Title: Quantum Error Correction 2A

Date: Jan 16, 2007 03:30 PM

URL: http://pirsa.org/07010020

Abstract: Stabilizer codes (definition of stabilizer, basic properties of stabilizer, binary vector representation of stabilizer)

Tensor produc[illegible] Z w/ overall phase $\pm 1, \pm i$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} [illegible] \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\qquad Y = iXZ$

$XY = -YX$, $XZ = -ZX$, $YZ = -ZY$, $X^2 = Y^2 = Z^2 = I$

$\forall P, Q \in \mathcal{P}_n$, $PQ = QP \; (\Leftrightarrow [P,Q] = 0)$ or $PQ = -QP \; (\Leftrightarrow \{P,Q\} = 0)$

$P^2 = \pm I$

wt P = # of non-identity tensor factors

Pauli group n qubits:

Tensor products of I, X, Y, Z w/ overall phase $\pm 1, \pm i$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad Y = iXZ$

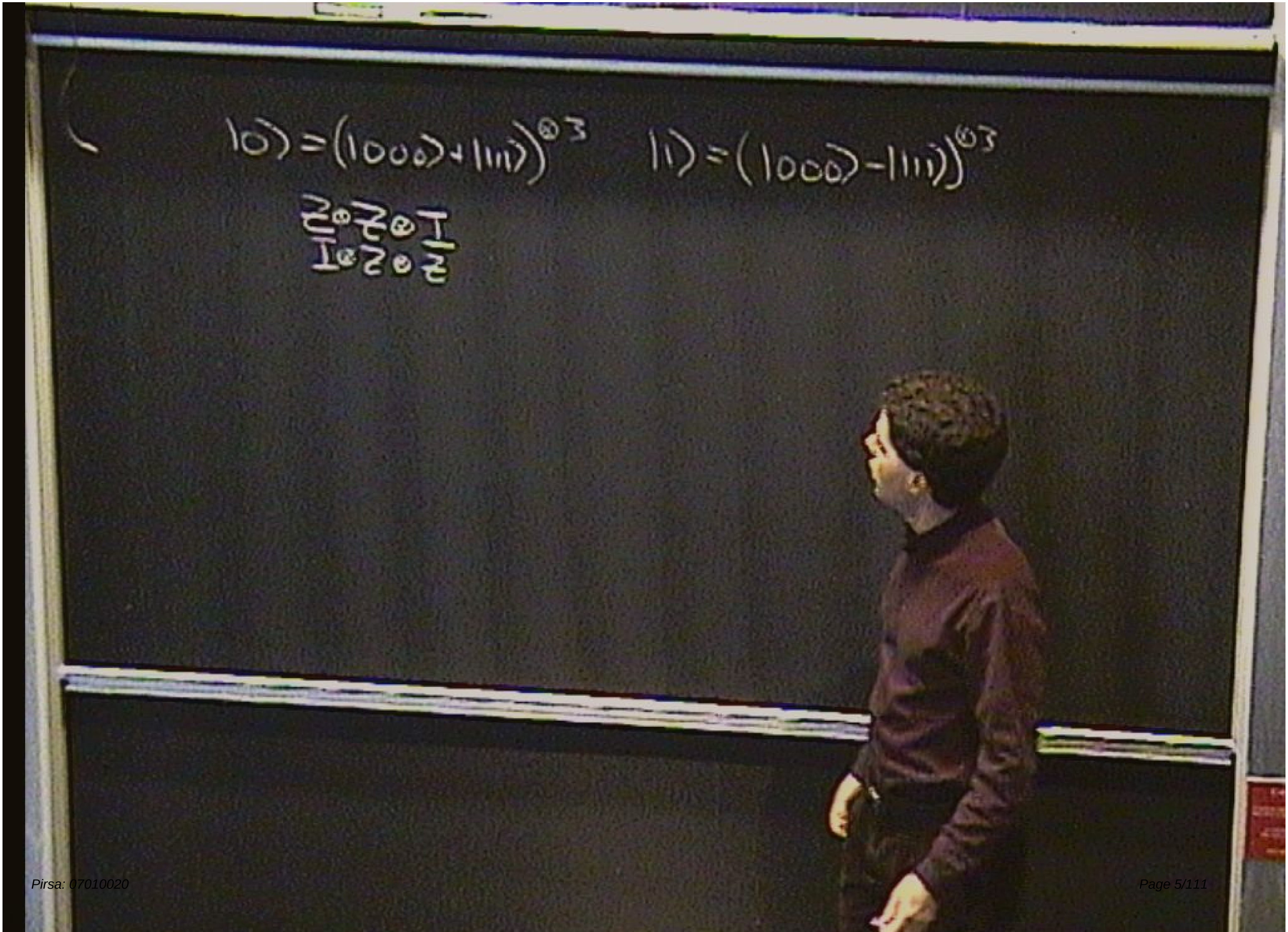
$XY = -YX$, $XZ = -ZX$, $YZ = -ZY$, $\quad X^2 = Y^2 = Z^2 = I$

$\forall P, Q \in \mathcal{P}_n$, $\quad PQ = QP \; (\Leftrightarrow [P,Q] = 0)$ $\underline{\text{or}}$ $PQ = -QP \; (\Leftrightarrow \{P,Q\} = 0)$

$P^2 = \pm I$

wt P = # of non-identity tensor factors

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \qquad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

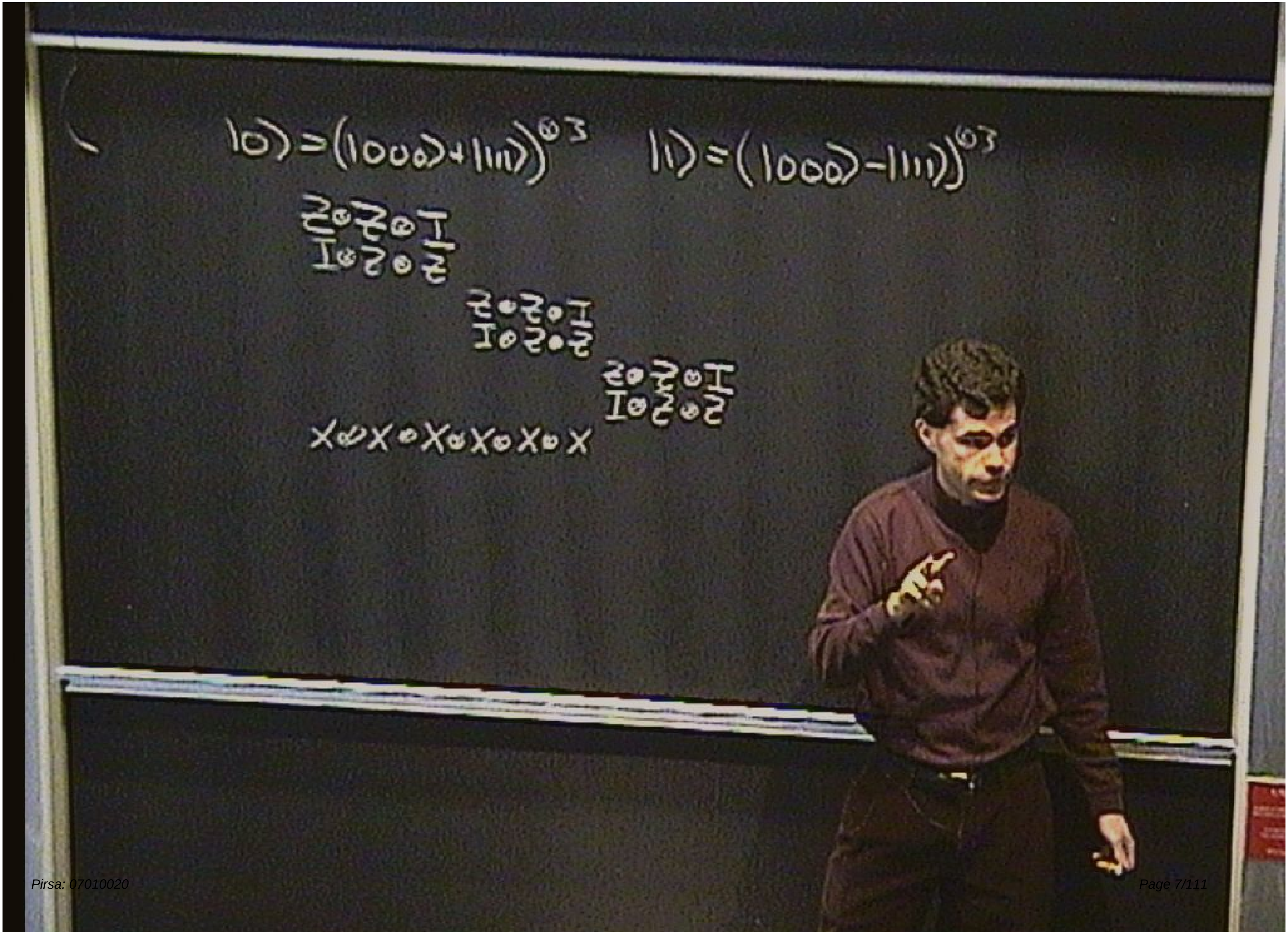

$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$
$|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$
$Z \otimes Z \otimes I$
$I \otimes Z \otimes Z$

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \qquad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$

$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$

$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$


$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$
$|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$
$Z \otimes Z \otimes I$
$I \otimes Z \otimes Z$
$Z \otimes Z \otimes I$
$I \otimes Z \otimes Z$
$Z \otimes Z \otimes I$
$I \otimes Z \otimes Z$
$X \otimes X \otimes X \otimes X \otimes X \otimes X$

$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \qquad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

$Z \otimes Z \otimes I$

$I \otimes Z \otimes Z$

$Z \otimes Z \otimes I$

$I \otimes Z \otimes Z$

$Z \otimes Z \otimes I$

$I \otimes Z \otimes Z$

$X \otimes X \otimes X \otimes X \otimes X \otimes X$

$X \otimes X \otimes X \otimes X \otimes X \otimes X$

$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$ $|1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$

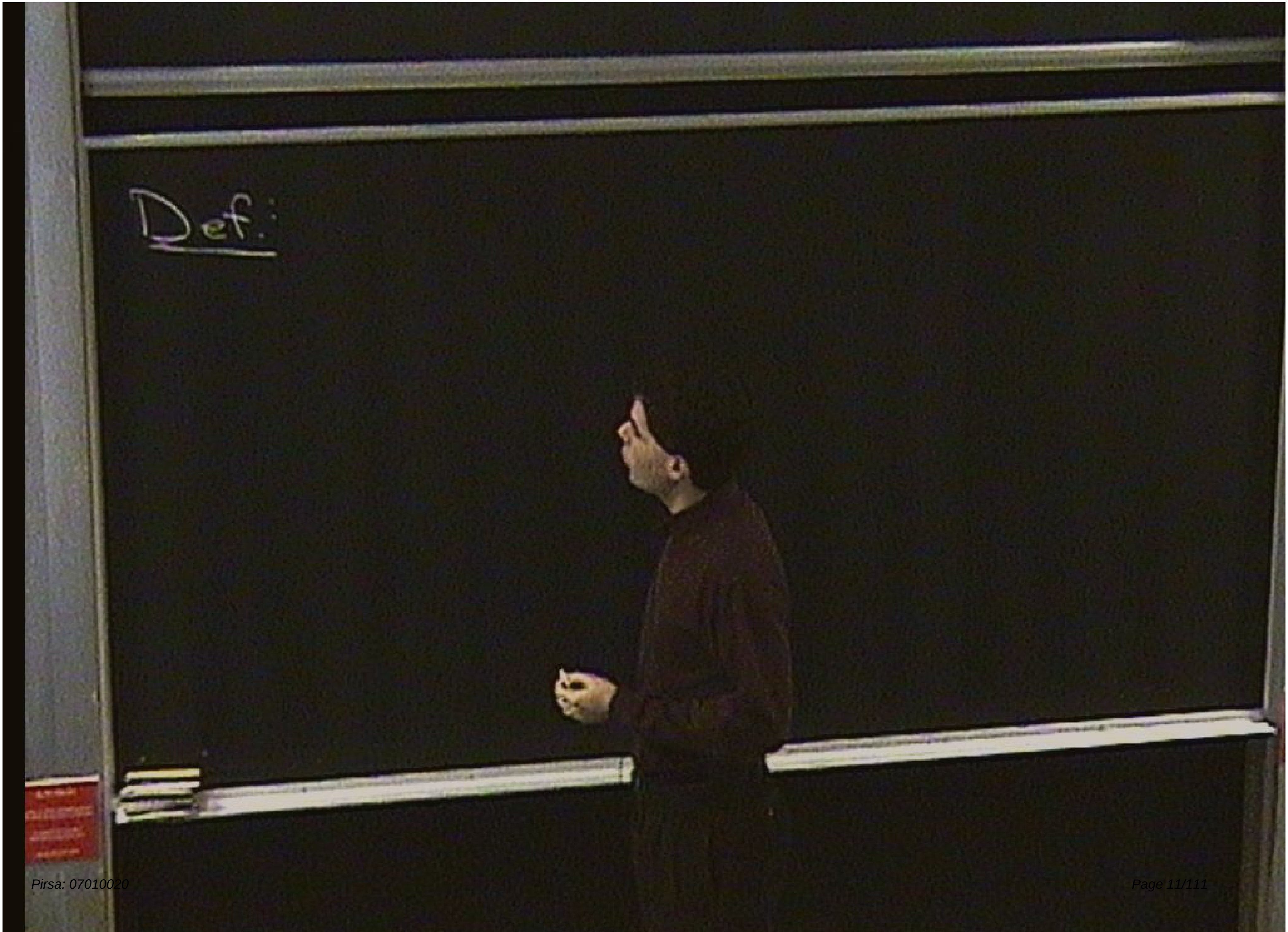
$$\left.\begin{array}{l}
Z\otimes Z\otimes I \\
I\otimes Z\otimes Z \\
\qquad Z\otimes Z\otimes I \\
\qquad I\otimes Z\otimes Z \\
\qquad\qquad Z\otimes Z\otimes I \\
\qquad\qquad I\otimes Z\otimes Z \\
X\otimes X\otimes X\otimes X\otimes X\otimes X \\
\qquad X\otimes X\otimes X\otimes X\otimes X\otimes X
\end{array}\right]$$

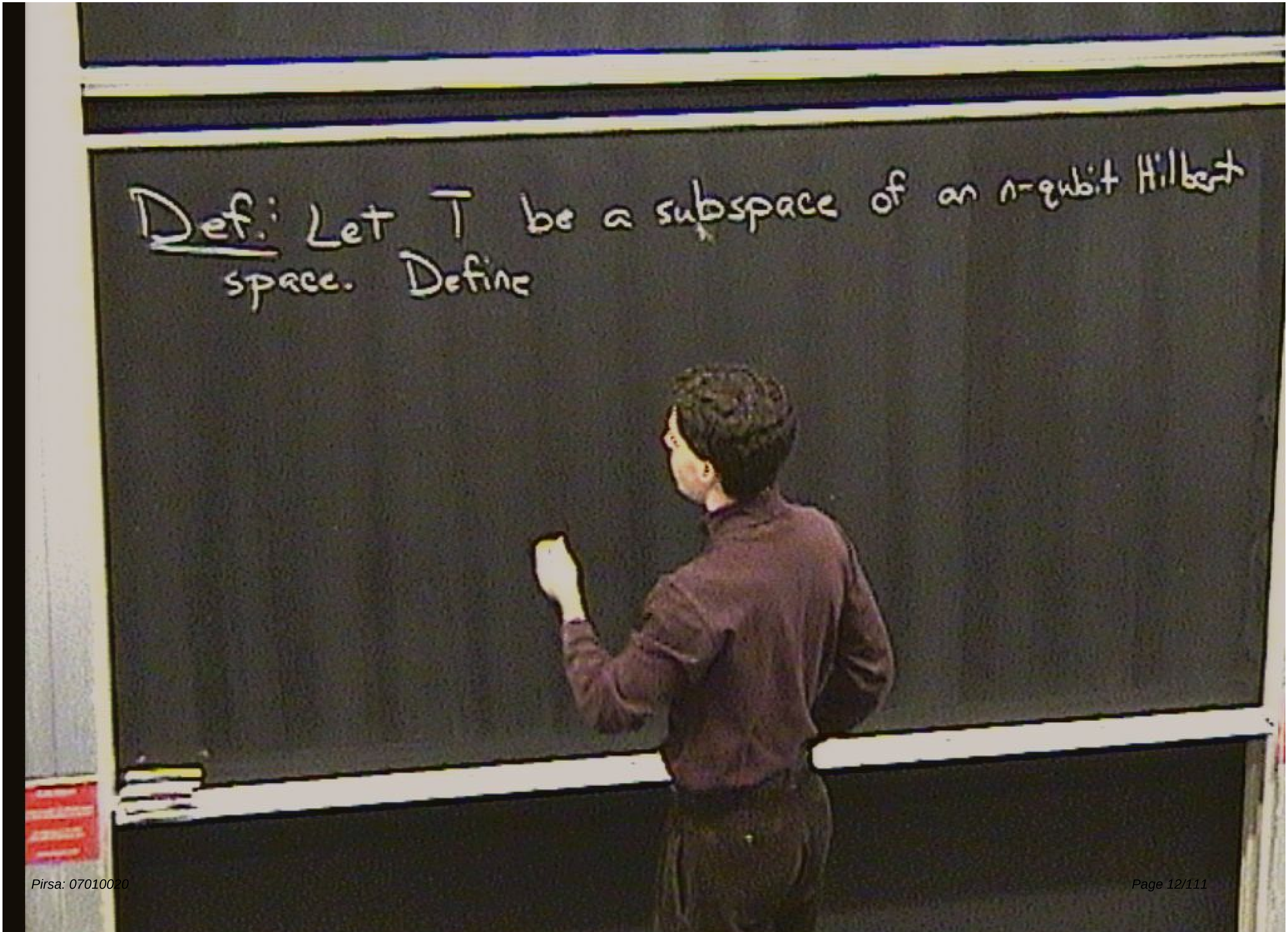
8 operators
eigenvalues determine
error syndrome

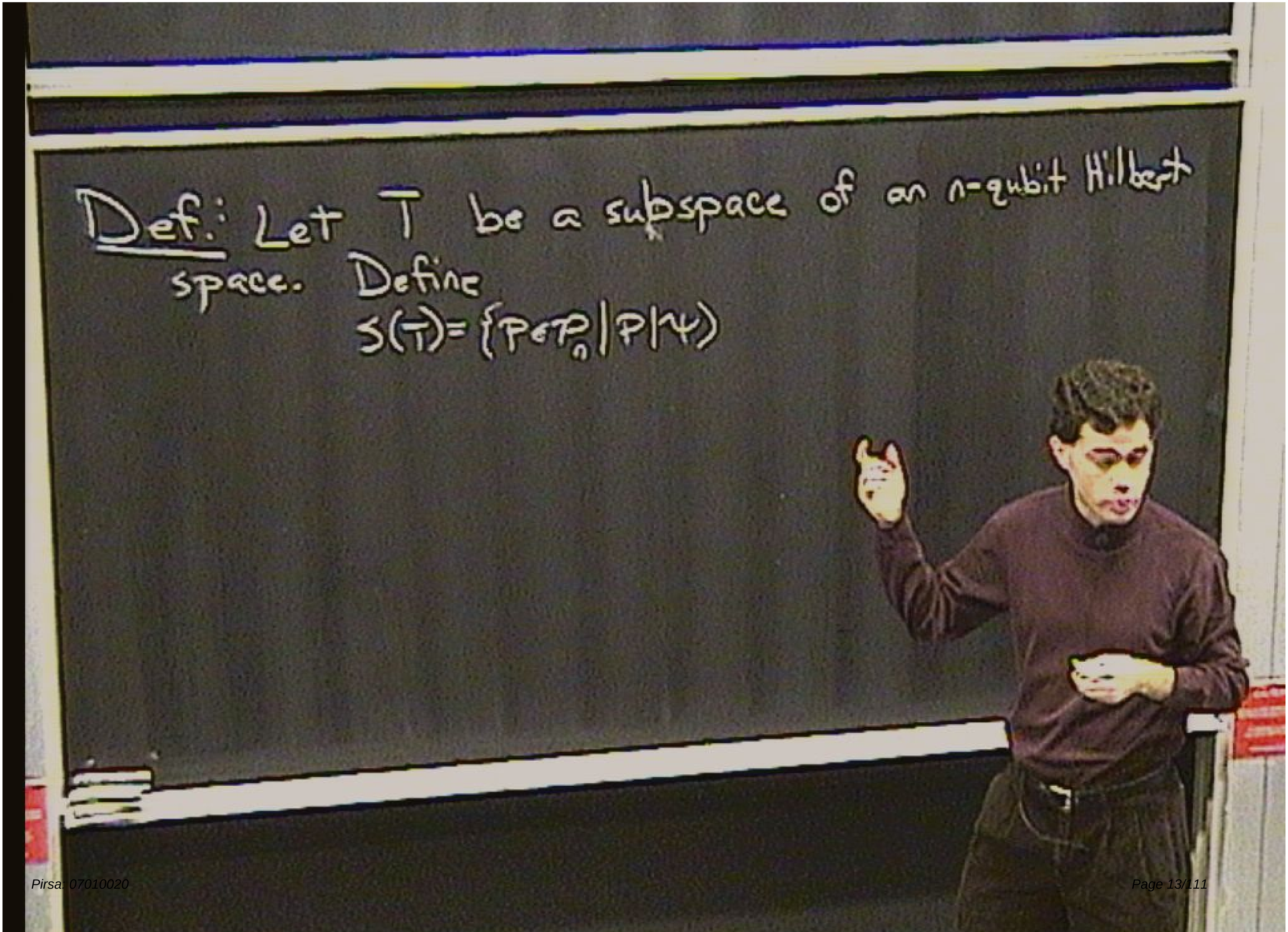
$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \qquad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

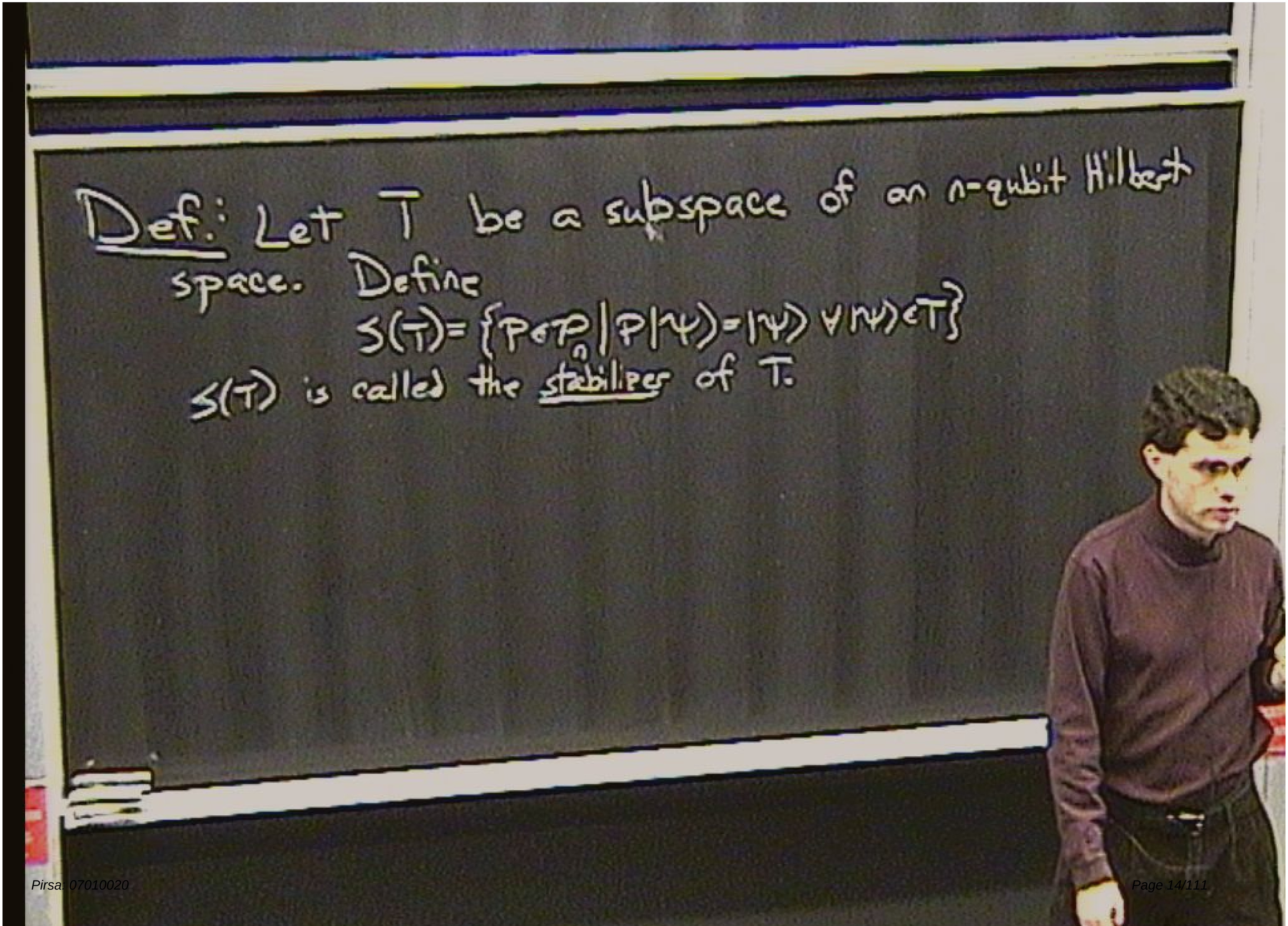
$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$
$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$
$$Z \otimes Z \otimes I$$
$$I \otimes Z \otimes Z$$
$$X \otimes X \otimes X \otimes X \otimes X \otimes X$$
$$X \otimes X \otimes X \otimes X \otimes X \otimes X$$

8 operators
eigenvalues determine
error syndrome


Def:


Def.: Let T be a subspace of an n-qubit Hilbert
space. Define


Def.: Let T be a subspace of an n-qubit Hilbert
space. Define
$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle$


Def.: Let T be a subspace of an n-qubit Hilbert
space. Define
$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$
S(T) is called the stabilizer of T.

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \; \forall |\psi\rangle \in T\}$$

$S(T)$ is called the stabilizer of T.

Properties of the stabilizer:

(1) $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle$

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

$S(T)$ is called the stabilizer of T.

Properties of the stabilizer:

1. $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$
2. $S(T)$ is Abelian:

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

$S(T)$ is called the stabilizer of T.

Properties of the stabilizer:

1. $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$
2. $S(T)$ is Abelian: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = |\psi\rangle = QP|\psi\rangle \Rightarrow [P,Q]|\psi\rangle = 0$

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

$S(T)$ is called the stabilizer of T.

Properties of the stabilizer:

① $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$

② $S(T)$ is Abelian: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = |\psi\rangle = QP|\psi\rangle \Rightarrow [P,Q]|\psi\rangle = 0$

For Paulis $\Rightarrow [P,Q] = 0$

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

$S(T)$ is called the <u>stabilizer</u> of T.

