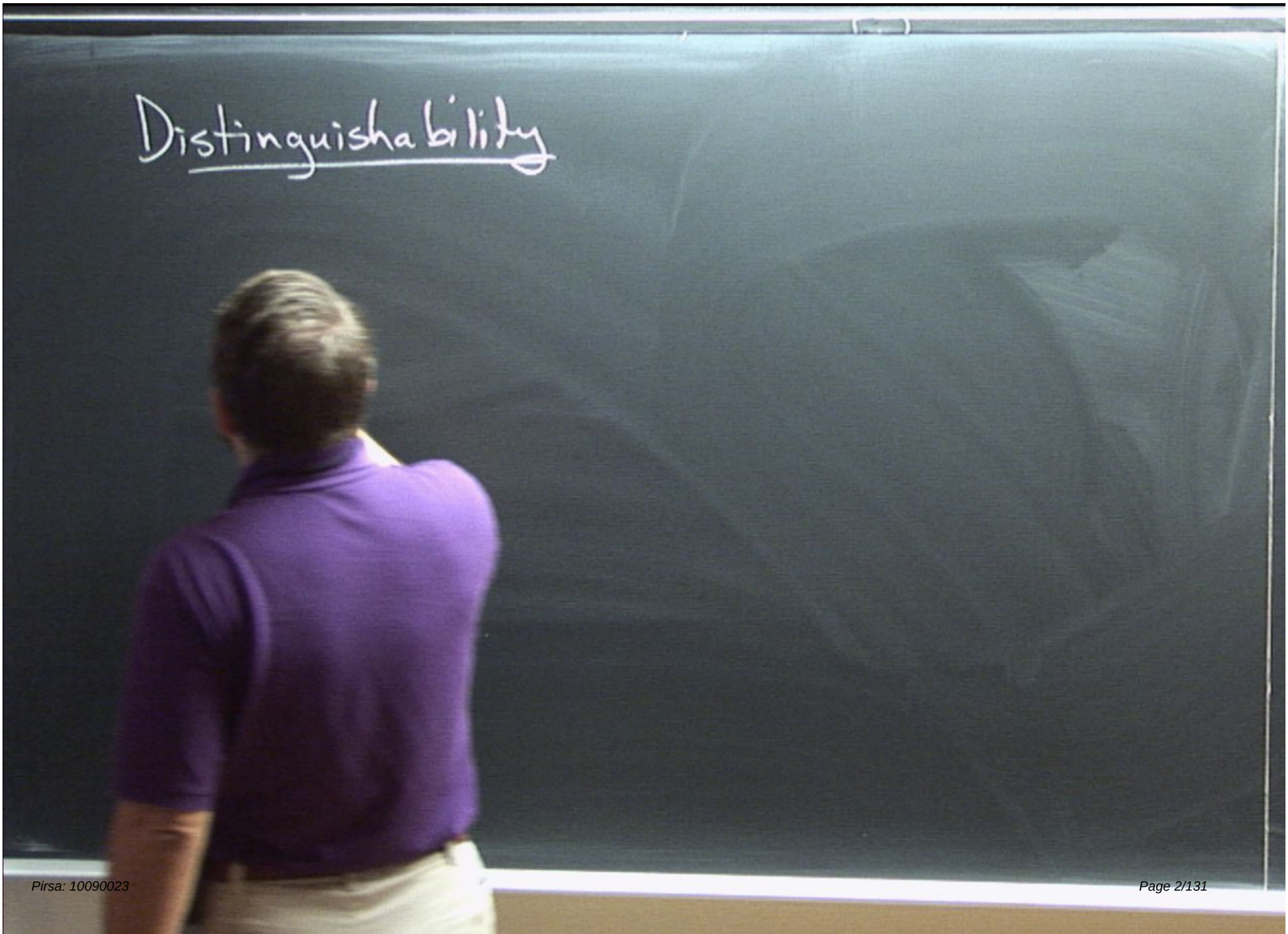
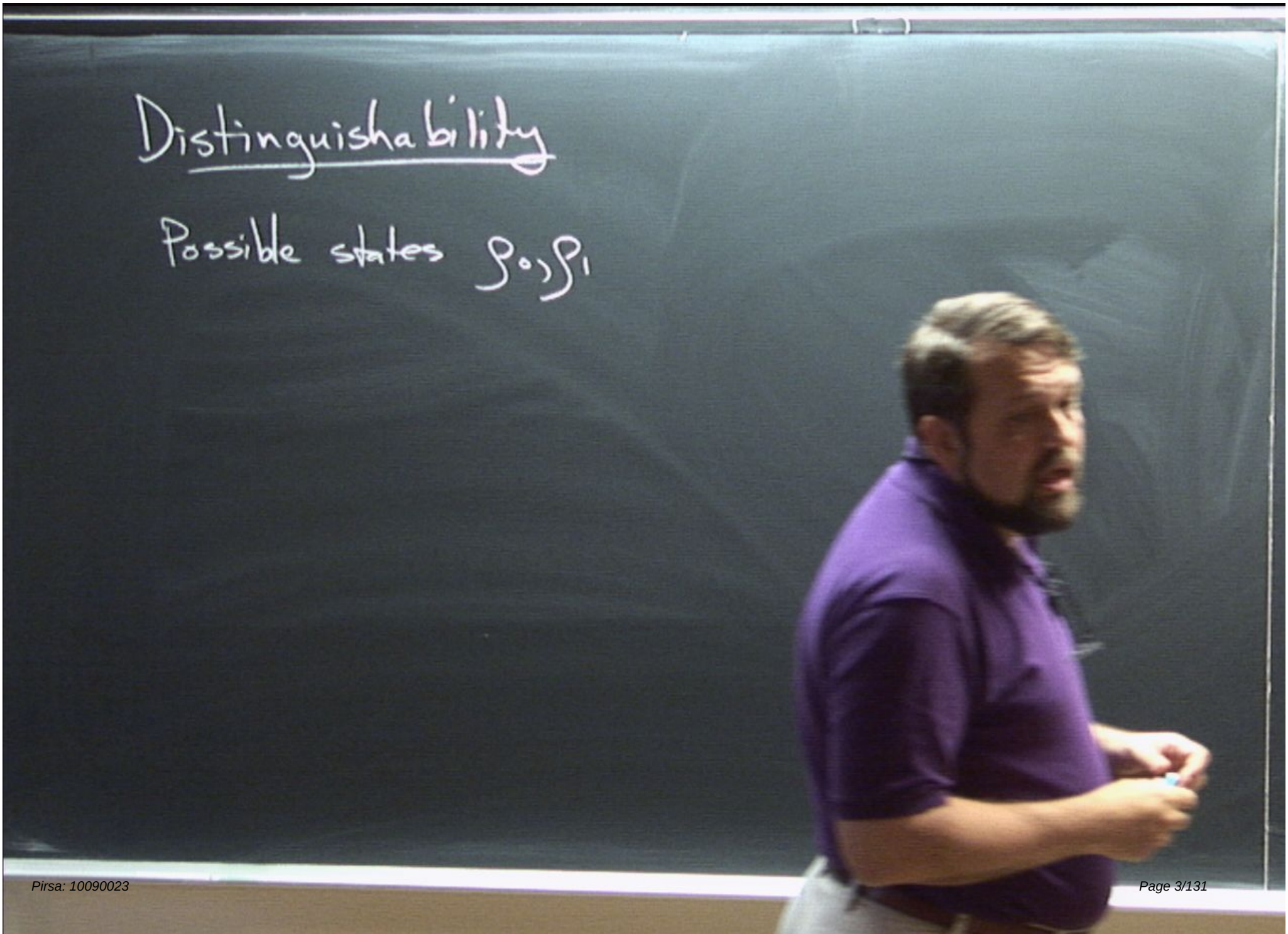
Title: Quantum Theory (PHYS 605) - Lecture 12

Date: Sep 28, 2010 09:00 AM

URL: http://pirsa.org/10090023

Abstract:


Distinguishability


Distinguishability
Possible states ρ_0, ρ_1

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result $0 \Rightarrow$ infer ρ_0

" $1 \Rightarrow$ " ρ_1

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_0)$$

Distinguishability

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right.$$

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2}P(0|\rho_0) + \frac{1}{2}P(1|\rho_1)$$

Distinguishability

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2}P(0|\rho_0) + \frac{1}{2}P(1|\rho_1)$$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$= \frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{P_s = \frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$$\Delta = \rho_0 - \rho_1$$

ility

ρ_0, ρ_1

ith prob. $1/2$)

$\{E_0, E_1\}$

$\Rightarrow$ infer ρ_0

$\Rightarrow$ " ρ_1

$s) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$= \frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{P_s = \frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$\Delta = \rho_0 - \rho_1$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalues

ility

ρ_0, ρ_1

ith prob. $1/2$)

$\{E_0, E_1\}$

$\Rightarrow$ infer ρ_0

$\Rightarrow$ " ρ_1

$s) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$= \frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{P_s = \frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$\Delta = \rho_0 - \rho_1$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalues

$P_s = \frac{1}{2}($

$$\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$\frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{\frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$$\Delta = \rho_0 - \rho_1$$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalue

$$P_s = \frac{1}{2}\left(1 + \right.$$

$$\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$\frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{\frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$$\Delta = \rho_0 - \rho_1$$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalue

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$\frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

$$\boxed{\frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$$\Delta = \rho_0 - \rho_1$$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalues

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right)$$

$$E_0 + E_1 = \mathbb{1}$$

$$\frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0 - \rho_1) E_0\right)$$

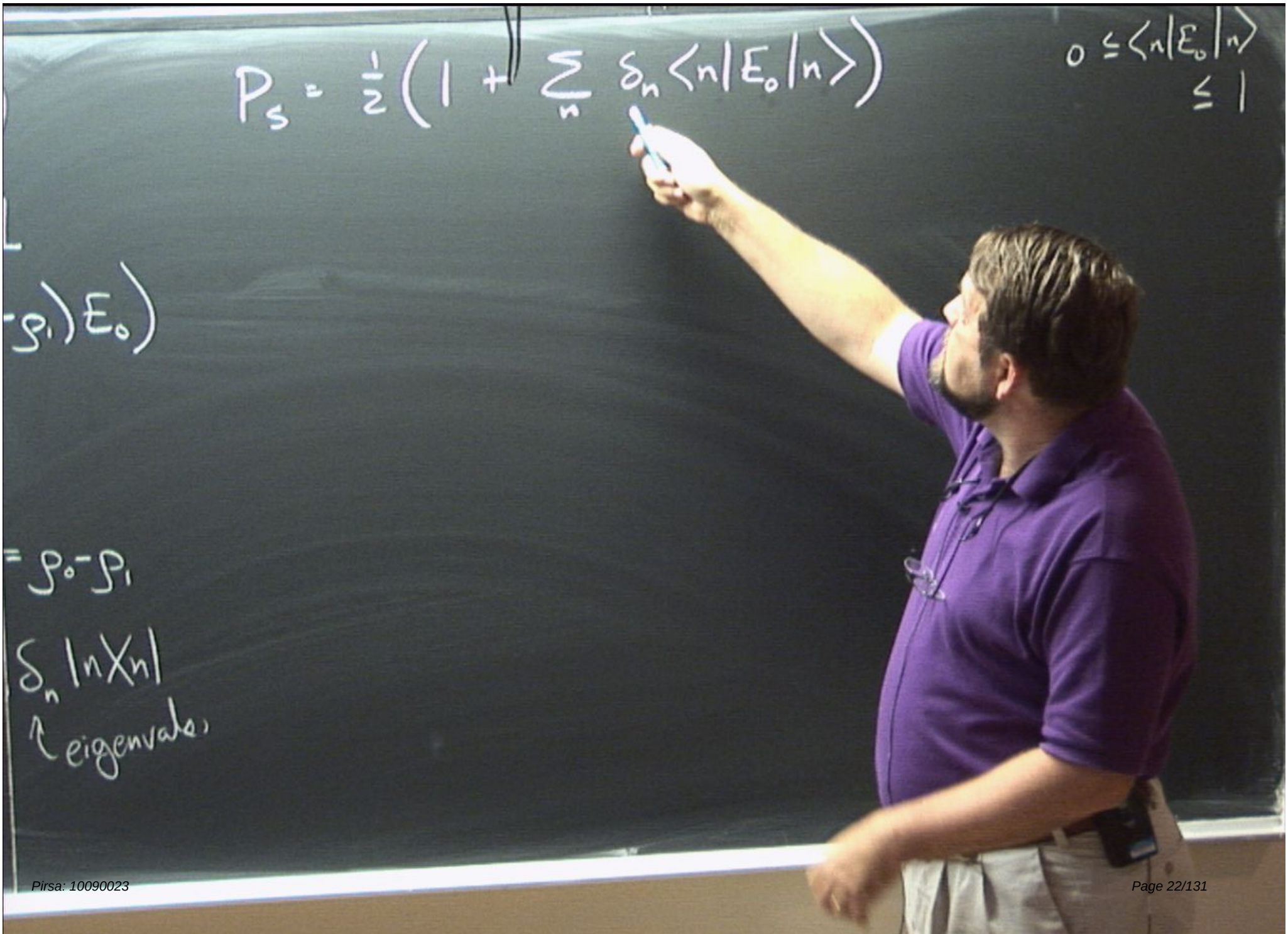
$$\boxed{\frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

$$\Delta = \rho_0 - \rho_1$$

Write $\Delta = \sum_n \delta_n |n\rangle\langle n|$

eigenvalue

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$


$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$
$0 \le \langle n|E_0|n\rangle \le 1$
$-\rho_1)E_0)$
$= \rho_0 - \rho_1$
$\delta_n |n\rangle\langle n|$
eigenvalue

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$)E_0)$

$\rho_0 - \rho_1$

$|n\rangle\langle n|$

eigenvalue

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$)E_0)$

$\rho_0 - \rho_1$

$|n\rangle\langle n|$

eigenvalu

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle$ $\begin{cases} |n\rangle & \delta_n > 0 \\ & \delta_n \le 0 \end{cases}$

$$\boxed{P_s \le P_{s(max)} = \frac{1}{2}\left(1 + \delta_+\right)}$$

sum of pos. eigenvalues of $\Delta = \rho_0 - \rho_1$

$\rho_0 - \rho_1$

$|n\rangle\langle n|$

eigenvalues

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$$\boxed{P_s \le P_{s(max)} = \frac{1}{2}\left(1 + \delta_+\right)}$$

sum of pos. eigenvalues of $\Delta = \rho_0 - \rho_1$

$$\rho_0 = \rho_1 \Rightarrow P_{s(max)} = \frac{1}{2}$$

$)E_0)$

$\rho_0 - \rho_1$

$|n\rangle\langle n|$

eigenvals

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$$\boxed{P_s \le P_{s(max)} = \frac{1}{2}\left(1 + \delta_+\right)}$$

sum of pos. eigenvalues of $\Delta = \rho_0 - \rho_1$

$\rho_0 = \rho_1 \Rightarrow P_{s(max)} = \frac{1}{2}$ (no better than chance)

$\rho_0 \neq \rho_1 \Rightarrow P_{s(max)} > \frac{1}{2}$

$)E_0)$

$\rho_0 - \rho_1$

$|n\rangle\langle n|$

eigenvalues

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \end{cases}$

$$\boxed{P_s \le P_{s(max)} = \frac{1}{2}\left(1 + \delta_+\right)}$$

sum of pos. eigenvalues of $\Delta = \rho_0 - \rho_1$

$\rho_0 = \rho_1 \Rightarrow P_{s(max)} = \frac{1}{2}$ (no better than

$\rho_0 \neq \rho_1 \Rightarrow P_{s(max)} > \frac{1}{2}$

To make $P_{s(max)} = 1$,

$$P_s = \frac{1}{2}\left(1 + \sum_n \delta_n \langle n|E_0|n\rangle\right)$$

$$0 \le \langle n|E_0|n\rangle \le 1$$

To maximize P_s,

Choose E_0 s.t. $E_0|n\rangle = \begin{cases} |n\rangle & \delta_n > 0 \\ 0 & \delta_n \le 0 \end{cases}$

$$\boxed{P_s \le P_{s(max)} = \frac{1}{2}\left(1 + \delta_+\right)}$$

sum of pos. eigenvalues of $\Delta = \rho_0 - \rho_1$

$\rho_0 = \rho_1 \Rightarrow P_{s(max)} = \frac{1}{2}$ (no better than chance)

$\rho_0 \ne \rho_1 \Rightarrow P_{s(max)} > \frac{1}{2}$

To make $P_{s(max)} = 1$, ρ_0 and ρ_1 "live in" orthog. subspaces

Distinguishability

Possible states ρ_0, ρ_1

(each with prob. $1/2$)

Measurement $\{E_0, E_1\}$

result 0 $\Rightarrow$ infer ρ_0

" 1 $\Rightarrow$ " ρ_1

$$P_s = \Pr(\text{success}) = \frac{1}{2} P(0|\rho_0) + \frac{1}{2} P(1|\rho_1)$$

$$P_s = \frac{1}{2}\left(\mathrm{tr}\,\rho_0 E_0 + \mathrm{tr}\,\rho_1 E_1\right.$$

$$E_0 + E_1 =$$

$$= \frac{1}{2}\left(\mathrm{tr}\,\rho_1 \mathbb{1} + \mathrm{tr}\,(\rho_0\right.$$

$$\boxed{P_s = \frac{1}{2}\left(1 + \mathrm{tr}\,\Delta E_0\right)}$$

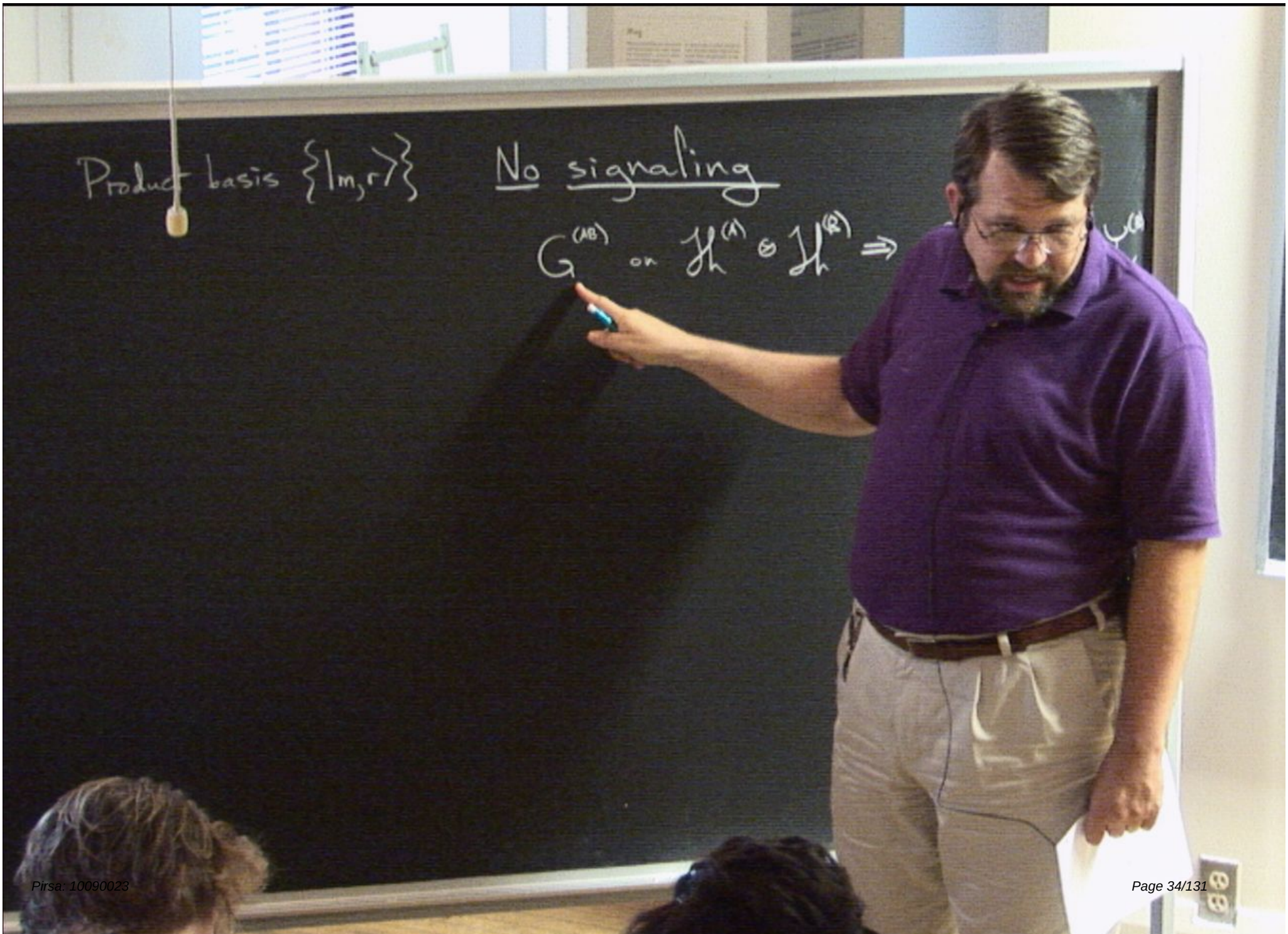
$\Delta =$

Write $\Delta = \sum_n$

No signaling

<u>No signaling</u>

$$G^{(AB)} \text{ on } \mathcal{H}_h^{(A)} \otimes \mathcal{H}_h^{(B)} \Rightarrow G^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$$


