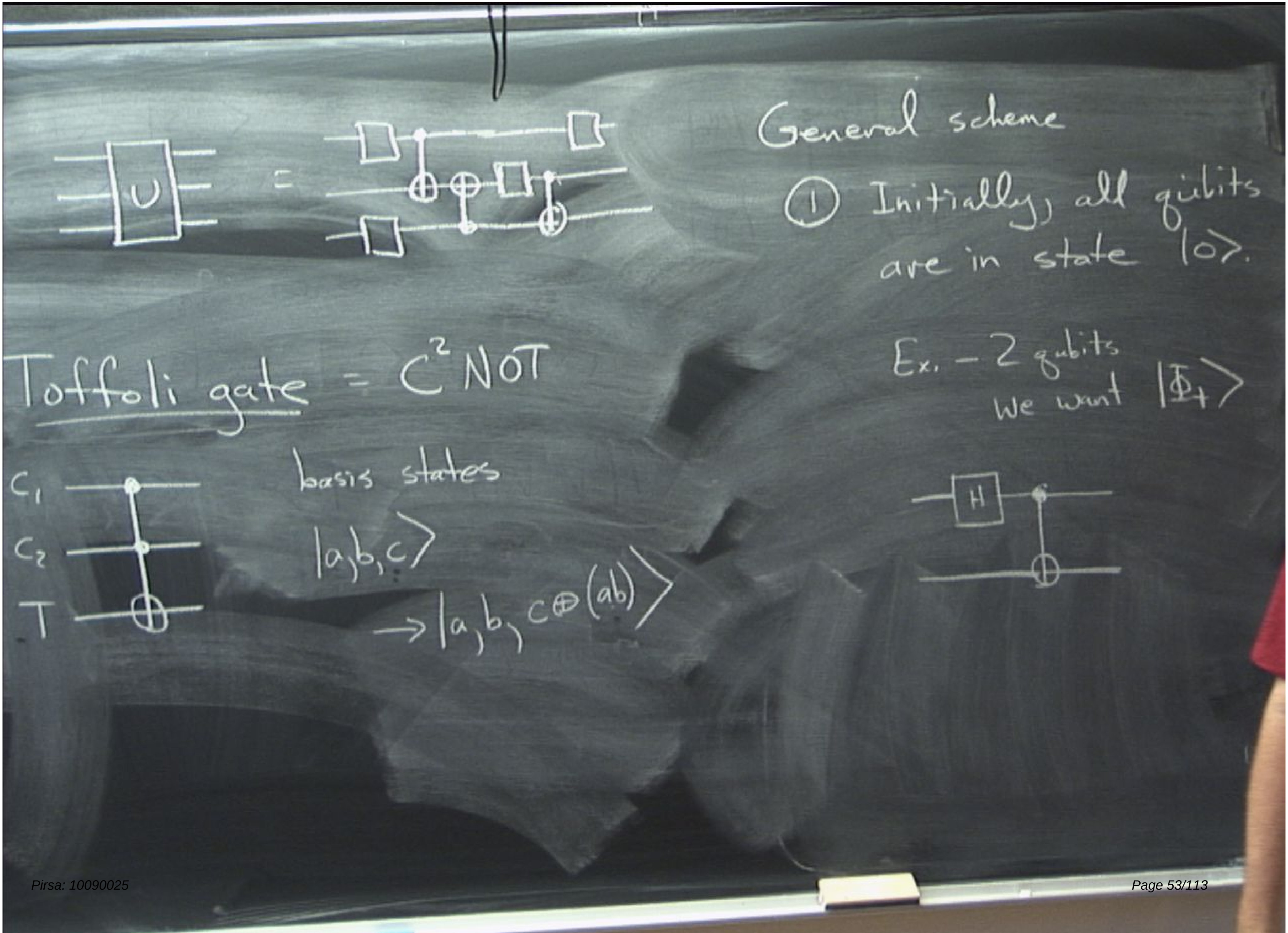
General scheme

① Initially, all qubits are in state $|0\rangle$.

Toffo = C^2NOT

states

$b, c\oplus(ab)\rangle$



General scheme

① Initially, all qubits are in state $|0\rangle$.

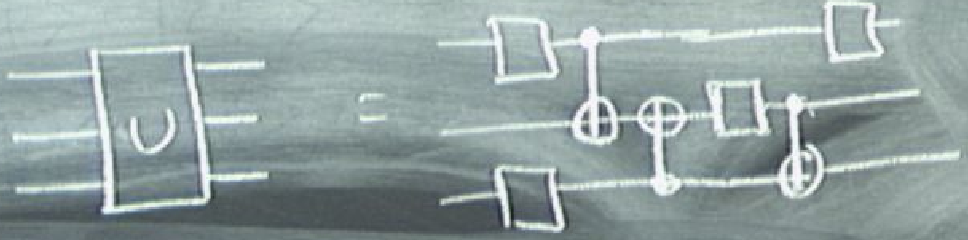
Ex. – 2 qubits
we want $|\Phi_+\rangle$

Toffoli gate = C^2NOT

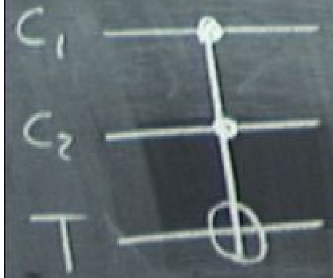
basis states

$|a,b,c\rangle$

$\rightarrow |a,b,c\oplus(ab)\rangle$



Toffoli gate = $C^2 NOT$



basis states

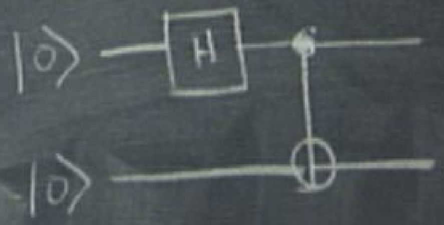
$|a,b,c\rangle$

$\rightarrow |a,b,c\oplus(ab)\rangle$

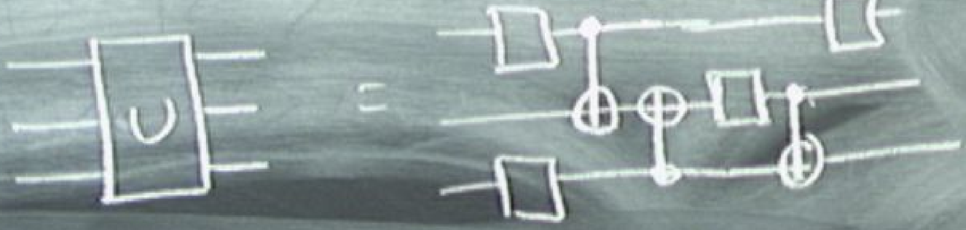
General scheme

① Initially, all qubits are in state $|0\rangle$.

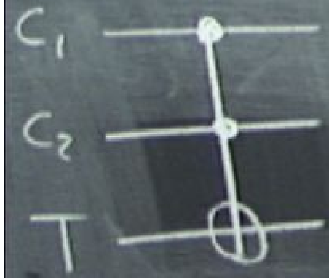
Ex. – 2 qubits
we want $|\Phi_+\rangle$



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



Toffoli gate = C^2NOT



basis states

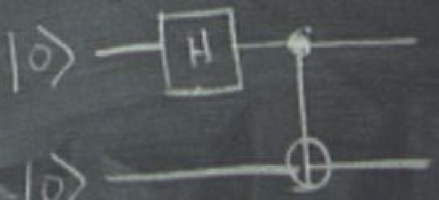
$|a,b,c\rangle$

$\rightarrow |a,b,c \oplus (ab)\rangle$

General scheme

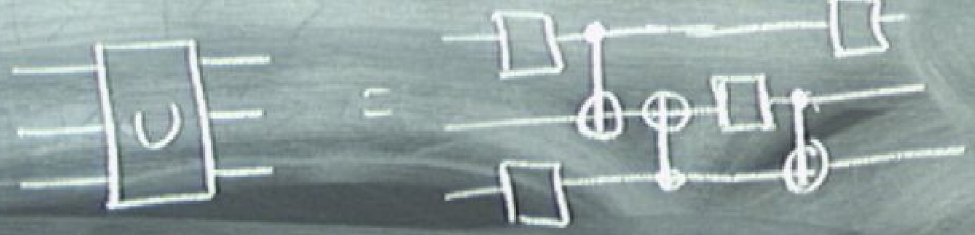
① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits
we want $|\Phi_+\rangle$

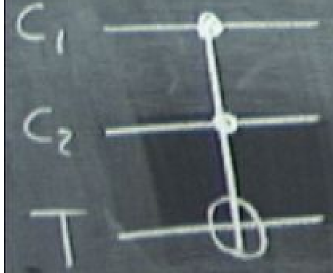


$|0,0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0,0\rangle + |1,0\rangle)$

$\rightarrow \frac{1}{\sqrt{2}}($



Toffoli gate = $C^2 NOT$



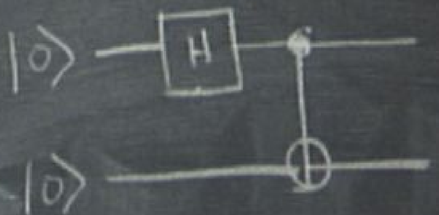
basis states

$$|a,b,c\rangle \rightarrow |a,b,c \oplus (ab)\rangle$$

General scheme

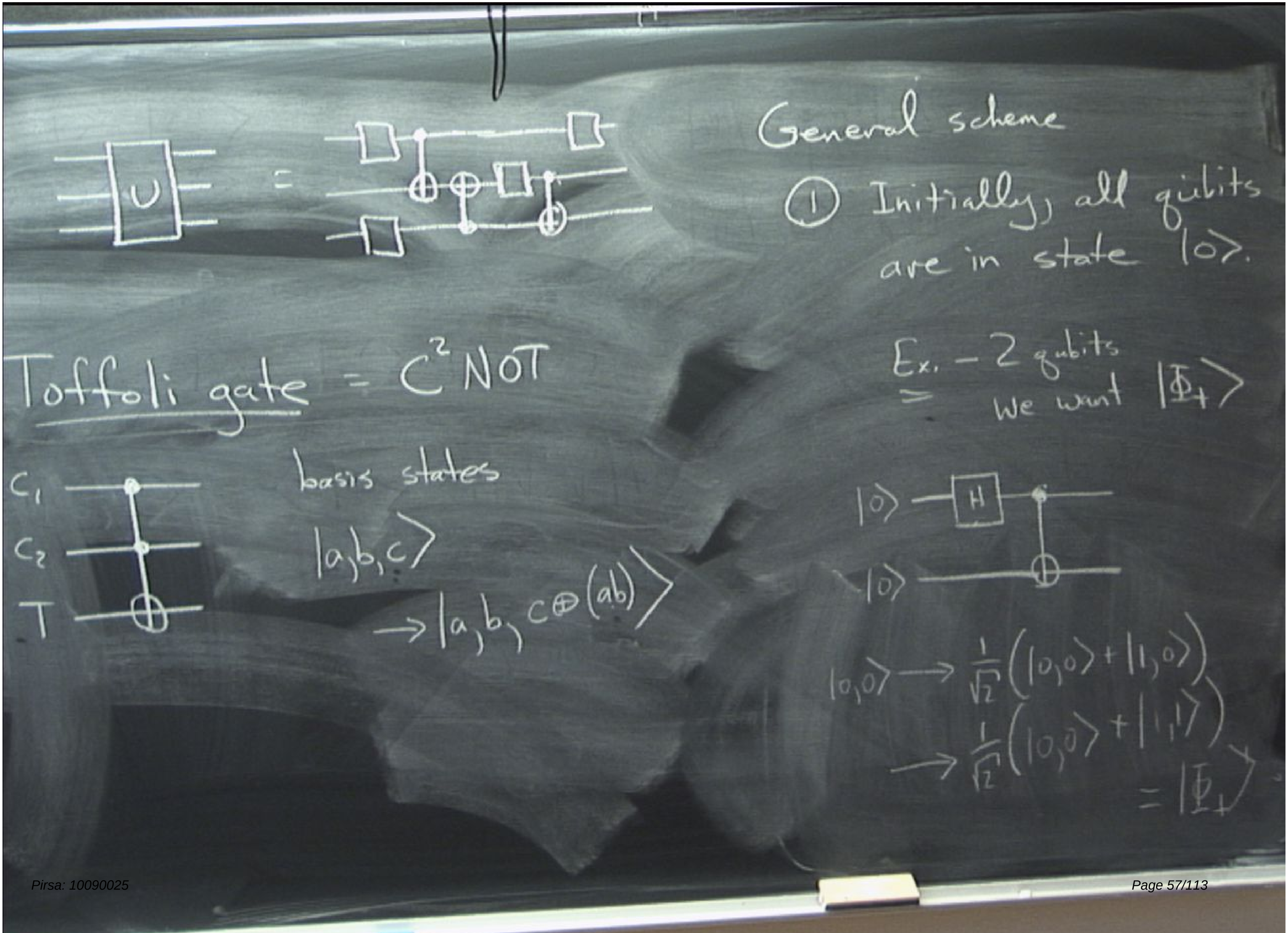
① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits
we want $|\Phi_+\rangle$



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

$$\rightarrow \frac{1}{\sqrt{2}}\left(|0,0\rangle + |\right.$$



General scheme

① Initially, all qubits are in state $|0\rangle$.

Toffoli gate = C^2NOT

basis states

$|a,b,c\rangle$

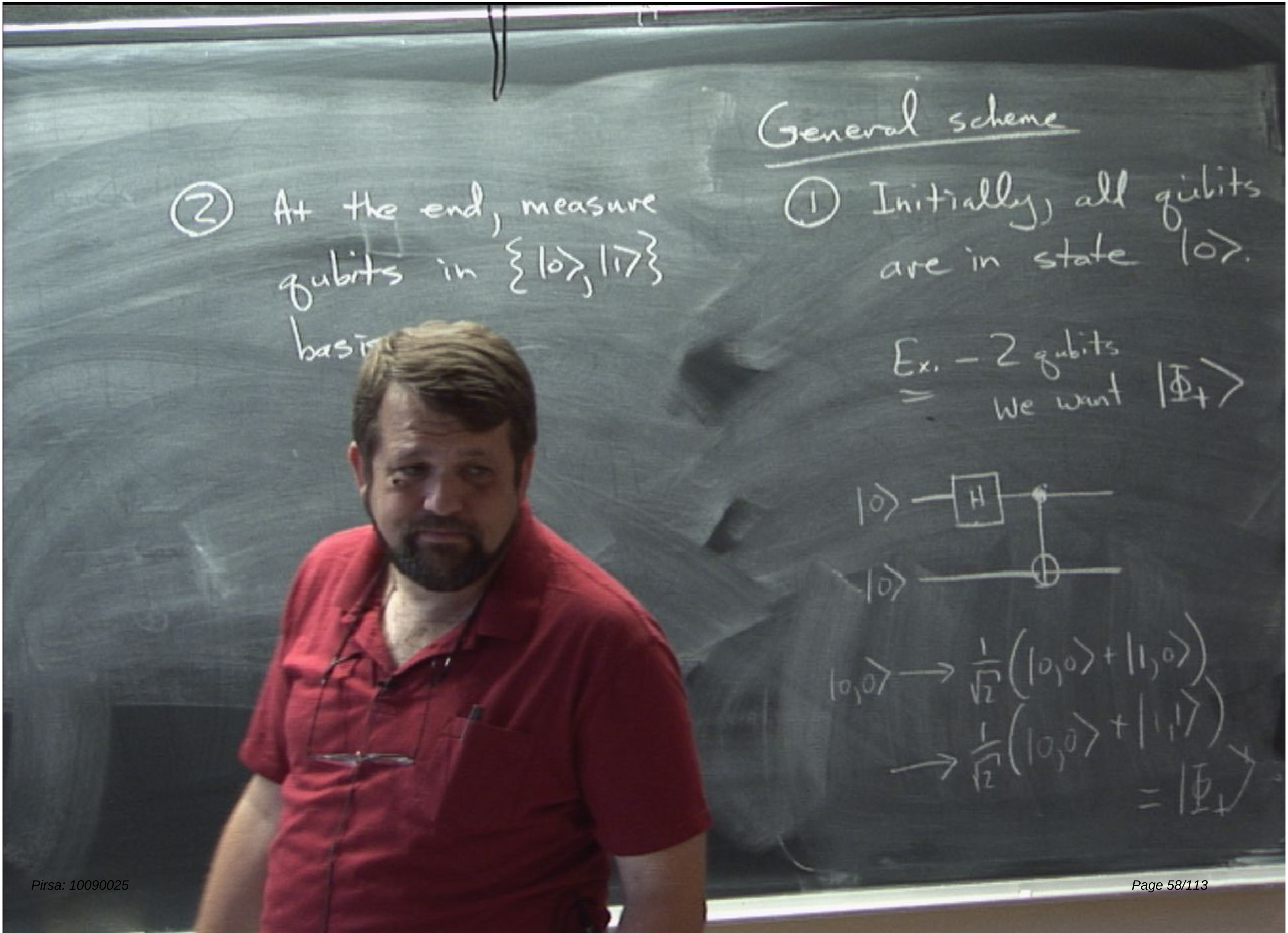
$\rightarrow |a,b,c\oplus(ab)\rangle$

Ex. – 2 qubits

$\Rightarrow$ we want $|\Phi_+\rangle$

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

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



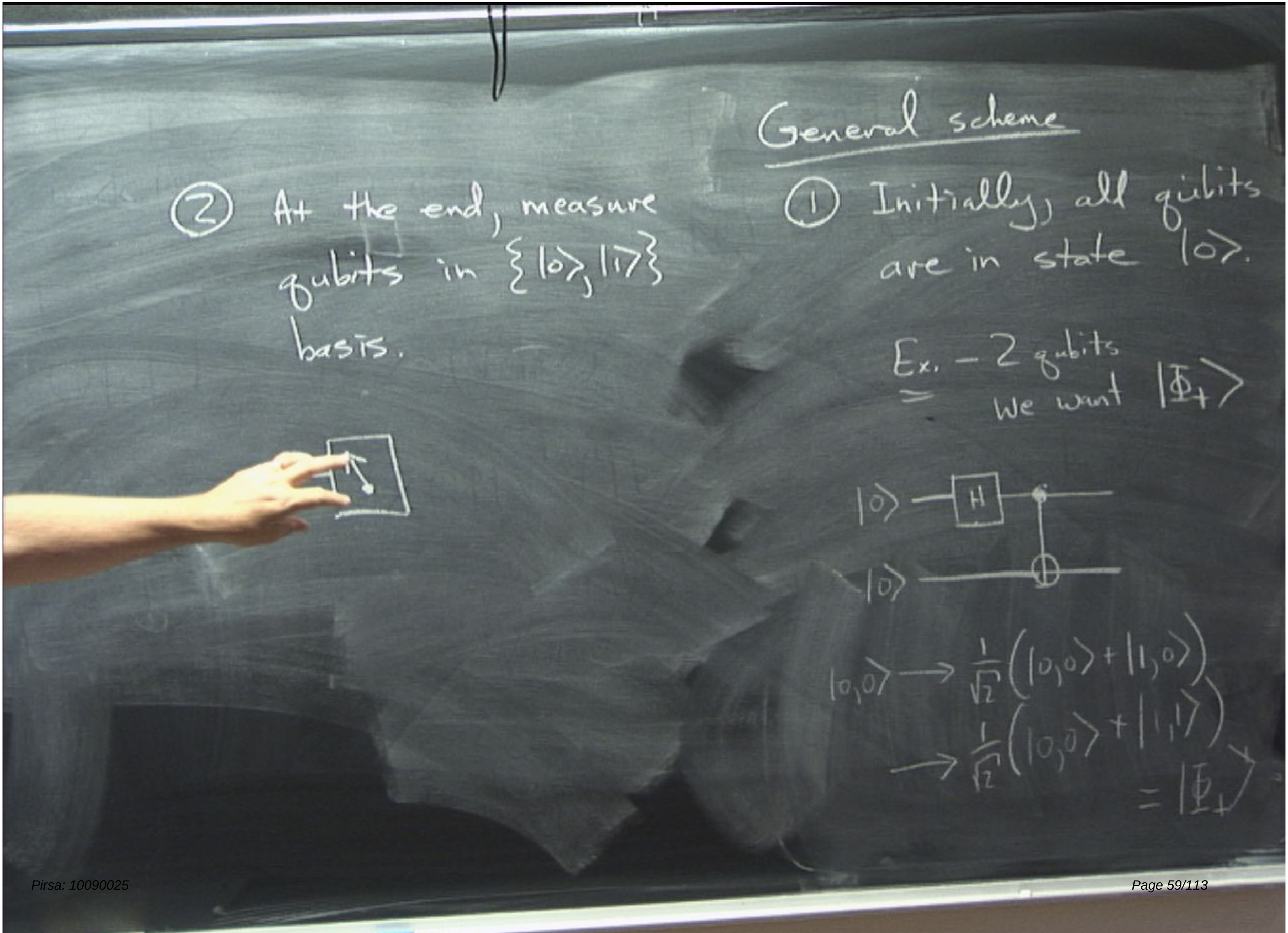
General scheme

① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits
$\Rightarrow$ we want $|\Phi_+\rangle$

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

② At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis



General scheme

① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits

$\Rightarrow$ we want $|\Phi_+\rangle$

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

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

$$= |\Phi_+\rangle$$

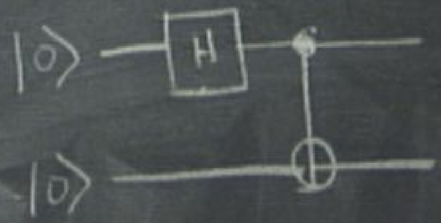
② At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis.