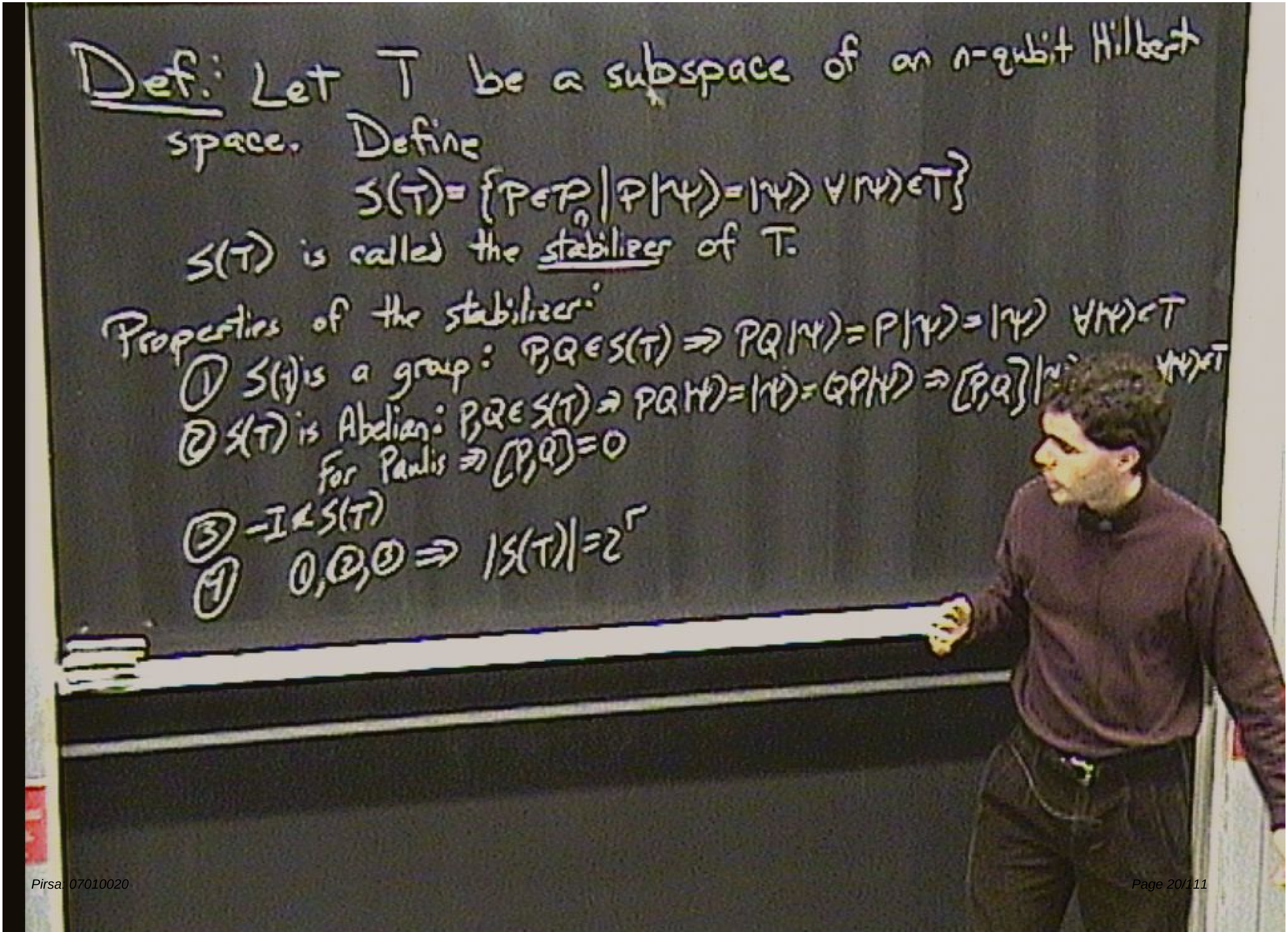
Properties of the stabilizer:

① $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$

② $S(T)$ is Abelian: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = |\psi\rangle = QP|\psi\rangle \Rightarrow [P,Q]|\psi\rangle = 0 \ \forall |\psi\rangle \in T$

For Paulis $\Rightarrow [P,Q] = 0$

③ $-I \notin S(T)$


Def: Let T be a subspace of an n-qubit Hilbert space. Define
S(T) = {P ∈ P_n | P|ψ⟩ = |ψ⟩ ∀|ψ⟩ ∈ T}
S(T) is called the stabilizer of T.
Properties of the stabilizer:
① S(T) is a group: P,Q ∈ S(T) ⇒ PQ|ψ⟩ = P|ψ⟩ = |ψ⟩ ∀|ψ⟩ ∈ T
② S(T) is Abelian: P,Q ∈ S(T) ⇒ PQ|ψ⟩ = |ψ⟩ = QP|ψ⟩ ⇒ [P,Q]|
∀|ψ⟩ ∈ T
For Paulis ⇒ [P,Q] = 0
③ −I ∉ S(T)
④ ①,②,③ ⇒ |S(T)| = 2^r

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

$S(T)$ is called the stabilizer of T.

Properties of the stabilizer:

① $S(T)$ is a group: $P,Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$

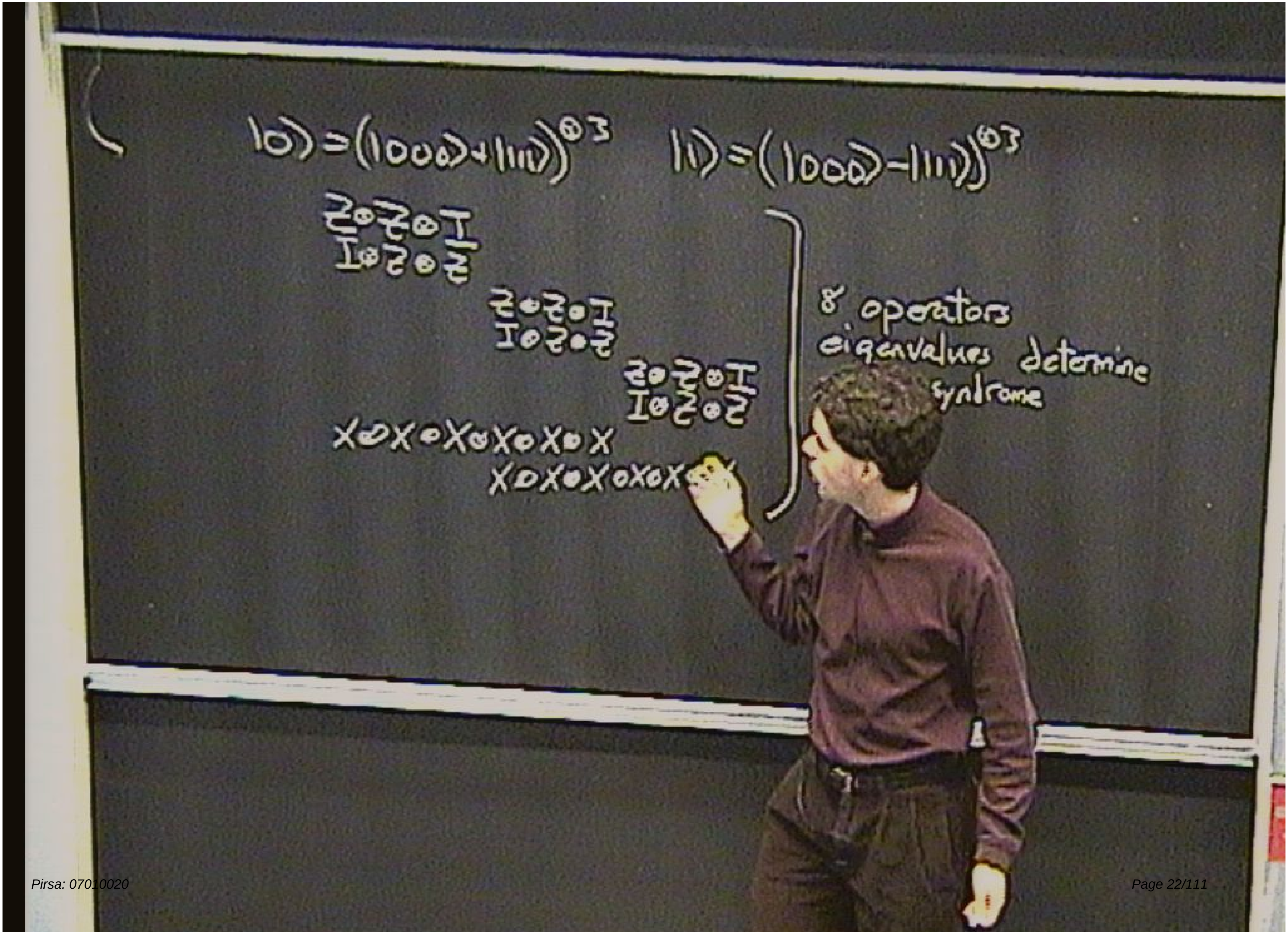
② $S(T)$ is Abelian: $P,Q \in S(T) \Rightarrow PQ|\psi\rangle = |\psi\rangle = QP|\psi\rangle \Rightarrow [P,Q]|\psi\rangle = 0 \ \forall |\psi\rangle \in T$

For Paulis $\Rightarrow [P,Q] = 0$

③ $-I \notin S(T)$

④ ①,②,③ $\Rightarrow |S(T)| = 2^r$ $\quad$ r generators $M_1, \ldots, M_r$

$M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r} \quad (a_i \in \{0,1\})$


|0⟩ = (|000⟩ + |111⟩)⊗3
|1⟩ = (|000⟩ − |111⟩)⊗3
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
X⊗X⊗X⊗X⊗X⊗X
X⊗X⊗X⊗X⊗X⊗X
8 operators
eigenvalues determine
syndrome

Def: Let T be a subspace of an n-qubit Hilbert space. Define

$$S(T) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}$$

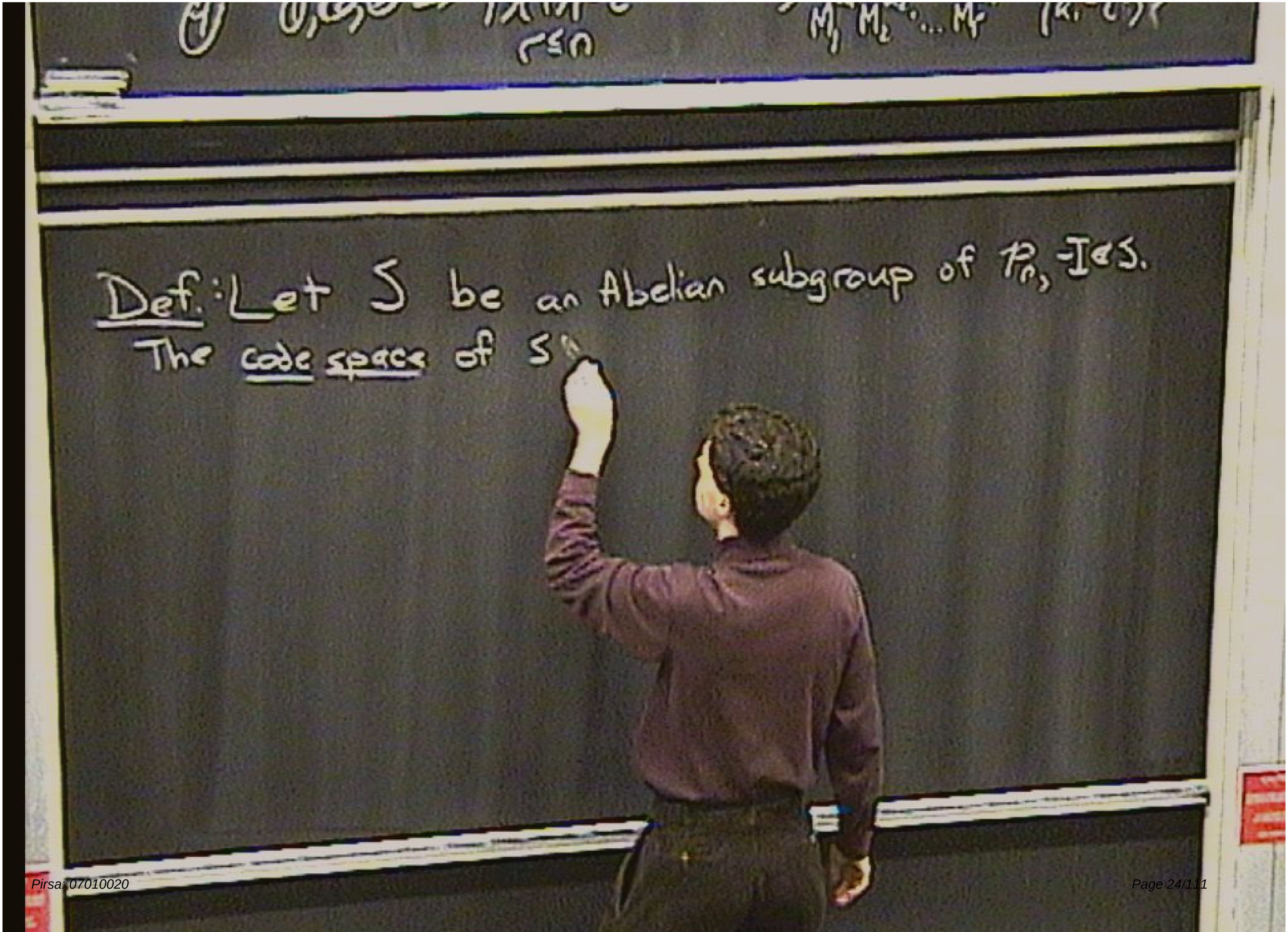
$S(T)$ is called the stabilizer of T.

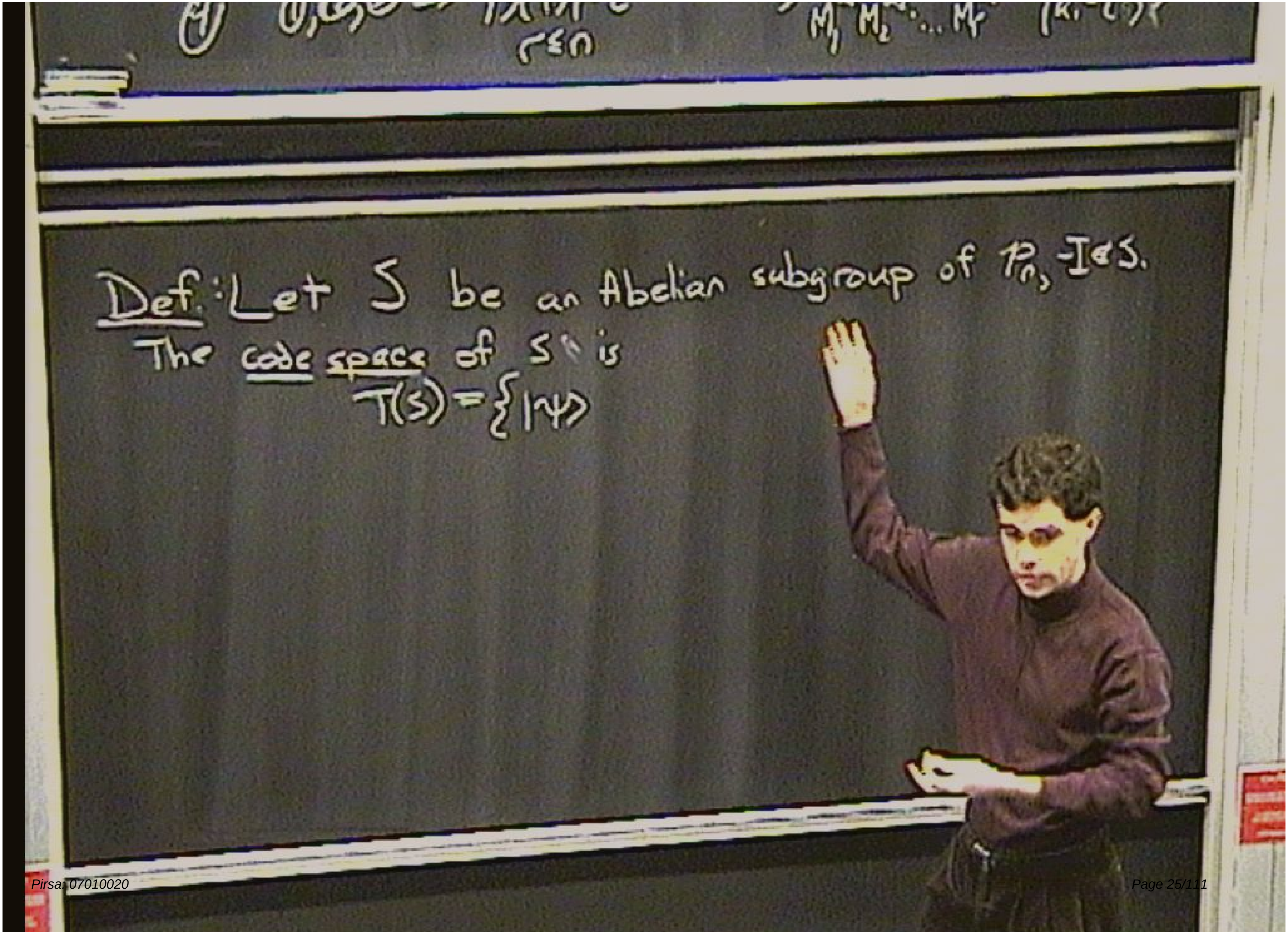
Properties of the stabilizer:

1. $S(T)$ is a group: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = P|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T$
2. $S(T)$ is Abelian: $P, Q \in S(T) \Rightarrow PQ|\psi\rangle = |\psi\rangle = QP|\psi\rangle \Rightarrow [P,Q]|\psi\rangle = 0 \ \forall |\psi\rangle \in T$

   for Paulis $\Rightarrow [P,Q] = 0$
3. $-I \notin S(T)$
4. 1, 2, 3 $\Rightarrow |S(T)| = 2^r$, $r \leq n$ r generators $M_1, \ldots, M_r$

   $M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r}$ $(a_i \in \{0,1\})$


Def.: Let S be an Abelian subgroup of P_n, $-I \notin S$.
The code space of S


Def.: Let S be an Abelian subgroup of P_n, $-I \notin S$.
The code space of S is
$T(S) = \{ |\psi\rangle$

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \,|\, P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$

$r \leq n$

$M_1 \; M_2 \; \ldots \; M_r$

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \;\; \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$

(but $T \subseteq T(S(T))$)

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

The code space of S is

$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

S or $T(S)$ is a stabilizer code

$S = S(T(S))$ but not always true that $T = T(S(T))$ (but $T \subseteq T(S(T))$)

(Sometimes symplectic code or additive / additive $GF(4)$)

Def.: Let S be an Abelian subgroup of $\mathcal{P}_n$, $-I \notin S$.

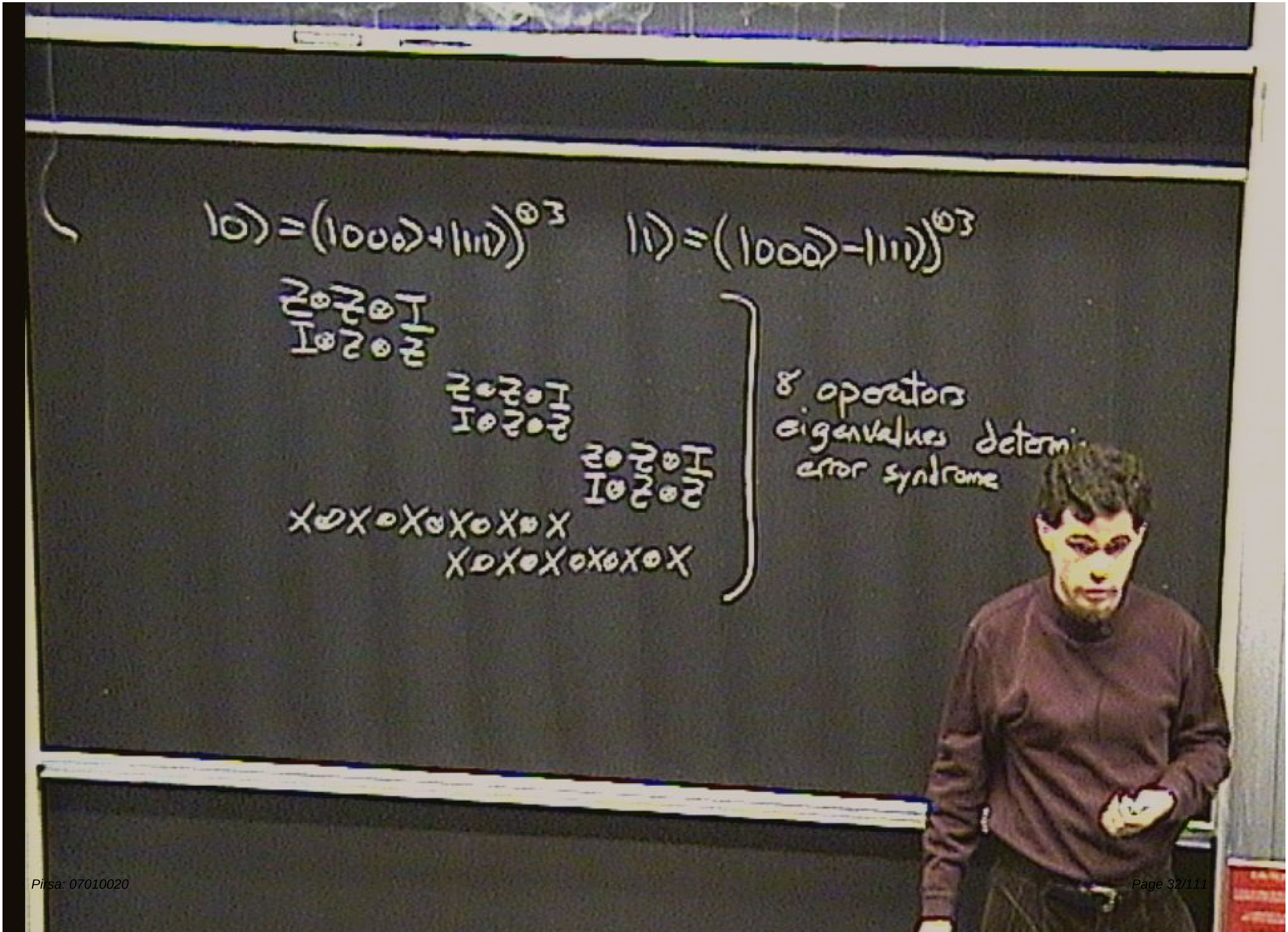
The **code space** of S is

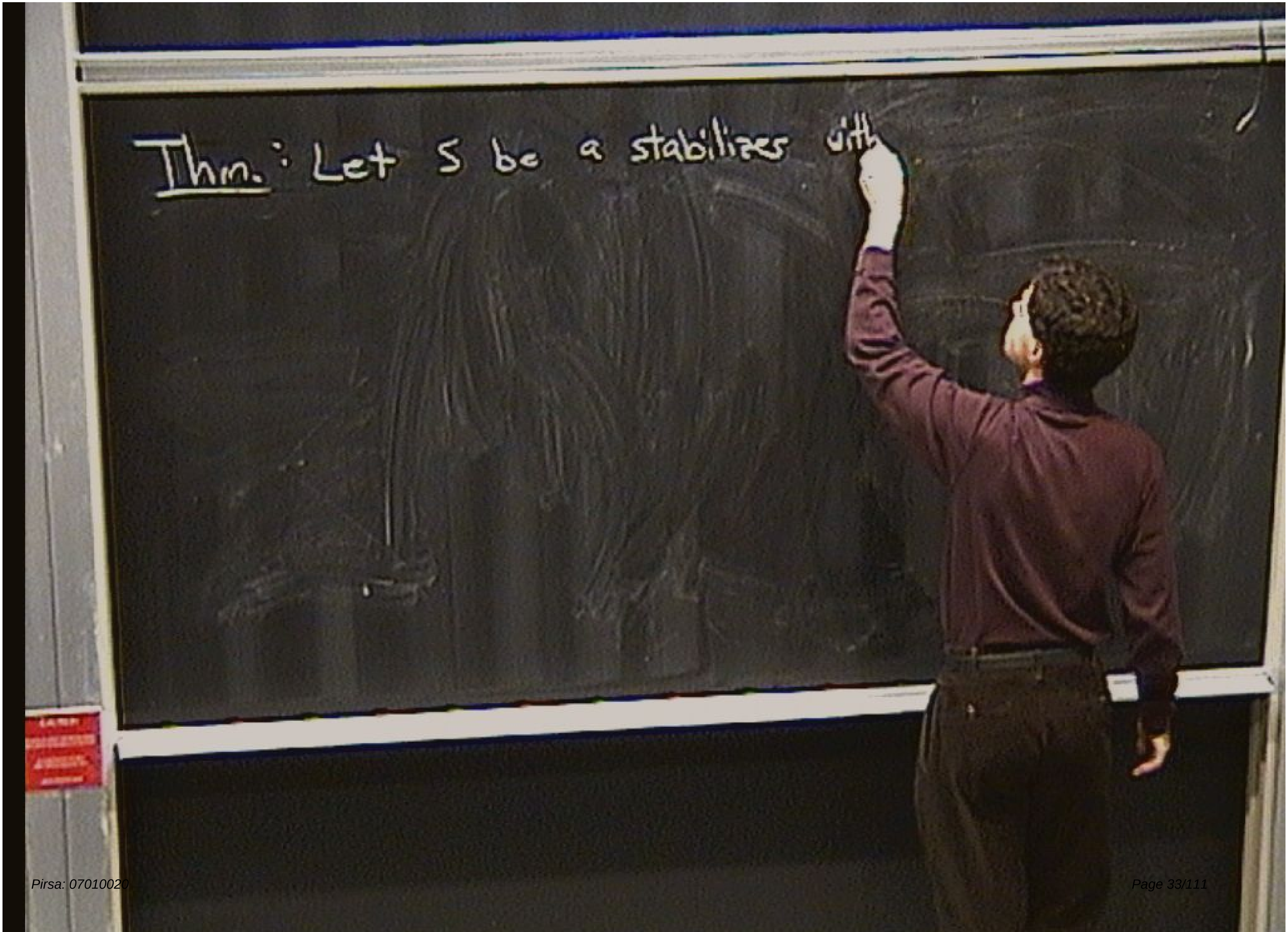
$$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$$