Product basis $\{|m,r\rangle\}$
No signaling
$G^{(AB)}$ on $\mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)} \Rightarrow$

Product basis $\{|m,r\rangle\}$

$$G^{(AB)} = \sum_{\substack{m\,r \\ n\,s}} G_{mr,ns}\, |m,r\rangle\langle n,s|$$

$$|m\rangle\langle n| \otimes |r\rangle\langle s|$$

No signaling

$$G^{(AB)} \text{ on } \mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)} \Rightarrow G^{(AB)} = \sum_{\alpha} X_{\alpha}^{(A)} \otimes Y_{\alpha}^{(B)}$$

Product basis $\{|m,r\rangle\}$

$$G^{(AB)} = \sum_{\substack{m\,r \\ n\,s}} G_{mr,ns}\, |m,r\rangle\langle n,s|$$

$$|m\rangle\langle n| \otimes |r\rangle\langle s|$$

<u>No signaling</u>

$$G^{(AB)} \text{ on } \mathcal{H}_h^{(A)} \otimes \mathcal{H}_h^{(B)} \Rightarrow G^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$$

Product basis $\{|m,r\rangle\}$

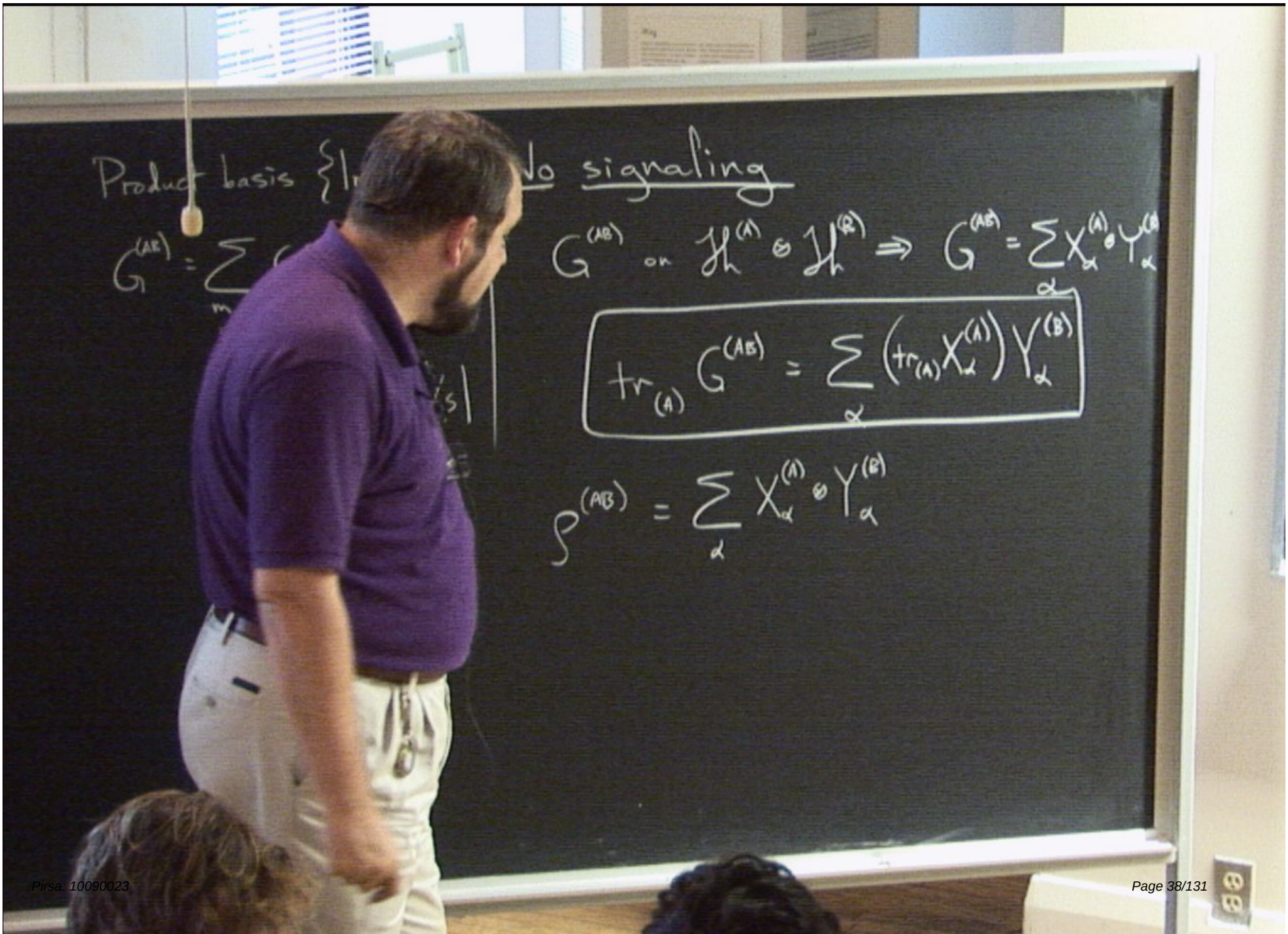
$$G^{(AB)} = \sum_{\substack{m\,r \\ n\,s}} G_{mr,ns}\, |m,r\rangle\langle n,s|$$

$$|m\rangle\langle n| \otimes |r\rangle\langle s|$$

No signaling

$$G^{(AB)} \text{ on } \mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)} \Rightarrow G^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$$

$$\boxed{\mathrm{tr}_{(A)}\, G^{(AB)} = \sum_\alpha \left(\mathrm{tr}_{(A)} X_\alpha^{(A)}\right) Y_\alpha^{(B)}}$$


Product basis
No signaling
$G^{(AB)} = \sum_m$
$G^{(AB)}$ on $\mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)} \Rightarrow G^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$
$\mathrm{tr}_{(A)} G^{(AB)} = \sum_\alpha \left(\mathrm{tr}_{(A)} X_\alpha^{(A)}\right) Y_\alpha^{(B)}$
$\rho^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$

$\mathbb{1} \otimes \mathbb{1}$

$\mathbb{1} \otimes X$, etc.

$X \otimes Y$, etc.

Product basis $\{|m,r\rangle\}$

$$G^{(AB)} = \sum_{\substack{m\,r \\ n\,s}} G_{mr,ns}\, |m,r\rangle\langle n,s|$$

$$|m\rangle\langle n| \otimes |r\rangle\langle s|$$

<u>No signaling</u>

$$G^{(AB)} \text{ on } \mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)} \Rightarrow G^{(AB)} = \sum_\alpha X$$

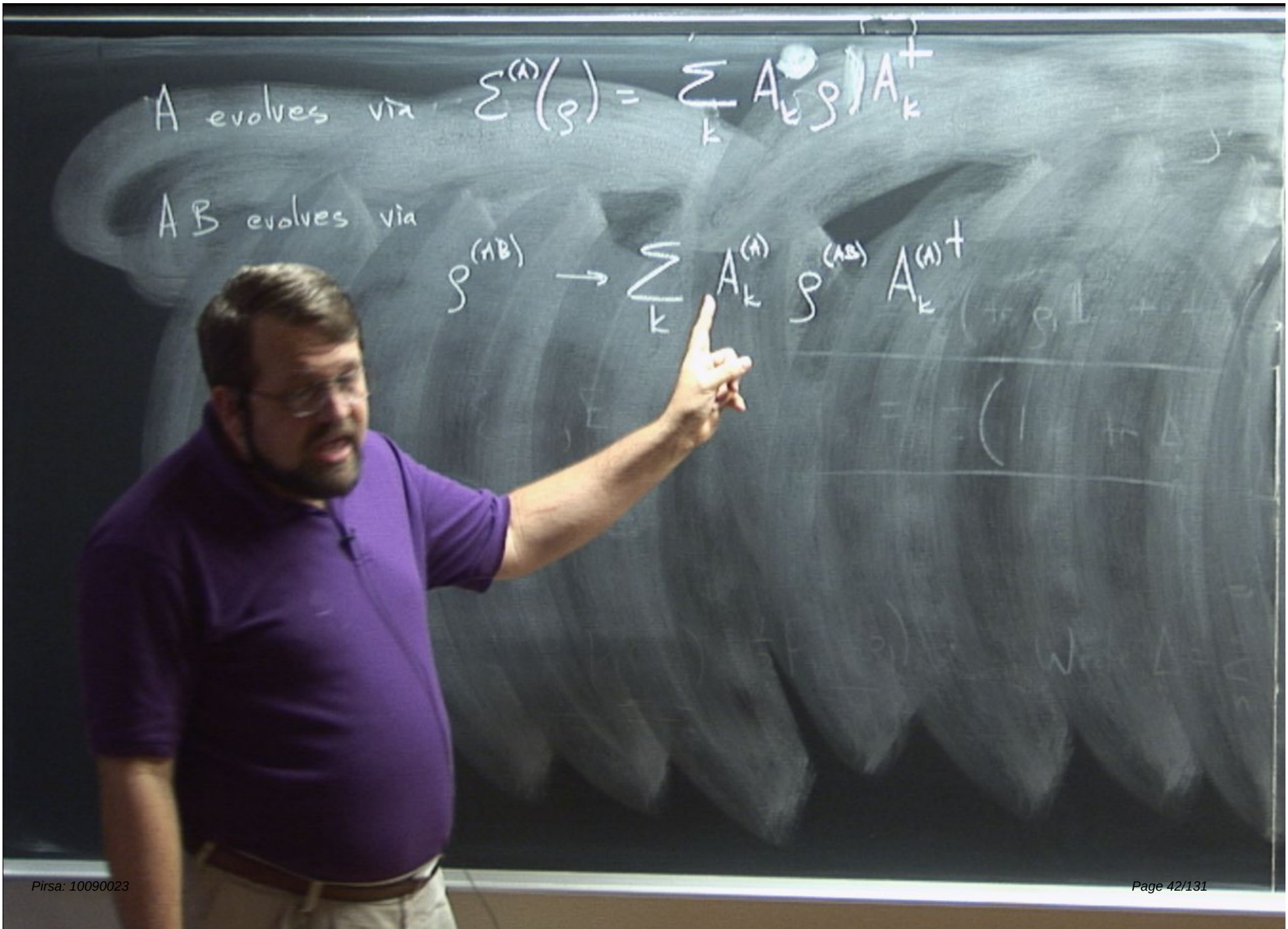
$$\boxed{\mathrm{tr}_{(A)}\, G^{(AB)} = \sum_\alpha \left(\mathrm{tr}_{(A)} X_\alpha^{(A)}\right) Y_\alpha^{(B)}}$$

$$\rho^{(AB)} = \sum_\alpha X_\alpha^{(A)} \otimes Y_\alpha^{(B)}$$

$$\rho^{(B)} = \mathrm{tr}_{(A)}\, \rho^{(AB)} = \sum_\alpha \left(\mathrm{tr}_{(A)} X_\alpha^{(A)}\right) Y_\alpha^{(B)}$$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$


A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$
AB evolves via
$\rho^{(AB)} \rightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$


A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$
AB evolves via
$\rho^{(AB)} \to \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$
$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

AB evolves via

$$\rho^{(AB)} \longrightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$A_k^{(A)} = A_k^{(A)} \otimes$$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

AB evolves via

$$\rho^{(AB)} \longrightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$$

$$\rho^{(B)} \longrightarrow \mathrm{tr}_{(A)} \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

AB evolves via

$$\rho^{(AB)} \longrightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$$

$$\rho^{(B)} \longrightarrow \mathrm{tr}_{(A)} \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$= \mathrm{tr}_{(A)} \sum_{k\alpha} A_k^{(A)} \left(X_\alpha^{(A)} \otimes Y_\alpha^{(B)} \right) A_k^{(A)\dagger}$$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

AB evolves via

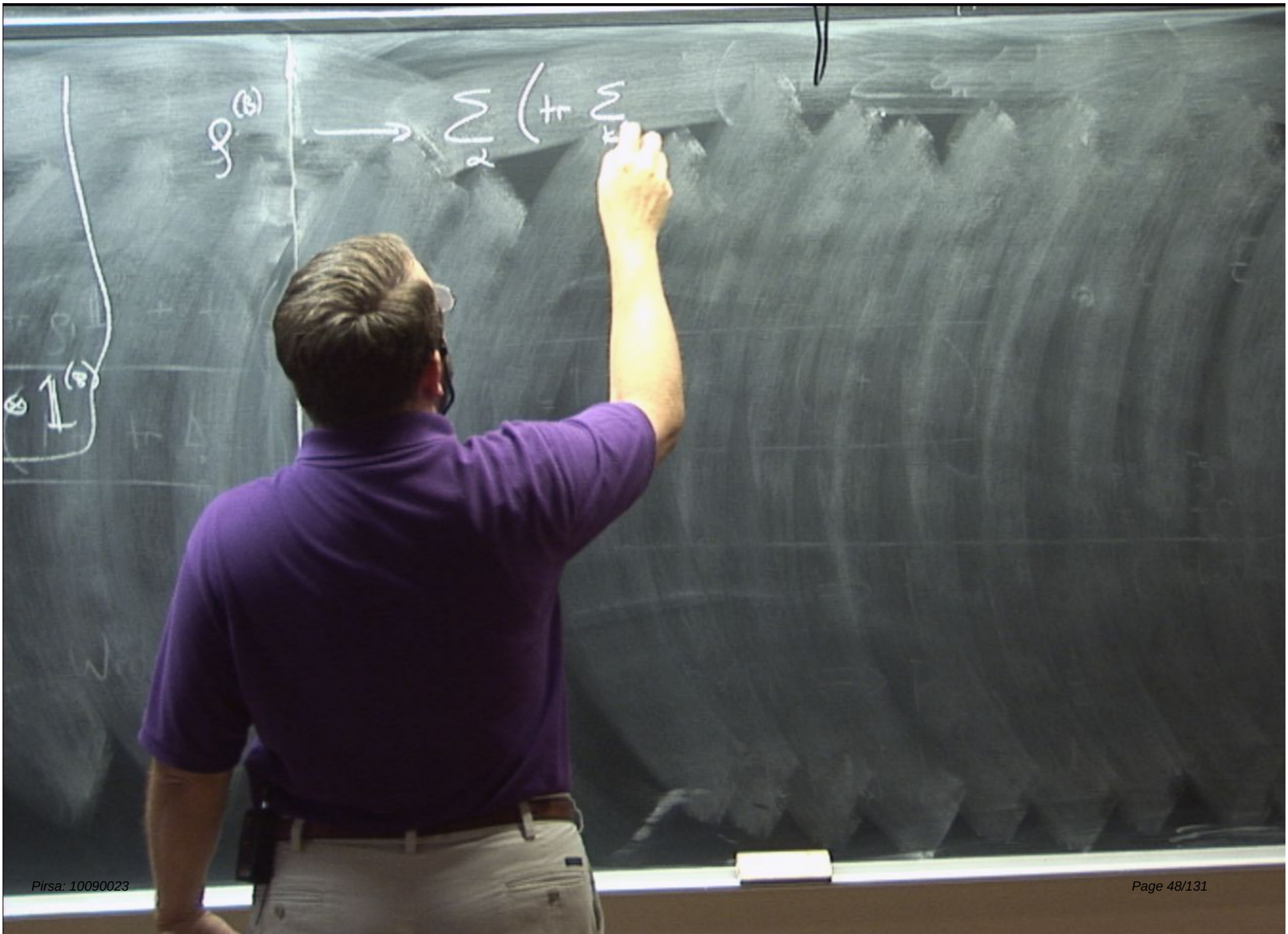
$$\rho^{(AB)} \longrightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

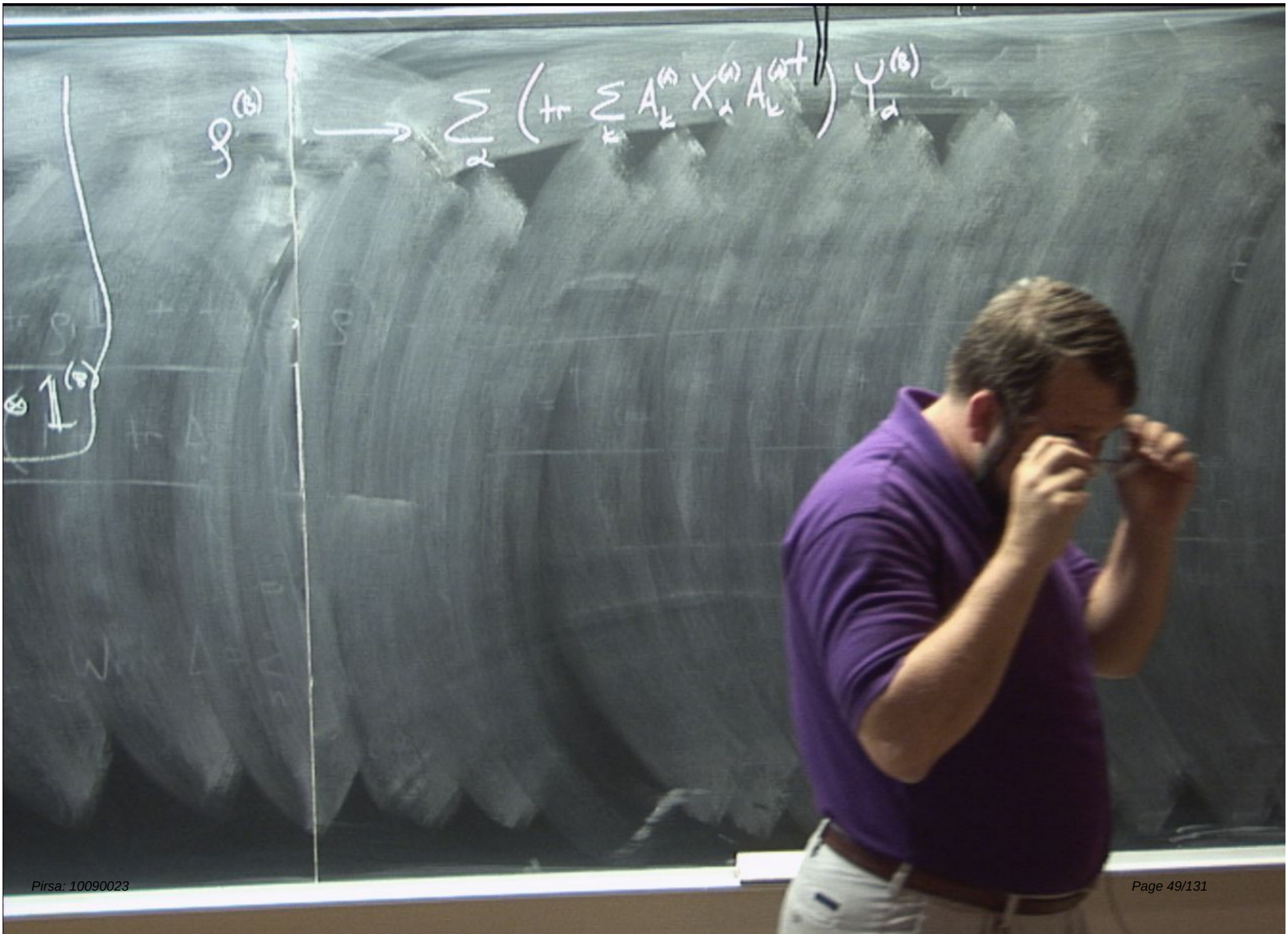
$$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$$

$$\rho^{(B)} \longrightarrow \mathrm{tr}_{(A)} \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$= \mathrm{tr}_{(A)} \sum_{k\alpha} A_k^{(A)} \left(X_\alpha^{(A)} \otimes Y_\alpha^{(B)} \right) A_k^{(A)\dagger}$$

$$= \mathrm{tr}_{(A)} \sum_{k\alpha} \left(A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) \otimes Y_\alpha^{(B)}$$