General scheme

(1) Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits

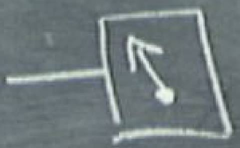
$\Rightarrow$ we want $|\Phi_+\rangle$



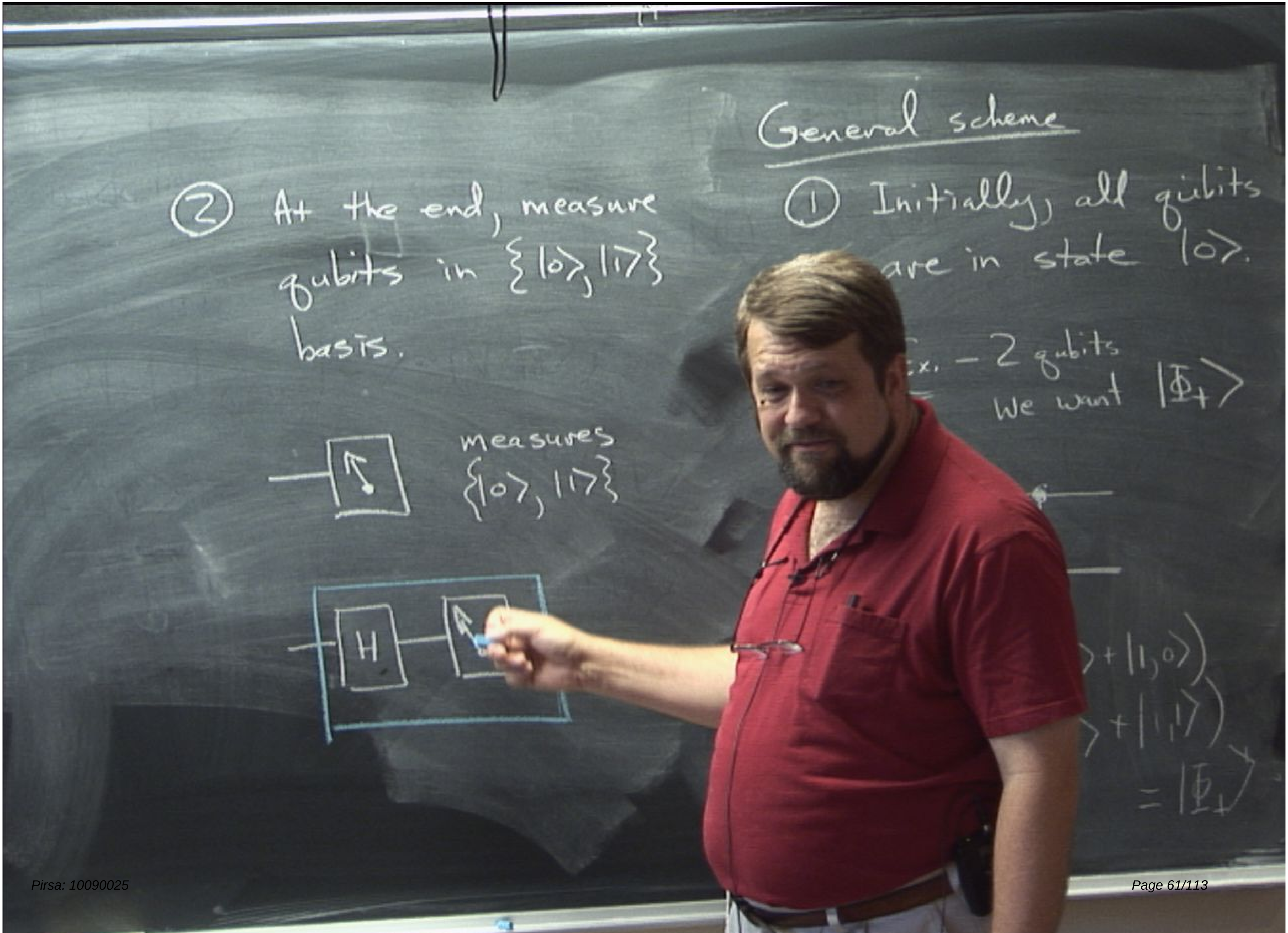
$$|0,0\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,0\rangle\right)$$

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

(2) At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis.



measures $\{|0\rangle, |1\rangle\}$



General scheme

① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits

we want $|\Phi_+\rangle$

$\rangle + |1,0\rangle)$

$\rangle + |1,1\rangle)$

$= |\Phi_+\rangle$

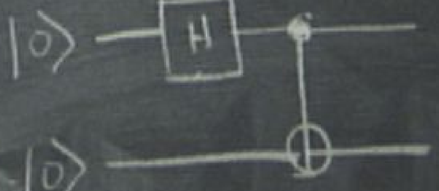
② At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis.

measures $\{|0\rangle, |1\rangle\}$

General scheme

① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits
= we want $|\Phi_+\rangle$

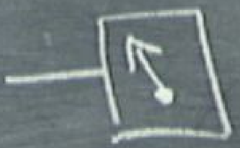


$$|0,0\rangle \longrightarrow \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,0\rangle\right)$$

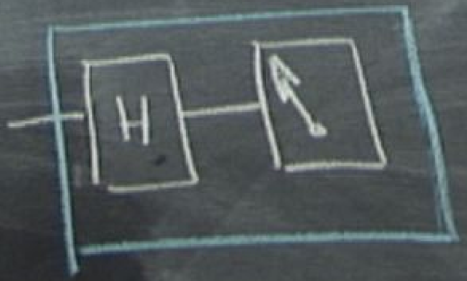
$$\longrightarrow \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,1\rangle\right)$$

$$= |\Phi_+\rangle$$

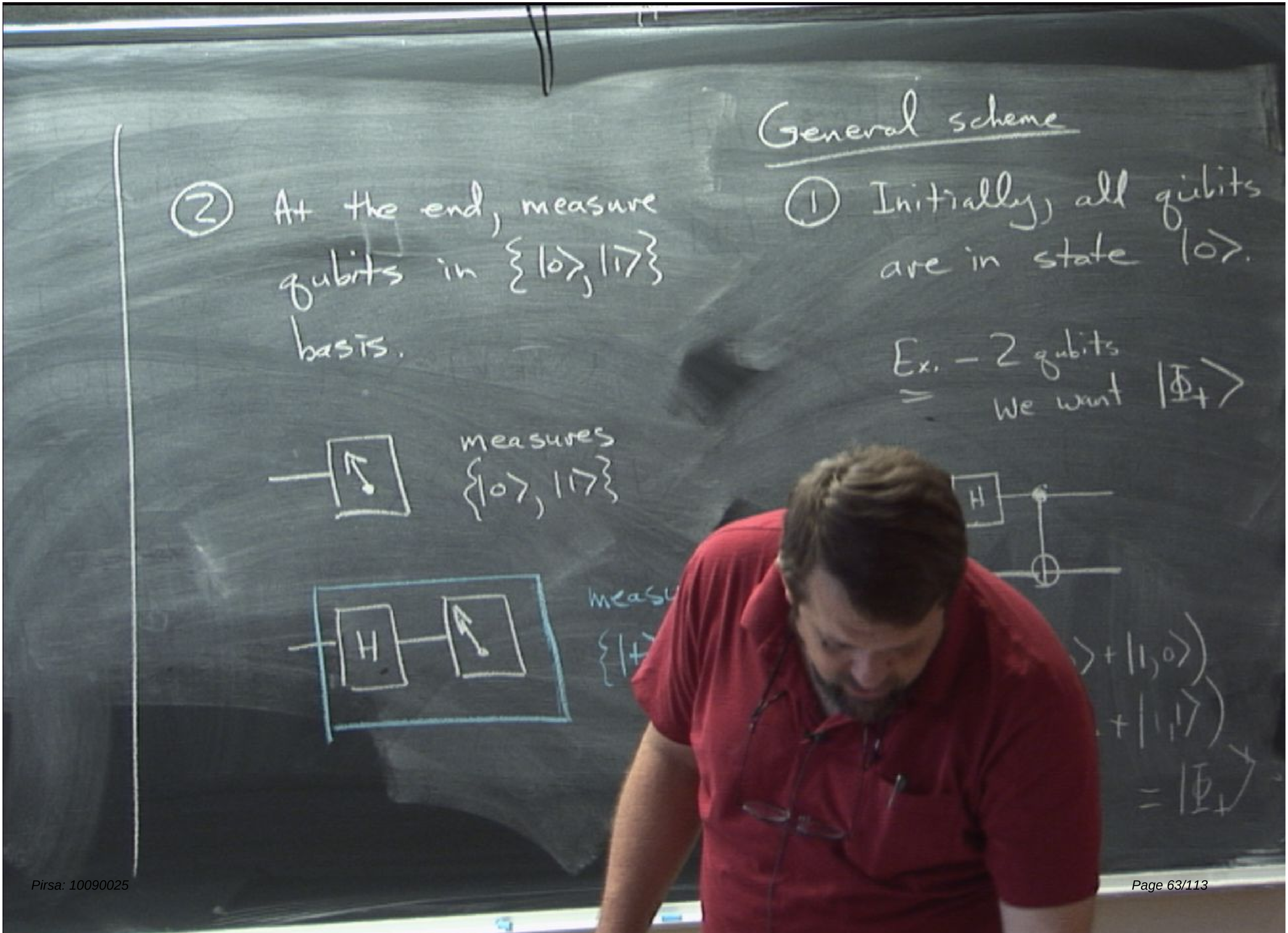
② At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis.



measures $\{|0\rangle, |1\rangle\}$



measures $\{|+\rangle, |-\rangle\}$



General scheme

① Initially, all qubits are in state $|0\rangle$.

Ex. – 2 qubits

$\Rightarrow$ we want $|\Phi_+\rangle$

$\rangle + |1,0\rangle)$

$+ |1,1\rangle)$

$= |\Phi_+\rangle$

② At the end, measure qubits in $\{|0\rangle, |1\rangle\}$ basis.

measures $\{|0\rangle, |1\rangle\}$

measu

$\{|+$

Function evaluation

Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b \oplus f(a))$$

reversible!

Function evaluation

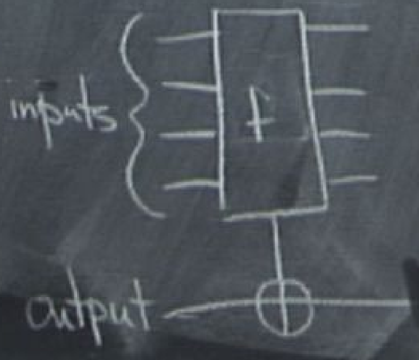
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b \oplus f(a))$$

reversible!

QM – f-controlled-NOT



Function evaluation

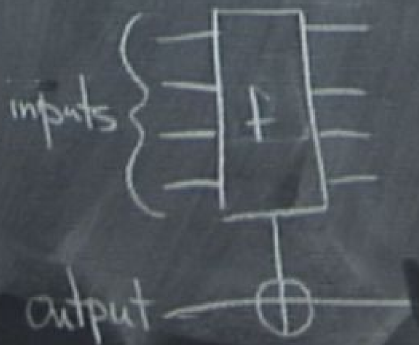
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

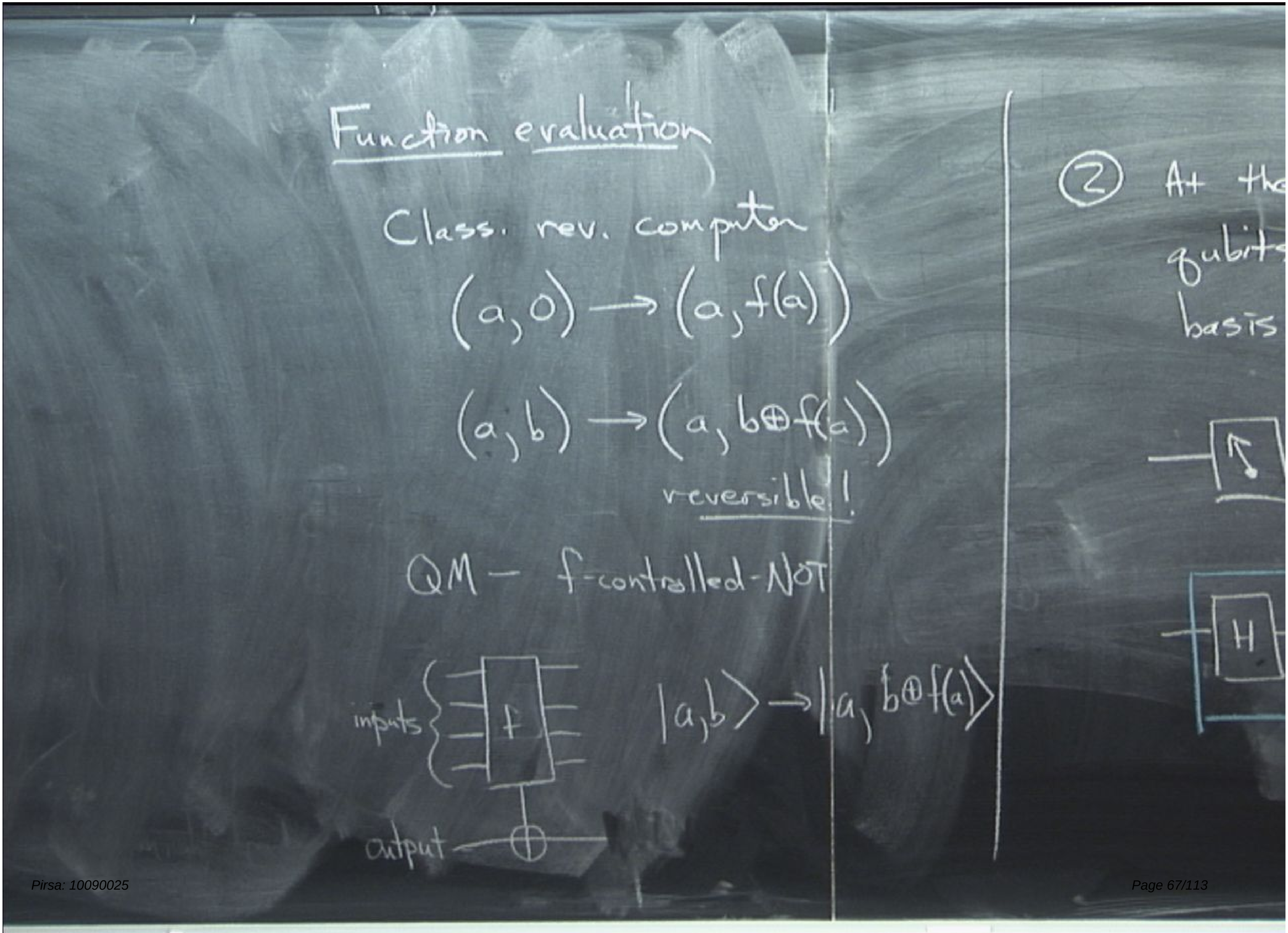
$$(a,b) \longrightarrow (a, b \oplus f(a))$$

reversible!

QM – f-controlled-NOT



$|a,b\rangle \longrightarrow |a,$ [illegible] $f(a)\rangle$



Function evaluation

Class. rev. computer

$$(a, 0) \longrightarrow (a, f(a))$$

$$(a, b) \longrightarrow (a, b \oplus f(a))$$

reversible!

QM — f-controlled-NOT

$$|a, b\rangle \longrightarrow |a, b \oplus f(a)\rangle$$

② At the
qubits
basis

Function evaluation

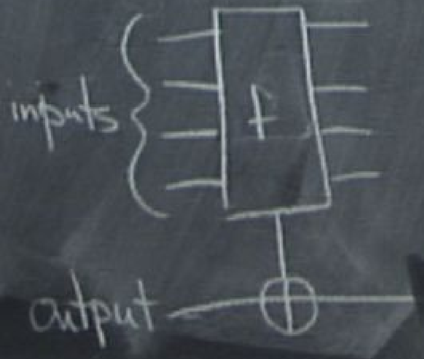
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b \oplus f(a))$$

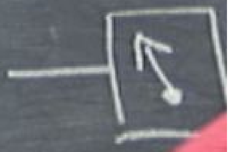
reversible!

QM – f-controlled-NOT



$$|a,b\rangle \longrightarrow |a, b\oplus f(a)\rangle$$

② At the
qubits
basis



Function evaluation

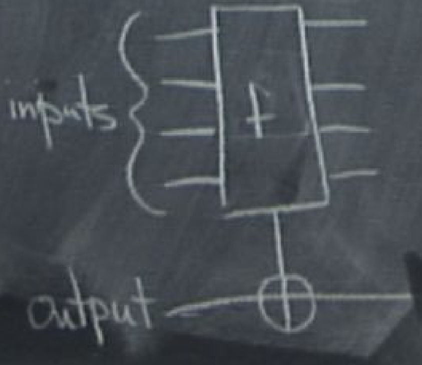
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b \oplus f(a))$$

reversible!

QM — f-controlled-NOT



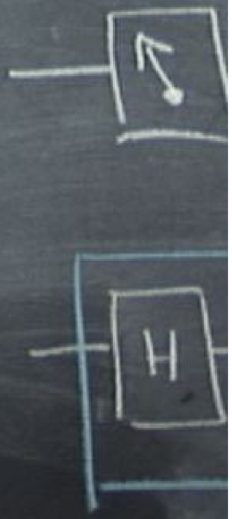
$$|a,b\rangle \longrightarrow |a, b\oplus f(a)\rangle$$

$$U_f$$

② At th

qubits

basis



Oracle problem

Given a way of evaluating f

Function evaluation

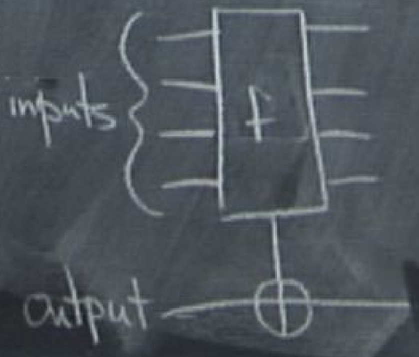
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b \oplus f($$

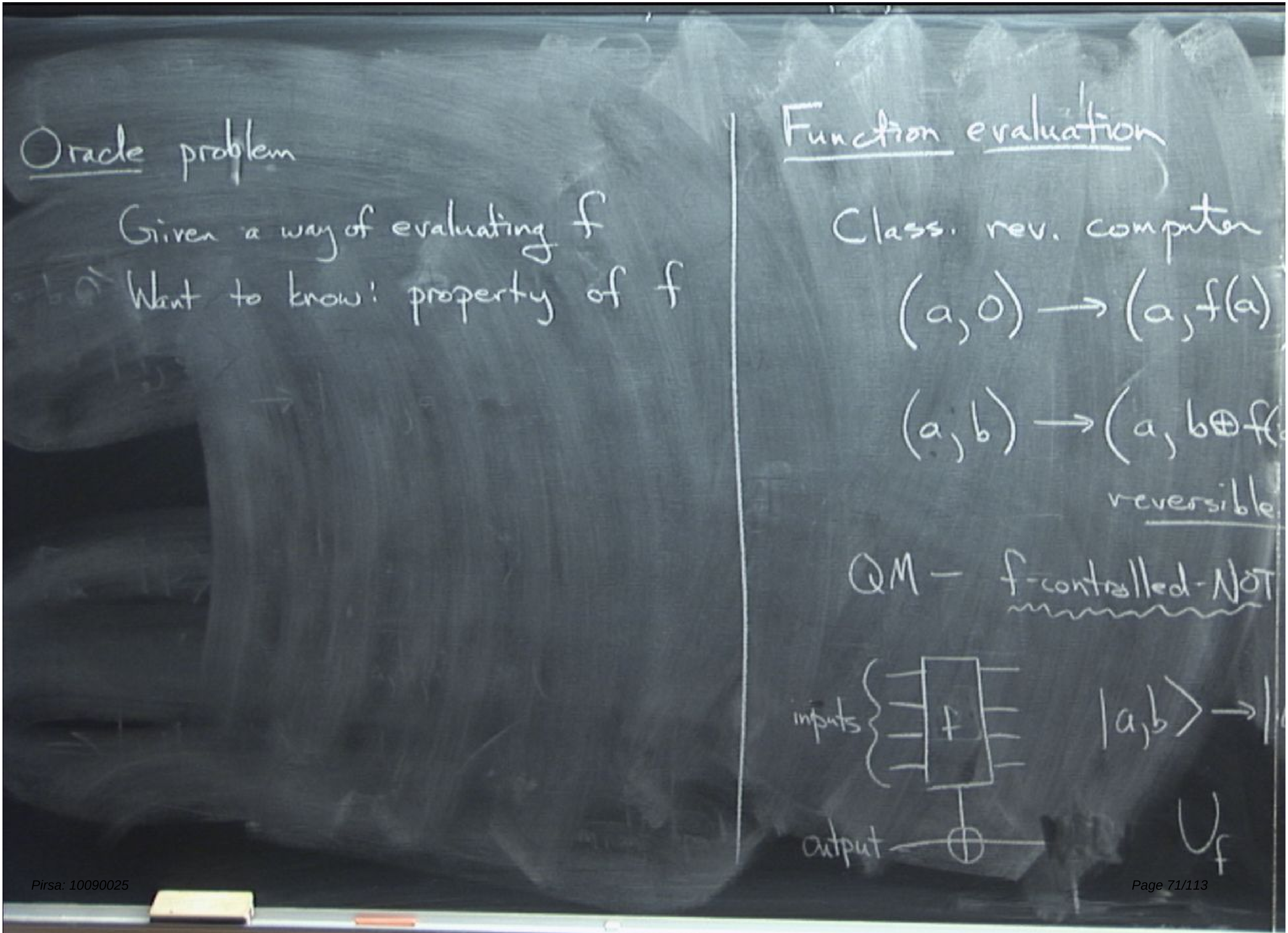
reversible

QM – f-controlled-NOT



$$|a,b\rangle \longrightarrow |$$

U_f



Oracle problem

Given a way of evaluating f

Want to know: property of f

Function evaluation

Class. rev. computer

$(a,0) \longrightarrow (a, f(a))$

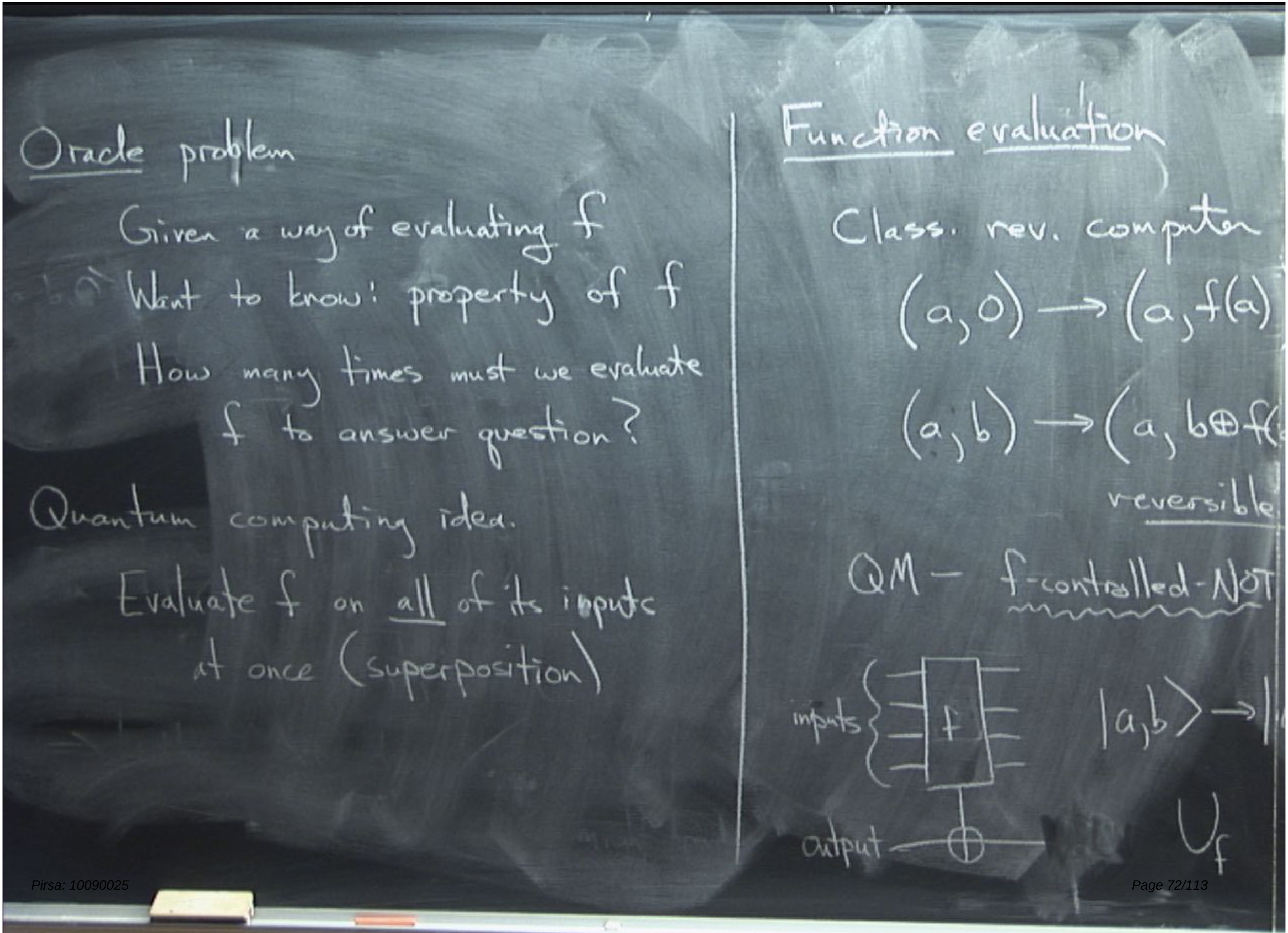
$(a,b) \longrightarrow (a, b \oplus f($

reversible

QM — f-controlled-NOT

$|a,b\rangle \longrightarrow |$

U_f



Oracle problem

Given a way of evaluating f

Want to know: property of f

How many times must we evaluate f to answer question?