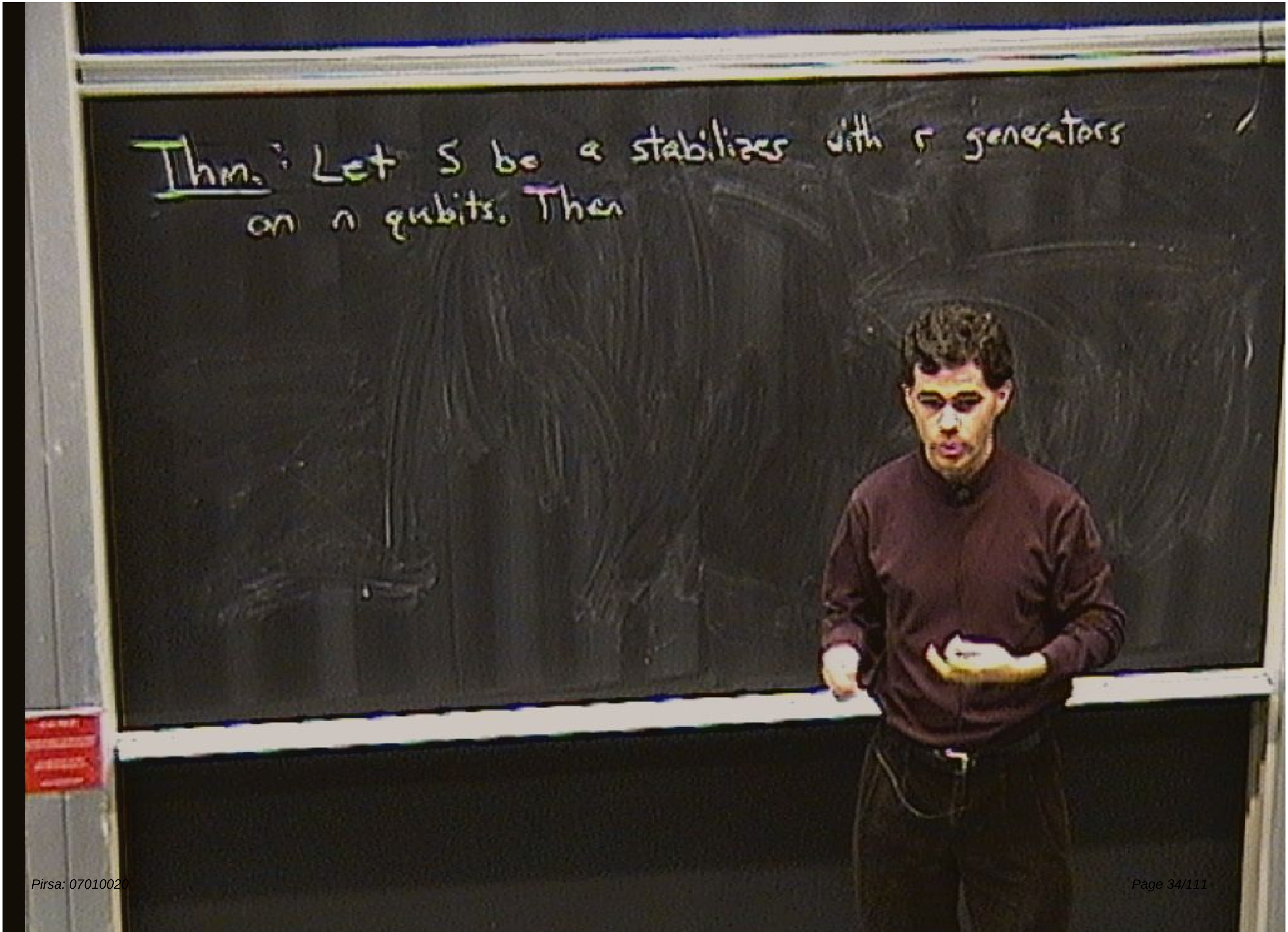
S or $T(S)$ is a **stabilizer code**

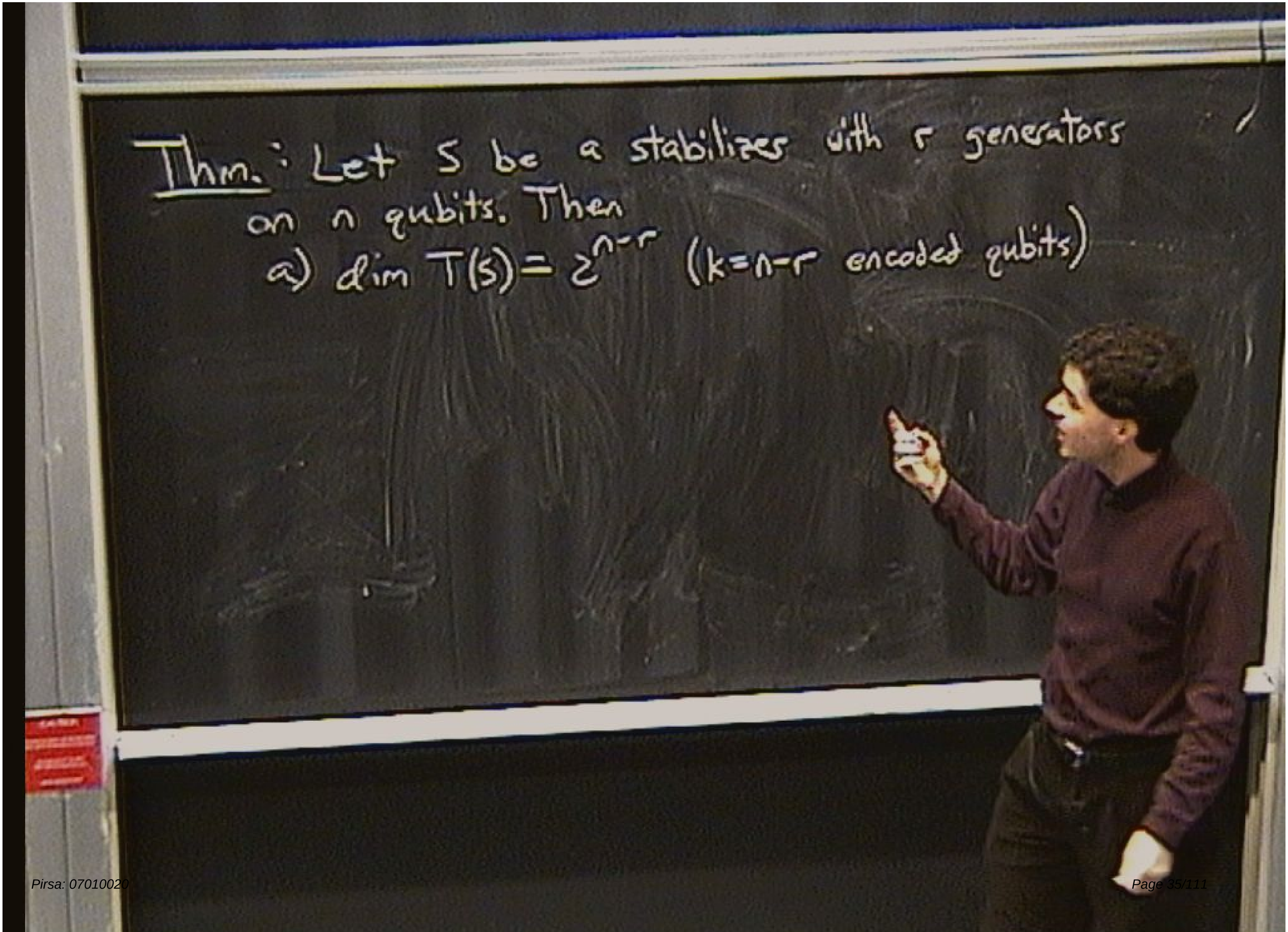
$S = S(T(S))$ but not always true that $T = T(S(T))$ ((but $T \subseteq T(S(T))$)

(Sometimes symplectic code or additive code / additive $GF(4)$)


|0⟩ = (|000⟩+|111⟩)⊗3
|1⟩ = (|000⟩−|111⟩)⊗3
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
X⊗X⊗X⊗X⊗X⊗X
X⊗X⊗X⊗X⊗X⊗X
8 operators
eigenvalues determi
error syndrome


Thm.: Let S be a stabilizer with

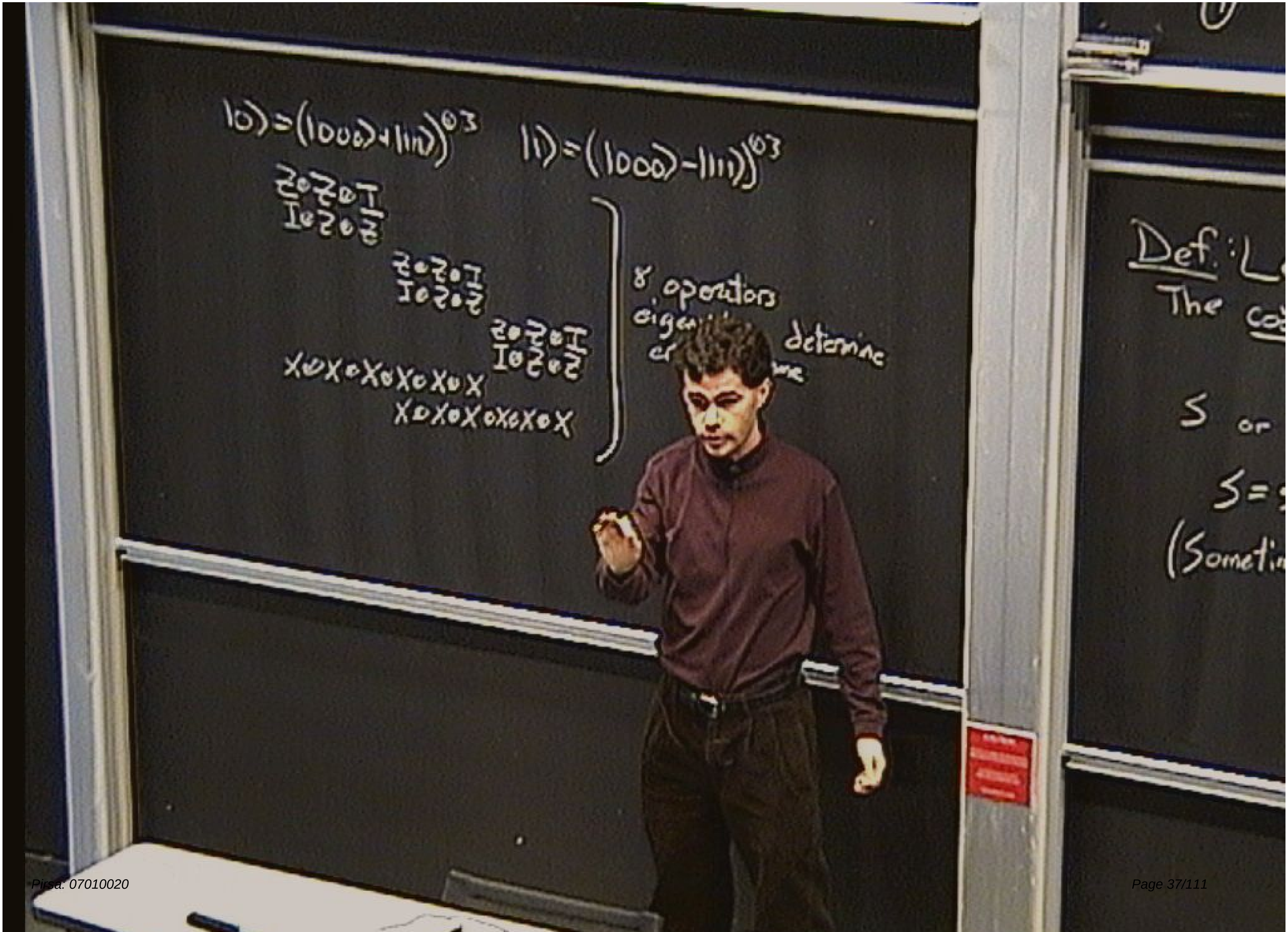

Thm.: Let S be a stabilizer with r generators
on n qubits. Then

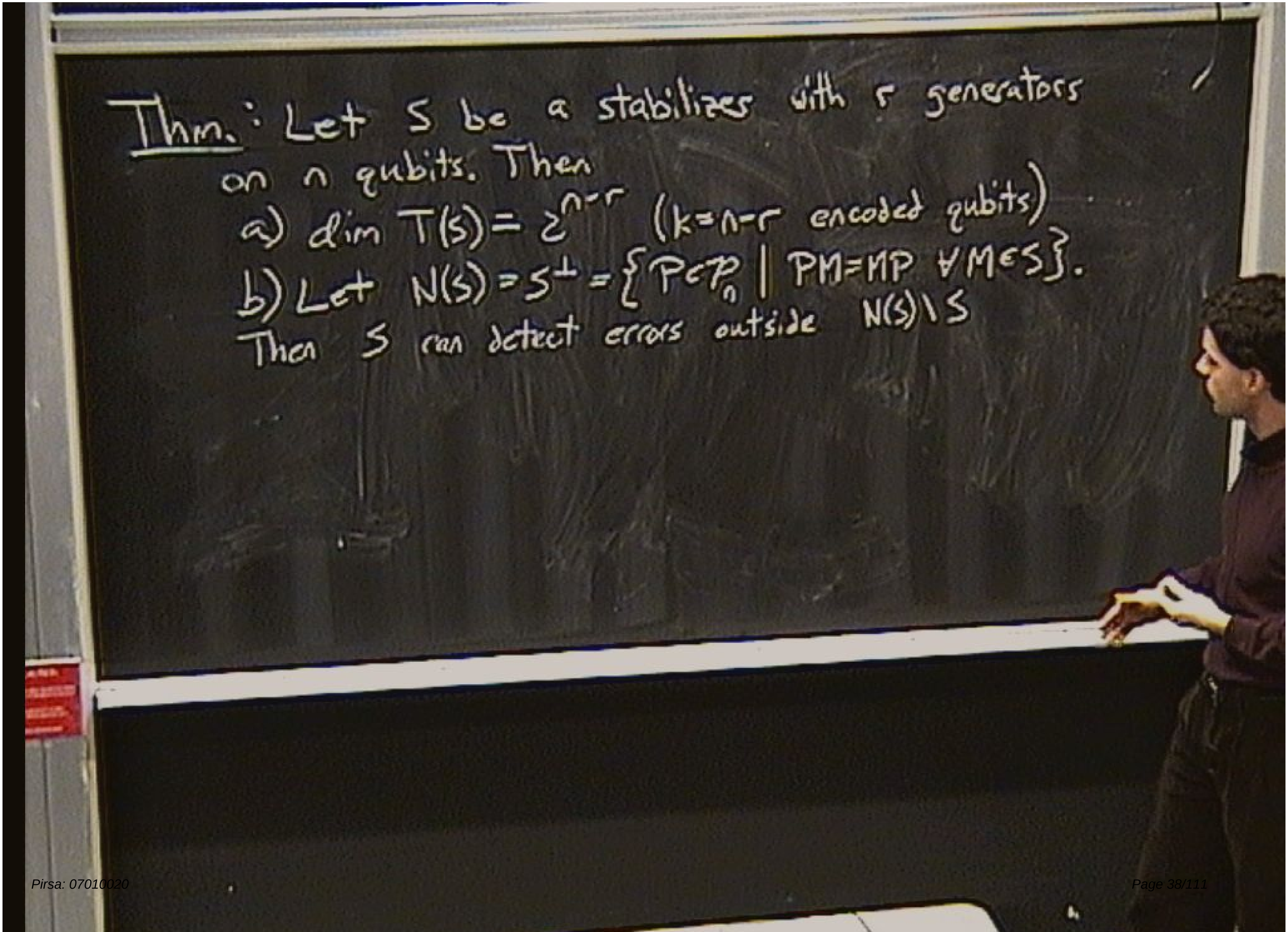

Thm.: Let S be a stabilizer with r generators
on n qubits. Then
a) dim T(S) = 2^{n-r} (k=n-r encoded qubits)

Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k = n-r$ encoded qubits)

b) Let $N(S) = S^{\perp} = \{ P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S \}$


|0⟩=(|000⟩+|111⟩)^⊗3
|1⟩=(|000⟩−|111⟩)^⊗3
8 operators
determine
XⓍXⓍXⓍXⓍXⓍXⓍX
XⓍXⓍXⓍXⓍXⓍX
Def.:
The
S
or
S=
(Someti


Thm.: Let S be a stabilizer with r generators on n qubits. Then
a) dim $T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)
b) Let $N(S) = S^{\perp} = \{P \in \mathcal{P}_n \mid PM=MP \ \forall M \in S\}$.
Then S can detect errors outside $N(S)\setminus S$

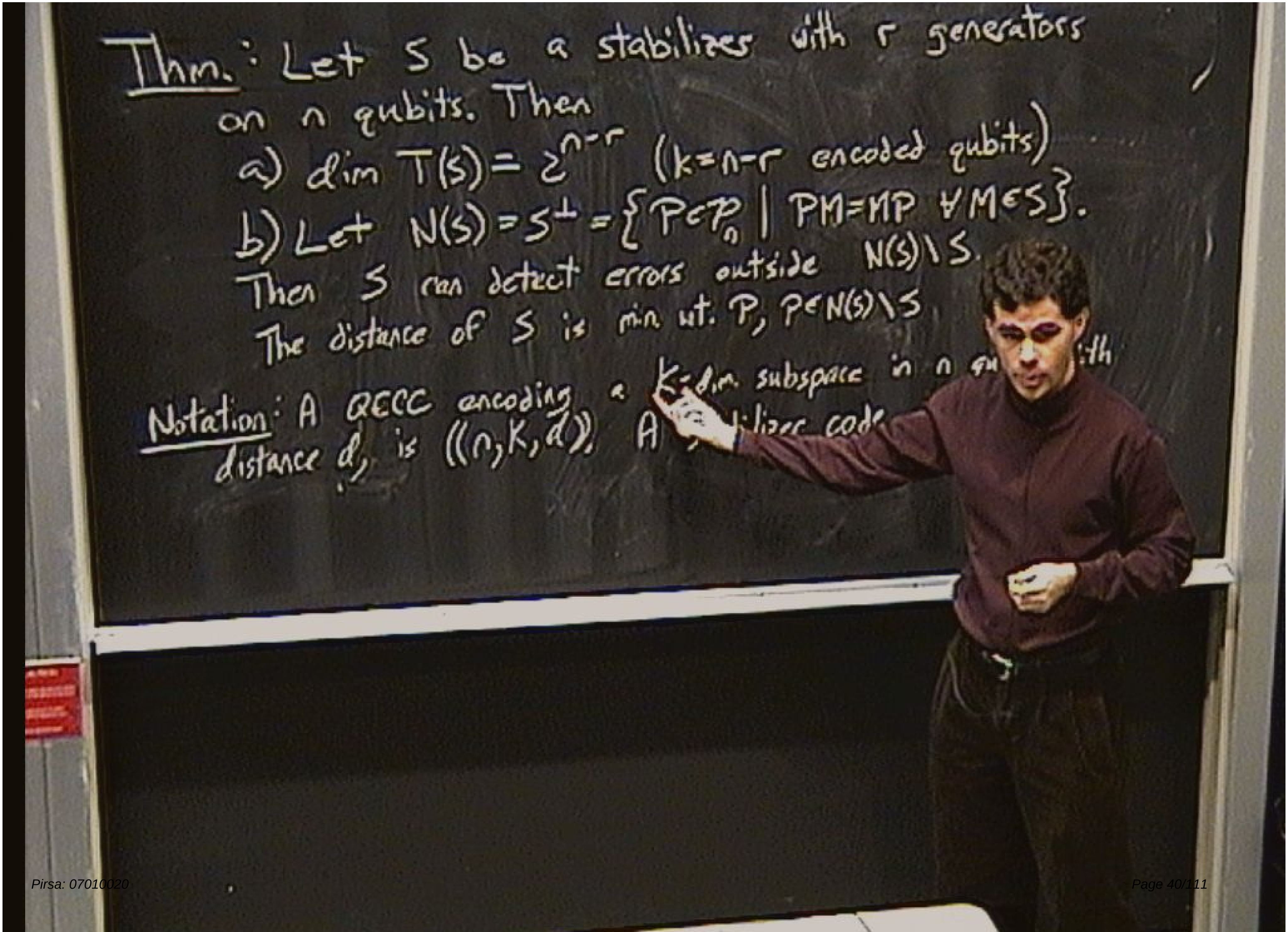
Thm.: Let S be a stabilizer with r generators on n qubits. Then

a) $\dim T(S) = 2^{n-r}$ ($k = n-r$ encoded qubits)

b) Let $N(S) = S^{\perp} = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min wt. P, $P \in N(S) \setminus S$


Thm.: Let S be a stabilizer with r generators
on n qubits. Then
a) dim T(S) = 2^{n-r} ($k=n-r$ encoded qubits)
b) Let $N(S) = S^{\perp} = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$.
Then S can detect errors outside $N(S) \setminus S$.
The distance of S is min wt. P, $P \in N(S) \setminus S$
Notation: A QECC encoding a K-dim subspace in n
distance d, is ((n, K, d)). A
code

Thm: Let S be
on n qubits. Then

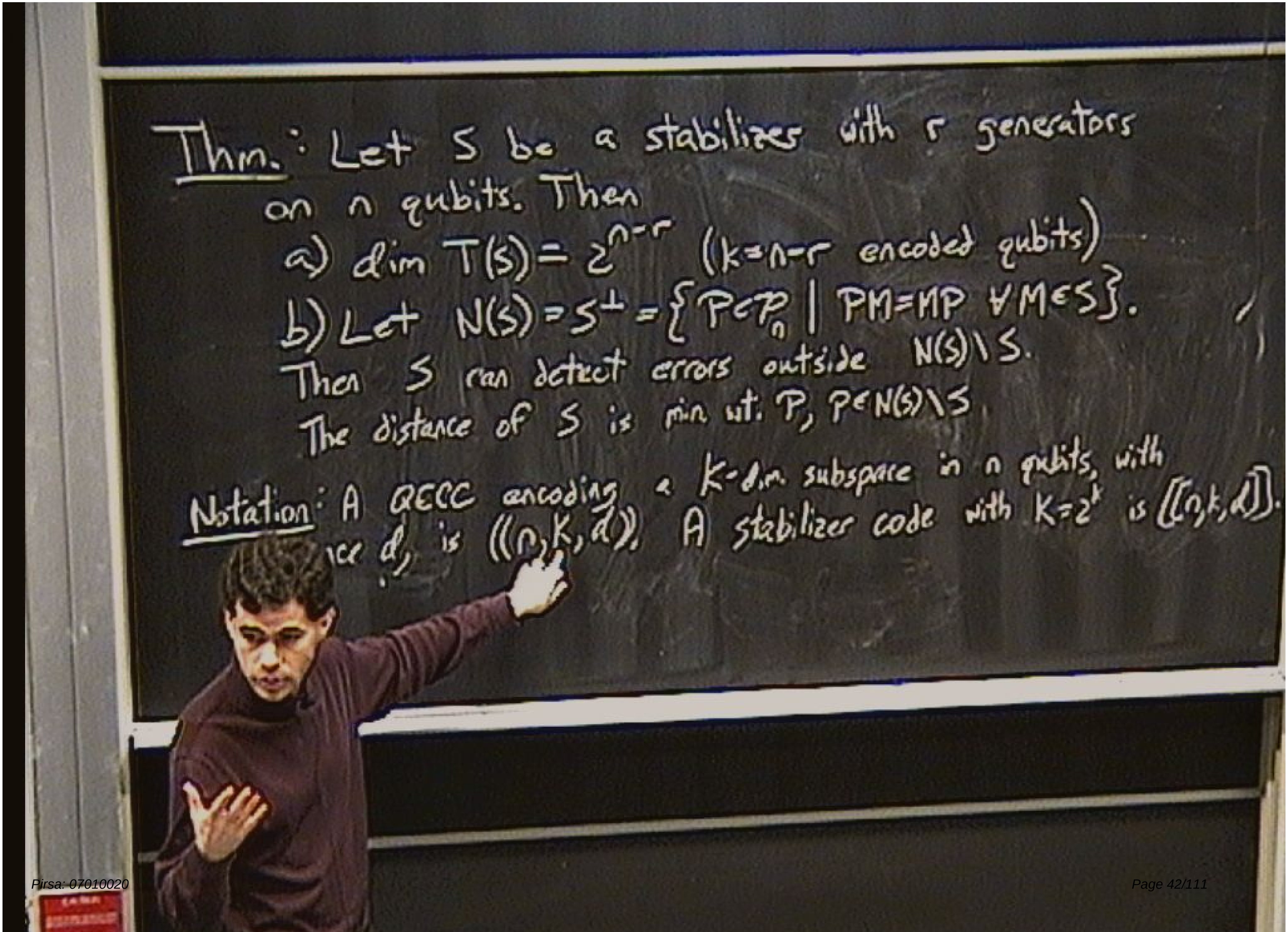
a) $\dim T(S) = 2^{n-r}$ ($k = n-r$ encoded qubits)

b) Let $N(S) = S^{\perp} = \{ P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S \}$.

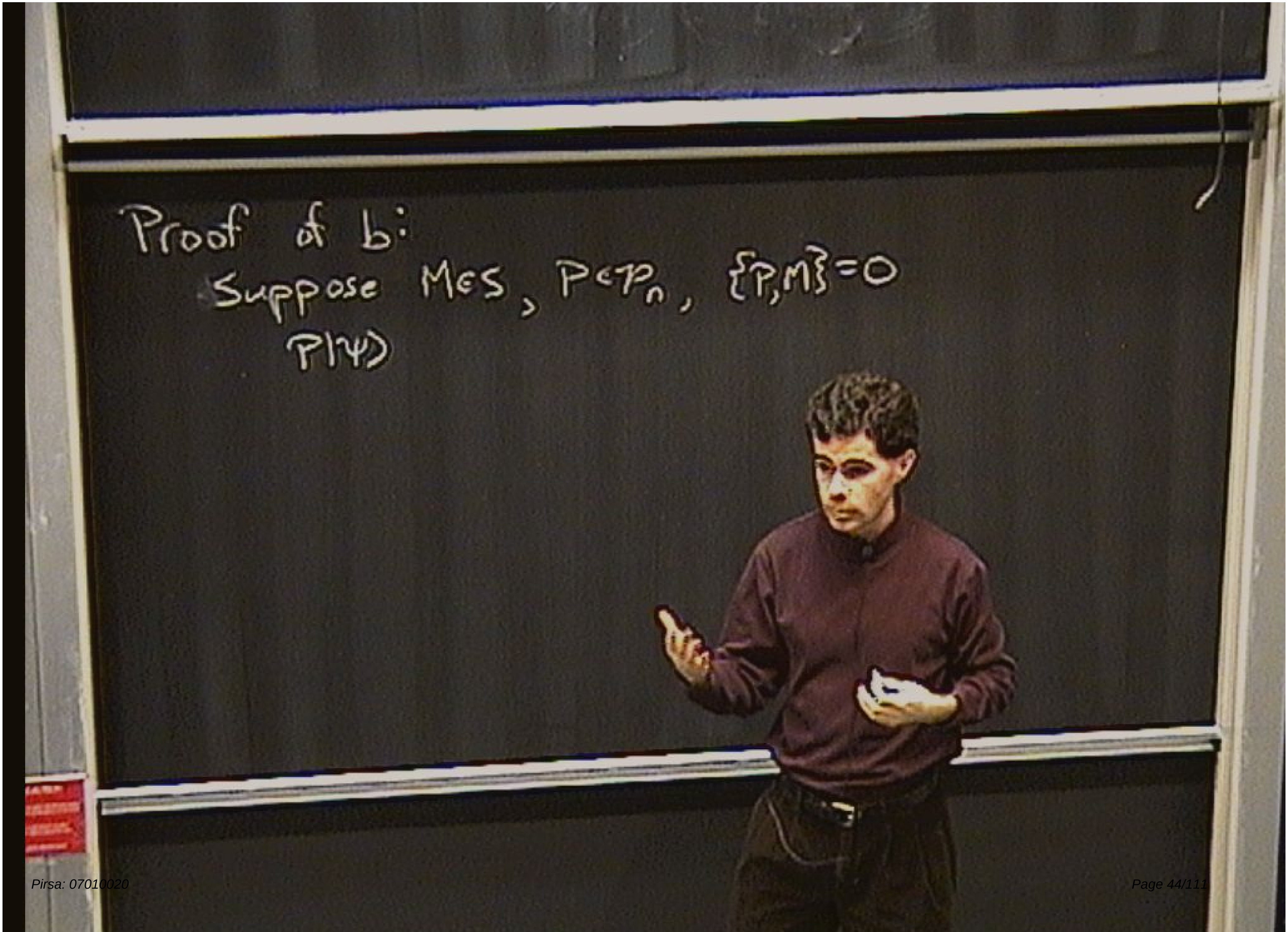
Then S can detect errors outside $N(S) \setminus S$.

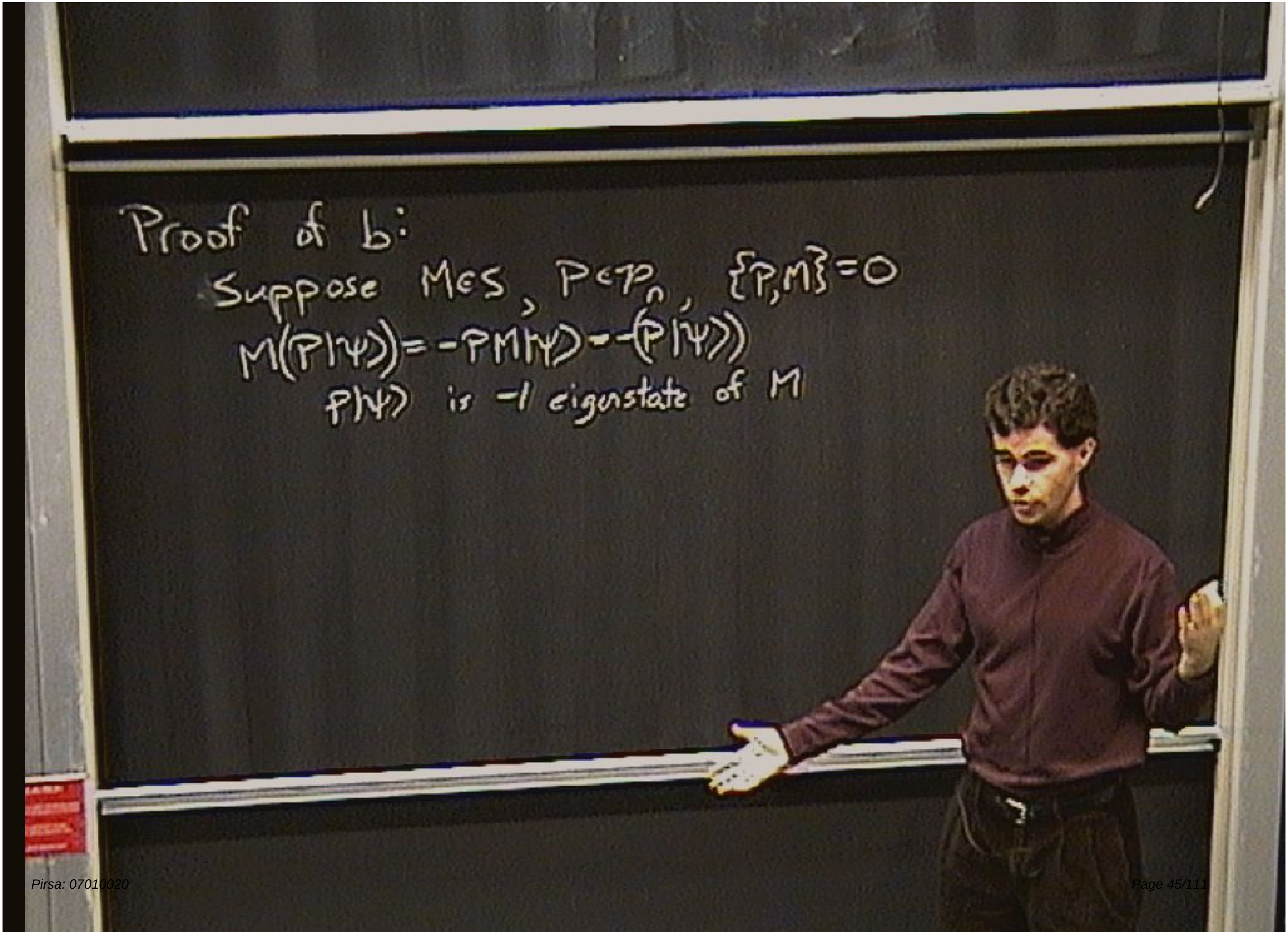
The distance of S is min wt. P, $P \in N(S) \setminus S$

Notation: A QECC encoding a K-dim subspace in n qubits, with distance d, is $((n,K,d))$. A stabilizer code with $K = 2^k$ is $[[n,k,d]]$.


