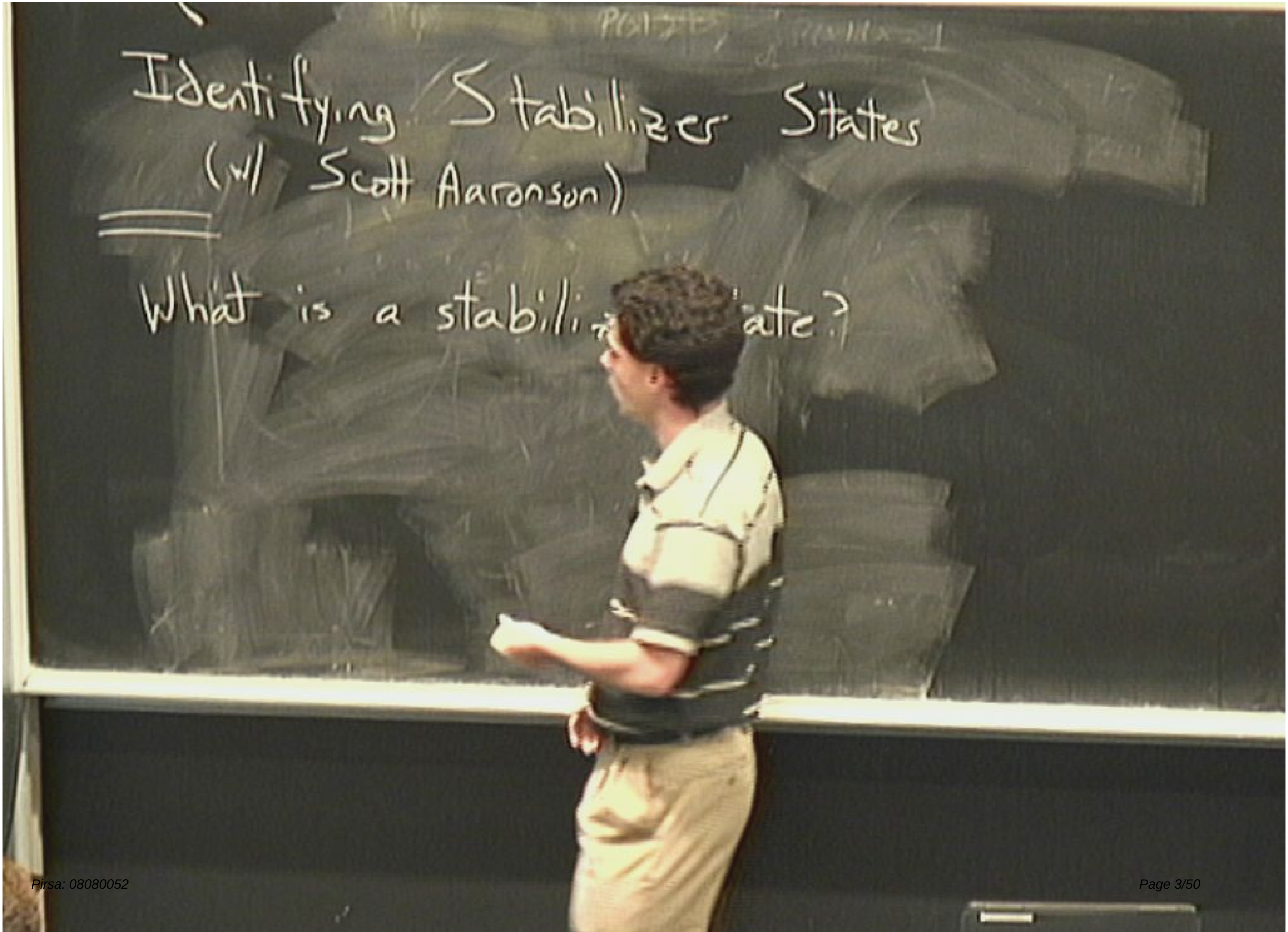
Title: Identifying Stabilizer States

Date: Aug 29, 2008 02:45 PM

URL: http://pirsa.org/08080052

Abstract: Suppose you are given m copies of an unknown n-qubit stabilizer state. How many copies do you need before you can figure out exactly what state it is? Just to specify the state requires about n^2/2 bits, so certainly m is at least n/2. Using only single-copy measurements, we show how to identify the state with high probability using m=O(n^2) copies. If one can make joint measurements, O(n) copies is sufficient.This is joint work with Scott Aaronson.

Identifying Stabilizer States
(w/ Scott Aaronson)


Identifying Stabilizer States
(w/ Scott Aaronson)
What is a stabili
tate?