Quantum computing idea.

Evaluate f on <u>all</u> of its inputs at once (superposition)

Function evaluation

Class. rev. comput

$$(a,0) \longrightarrow (a, f(a))$$

$$(a,b) \longrightarrow (a, b\oplus f($$

reversible

QM — f-controlled-NOT

$$|a,b\rangle \longrightarrow |$$

Oracle problem

Given a way of evaluating f

Want to know: property of f

How many times must we evaluate f to answer question?

Quantum computing idea.

Evaluate f on all of its inputs at once (superposition)

Function evaluation

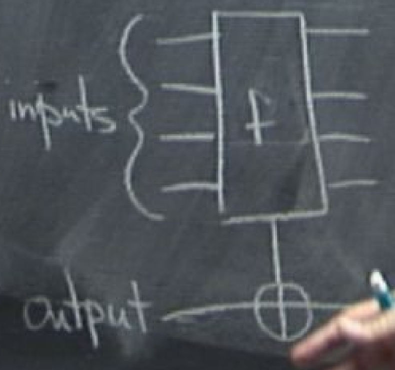
Class. rev. computer

$$(a,0) \longrightarrow (a, f(a)$$

$$(a,b) \longrightarrow (a, b \oplus f($$

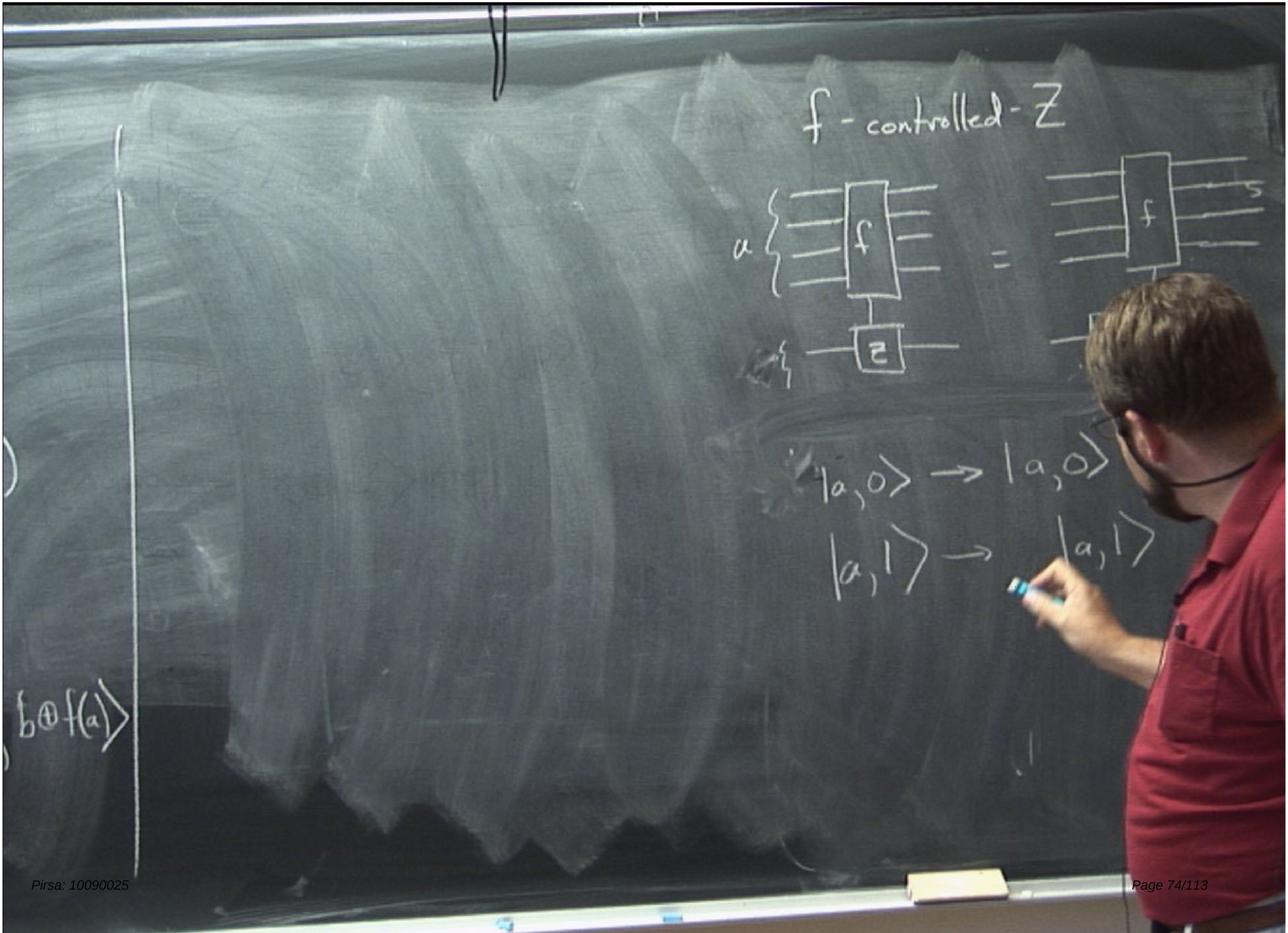
reversible

QM — f-controlled-NOT



$|a,b\rangle$

U_f

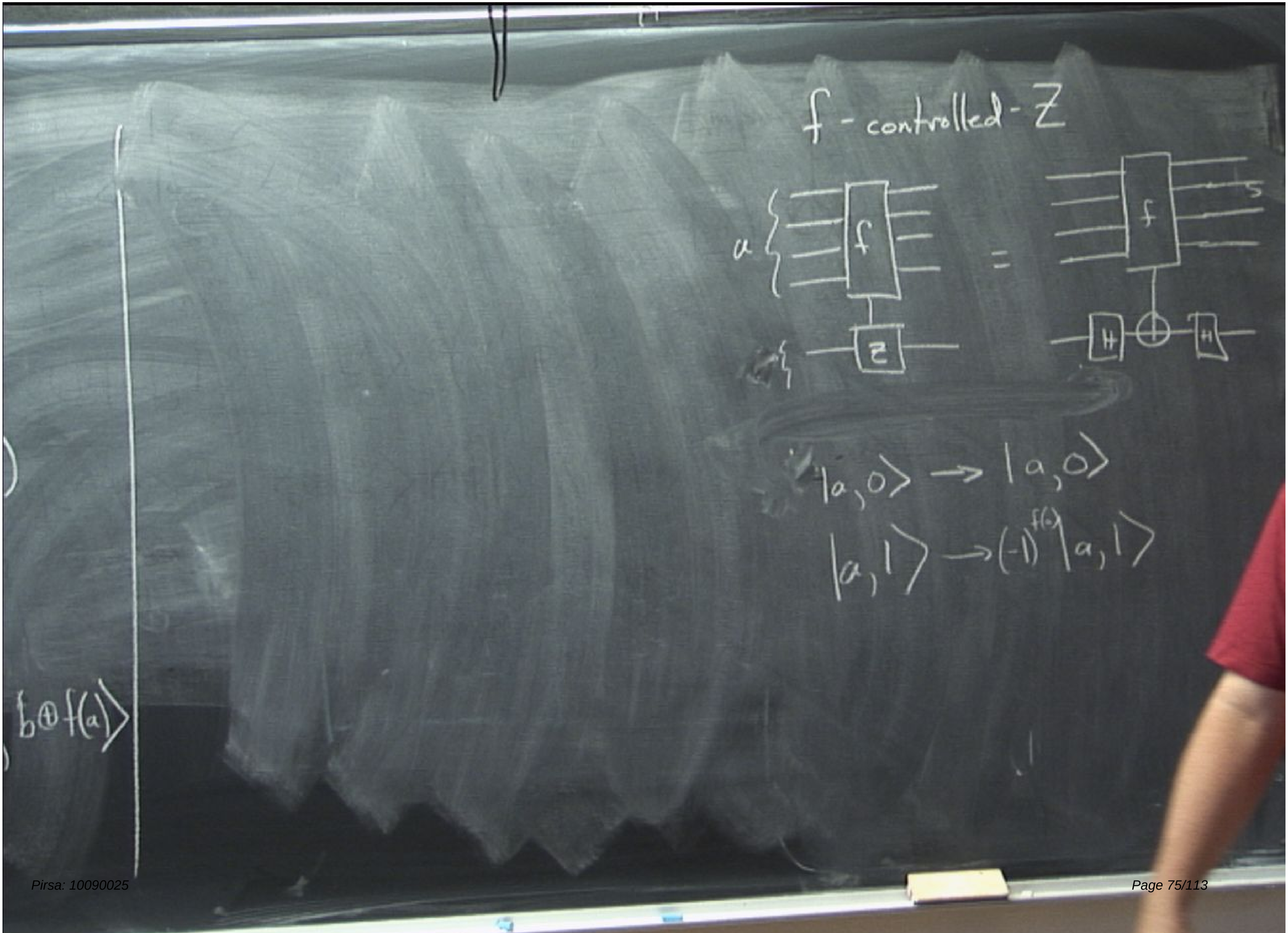


f - controlled - Z

$|a,0\rangle \to |a,0\rangle$

$|a,1\rangle \to \quad |a,1\rangle$

$b \oplus f(a)\rangle$



f-controlled-Z

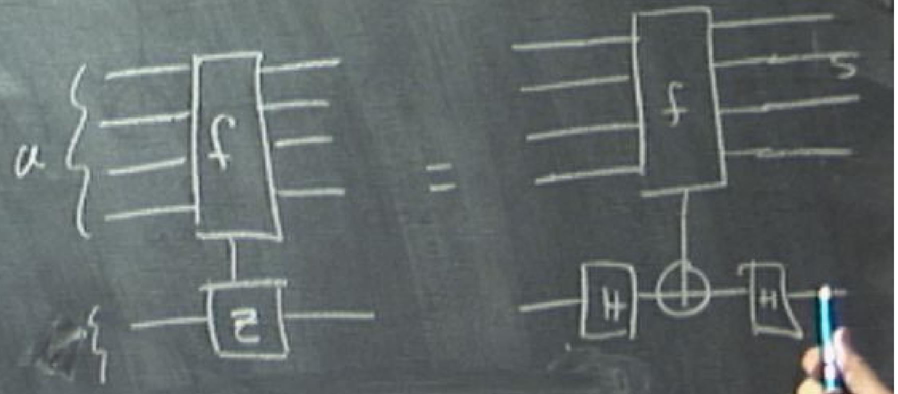
$$|a,0\rangle \rightarrow |a,0\rangle$$

$$|a,1\rangle \rightarrow (-1)^{f(a)}|a,1\rangle$$

$b \oplus f(a)\rangle$

$b \oplus f(a)\rangle$

f - controlled - Z

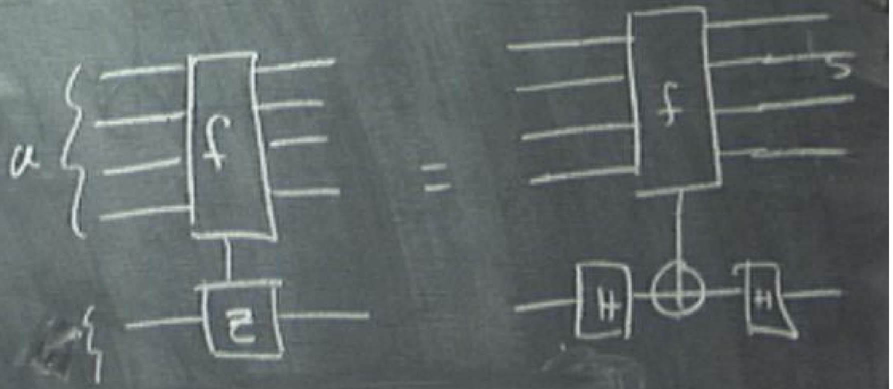


$$|a,0\rangle \to |a,0\rangle$$

$$|a,1\rangle \to (-1)^{f(a)}|a,1\rangle$$

$\oplus f(a)\rangle$

f - controlled - Z



$$|a,0\rangle \longrightarrow |a,0\rangle$$

$$|a,1\rangle \longrightarrow (-1)^{f(a)}|a,1\rangle$$

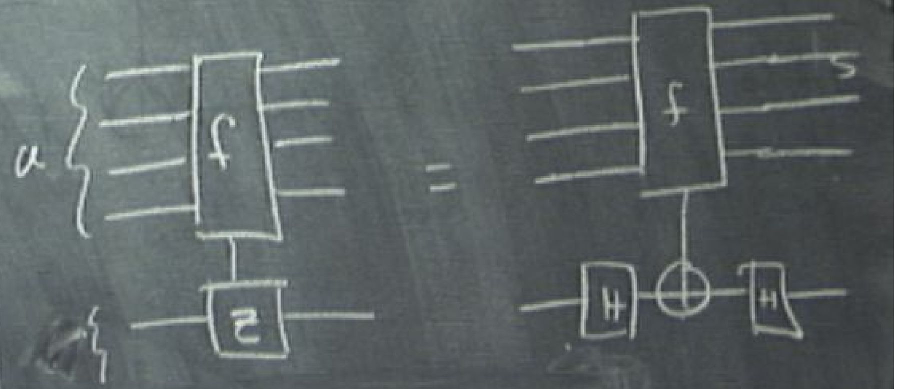
$b \oplus f(a)\rangle$

② $H^{\otimes n}$

We saw: $H^{\otimes n}|0^n\rangle$

$$= \frac{1}{2^{n/2}} \sum_a |a\rangle$$

f - controlled - Z



$|a,0\rangle \rightarrow |a,0\rangle$

$|a,1\rangle \rightarrow (-1)^{f(a)}|a,1\rangle$

$)$

$b \oplus f(a)\rangle$

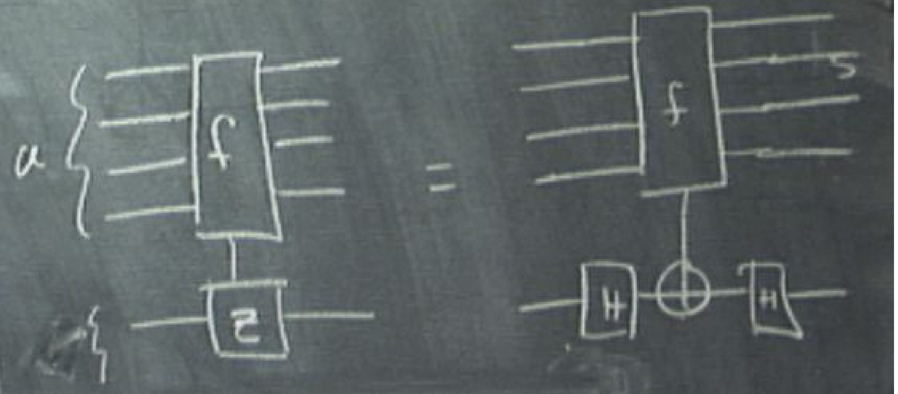
② $H^{\otimes n}$

We saw: $H^{\otimes n}|0^n\rangle$

$$= \frac{1}{2^{n/2}} \sum_a |a\rangle$$

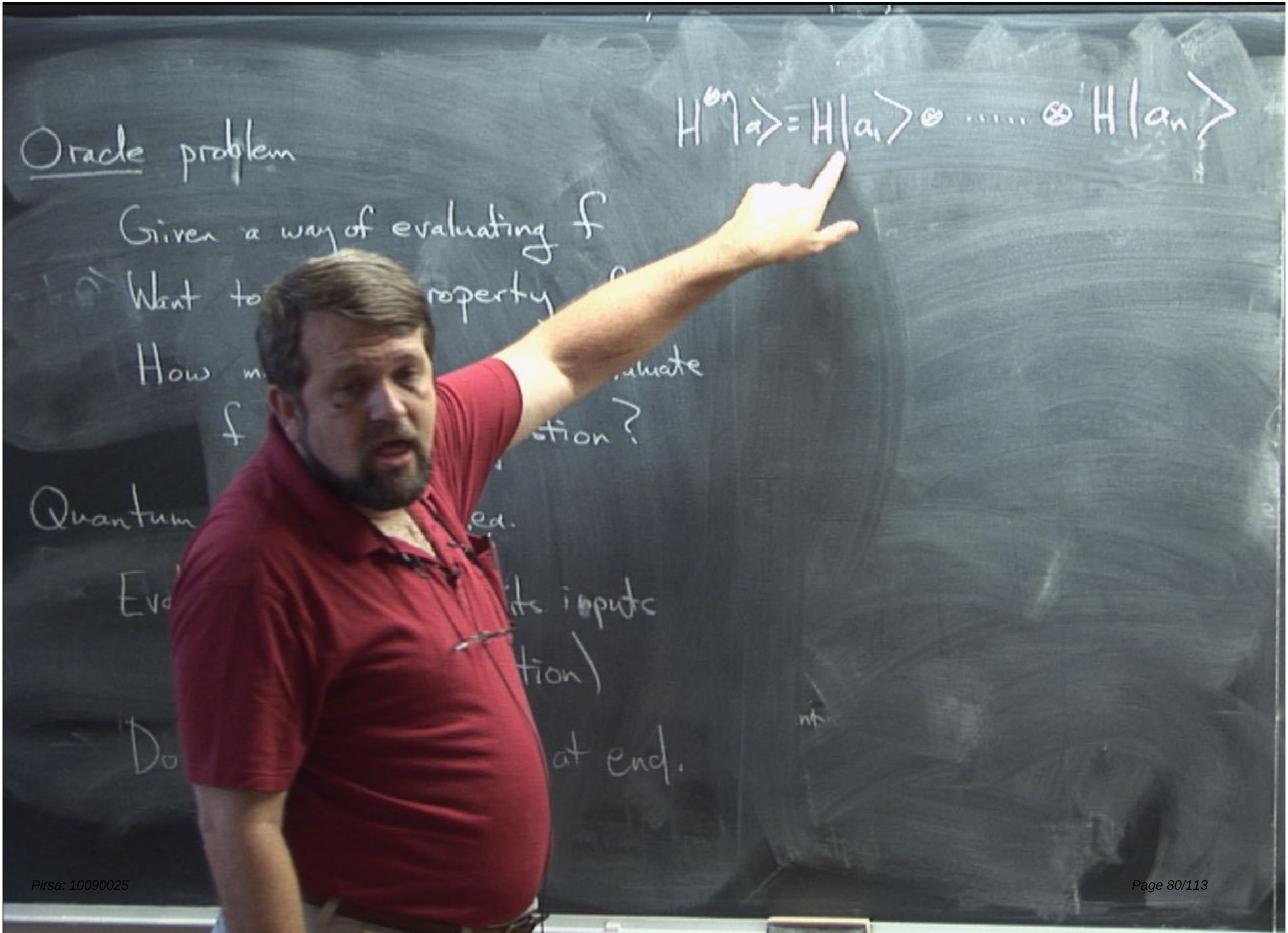
$H^{\otimes n}|a\rangle = ?$ a = n-bit string