Thm.: Let S be a stabilizer with r generators
on n qubits. Then
a) dim $T(S) = 2^{n-r}$ ($k=n-r$ encoded qubits)
b) Let $N(S) = S^{\perp} = \{P \in \mathcal{P}_n \mid PM=MP \ \forall M \in S\}$.
Then S can detect errors outside $N(S) \setminus S$.
The distance of S is min wt. P, $P \in N(S) \setminus S$
Notation: A QECC encoding a K-dim. subspace in n qubits, with
ce d, is ((n,K,d)). A stabilizer code with $K=2^k$ is [[n,k,d]].

Proof of b:


Proof of b:
Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0$
$P|\psi\rangle$


Proof of b:
Suppose M∈S, P∈𝒫n, {P,M}=0
M(P|ψ⟩) = −PM|ψ⟩ = −(P|ψ⟩)
P|ψ⟩ is −1 eigenstate of M

Proof of b:

Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0$

$M(P|\psi\rangle) = -PM|\psi\rangle = -(P|\psi\rangle)$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n$, $[P, M] = 0$ $\forall M \in S$ $(P \in N(S))$:

$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$

$P|\psi\rangle \in T(S)$

Proof of b:

Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0$

$M(P|\psi\rangle) = -PM|\psi\rangle = -(P|\psi\rangle)$

$P|\psi\rangle$ is -1 eigenstate of M

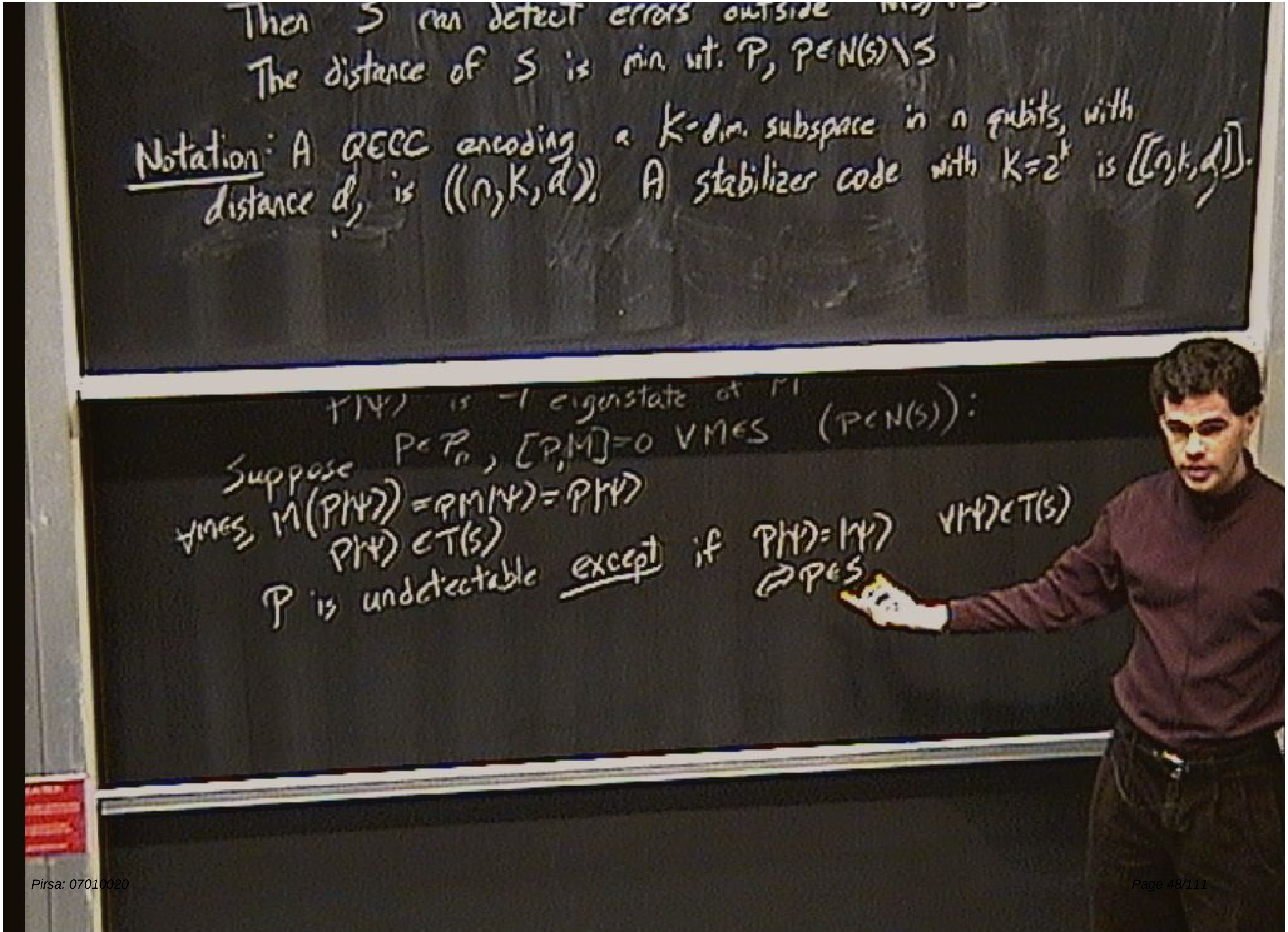
Suppose $P \in \mathcal{P}_n$, $[P, M] = 0$ $\forall M \in S$ $(P \in N(S))$:

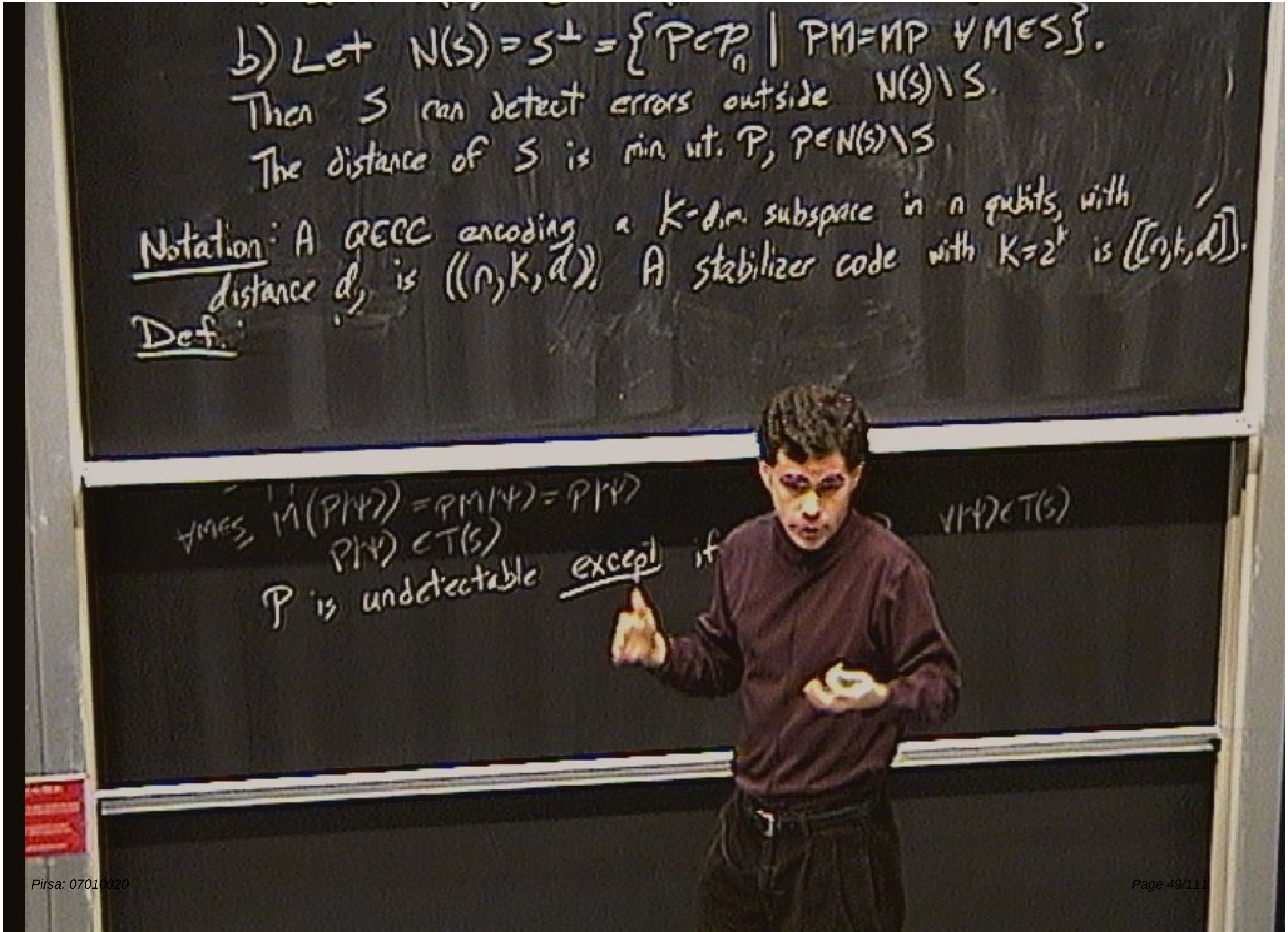
$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$

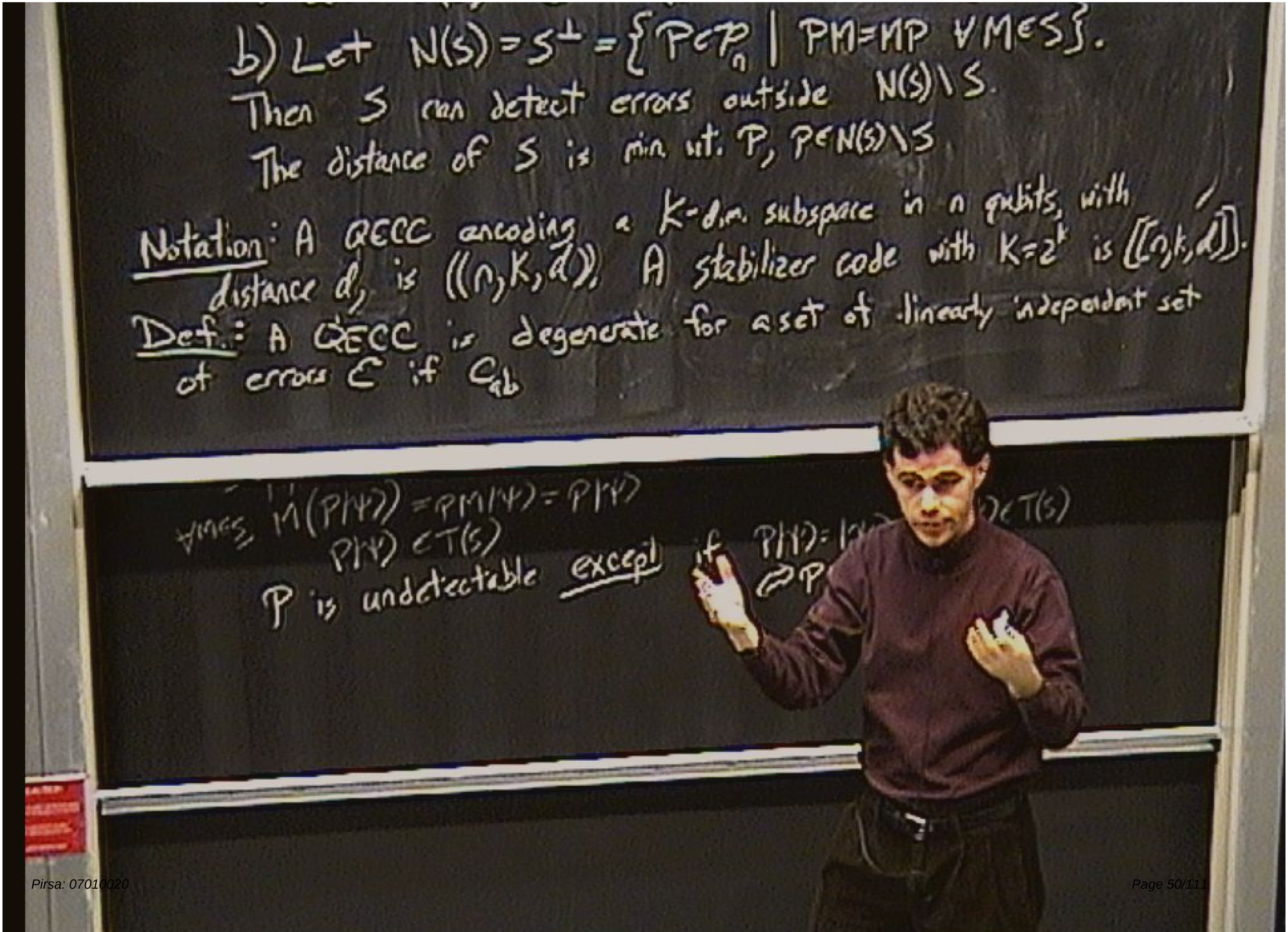
$P|\psi\rangle \in T(S)$

P is undetectable <u>except</u> if $P|\psi\rangle = |\psi\rangle$ $\forall |\psi\rangle \in T(S)$

$\Leftrightarrow P \in S$


Then S can detect errors outside
The distance of S is min wt. P, $P \in N(S) \setminus S$
Notation: A QECC encoding a K-dim. subspace in n qubits, with distance d, is $((n,K,d))$. A stabilizer code with $K=2^k$ is $[[n,k,d]]$.
$P|\psi\rangle$ is -1 eigenstate of M
Suppose $P \in \mathcal{P}_n$, $[P,M]=0$ $\forall M \in S$ $(P \in N(S))$:
$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$
$P|\psi\rangle \in T(S)$
P is undetectable except if $P|\psi\rangle = |\psi\rangle$ $\forall |\psi\rangle \in T(S)$
$\Leftrightarrow P \in S$


b) Let N(S) = S⊥ = {P ∈ 𝒫n | PM = MP ∀M ∈ S}.
Then S can detect errors outside N(S)\S.
The distance of S is min wt. P, P ∈ N(S)\S
Notation: A QECC encoding a K-dim. subspace in n qubits, with distance d, is ((n,K,d)). A stabilizer code with K=2^k is [[n,k,d]].
Def.:
∀M∈S, M(P|ψ⟩) = PM|ψ⟩ = P|ψ⟩
∀|ψ⟩∈T(S)
P|ψ⟩ ∈ T(S)
P is undetectable except if


b) Let N(S) = S^⊥ = { P ∈ P_n | PM = MP ∀ M ∈ S }.
Then S can detect errors outside N(S) \ S.
The distance of S is min wt. P, P ∈ N(S) \ S
Notation: A QECC encoding a K-dim. subspace in n qubits, with distance d, is ((n, K, d)). A stabilizer code with K = 2^k is [[n, k, d]].
Def.: A QECC is degenerate for a set of linearly independent set of errors E if C_ab
∀ M ∈ S, M(P|ψ⟩) = PM|ψ⟩ = P|ψ⟩
P|ψ⟩ ∈ T(S)
P is undetectable except if P|ψ⟩ = |

b) Let $N(S) = S^{\perp} = \{ P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S \}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min wt. P, $P \in N(S) \setminus S$

<u>Notation</u>: A QECC encoding a K-dim. subspace in n qubits, with distance d, is $((n, K, d))$. A stabilizer code with $K = 2^k$ is $[[n, k, d]]$.

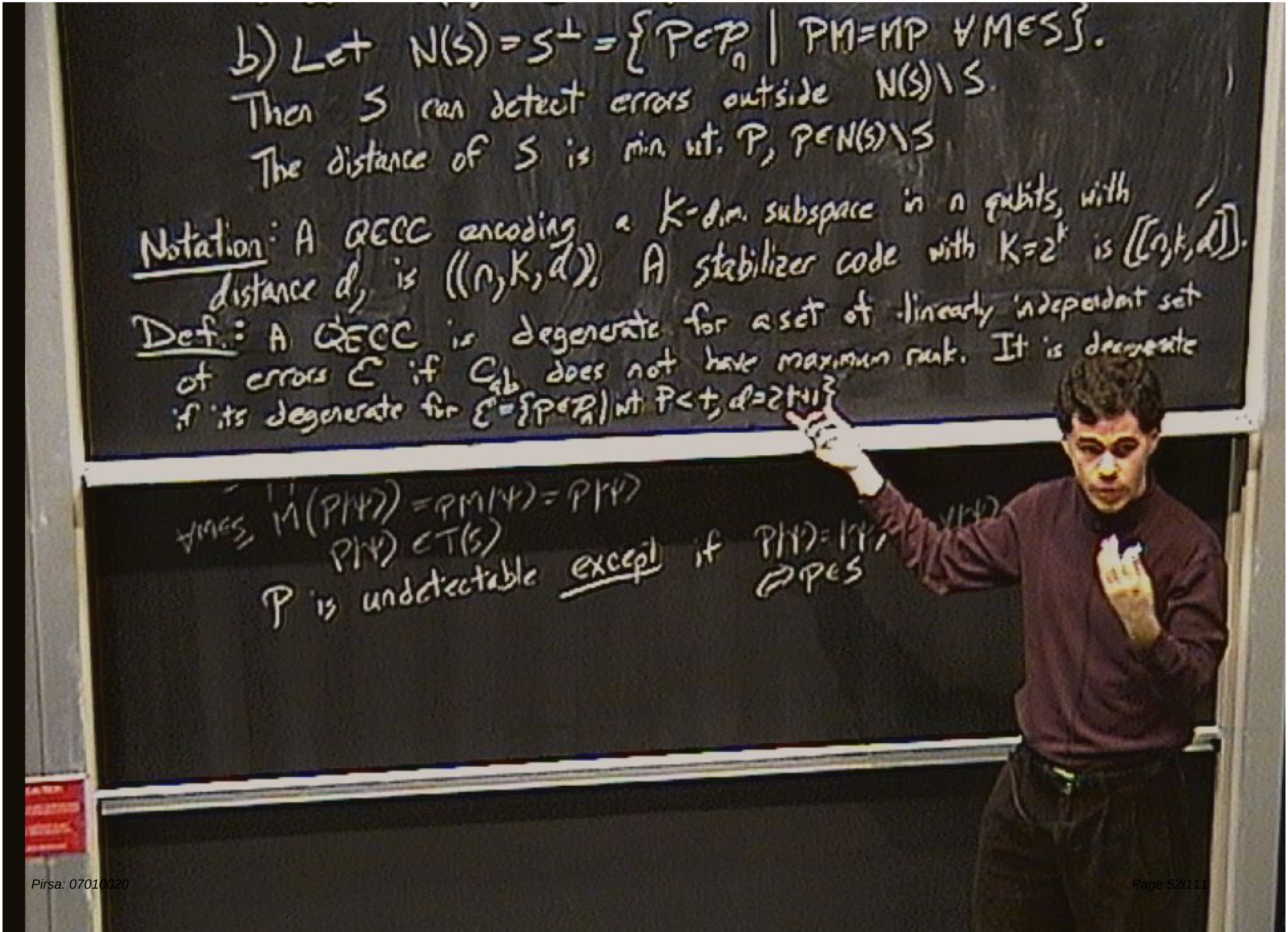
<u>Def.</u>: A QECC is degenerate for a set of linearly independent set of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate

$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$ $\quad \forall |\psi\rangle \in T(S)$

$P|\psi\rangle \in T(S)$

P is undetectable <u>except</u> if $P|\psi\rangle = |\psi\rangle$

$\Leftrightarrow P \in S$


b) Let N(S) = S^⊥ = {P ∈ P_n | PM = MP ∀ M ∈ S}.
Then S can detect errors outside N(S)\S.
The distance of S is min. wt. P, P ∈ N(S)\S
Notation: A QECC encoding a K-dim. subspace in n qubits, with distance d, is ((n,K,d)). A stabilizer code with K=2^k is [[n,k,d]].
Def.: A QECC is degenerate for a set of linearly independent set of errors E if C_ab does not have maximum rank. It is degenerate if its degenerate for E={P∈P_n | wt P < t, d=2t+1}
∀M∈S, M(P|ψ⟩) = PM|ψ⟩ = P|ψ⟩
P|ψ⟩ ∈ T(S)
P is undetectable except if P|ψ⟩ = |ψ⟩
⇔ P∈S

b) Let $N(S) = S^{\perp} = \{ P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S \}$.

Then S can detect errors outside $N(S) \setminus S$.

The distance of S is min. wt. P, $P \in N(S) \setminus S$

Notation: A QECC encoding a K-dim. subspace in n qubits, with distance d, is $((n, K, d))$. A stabilizer code with $K = 2^k$ is $[[n,k,d]]$.

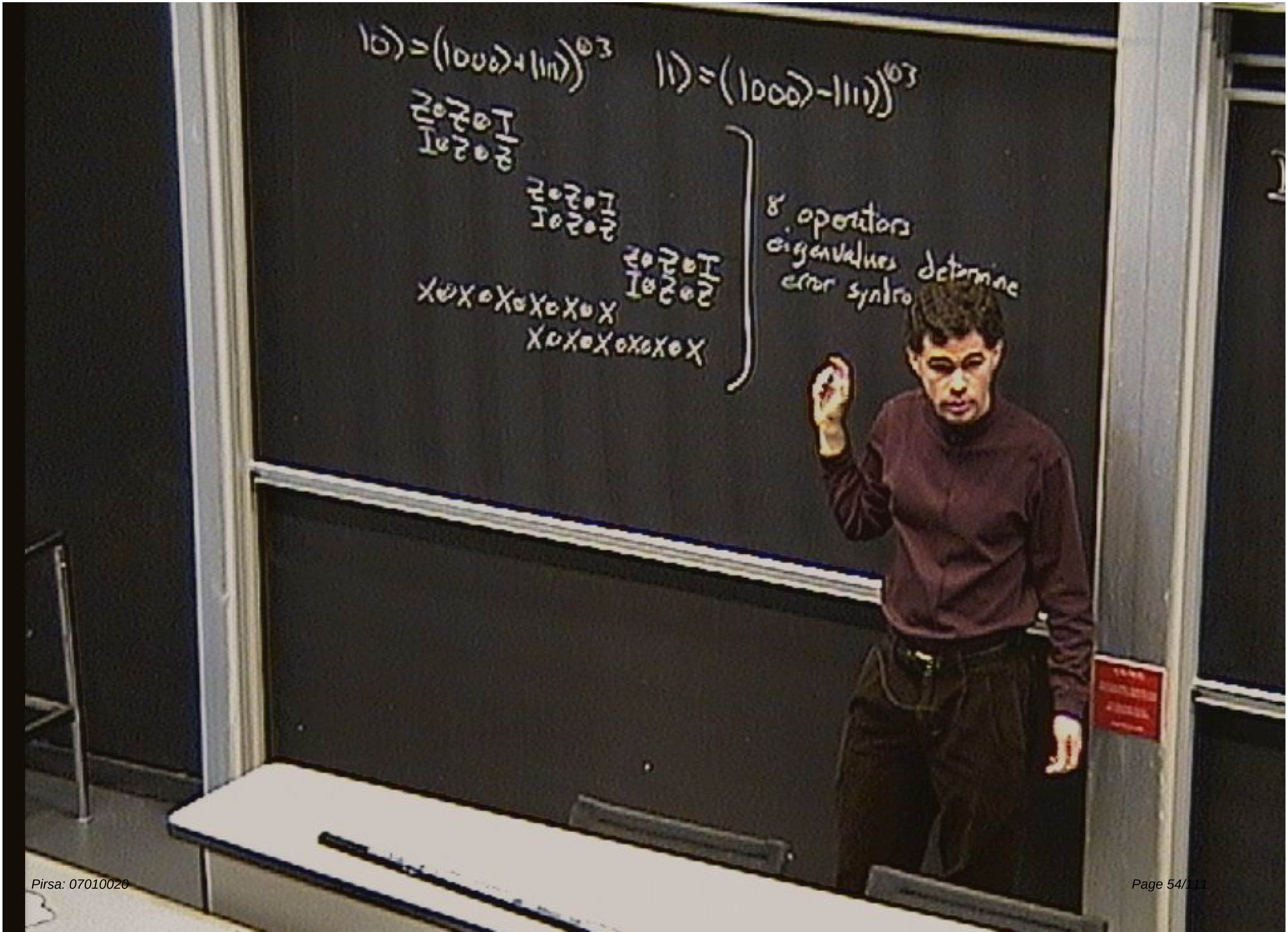
Def.: A QECC is degenerate for a set of linearly independent set of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E} = \{ P \in \mathcal{P}_n \mid \text{wt } P < t, \ d = 2t+1 \}$

$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$

$P|\psi\rangle \in T(S)$

P is undetectable <u>except</u> if $P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in T(S)$

$\Leftrightarrow P \in S$


|0⟩=(|000⟩+|111⟩)⊗3
|1⟩=(|000⟩-|111⟩)⊗3
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
Z⊗Z⊗I
I⊗Z⊗Z
X⊗X⊗X⊗X⊗X⊗X
X⊗X⊗X⊗X⊗X⊗X
8 operators
eigenvalues determine
error syndro

of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E}=\{P\in\mathcal{P}_n \mid wt\,P<t,\ d=2t+1\}$

Proof of b:

Suppose $M\in S$, $P\in\mathcal{P}_n$, $\{P,M\}=0$ $\quad P\notin N(S)$

$M(P|\psi\rangle)=-PM|\psi\rangle=-(P|\psi\rangle)$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P\in\mathcal{P}_n$, $[P,M]=0$ $\forall M\in S$ $\quad (P\in N(S))$:

$\forall M\in S$, $M(P|\psi\rangle)=PM|\psi\rangle=P|\psi\rangle$

$P|\psi\rangle\in T(S)$

P is undetectable except if $P|\psi\rangle=|\psi\rangle$ $\forall|\psi\rangle\in$

$\Leftrightarrow P\in S$

(A stabilizer code is degenerate if $C_{ab}E_b$

of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E}=\{P\in\mathcal{P}_n \mid \text{wt } P<t,\ d=2t+1\}$

Proof of b:

Suppose $M\in S$, $P\in\mathcal{P}_n$, $\{P,M\}=0$ $\quad P\notin N(S)$

$M(P|\psi\rangle)=-PM|\psi\rangle=-(P|\psi\rangle)$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P\in\mathcal{P}_n$, $[P,M]=0$ $\forall M\in S$ $\quad (P\in N(S))$:

$\forall M\in S$, $M(P|\psi\rangle)=PM|\psi\rangle=P|\psi\rangle$

$P|\psi\rangle\in T(S)$

P is undetectable <u>except</u> if $P|\psi\rangle=|\psi\rangle$ $\quad \forall|\psi\rangle\in T(S)$

$\Leftrightarrow P\in S$

(A stabilizer code is degenerate if $E_a^\dagger E_b\in S$ for E_a, E_b distinct correctable errors.

of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate
if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n \mid wt\ P < t,\ d = 2t+1\}$

$$M(P|\psi\rangle) = -PM|\psi\rangle = -(P|\psi\rangle)$$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n$, $[P, M] = 0$ $\forall M \in S$ $(P \in N(S))$:

$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$

$P|\psi\rangle \in T(S)$

P is undetectable <u>except</u> if $P|\psi\rangle = |\psi\rangle$ $\forall |\psi\rangle \in T(S)$

$\Leftrightarrow P \in S$

(A <u>stabilizer</u> code is degenerate if $E_a^\dagger E_b \in S$ for E_a, E_b distinct correctable errors.)