$\rho^{(B)} \longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k \right.$
$\otimes \mathbb{1}^{(B)}$


$\rho^{(B)} \longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$
$\otimes \mathbb{1}^{(B)}$

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$

$\rho^{(B)}$

AB evolves via

$$\rho^{(AB)} \longrightarrow \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$$

$$\rho^{(B)} \longrightarrow \mathrm{tr}_{(A)} \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$$

$$= \mathrm{tr}_{(A)} \sum_{k\alpha} A_k^{(A)} \left(X_\alpha^{(A)} \otimes Y_\alpha^{(B)} \right) A_k^{(A)\dagger}$$

$$= \mathrm{tr}_{(A)} \sum_{k\alpha} \left(A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) \otimes Y_\alpha^{(B)}$$

$$\rho^{(B)} \longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \mathcal{E}^{(A)} \text{ trace-preserving}$$

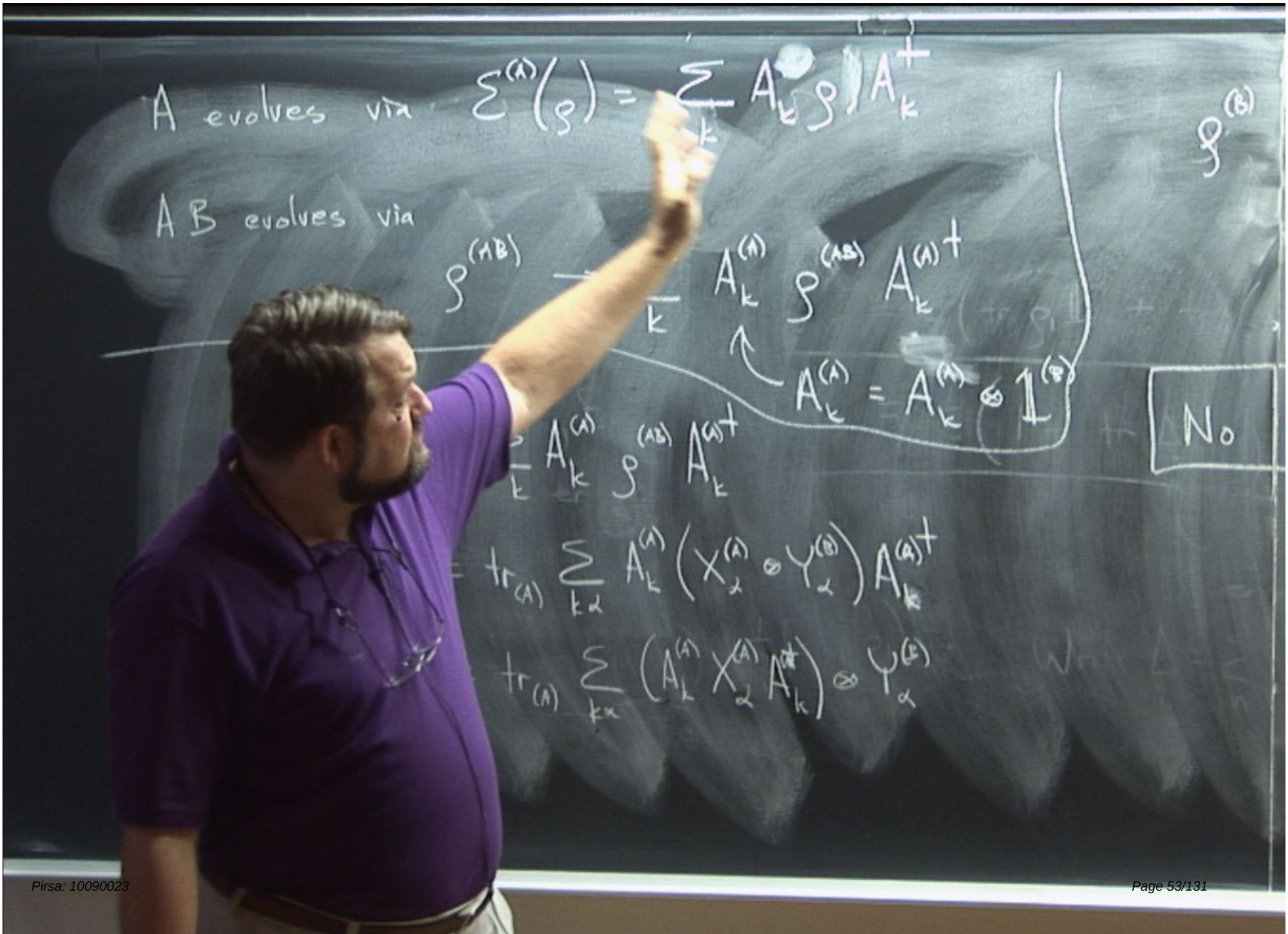
$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)}$$

$$\rho^{(B)} \longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \mathcal{E}^{(A)} \text{ trace-preserving}$$

$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)} = \rho^{(B)}$$

No	A-operation changes $\rho^{(B)}$!

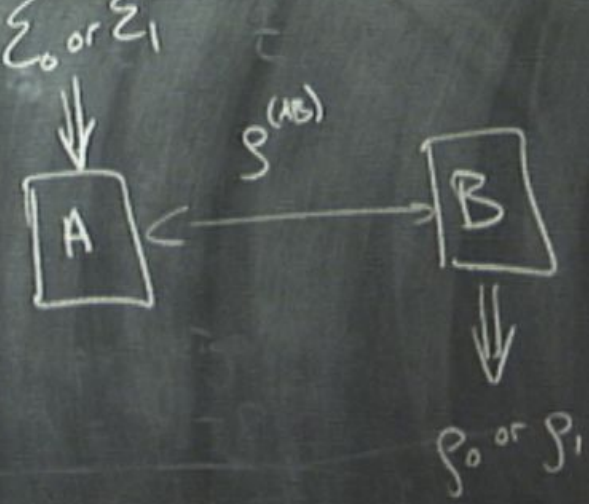

A evolves via $\mathcal{E}^{(A)}(\rho) = \sum_k A_k \rho A_k^\dagger$
AB evolves via
$\rho^{(AB)} = \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$
$A_k^{(A)} = A_k^{(A)} \otimes \mathbb{1}^{(B)}$
$\rho^{(B)}$
No
$= \sum_k A_k^{(A)} \rho^{(AB)} A_k^{(A)\dagger}$
$= \mathrm{tr}_{(A)} \sum_{k\alpha} A_k^{(A)} \left(X_\alpha^{(A)} \otimes Y_\alpha^{(B)} \right) A_k^{(A)\dagger}$
$= \mathrm{tr}_{(A)} \sum_{k\alpha} \left(A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) \otimes Y_\alpha^{(B)}$

$$\longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \; \mathcal{E}^{(A)} \text{ trace-preserving}$$

$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)} = \rho^{(B)}$$

$$\boxed{\text{A-operation changes } \rho^{(B)}!}$$

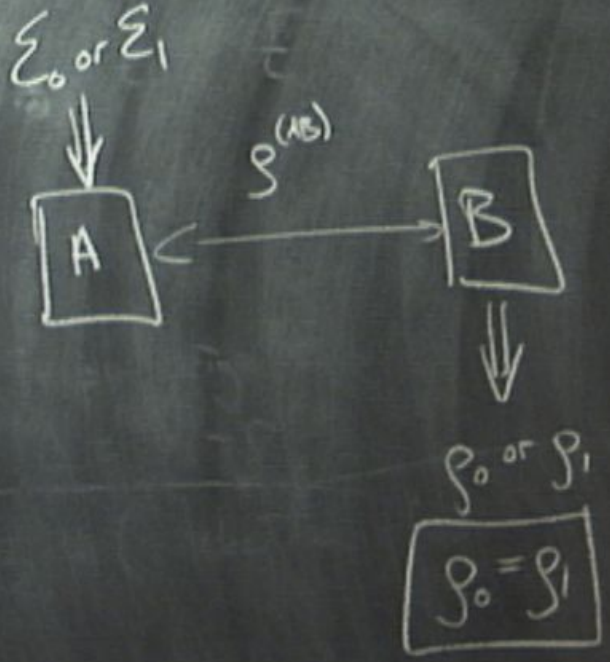


$$\longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \; \mathcal{E}^{(A)} \text{ trace-preserving}$$

$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)} = \rho^{(B)}$$

$$\boxed{\text{A-operation changes } \rho^{(B)}!}$$

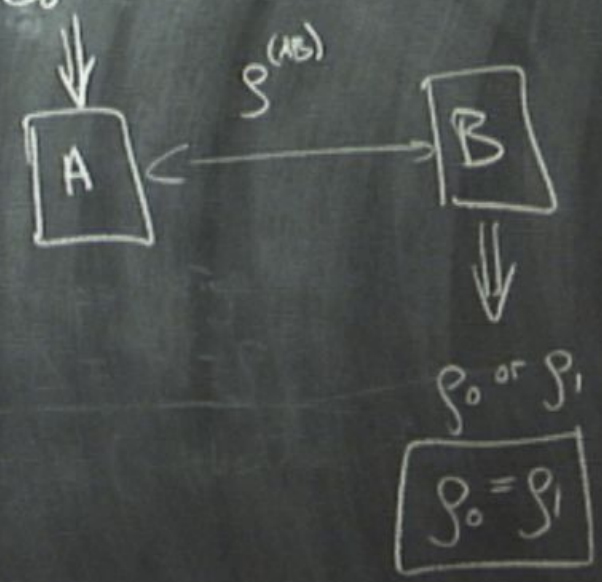


$$\longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \; \mathcal{E}^{(A)} \text{ trace-preserving}$$

$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)} = \rho^{(B)}$$

$$\boxed{\text{A-operation changes } \rho^{(B)}!}$$



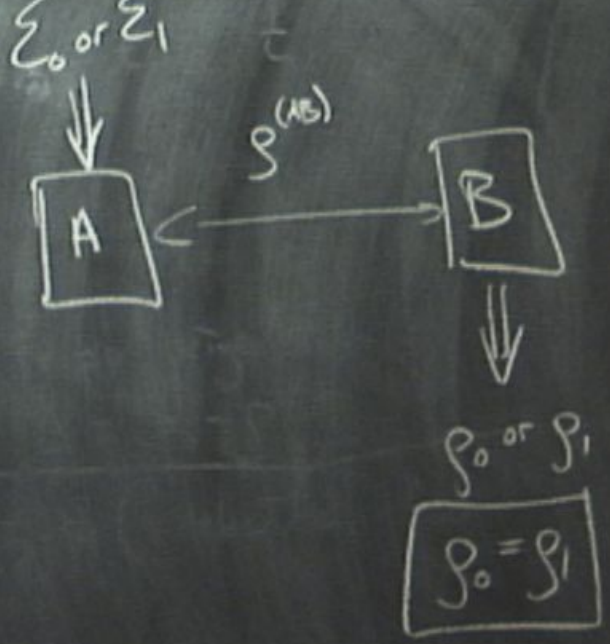

$\sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$
$\mathcal{E}^{(A)}$ trace-preserving
$= \sum_\alpha (\quad) Y_\alpha^{(B)} = \rho^{(B)}$
A -operation
$\rho^{(B)}$!
$\mathcal{E}_0$ or $\mathcal{E}_1$
$\rho^{(AB)}$
A
B
ρ_0 or ρ_1
$\rho_0 = \rho_1$

$$\longrightarrow \sum_\alpha \left(\mathrm{tr} \sum_k A_k^{(A)} X_\alpha^{(A)} A_k^{(A)\dagger} \right) Y_\alpha^{(B)}$$

$$\Big\downarrow \mathcal{E}^{(A)} \text{ trace-preserving}$$

$$= \sum_\alpha \left(\mathrm{tr}\, X_\alpha^{(A)} \right) Y_\alpha^{(B)} = \rho^{(B)}$$

$$\boxed{\text{A-operation changes } \rho^{(B)}!}$$



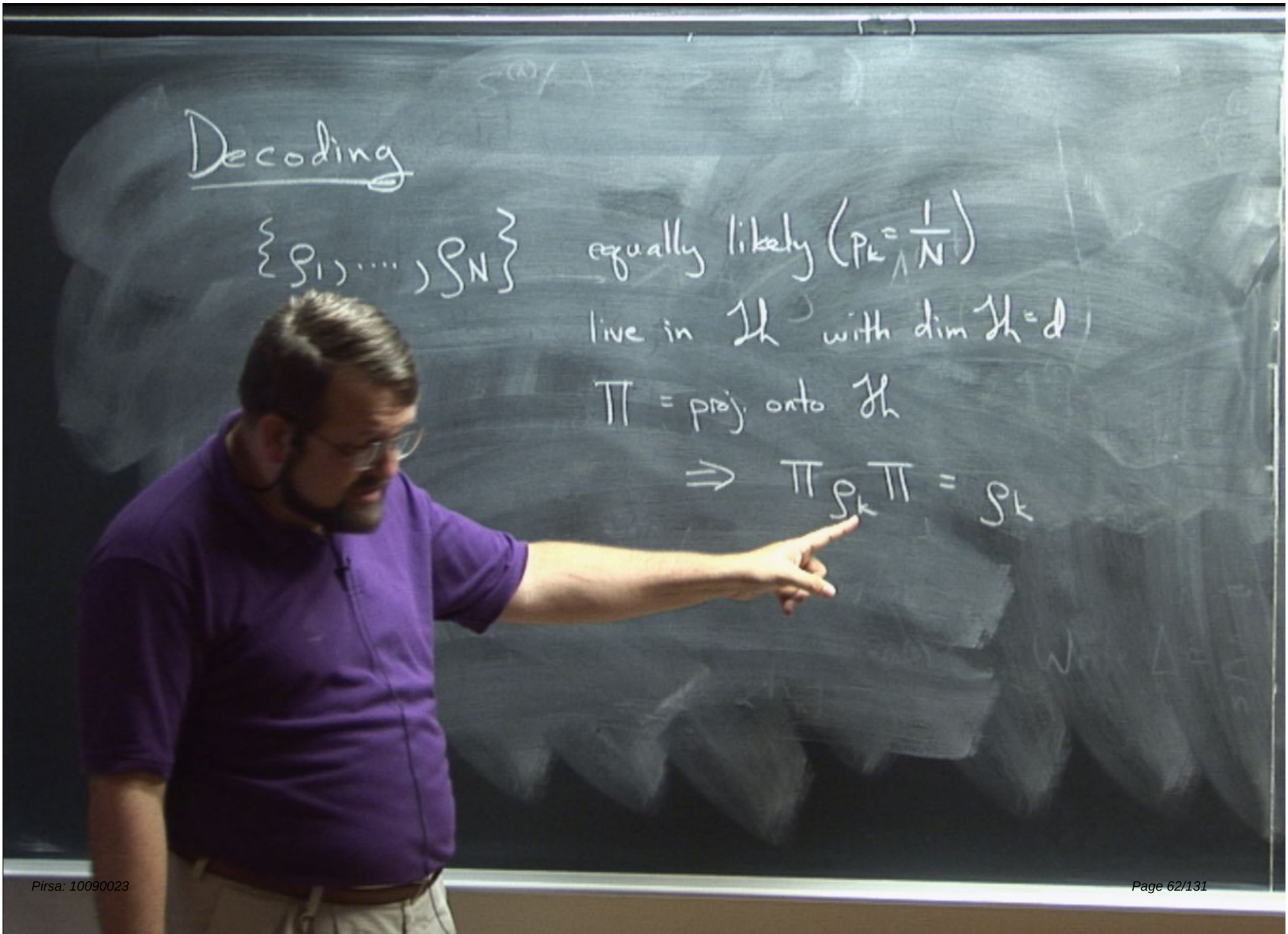

$\mathcal{E}_0$ or $\mathcal{E}_1$
$\rho^{(AB)}$
A
B
ρ_0 or ρ_1
$\rho_0 = \rho_1$


Decoding
$\{\rho_1, \dots, \rho_N\}$ equally likely $\left(p_k = \frac{1}{N}\right)$

Decoding

$\{\rho_1, \dots, \rho_N\}$ equally likely $\left(p_k = \frac{1}{N}\right)$

live in $\mathcal{H}$ with $\dim \mathcal{H} = d$


Decoding
$\{\rho_1, \dots, \rho_N\}$ equally likely $(p_k = \frac{1}{N})$
live in $\mathcal{H}$ with $\dim \mathcal{H} = d$
Π = proj. onto $\mathcal{H}$
$\Rightarrow \Pi \rho_k \Pi = \rho_k$