f - controlled - Z



$|a,0\rangle \to |a,0\rangle$

$|a,1\rangle \to (-1)^{f(a)}|a,1\rangle$



$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

Oracle problem

Given a way of evaluating f

Want to … roperty …

How m… …aluate

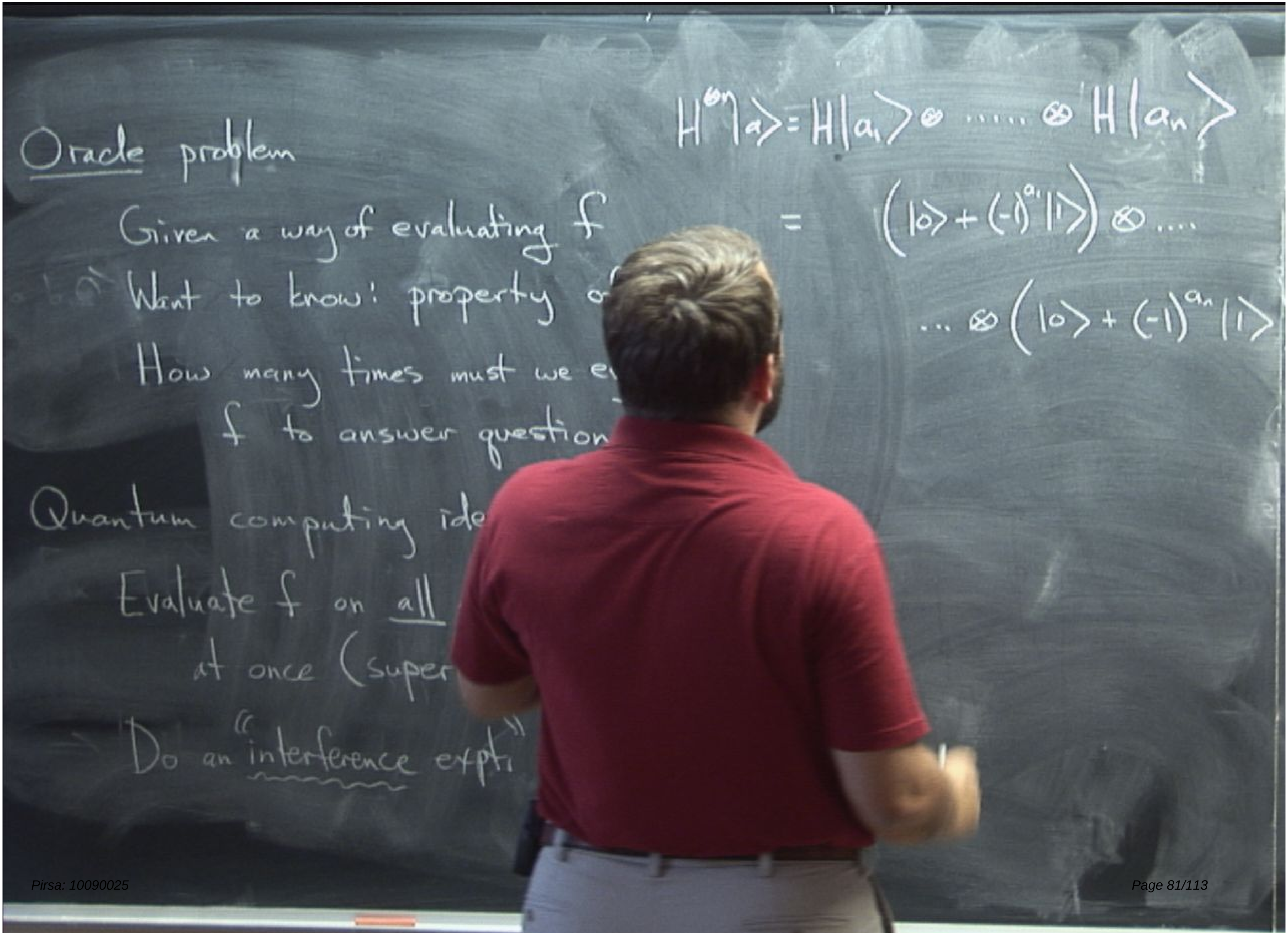
f … …tion?

Quantum … …ed.

Ev… …its inputs

…tion)

Do … at end.



Oracle problem

Given a way of evaluating f

Want to know: property o

How many times must we ev

f to answer question

Quantum computing ide

Evaluate f on all

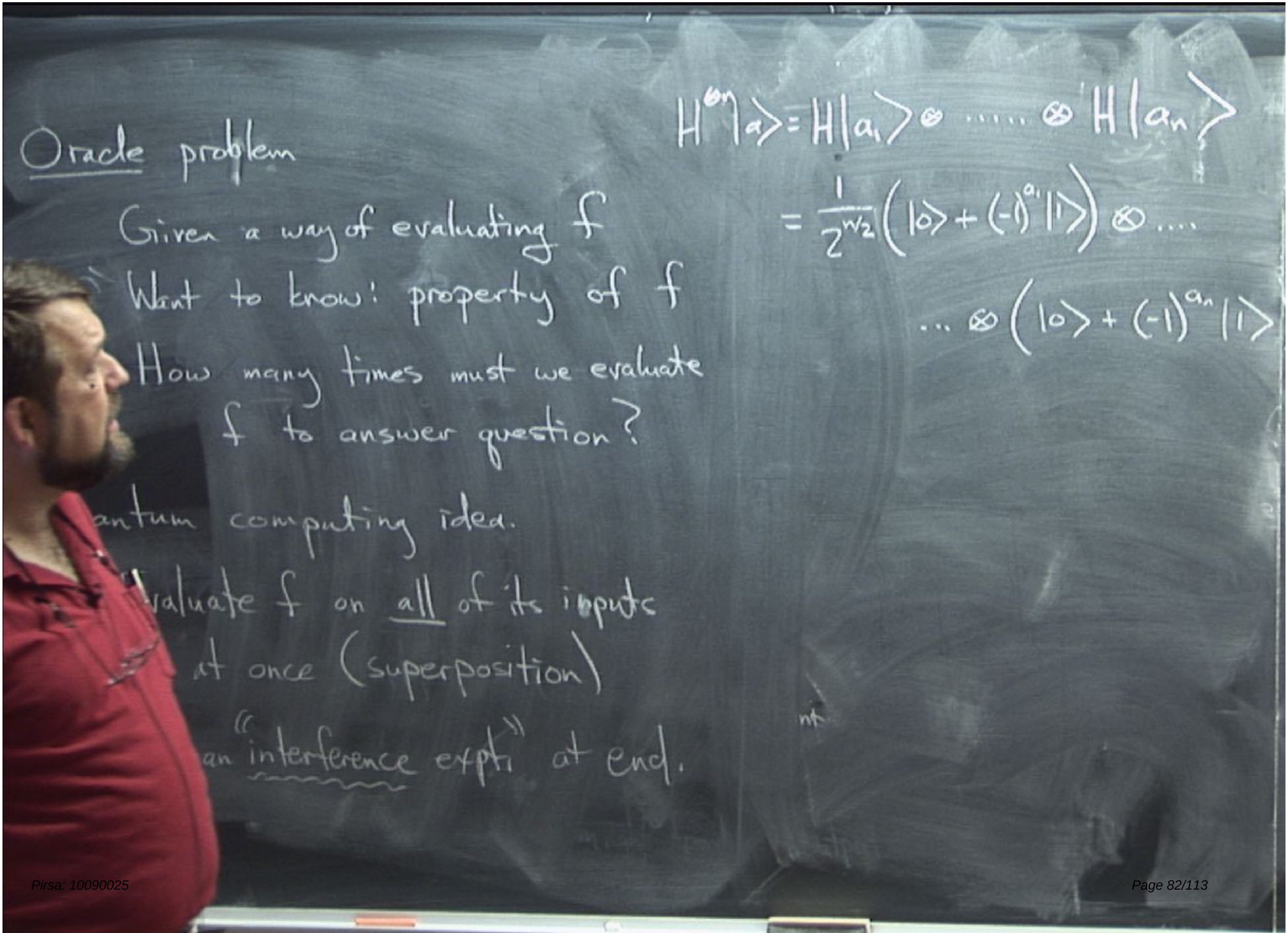
at once (super

Do an "interference expt"

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

$$= \left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots\cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$



Oracle problem

Given a way of evaluating f

Want to know: property of f

How many times must we evaluate f to answer question?

antum computing idea.

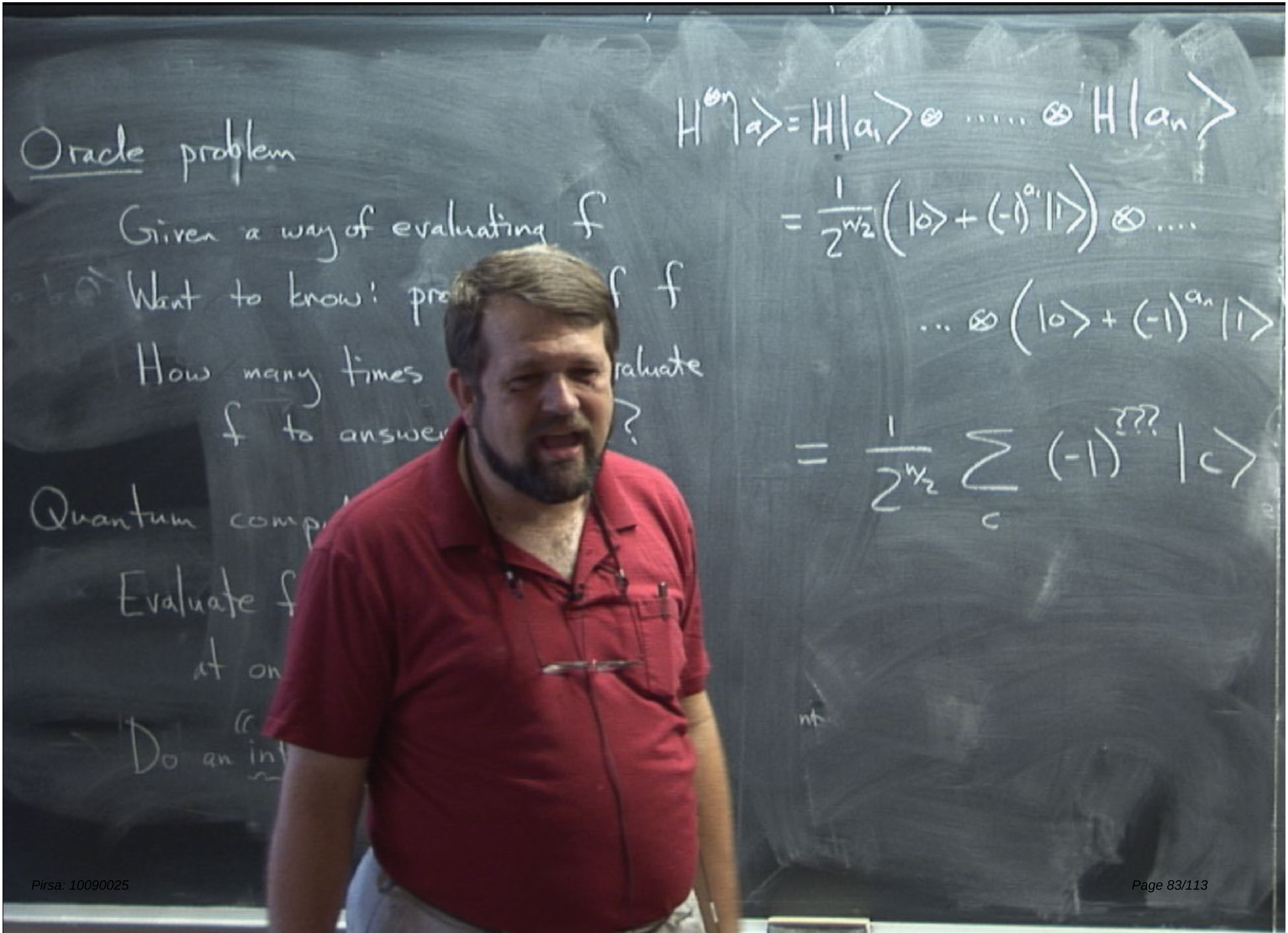
valuate f on all of its inputs at once (superposition)

an "interference expt" at end.

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$



Oracle problem

Given a way of evaluating f

Want to know: pre f f

How many times ralnate

f to answer ?

Quantum comp

Evaluate f

at on

((

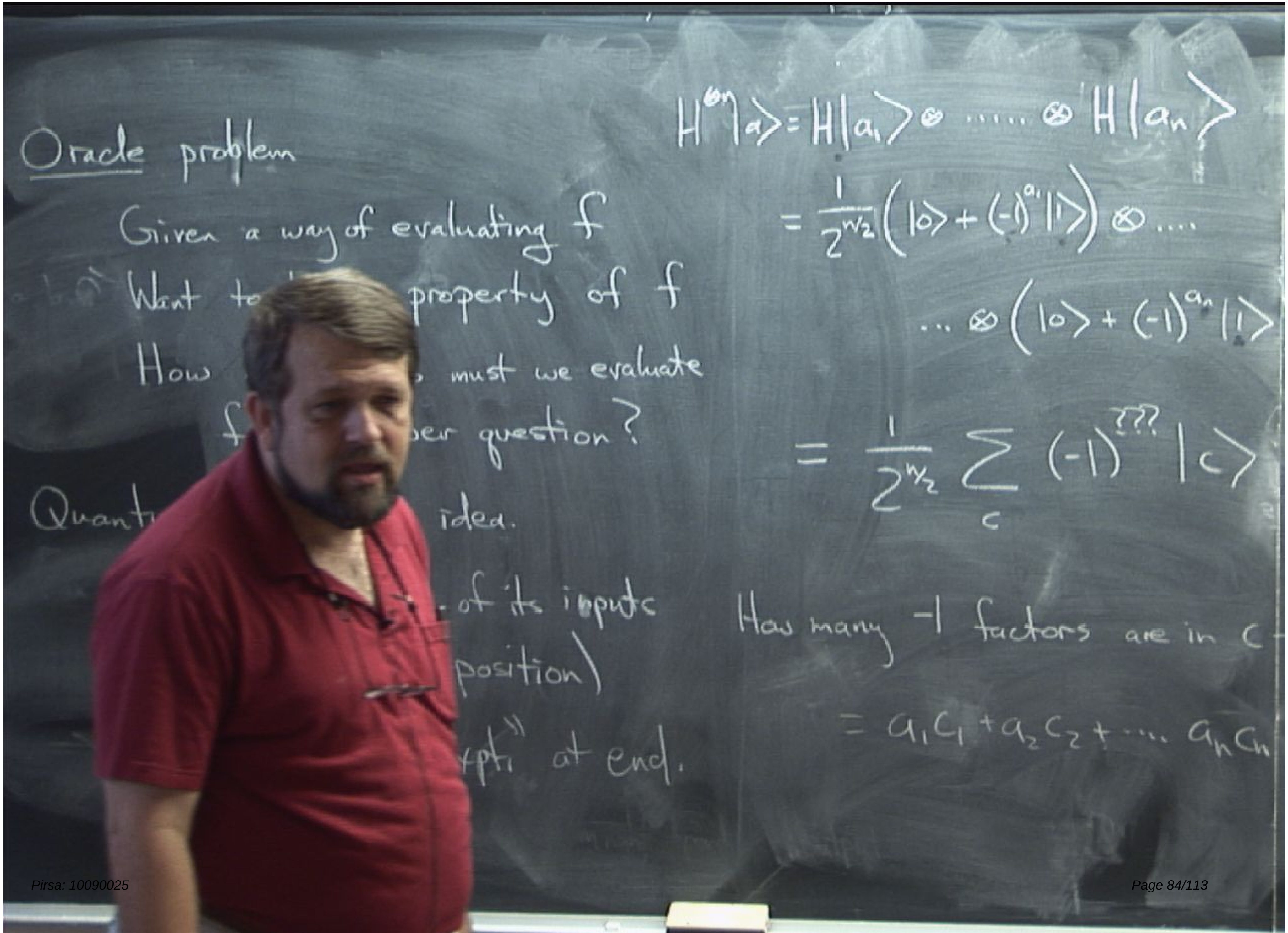
Do an in

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots\cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$

$$= \frac{1}{2^{n/2}} \sum_c (-1)^{???} |c\rangle$$



Oracle problem

Given a way of evaluating f

Want to property of f

How must we evaluate

f er question?

Quant idea.

of its inputs

position)

ypt" at end.

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

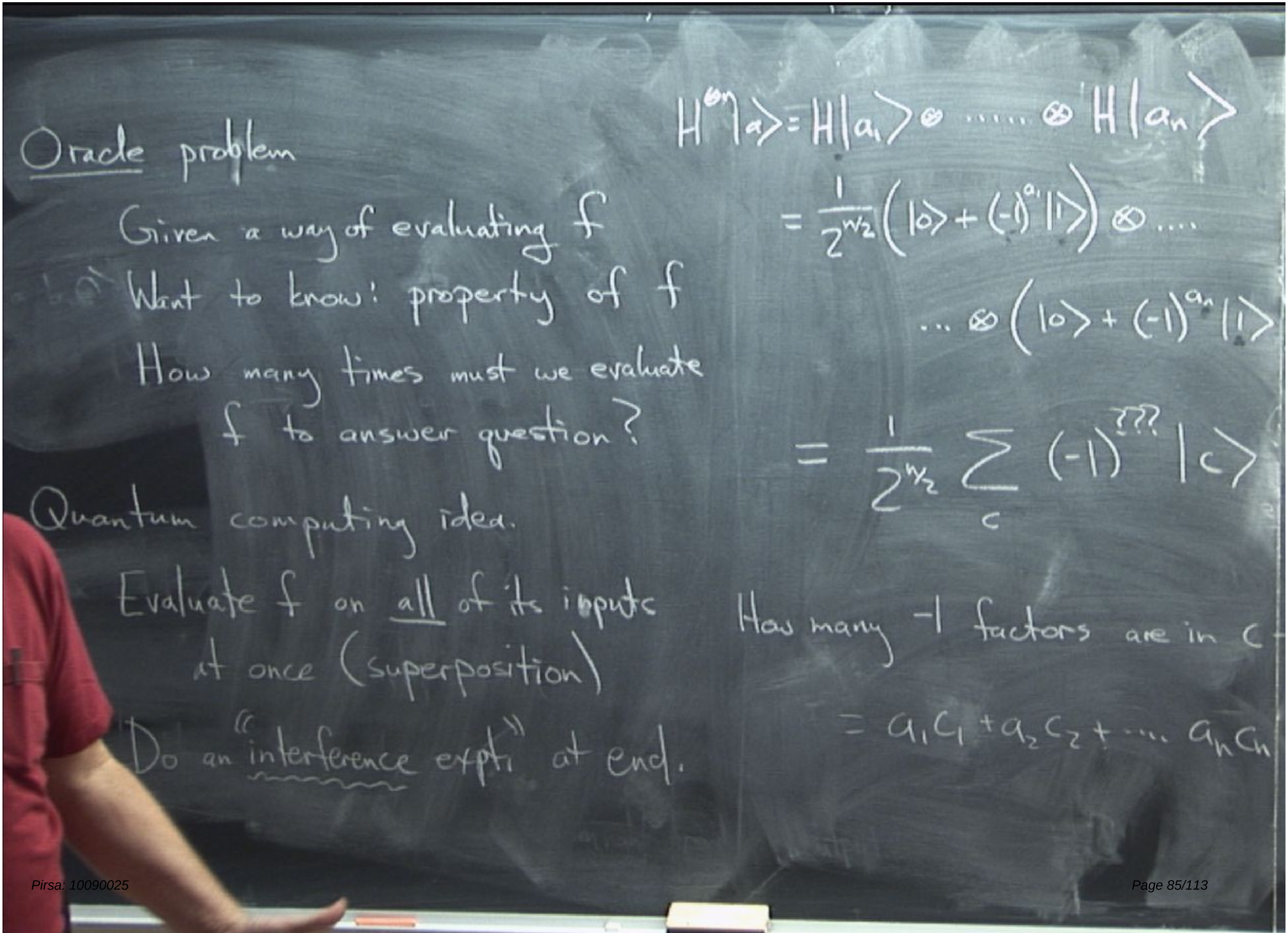
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots\cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$

$$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{???} |c\rangle$$

How many -1 factors are in c

$$= a_1c_1 + a_2c_2 + \cdots\cdots a_nc_n$$



Oracle problem

Given a way of evaluating f

Want to know: property of f

How many times must we evaluate f to answer question?

Quantum computing idea.

Evaluate f on all of its inputs at once (superposition)

Do an "interference expt" at end.

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$

$$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{???} |c\rangle$$

How many -1 factors are in c

$$= a_1c_1 + a_2c_2 + \cdots a_nc_n$$

Oracle problem

Given a way of evaluating f

Want to know: pro f

How many times m luate

f to answer ?