In a non-degenerate stabilizer code, dist = min wt $N(S)$

of errors $\mathcal{E}$ if C_{ab} does not have maximum rank. It is degenerate if its degenerate for $\mathcal{E} = \{P \in \mathcal{P}_n \mid \text{wt } P < t, d = 2t+1\}$

Proof of b:

Suppose $M \in S$, $P \in \mathcal{P}_n$, $\{P, M\} = 0$ $\quad P \notin N(S)$

$M(P|\psi\rangle) = -PM|\psi\rangle = -(P|\psi\rangle)$

$P|\psi\rangle$ is -1 eigenstate of M

Suppose $P \in \mathcal{P}_n$, $[P, M] = 0$ $\forall M \in S$ $\quad (P \in N(S))$:

$\forall M \in S$, $M(P|\psi\rangle) = PM|\psi\rangle = P|\psi\rangle$

$P|\psi\rangle \in T(S)$

P is undetectable except if $P|\psi\rangle = |\psi\rangle$ $\forall |\psi\rangle \in T(S)$
$\Leftrightarrow P \in S$

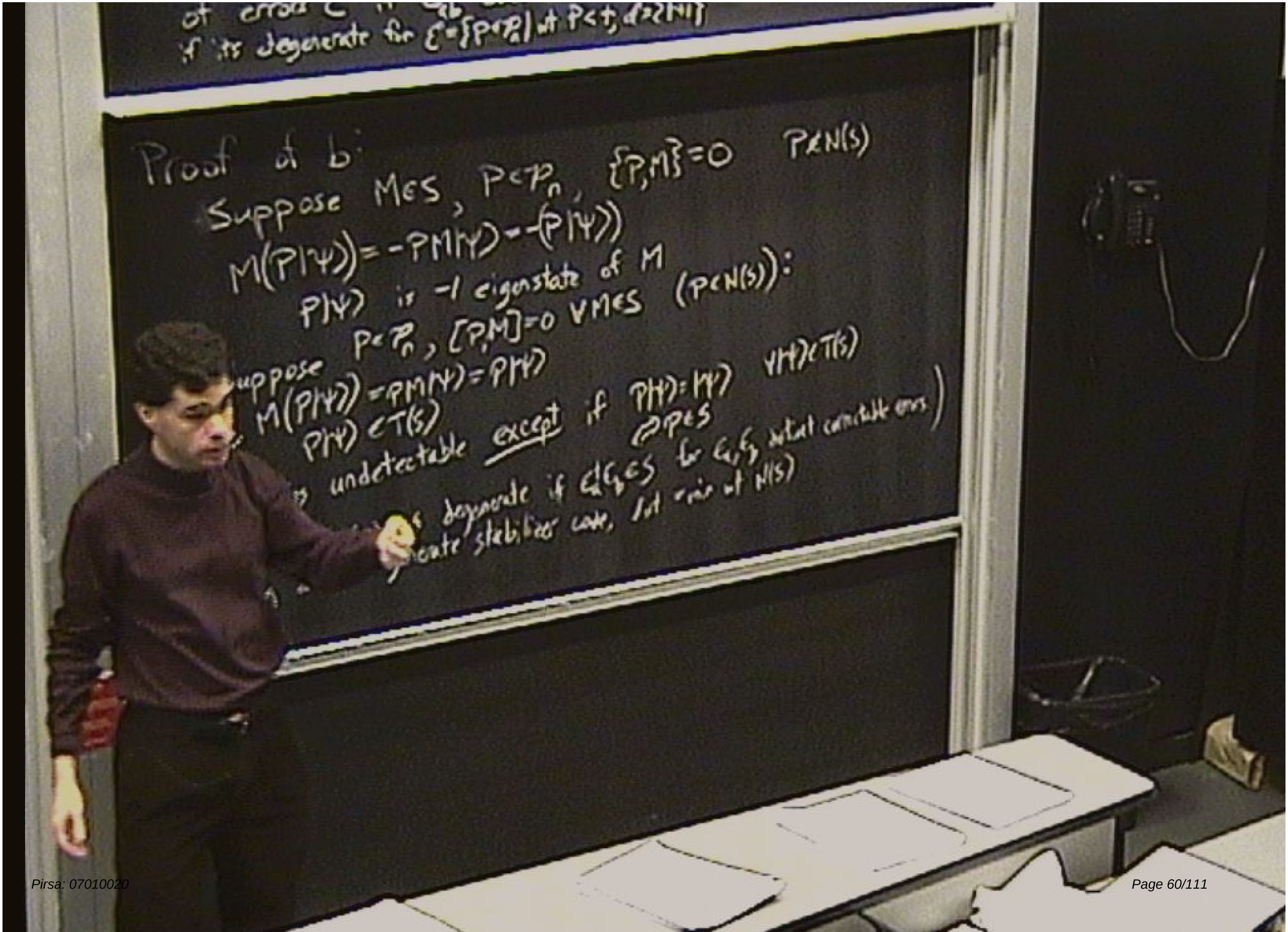
(A stabilizer code is degenerate if $E_a^\dagger E_b \in S$ for E_a, E_b distinct correctable errors.)

In a non-degenerate stabilizer code, $d = \min \text{wt } N(S)$

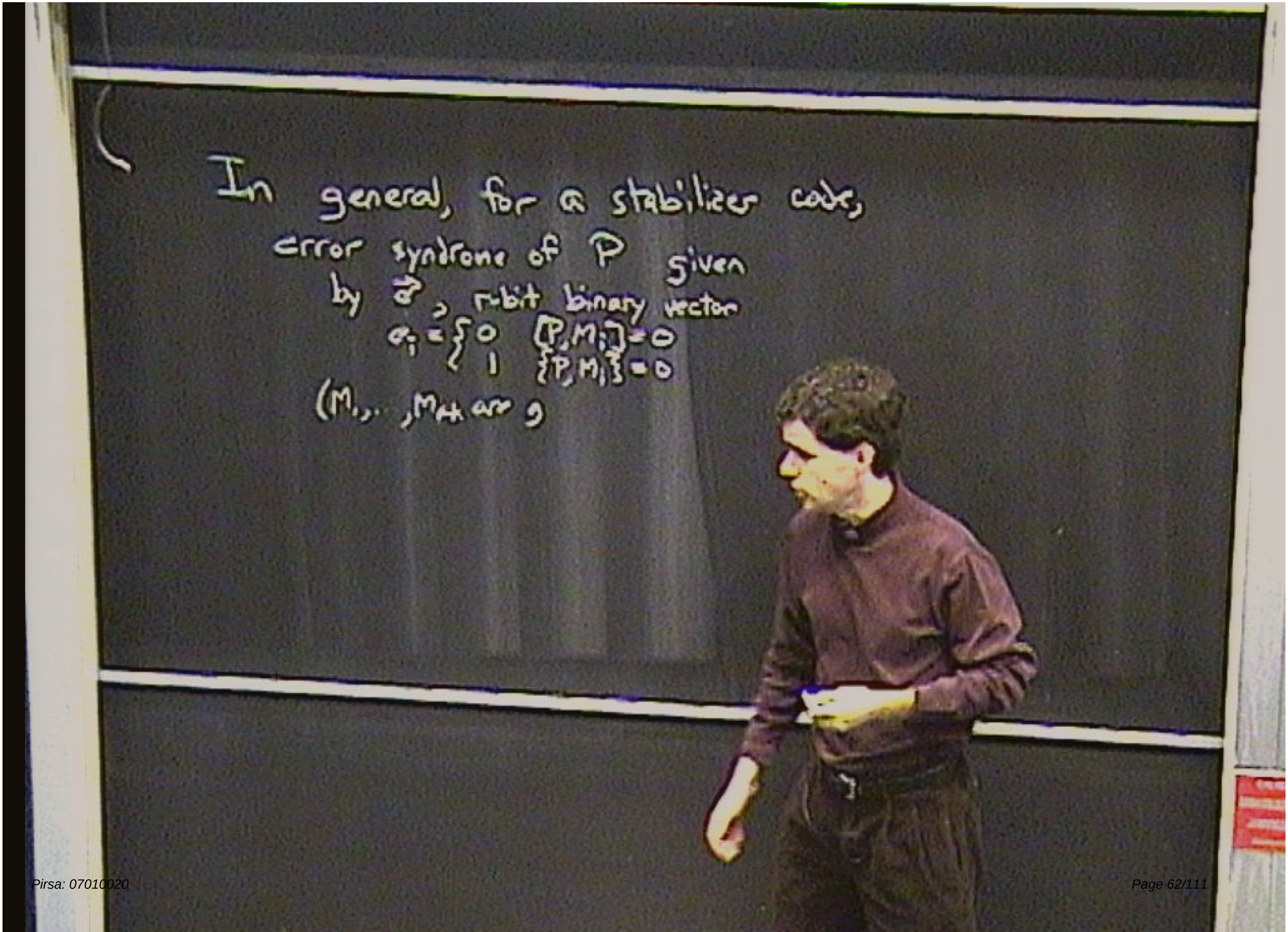
$$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3} \qquad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$$

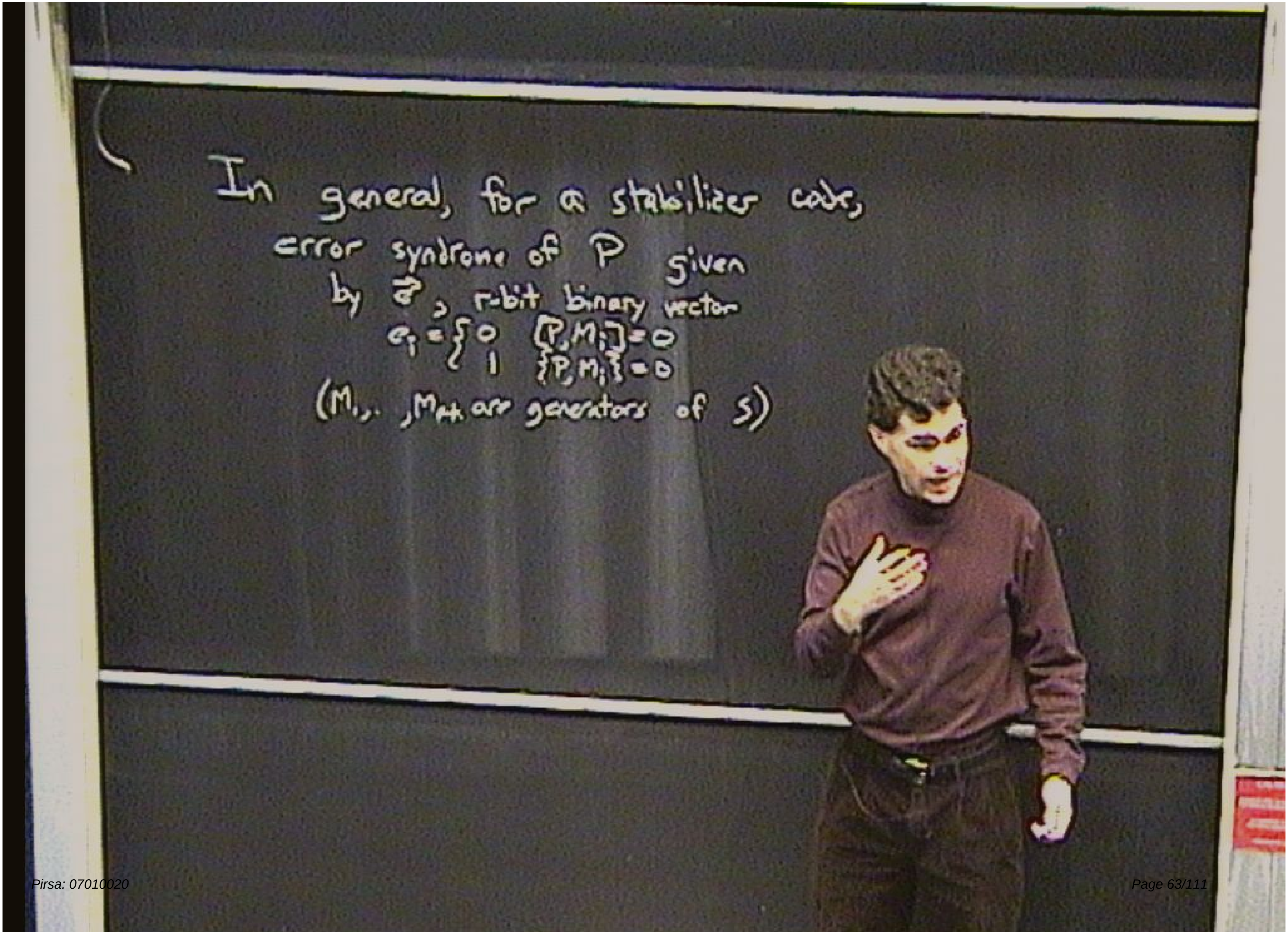
$$\left.\begin{array}{lll}
Z\otimes Z\otimes I & & \\
I\otimes Z\otimes Z & & \\
 & Z\otimes Z\otimes I & \\
 & I\otimes Z\otimes Z & \\
 & & Z\otimes Z\otimes I \\
 & & I\otimes Z\otimes Z \\
X\otimes X\otimes X\otimes X\otimes X\otimes X & & \\
 & X\otimes X\otimes X\otimes X\otimes X\otimes X &
\end{array}\right\}$$

8 operators
eigenvalues determine error syndrome


Proof of b:
Suppose M∈S, P∈P_n, {P,M}=0 P∉N(S)
M(P|ψ⟩)=-PM|ψ⟩=-(P|ψ⟩)
P|ψ⟩ is -1 eigenstate of M
P∈P_n, [P,M]=0 ∀M∈S (P∈N(S)):
Suppose
M(P|ψ⟩)=PM|ψ⟩=P|ψ⟩
P|ψ⟩∈T(S)
undetectable except if P|ψ⟩=|ψ⟩ ∀|ψ⟩∈T(S)
P∈S

In general, for a stabilizer code,
error syndrome of P


In general, for a stabilizer code,
error syndrome of P given
by $\vec{a}$, r-bit binary vector
$a_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & \{P, M_i\} = 0 \end{cases}$
($M_1, \ldots, M_{n-k}$ are g


In general, for a stabilizer code,
error syndrome of P given
by $\vec{e}$, r-bit binary vector
$e_i = \begin{cases} 0 & [P,M_i]=0 \\ 1 & \{P,M_i\}=0 \end{cases}$
($M_1, \ldots, M_{n-k}$ are generators of S)

In general, for a stabilizer code,

error syndrome of P given
by $\vec{e}$, r-bit binary vector

$$e_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & \{P, M_i\} = 0 \end{cases}$$

($M_1, \ldots, M_{n-k}$ are generators of S)

$$\text{Syndrome}(PQ) = \text{Syndrome}(P) + \text{syndrome}(Q)$$

In general, for a stabilizer code,
error syndrome of P given
by $\vec{e}$, r-bit binary vector

$$e_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & \{P, M_i\} = 0 \end{cases}$$

($M_1, \ldots, M_{n-k}$ are generators of S)

Syndrome (PQ) = Syndrome (P) + syndrome (Q) ((binary))

In general, for a stabilizer code,

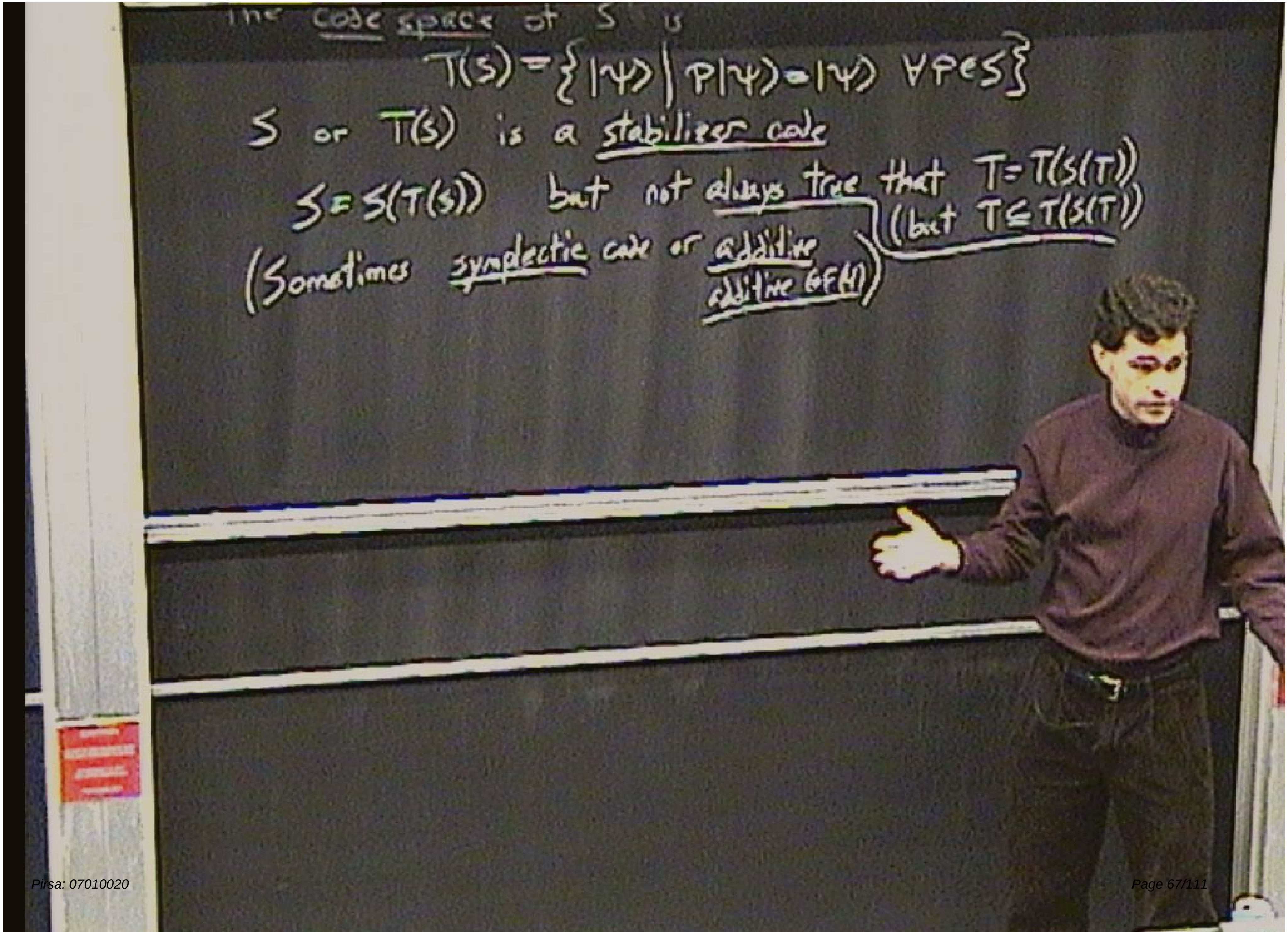
error syndrome of P given by $\vec{a}$, r-bit binary vector

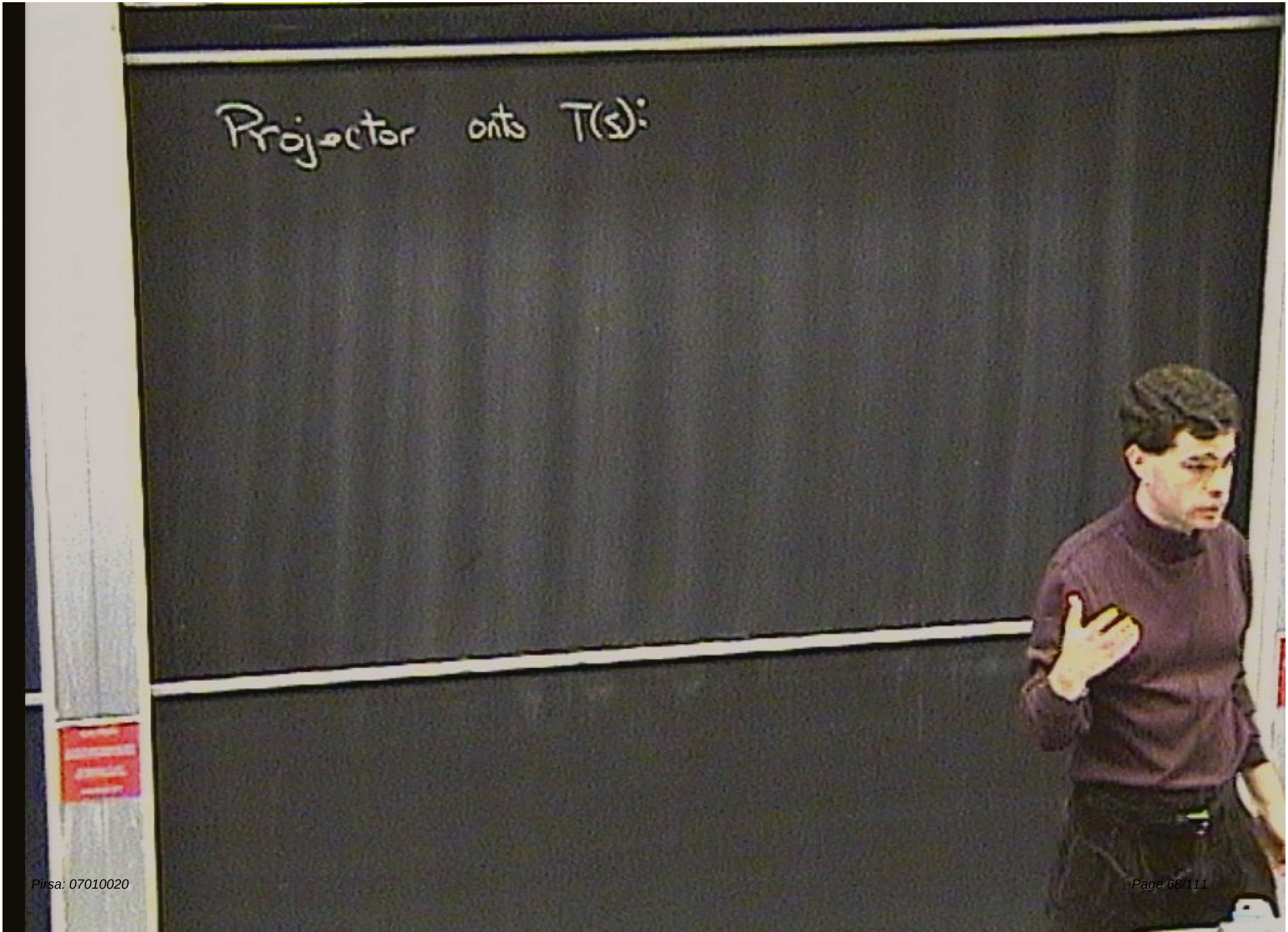
$$a_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & \{P, M_i\} = 0 \end{cases}$$

($M_1, \dots, M_{n-k}$ are generators of S)

$$\text{Syndrome}(PQ) = \text{Syndrome}(P) + \text{syndrome}(Q) \quad (\text{(binary)})$$

$$\text{syndrome } P = \text{syndrome } Q \Leftrightarrow \text{syndrome}(PQ) = 0 \Leftrightarrow PQ \in N(S)$$


The code space of S is
$T(S) = \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S \}$
S or T(S) is a stabilizer code
$S = S(T(S))$ but not always true that $T = T(S(T))$
(but $T \subseteq T(S(T))$)
(Sometimes symplectic code or additive
additive GF(4))


Projector onto T(s):

Projector onto $T(S)^\dagger \Pi_S$:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$:

Projector onto $T(S)$, Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $I+M$

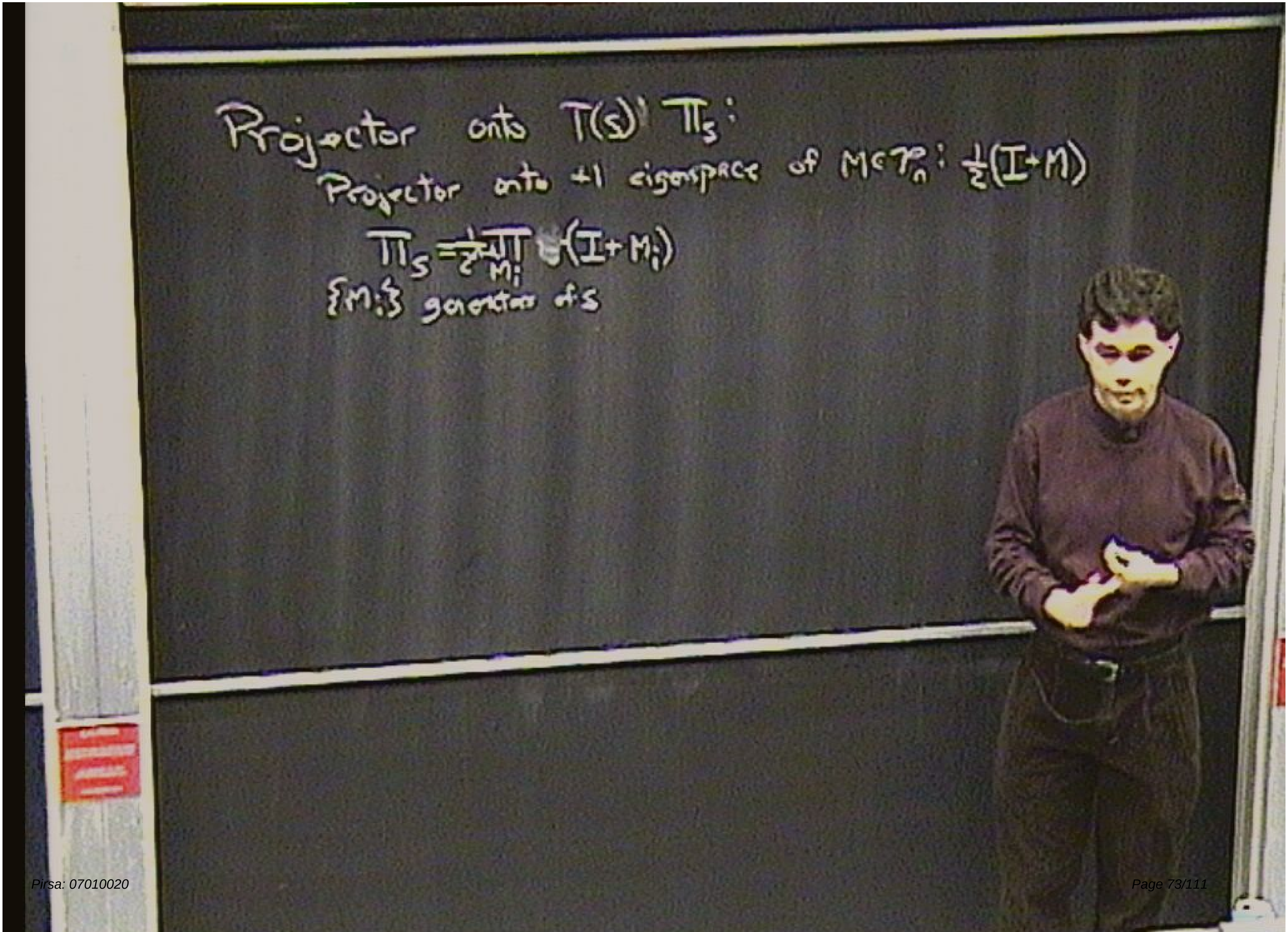
Projector onto $T(S)$ Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

Projector onto $T(S)$: Π_S:

Projector onto $+1$ eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$\Pi_S =$

