Title: Quantum Error Correction 3B

Date: Jan 23, 2007 05:00 PM

URL: http://pirsa.org/07010023

Abstract: Clifford group as symplectic group, generators of the Clifford group & encoding circuits for stabilizer codes, efficient simulation of Clifford group circuits, efficient simulation of Pauli measurements

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$

E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$ or $C_n / \{e^{i\theta} I\}$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

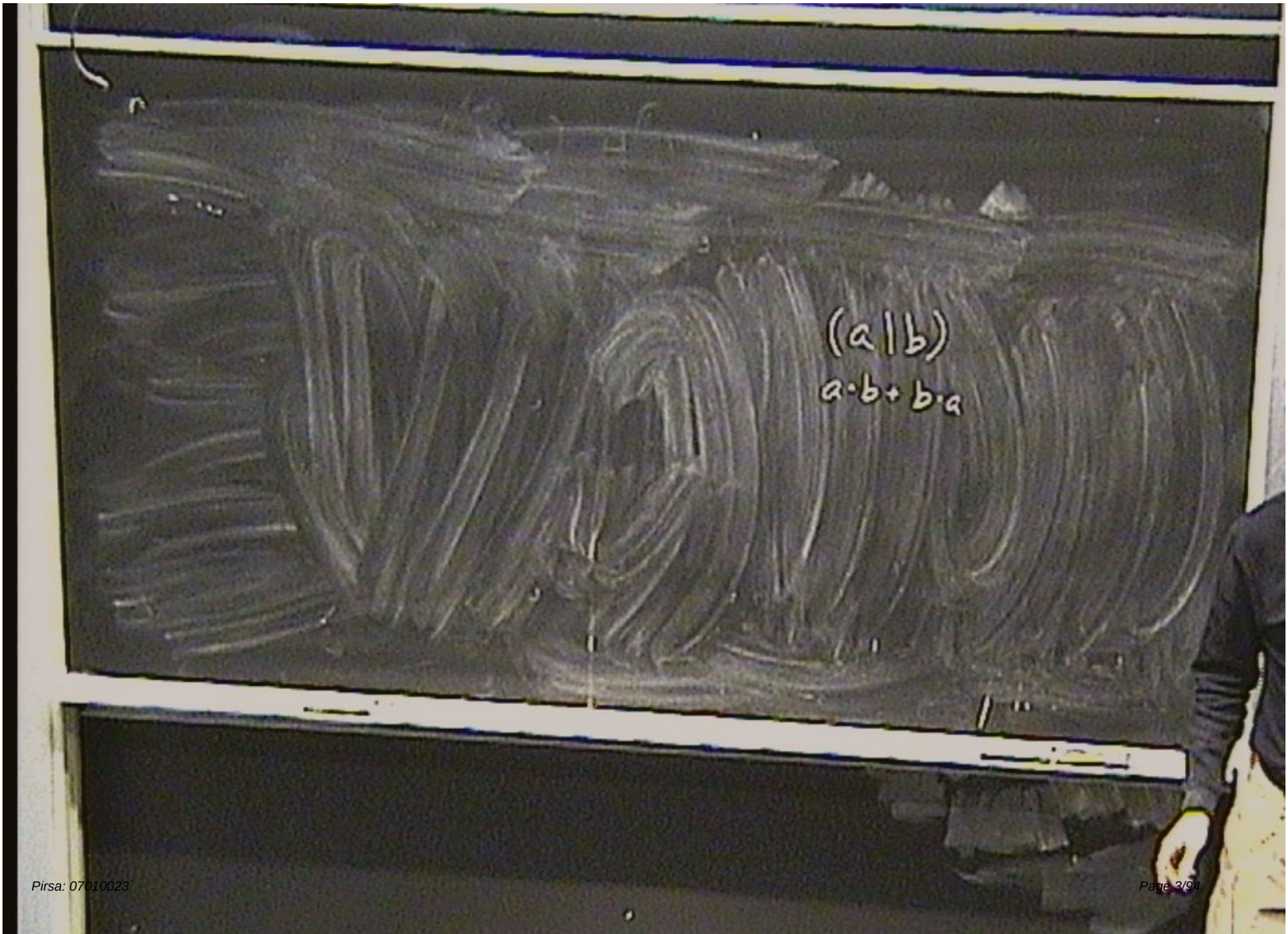
$X \to Z$
$Z \to X$
$Y \to -Y$

$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

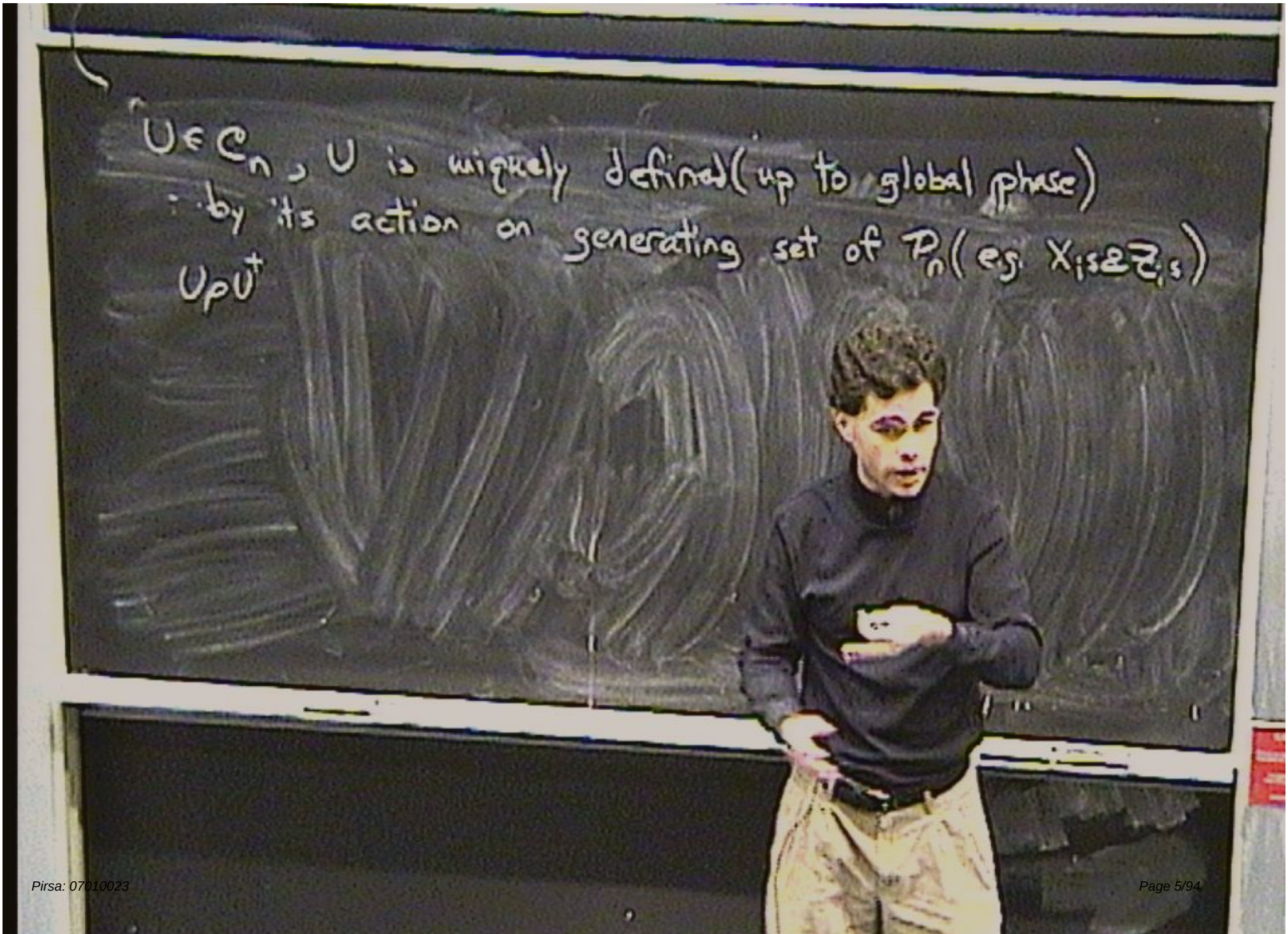
$X \to Y$
$Y \to -X$
$Z \to Z$

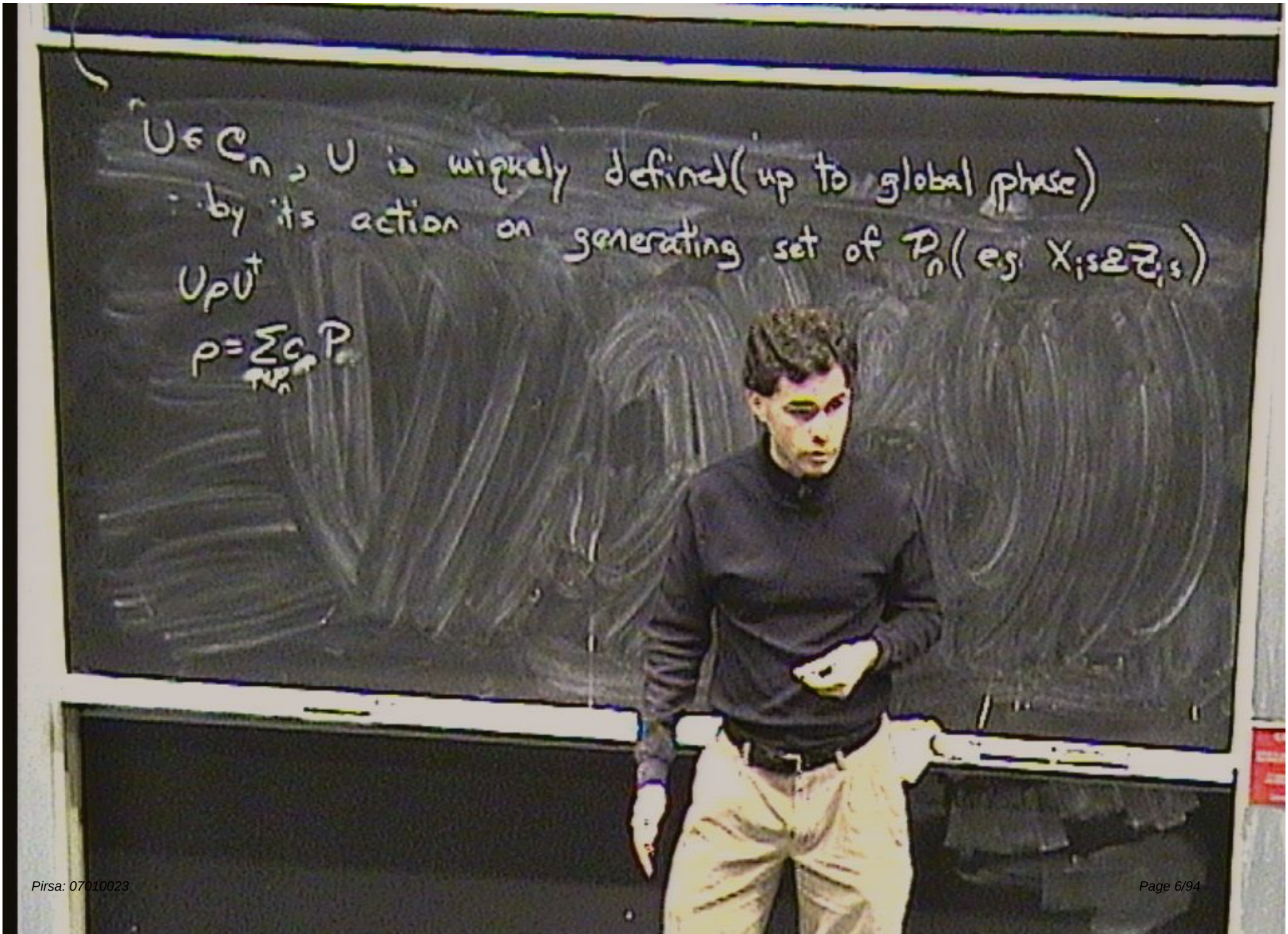
CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$

Permutations of qubits


(a|b)
a·b+b·a

$U \in \mathbb{C}_n$, U is uniquely defined (up to global phase)
by its action on generating set of $\mathcal{P}_n$ (e.g. X_i's & Z_i's)


$U \in \mathbb{C}_n$, U is uniquely defined (up to global phase)
: by its action on generating set of $\mathcal{P}_n$ (e.g. X_i & Z_i's)
$UpU^\dagger$


$U \in \mathbb{C}_n$, U is uniquely defined (up to global phase)
by its action on generating set of $\mathcal{P}_n$ (e.g. X_i & Z_i's)
$UpU^\dagger$
$p = \sum_{\text{sup}_n} c_p P$

$U \in \mathbb{C}_n$, U is uniquely defined (up to global phase)
: by its action on generating set of $\mathcal{P}_n$ (e.g. $X_1 \otimes \mathbb{1}_{2^{n-1}}$)

$U \rho U^\dagger = U(\sum_\phi c_\phi P) U^\dagger = \sum_\phi c_\phi U P U^\dagger$

$\rho = \sum_{P \in \mathcal{P}_n} c_P P$

$U \in \mathbb{C}_n$, U is uniquely defined (up to global phase)
by its action on generating set of $\mathcal{P}_n$ (e.g. X_i's & Z_i's)

$U\rho U^\dagger = U(\sum_\rho c_\rho P)U^\dagger = \sum_\rho c_\rho UPU^\dagger \Rightarrow U$ defined up to phase

$\rho = \sum_{P \in \mathcal{P}_n} c_\rho P$.

$U \in \mathcal{C}_n$, U is uniquely defined (up to global phase)
by its action on generating set of $\mathcal{P}_n$ (e.g. X_is & Z_is)

$UpU^\dagger = U(\sum_\phi c_\phi P)U^\dagger = \sum_\phi c_\phi UPU^\dagger \Rightarrow U$ defined up to phase

$p = \sum_{P \in \mathcal{P}_n} c_P P$

$U \in \mathcal{C}_n$, U is uniquely defined (up to global phase)
∴ by its action on generating set of $\mathcal{P}_n$ (eg. X_is & Z_is)

$U\rho U^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

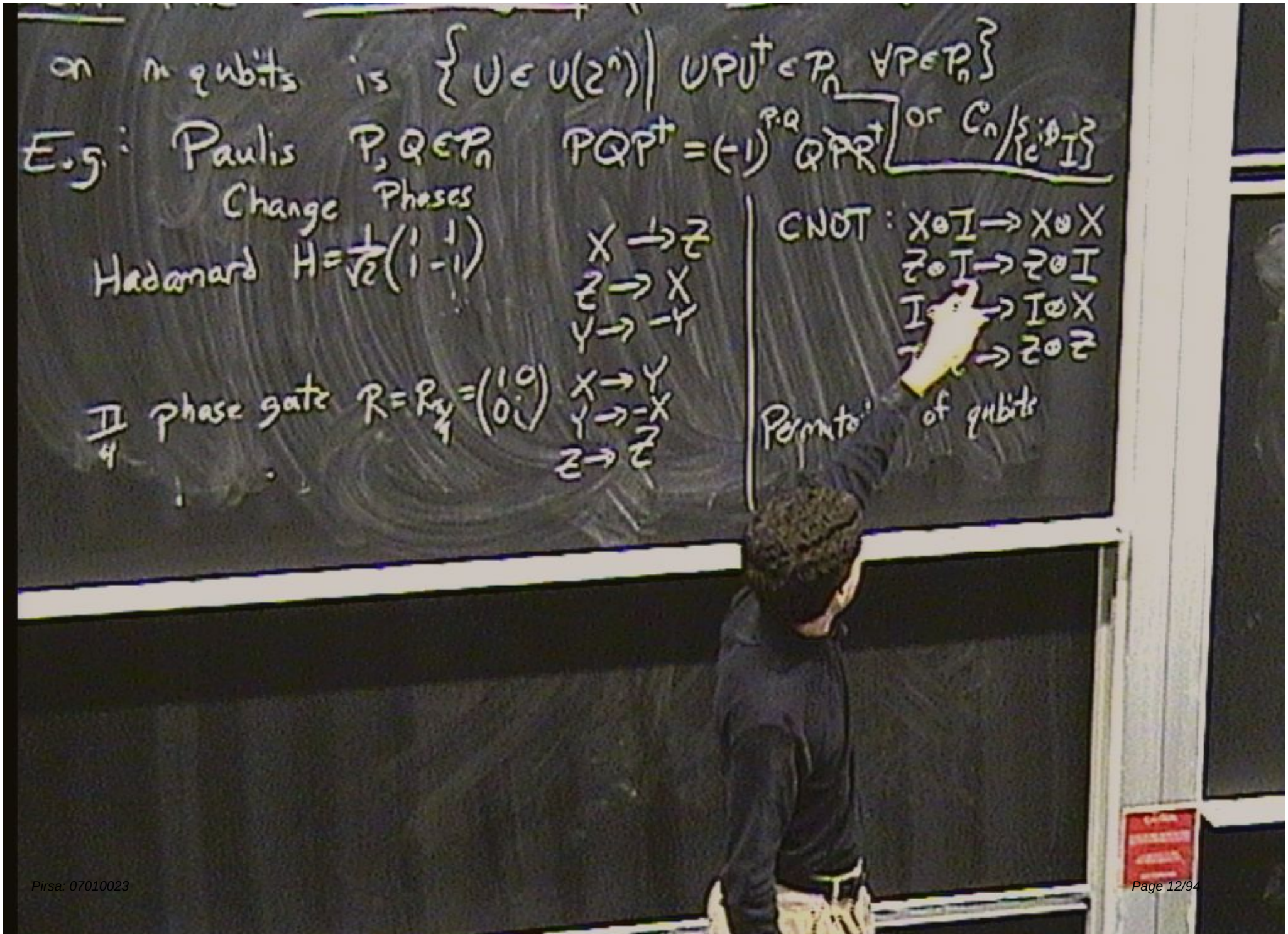
$\rho = \sum_{P \in \mathcal{P}_n} c_P P$

$U \in C_n$, U is uniquely defined (up to global phase)
∴ by its action on generating set of P_n (eg. X_1s & Z_1s)

$UpU^\dagger = U(\sum_p c_p p)U^\dagger = \sum_p c_p UpU^\dagger \Rightarrow U$ defined up to phase

$p = \sum_{p \in P_n} c_p p$

$P_n \triangleleft C_n$ (normal subgroup of C_n)


on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$
E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$
or $C_n/\{e^{i\theta} I\}$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$X \to Z$
$Z \to X$
$Y \to -Y$
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$X \to Y$
$Y \to -X$
$Z \to Z$
CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \to I \otimes X$
$\to Z \otimes Z$
Permute of qubits

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_i's & Z_i's)

$U\rho U^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

$\rho = \sum_{P \in P_n} c_p P$

$P_n \triangleleft C_n$ (normal subgroup of C_n)

Pauli control phases

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_i's & Z_i's)