Identifying Stabilizer States
(w/ Scott Aaronson)

What is a stabilizer state?

Pauli group $\mathcal{P}_n$ on n qubits:

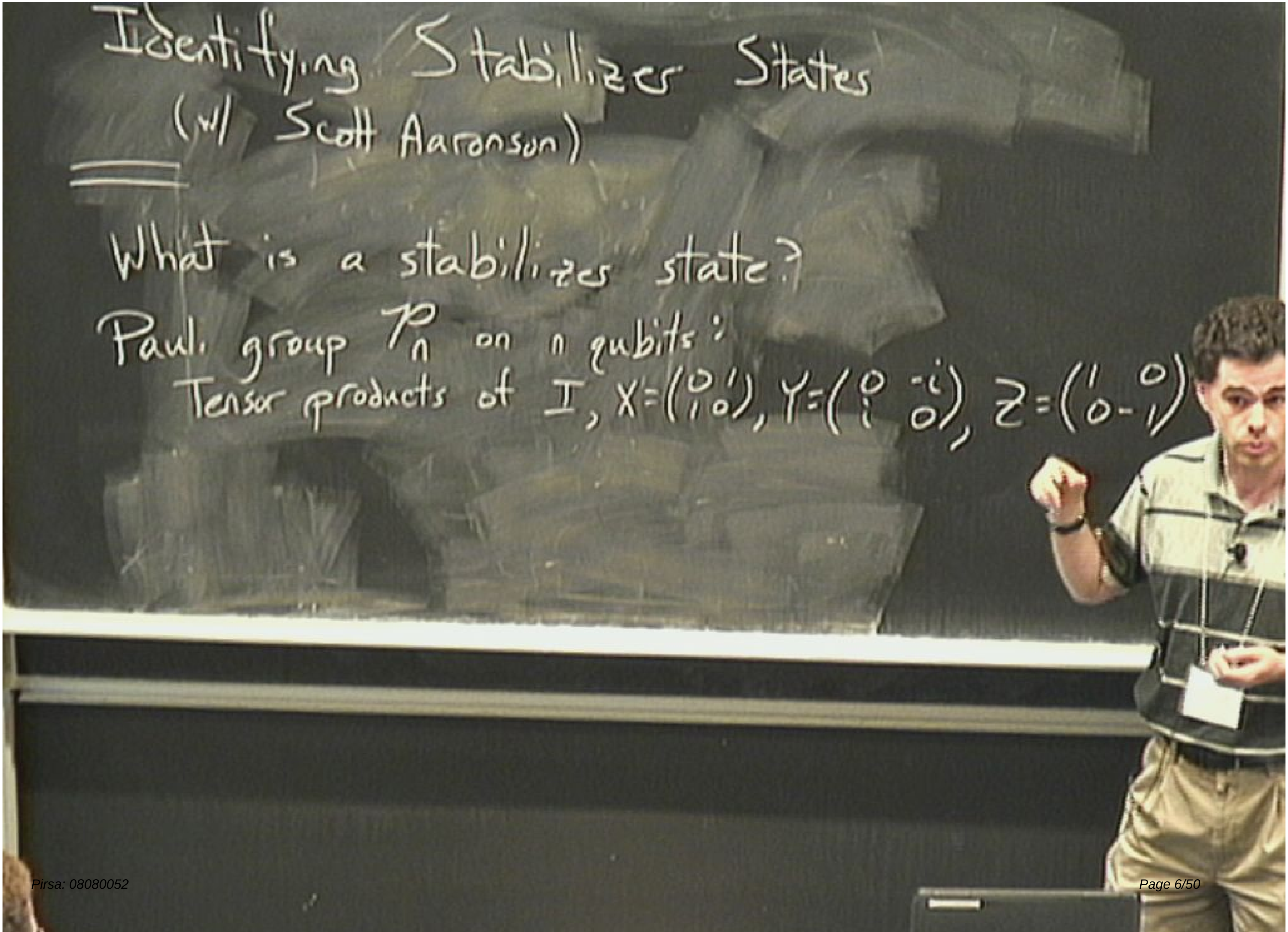
Tensor products of I, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\ &1\end{pmatrix}$

Identifying Stabilizer States
(w/ Scott Aaronson)

What is a stabilizer state?