Decoding

$\{\rho_1, \dots, \rho_N\}$ equally likely $\left(p_k = \frac{1}{N}\right)$

live in $\mathcal{H}$ with $\dim \mathcal{H} = d$

Π = proj. onto $\mathcal{H}$

$$\Rightarrow \quad \Pi \rho_k \Pi = \rho_k$$

$$\operatorname{tr} \Pi = d$$

Decoding

$\{\rho_1, \dots, \rho_N\}$ equally likely $\left(p_k = \frac{1}{N}\right)$

live in $\mathcal{H}$ with $\dim \mathcal{H} = d$

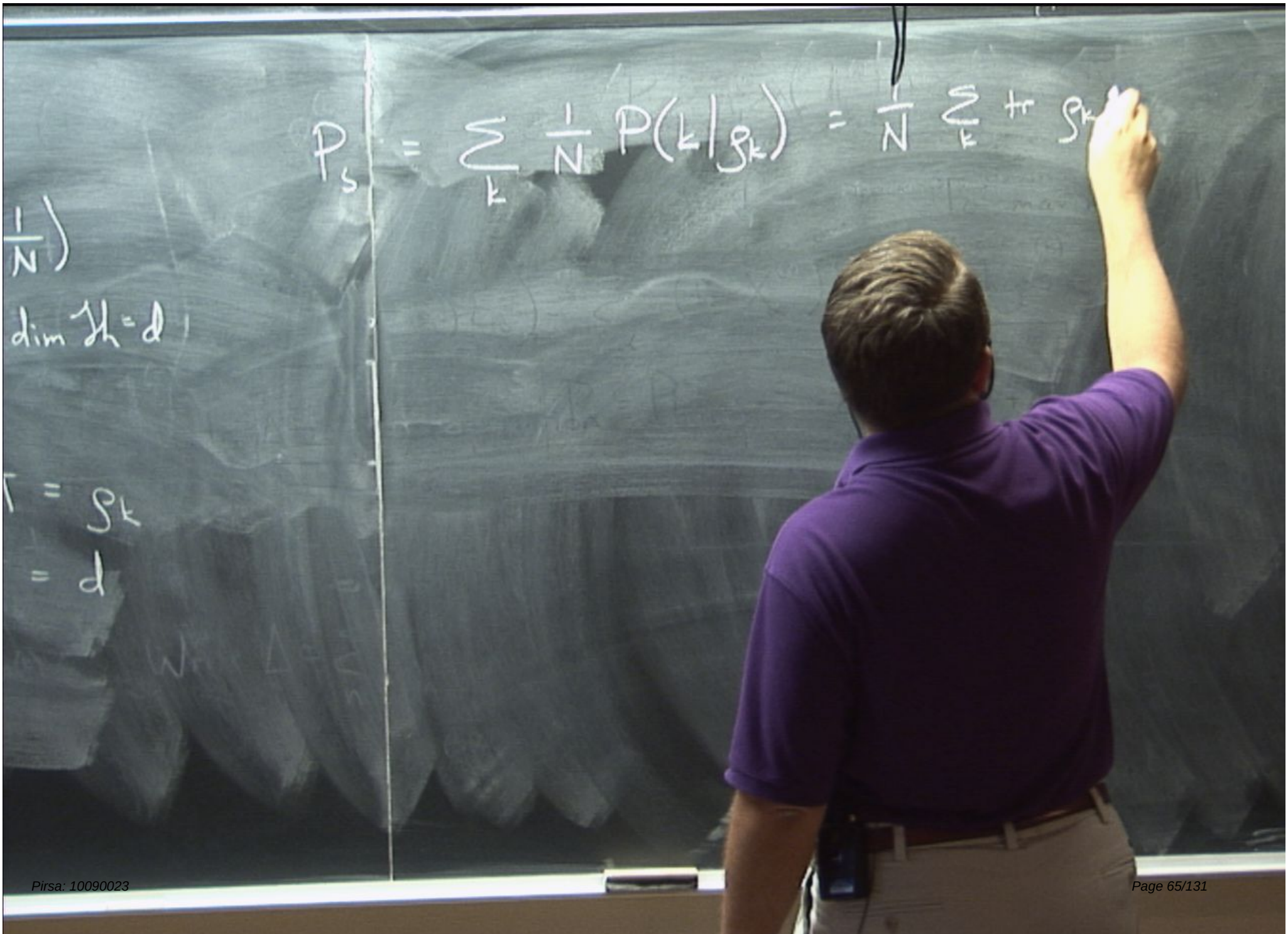
Π = proj. onto $\mathcal{H}$

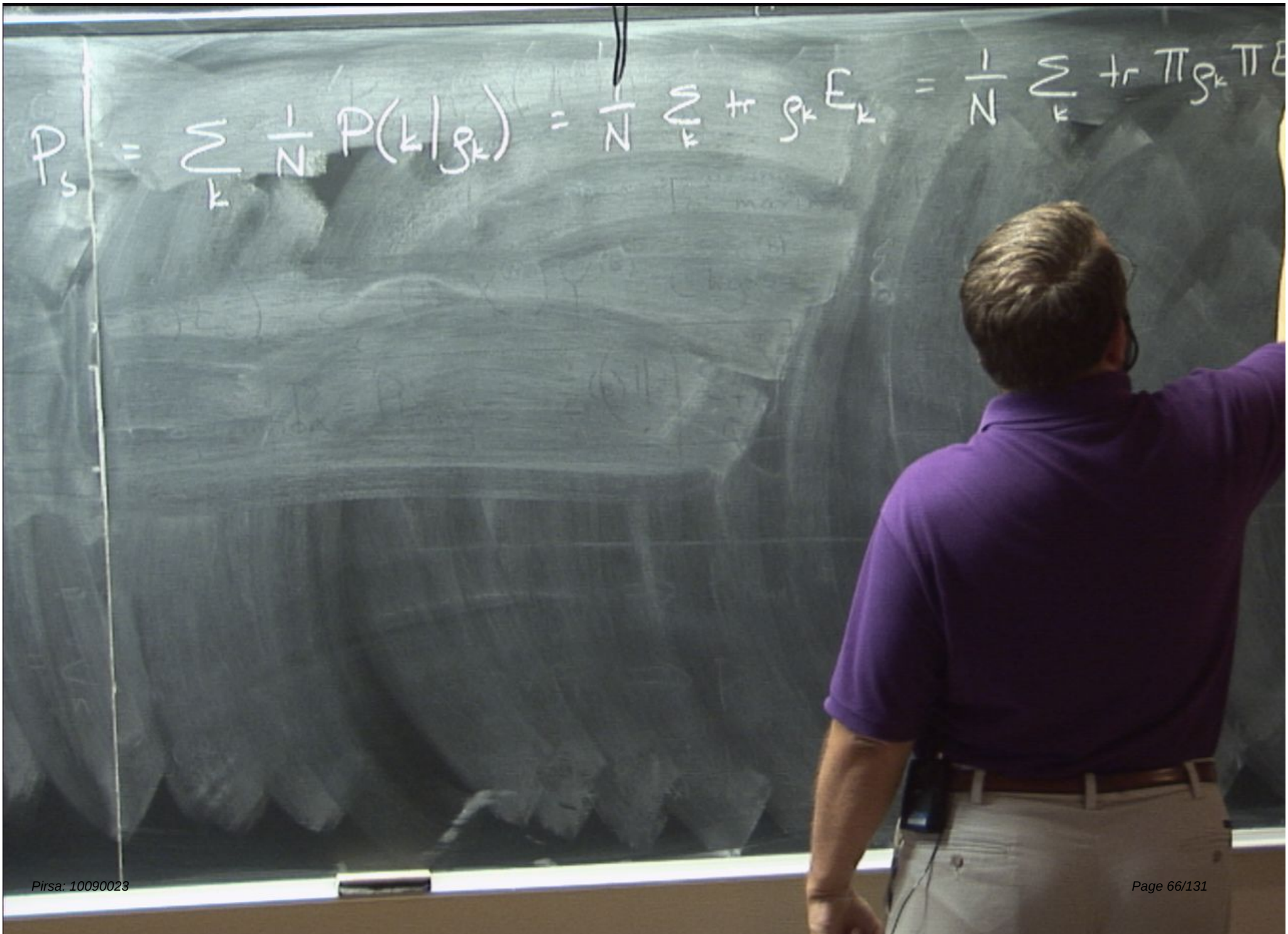
$$\Rightarrow \Pi \rho_k \Pi = \rho_k$$

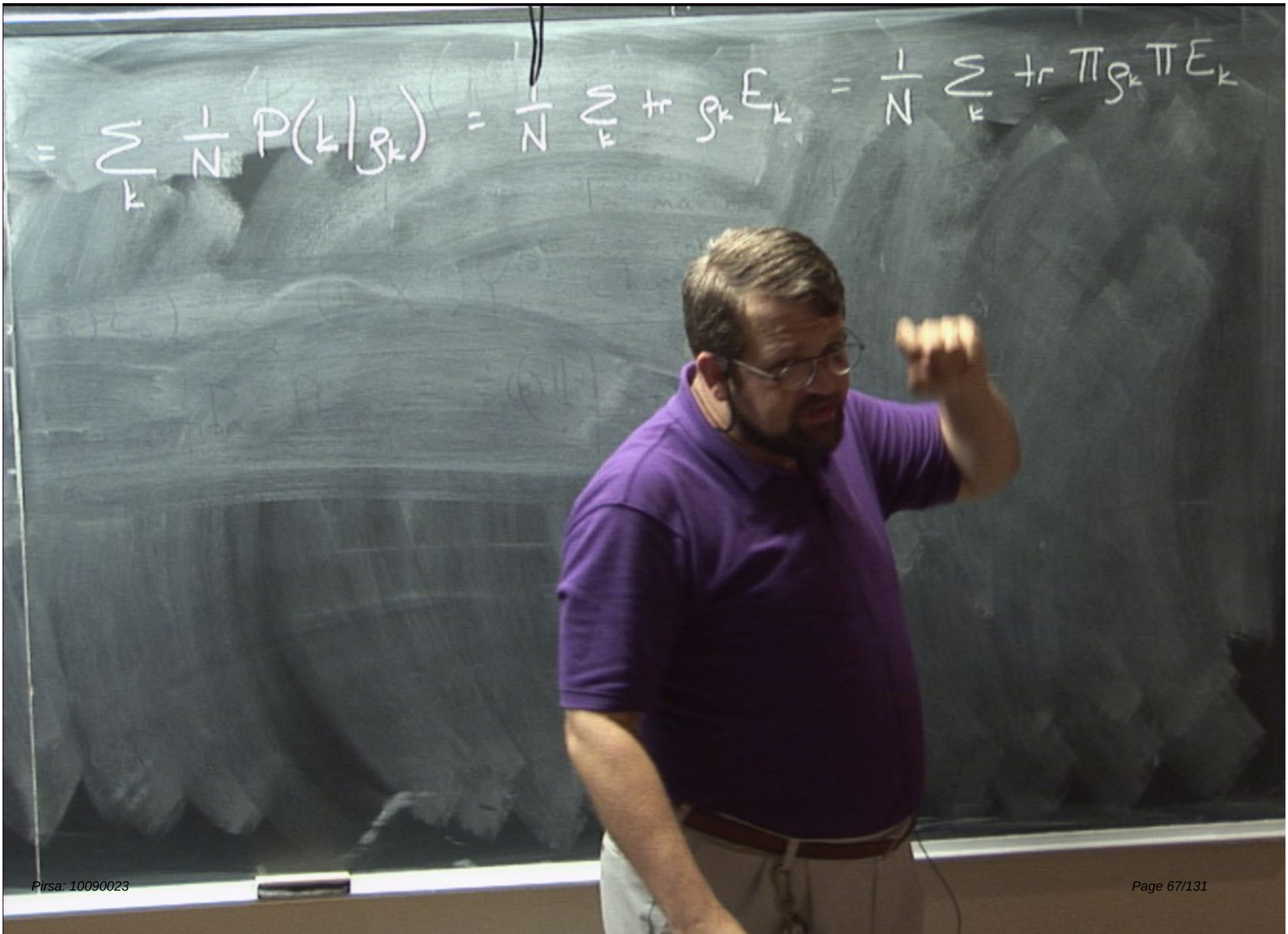
$$\operatorname{tr} \Pi = d$$

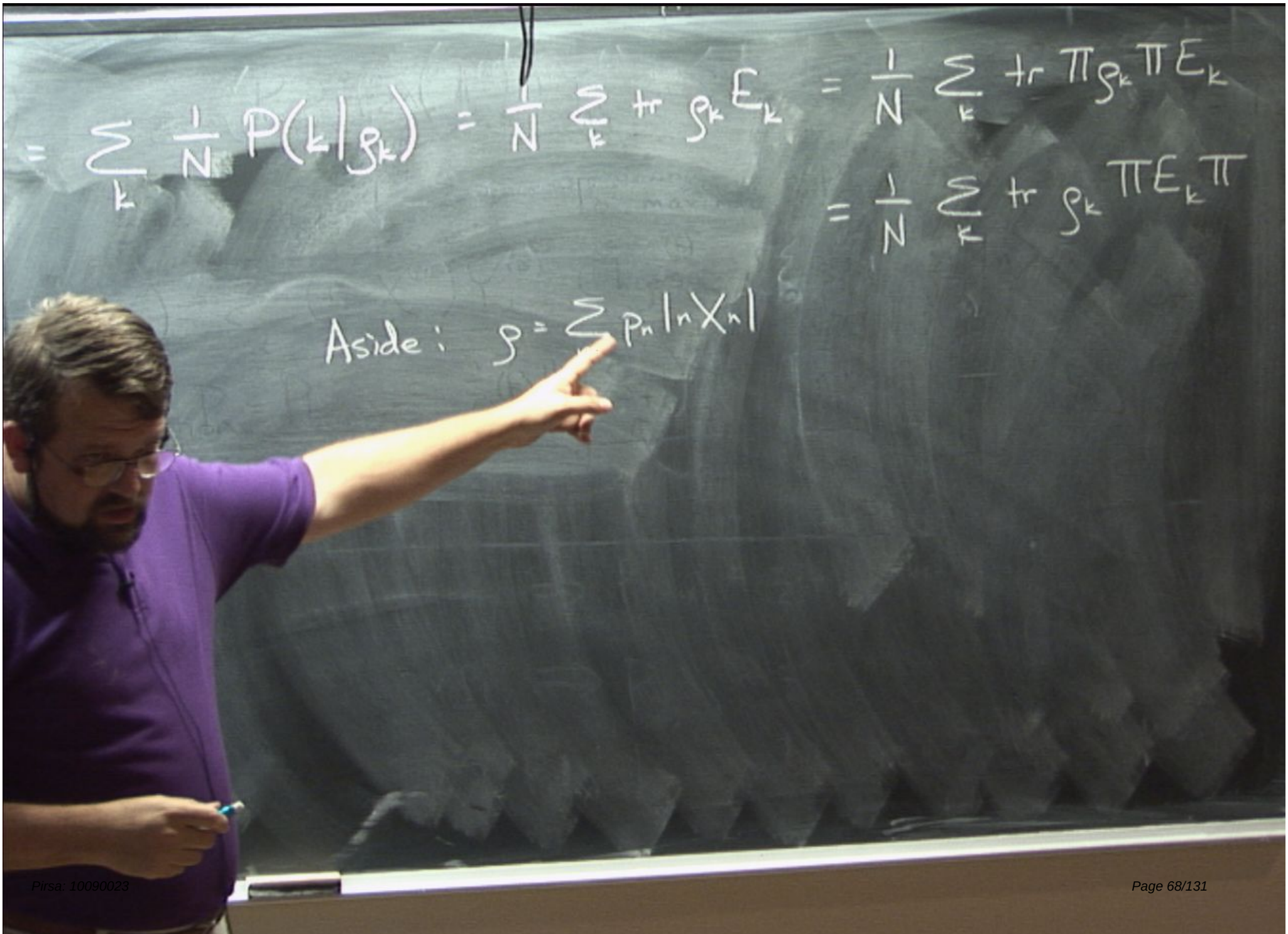
Decoding obs. $\{E_1, \dots, E_N\}$

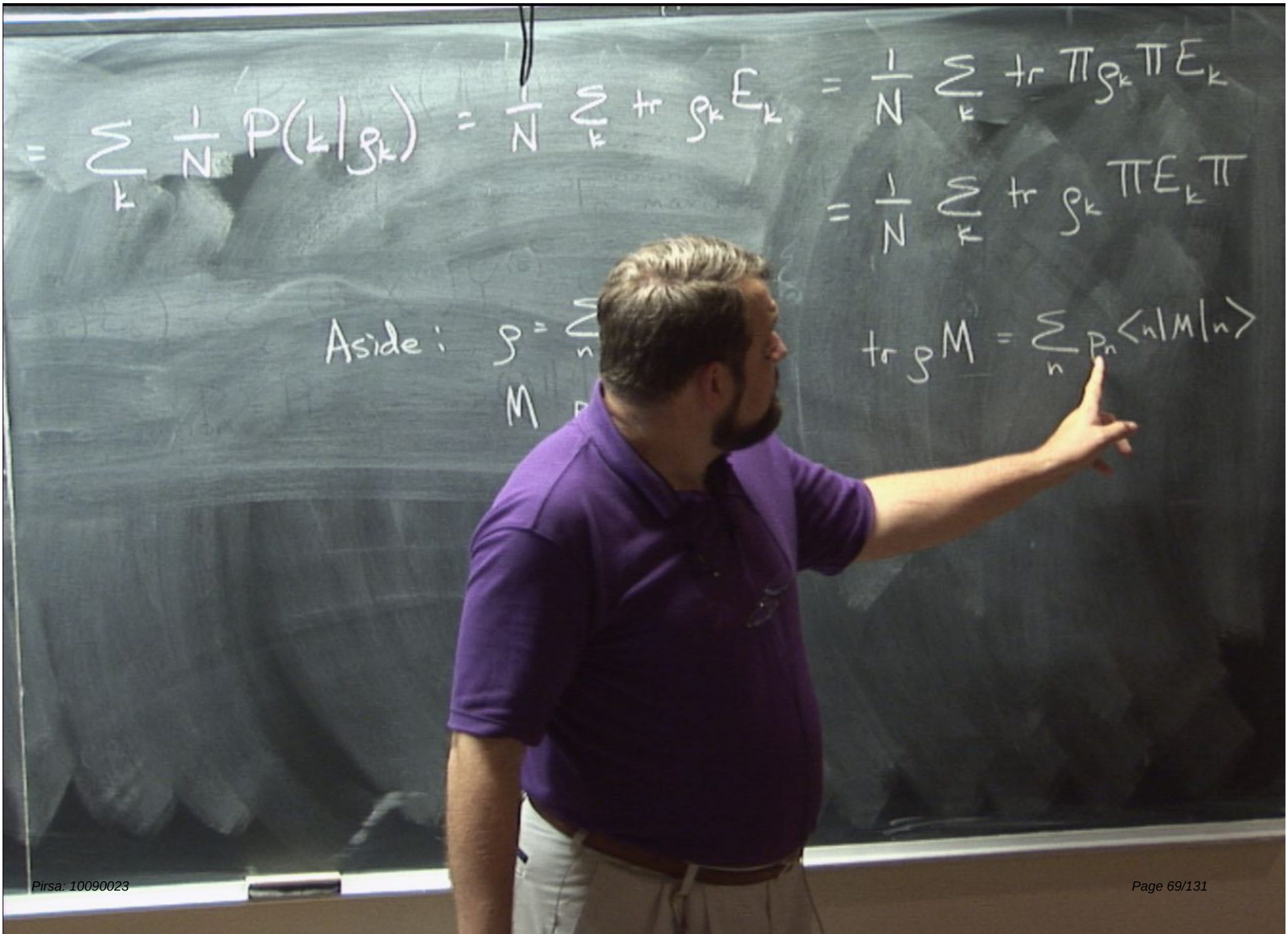
Obtain $k \Rightarrow$ infer ρ_k

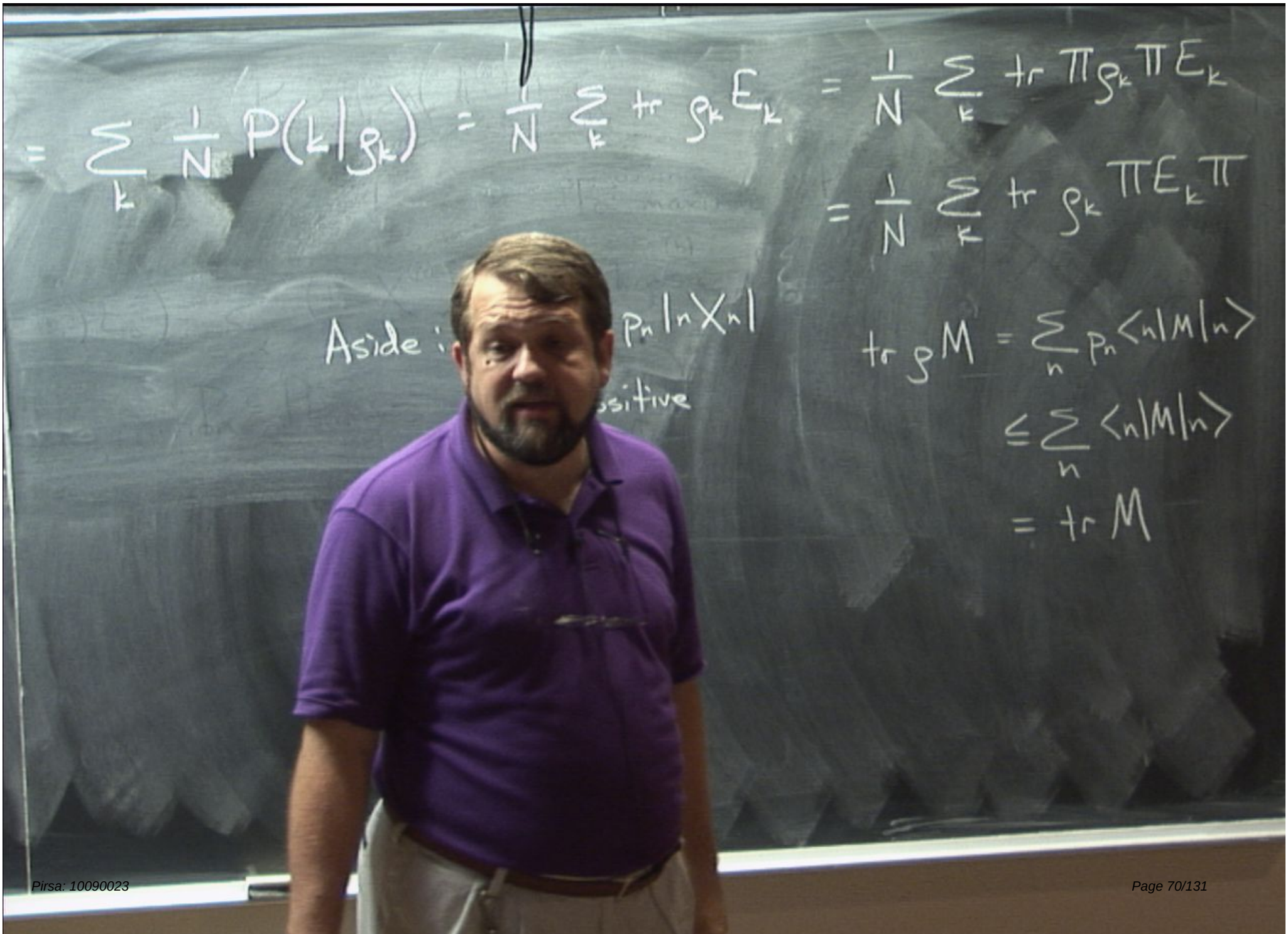

$P_s = \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k$
$\frac{1}{N})$
$\dim \mathcal{H} = d$
$= \rho_k$
$= d$