Quantum comp

Evaluate f

at on

→ Do an "in

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

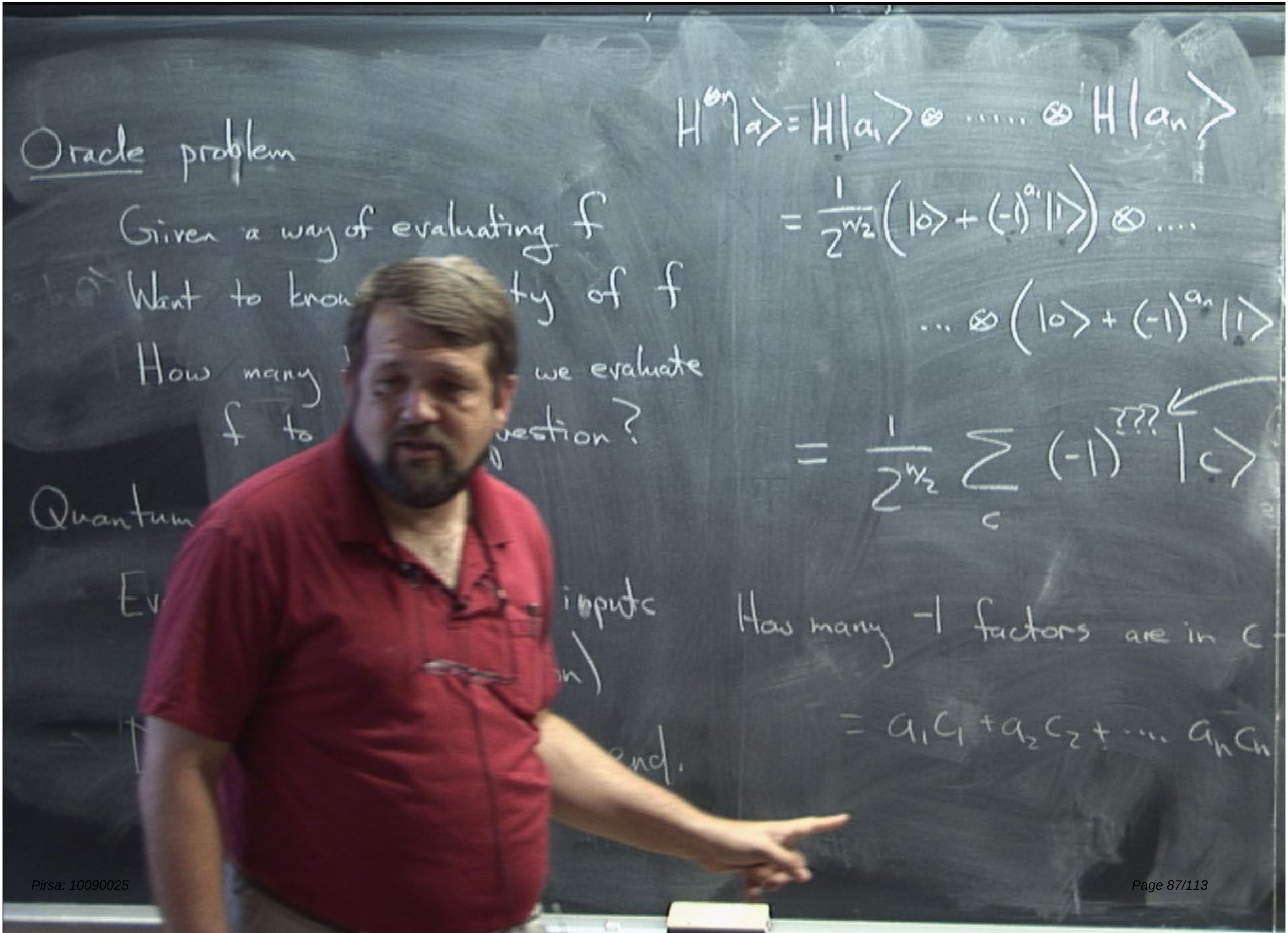
$$= \frac{1}{2^{n/2}}\Big(|0\rangle + (-1)^{a_1}|1\rangle\Big) \otimes \cdots\cdots$$

$$\cdots \otimes \Big(|0\rangle + (-1)^{a_n}|1\rangle$$

$$= \frac{1}{2^{n/2}} \sum (-1)^{???} |c\rangle$$

How many −1 factors are in c

$$= a_1c_1 + a_2c_2 + \cdots\cdots a_nc_n$$



<u>Oracle</u> problem

Given a way of evaluating f

Want to know ty of f

How many we evaluate

f to question?

Quantum

Ev inputs

n)

end.

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|a_n\rangle$$

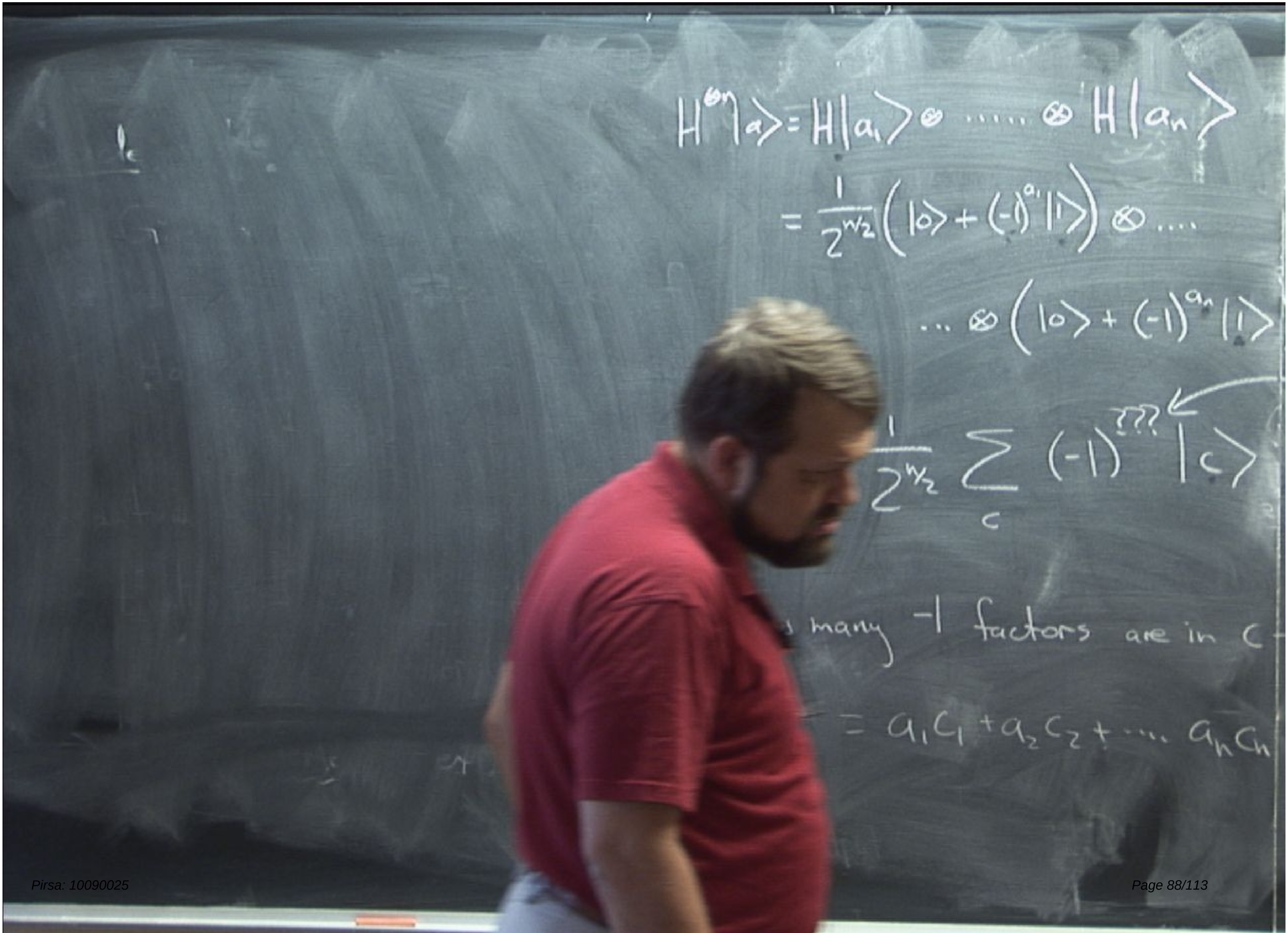
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$

$$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{???} |c\rangle$$

How many -1 factors are in c

$$= a_1c_1 + a_2c_2 + \cdots a_nc_n$$



ℓ_c

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \ldots\ldots \otimes H|a_n\rangle$$

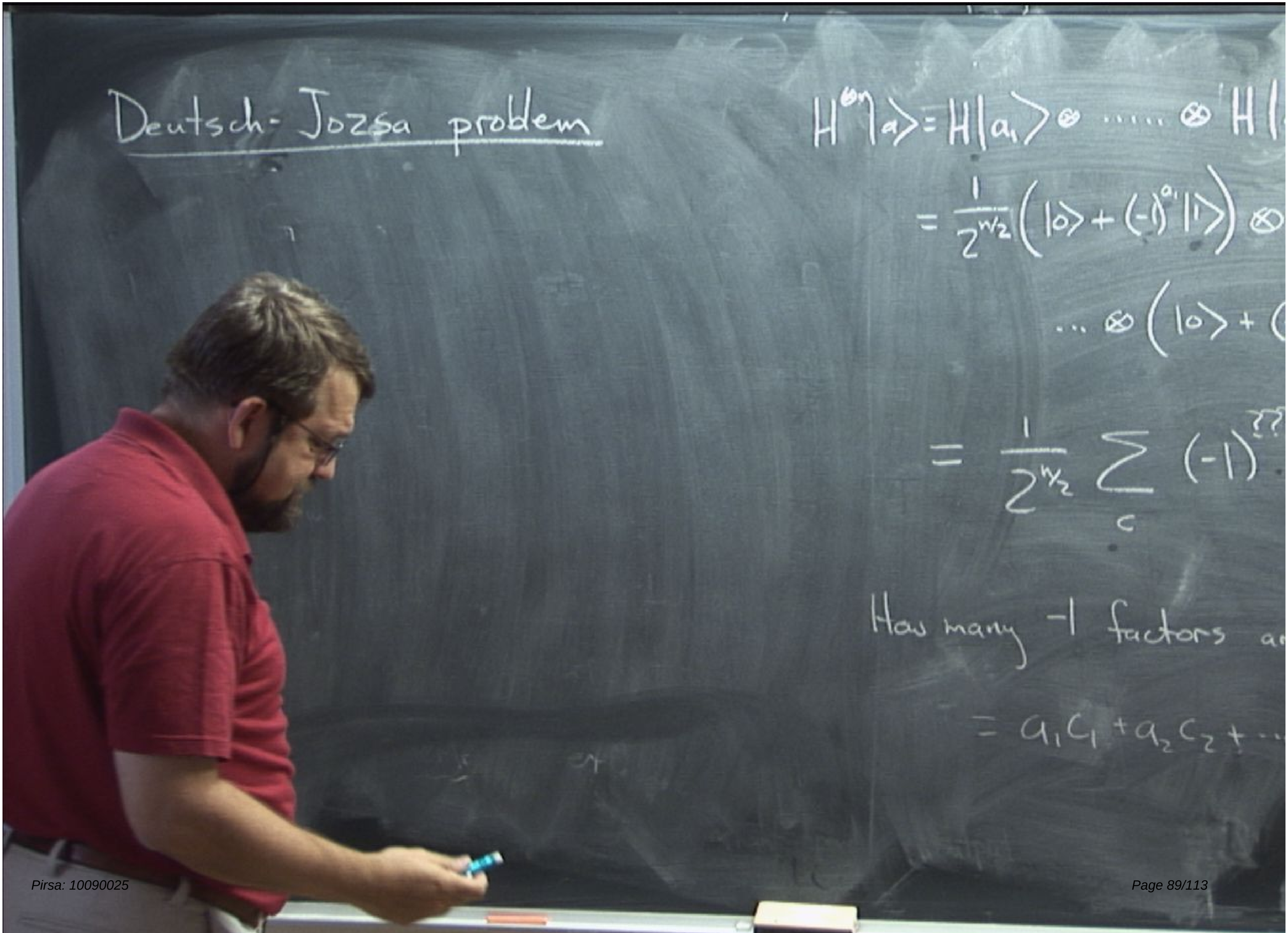
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes \ldots.$$

$$\ldots \otimes \left(|0\rangle + (-1)^{a_n}|1\rangle\right.$$

$$\frac{1}{2^{n/2}} \sum_{c} (-1)^{???} |c\rangle$$

many -1 factors are in c

$$= a_1c_1 + a_2c_2 + \ldots\, a_nc_n$$



Deutsch-Jozsa problem

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$$

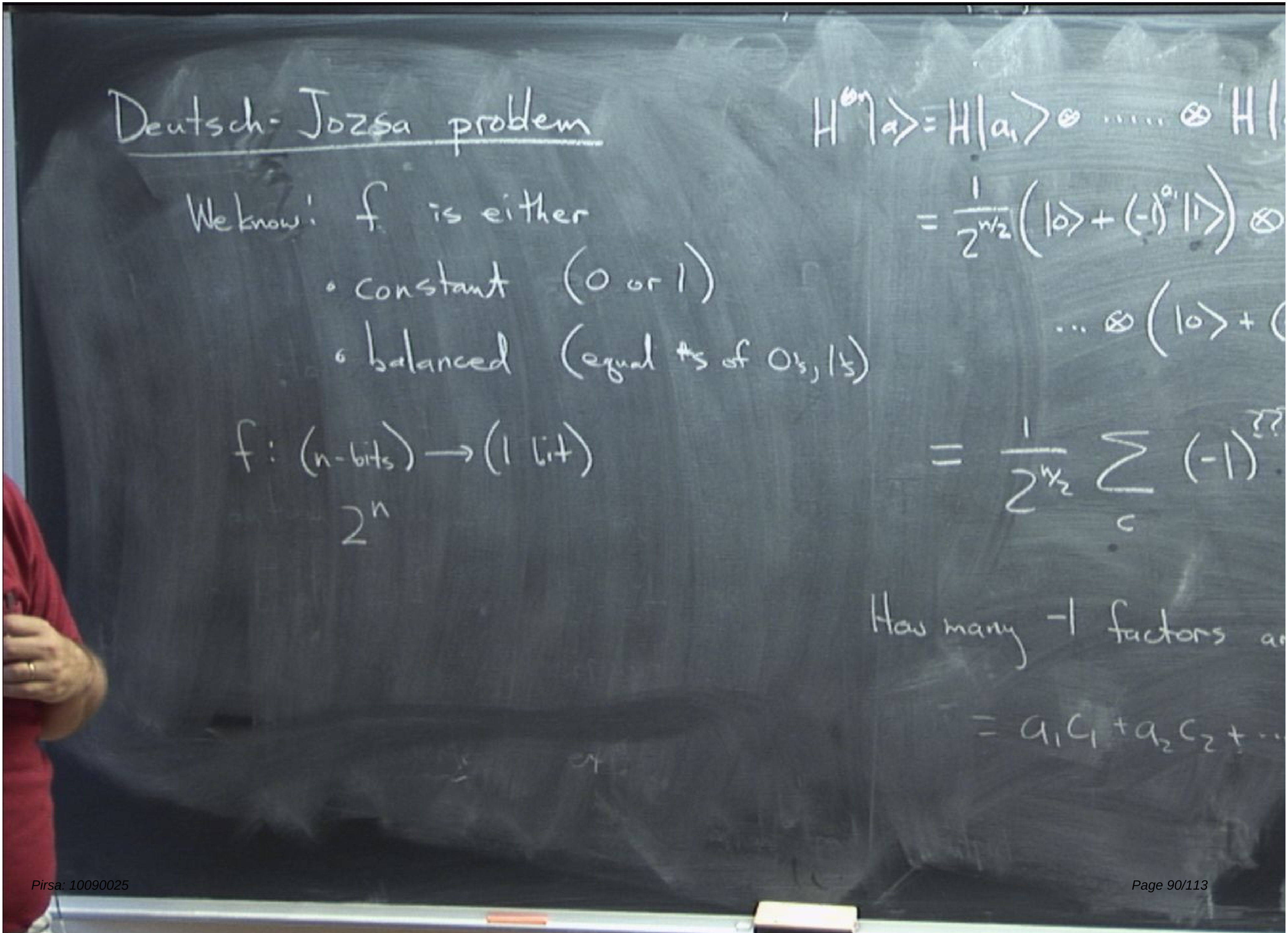
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$$

$$\cdots \otimes \left(|0\rangle + (\right.$$

$$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{??}$$

How many -1 factors a

$$= a_1 c_1 + a_2 c_2 + \cdots$$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

$f: (n\text{-bits}) \longrightarrow (1 \text{ bit})$

2^n

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$$

$$\cdots \otimes \left(|0\rangle + (\right.$$

$$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{??}$$

How many -1 factors a

$$= a_1 c_1 + a_2 c_2 + \cdots$$

Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

$f : (n\text{-bits}) \longrightarrow (1 \text{ bit})$

2^n

How many times must we evaluate f to be sure which?

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$$

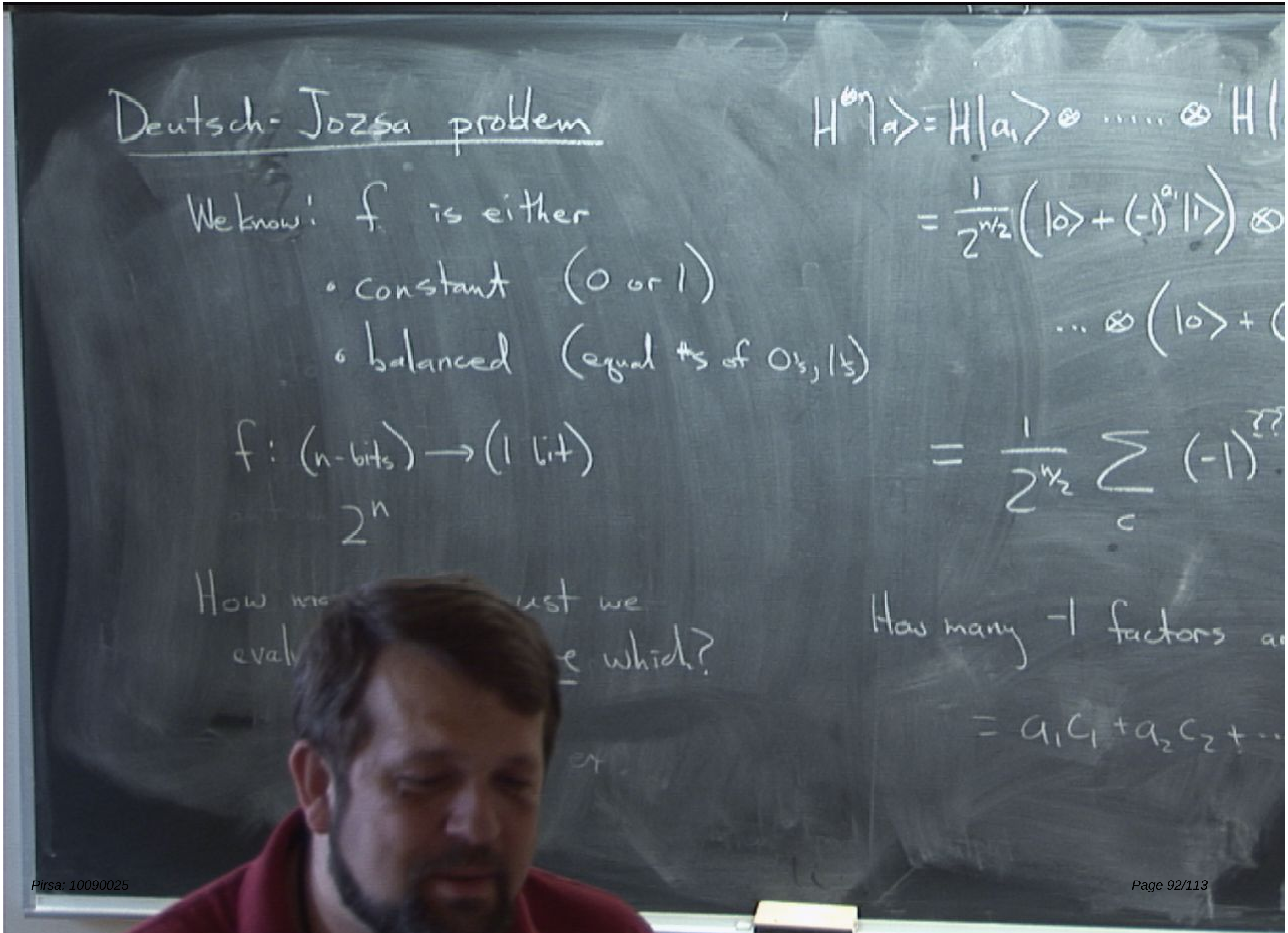
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$$

$$\cdots \otimes \left(|0\rangle + (\right.$$

$$= \frac{1}{2^{n/2}} \sum_c (-1)^{??}$$

How many -1 factors a

$$= a_1 c_1 + a_2 c_2 + \cdots$$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

$f: (n\text{-bits}) \longrightarrow (1 \text{ bit})$

2^n

How m ust we

eval e which?

er

$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$

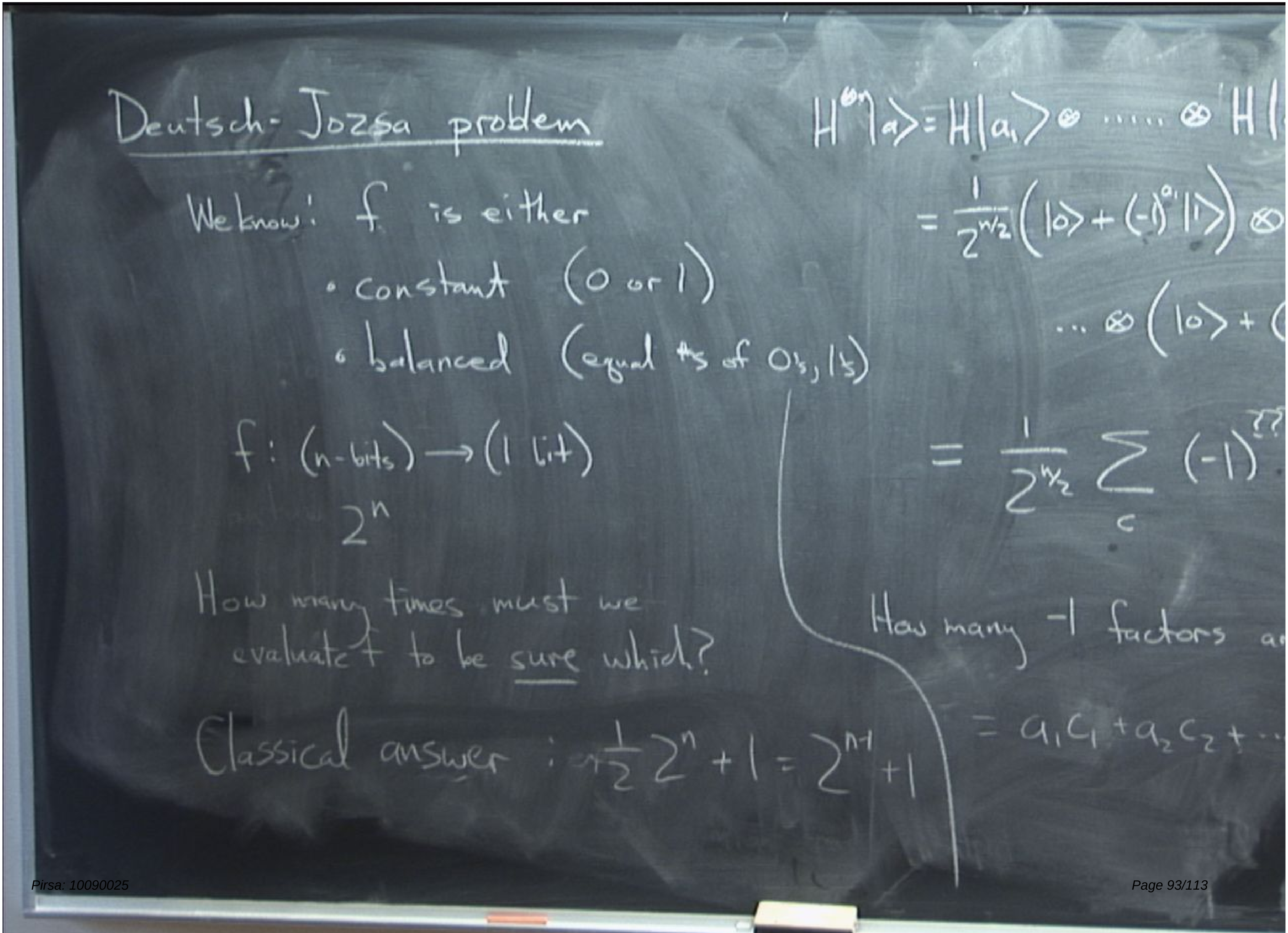
$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$

$\cdots \otimes \left(|0\rangle + (\right.$

$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{??}$

How many −1 factors a

$= a_1c_1 + a_2c_2 + \cdots$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

$f : (n\text{-bits}) \longrightarrow (1 \text{ bit})$

2^n

How many times must we evaluate f to be <u>sure</u> which?