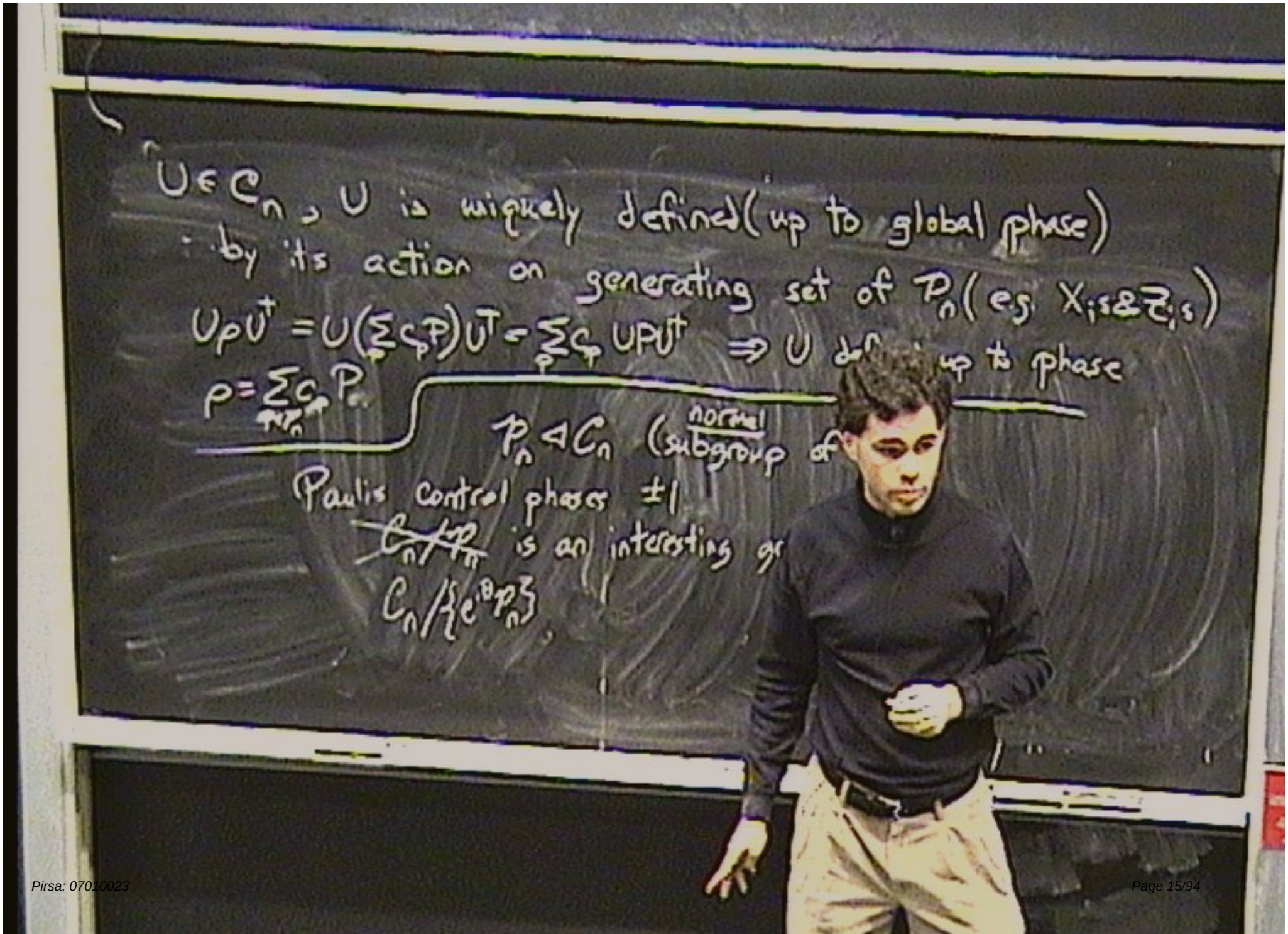
$UPU^\dagger = U(\sum_P c_P P)U^\dagger = \sum_P c_P UPU^\dagger \Rightarrow U$ defined up to phase

$P = \sum_{P \in P_n} c_P P$

$P_n \triangleleft C_n$ (normal subgroup of C_n)

Paulis control phases

C_n / P_n is an interesting group too


$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_i's & Z_i's)
$UPU^\dagger = U(\sum_P c_P P)U^\dagger = \sum_P c_P UPU^\dagger \Rightarrow U$ d
up to phase
$P = \sum_{P \in P_n} c_P P$
$P_n \triangleleft C_n$ (normal subgroup of
Pauli control phases ± 1
C_n/P_n is an interesting gr
$C_n/\{e^{i\theta} P_n\}$,

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_i's & Z_i's)

$UpU^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

$P = \sum_{p \in P_n} c_p P$

$P_n \triangleleft C_n$ (normal subgroup of C_n)

Pauli's control phases ± 1

~~C_n / P_n~~ is an interesting group too

$C_n / \{e^{i\theta} P_n\}$

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_i's & Z_i's)

$UpU^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

$p = \sum_{P \in P_n} c_P P$

$P_n \triangleleft C_n$ (normal subgroup of C_n)

Paulis control phases ± 1

C_n / P_n is an interesting group too

Thm.: $C_n / \{e^{i\theta} P_n\} = S_p(2n, \mathbb{Z})$ symplectic group

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of P_n (e.g. X_is & Z_is)

$UpU^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

$p = \sum_{p \in P_n} c_p P$.

$P_n \triangleleft C_n$ (normal subgroup of C_n)

Paulis control phases ± 1

~~C_n / P_n~~ is an interesting group too

Thm.: $C_n / \{e^{i\theta} P_n\} = Sp(2n, \mathbb{Z})$ symplectic g

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$- tors that preserve symplectic inner product

$U \in C_n$, U is uniquely defined (up to global phase)
by its action on generating set of $\mathcal{P}_n$ (e.g. X_is & Z_is)

$UpU^\dagger = U(\sum_p c_p P)U^\dagger = \sum_p c_p UPU^\dagger \Rightarrow U$ defined up to phase

$p = \sum_{p \in \mathcal{P}_n} c_p P$

$\mathcal{P}_n \triangleleft C_n$ ($\frac{\text{normal}}{\text{subgroup}}$ of C_n)

Paulis control phases ± 1

~~$C_n / \mathcal{P}_n$~~ is an interesting group too

Thm.: $C_n / \{e^{i\theta} p_n\} = Sp(2n, \mathbb{Z})$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

$\rho = \sum_{P_n \in C_n} c_P P$

$P_n \triangleleft C_n$ (normal subgroup of C_n)

(Pauli central phases ± 1)

~~C_n / P_n~~ is an interesting group too

Thm.: $C_n / \{e^{i\theta} P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b) \cdot (c|d) = a \cdot d + b \cdot c$

Thm.: $C_n/\{e^{i\theta}P_n\} \equiv Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations:

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$:

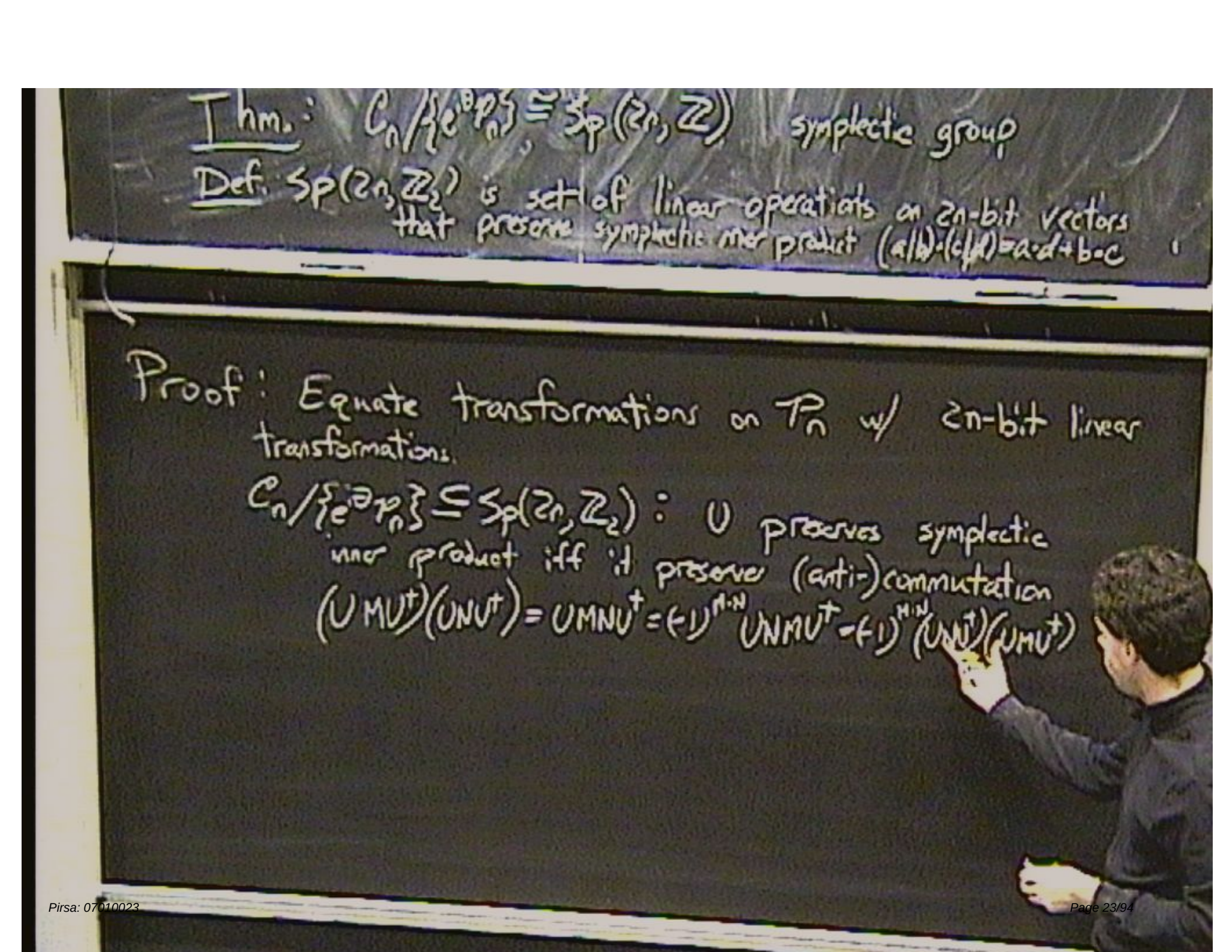
Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$



Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$:

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Define $U \in C_n$ $\vec{v} \mapsto P \cdot \{X_i, Z_i\}$ $UPU^\dagger \leftrightarrow T(\vec{v}_P)$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Define $U \in C_n$ $\vec{v}_p \mapsto P: \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow T(\vec{v}_p)$

Pick ± 1 for each X_i & Z_i → extend U to $\forall P \in P_n$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

transformations

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$

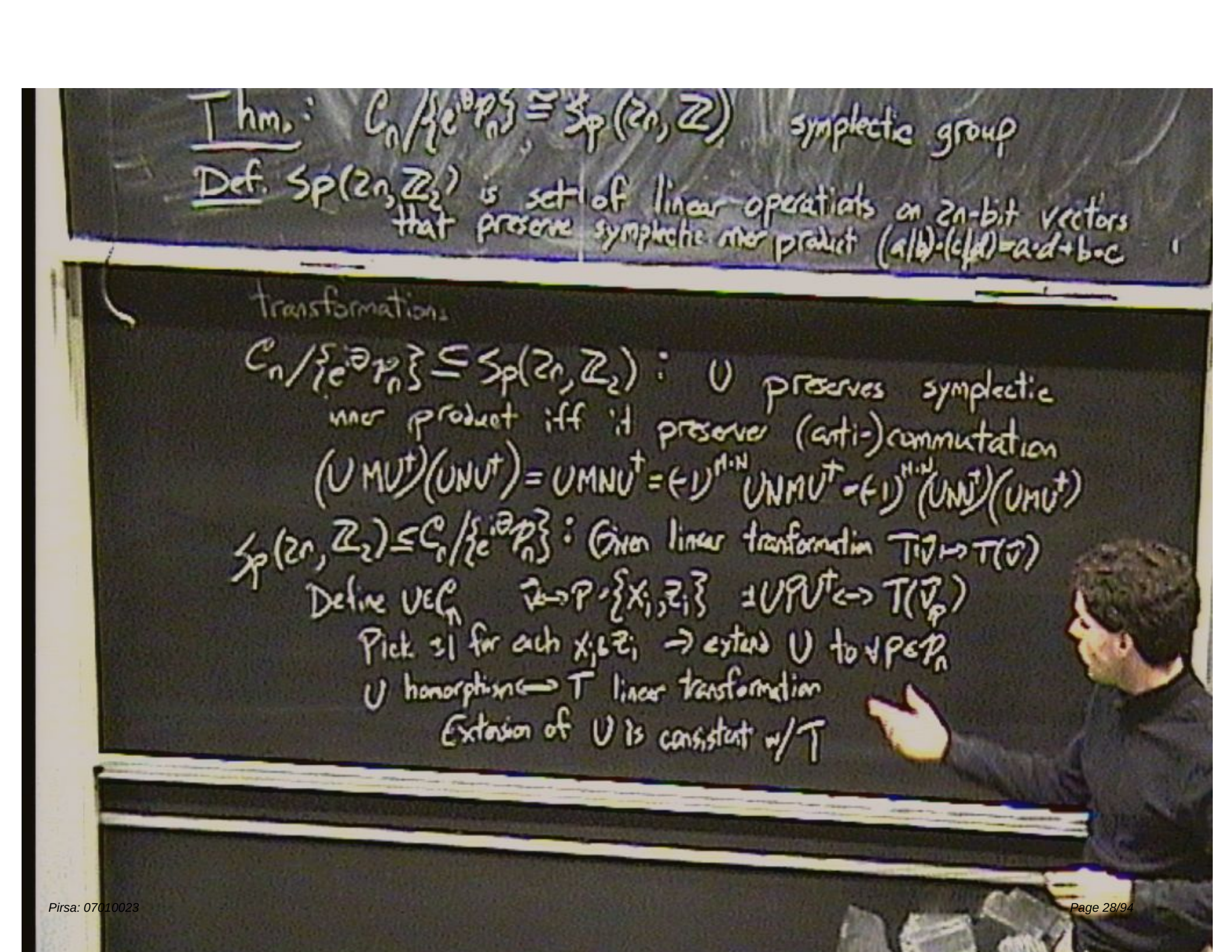
$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Define $U \in C_n$ $\vec{v} \mapsto P = \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow T(\vec{v}_P)$

Pick ± 1 for each X_i & Z_i → extend U to $\forall P \in P_n$

U homomorphism $\leftrightarrow$ T linear transformation

Extension of U is consistent w/ T



Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z})$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

transformations:

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Define $U \in C_n$ $\vec{v} \mapsto P = \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow T(\vec{v}_P)$

Pick ± 1 for each X_i, Z_i → extend U to $\forall P \in \mathcal{P}_n$

U homomorphism ⟷ T linear transformation

Extension of U is consistent w/ T

$U \sim T$

U, U', $UU'U' \in \{e^{i\theta}P_n\}$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$Sp(2n,\mathbb{Z}_2)$ $C_n/(\ )$

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserve (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}($

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation T:?

Define $U \in C_n$ $\vec{v} \mapsto P = \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow$ -

Pick ± 1 for each X_i, Z_i → extend U to $\forall$

U homorphism → T linear transformation

Extension of U is consistent w/ T

same T

$'s\{e^{i\theta}P_n\}$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{\cdots}$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $-$ $\cdots$

Define $U \in C_n$ $\vec{v} \to P = \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow$

Pick ± 1 for each X_i, Z_i → extend U to U homomorphism → T linear transformation

Extension of U is consistent w/ T

$Sp(2n, \mathbb{Z}_2) \cong C_n/(\quad)$

C_n

same T

$\in \{e^{i\theta}P_n\}$

Thm.: $C_n/\{e^{i\theta}P_n\} \cong Sp(2n, \mathbb{Z}_2)$ symplectic group

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Proof: Equate transformations on P_n w/ $2n$-bit linear transformations.

$C_n/\{e^{i\theta}P_n\} \subseteq Sp(2n, \mathbb{Z}_2)$: U preserves symplectic inner product iff it preserves (anti-)commutation

$(UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = (-1)^{M\cdot N} UNMU^\dagger = (-1)^{M\cdot N}(UNU^\dagger)(UMU^\dagger)$

$Sp(2n, \mathbb{Z}_2) \subseteq C_n/\{e^{i\theta}P_n\}$: Given linear transformation $T: \vec{v} \mapsto T(\vec{v})$

Define $U \in C_n$ $\vec{v} \mapsto P = \{X_i, Z_i\}$ $\pm UPU^\dagger \leftrightarrow T(\vec{v}_P)$

Pick ± 1 for each X_i, Z_i → extend U to $\forall P \in P_n$

U homomorphism → T linear transformation

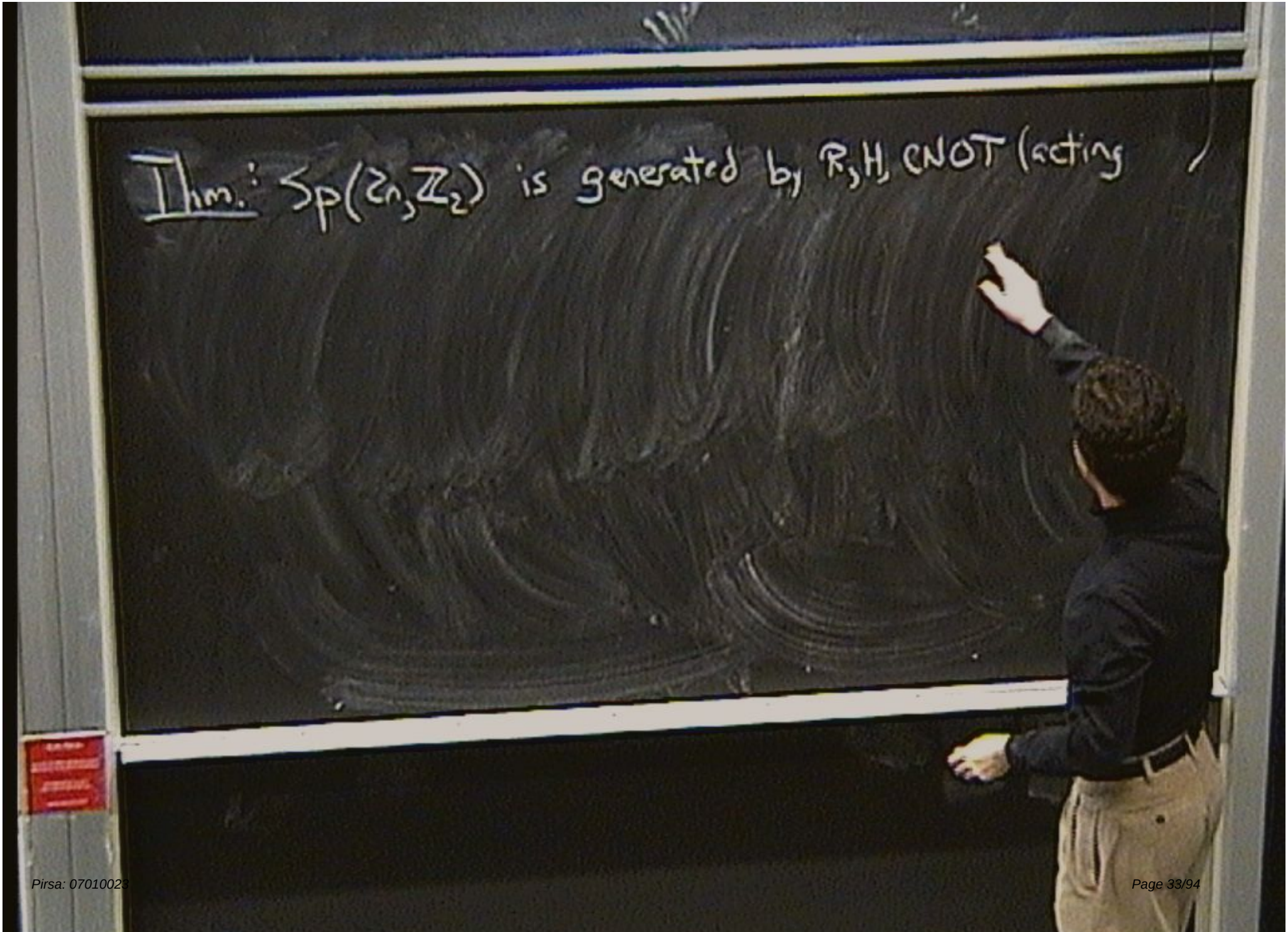
Extension of U is consistent w/ T

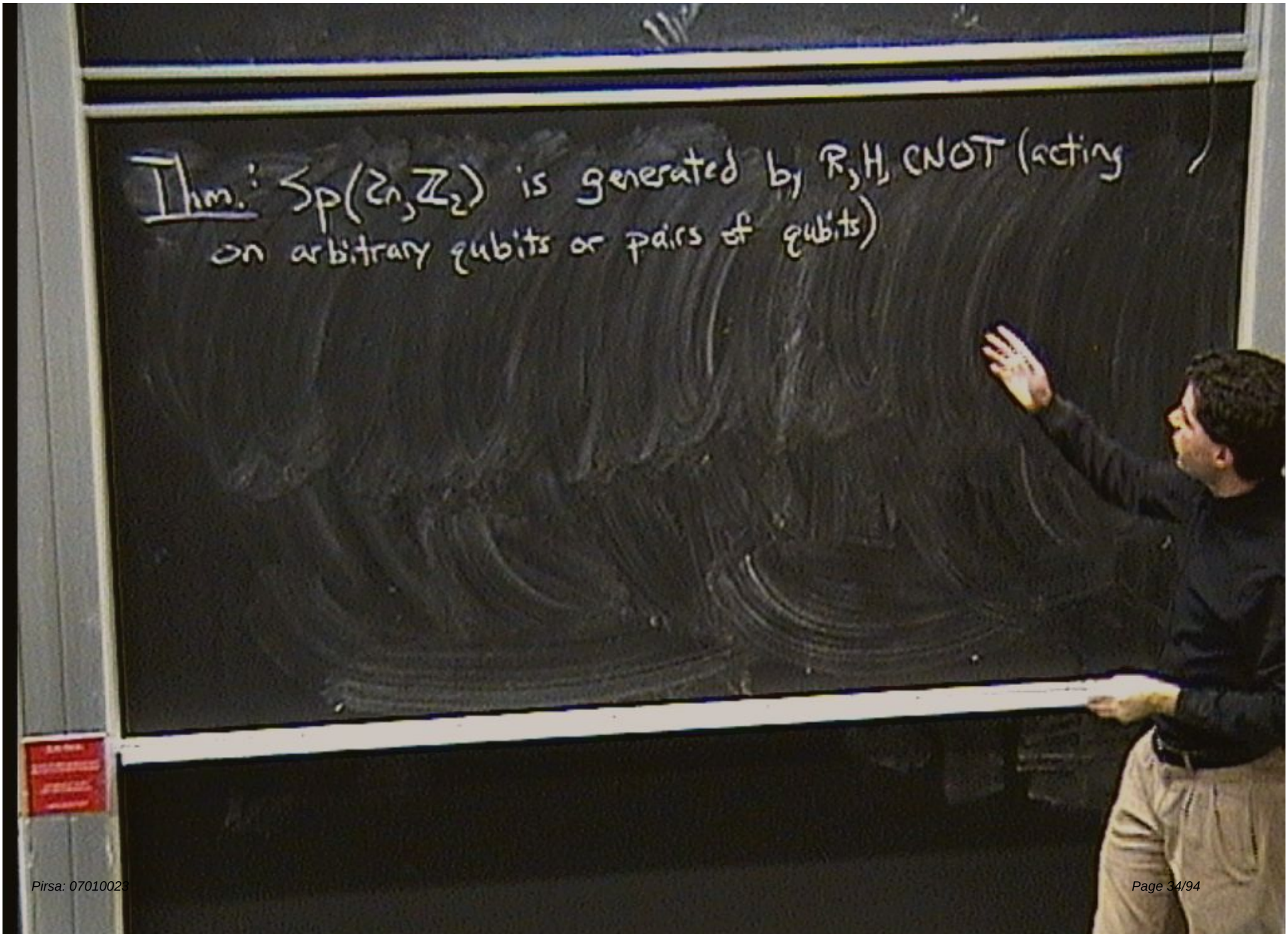
$Sp(2n, \mathbb{Z}_2) \cong C_n/(\quad)$