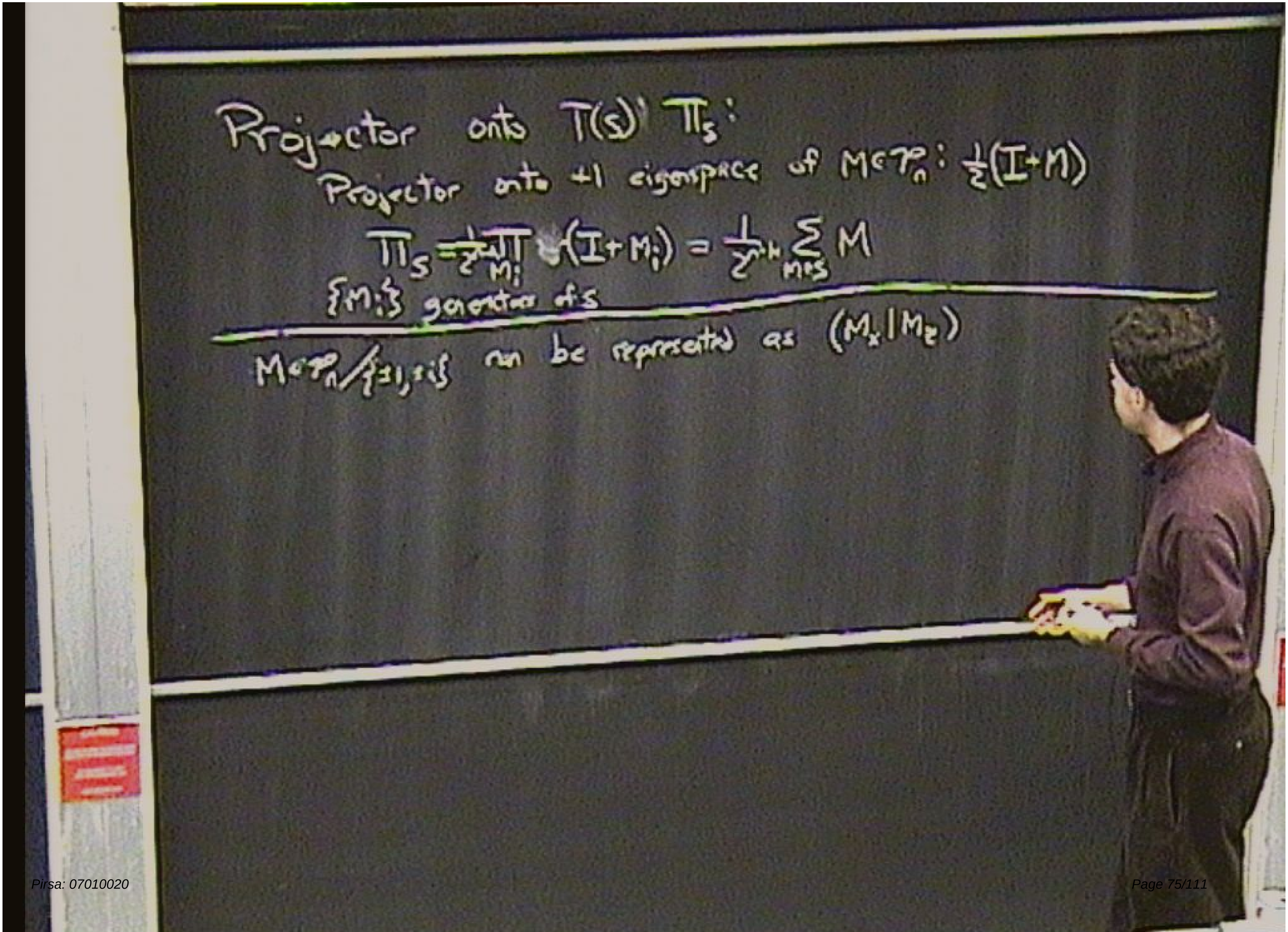

Projector onto $T(S)$: Π_S:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$
$\Pi_S = \prod_{M_i} \frac{1}{2}(I+M_i)$
$\{M_i\}$ generators of S

Projector onto $T(S)$: Π_S:

Projector onto $+1$ eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S


Projector onto $T(S)$: Π_S:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$
$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$\{M_i\}$ generators of S
$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$

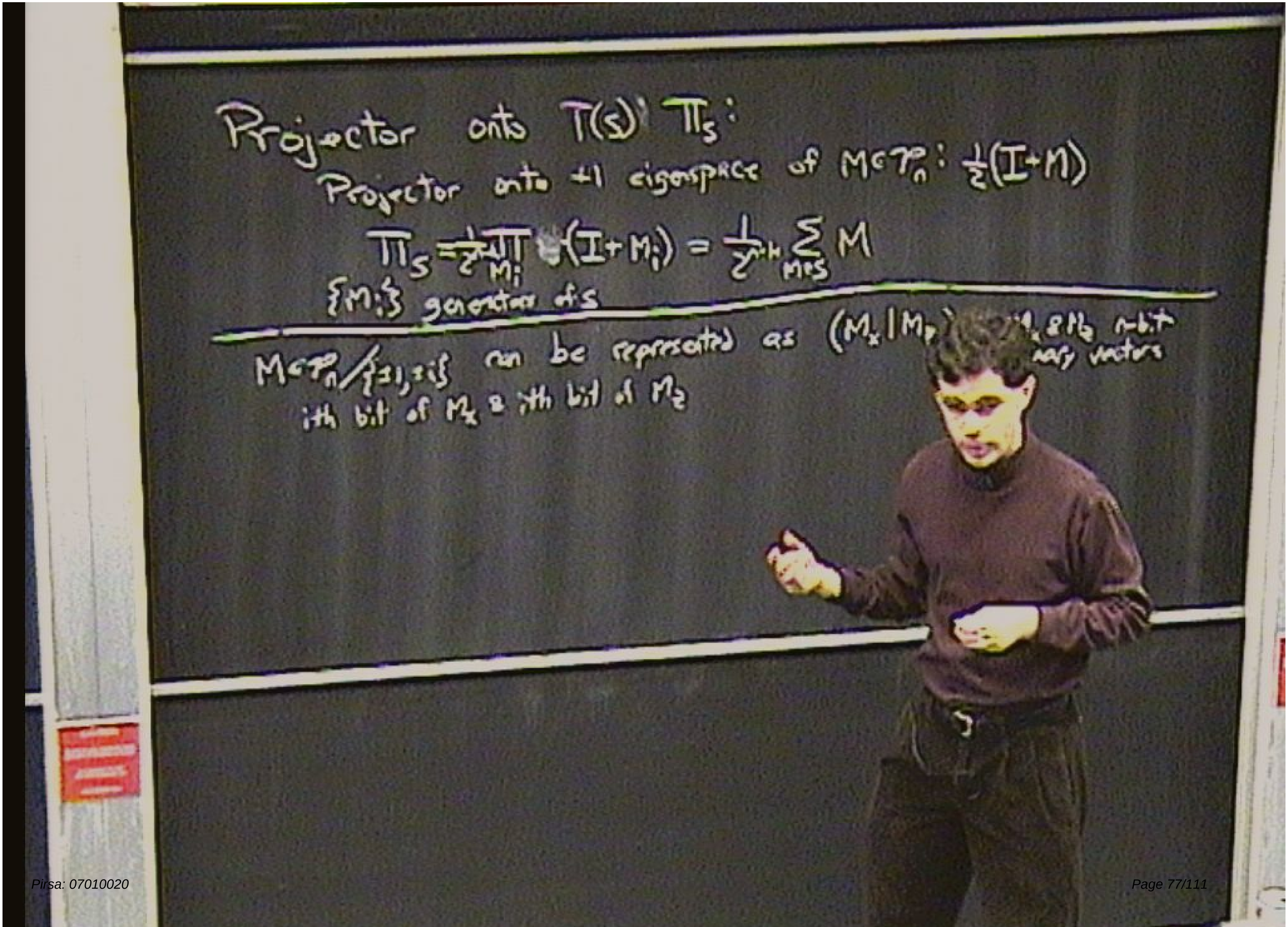
Projector onto $T(S)$: Π_S:

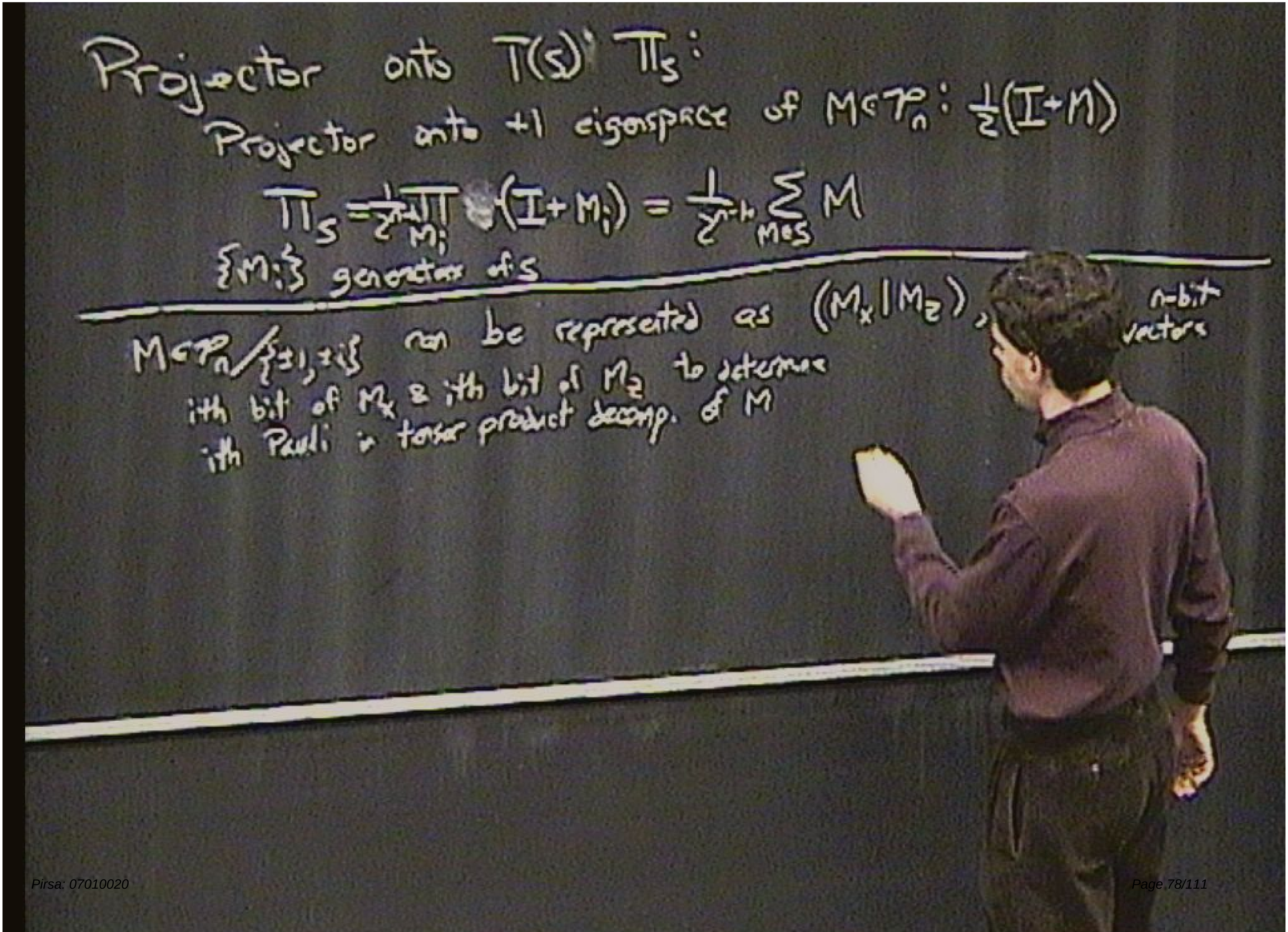
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors


Projector onto T(S): Π_S:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$
$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$\{M_i\}$ generators of S
$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$
M_x & M_z n-bit
vectors
ith bit of M_x & ith bit of M_z


Projector onto $T(S)$: Π_S:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$
$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$\{M_i\}$ generators of S
$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, n-bit vectors
ith bit of M_x & ith bit of M_z to determine
ith Pauli in tensor product decomp. of M

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$(M_x)_i = 1$, $(M_z)_i = 0$ $\Rightarrow X$ in ith position

$\vdots$

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

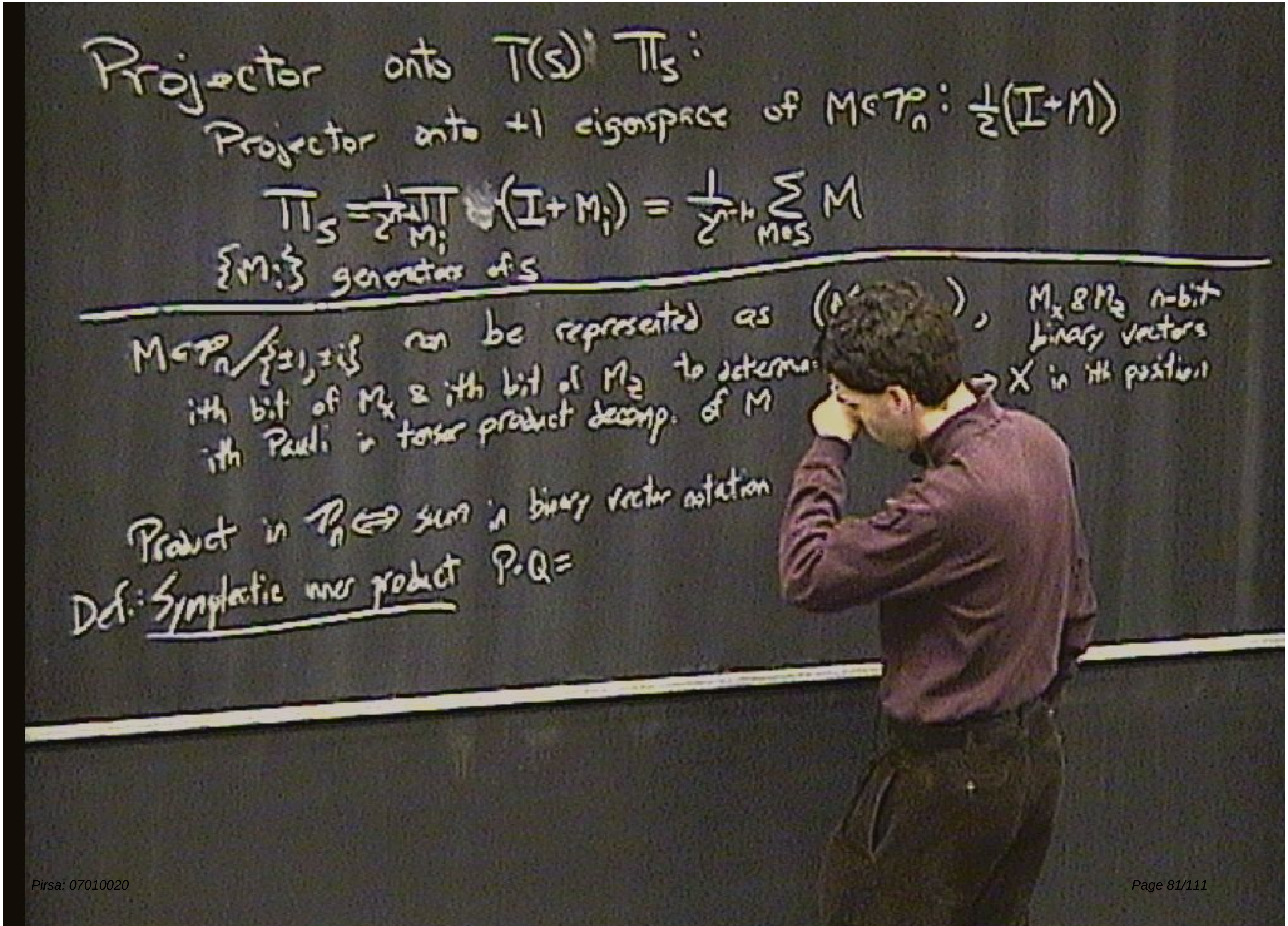
$\{M_i\}$ generators of S

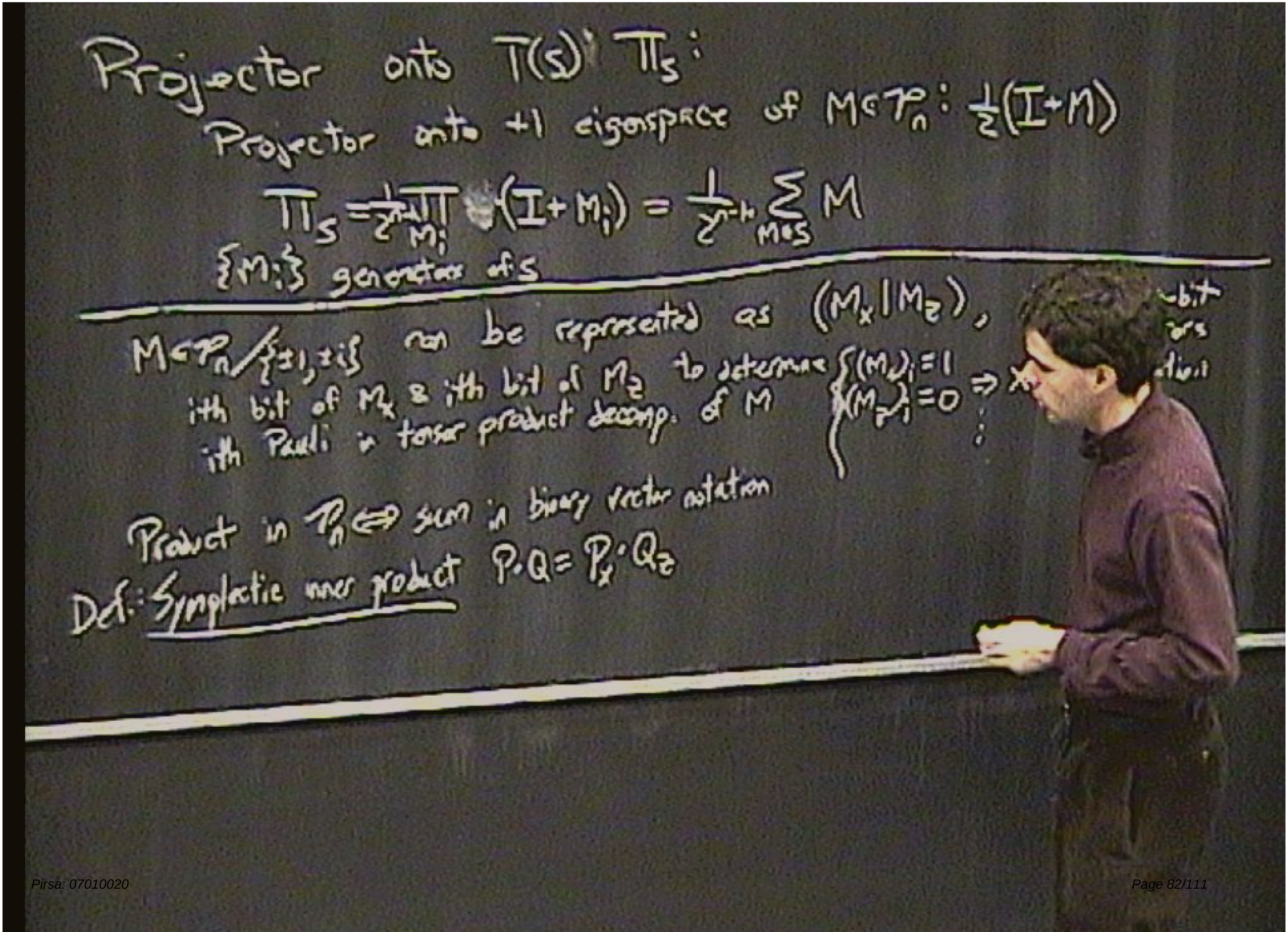
$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$$\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X \text{ in ith position} \quad \vdots$$

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation


Projector onto T(S): Π_S:
Projector onto +1 eigenspace of M∈P_n: ½(I+M)
Π_S = ½ⁿ⁻ᵏ... ∏_{M_i} (I+M_i) = 1/2^{n-k} Σ_{M∈S} M
{M_i} generators of S
M∈P_n/{±1,±i} can be represented as ( ), M_x & M_z n-bit binary vectors
ith bit of M_x & ith bit of M_z to determine
X in ith position
ith Pauli in tensor product decomp. of M
Product in P_n ⟺ sum in binary vector notation
Def.: Symplectic inner product P·Q=


Projector onto $T(S)$: Π_S:
Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$
$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$\{M_i\}$ generators of S
$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$,
ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M
$(M_x)_i = 1$, $(M_z)_i = 0 \Rightarrow X$
Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation
Def: Symplectic inner product $P \cdot Q = P_x \cdot Q_z$

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \Rightarrow X \text{ in ith position} \\ \vdots \end{cases}$

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

Def.: Symplectic inner product $P \cdot Q = P_x \cdot Q_z + Q_x \cdot P_z$

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$(M_x)_i = 1$, $(M_z)_i = 0$ $\Rightarrow X$ in ith position

⋮

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

$(P_x | P_z)$

$(Q_x | Q_z)$

Def.: Symplectic inner product $P \cdot Q = P_x \cdot Q_z + Q_x \cdot P_z$

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I+M_i) = \frac{1}{2^{n-k}} \sum_{M\in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n/\{\pm 1, \pm i\}$ can be represented as $(M_x|M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$$\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \\ \vdots \end{cases} \Rightarrow X \text{ in ith position}$$

Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

$(P_x|P_z)$

$(Q_x|Q_z)$

Def: Symplectic inner product $P\cdot Q = P_x\cdot Q_z + Q_x\cdot P_z$ (mod 2 arithmetic)

Projector onto $T(S)$: Π_S:

Projector onto +1 eigenspace of $M \in \mathcal{P}_n$: $\frac{1}{2}(I+M)$

$$\Pi_S = \frac{1}{2^{n-k}} \prod_{M_i} (I + M_i) = \frac{1}{2^{n-k}} \sum_{M \in S} M$$

$\{M_i\}$ generators of S

$M \in \mathcal{P}_n / \{\pm 1, \pm i\}$ can be represented as $(M_x | M_z)$, M_x & M_z n-bit binary vectors

ith bit of M_x & ith bit of M_z to determine ith Pauli in tensor product decomp. of M

$\begin{cases} (M_x)_i = 1 \\ (M_z)_i = 0 \end{cases} \Rightarrow X$ in ith position

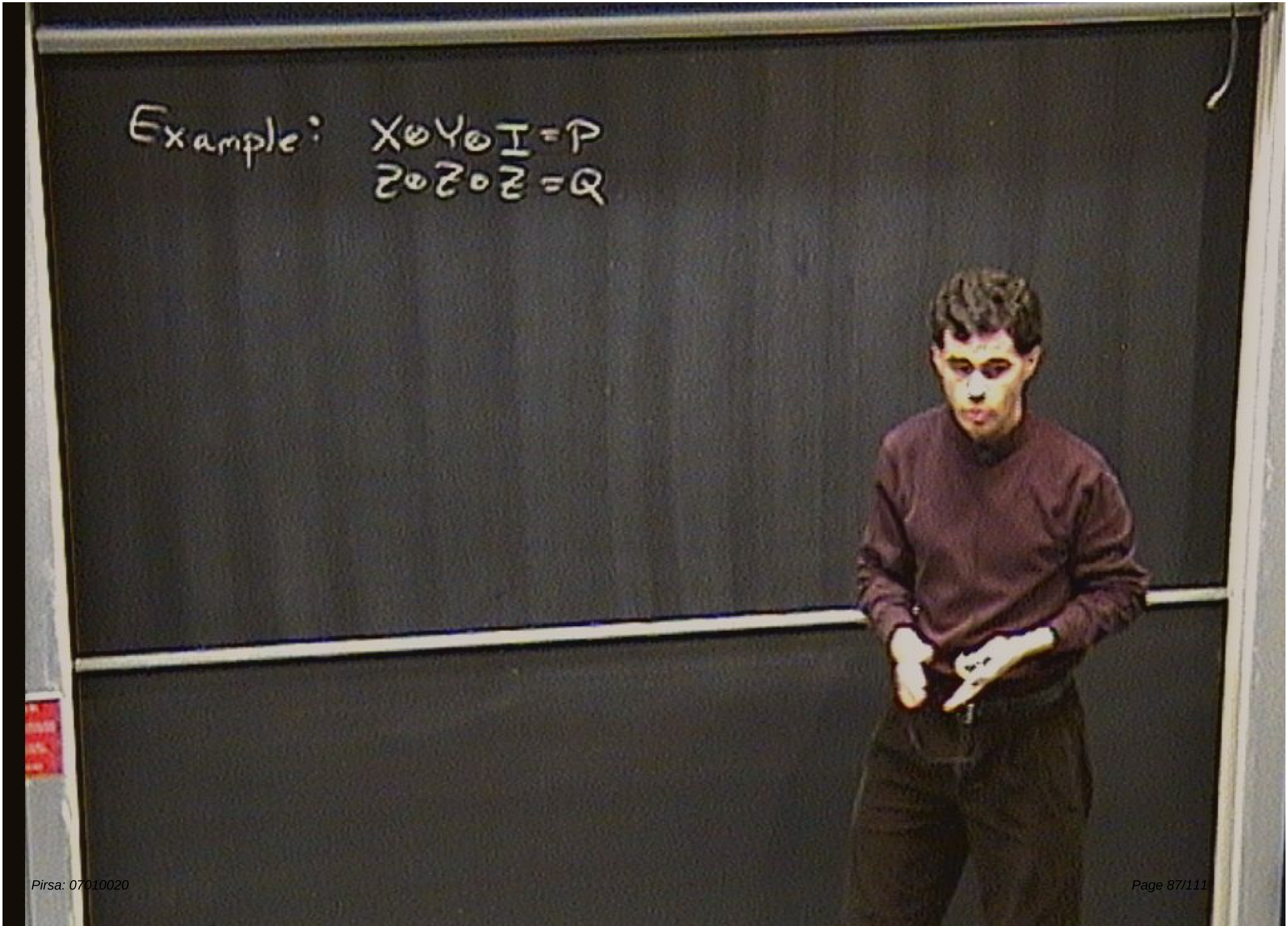
Product in $\mathcal{P}_n \Leftrightarrow$ sum in binary vector notation