Classical answer : $\frac{1}{2} 2^n + 1 = 2^{n-1} + 1$

$H^{\otimes n} |a\rangle = H|a_1\rangle \otimes \ldots\ldots \otimes H|$

$= \frac{1}{2^{n/2}} \left(|0\rangle + (-1)^{a_1} |1\rangle \right) \otimes$

$\ldots \otimes \left(|0\rangle + (\right.$

$= \frac{1}{2^{n/2}} \sum_c (-1)^{??}$

How many −1 factors ar

$= a_1 c_1 + a_2 c_2 + \cdots$

Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

f: (n-bits) → (1 bit)

2^n

How many times must we evaluate f to be sure which?

Classical answer: $\frac{1}{2} 2^n + 1 = 2^{n-1} + 1$

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \ldots\ldots \otimes H|$$

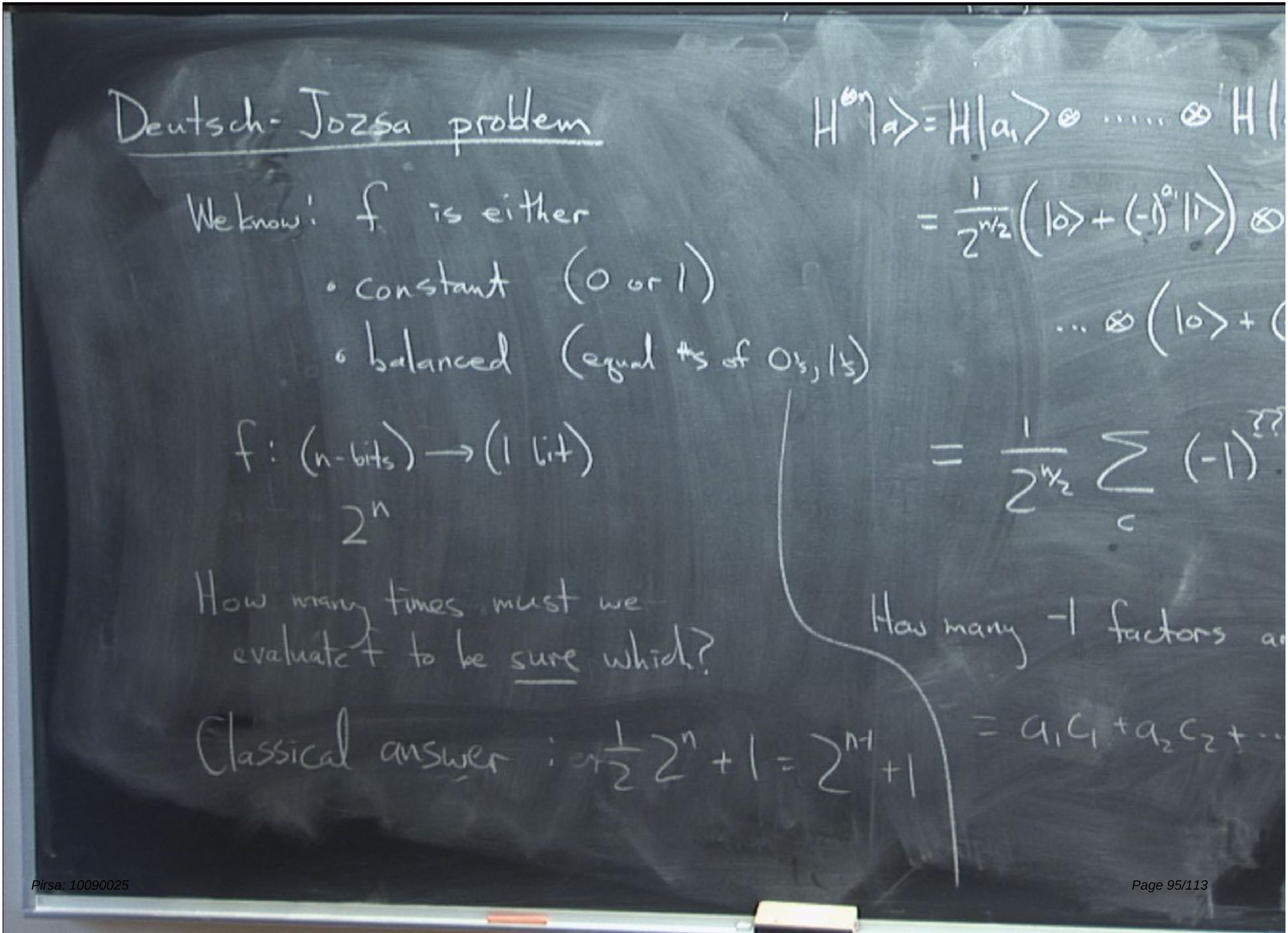
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$$

$$\ldots \otimes \left(|0\rangle + (\right.$$

$$= \frac{1}{2^{n/2}} \sum_c (-1)^{??}$$

How many −1 factors a

$$= a_1 c_1 + a_2 c_2 + \cdots$$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

$f: (n\text{-bits}) \longrightarrow (1\text{ bit})$

2^n

How many times must we evaluate f to be sure which?

Classical answer : $\frac{1}{2}2^n + 1 = 2^{n-1}+1$

$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$

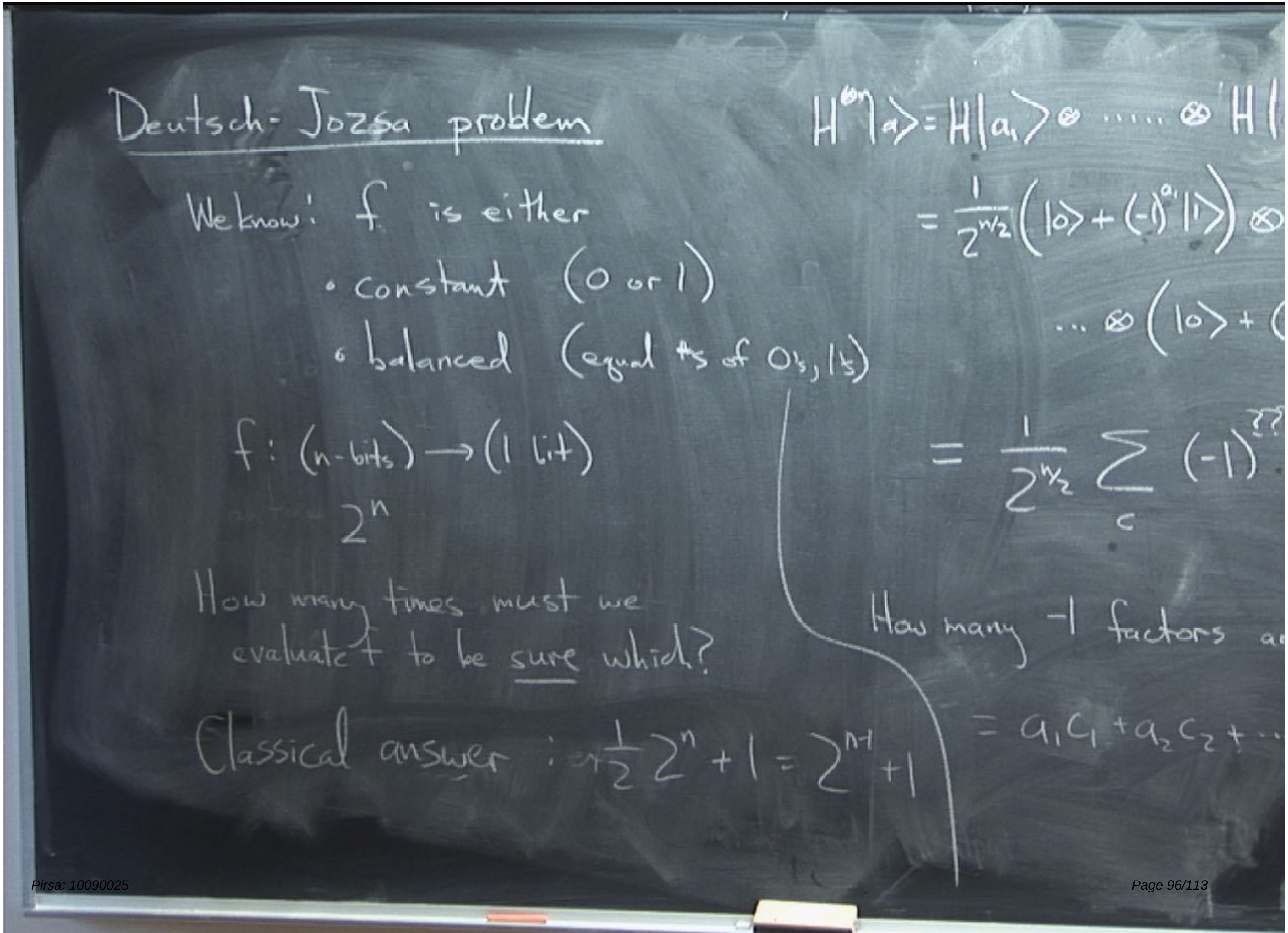
$= \frac{1}{2^{n/2}}\Big(|0\rangle + (-1)^{a_1}|1\rangle\Big) \otimes$

$\cdots \otimes \Big(|0\rangle + ($

$= \frac{1}{2^{n/2}} \sum_{c} (-1)^{??}$

How many -1 factors a

$= a_1c_1 + a_2c_2 + \cdots$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's, 1's)

f: (n-bits) → (1 bit)

2^n

How many times must we evaluate f to be sure which?

Classical answer: $\frac{1}{2}2^n + 1 = 2^{n-1} + 1$

$$H^{\otimes n}|a\rangle = H|a_1\rangle \otimes \cdots\cdots \otimes H|$$

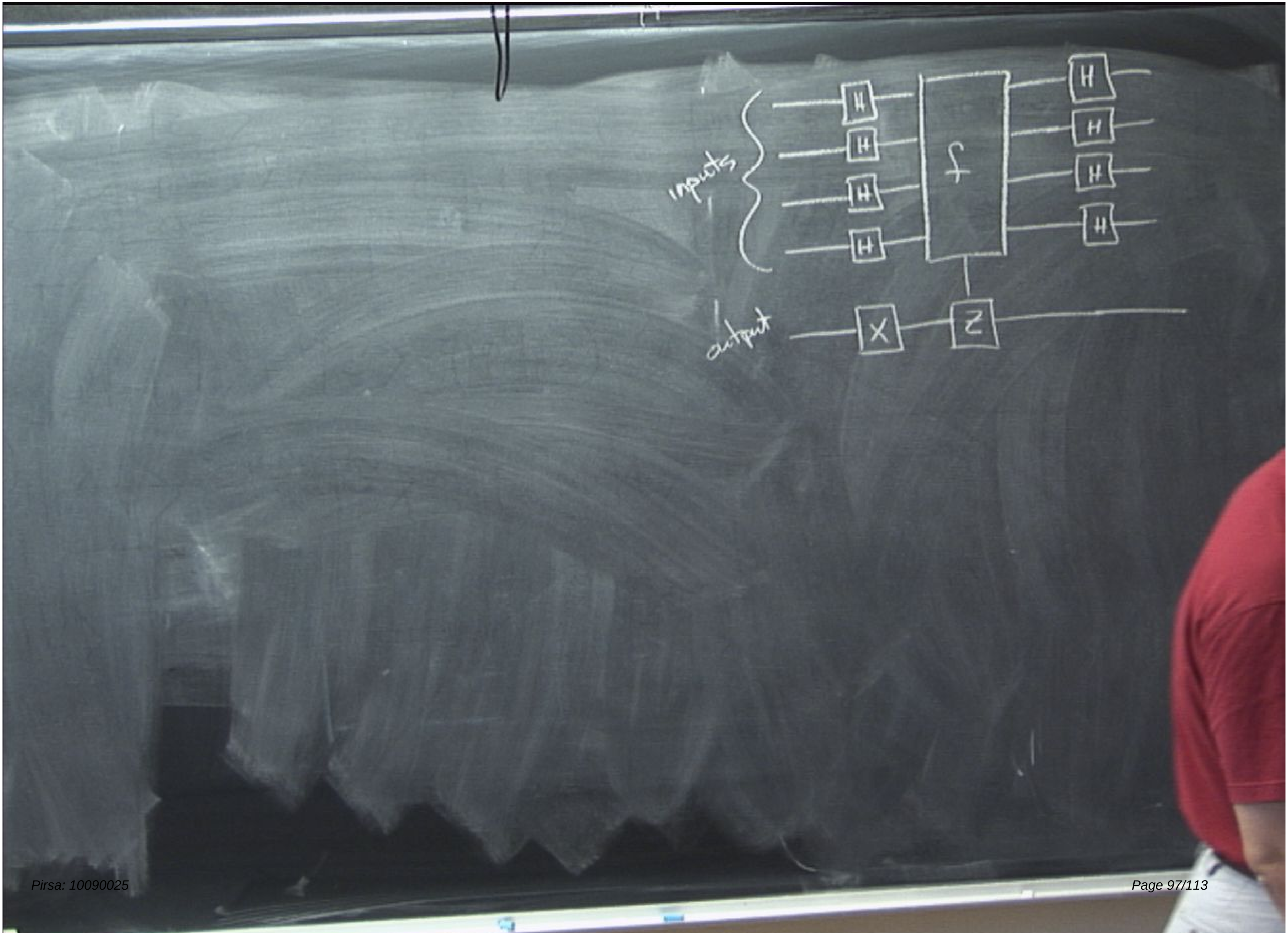
$$= \frac{1}{2^{n/2}}\left(|0\rangle + (-1)^{a_1}|1\rangle\right) \otimes$$

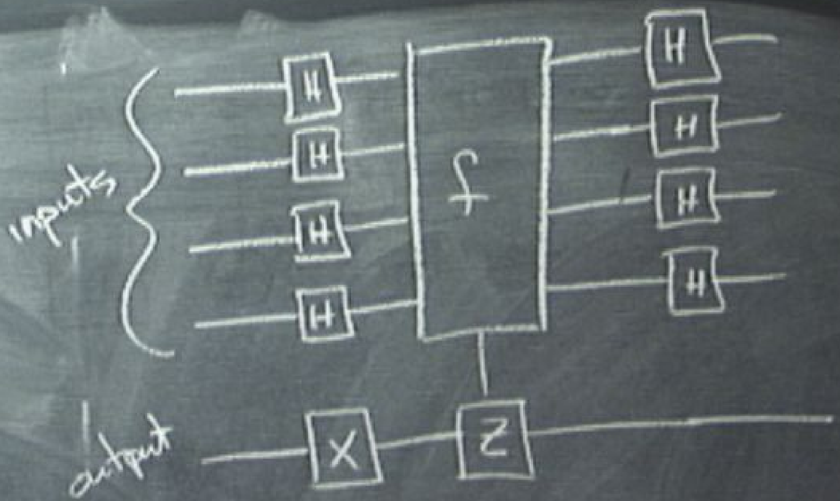
$$\cdots \otimes \left(|0\rangle + (\right.$$

$$= \frac{1}{2^{n/2}} \sum_c (-1)^{??}$$

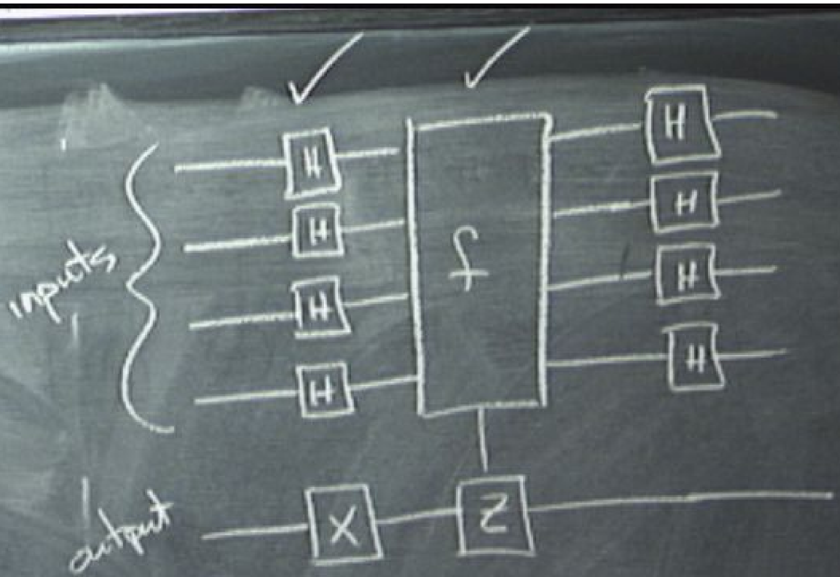
How many −1 factors a

$$= a_1 c_1 + a_2 c_2 + \cdots$$


inputs
H
H
H
H
f
H
H
H
H
output
X
Z

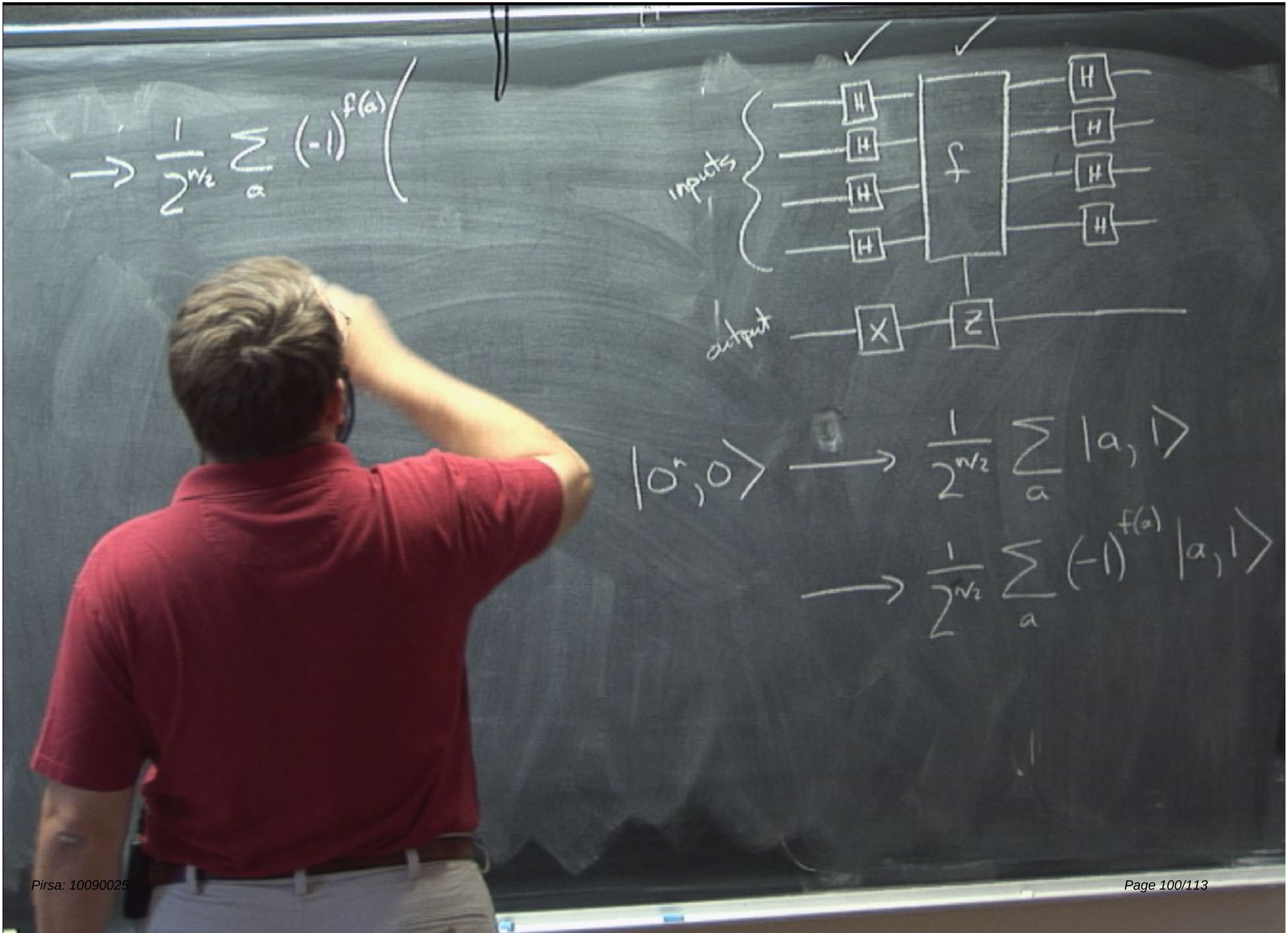


$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}}\sum_{a}|a,1\rangle$$



$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}}\sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}}\sum_a (-1)$$