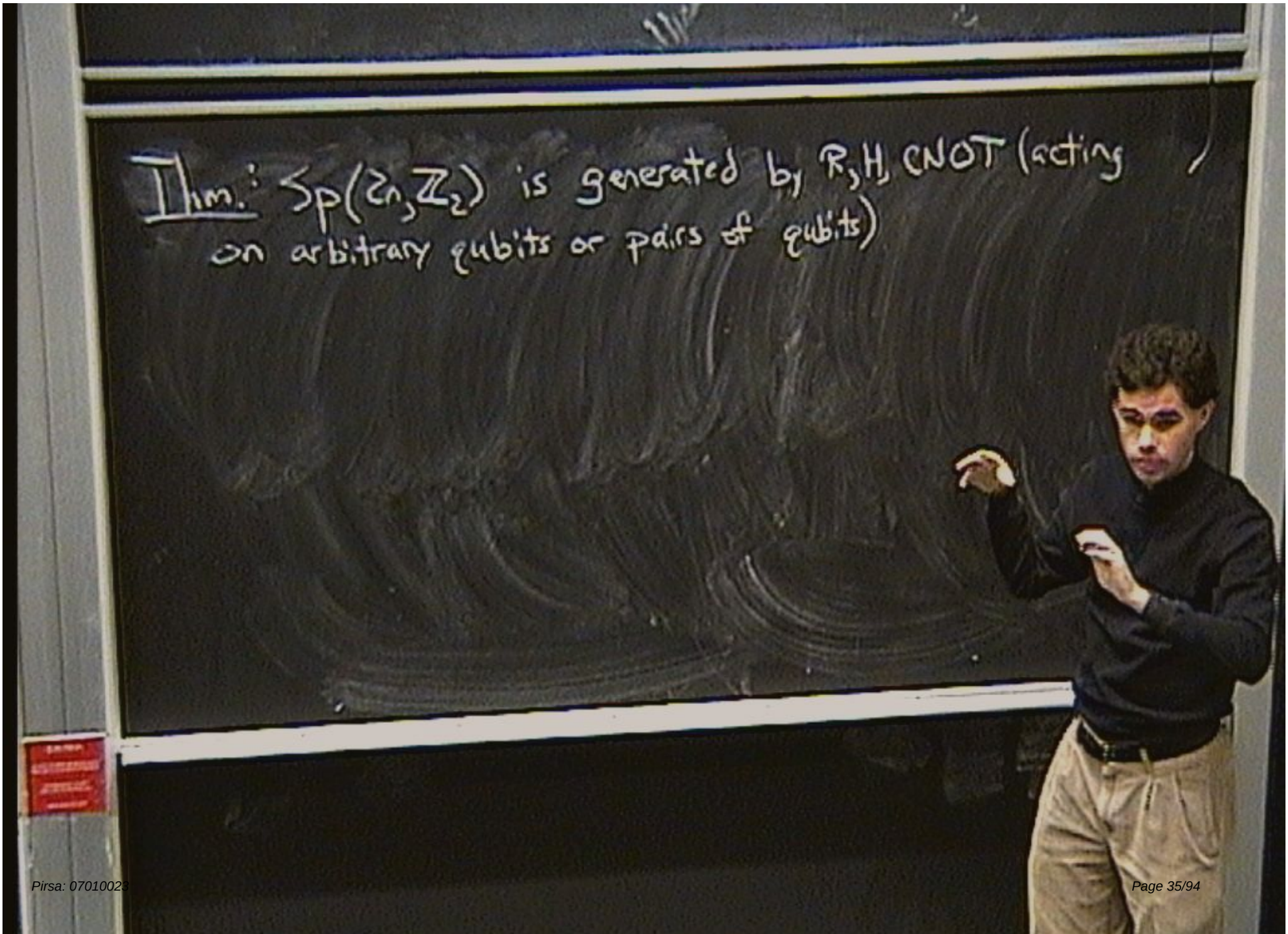
C_n

$U \sim T$ (same T)

U, U', $UU' \in \{e^{i\theta}P_n\}$


Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting


Thm.: Sp(2n, Z2) is generated by R, H, CNOT (acting
on arbitrary qubits or pairs of qubits)


Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting on arbitrary qubits or pairs of qubits)

Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting on arbitrary qubits or pairs of qubits)

Proof:

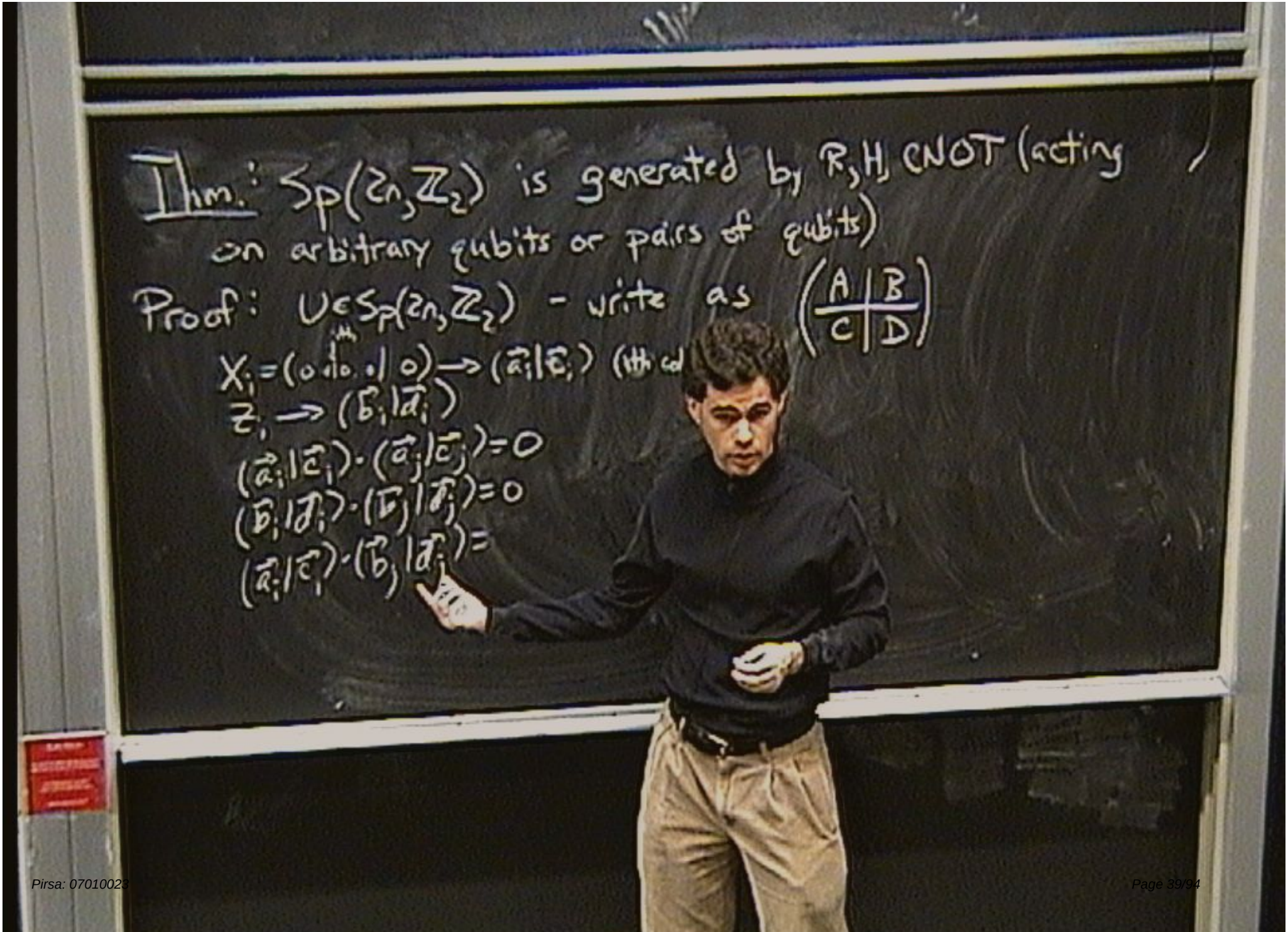
Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by $R, H, CNOT$ (acting on arbitrary qubits or pairs of qubits)

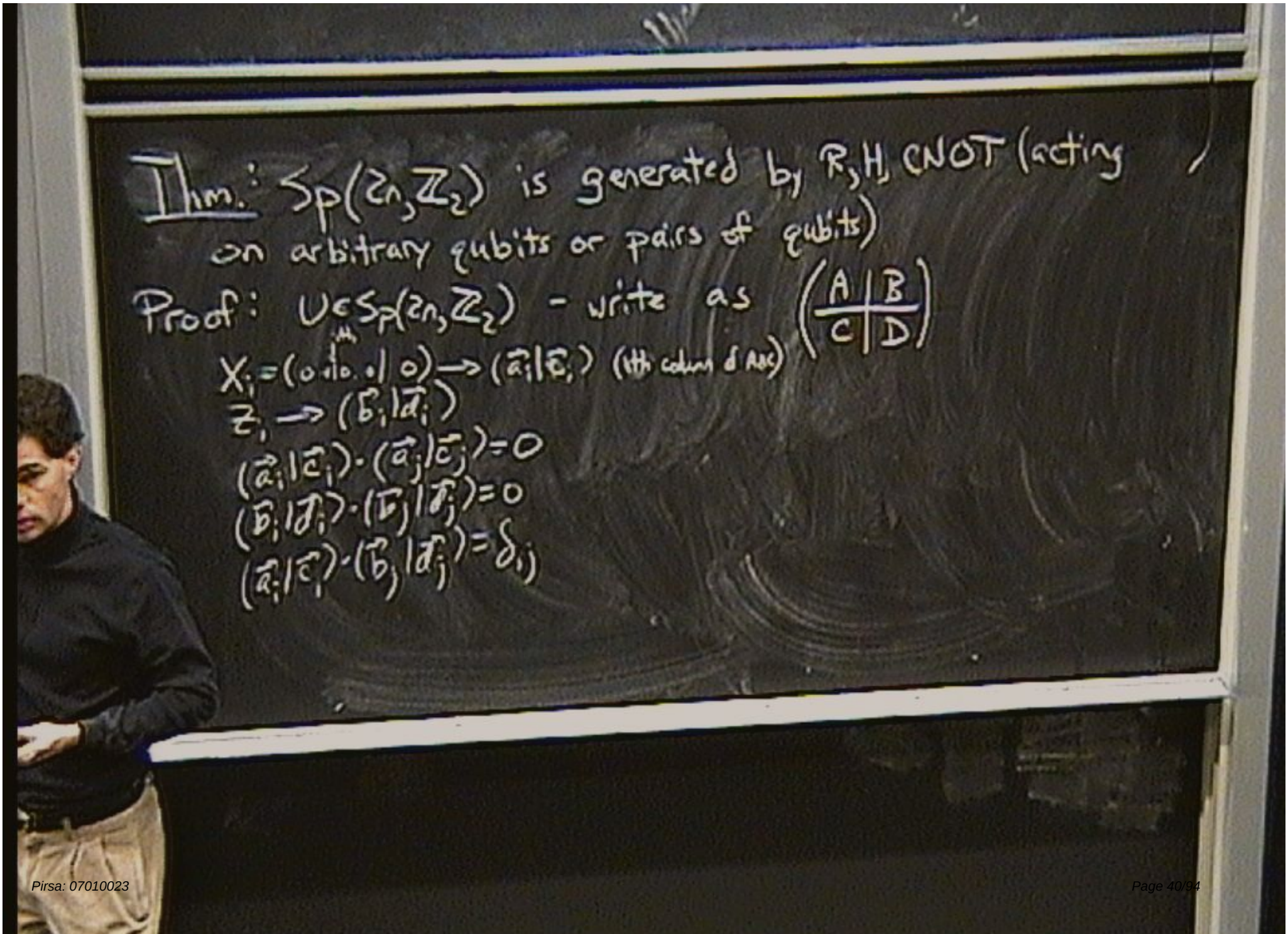
Proof: $U \in Sp(2n, \mathbb{Z}_2)$ - write as $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$

Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by $R, H, CNOT$ (acting on arbitrary qubits or pairs of qubits)

Proof: $U \in Sp(2n, \mathbb{Z}_2)$ - write as $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$

$X_i = (0 \ldots 0 \overset{i}{1} 0 \ldots 0 \,|\, 0) \to (\vec{a}_i | \vec{c}_i)$ (ith column of $A|C$)


Thm.: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting on arbitrary qubits or pairs of qubits)
Proof: $U \in Sp(2n, \mathbb{Z}_2)$ - write as $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$
$X_i = (0 \ldots 0 \ldots 0 \mid 0) \to (\vec{a}_i \mid \vec{c}_i)$
$Z_i \to (\vec{b}_i \mid \vec{d}_i)$
$(\vec{a}_i \mid \vec{c}_i) \cdot (\vec{a}_j \mid \vec{c}_j) = 0$
$(\vec{b}_i \mid \vec{d}_i) \cdot (\vec{b}_j \mid \vec{d}_j) = 0$
$(\vec{a}_i \mid \vec{c}_i) \cdot (\vec{b}_j \mid \vec{d}_j) =$


Thm: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting on arbitrary qubits or pairs of qubits)
Proof: $U \in Sp(2n, \mathbb{Z}_2)$ - write as $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$
$X_i = (0 \ldots 1 \ldots 0 \mid 0) \to (\vec{a}_i \mid \vec{c}_i)$ (ith column of ABCD)
$Z_i \to (\vec{b}_i \mid \vec{d}_i)$
$(\vec{a}_i \mid \vec{c}_i) \cdot (\vec{a}_j \mid \vec{c}_j) = 0$
$(\vec{b}_i \mid \vec{d}_i) \cdot (\vec{b}_j \mid \vec{d}_j) = 0$
$(\vec{a}_i \mid \vec{c}_i) \cdot (\vec{b}_j \mid \vec{d}_j) = \delta_{ij}$

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$

E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$ or $C_n / \{e^{i\theta} I\}$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

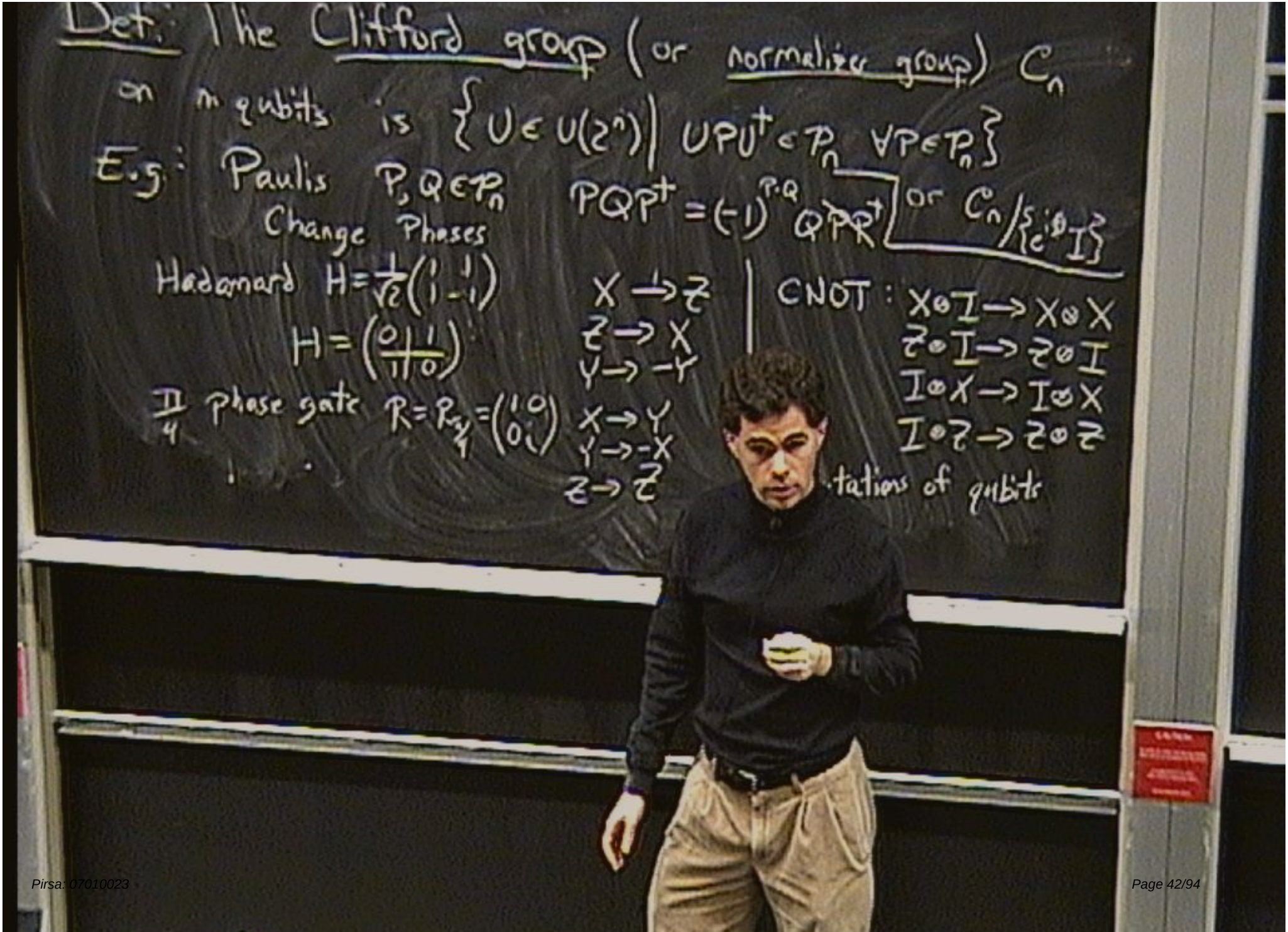
$X \to Z$
$Z \to X$
$Y \to -Y$

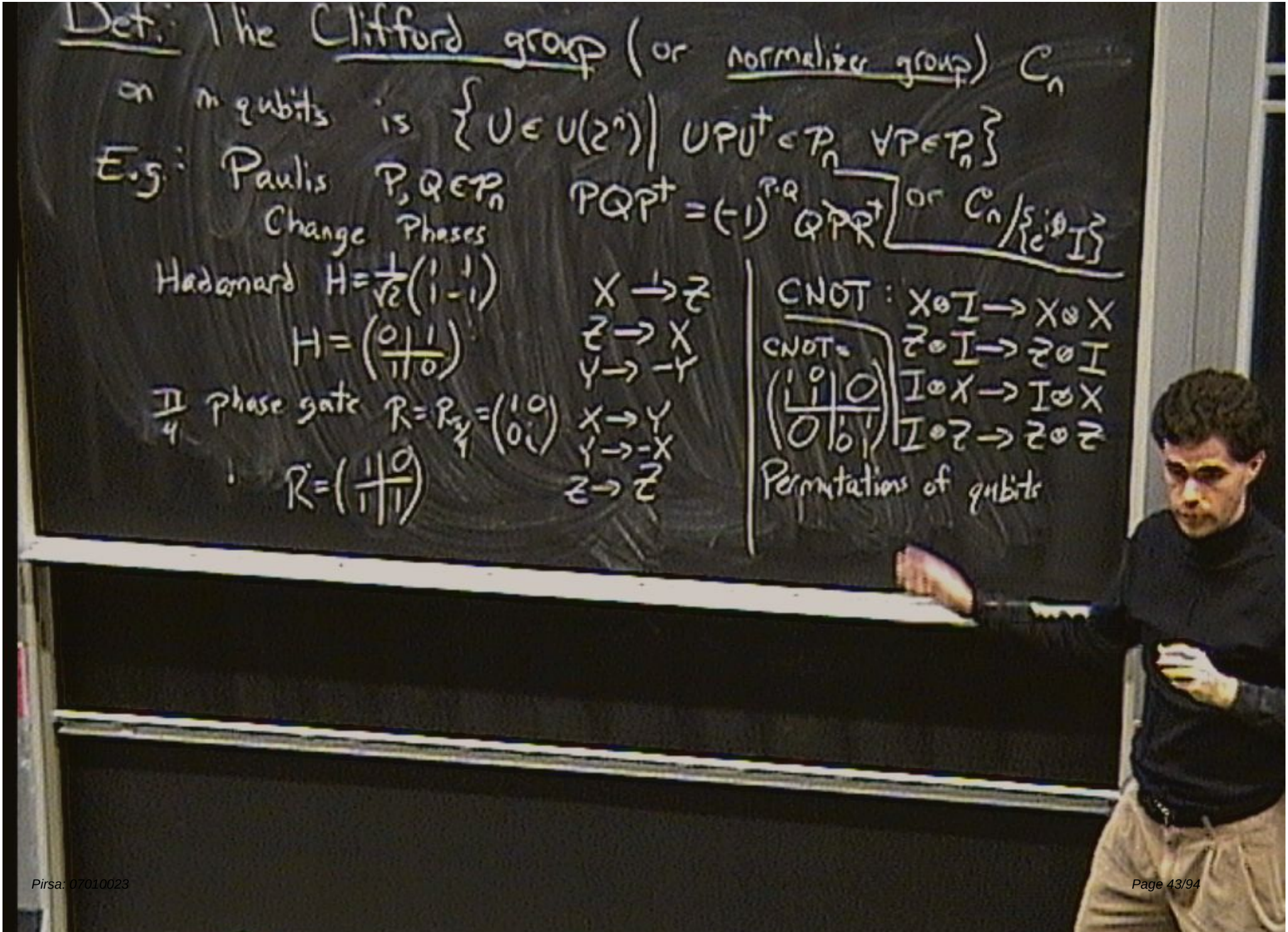
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