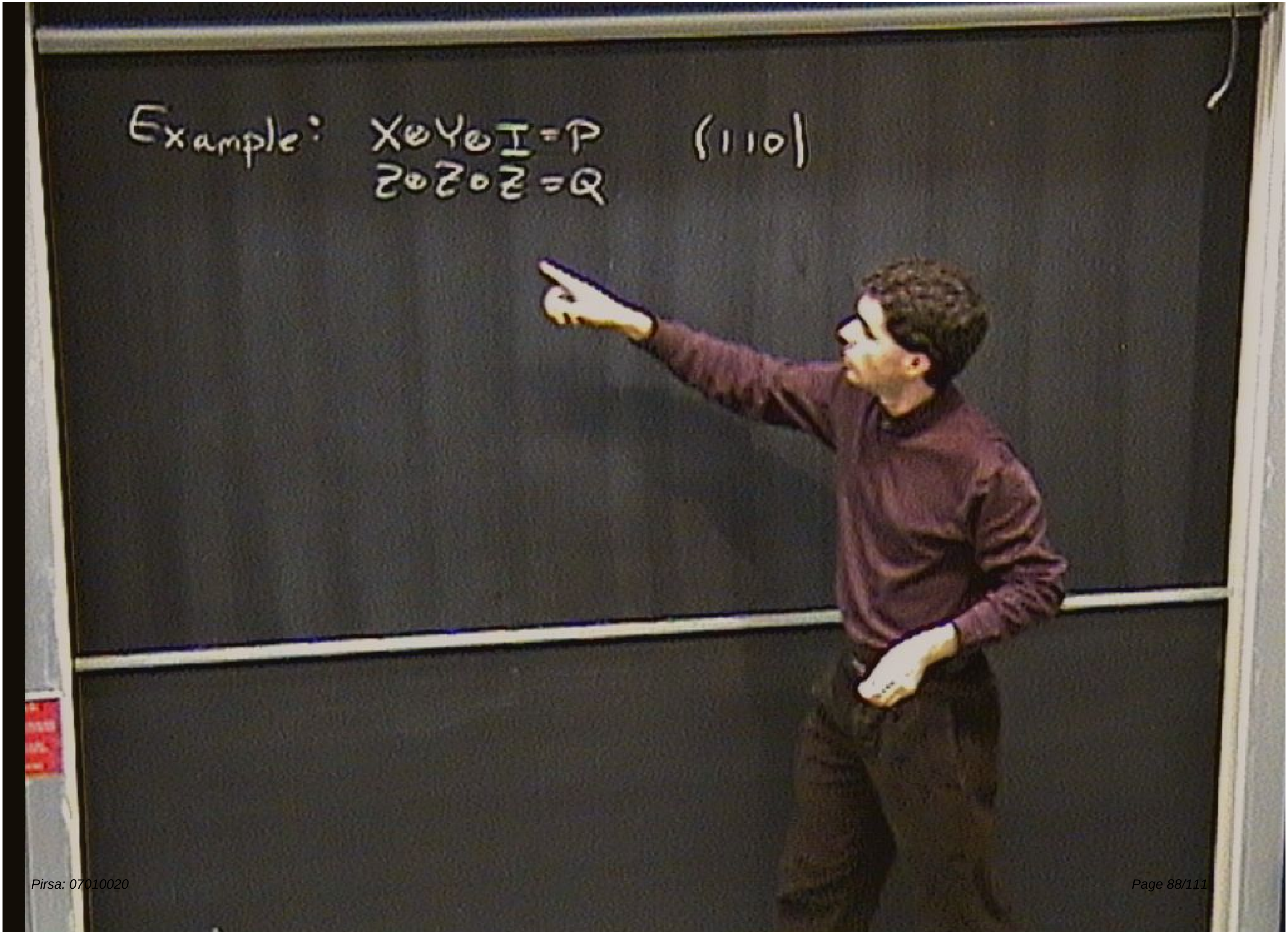
$(P_x | P_z)$

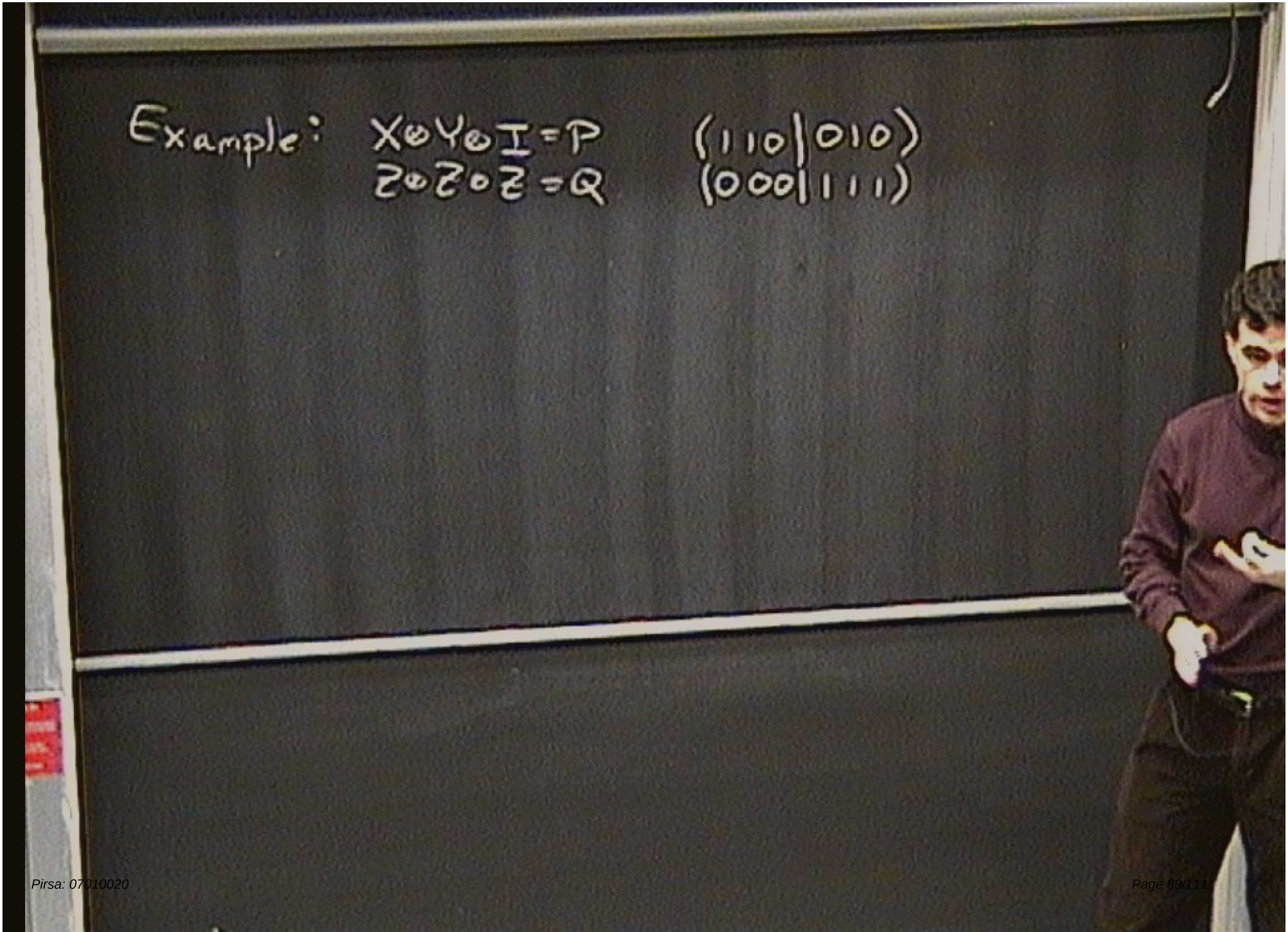
$(Q_x | Q_z)$

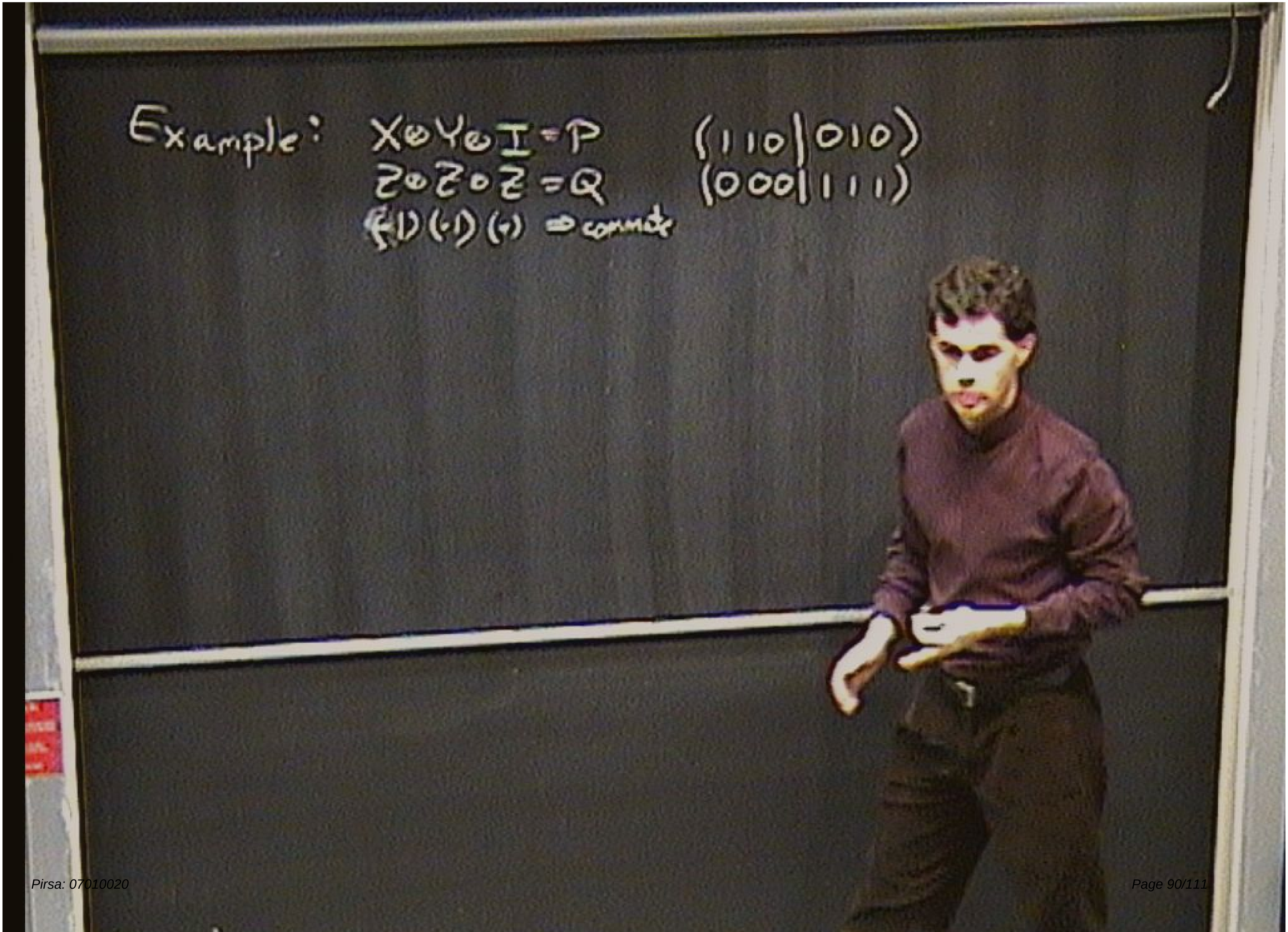
Def.: Symplectic inner product $P \cdot Q = P_x \cdot Q_z + Q_x \cdot P_z$ (mod 2 arithmetic)

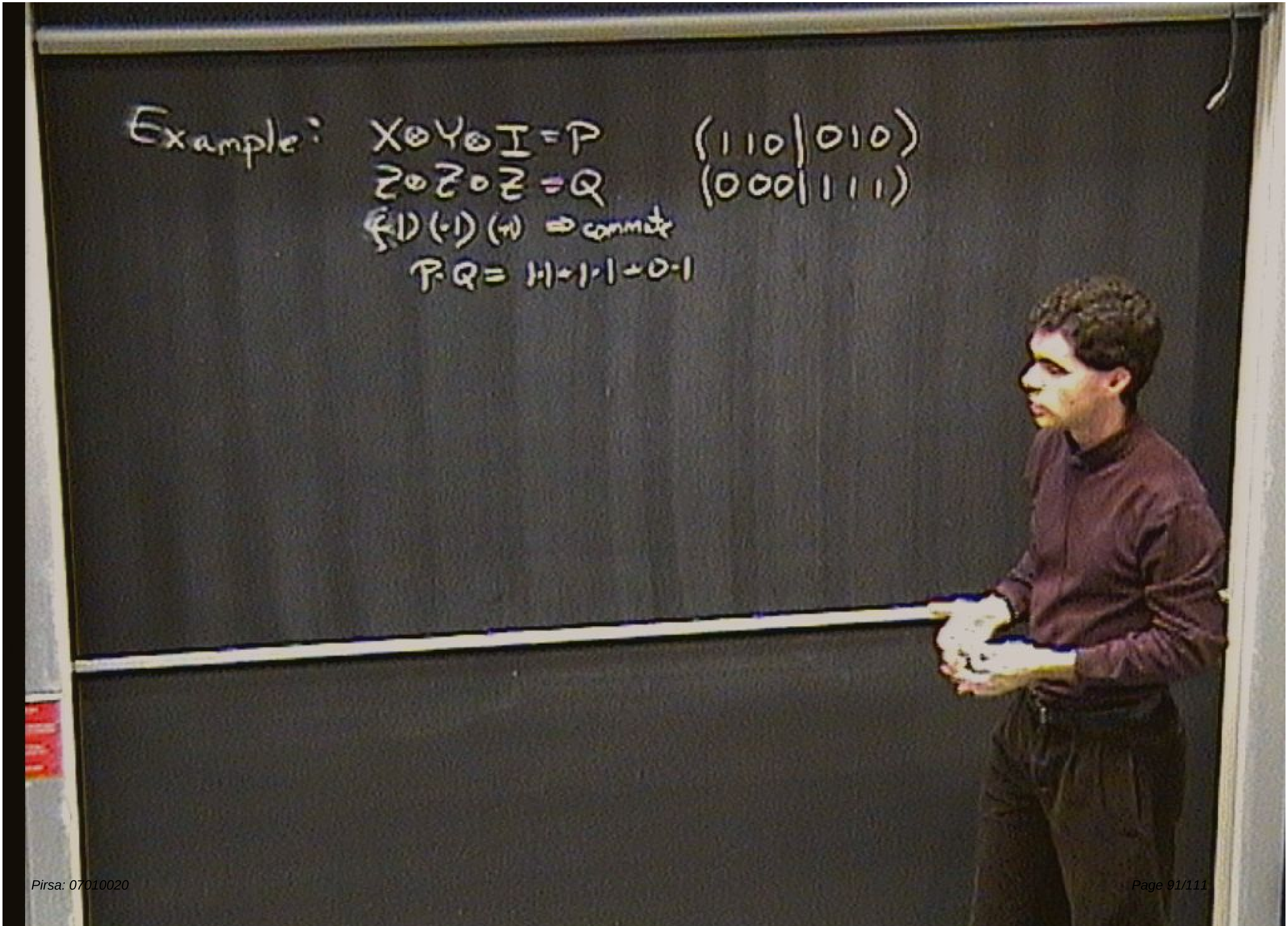
$P \cdot Q = 0$ iff $[P, Q] = 0$

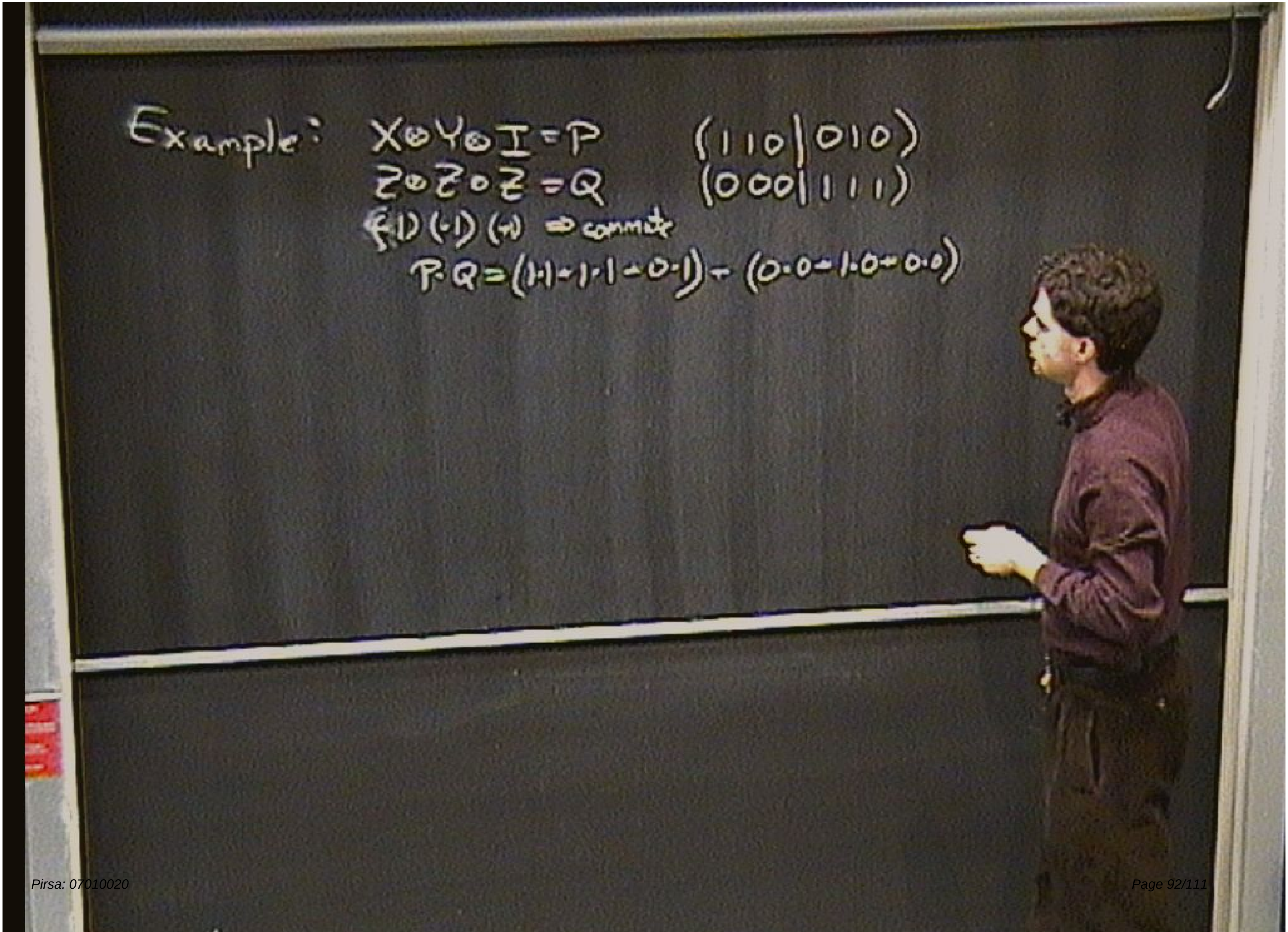

Example: $X \otimes Y \otimes I = P$
$Z \otimes Z \otimes Z = Q$

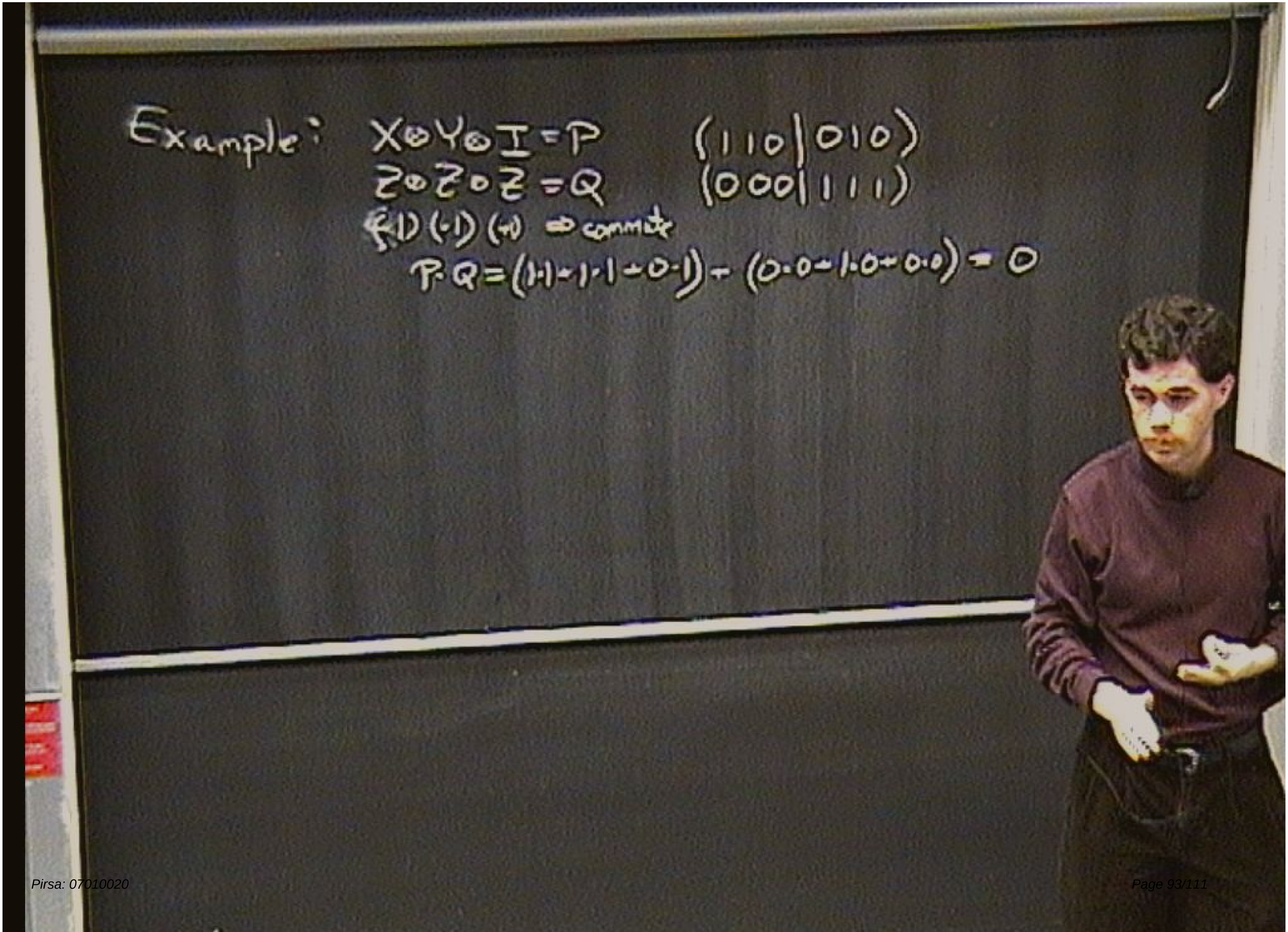

Example: X⊗Y⊗I = P (1110|
Z⊗Z⊗Z = Q


Example: X⊗Y⊗I = P (110|010)
Z⊗Z⊗Z = Q (000|111)


Example: X⊗Y⊗I = P
(1 1 0 | 0 1 0)
Z⊗Z⊗Z = Q
(0 0 0 | 1 1 1)
(-1)(-1)(+) ⇒ commute


Example: X⊗Y⊗I = P (110|010)
Z⊗Z⊗Z = Q (000|111)
(-1)(-1)(+1) ⇒ commute
P·Q = 1·1 + 1·1 + 0·1


Example: $X \otimes Y \otimes I = P$ $(1 1 0 | 0 1 0)$
$Z \otimes Z \otimes Z = Q$ $(0 0 0 | 1 1 1)$
$(-1)(-1)(-1) \Rightarrow$ commute
$P \cdot Q = (1\cdot1 + 1\cdot1 + 0\cdot1) + (0\cdot0 + 1\cdot0 + 0\cdot0)$


Example: $X \otimes Y \otimes I = P$ $(1\,1\,0 \mid 0\,1\,0)$
$Z \otimes Z \otimes Z = Q$ $(0\,0\,0 \mid 1\,1\,1)$
$(-1)(-1)(+1) \Rightarrow$ commute
$P \cdot Q = (1\cdot1 + 1\cdot1 + 0\cdot1) + (0\cdot0 + 1\cdot0 + 0\cdot0) = 0$

Example: $X \otimes Y \otimes I = P$ $\quad (1\,1\,0 \mid 0\,1\,0)$

$Z \otimes Z \otimes Z = Q$ $\quad (0\,0\,0 \mid 1\,1\,1)$

$(-1)(-1)(+1) \Rightarrow$ commute

$P \cdot Q = (1\cdot1 + 1\cdot1 + 0\cdot1) + (0\cdot0 + 1\cdot0 + 0\cdot0) = 0$

Proof of b:

<u>Lemma</u>:

Example: $X \otimes Y \otimes I = P \qquad (1\,1\,0 \mid 0\,1\,0)$

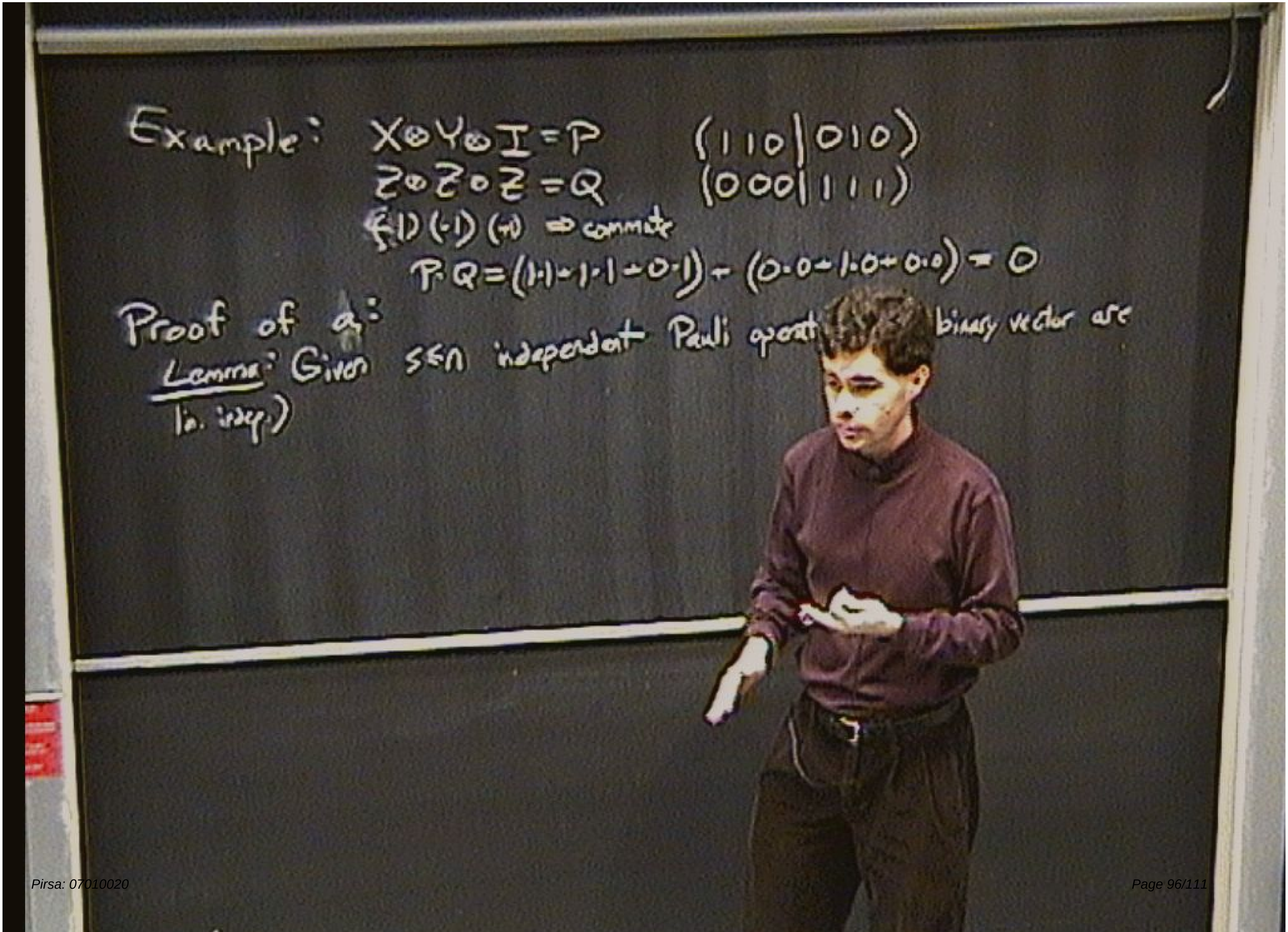
$Z \otimes Z \otimes Z = Q \qquad (0\,0\,0 \mid 1\,1\,1)$

$(-1)(-1)(+1) \Rightarrow$ commute

$$P \cdot Q = (1\cdot 1 + 1\cdot 1 + 0\cdot 1) + (0\cdot 0 + 1\cdot 0 + 0\cdot 0) = 0$$

Proof of a:

Lemma: Given $s \leq n$ independent Pauli operators


Example: X⊗Y⊗I = P (1 1 0 | 0 1 0)
Z⊗Z⊗Z = Q (0 0 0 | 1 1 1)
(-1) (-1) (+1) ⇒ commute
P·Q = (1·1 + 1·1 + 0·1) + (0·0 + 1·0 + 0·0) = 0
Proof of a:
Lemma: Given s≤n independent Pauli operat… binary vector are
(lin. indep.)