$P_s = \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E$


$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$


$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$
$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$
Aside: $\rho = \sum p_n |n\rangle\langle n|$


$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$
$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$
Aside: $\rho = \sum_n$
$\mathrm{tr}\, \rho M = \sum_n p_n \langle n|M|n\rangle$
M


$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$
$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$
Aside :
$p_n |n\rangle\langle n|$
ssitive
$\mathrm{tr}\, \rho M = \sum_n p_n \langle n|M|n\rangle$
$\leq \sum_n \langle n|M|n\rangle$
$= \mathrm{tr}\, M$

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

$$\mathrm{tr}\, \rho M = \sum_n p_n \langle n|M|n\rangle$$

$$\leq \sum_n \langle n|M|n\rangle$$

$$= \mathrm{tr}\, M$$

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

$$\mathrm{tr}\, \rho M = \sum_n p_n \langle n|M|n\rangle$$

$$\leq \sum_n \langle n|M|n\rangle$$

$$= \mathrm{tr}\, M$$

$$P_s \leq \frac{1}{N} \sum_k \mathrm{tr}\, \Pi E_k \Pi$$

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

$$\boxed{\mathrm{tr}\, \rho M} = \sum_n p_n \langle n|M|n\rangle$$

$$\leq \sum_n \langle n|M|n\rangle$$

$$= \boxed{\mathrm{tr}\, M}$$

$$P_s \leq \frac{1}{N} \sum_k \mathrm{tr}\, \Pi E_k \Pi = \frac{1}{N} \mathrm{tr}\, \Pi \left(\sum_k E_k\right) \Pi$$

$$=$$

Decoding

P_s

$\{\rho_1, \dots, \rho_N\}$ equally likely $\left(p_k = \frac{1}{N}\right)$

live in $\mathcal{H}$ with $\dim \mathcal{H} = d$

Π = proj. onto $\mathcal{H}$

$$\Rightarrow \quad \Pi \rho_k \Pi = \rho_k$$

$$\operatorname{tr} \Pi = d$$

Decoding obs. $\{E_1, \dots, E_N\}$ $\quad \sum_k E_k = \mathbb{1}$

Obtain $k \Rightarrow$ infer ρ_k

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

$$\boxed{\mathrm{tr}\, \rho M} = \sum_n p_n \langle n|M|n\rangle$$

$$\leq \sum_n \langle n|M|n\rangle$$

$$= \boxed{\mathrm{tr}\, M}$$

$$\leq \frac{1}{N} \sum_k \mathrm{tr}\, \Pi E_k \Pi = \frac{1}{N} \mathrm{tr}\, \Pi \left(\sum_k E_k\right) \Pi$$

$$= \frac{1}{N} \mathrm{tr}\, \Pi = \frac{d}{N}$$

$$\boxed{P_E = 1 - \quad \geq 1 - \frac{d}{N}}$$

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

$$\boxed{\mathrm{tr}\, \rho M} = \sum_n p_n \langle n|M|n\rangle$$

$$\leq \sum_n \langle n|M|n\rangle$$

$$= \boxed{\mathrm{tr}\, M}$$

$$P_s \leq \frac{1}{N} \sum_k \mathrm{tr}\, \Pi E_k \Pi = \frac{1}{N} \mathrm{tr}\, \Pi \left(\sum_k E_k\right) \Pi$$

$$= \frac{1}{N} \mathrm{tr}\, \Pi = \frac{d}{N}$$

$$\boxed{P_E = 1 - P_s \geq 1 - \frac{d}{N}}$$

$$= \sum_k \frac{1}{N} P(k|\rho_k) = \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k E_k = \frac{1}{N} \sum_k \mathrm{tr}\, \Pi \rho_k \Pi E_k$$

$$= \frac{1}{N} \sum_k \mathrm{tr}\, \rho_k \Pi E_k \Pi$$

Aside: $\rho = \sum_n p_n |n\rangle\langle n|$

M positive

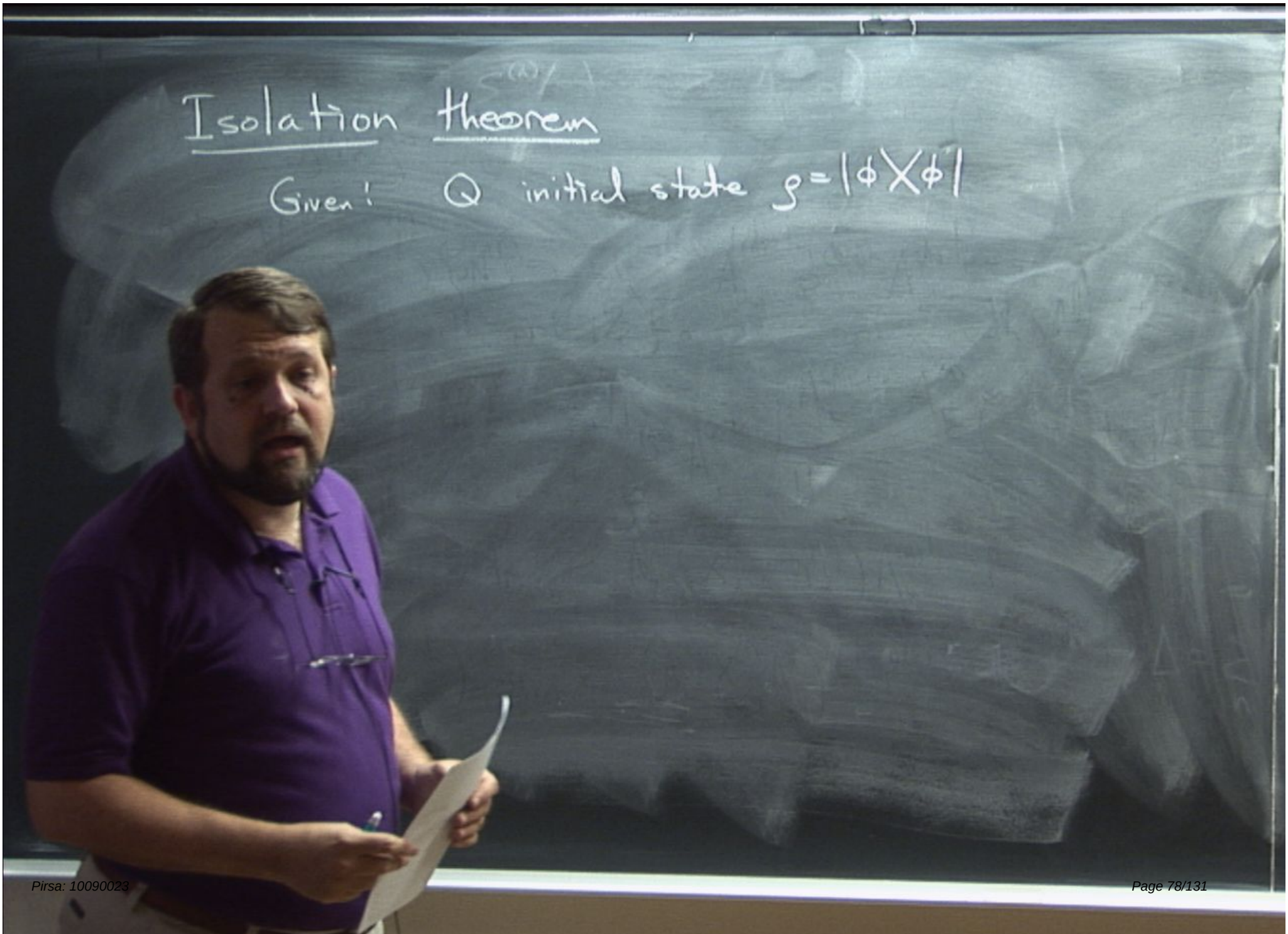
$$= \sum_n p_n \langle n|M|n\rangle$$

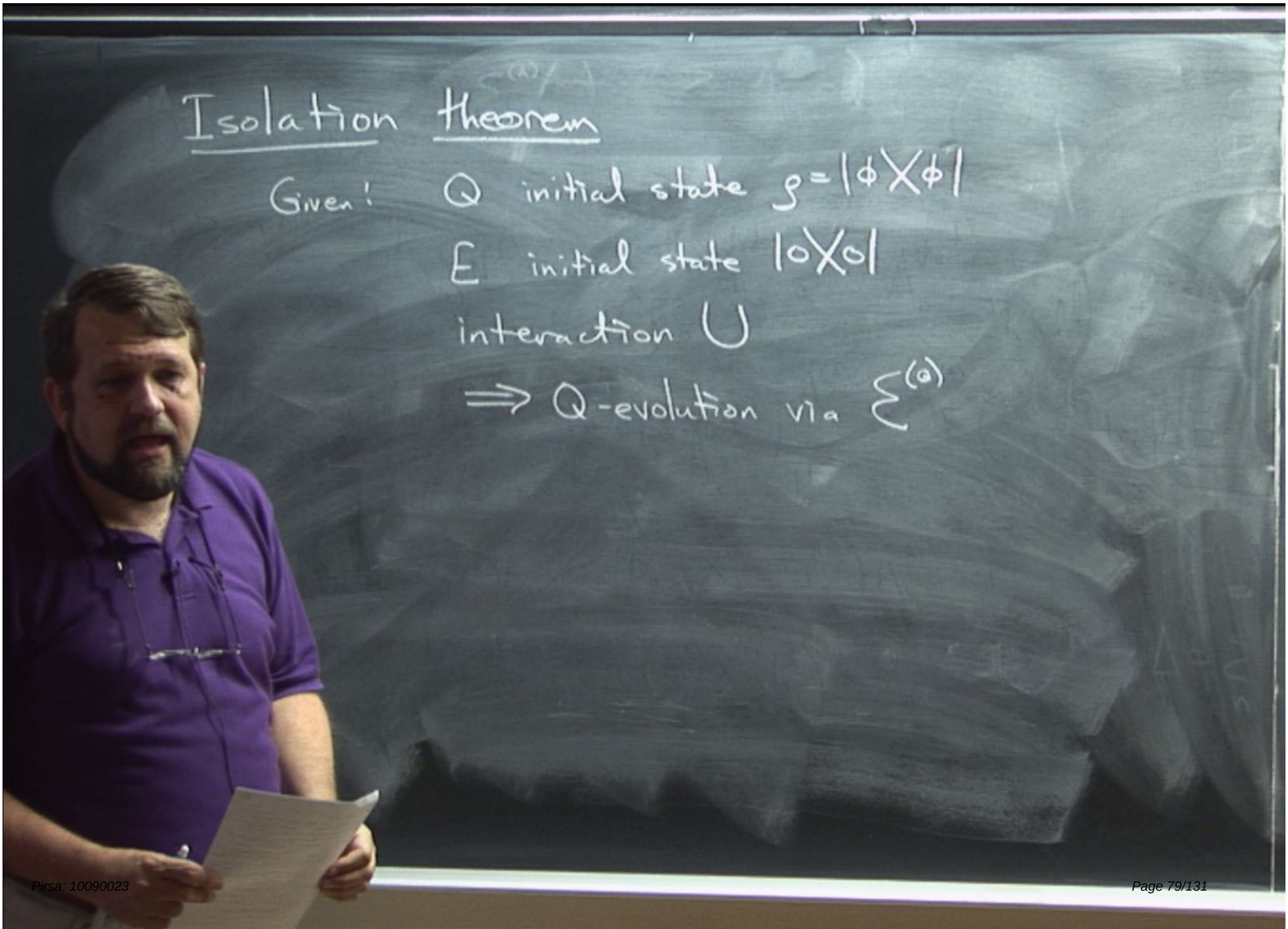
$$\langle n|M|n\rangle$$

$$P_s \leq \frac{1}{N} \sum_k \mathrm{tr}\, \Pi E_k \Pi = \frac{1}{N} \mathrm{tr}\, \Pi \left(\sum_k E\right.$$

$$= \frac{1}{N}$$

$$\boxed{P_E = 1 - P_s \geq 1 - \frac{d}{N}}$$


Isolation theorem
Given: Q initial state $\rho = |\phi\rangle\langle\phi|$


Isolation theorem
Given: Q initial state $\rho = |\phi\rangle\langle\phi|$
E initial state $|0\rangle\langle 0|$
interaction U
$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(a)}$

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(0)}$

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(a)}$

Two conditions: QU = Q-evolution is unitary

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(0)}$

Two conditions: QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(a)}$

Two conditions: ① QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

② QI^2 = Q is informationally isolated

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(Q)}$

Two conditions: ① QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

② QI^2 = Q is informationally isolated

Final E-state $\sigma^{(E)} = \mathrm{tr}_{(Q)}\, U\left(|\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|\right)U^{\dagger}$

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(Q)}$

Two conditions: ① QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

② QI^2 = Q is informationally isolated

Final E-state $\sigma^{(E)} = \mathrm{tr}_{(Q)}\, U\left(|\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|\right)U^{\dagger}$

is independent of $|\phi\rangle\langle\phi|$.

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction U

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(Q)}$

Two conditions: ① QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

② QI^2 = Q is informationally isolated

Final E-state $\sigma^{(E)} = \mathrm{tr}_{(Q)}\, U\left(|\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|\right)U^{\dagger}$

is independent of $|\phi\rangle\langle\phi|$.

Thm. $QU \Longleftrightarrow QI$

Isolation theorem

Given: Q initial state $\rho = |\phi\rangle\langle\phi|$

E initial state $|0\rangle\langle 0|$

interaction $U^{(QE)}$

$\Longrightarrow$ Q-evolution via $\mathcal{E}^{(Q)}$

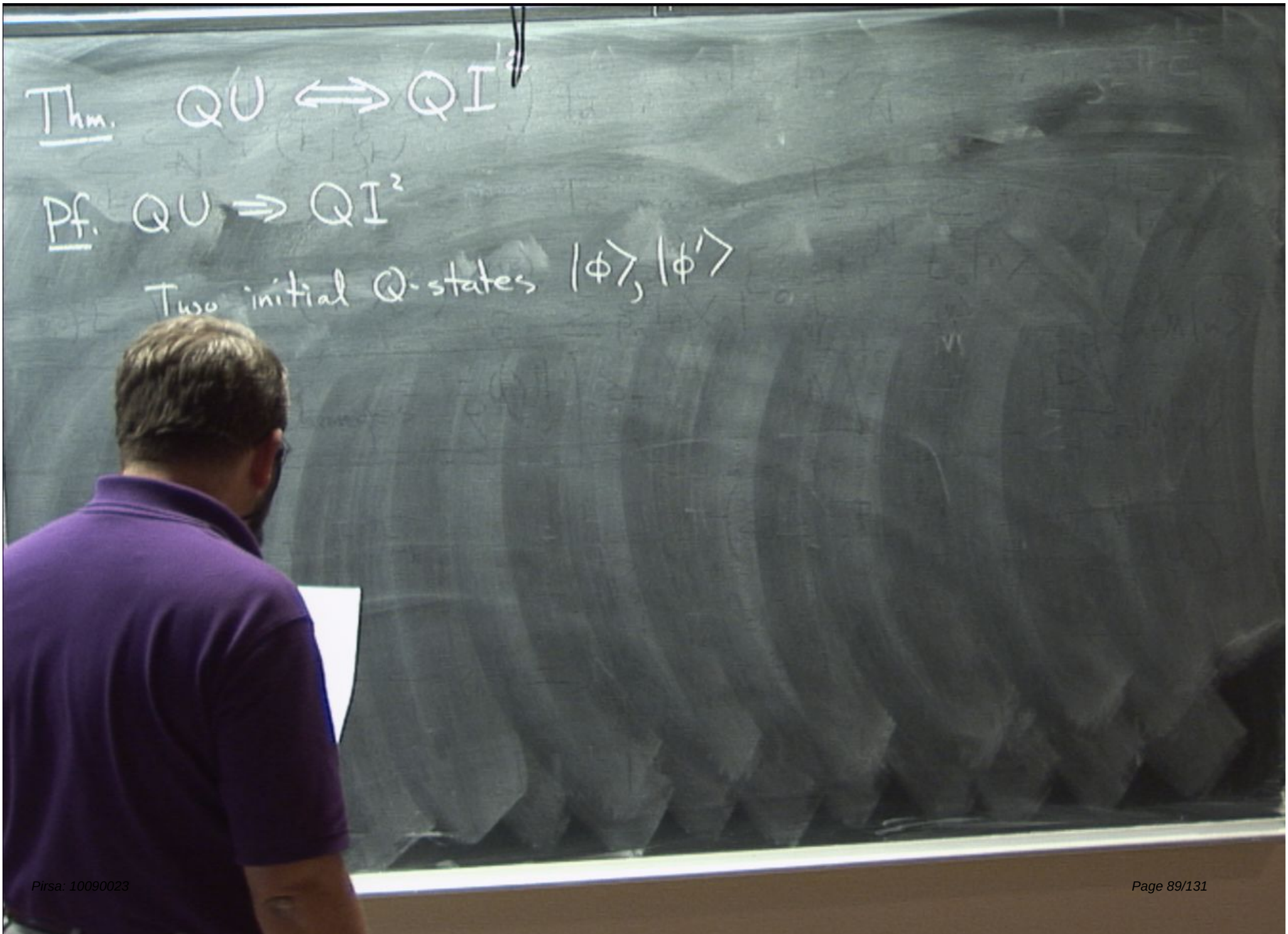
Two conditions: ① QU = Q-evolution is unitary

There is V s.t. $\mathcal{E}(\rho) = V\rho V^{\dagger}$

② QI^2 = Q is informationally isolated

Final E-state $\sigma^{(E)} = \mathrm{tr}_{(Q)}\, U\left(|\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|\right)U^{\dagger}$

is independent of $|\phi\rangle\langle\phi|$.