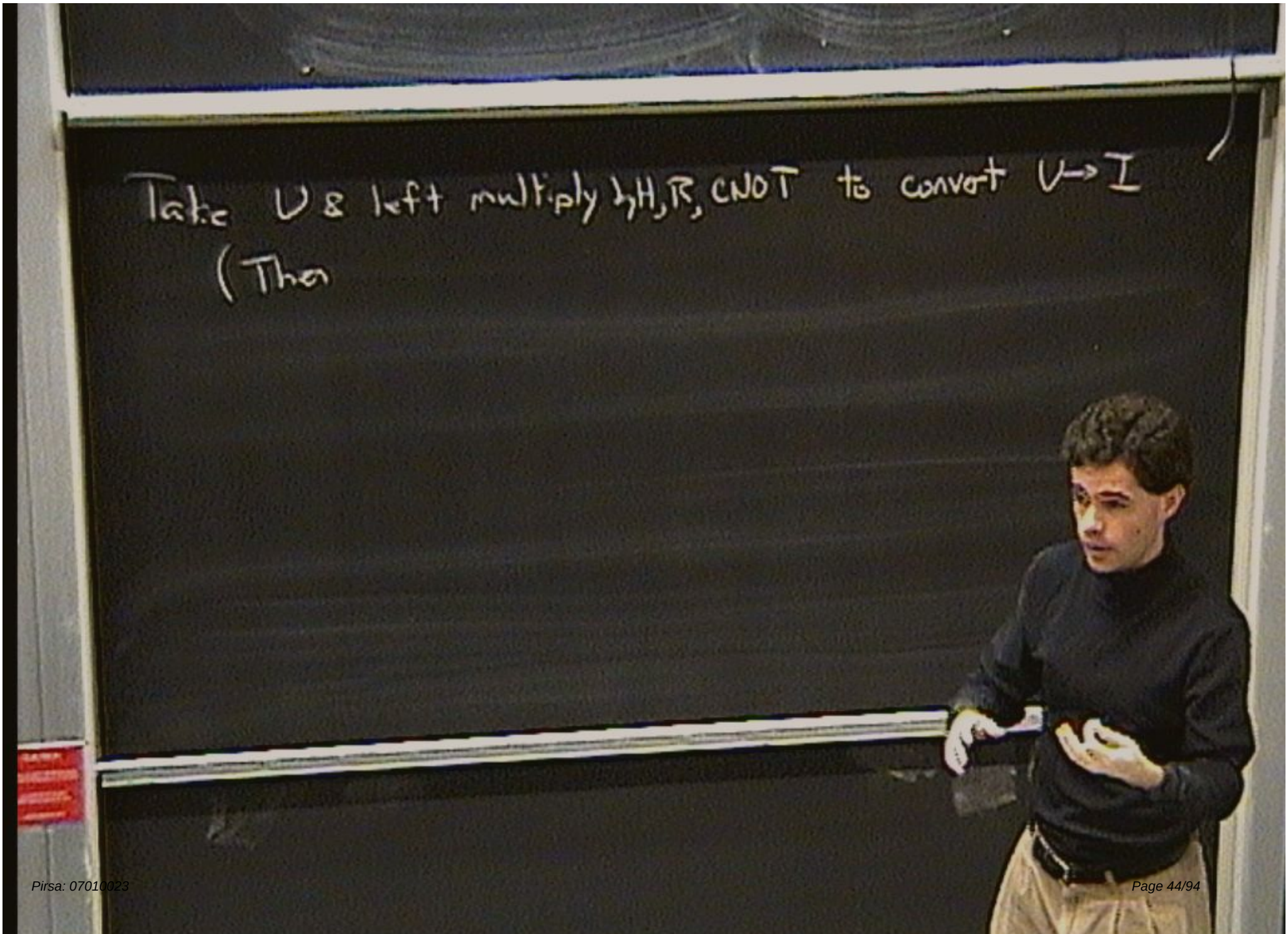
$X \to Y$
$Y \to -X$
$Z \to Z$

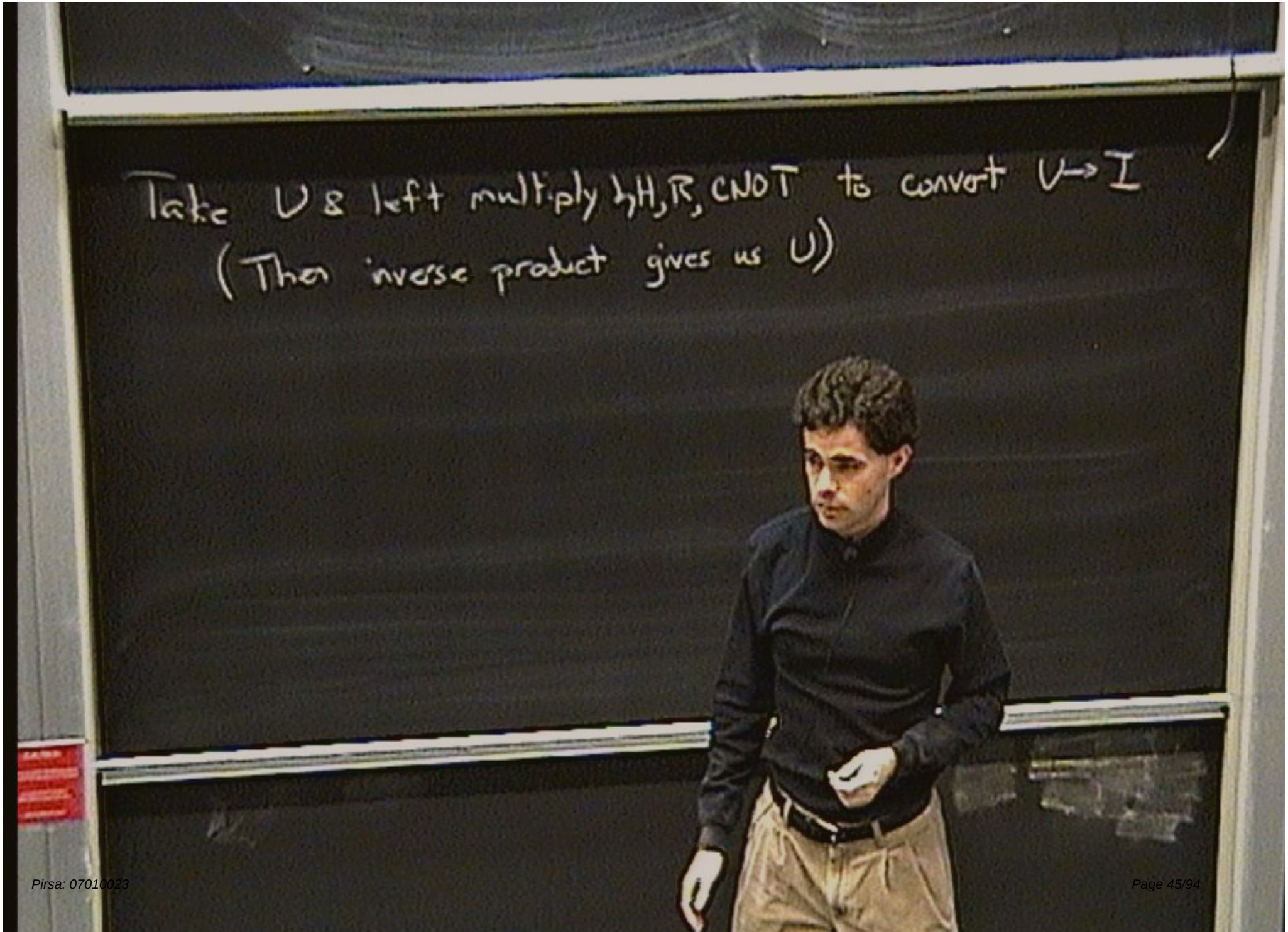
CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$

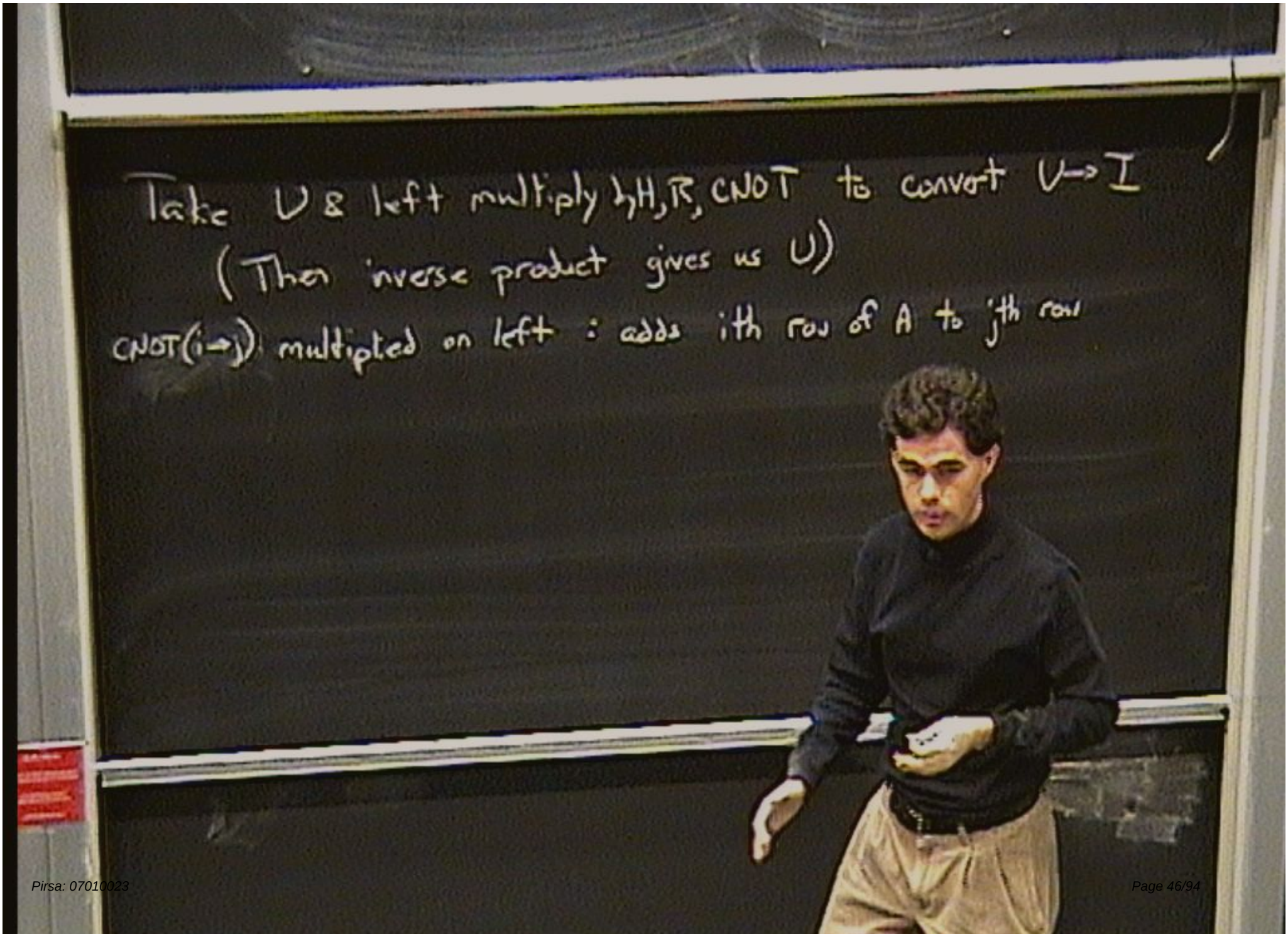
Permutations of qubits


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$
E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$
or $C_n/\{e^{i\theta} I\}$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$X \to Z$
$Z \to X$
$Y \to -Y$
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$X \to Y$
$Y \to -X$
$Z \to Z$
CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$
tations of qubits


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$
E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$
or $C_n/\{e^{i\theta} I\}$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$X \to Z$
$Z \to X$
$Y \to -Y$
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
$X \to Y$
$Y \to -X$
$Z \to Z$
CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$
CNOT $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Permutations of qubits


Take U & left multiply by H, R, CNOT to convert U → I
(Then


Take U & left multiply by H, R, CNOT to convert U → I
(Then inverse product gives us U)


Take U & left multiply by H, T, CNOT to convert U -> I
(Then inverse product gives us U)
CNOT(i->j) multiplied on left : adds ith row of A to jth row

Take U & left multiply by H, T, CNOT to convert $U \to I$

(Then inverse product gives us U)

$\text{CNOT}(i \to j)$ multiplied on left : adds ith row of A to j^{th} row

Using CNOTs & row reduction, convert $A = \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

Take U & left multiply by $H, R, CNOT$ to convert $U \to I$

(Then inverse product gives us U)

$CNOT(i \to j)$ multiplied on left : adds ith row of A to j^{th} row

Using CNOTs & row reduction, convert $A = \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$

E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P,Q} QPP^\dagger$ or $C_n / \{e^{i\theta} I\}$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$X \to Z$
$Z \to X$
$Y \to -Y$

$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$X \to Y$
$Y \to -X$
$Z \to Z$

CNOT: $X \otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$

CNOT $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Permutations of qubits

Take U & left multiply by H, R, CNOT to convert U → I

(Then inverse product gives us U)

CNOT(i→j): multiplied on left : adds [illegible] of A to jth row

Using CNOTs & row reduction, co[illegible] $= \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

R adds ith row of A to [illegible]

Take U & left multiply by H, R, CNOT to convert $U \to I$

(Then inverse product gives us U)

$\text{CNOT}(i \to j)$: multiplied on left : adds ith row of A to j^{th} row

Using CNOTs & row reduction, convert $A = \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

R adds ith row of A to ith row of C

Take U & left multiply by H, R, CNOT to convert $U \to I$

(Then inverse product gives us U)

$\text{CNOT}(i \to j)$: multiplied on left : adds ith row of A to j^{th} row

Using CNOTs & row reduction, convert $A = \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

R adds ith row of A to ith row of C

H switches A/B with C/D

Thm: $Sp(2n, \mathbb{Z}_2)$ is generated by R, H, CNOT (acting on arbitrary qubits or pairs of qubits)

Proof: $U \in Sp(2n, \mathbb{Z}_2)$ - write as $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$

$X_i = (0 \ldots 0 \overset{i^{th}}{1} 0 \ldots 0 \,|\, 0 \ldots 0) \to (\vec{a}_i | \vec{c}_i)$ (i^{th} column of $A|C$)

$Z_i \to (\vec{b}_i | \vec{d}_i)$

$(\vec{a}_i | \vec{c}_i) \cdot (\vec{a}_j | \vec{c}_j) = 0$

$(\vec{b}_i | \vec{d}_i) \cdot (\vec{b}_j | \vec{d}_j) = 0$

$(\vec{a}_i | \vec{c}_i) \cdot (\vec{b}_j | \vec{d}_j) = \delta_{ij}$

Take U & left multiply by H, R, CNOT to convert $U \to I$

(Then inverse product gives us U)

Take U & left multiply by $H, R, CNOT$ to convert $U \to I$

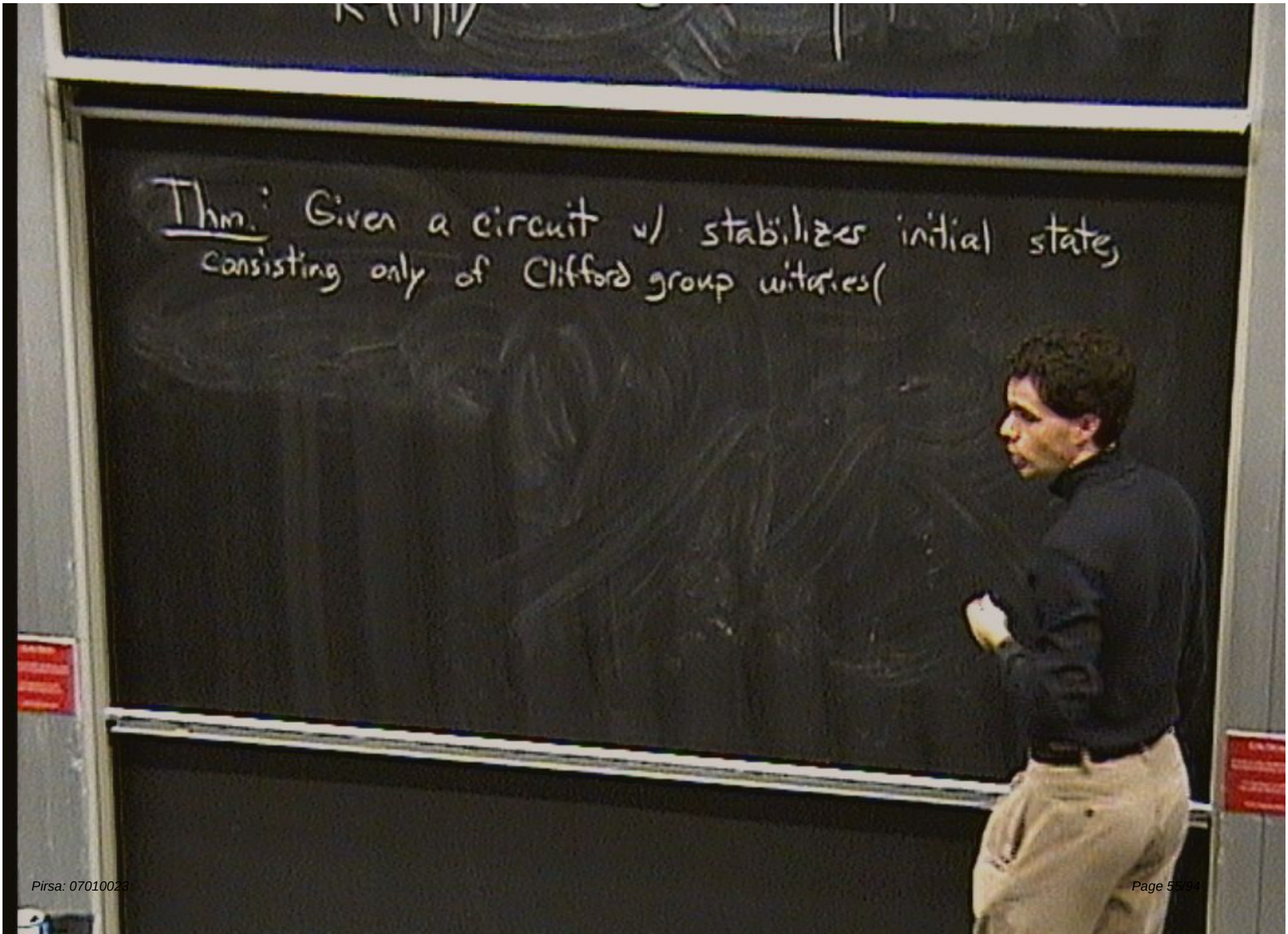
(Then inverse product gives us U)