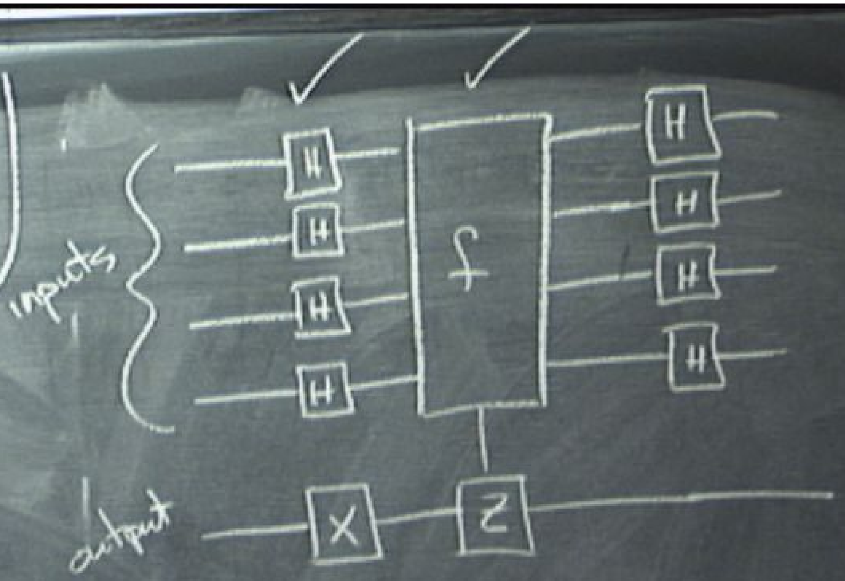


$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \Big($$

$$|0^n, 0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a, 1\rangle$$

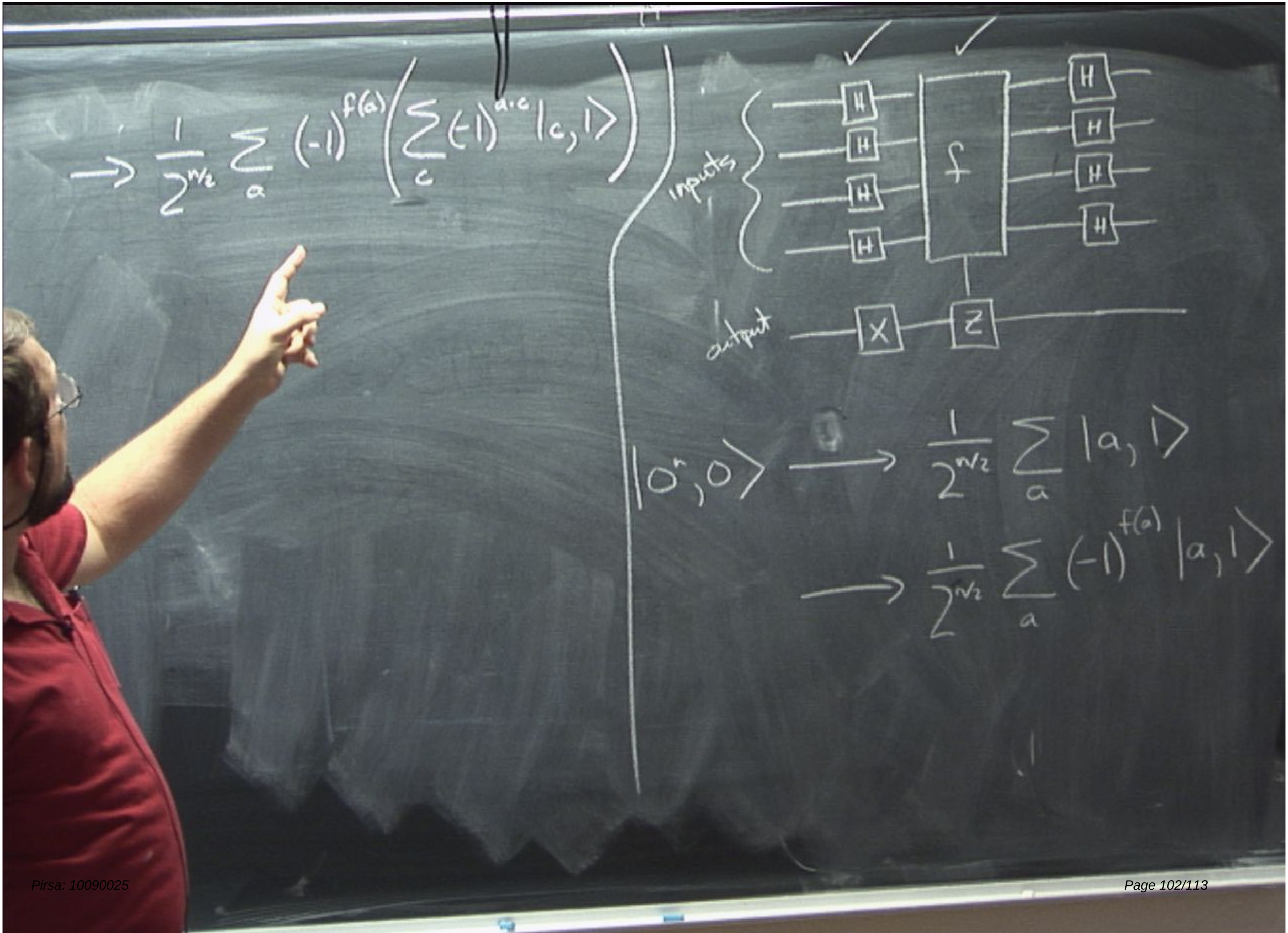
$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} |a, 1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$



$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

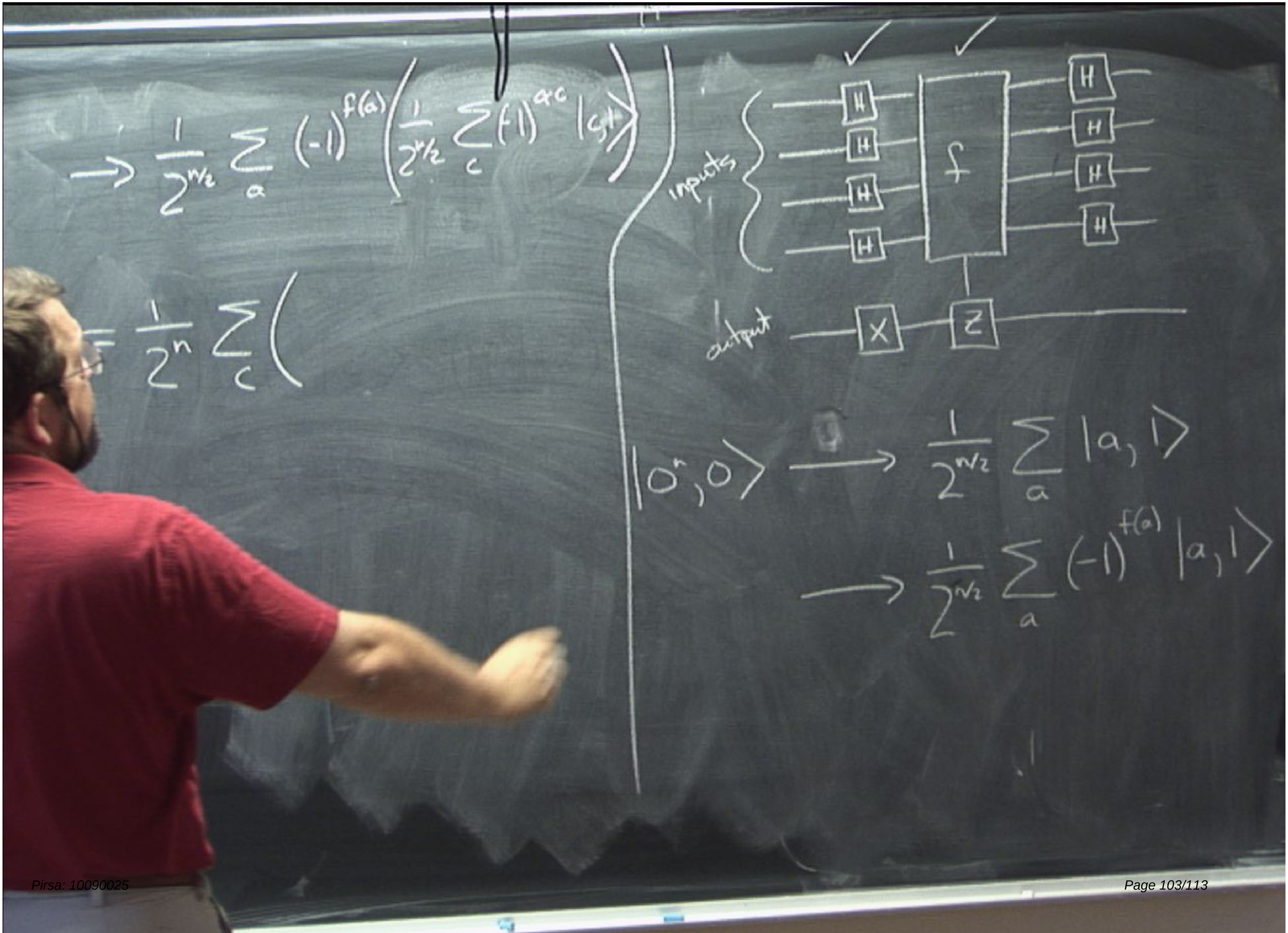
$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} |a,1\rangle$$



$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

$$|0^n, 0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} |a,1\rangle$$



$$\longrightarrow \frac{1}{2^{n/2}} \sum_{a} (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_{c} (-1)^{a c} |c,1\rangle \right)$$

$$= \frac{1}{2^{n}} \sum_{c} \Big($$

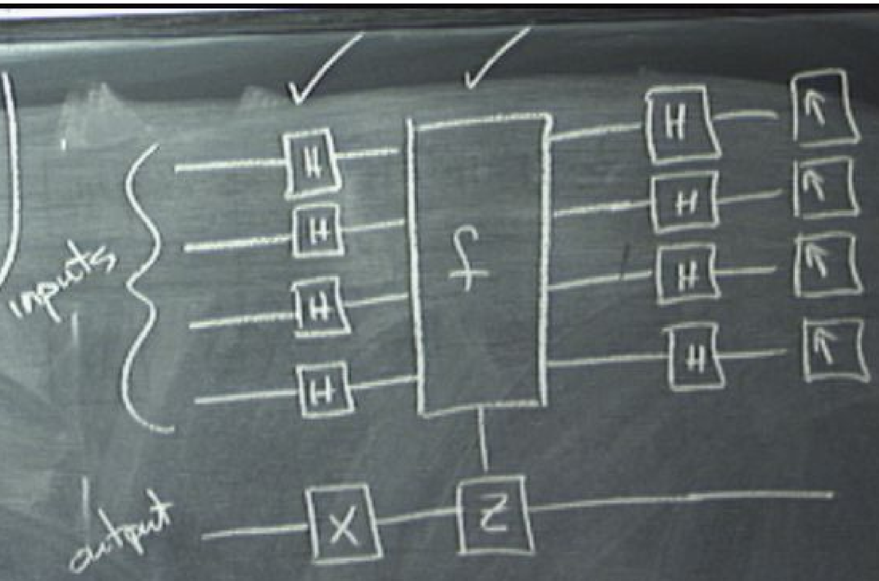
$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{a} |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_{a} (-1)^{f(a)} |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

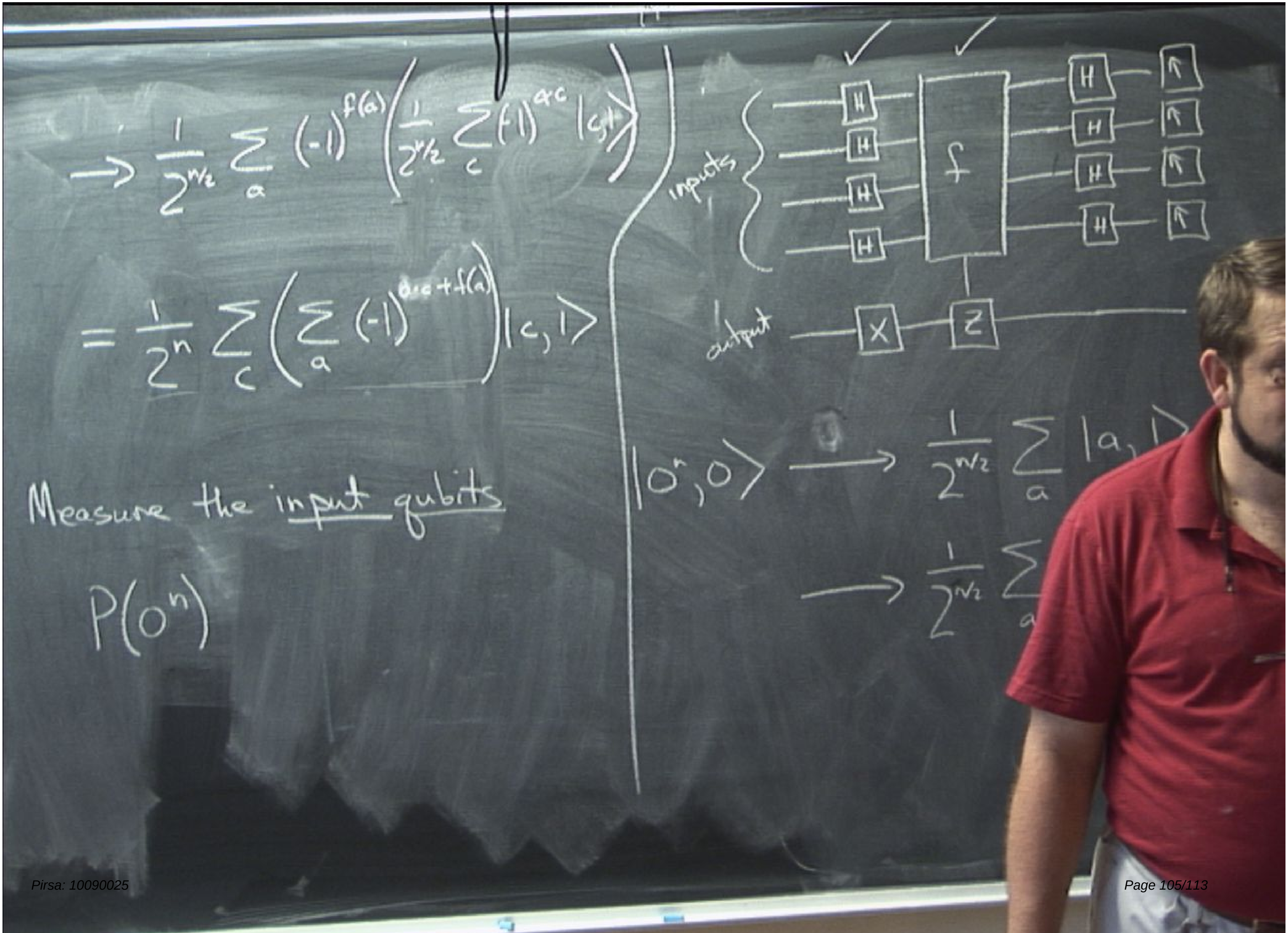
$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a\cdot c + f(a)} \right) |c,1\rangle$$

Measure the input qubits



$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} |a,1\rangle$$



$$\rightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a\cdot c + f(a)} \right) |c,1\rangle$$

Measure the input qubits

$$P(0^n)$$

$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

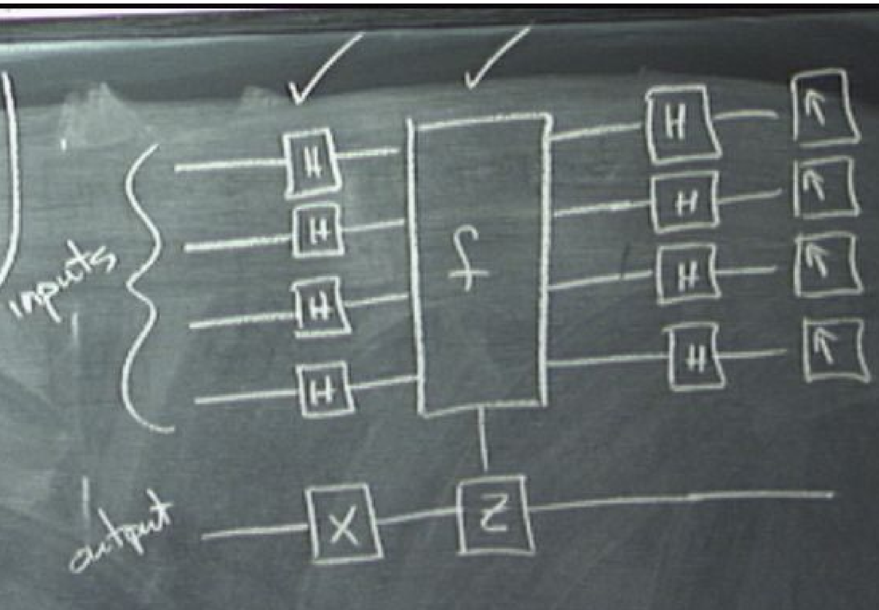
$$\longrightarrow \frac{1}{2^{n/2}} \sum_a$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a\cdot c + f(a)} \right) |c,1\rangle$$

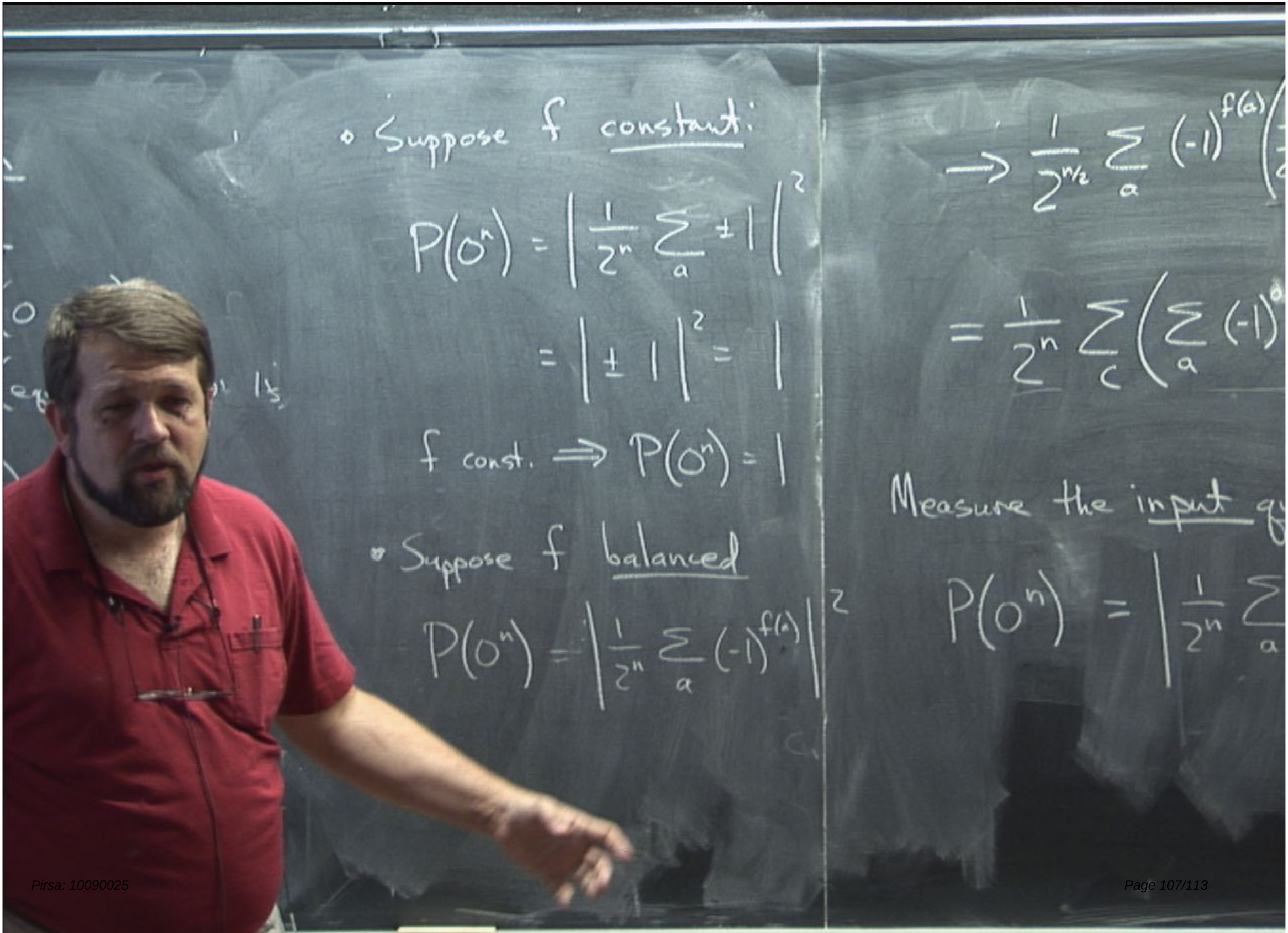
Measure the input qubits

$$P(0^n) = \left| \frac{1}{2^n} \sum_a (-1)^{f(a)} \right|^2$$



$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} |a,1\rangle$$



• Suppose f constant:

$$P(0^n) = \left| \frac{1}{2^n} \sum_a \pm 1 \right|^2$$

$$= \left| \pm 1 \right|^2 = 1$$

f const. $\Longrightarrow P(0^n) = 1$

• Suppose f balanced

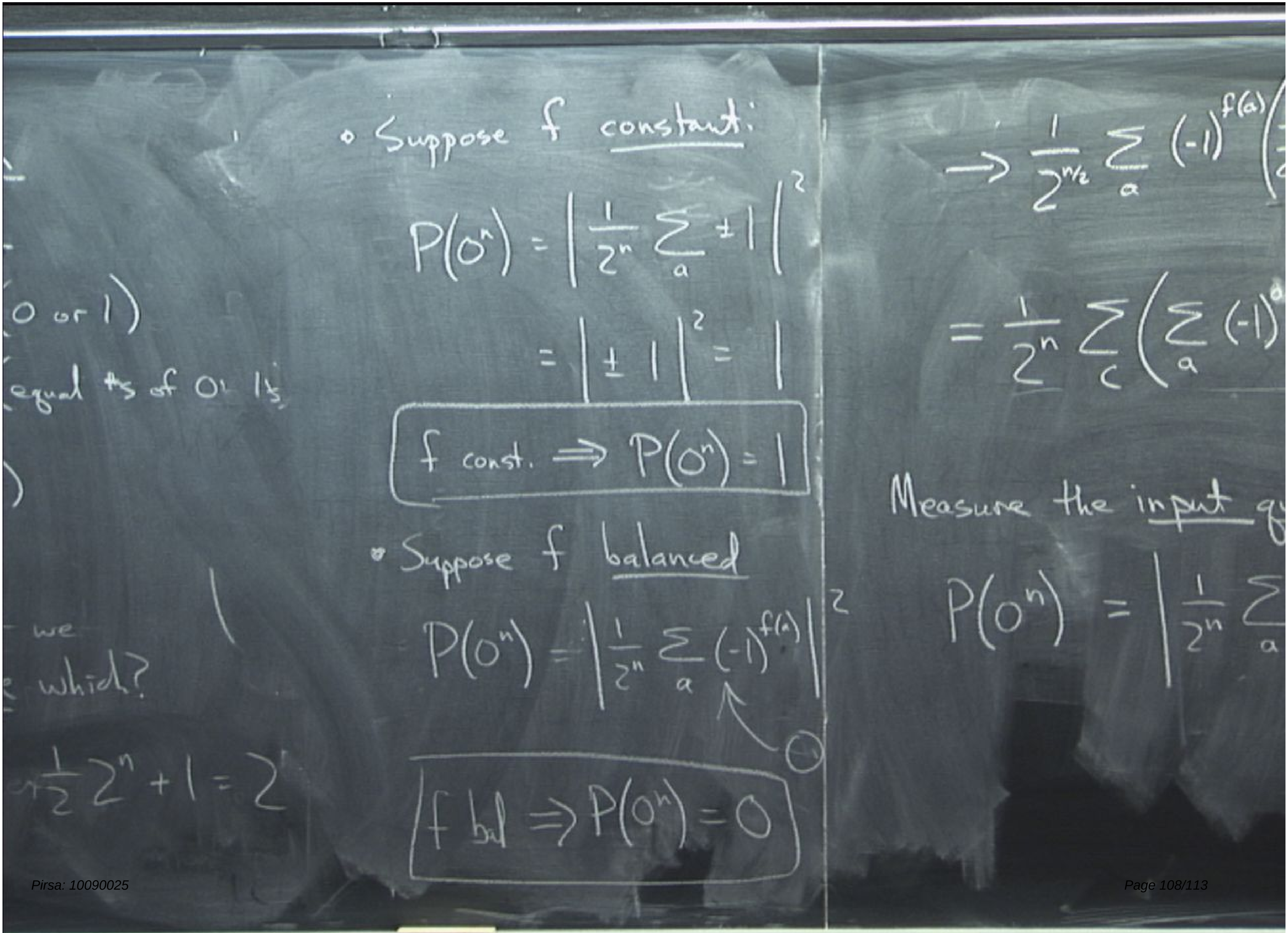
$$P(0^n) = \left| \frac{1}{2^n} \sum_a (-1)^{f(a)} \right|^2$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \Big($$

$$= \frac{1}{2^n} \sum_c \Big(\sum_a (-1)$$

Measure the input q

$$P(0^n) = \Big| \frac{1}{2^n} \sum_a$$



(0 or 1)

equal #s of 0's 1's

)

we

which?

$\frac{1}{2}2^n + 1 = 2$

• Suppose f constant:

$$P(0^n) = \left|\frac{1}{2^n}\sum_a \pm 1\right|^2$$

$$= |\pm 1|^2 = 1$$

$$\boxed{f \text{ const.} \Rightarrow P(0^n) = 1}$$

• Suppose f balanced

$$P(0^n) = \left|\frac{1}{2^n}\sum_a \underset{\bigcirc}{(-1)^{f(a)}}\right|^2$$

$$\boxed{f \text{ bal} \Rightarrow P(0^n) = 0}$$

$$\rightarrow \frac{1}{2^{n/2}}\sum_a (-1)^{f(a)}\Big($$

$$= \frac{1}{2^n}\sum_c \Big(\sum_a (-1)$$

Measure the input q

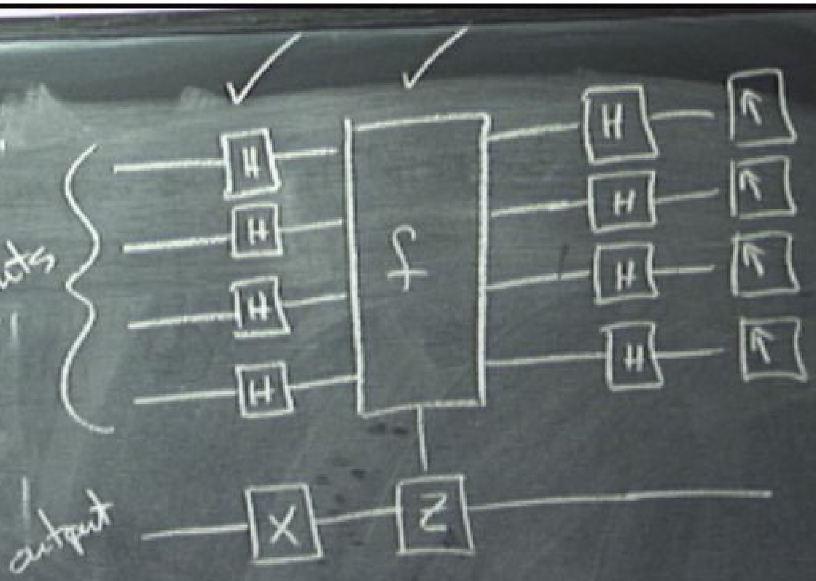
$$P(0^n) = \Big|\frac{1}{2^n}\sum_a$$

$$\rightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a \cdot c} |c, 1\rangle \right)$$

$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a \cdot c + f(a)} \right) |c, 1\rangle$$

asure the input qubits

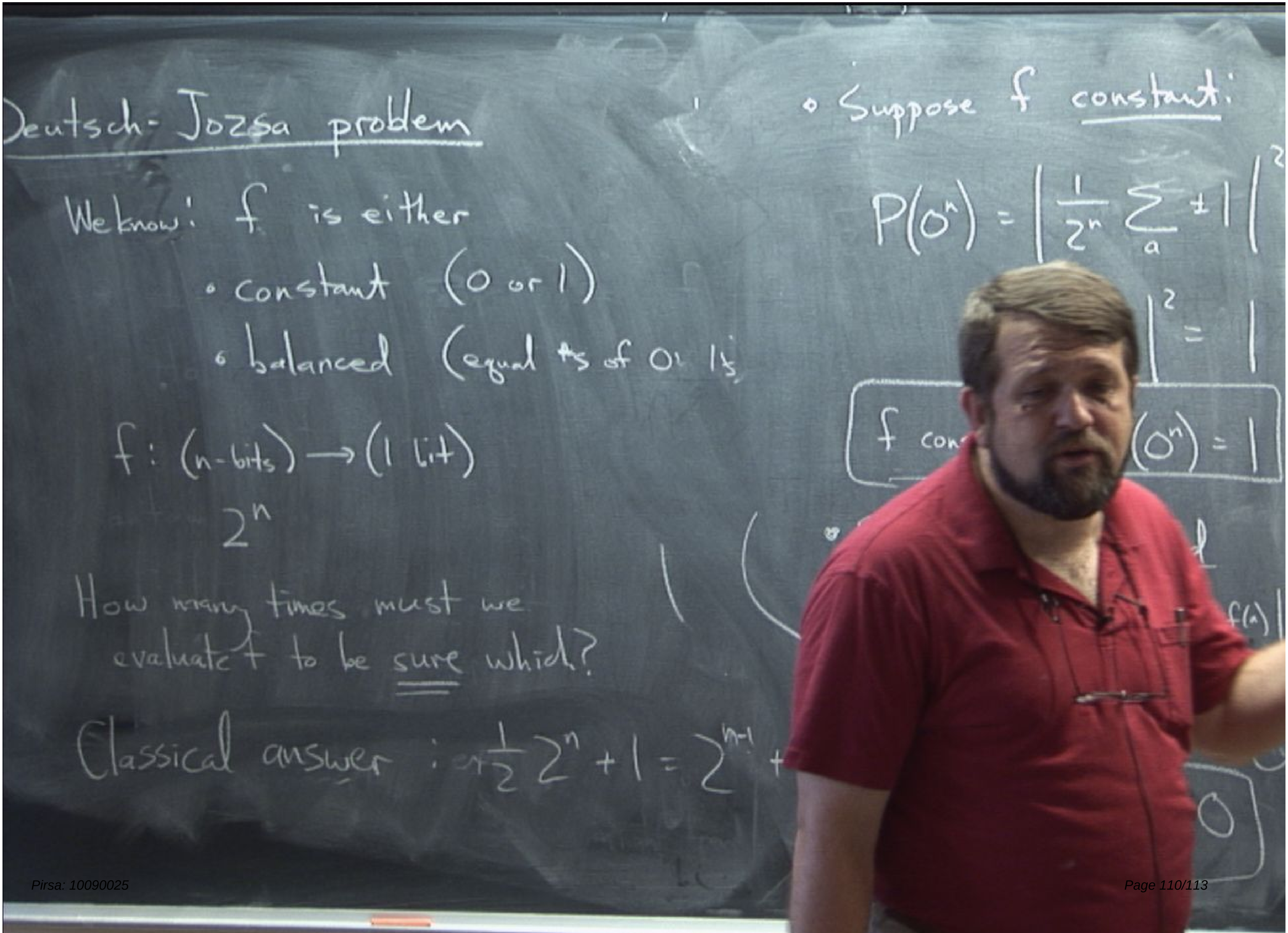
$$P(0^n) = \left| \frac{1}{2^n} \sum_a (-1)^{f(a)} \right|^2$$



$$|0^n, 0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a, 1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \underbrace{\sum_a (-1)^{f(a)} |a, 1\rangle}$$

$$= \frac{1}{2^{n/2}} \left(\sum_a (-1)^{f(a)} |a\rangle \right) \otimes |1\rangle$$



Deutsch-Jozsa problem

We know: f is either

- constant (0 or 1)
- balanced (equal #s of 0's 1's

$f: (n\text{-bits}) \longrightarrow (1 \text{ bit})$

2^n

How many times must we evaluate f to be <u>sure</u> which?

Classical answer : $\frac{1}{2}2^n + 1 = 2^{n-1} +$

- Suppose f <u>constant</u>:

$$P(0^n) = \left|\frac{1}{2^n}\sum_a \pm 1\right|^2$$

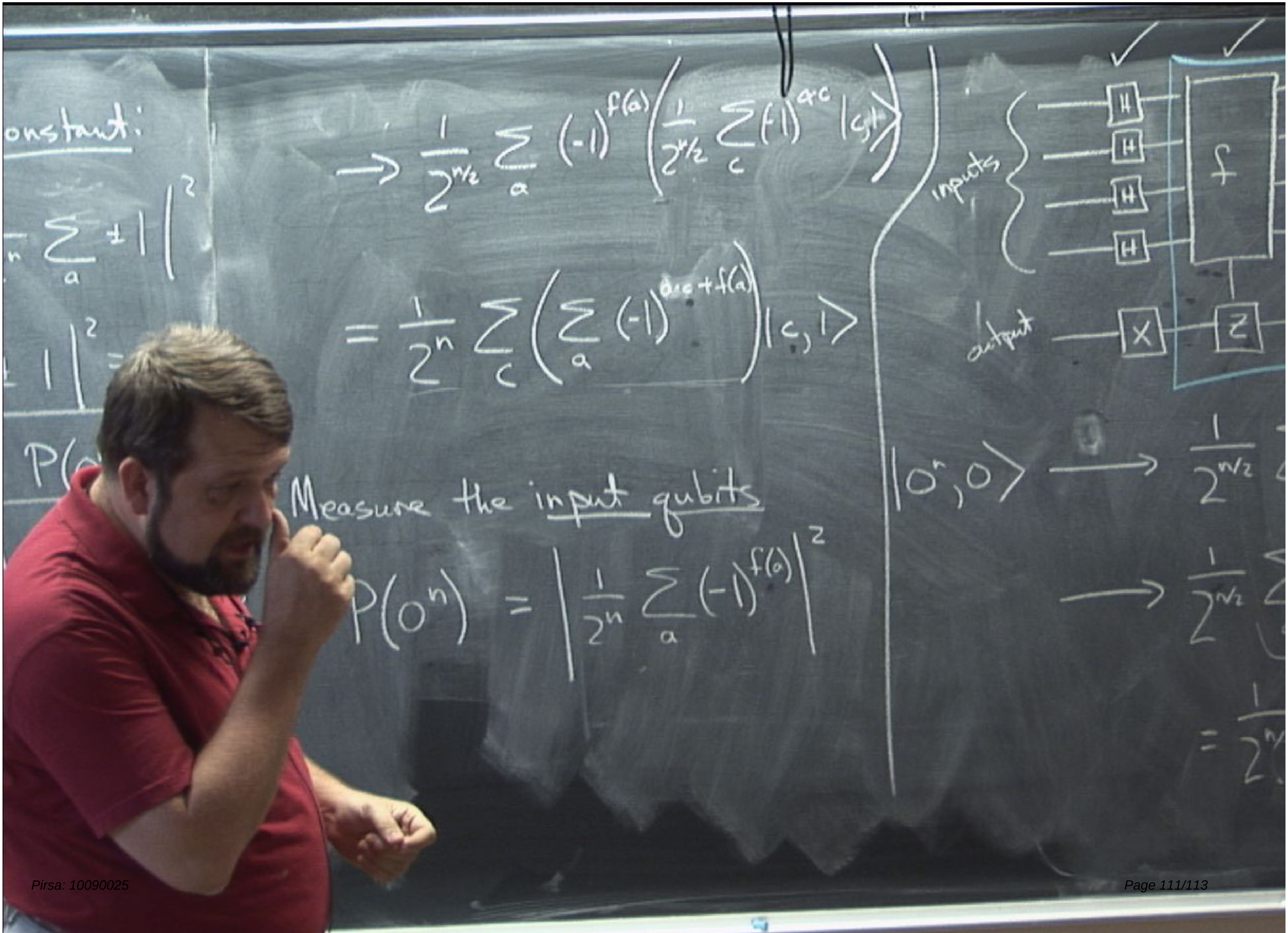
$$\Big|\quad\Big|^2 = 1$$

$$\boxed{f \text{ con} \quad (0^n) = 1}$$

- d

$f(a)|$

0



onstant:

$$\sum_a \pm 1 \Big|^2$$

$$\pm 1 \Big|^2 =$$

P(

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a\cdot c + f(a)} \right) |c,1\rangle$$

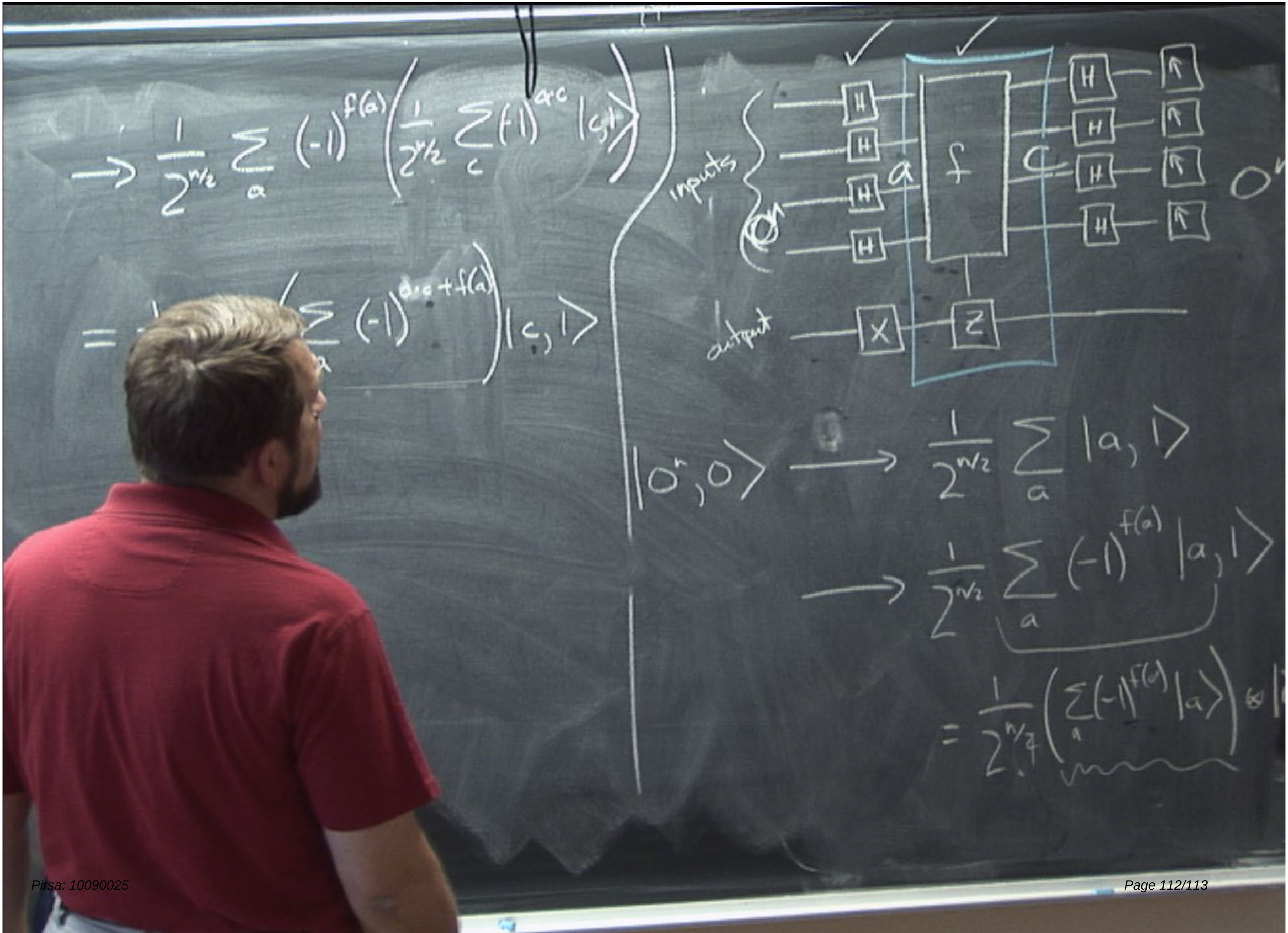
Measure the <u>input qubits</u>

$$P(0^n) = \left| \frac{1}{2^n} \sum_a (-1)^{f(a)} \right|^2$$

$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}}$$

$$\longrightarrow \frac{1}{2^{n/2}}$$

$$= \frac{1}{2^{n/2}}$$



$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a \cdot c} |c,1\rangle \right)$$

$$= \left(\sum_a (-1)^{a \cdot c + f(a)} \right) |c,1\rangle$$

$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \underbrace{\sum_a (-1)^{f(a)} |a,}\, 1\rangle$$

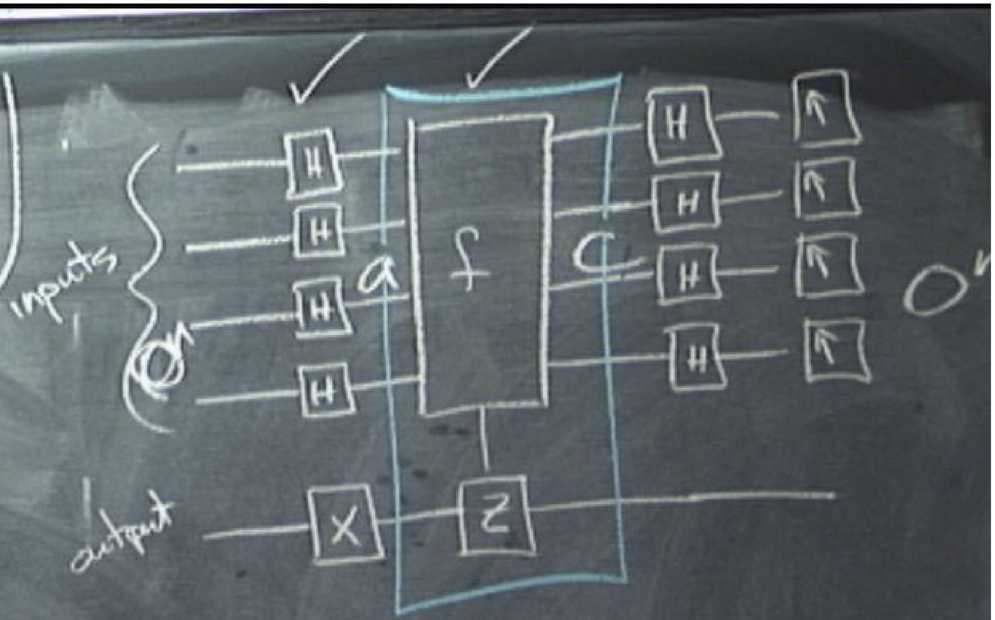
$$= \frac{1}{2^{n/2}} \underbrace{\left(\sum_a (-1)^{f(a)} |a\rangle \right)} \otimes |$$

$$\longrightarrow \frac{1}{2^{n/2}} \sum_a (-1)^{f(a)} \left(\frac{1}{2^{n/2}} \sum_c (-1)^{a\cdot c} |c,1\rangle \right)$$

$$= \frac{1}{2^n} \sum_c \left(\sum_a (-1)^{a\cdot c + f(a)} \right) |c,1\rangle$$

$$0 \nearrow a \longrightarrow c \searrow 0$$

$$\frac{1}{2^n} \sum_a (-1)^{f(a)}.$$



$$|0^n,0\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_a |a,1\rangle$$

$$\longrightarrow \frac{1}{2^{n/2}} \underbrace{\sum_a (-1)^{f(a)} |a,1\rangle}$$

$$= \frac{1}{2^{n/2}} \underbrace{\left(\sum_a (-1)^{f(a)} |a\rangle \right)} \otimes |$$