Thm. QU ⟺ QI²
Pf. QU ⇒ QI²
Two initial Q-states |φ⟩, |φ'⟩

Thm. $QU \Longleftrightarrow QI^2$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$|\langle\phi|\phi'\rangle| > 0$ (not orthog)

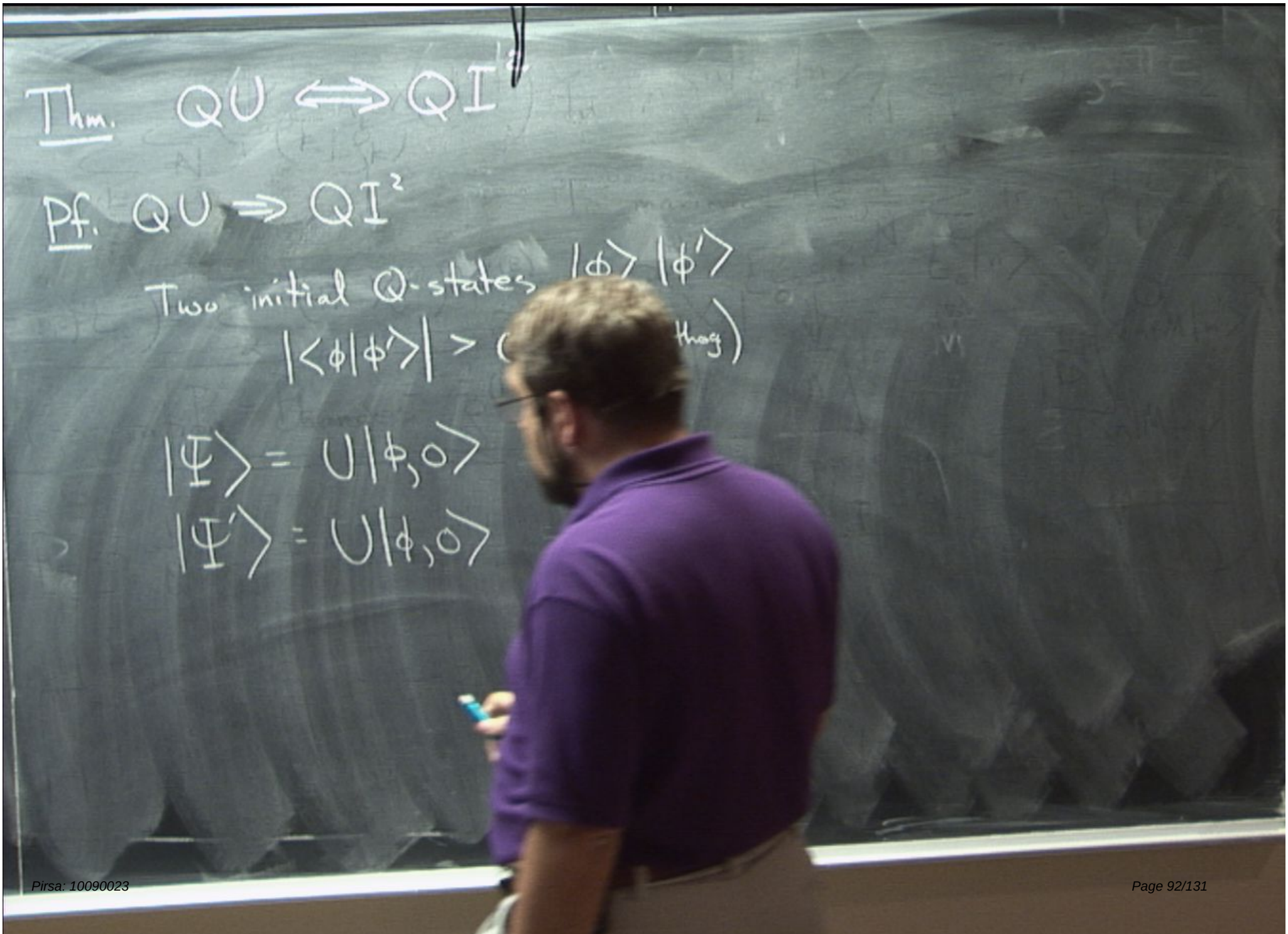
Thm. $QU \Longleftrightarrow QI^2$

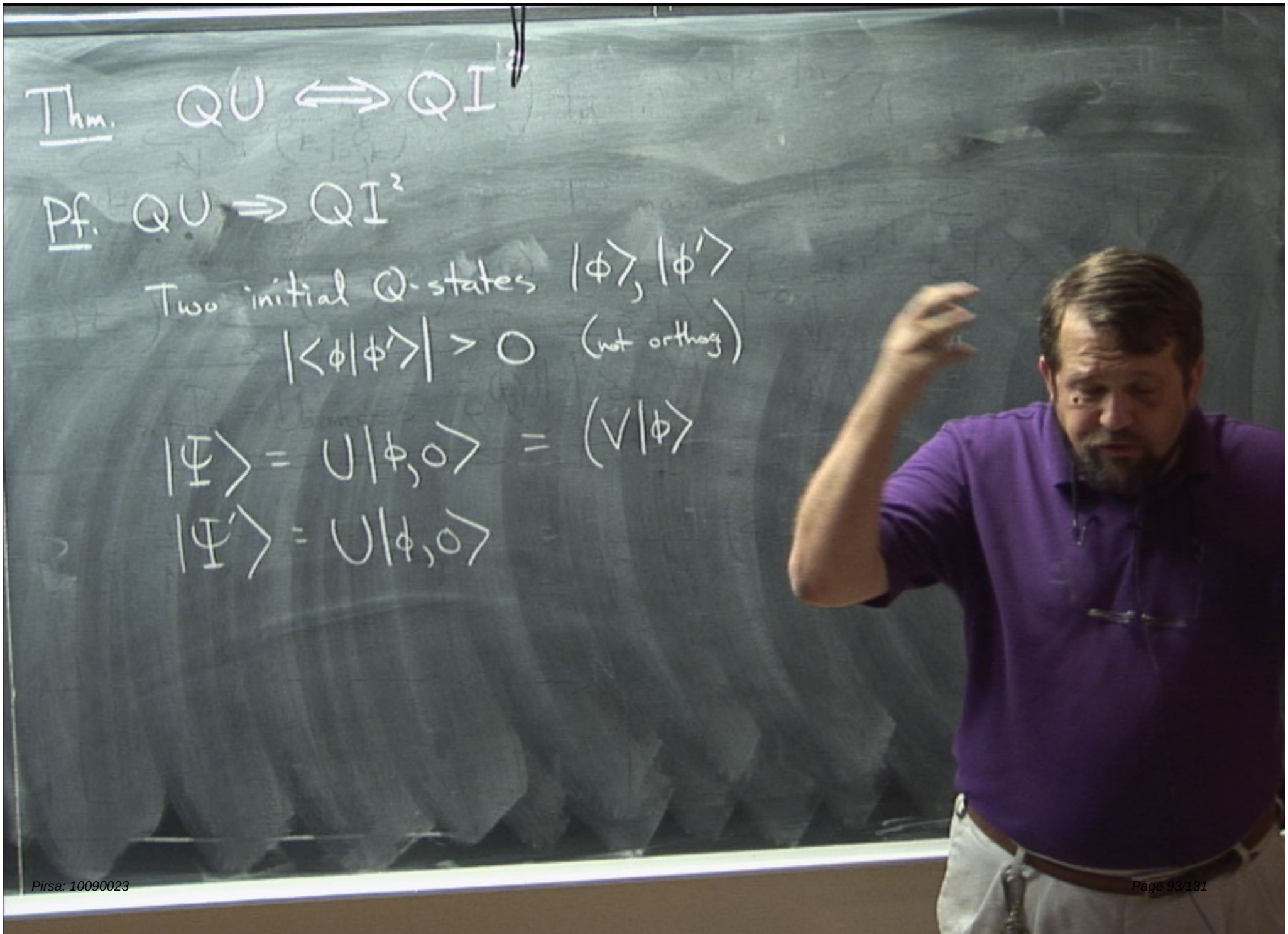
Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi, 0\rangle$$


Thm. QU ⟺ QI²
Pf. QU ⇒ QI²
Two initial Q-states |φ⟩ |φ'⟩
|⟨φ|φ'⟩| >
|Ψ⟩ = U|φ,0⟩
|Ψ'⟩ = U|φ,0⟩


Thm. QU ⟺ QI²
Pf. QU ⇒ QI²
Two initial Q-states |φ⟩, |φ'⟩
|⟨φ|φ'⟩| > 0 (not orthog)
|Ψ⟩ = U|φ,0⟩ = (V|φ⟩
|Ψ'⟩ = U|φ,0⟩

Thm. $QU \Longleftrightarrow QI^2$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi, 0\rangle = \left(V|\phi\rangle\right) \otimes |e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi', 0\rangle = \left(V|\phi'\rangle\right) \otimes |e_{\phi'}\rangle$$

$$\langle\phi, 0|U^\dagger U|\phi', 0\rangle = \langle\Psi|\Psi'\rangle$$

Thm. $QU \Longleftrightarrow QI^2$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi,0\rangle = (V|\phi\rangle) \otimes |e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi',0\rangle = (V|\phi'\rangle) \otimes |e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle \langle e_\phi|e_{\phi'}\rangle$$

$$\| $$

$$\langle\phi,0|\phi',0\rangle$$

$$\| $$

$$\langle\phi|\phi'\rangle$$

Thm. $QU \Longleftrightarrow QI^2$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi, 0\rangle = (V|\phi\rangle) \otimes |e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi', 0\rangle = (V|\phi'\rangle) \otimes |e_{\phi'}\rangle$$

$$\langle\phi, 0|U^\dagger U|\phi', 0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle \langle e_\phi|e_{\phi'}\rangle$$

$$\| \qquad\qquad\qquad\qquad = \langle\phi|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle$$

$$\langle\phi, 0|\phi', 0\rangle$$

$$\|$$

$$\langle\phi|\phi'\rangle$$

Thm. $QU \Longleftrightarrow QI^2$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi,0\rangle = (V|\phi\rangle)\otimes|e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi',0\rangle = (V|\phi'\rangle)\otimes|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\phi,0|\phi',0\rangle = \langle\phi|\phi'\rangle$$

$$= \langle\phi|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle \Rightarrow \langle e_\phi|e_{\phi'}\rangle = 1$$

$$\boxed{|e_\phi\rangle = |e_{\phi'}\rangle}$$

Thm. $QU \Longleftrightarrow QI^2$

$$\boxed{\therefore\ U|\phi,0\rangle = (V|\phi\rangle)\otimes|e\rangle}$$

indep. of $|\phi\rangle$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi,0\rangle = (V|\phi\rangle)\otimes|e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi',0\rangle = (V|\phi'\rangle)\otimes|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\phi,0|\phi',0\rangle = \langle\phi|\phi'\rangle$$

$$= \langle\phi|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle \Rightarrow \langle e_\phi|e_{\phi'}\rangle = 1$$

$$\boxed{|e_\phi\rangle = |e_{\phi'}\rangle}$$

m. $QU \Longleftrightarrow QI^2$

$$\boxed{\therefore\ U|\phi,0\rangle = (V|\phi\rangle)\otimes|e\rangle}$$

indep. of $|\phi\rangle$

f. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi,0\rangle = (V|\phi\rangle)\otimes|e_\phi\rangle$$

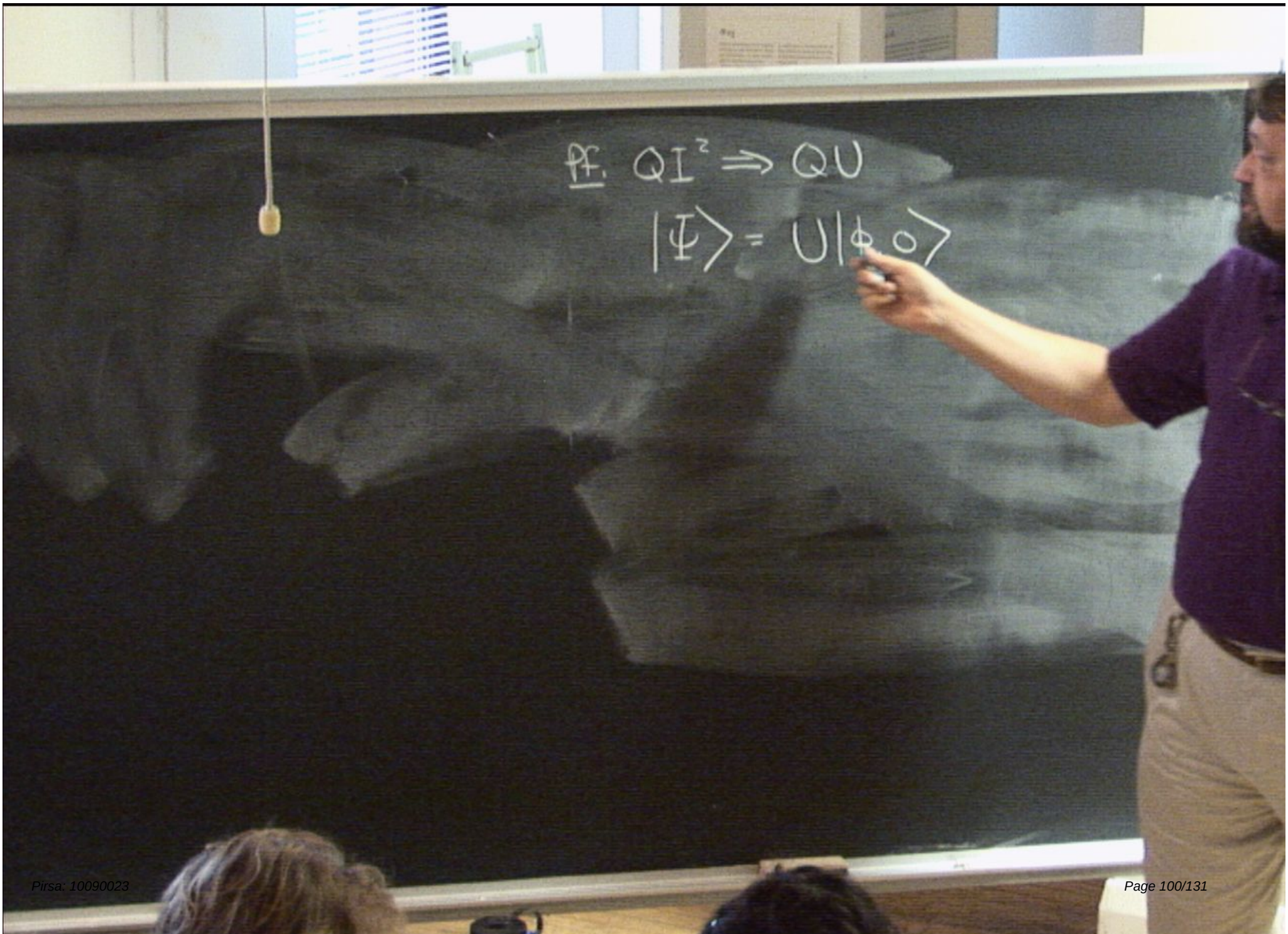
$$|\Psi'\rangle = U|\phi',0\rangle = (V|\phi'\rangle)\otimes|e_{\phi'}\rangle$$

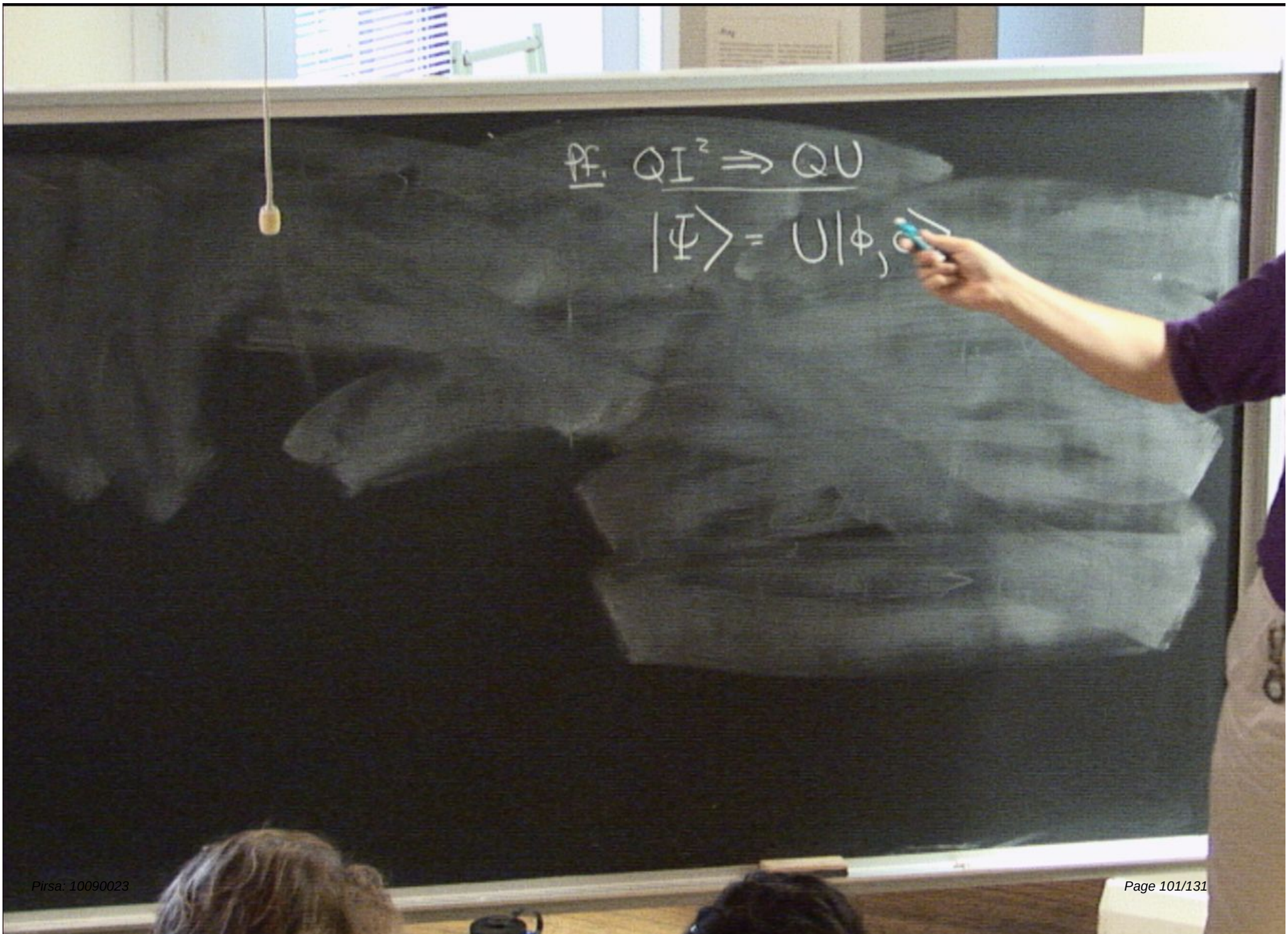
$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle\,\langle e_\phi|e_{\phi'}\rangle$$