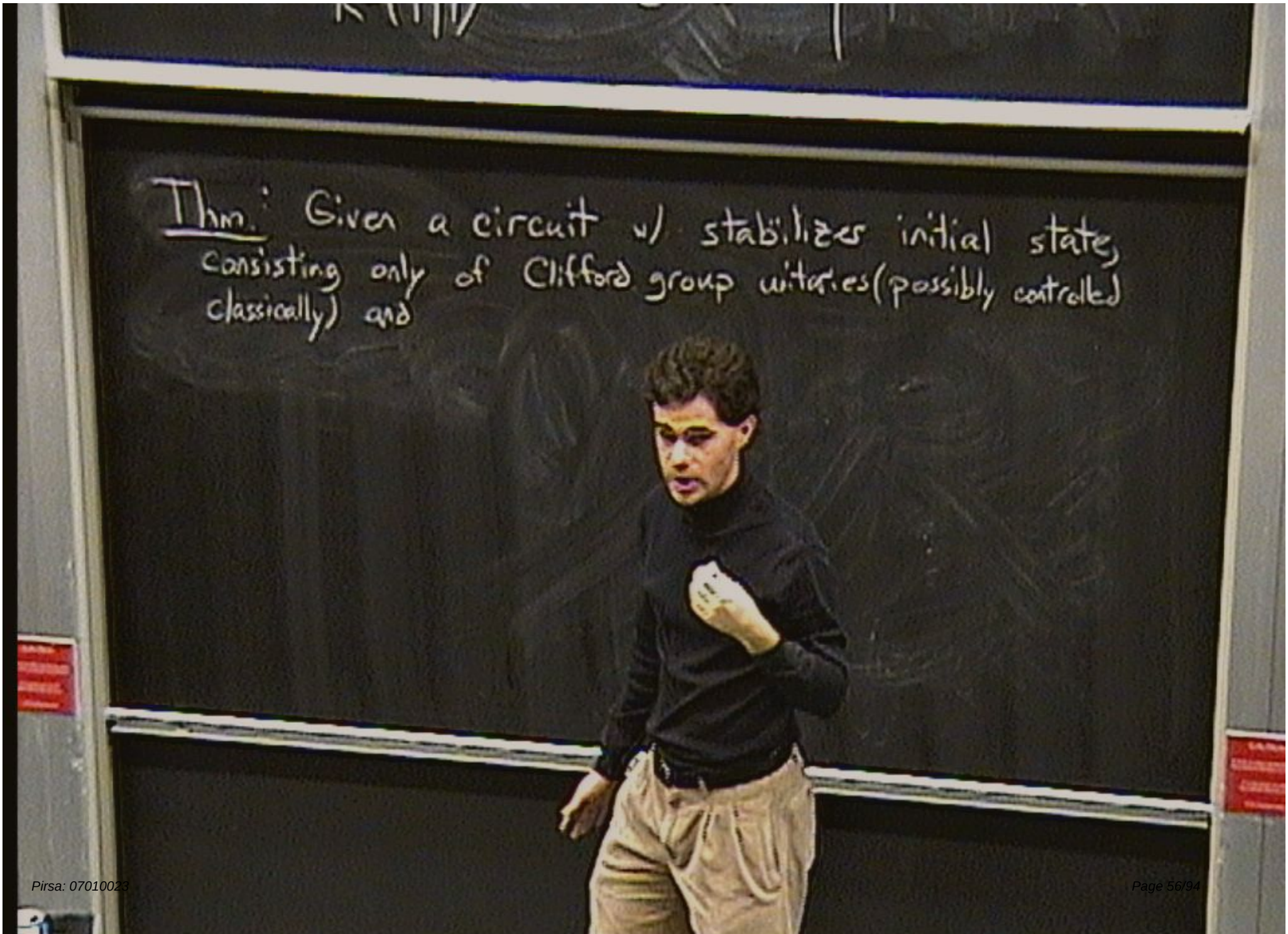
$CNOT(i \to j)$: multiplied on left : adds i^{th} row of A to j^{th} row

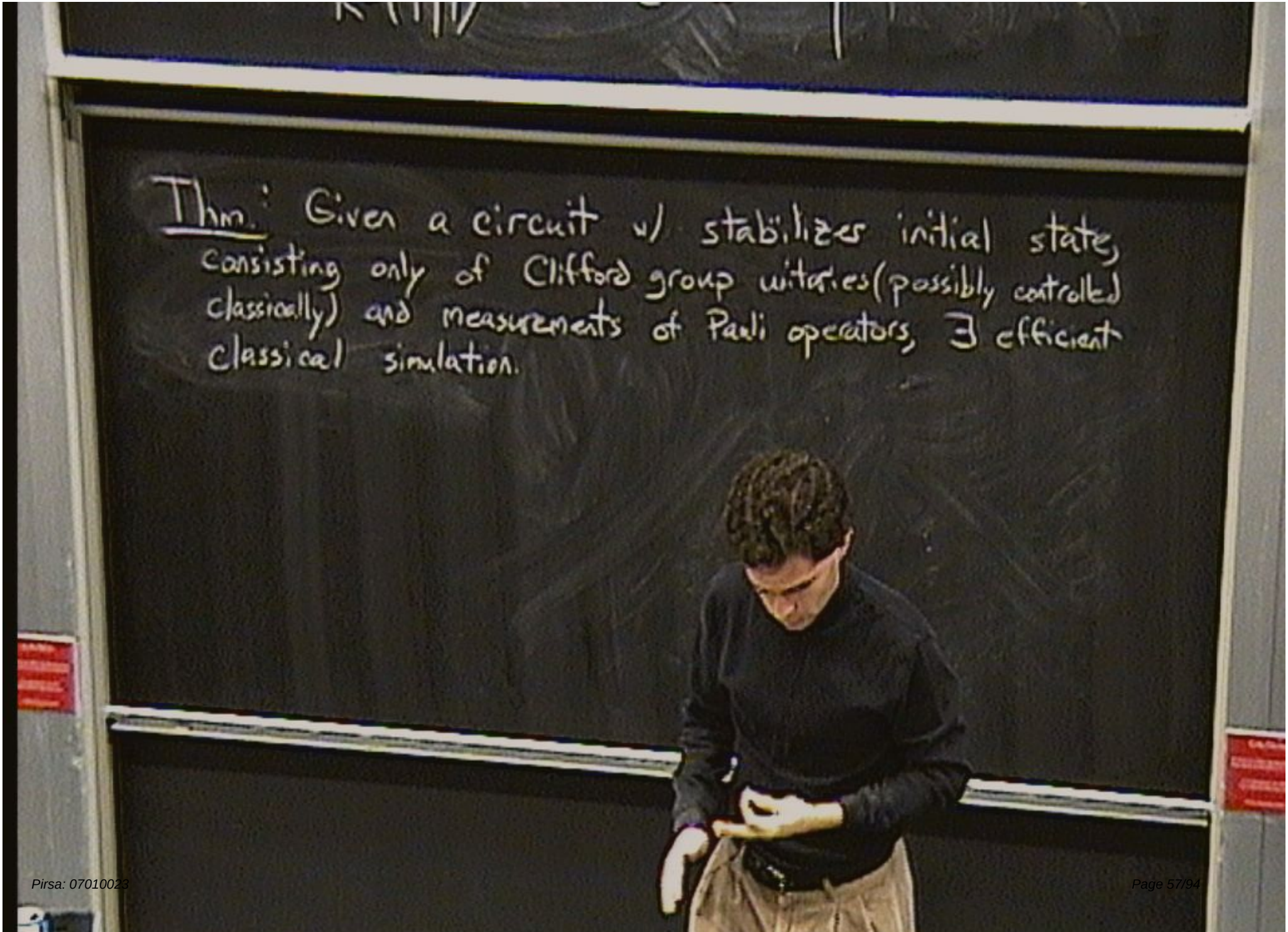
Using CNOTs & row reduction, convert $A = \left(\begin{array}{c|c} I & A' \\ \hline 0 & 0 \end{array}\right)$

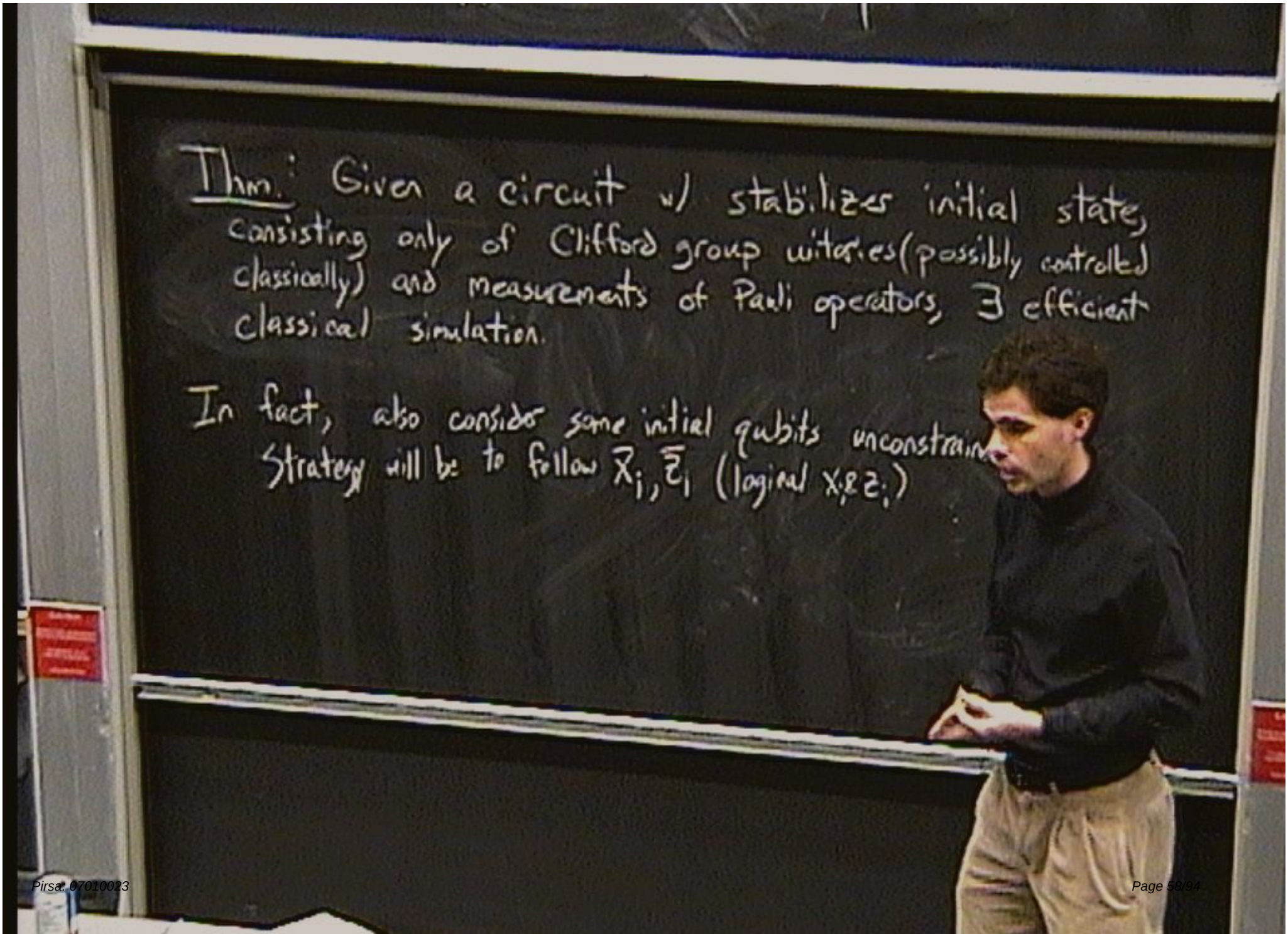
R adds i^{th} row of A to i^{th} row of C

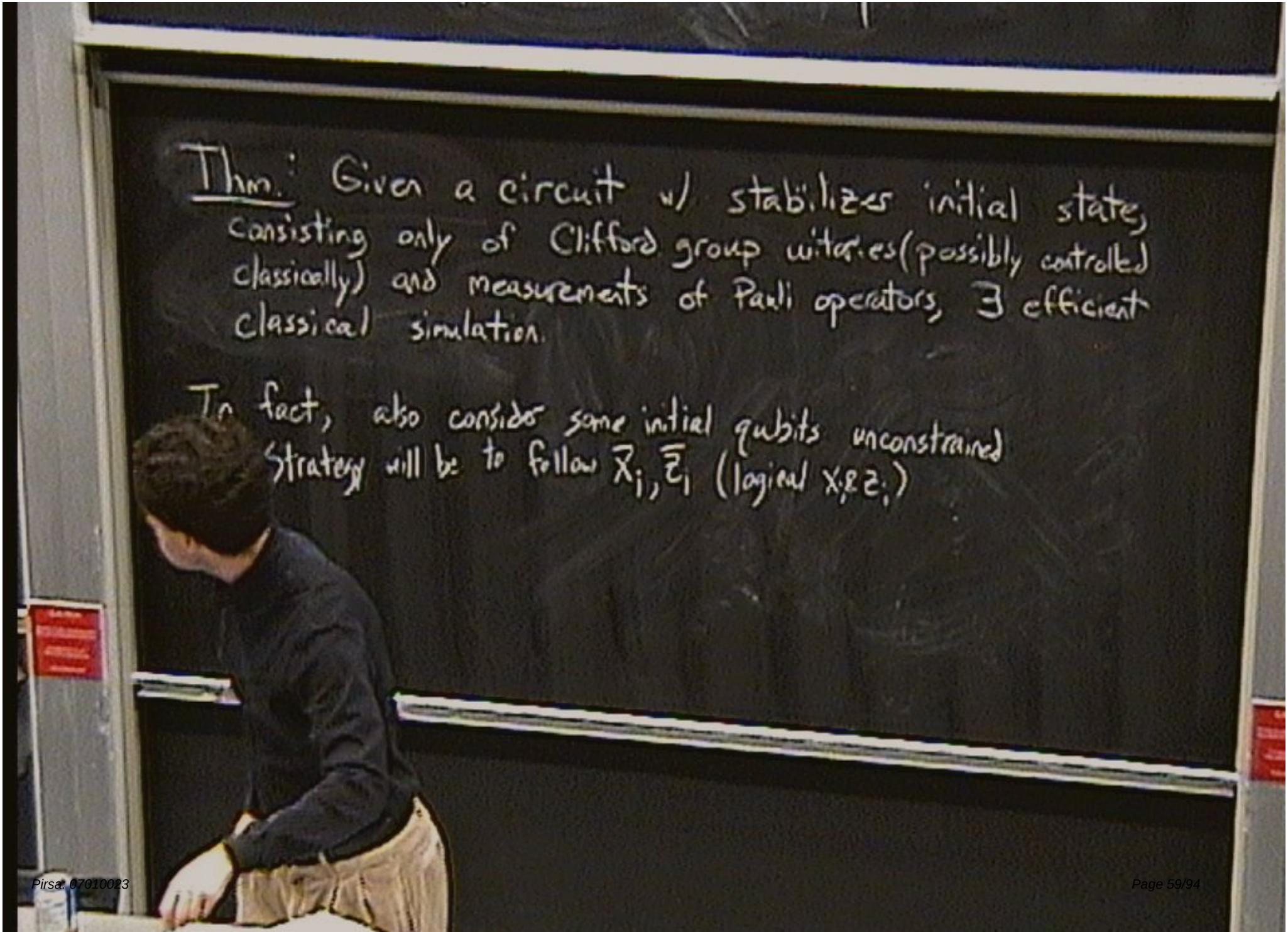
H switches A/B with C/D

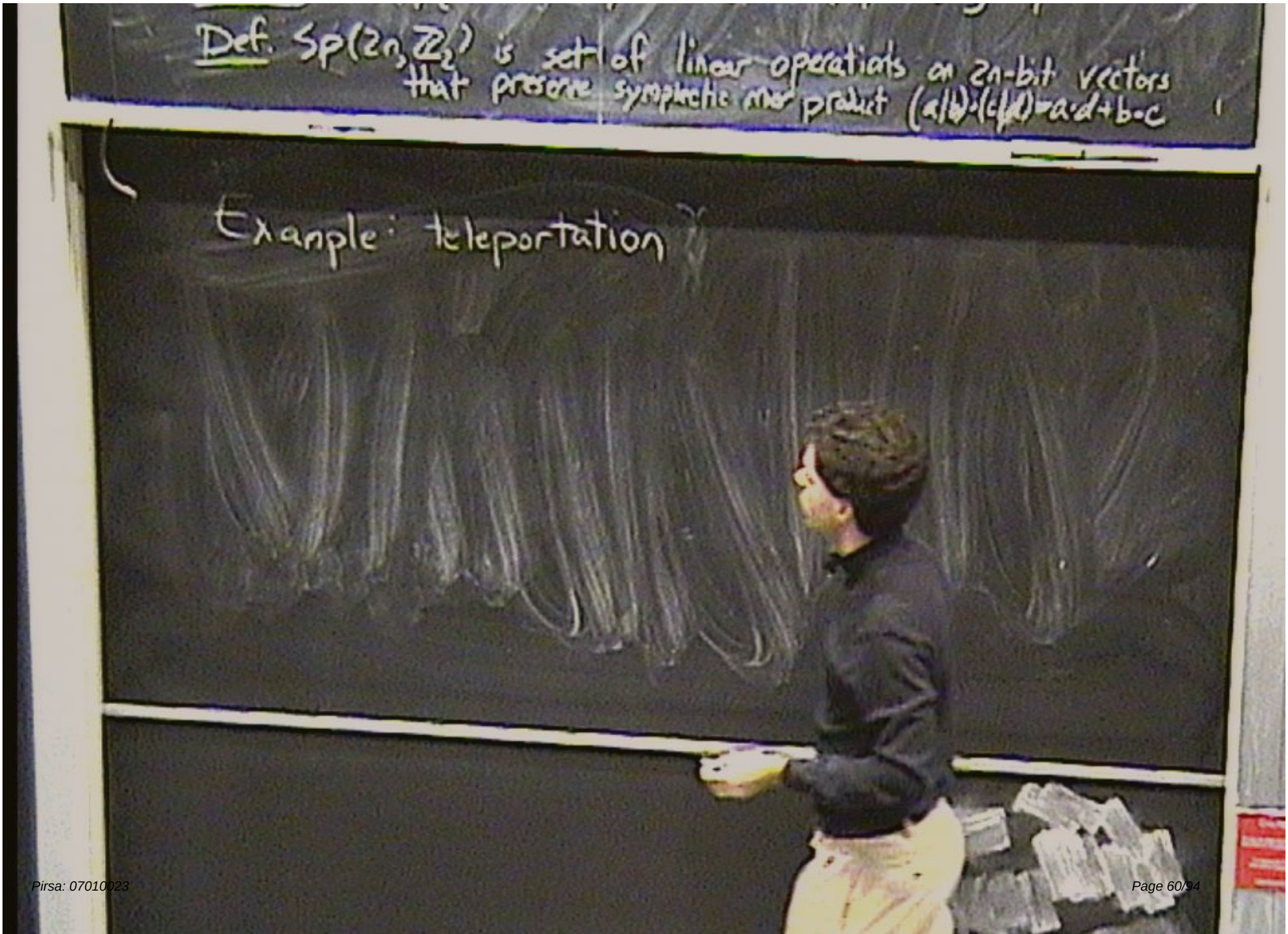

Thm: Given a circuit w/ stabilizer initial state,
consisting only of Clifford group unitaries(


Thm: Given a circuit w/ stabilizer initial state, consisting only of Clifford group unitaries (possibly controlled classically) and


Thm: Given a circuit w/ stabilizer initial state, consisting only of Clifford group unitaries (possibly controlled classically) and measurements of Pauli operators, ∃ efficient classical simulation.