Example: $X \otimes Y \otimes I = P \qquad (1\,1\,0 \mid 0\,1\,0)$

$Z \otimes Z \otimes Z = Q \qquad (0\,0\,0 \mid 1\,1\,1)$

$(-1)(-1)(+1) \Rightarrow$ commute

$$P \cdot Q = (1\cdot 1 + 1\cdot 1 + 0\cdot 1) + (0\cdot 0 + 1\cdot 0 + 0\cdot 0) = 0$$

Proof of a_i:

Lemma: Given $s \le n$ independent Pauli operators (i.e. binary vector are lin. indep.), vector z (s bits)

Example: $X \otimes Y \otimes I = P \qquad (1\,1\,0 \mid 0\,1\,0)$

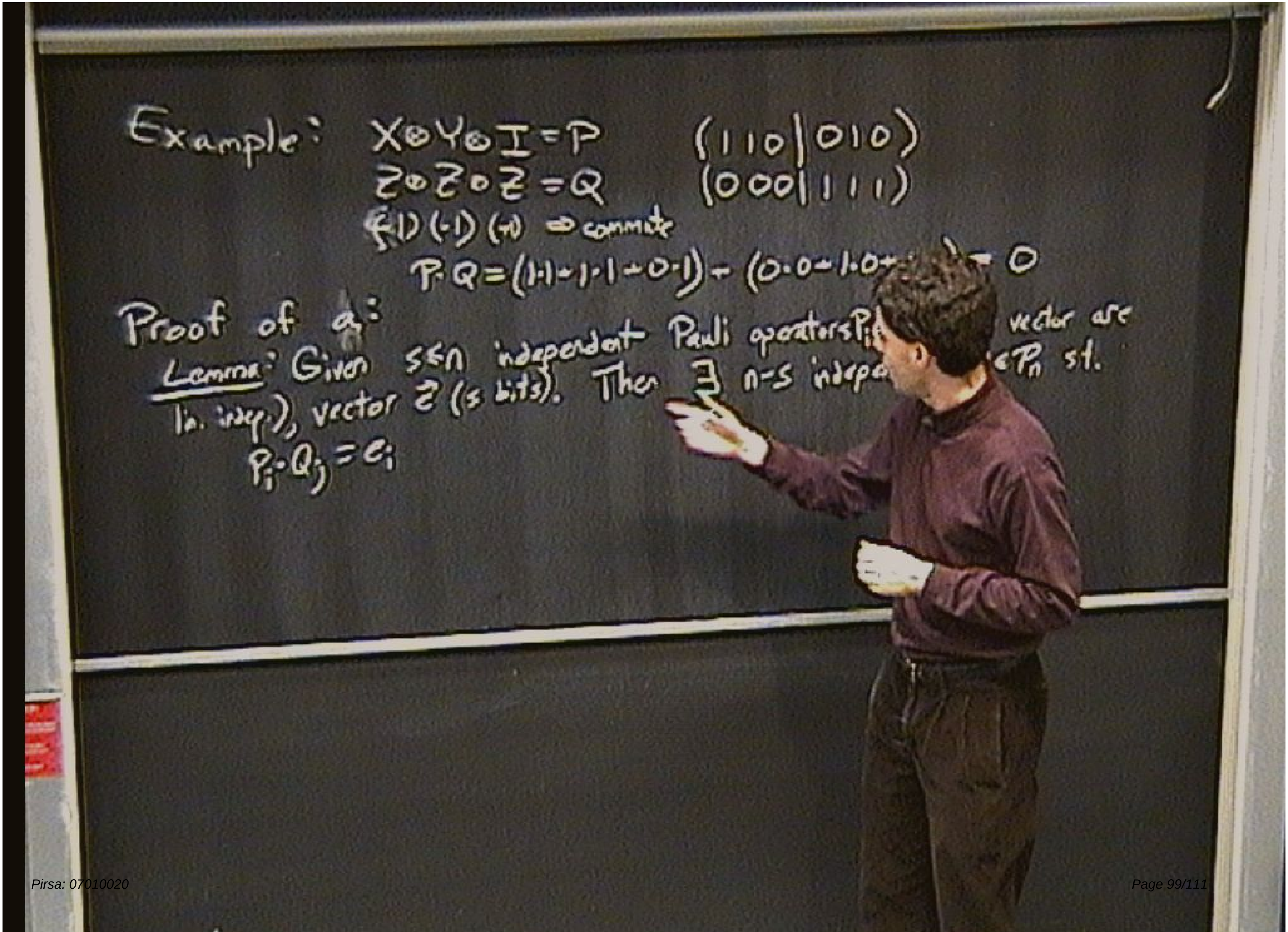
$Z \otimes Z \otimes Z = Q \qquad (0\,0\,0 \mid 1\,1\,1)$

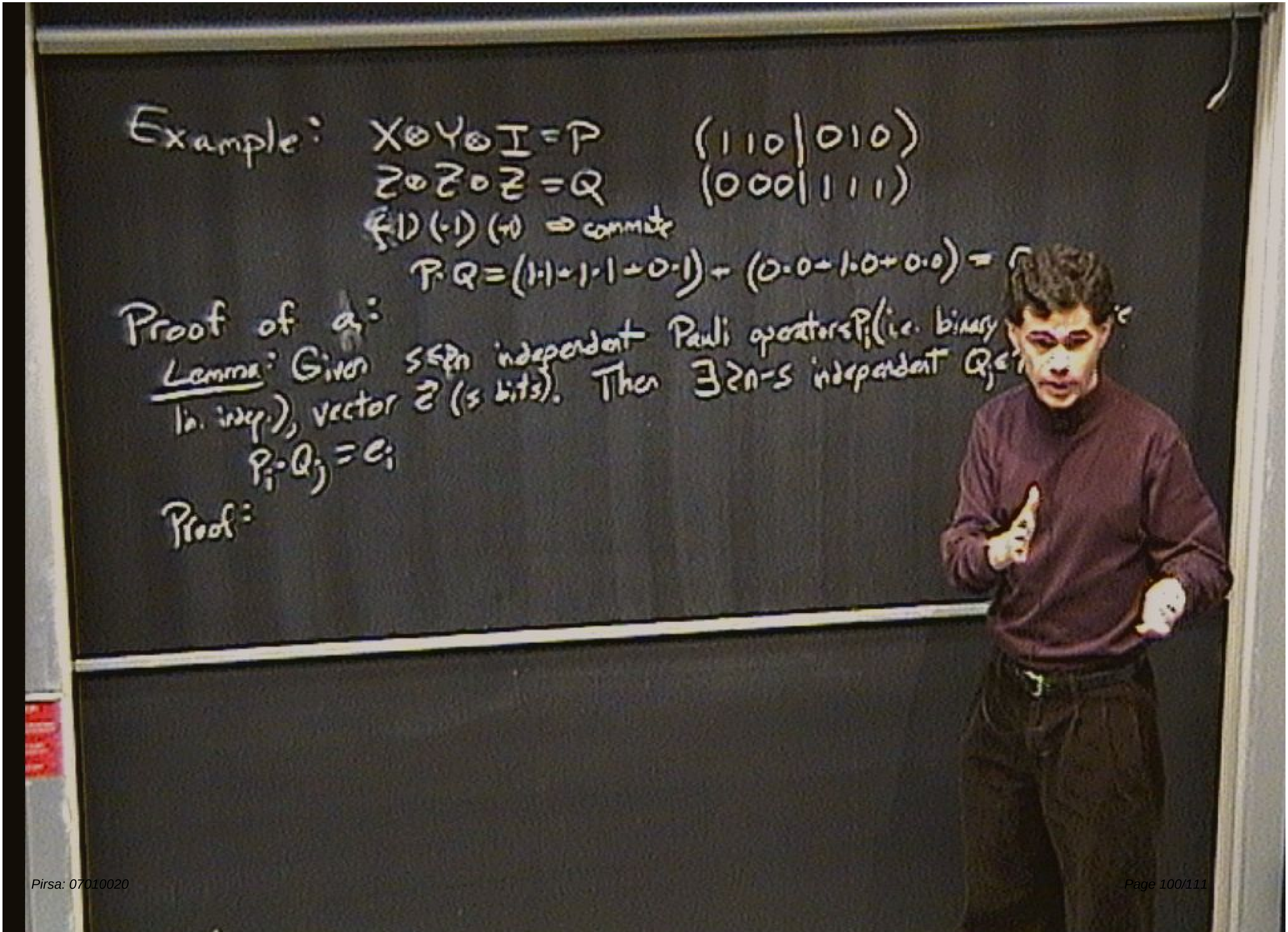
$(-1)(-1)(+1) \Rightarrow$ commute

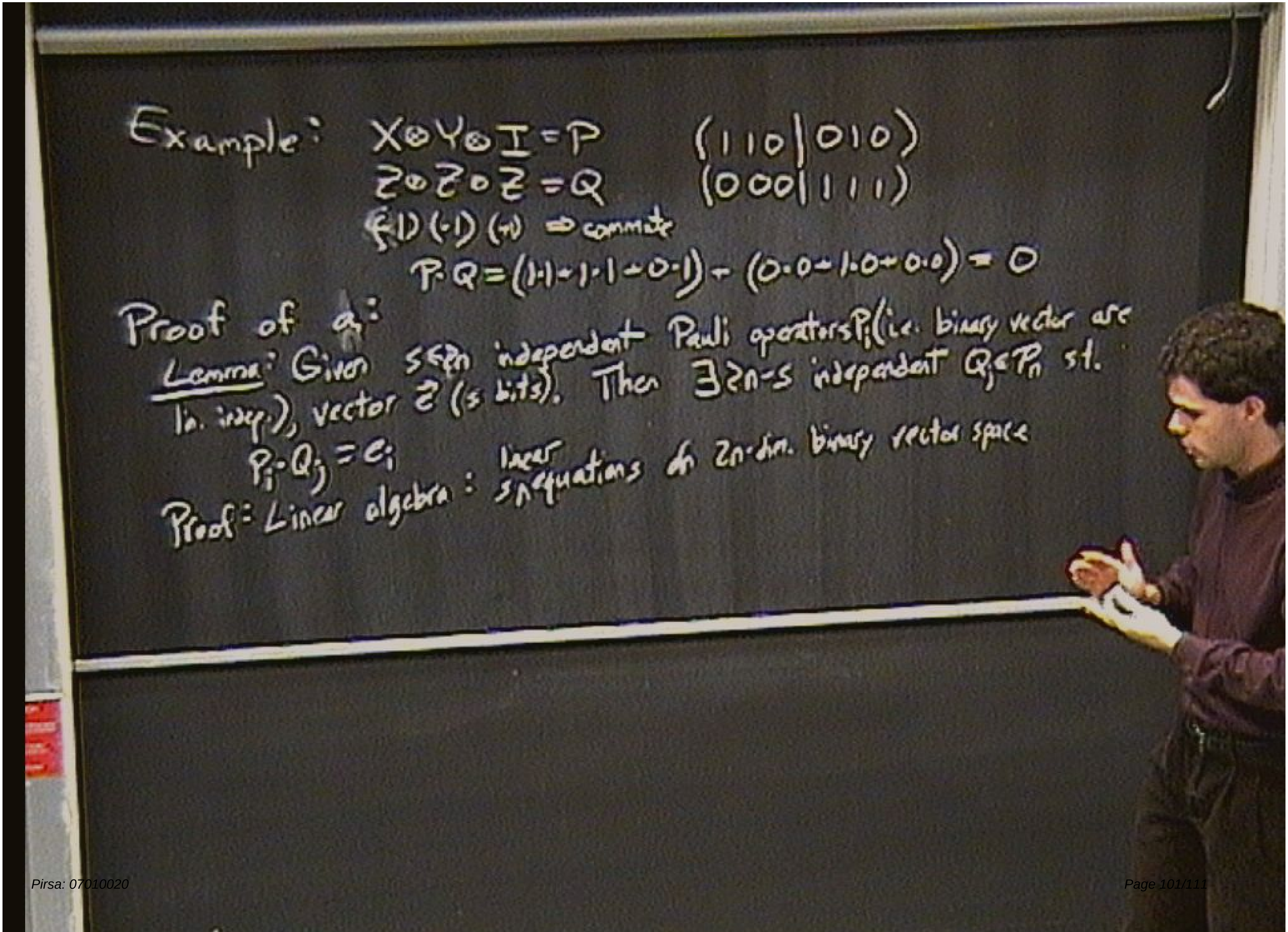
$P \cdot Q = (1\cdot1 + 1\cdot1 + 0\cdot1) + (0\cdot0 + 1\cdot0 + 0\cdot0) = 0$

Proof of a_i:

Lemma: Given $s \le n$ independent Pauli operators (i.e. binary vector are lin. indep.), vector $\vec{z}$ (s bits). Then $\exists$ $n-s$ independent


Example: X⊗Y⊗I = P (110|010)
Z⊗Z⊗Z = Q (000|111)
(-1)(-1)(+1) ⇒ commute
P·Q = (1·1+1·1+0·1)+(0·0+1·0+
= 0
Proof of a:
Lemma: Given s≤n independent Pauli operators
vector are
∈ P_n s.t.
lin. indep.), vector z (s bits). Then ∃ n-s
P_i·Q_j = e_i


Example: X⊗Y⊗I = P (110|010)
Z⊗Z⊗Z = Q (000|111)
(-1)(-1)(+1) ⇒ commute
P·Q = (1·1+1·1+0·1) + (0·0+1·0+0·0) =
Proof of a_i:
Lemma: Given s ≤ 2n independent Pauli operators P_i (i.e. binary
lin. indep.), vector e (s bits). Then ∃ 2n−s independent Q_j
P_i·Q_j = e_i
Proof:


Example: $X \otimes Y \otimes I = P$ $(1 1 0 | 0 1 0)$
$Z \otimes Z \otimes Z = Q$ $(0 0 0 | 1 1 1)$
$(-1)(-1)(+1) \Rightarrow$ commute
$P \cdot Q = (1\cdot1 + 1\cdot1 + 0\cdot1) + (0\cdot0 + 1\cdot0 + 0\cdot0) = 0$
Proof of a_i:
Lemma: Given $s \leq n$ independent Pauli operators P_i (i.e. binary vector are lin. indep.), vector e (s bits). Then $\exists\ 2n-s$ independent $Q_j \in P_n$ s.t.
$P_i \cdot Q_j = e_i$ linear sn equations on $2n$-dim. binary vector space
Proof: Linear algebra:

Example: $X \otimes Y \otimes I = P \qquad (110|010)$

$Z \otimes Z \otimes Z = Q \qquad (000|111)$

$(-1)(-1)(+1) \Rightarrow$ commute

$P \cdot Q = (1\cdot 1 + 1\cdot 1 + 0\cdot 1) + (0\cdot 0 + 1\cdot 0 + 0\cdot 0) = 0$

Proof of a_i:

Lemma: Given $s \le 2n$ independent Pauli operators P_i (i.e. binary vector are lin. indep.), vector $\vec{e}$ (s bits). Then $\exists\, 2n-s$ independent $Q_j \in \mathcal{P}_n$ s.t.

$P_i \cdot Q_j = e_i$

Proof: Linear algebra: s linear equations on $2n$-dim. binary vector space

r' generators for S are $P_1, \ldots, P_r$

$$a_i = \begin{cases} 0 & [P, M_i] = 0 \\ 1 & \{P, M_i\} = 0 \end{cases}$$

($M_1, \ldots, M_{n-k}$ are generators of S)

$$\text{Syndrome}(PQ) = \text{Syndrome}(P) + \text{Syndrome}(Q) \quad (\text{binary})$$

$$\text{Syndrome } P = \text{Syndrome } Q \Leftrightarrow \text{Syndrome}(PQ) = 0 \Leftrightarrow PQ \in N(S)$$

r generators for S are $P_1', \ldots, P_r'$

By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

r generators for S are $P_1, \ldots, P_r$

By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

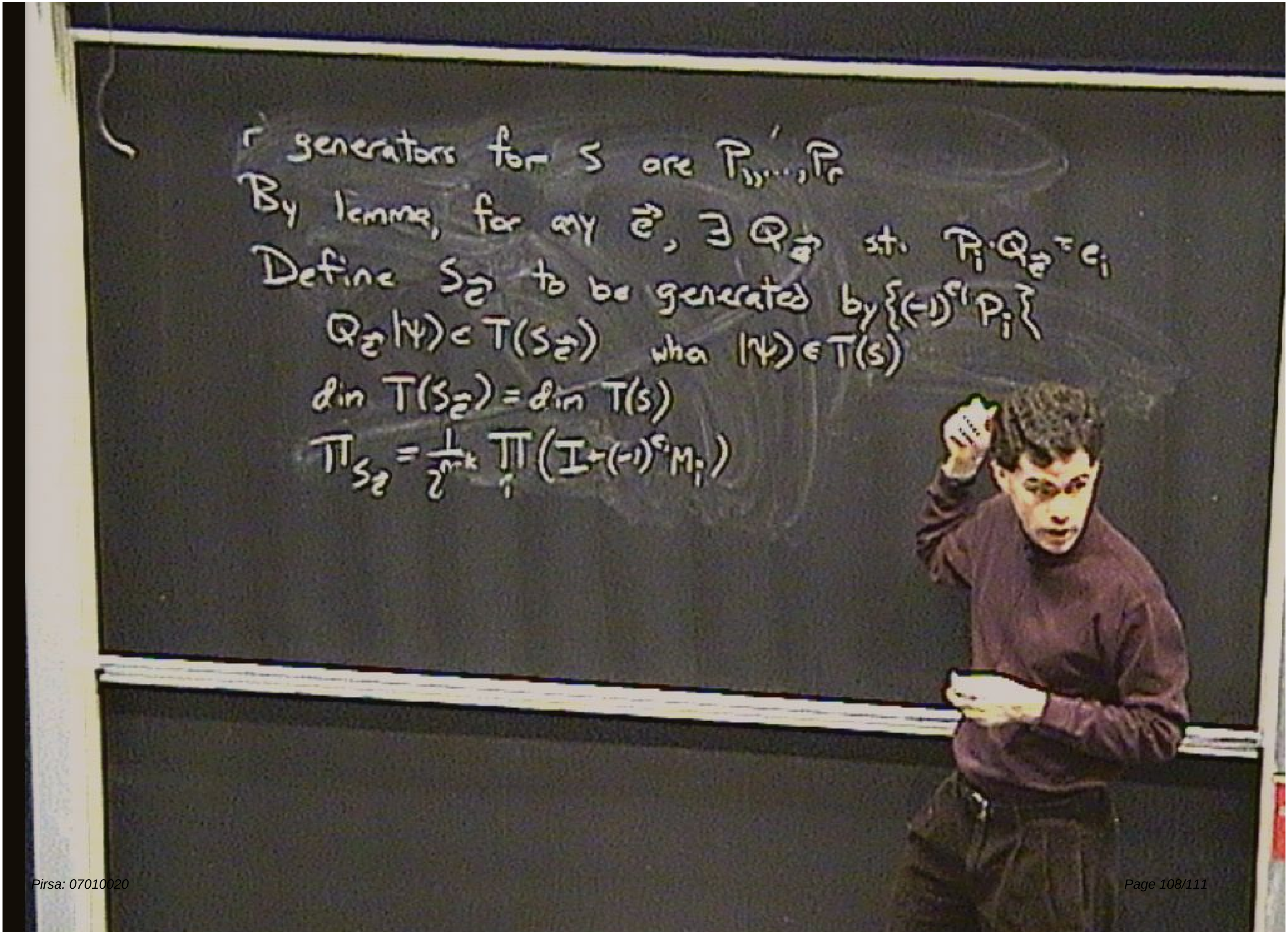
Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$

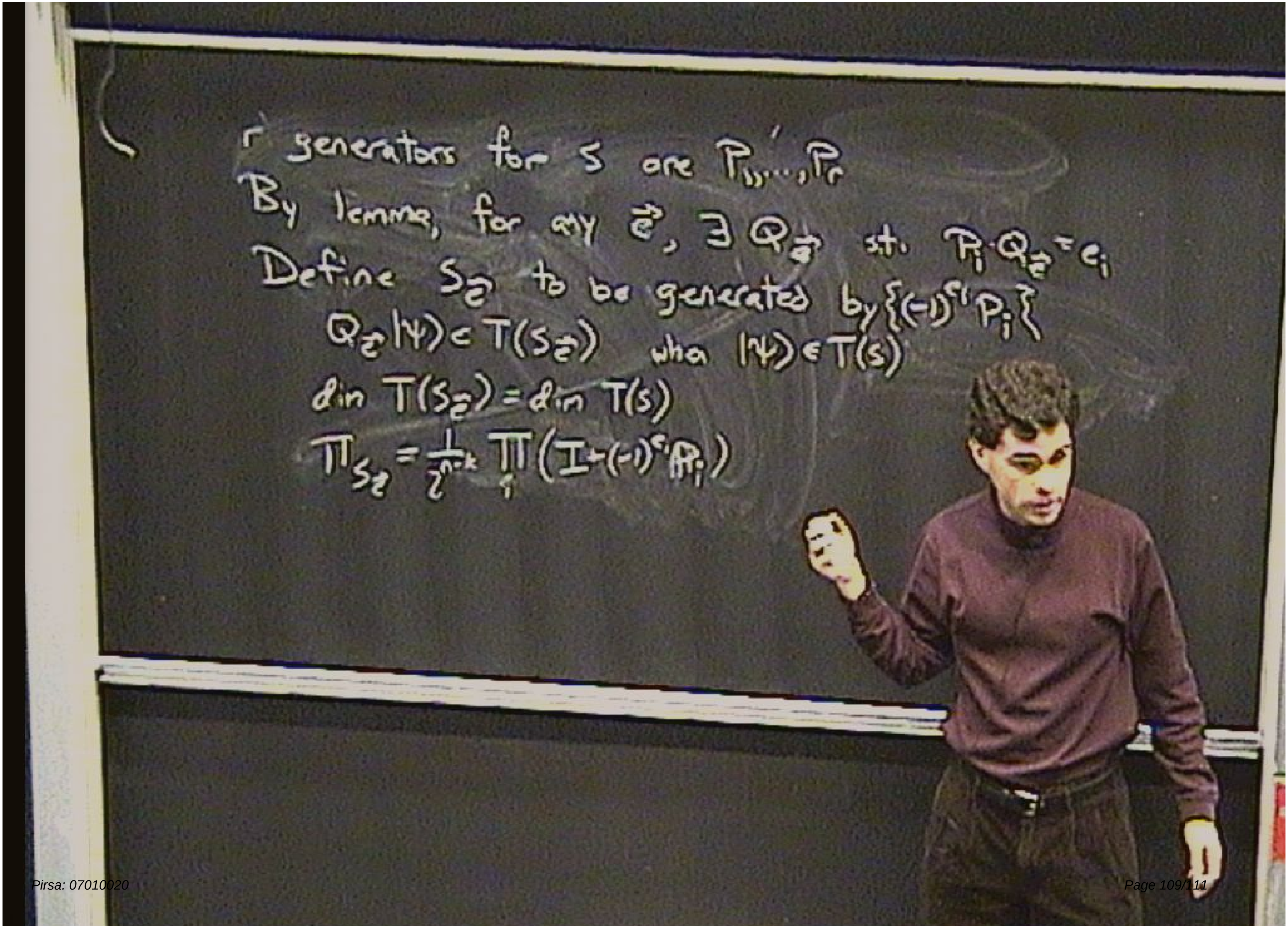
r generators for S are $P_1, \ldots, P_r$

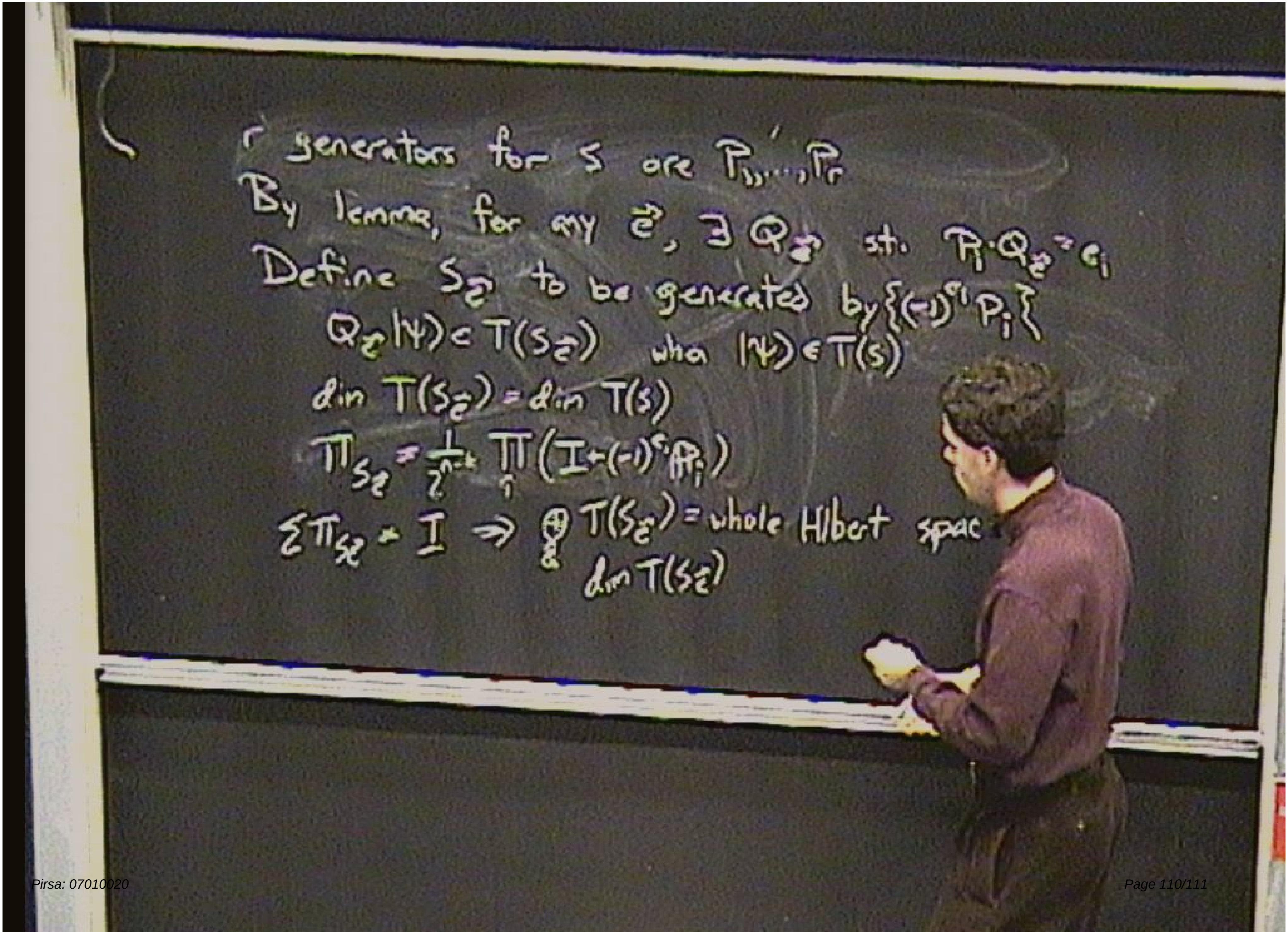
By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$

$Q_{\vec{e}}|\psi\rangle \in T(S_{\vec{e}})$ when $|\psi\rangle \in T(S)$


r generators for S are $P_1, \ldots, P_r$
By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$
Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$
$Q_{\vec{e}}|\psi\rangle \in T(S_{\vec{e}})$ when $|\psi\rangle \in T(S)$
$\dim T(S_{\vec{e}}) = \dim T(S)$
$\Pi_{S_{\vec{e}}} = \frac{1}{2^{n-k}} \prod_i \left(I + (-1)^{e_i} M_i\right)$


r generators for S are $P_1, \ldots, P_r$
By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$
Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$
$Q_{\vec{e}} |\psi\rangle \in T(S_{\vec{e}})$ when $|\psi\rangle \in T(S)$
$\dim T(S_{\vec{e}}) = \dim T(S)$
$\Pi_{S_{\vec{e}}} = \frac{1}{2^{n-k}} \prod_i \left(I + (-1)^{e_i} P_i\right)$


r generators for S are $P_1, \dots, P_r$
By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$
Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$
$Q_{\vec{e}}|\psi\rangle \in T(S_{\vec{e}})$ when $|\psi\rangle \in T(S)$
$\dim T(S_{\vec{e}}) = \dim T(S)$
$\Pi_{S_{\vec{e}}} = \frac{1}{2^{n-k}} \prod_i (I + (-1)^{e_i} P_i)$
$\sum \Pi_{S_{\vec{e}}} = I \Rightarrow \bigoplus_{\vec{e}} T(S_{\vec{e}})$ = whole Hilbert spac
$\dim T(S_{\vec{e}})$

r generators for S are $P_1, \dots, P_r$

By lemma, for any $\vec{e}$, $\exists\, Q_{\vec{e}}$ s.t. $P_i \cdot Q_{\vec{e}} = e_i$

Define $S_{\vec{e}}$ to be generated by $\{(-1)^{e_i} P_i\}$

$Q_{\vec{e}}|\psi\rangle \in T(S_{\vec{e}})$ when $|\psi\rangle \in T(S)$

$\dim T(S_{\vec{e}}) = \dim T(S)$

$$\Pi_{S_{\vec{e}}} = \frac{1}{2^{n-k}} \prod_i \left(I + (-1)^{e_i} P_i\right)$$

$\sum \Pi_{S_{\vec{e}}} = I \Rightarrow \bigoplus_{\vec{e}} T(S_{\vec{e}})$ = whole Hilbert space

$\dim T(S_{\vec{e}}) = 2^n / 2^r = 2^{n-r}$