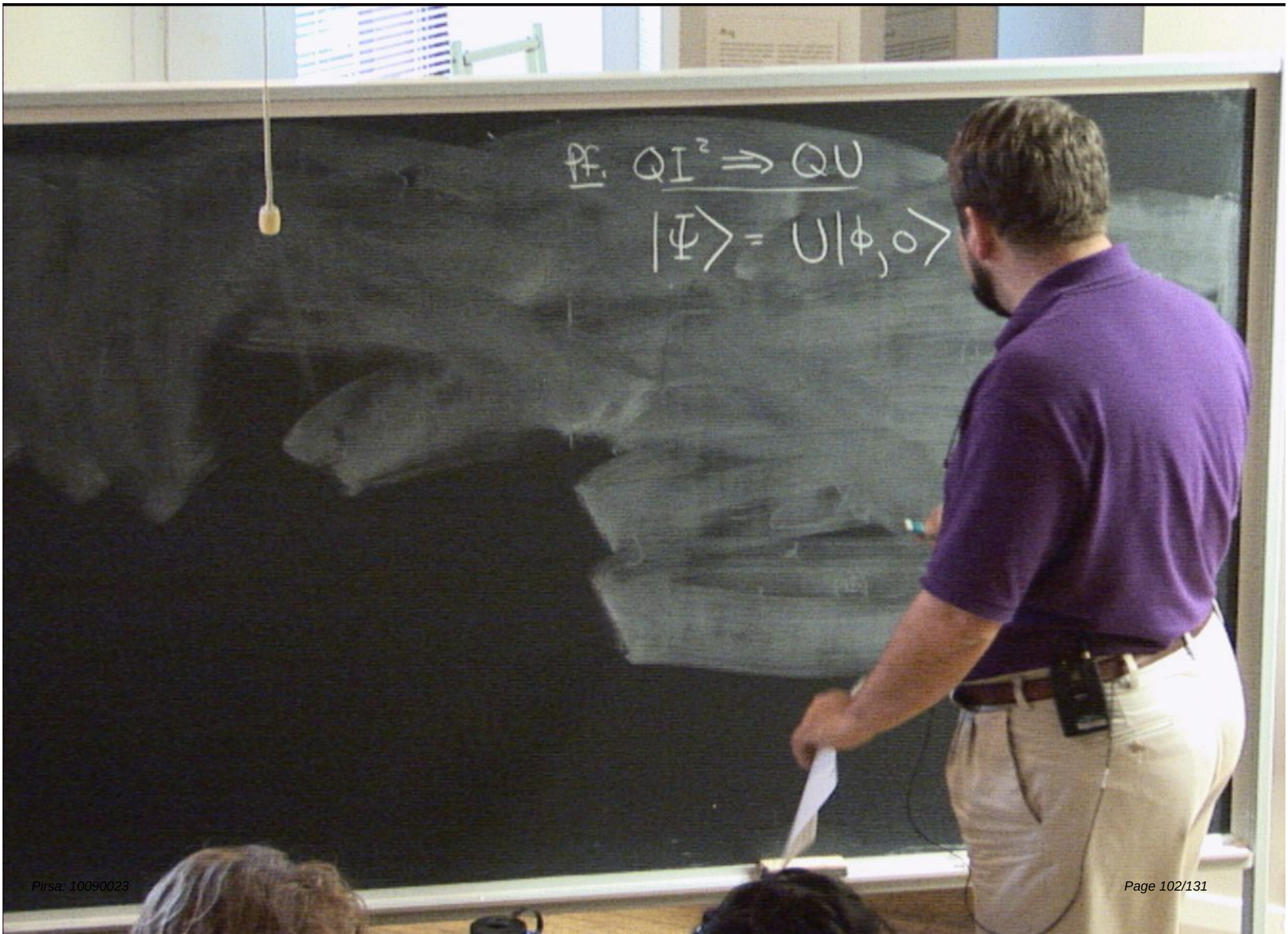
$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\phi,0|\phi',0\rangle = \langle\phi|\phi'\rangle$$

$$= \langle\phi|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle \Rightarrow \langle e_\phi|e_{\phi'}\rangle = 1$$

$$\boxed{|e_\phi\rangle = |e_{\phi'}\rangle}$$


Pf. QI² ⇒ QU
|Ψ⟩ = U|φ 0⟩


Pf. QI² ⇒ QU
|Ψ⟩ = U|φ,


Pf. QI² ⇒ QU
|Ψ⟩ = U|φ,0⟩

Pf. $QI^2 \Rightarrow QU$

$$|\Psi\rangle = U|\phi, 0\rangle$$

$$\sigma^{(E)} = \mathrm{tr}_{(Q)} |\Psi^{(QE)}\rangle\langle\Psi^{(QE)}|$$

Pf. $QI^2 \Rightarrow QU$

$$|\Psi\rangle = U|\phi, 0\rangle$$

$$\sigma^{(E)} = \mathrm{tr}_{(Q)} |\Psi^{(QE)}\rangle\langle\Psi^{(QE)}|$$

$$=$$

Pf. $QI^2 \Rightarrow QU$

$$|\Psi\rangle = U|\phi, 0\rangle$$

$$\sigma^{(A)} = \mathrm{tr}_{(Q)} |\Psi^{(QE)}\rangle\langle\Psi^{(QE)}|$$

$$= \sum_k \lambda_k |e_k\rangle\langle e_k|$$

Thm. $QU \Longleftrightarrow QI^2$

$$\boxed{\therefore\ U|\phi,0\rangle = \big(V|\phi\rangle\big)\otimes|e\rangle}$$

indep. of $|\phi\rangle$

Pf. $QU \Rightarrow QI^2$

Two initial Q-states $|\phi\rangle, |\phi'\rangle$

$$|\langle\phi|\phi'\rangle| > 0 \quad \text{(not orthog)}$$

$$|\Psi\rangle = U|\phi,0\rangle = \big(V|\phi\rangle\big)\otimes|e_\phi\rangle$$

$$|\Psi'\rangle = U|\phi',0\rangle = \big(V|\phi'\rangle\big)\otimes|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\Psi|\Psi'\rangle = \langle\phi|V^\dagger V|\phi'\rangle\,\langle e_\phi|e_{\phi'}\rangle$$

$$\langle\phi,0|U^\dagger U|\phi',0\rangle = \langle\phi,0|\phi',0\rangle = \langle\phi|\phi'\rangle$$

$$= \langle\phi|\phi'\rangle\langle e_\phi|e_{\phi'}\rangle \Rightarrow \langle e_\phi|e_{\phi'}\rangle = 1$$

$$\boxed{|e_\phi\rangle = |e_{\phi'}\rangle}$$

Schmidt decomposition for $|\Psi\rangle$

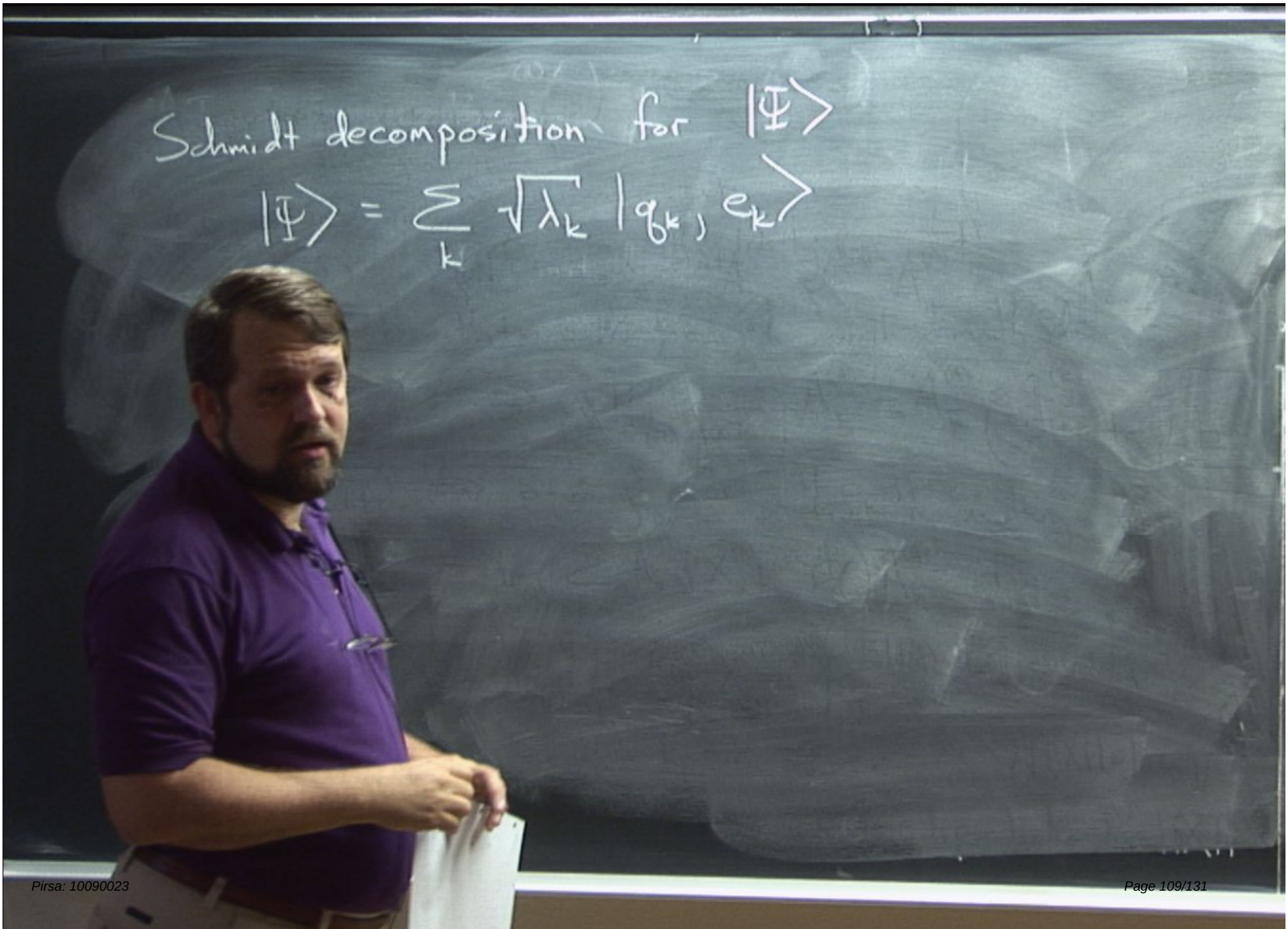
Pf. $QI^2 \Rightarrow QU$

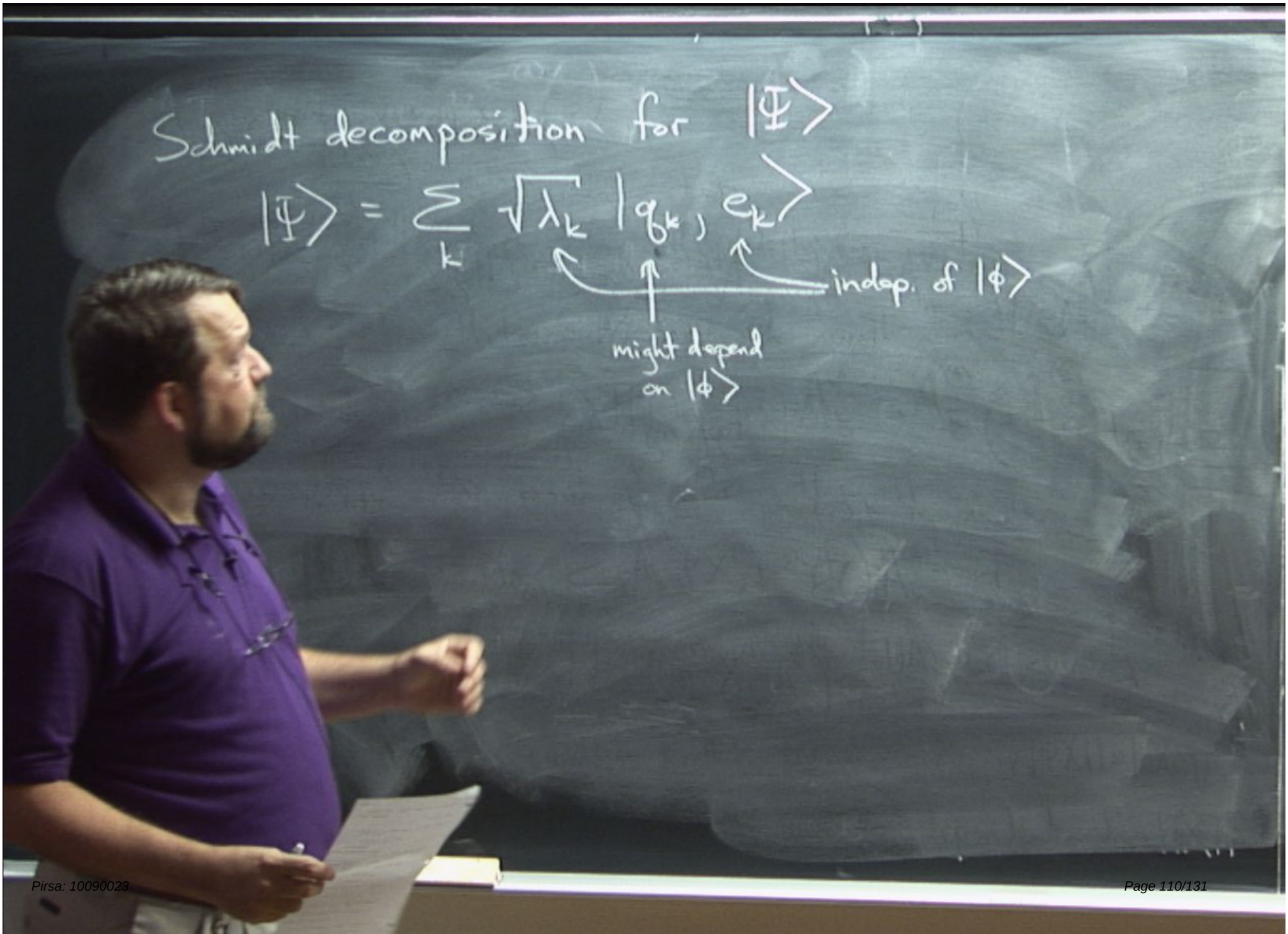
$$|\Psi\rangle = U|\phi, 0\rangle$$

$$\sigma^{(A)} = tr_{(Q)} |\Psi^{(QE)}\rangle\langle\Psi^{(QE)}|$$

$$= \sum_k \lambda_k |e_k\rangle\langle e_k|$$

Hyp: This is indep. of $|\phi\rangle$


Schmidt decomposition for $|\Psi\rangle$
$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$


Schmidt decomposition for $|\Psi\rangle$
$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$
indep. of $|\phi\rangle$
might depend on $|\phi\rangle$

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

For each k with $\lambda_k > 0$, define

$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle$$

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

each k with $\lambda_k > 0$, define

$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|\Psi\rangle$$

$$= |q_k\rangle$$

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

For each k with $\lambda_k > 0$, define

$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|\Psi\rangle$$

$$= |q_k\rangle$$

For any $|\phi\rangle$ $\langle q_k|q_k\rangle = 1$

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

For each k with $\lambda_k > 0$, define

$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|\Psi\rangle$$

$$= |q_k\rangle$$

for any $|\phi\rangle$

$$\langle q_k|q_k\rangle = 1 = \langle\phi|V_k^\dagger V_k|\phi\rangle$$

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

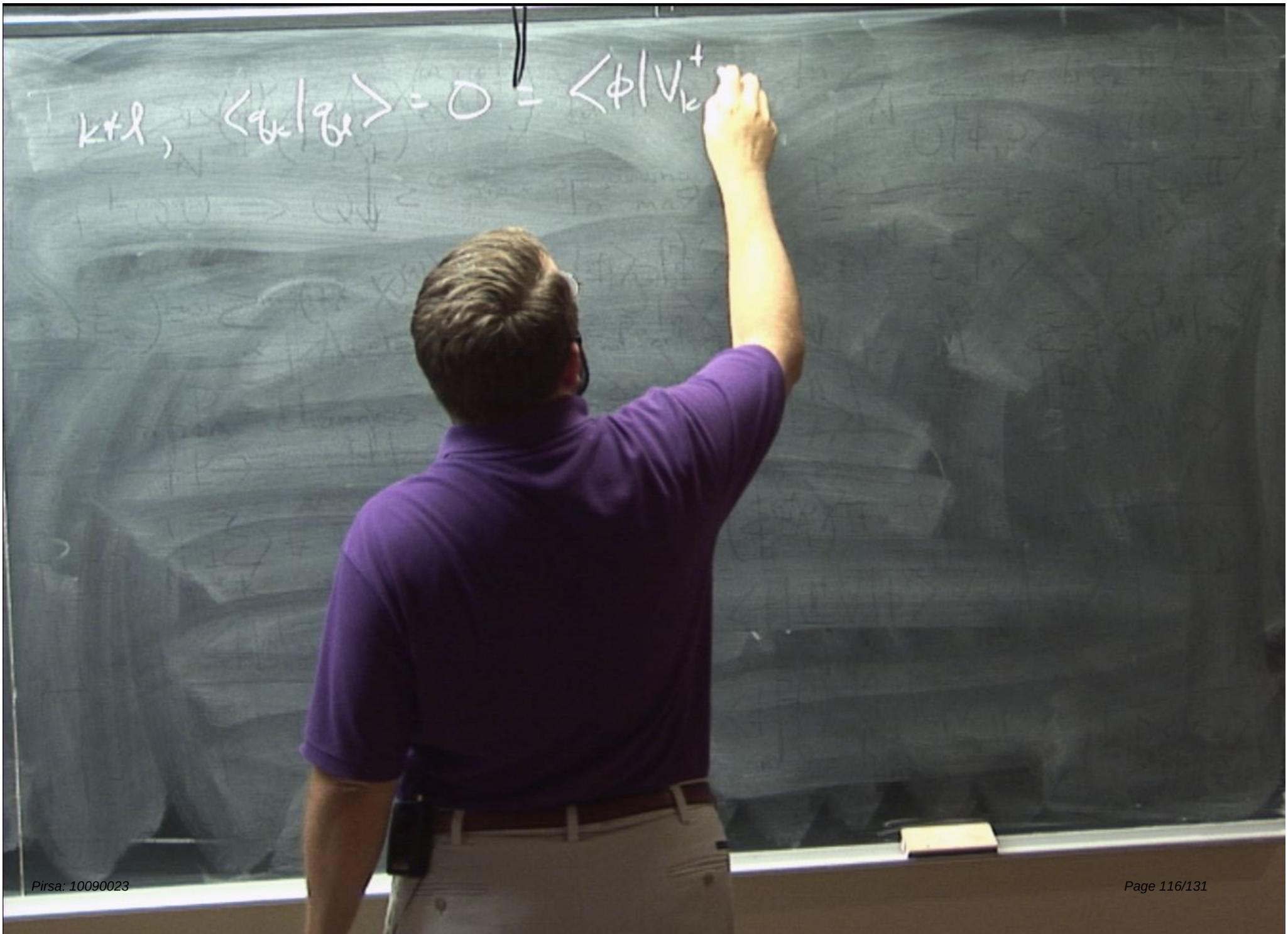
For each k with $\lambda_k > 0$, define

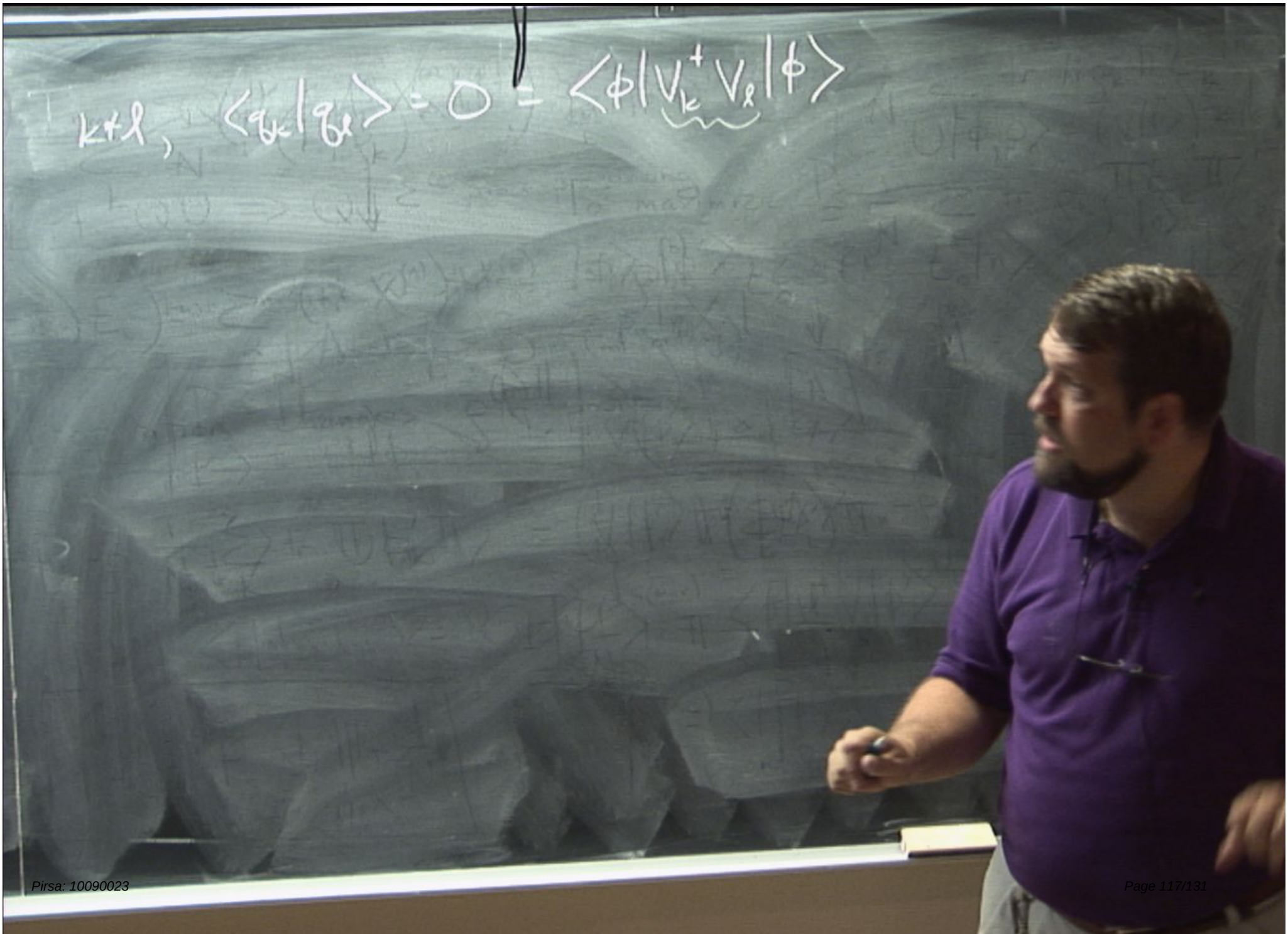
$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|\Psi\rangle$$

$$= |q_k\rangle$$

for any $|\phi\rangle$

$$\langle q_k|q_k\rangle = 1 = \langle\phi|V_k^\dagger V_k|\phi\rangle \Rightarrow V_k^\dagger V_k = \mathbb{I} \text{ (unitary)}$$