Thm: Given a circuit w/ stabilizes initial state, consisting only of Clifford group unitaries (possibly controlled classically) and measurements of Pauli operators, ∃ efficient classical simulation.
In fact, also consider some initial qubits unconstrain
Strategy will be to follow $\bar{X}_i, \bar{Z}_i$ (logical X_i & Z_i)


Thm: Given a circuit w/ stabilizes initial state, consisting only of Clifford group unitaries (possibly controlled classically) and measurements of Pauli operators, ∃ efficient classical simulation.
In fact, also consider some initial qubits unconstrained
Strategy will be to follow $\bar{X}_i, \bar{Z}_i$ (logical X_i & Z_i)


Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on 2n-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$
Example: teleportation

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\overline{1}$ $\overline{X}_2$ $\overline{X}_2$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer

Z_a	Z	I	I
	I	X	X
	I	Z	Z

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer

Z_3	I	I	I
Z_2	I	I	I
X_3	X	I	I
X_2	I	X	I
I	I	I	I

CNOT

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer

	II	XX	XX
	XI	I	I
	ZI	I	I

CNOT →

IXX

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizers

I	X	X
I	Z	Z
X	I	I
Z	I	I

CNOT →

I	X	X
I	Z	Z
X	X	I
Z	Z	I

$\frac{\pi}{4}$ phase gate $R = R_z(\pi/2)$ $\quad X \to -X$, $Y \to -Y$, $Z \to Z$

$R = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

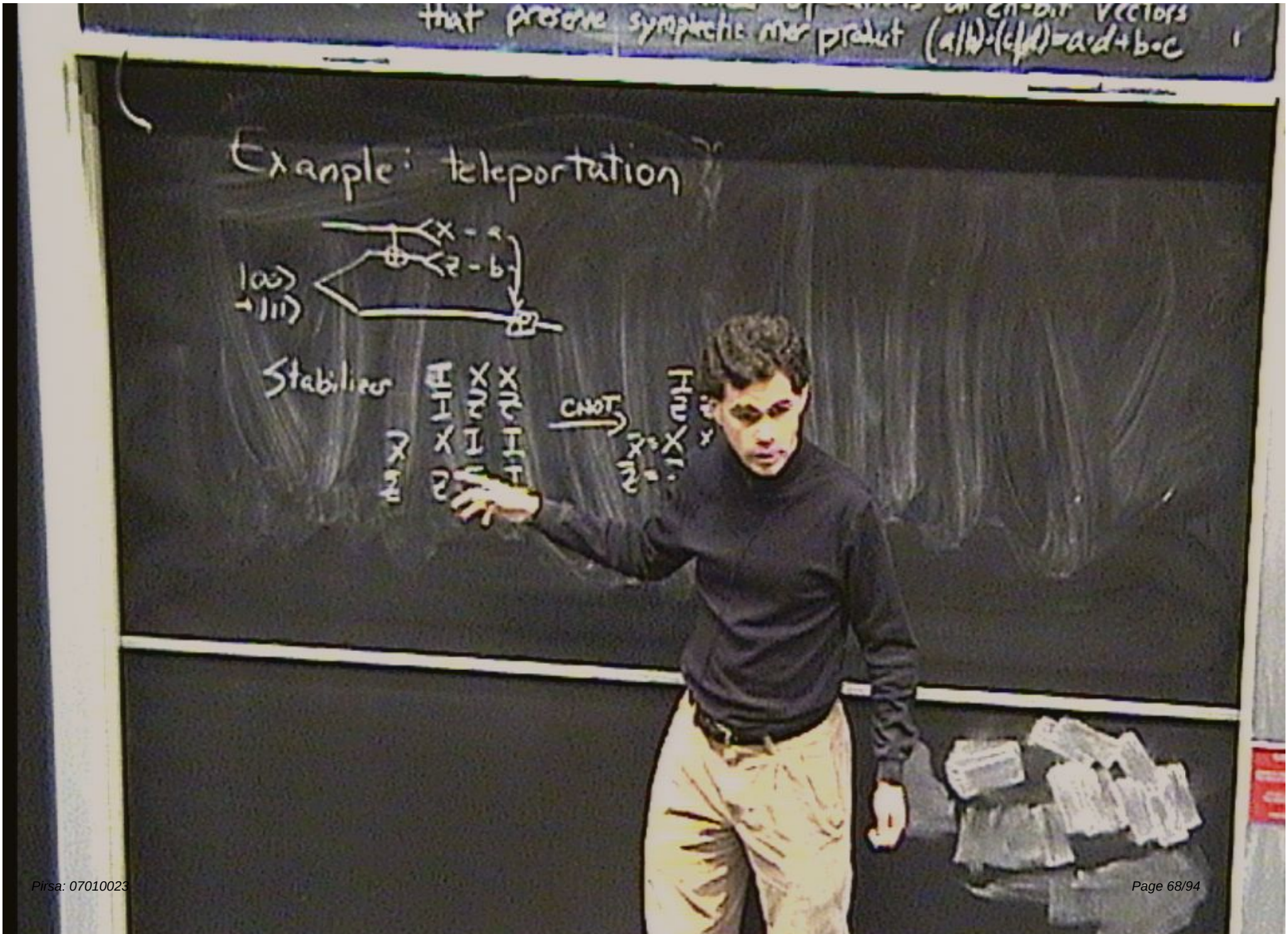
Permutations of qubits

Thm: Given a circuit w/ stabilizer initial state, consisting only of Clifford group unitaries (possibly controlled classically) and measurements of Pauli operators, $\exists$ efficient classical simulation.

In fact, also consider some initial qubits unconstrained

Strategy will be to follow $\bar{X}_i, \bar{Z}_i$ (logical X_i & Z_i)

Simulate Cliffords by following transformations of stabilizer, $\bar{X}_i, \bar{Z}_i$ ✓

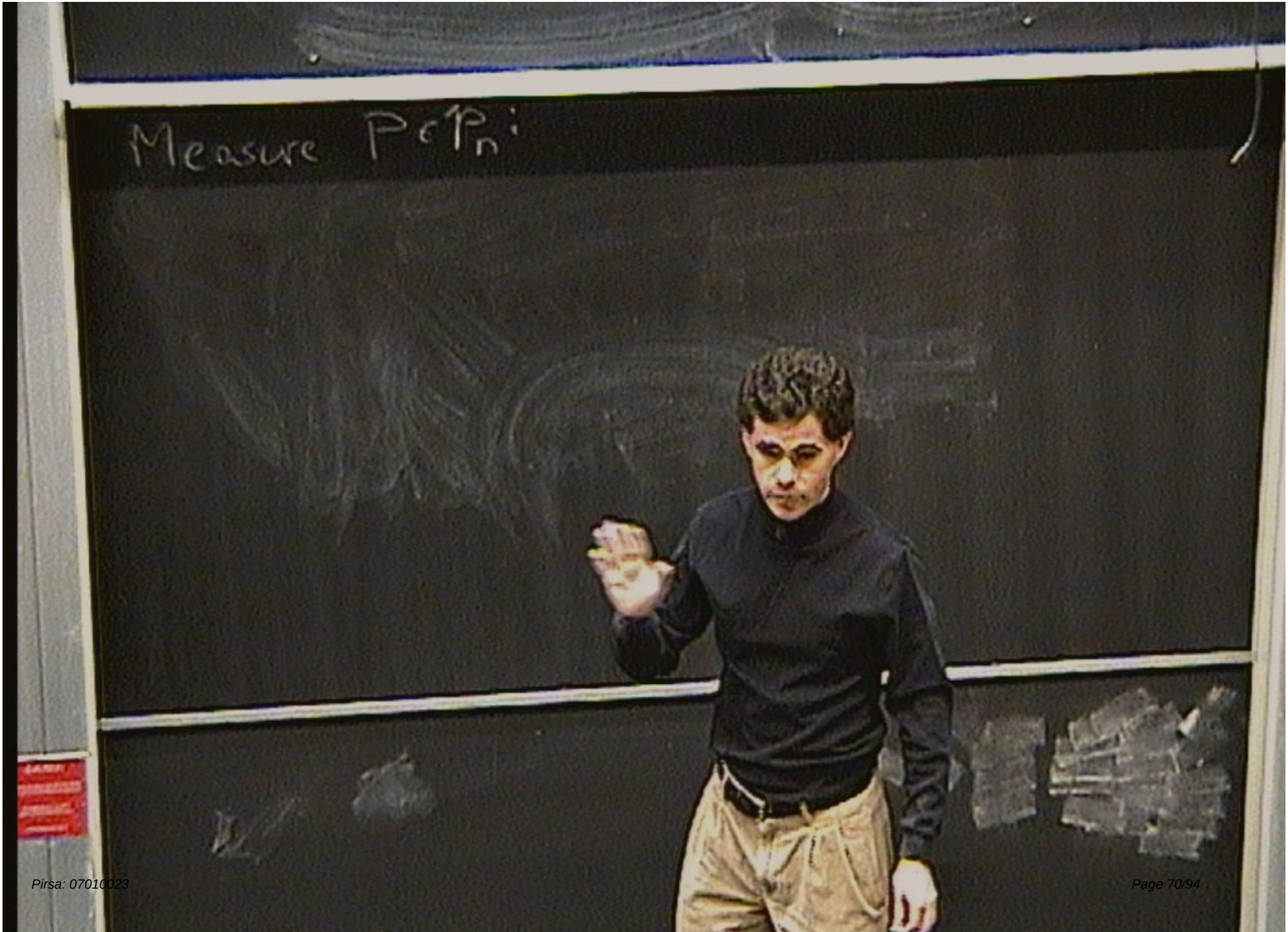

that preserve symplectic inner product
Example: teleportation
Stabilizer
CNOT

that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

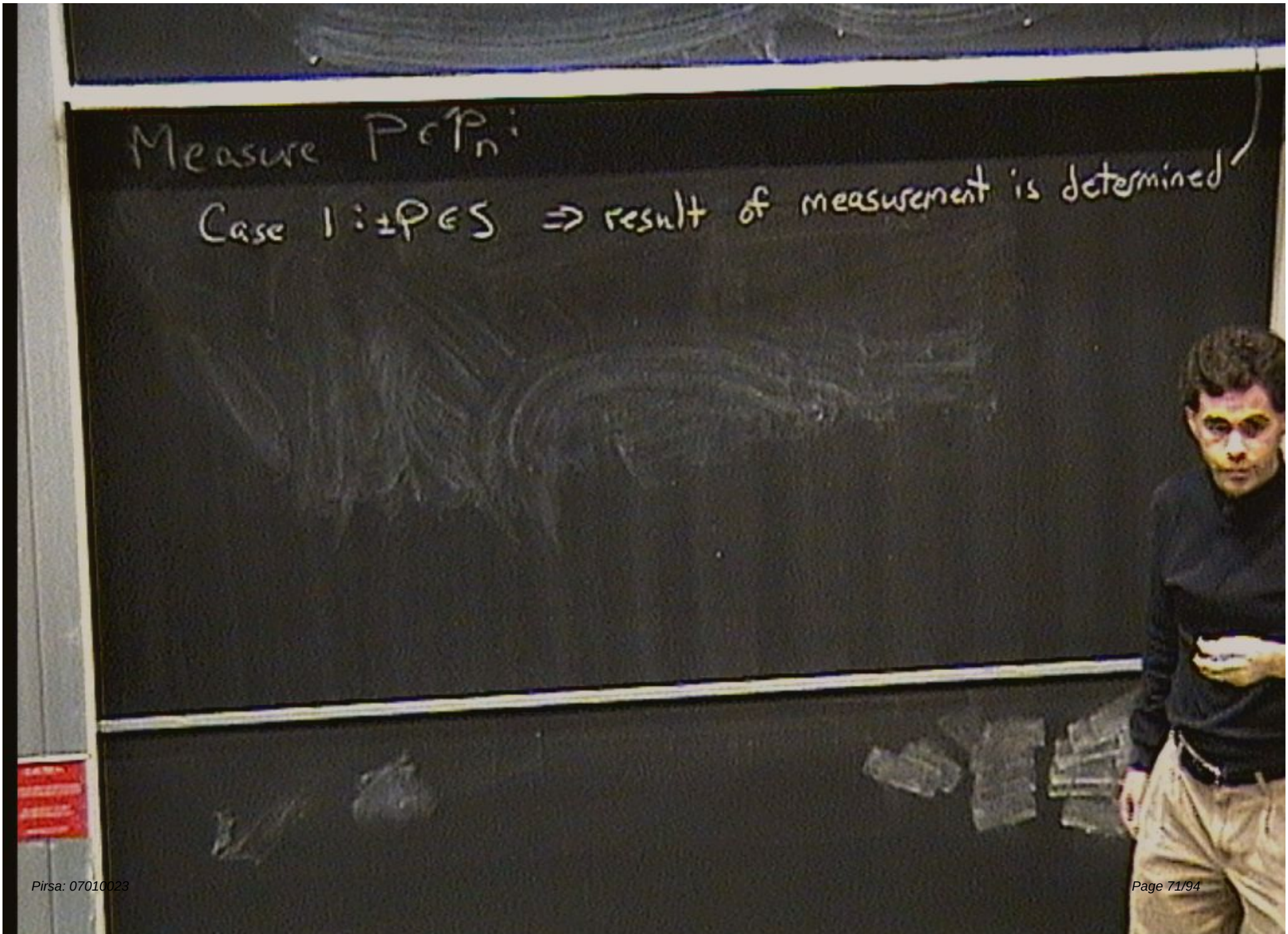
Stabilizer

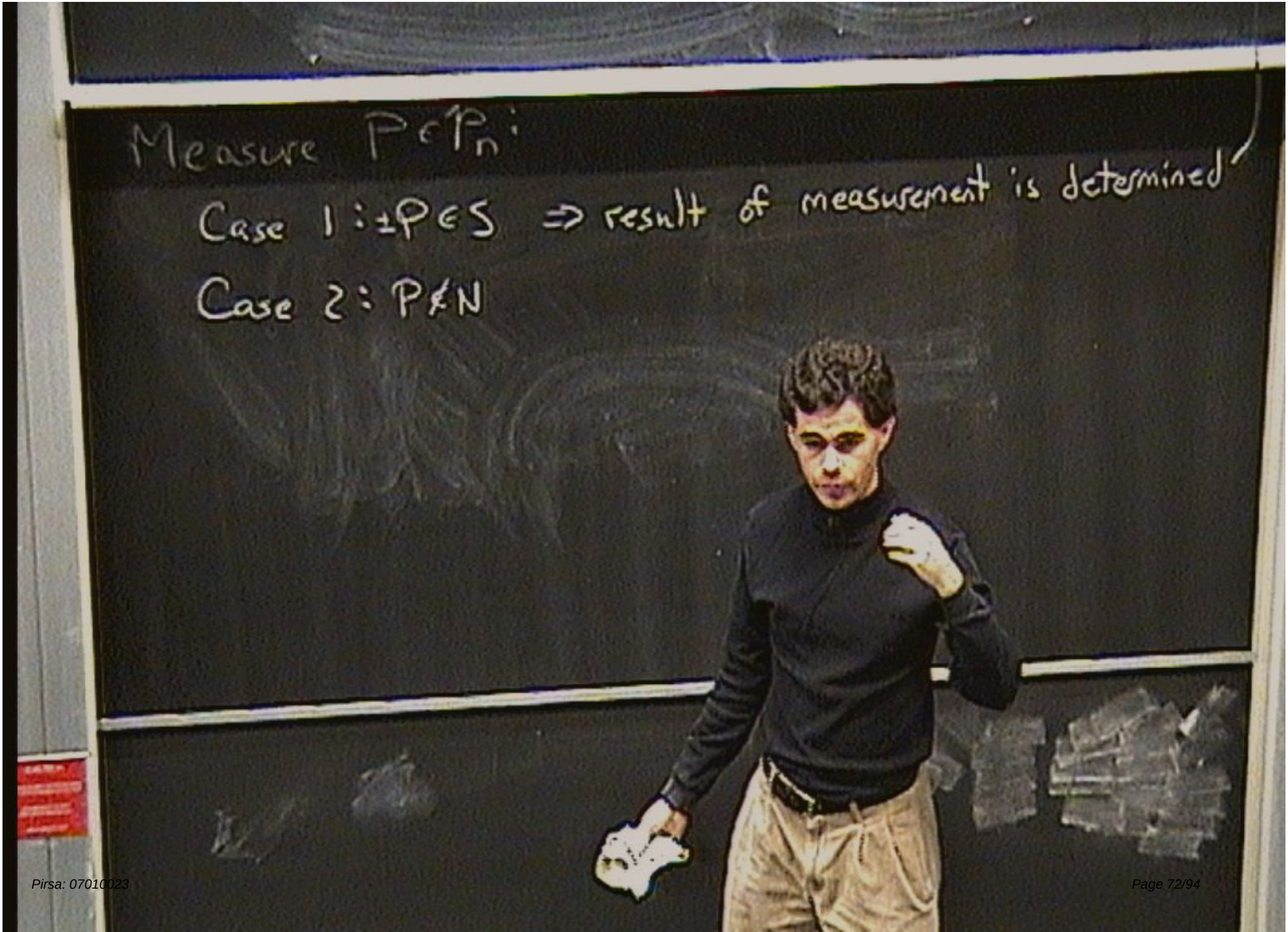
$$\begin{matrix} I & X & X \\ Z & I & I \\ I & Z & I \end{matrix} \xrightarrow{\text{CNOT}} \begin{matrix} I & X & X \\ Z & I & I \\ I & Z & Z \end{matrix}$$

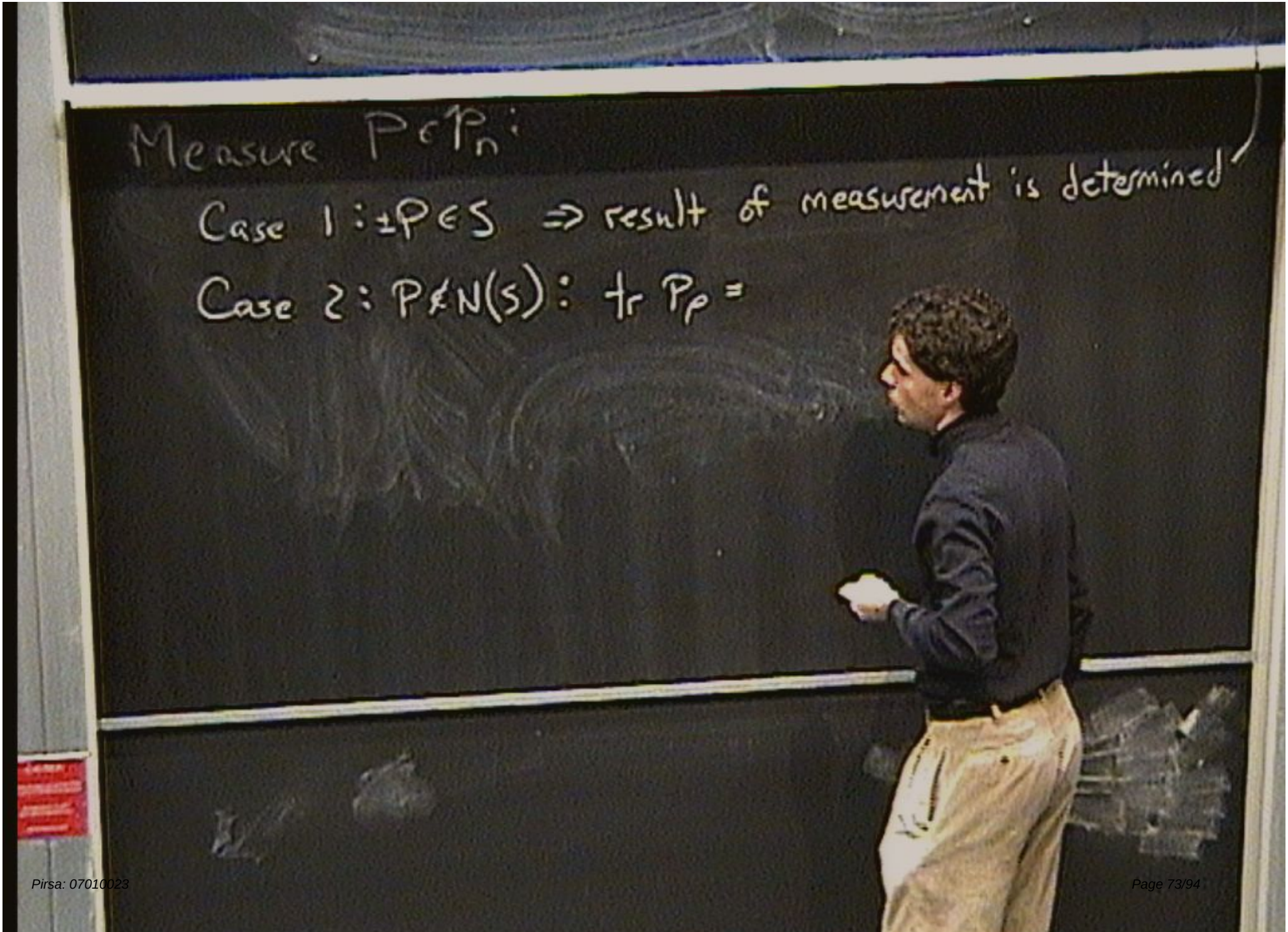

Measure PcPn

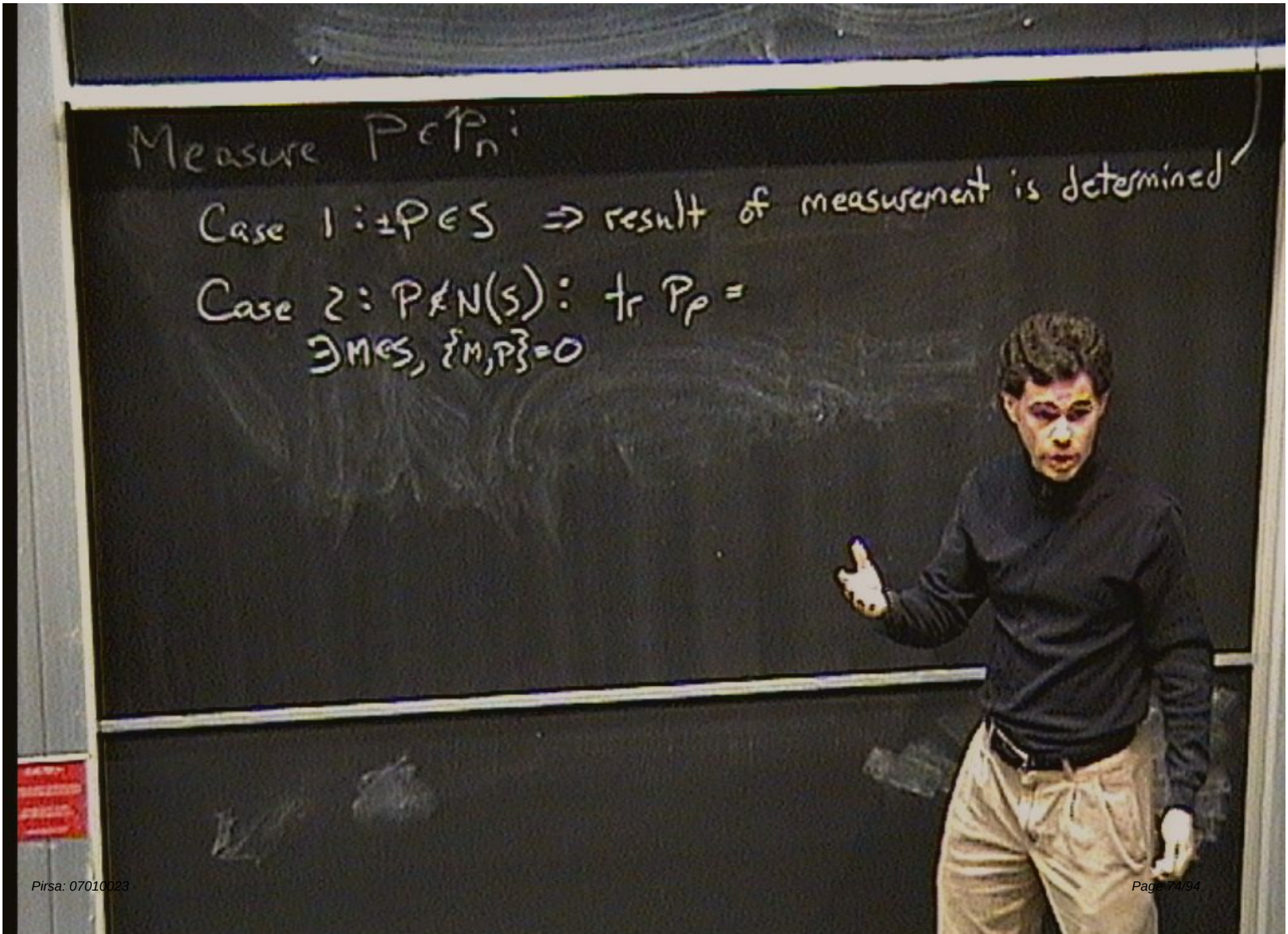
Measure $P \in P_n$:

Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined




Measure P∈Pn:
Case 1: ±P∈S ⇒ result of measurement is determined
Case 2: P∉N


Measure $P \in P_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\pm \operatorname{tr} P_P =$

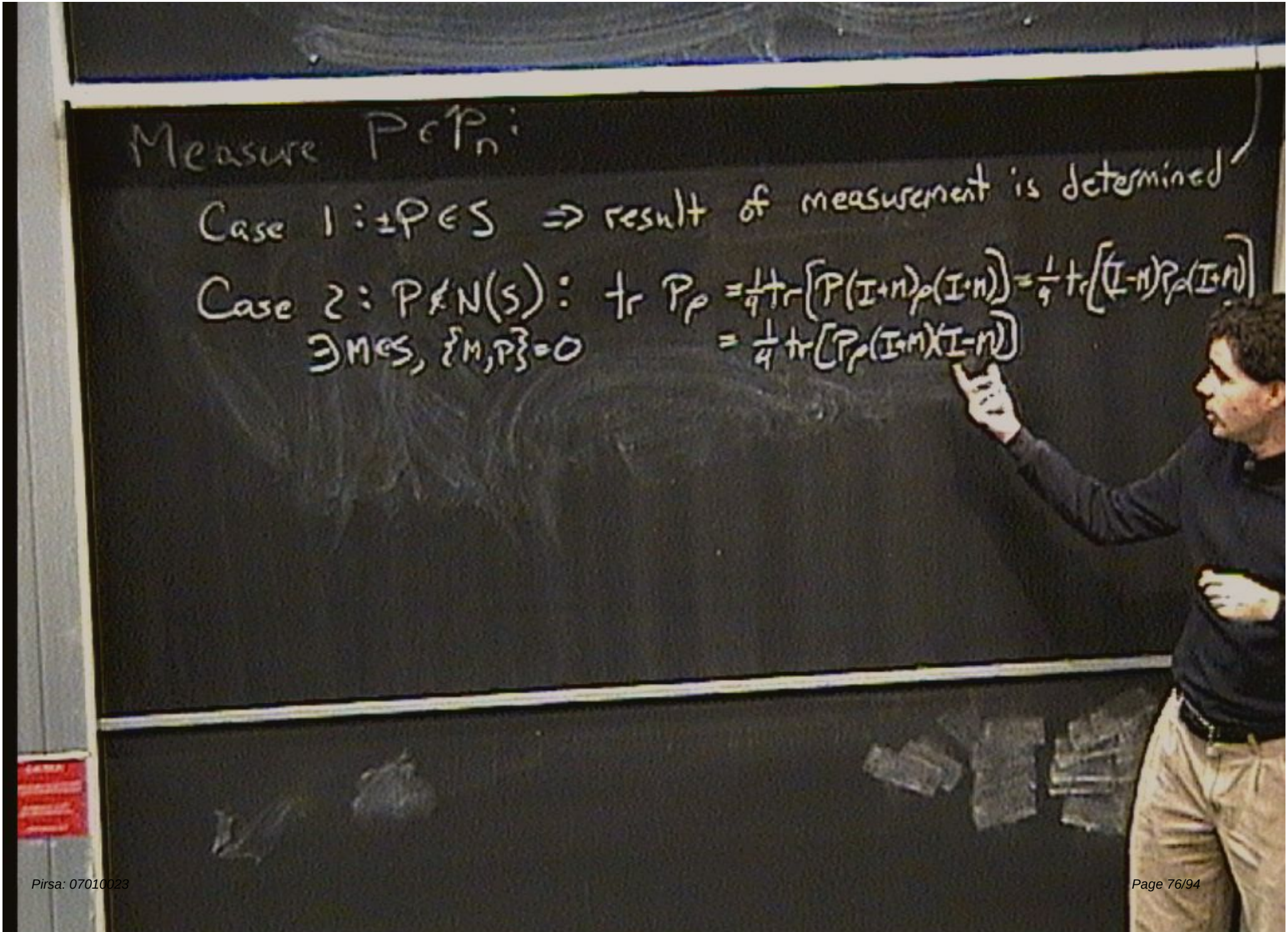

Measure $P \in \mathcal{P}_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\pm \mathrm{tr}\, P_P =$
$\exists M \in S, \{M, P\} = 0$

Measure $P \in \mathcal{P}_n$:

Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined

Case 2: $P \notin N(S)$: $\mathrm{tr}\, P\rho = \frac{1}{q}\mathrm{tr}\left[P(I+n)\rho(I+n)\right]$

$\exists M \in S,\ \{M, P\} = 0$


Measure $P \in \mathcal{P}_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M, P\} = 0$
$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}[P(I+M)\rho(I+M)] = \frac{1}{4}\mathrm{tr}[(I-M)P\rho(I+M)]$
$= \frac{1}{4}\mathrm{tr}[P\rho(I+M)(I-M)]$

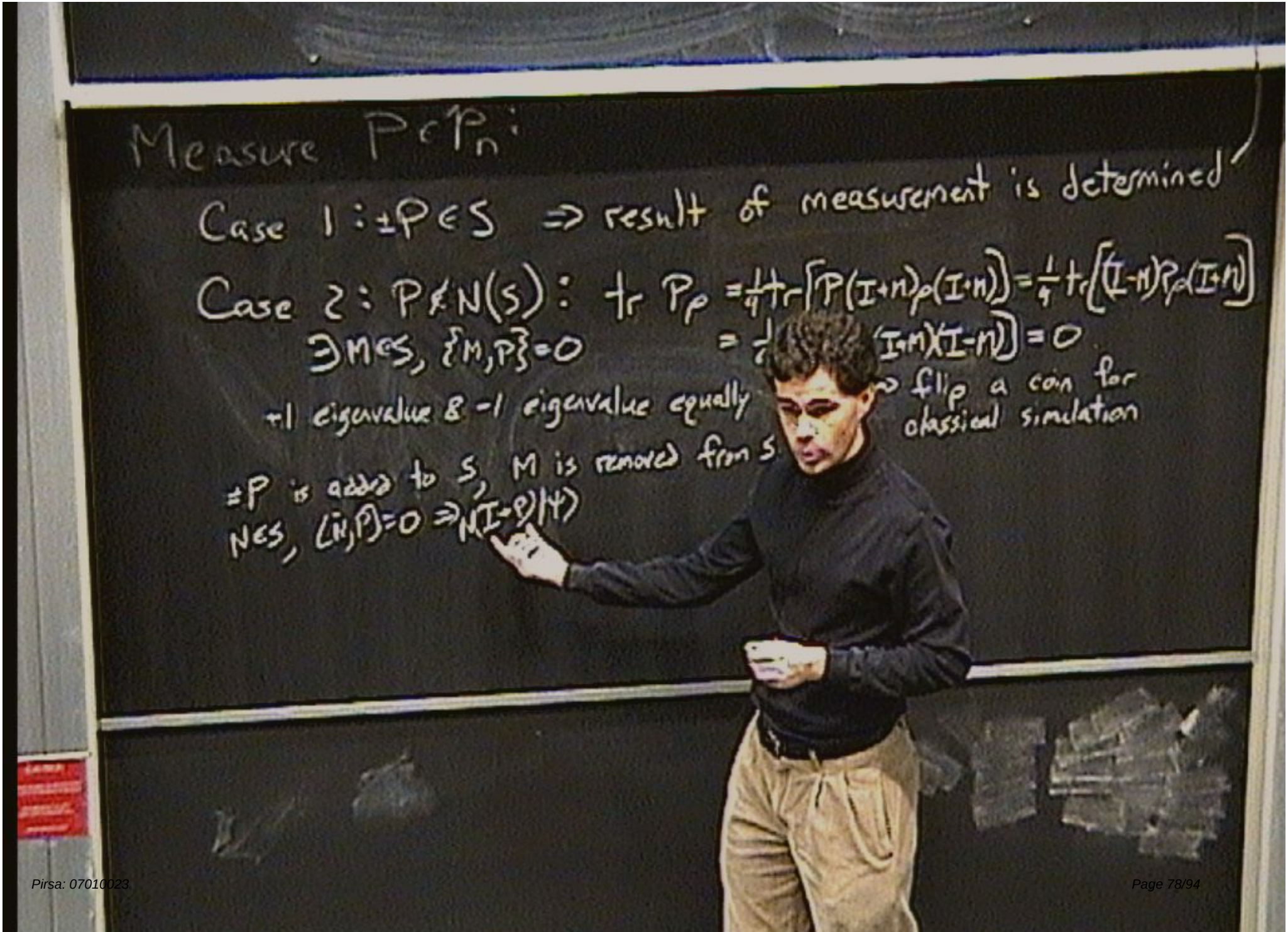
Measure $P \in \mathcal{P}_n$:

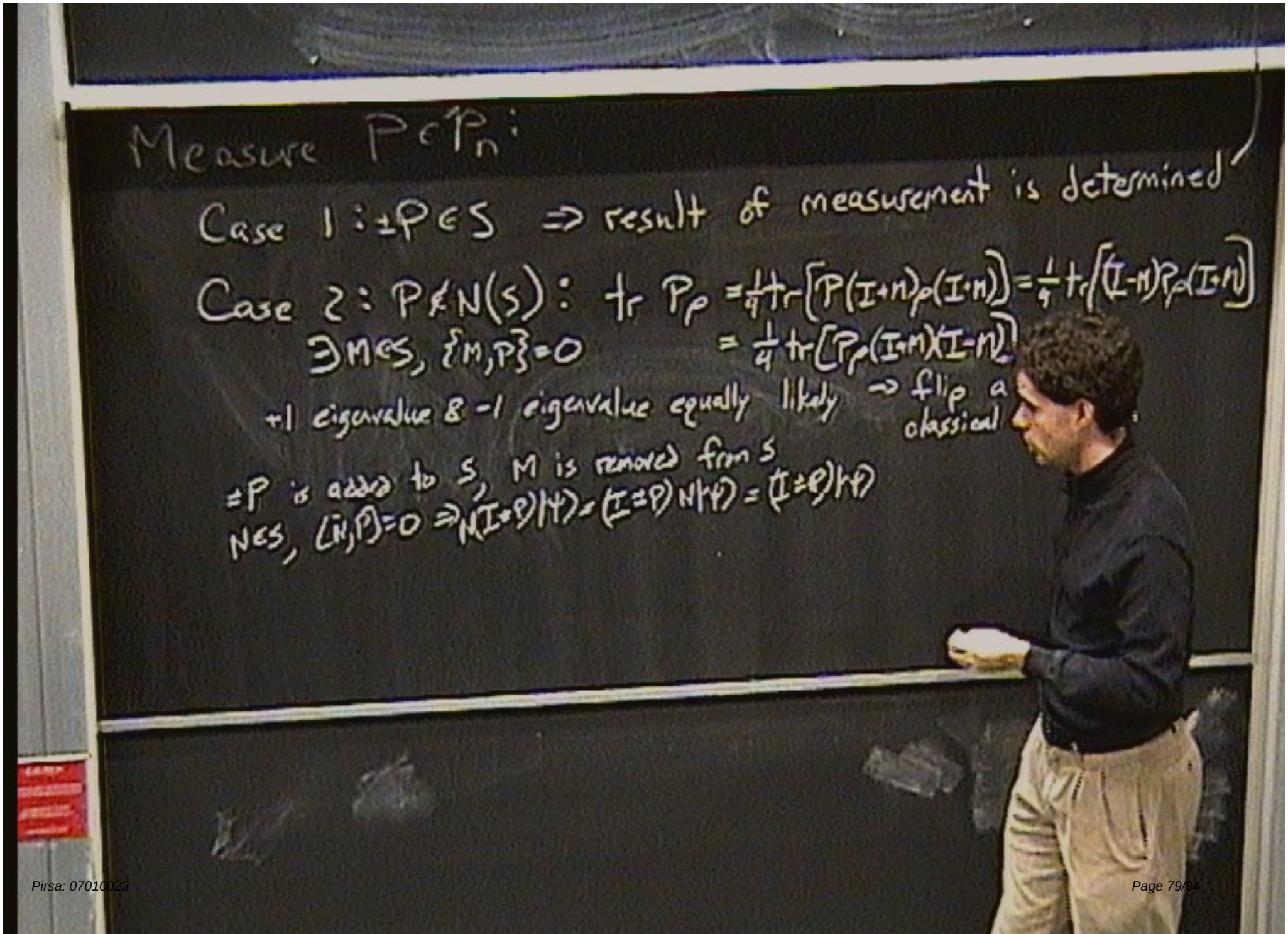
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined

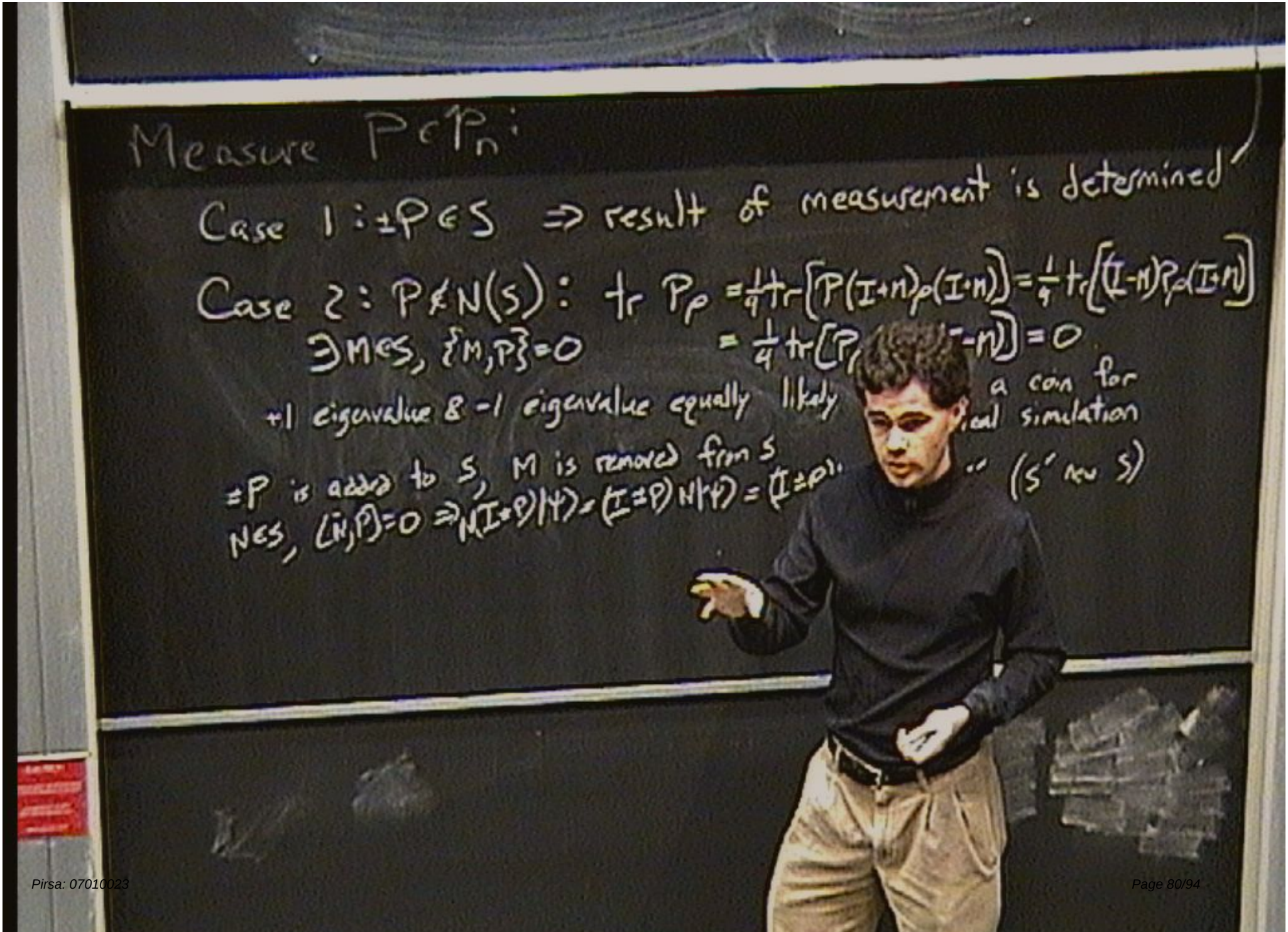
Case 2: $P \notin N(S)$: $\exists M \in S,\ \{M, P\} = 0$