$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | V_k^{\dagger}$


$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | V_k^\dagger V_l | \phi \rangle$

$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

Schmidt decomposition for $|\Psi\rangle$

$$|\Psi\rangle = \sum_k \sqrt{\lambda_k}\, |q_k, e_k\rangle$$

indep. of $|\phi\rangle$

might depend on $|\phi\rangle$

For each k with $\lambda_k > 0$, define

$$V_k|\phi\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|U|\phi, 0\rangle = \frac{1}{\sqrt{\lambda_k}} \langle e_k|\Psi\rangle$$

$$= |q_k\rangle$$

for any $|\phi\rangle$

$$\langle q_k|q_k\rangle = 1 = \langle\phi|V_k^\dagger V_k|\phi\rangle \Rightarrow V_k^\dagger V_k = \mathbb{1} \quad (\underline{u}$$

$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

$\therefore$ There is only one $\lambda_k > 0$

$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

$\therefore$ There is only one $\lambda_k > 0$

$\sigma^{(\varepsilon)} = |e\rangle\langle e|$

$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

$\therefore$ There is only one $\lambda_k > 0$

$|e\rangle\langle e|$ (fixed)

$U|\phi, 0\rangle = |q, e\rangle = (V|\phi\rangle) \otimes |e\rangle$

$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

$\therefore$ There is only one $\lambda_k > 0$

$\sigma^{(E)} = |e\rangle\langle e|$ (fixed)

$|\Psi\rangle = U|\phi, 0\rangle = |q, e\rangle = (V|\phi\rangle) \otimes |e\rangle$

QED — $\boxed{QU \Leftrightarrow QI^2}$

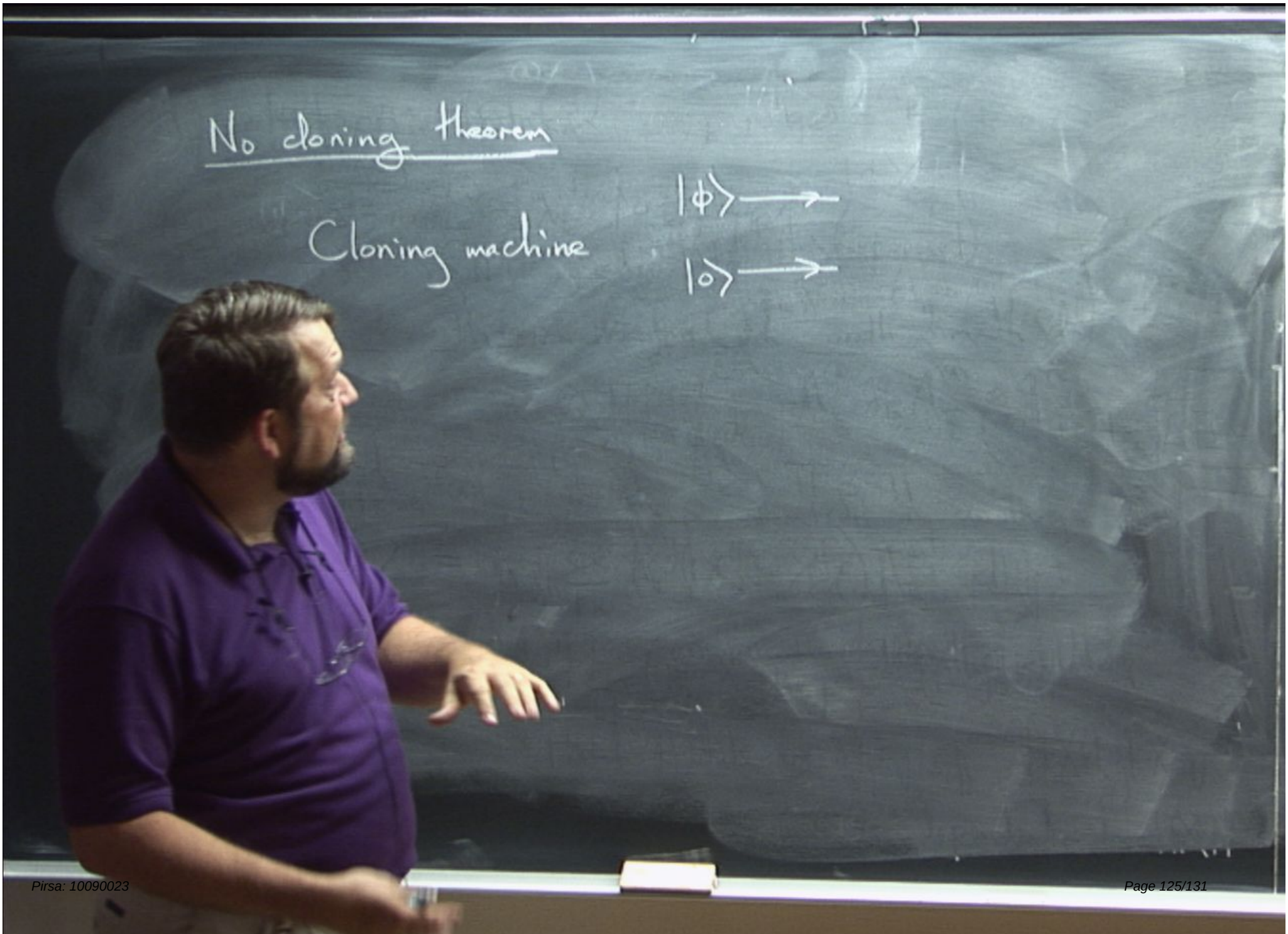
$k \neq l, \quad \langle q_k | q_l \rangle = 0 = \langle \phi | \underbrace{V_k^\dagger V_l}_{\text{must be unitary!}} | \phi \rangle$ Not $= 0$!

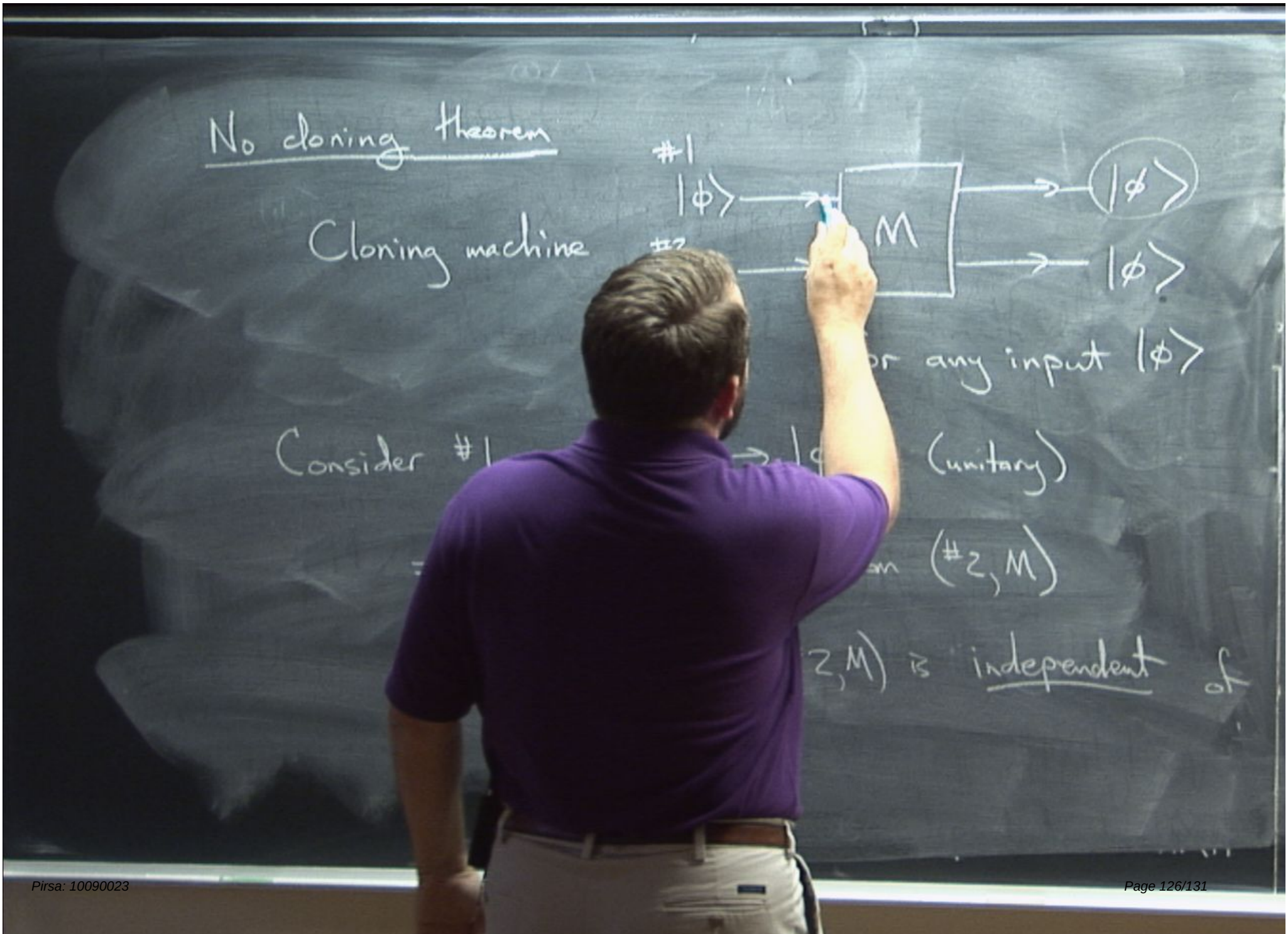
$\therefore$ There is only one $\lambda_k > 0$

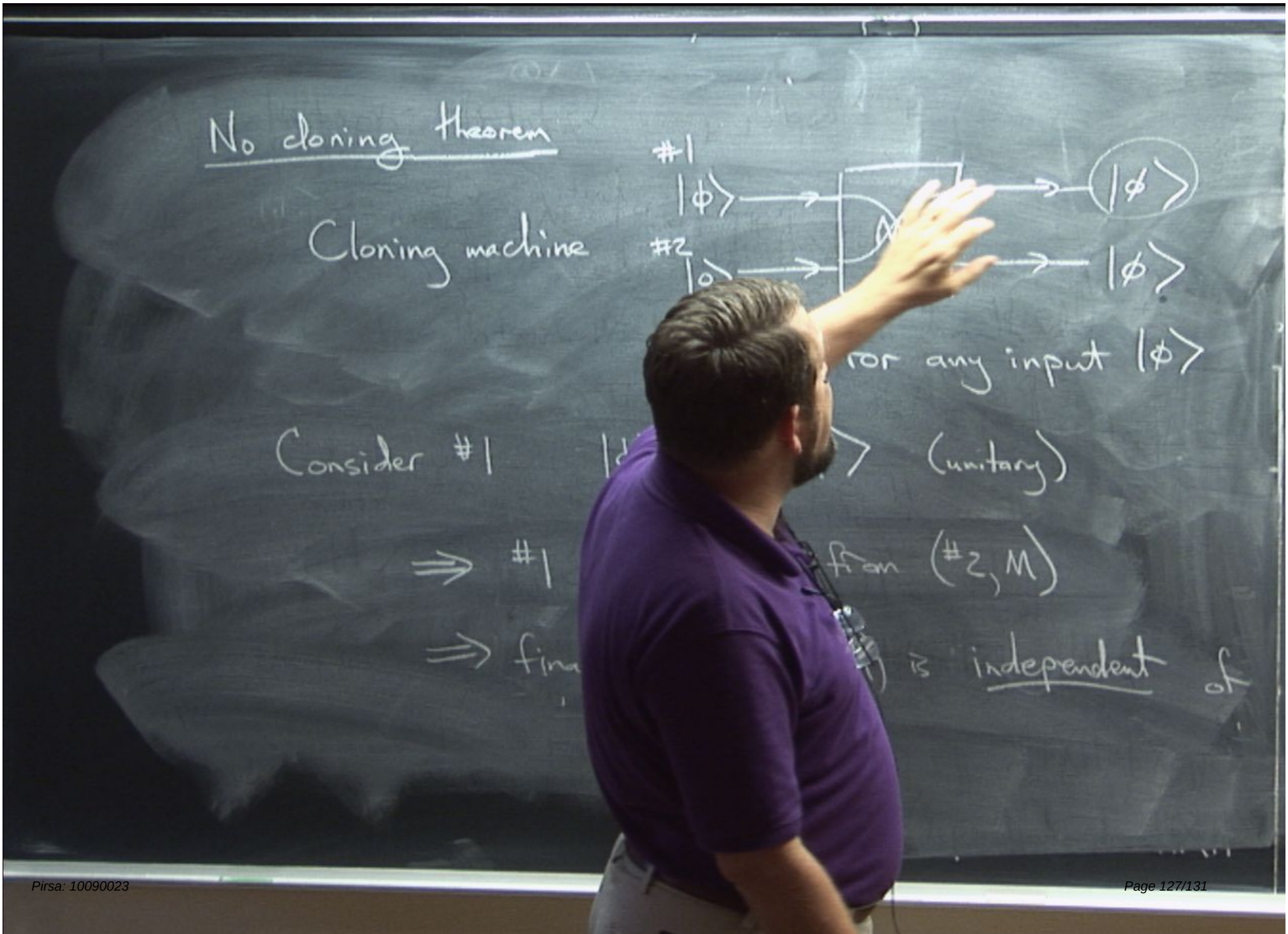
$\sigma^{(E)} = |e\rangle\langle e|$ (fixed)

$|\Psi\rangle = U|\phi, 0\rangle = |q, e\rangle = (V|\phi\rangle) \otimes |e\rangle$

QED — $\boxed{QU \Leftrightarrow QI^2}$

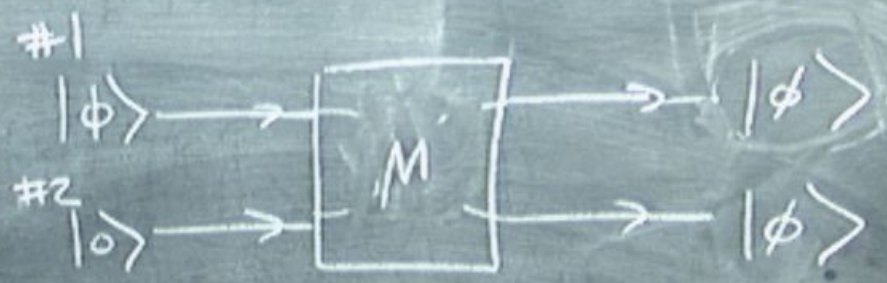

No cloning theorem
Cloning machine
$|\phi\rangle \longrightarrow$
$|0\rangle \longrightarrow$


No cloning theorem
#1
|φ⟩
M
|φ⟩
Cloning machine
|φ⟩
or any input |φ⟩
Consider #1
(unitary)
(#2, M)
2, M) is independent of


No cloning theorem
Cloning machine
#1
#2
|φ⟩
|0⟩
|φ⟩
|φ⟩
for any input |φ⟩
Consider #1
(unitary)
⇒ #1
from (#2, M)
⇒ fina
is independent of

No cloning theorem

Cloning machine



for any input $|\phi\rangle$

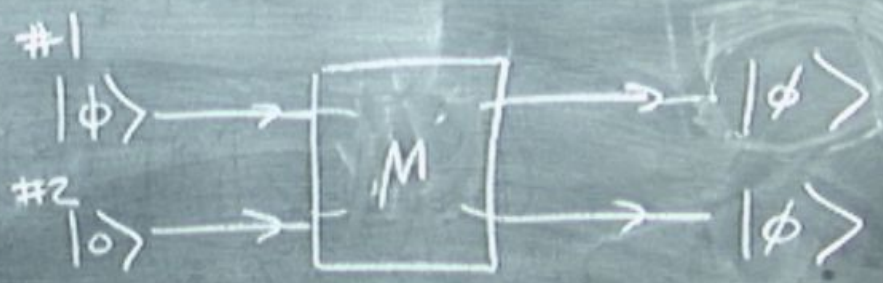
Consider #1 $\quad |\phi\rangle \longrightarrow |\phi\rangle$ (unitary)

$\Rightarrow$ #1 is info. isolated from (#2, M)

$\Rightarrow$ final state of (#2, M) is <u>independent</u> of

No cloning theorem

Cloning machine



for any input $|\phi\rangle$

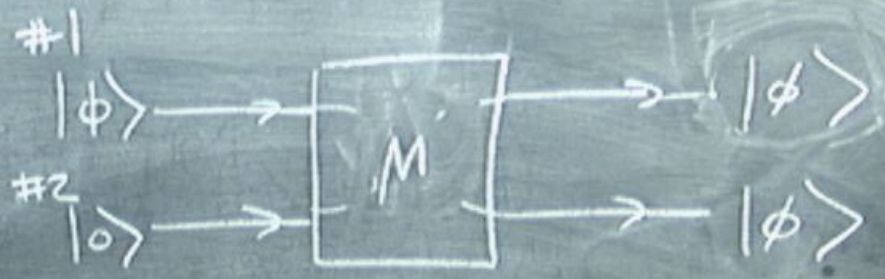
Consider #1 $\quad |\phi\rangle \longrightarrow |\phi\rangle$ (unitary)

$\Rightarrow$ #1 is info. isolated from (#2, M)

$\Rightarrow$ final state of (#2, M) is <u>independent</u> of

No cloning theorem

Cloning machine



for any input $|\phi\rangle$

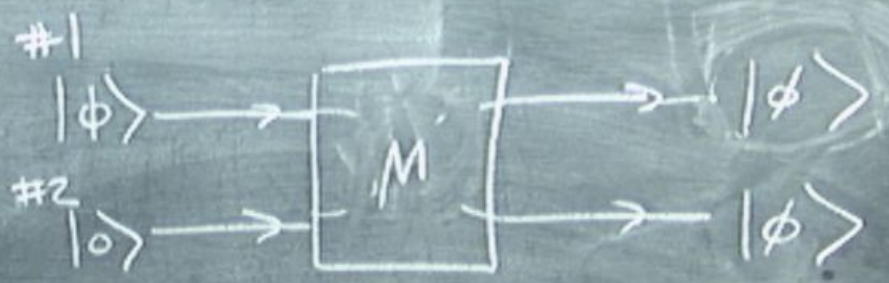
Consider #1 $\quad |\phi\rangle \longrightarrow |\phi\rangle$ (unitary)

$\Longrightarrow$ #1 is info. isolated from (#2, M)

$\Longrightarrow$ final state of (#2, M) is <u>independent</u> of

No cloning theorem

Cloning machine



for any input $|\phi\rangle$

Consider #1 $\quad |\phi\rangle \longrightarrow |\phi\rangle$ (unitary)

$\Rightarrow$ #1 is info. isolated from (#2, M)

$\Rightarrow$ final state of (#2, M) is <u>independent</u> of