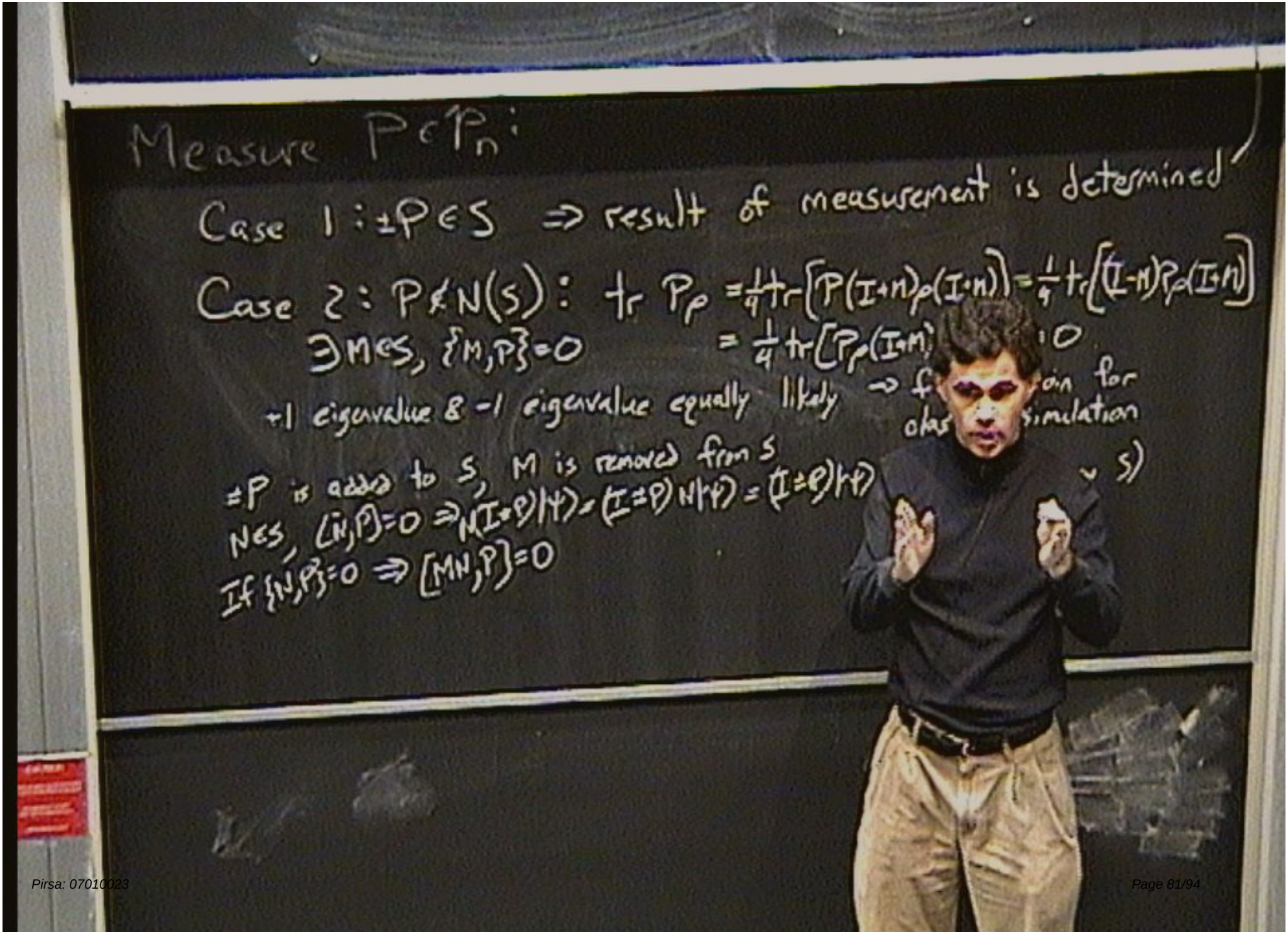
$$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}\left[P(I+M)\rho(I+M)\right] = \frac{1}{4}\mathrm{tr}\left[(I-M)P\rho(I+M)\right]$$
$$= \frac{1}{4}\mathrm{tr}\left[P\rho(I+M)(I-M)\right] = 0$$

$+1$ eigenvalue & -1 eigenvalue equally likely $\Rightarrow$ flip a coin for classical simulation


Measure $P \in P_n$:
Case 1: $\pm P \in S$ ⇒ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$
± 1 eigenvalue & -1 eigenvalue equally
$\pm P$ is added to S, M is removed from S
$N \in S, [N,P]=0 \Rightarrow N(I-P)|\psi\rangle$
$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}[P(I+n)\rho(I+n)] = \frac{1}{4}\mathrm{tr}[(I-n)P\rho(I+n)]$
$= \frac{1}{2}$ (I+n)(I-n)] = 0
⇒ flip a coin for classical simulation


Measure $P \in \mathcal{P}_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$
$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}[P(I+n)\rho(I+n)] = \frac{1}{4}\mathrm{tr}[(I-n)P\rho(I+n)]$
$= \frac{1}{4}\mathrm{tr}[P\rho(I+n)(I-n)]$
+1 eigenvalue & -1 eigenvalue equally likely $\rightarrow$ flip a classical
$\pm P$ is added to S, M is removed from S
$N \in S, [N,P]=0 \Rightarrow N(I \pm P)|\psi\rangle = (I \pm P)N|\psi\rangle = (I \pm P)|\psi\rangle$


Measure $P \in P_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$
$\mathrm{tr}\, P_\rho = \frac{1}{4}\mathrm{tr}[P(I+M)\rho(I+M)] = \frac{1}{4}\mathrm{tr}[(I-M)P\rho(I+M)]$
$= \frac{1}{4}\mathrm{tr}[P\rho(I-M)] = 0$
$+1$ eigenvalue & -1 eigenvalue equally likely
a coin for
simulation
$\pm P$ is added to S, M is removed from S
$N \in S$, $[N,P]=0 \Rightarrow N(I \pm P)|\psi\rangle = (I \pm P)N|\psi\rangle = (I \pm P)|\psi\rangle$
$\therefore$ (S' new S)


Measure $P \in P_n$:
Case 1: $\pm P \in S$ ⇒ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$
± 1 eigenvalue & -1 eigenvalue equally likely ⇒
$\pm P$ is added to S, M is removed from S
$N \in S, [N,P]=0 \Rightarrow N(I \pm P)|\psi\rangle = (I \pm P) N|\psi\rangle = (I \pm P)|\psi\rangle$
If $\{N,P\}=0 \Rightarrow [MN,P]=0$

Measure $P \in \mathcal{P}_n$:

Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined

Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$

$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}\left[P(I+M)\rho(I+M)\right] = \frac{1}{4}\mathrm{tr}\left[(I-M)P\rho(I+M)\right]$

$= \frac{1}{4}\mathrm{tr}\left[P\rho(I+M)(I-M)\right] = 0$

$+1$ eigenvalue & -1 eigenvalue equally likely $\Rightarrow$ flip a coin for classical simulation

$\pm P$ is added to S, M is removed from S

$N \in S$, $[N,P]=0 \Rightarrow N(I \pm P)|\psi\rangle = (I \pm P)N|\psi\rangle = (I \pm P)|\psi\rangle \Rightarrow N \in S'$ (S' new S)

If $\{N,P\}=0 \Rightarrow [MN,P]=0 \Rightarrow$ Replace generators N_i of S:

If $[N_i,P]=0$ keep N_i

$\{N_i,P\}=0$ $N_i \to MN_i$

Similarly $\bar{X}$ & $\bar{Z}$'s

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} I & X & X \\ Z & X & I \\ I & Z & I \end{matrix}$ $\xrightarrow{CNOT}$ $\begin{matrix} I & X & X \\ Z & X & I \\ I & Z & I \end{matrix}$ $\xrightarrow{Measure}$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} XII \\ IXX \\ ZZI \end{matrix}$ $\xrightarrow{CNOT}$ $\begin{matrix} IIX \\ IXX \\ ZZI \end{matrix}$ $\xrightarrow{Measure}$ $\begin{matrix} IIX \\ IXX \\ ZZI \end{matrix}$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} I & X & X \\ I & Z & Z \\ X & I & I \\ Z & I & I \end{matrix}$ $\xrightarrow{\text{CNOT}}$ $\begin{matrix} I & X & X \\ I & Z & Z \\ X & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{\text{Measure}}$ $\begin{matrix} I & X & X \\ X & I & I \\ Z & Z & I \\ I & I & Z \end{matrix}$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} II & XX \\ XI & IX \\ ZI & IZ \end{matrix}$ CNOT $\begin{matrix} II & XX \\ XX & IX \\ ZI & ZZ \end{matrix}$ Measure $\begin{matrix} II & XX \\ XX & IX \\ ZZ & ZI \end{matrix}$ $\begin{matrix} \bar{Z} = XX \\ \bar{X} = IX \end{matrix}$ $\bar{Z} = XX$ $\bar{X} = IX$ $\bar{Z} = IZ$ $\bar{X} = ZI$ $\bar{Z} = ZZ$ $\bar{X} = XI$ $\bar{Z} = IZ$ $\bar{X} = XI$ Measure Z $\bar{Z} = IZ$ $\bar{X} = XI$ $T \times I$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} II & XX & XX \\ XI & XI & II \\ ZI & ZI & II \end{matrix}$ CNOT $\begin{matrix} II & XX & XX \\ XI & XI & II \\ ZI & ZI & II \end{matrix}$ Measure $\begin{matrix} II & XX & XX \\ XI & XI & II \\ ZI & ZI & II \end{matrix}$ $(-1)^{}$

$\begin{matrix} II & XX & XX \\ XI & XI & II \\ ZI & ZI & II \end{matrix}$ $(-1)^{} = (-1)^{} IXI$

Measure $\begin{matrix} II & XX & XX \\ XI & XI & II \\ ZI & ZI & II \end{matrix}$

$ZZI = IZZ$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} I & X & X \\ Z & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{CNOT}$ $\begin{matrix} I & X & X \\ Z & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{Measure}$ $\begin{matrix} I & X & X \\ (-1)^{x} X & I & I \\ Z & I & I \end{matrix}$

$\xrightarrow{Measure}$ $\begin{matrix} I & X & X \\ (-1)^{x} X & I & I \\ (-1)^{z} Z & I & I \end{matrix}$

$\begin{matrix} I & X & X \\ X & I & I \\ Z & I & I \end{matrix}$

Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

Example: teleportation

Stabilizer $\begin{matrix} I & X & X \\ Z & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{CNOT}$ $\begin{matrix} I & X & X \\ Z & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{Measure}$ $\begin{matrix} I & X & X \\ (-1)^a X & I & I \\ Z & I & I \end{matrix}$

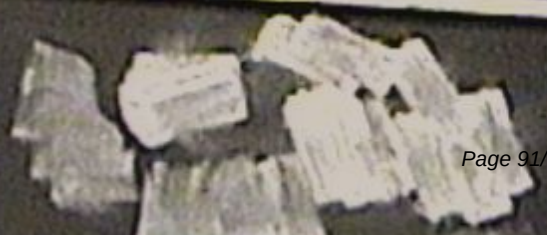
$\begin{matrix} I & X & X \\ (-1)^a X & I & I \\ (-1)^b Z & I & I \end{matrix}$ $\xrightarrow{Measure}$ $\begin{matrix} I & X & X \\ (-1)^a X & I & I \\ (-1)^b Z & I & I \end{matrix}$ $\xrightarrow{Pauli}$ $\begin{matrix} I & X & X \\ (-1)^a X & I & I \\ (-1)^b Z & I & I \end{matrix}$

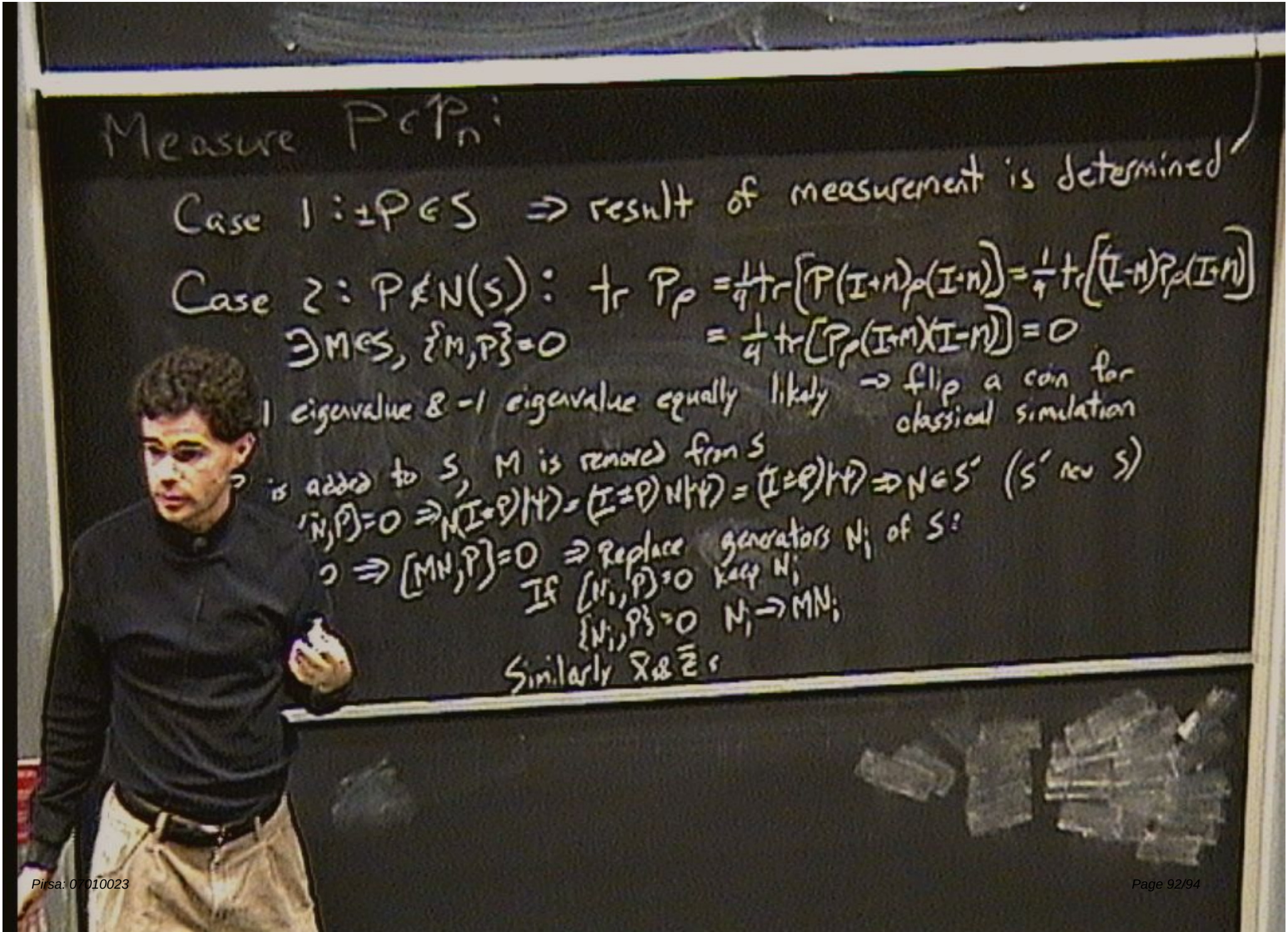
Def. $Sp(2n, \mathbb{Z}_2)$ is set of linear operations on $2n$-bit vectors that preserve symplectic inner product $(a|b)\cdot(c|d) = a\cdot d + b\cdot c$

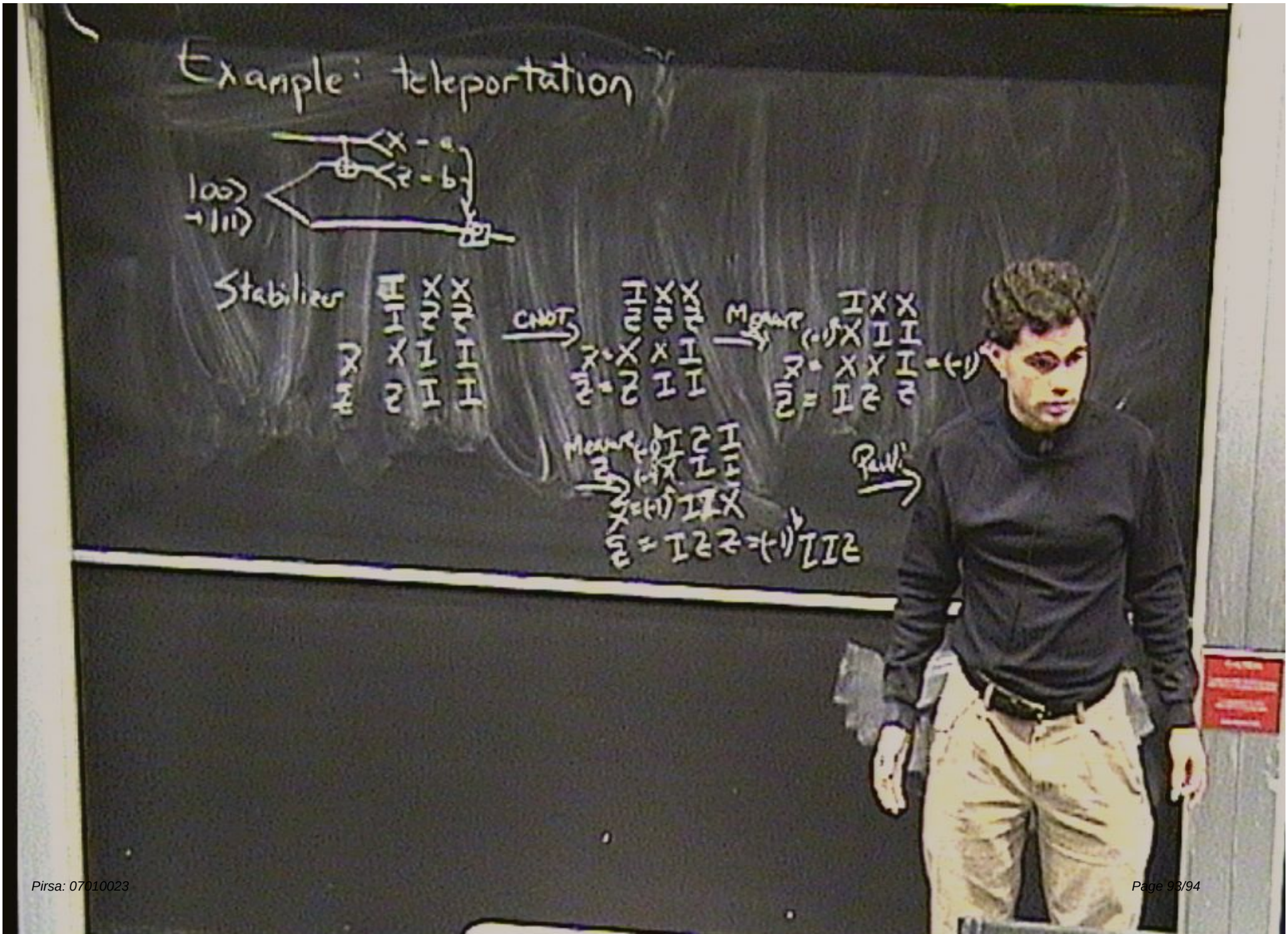
Example: teleportation

Stabilizer $\begin{matrix} I & X & X \\ Z & I & X \\ I & Z & I \end{matrix}$ $\xrightarrow{CNOT}$ $\begin{matrix} I & X & X \\ Z & X & I \\ Z & I & I \end{matrix}$ $\xrightarrow{Measure}$ $\begin{matrix} I & X & X \\ X & I & I \\ Z & I & I \end{matrix}$

$\xrightarrow{Measure}$ $\begin{matrix} I & I & X \\ X & I & I \\ I & I & I \end{matrix}$ $\xrightarrow{Pauli}$ $\begin{matrix} I & I & X \\ X & I & I \\ I & I & I \end{matrix}$




Measure $P \in \mathcal{P}_n$:
Case 1: $\pm P \in S \Rightarrow$ result of measurement is determined
Case 2: $P \notin N(S)$: $\exists M \in S, \{M,P\}=0$
$\mathrm{tr}\, P\rho = \frac{1}{4}\mathrm{tr}[P(I+M)\rho(I+M)] = \frac{1}{4}\mathrm{tr}[(I-M)P\rho(I+M)]$
$= \frac{1}{4}\mathrm{tr}[P\rho(I+M)(I-M)] = 0$
1 eigenvalue & -1 eigenvalue equally likely → flip a coin for classical simulation
P is added to S, M is removed from S
$\{N,P\}=0 \Rightarrow N(I \pm P)|\psi\rangle = (I \mp P)N|\psi\rangle = (I \mp P)|\psi\rangle \Rightarrow N \in S'$ (S' new S)
$\supset \Rightarrow [MN,P]=0 \Rightarrow$ Replace generators N_i of S:
If $[N_i,P]=0$ keep N_i
$\{N_i,P\}=0$ $N_i \to MN_i$
Similarly X & Z:


Example: teleportation
|00⟩ + |11⟩
Stabilizer
CNOT
Measure
Measure
Pauli

Example: teleportation

Stabilizer

CNOT

Measure

Measure

Rot