Pauli group $\mathcal{P}_n$ on n qubits:

Tensor products of I, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$


Identifying Stabilizer States
(w/ Scott Aaronson)
What is a stabilizer state?
Pauli group $\mathcal{P}_n$ on n qubits:
Tensor products of I, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$

Identifying Stabilizer States

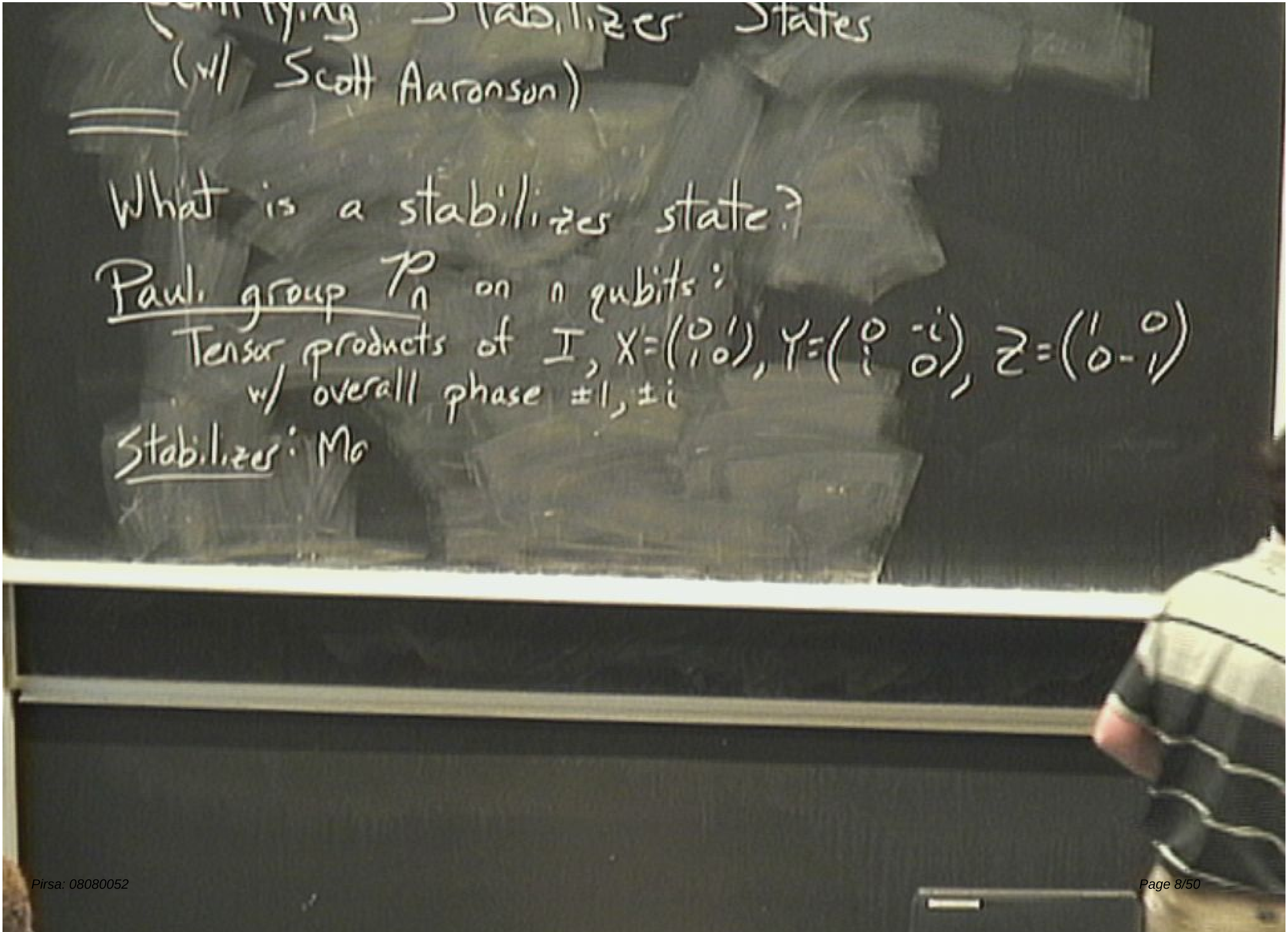
(w/ Scott Aaronson)

What is a stabilizer state?

Pauli group $\mathcal{P}_n$ on n qubits:

Tensor products of I, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

w/ overall phase $\pm 1, \pm i$


Stabilizer States
(w/ Scott Aaronson)
What is a stabilizer state?
Pauli group $\mathcal{P}_n$ on n qubits:
Tensor products of I, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
w/ overall phase $\pm 1, \pm i$
Stabilizer: Mo

Identifying Stabilizer States
(w/ Scott Aaronson)

What is a stabilizer state?

Pauli group $\mathcal{P}_n$ on n qubits:

Tensor products of I, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$

w/ overall phase $\pm 1, \pm i$

Stabilizer: Abelian subgroup of $\mathcal{P}_n$ that doesn't contain $-I$

Identifying Stabilizer States
(w/ Scott Aaronson)

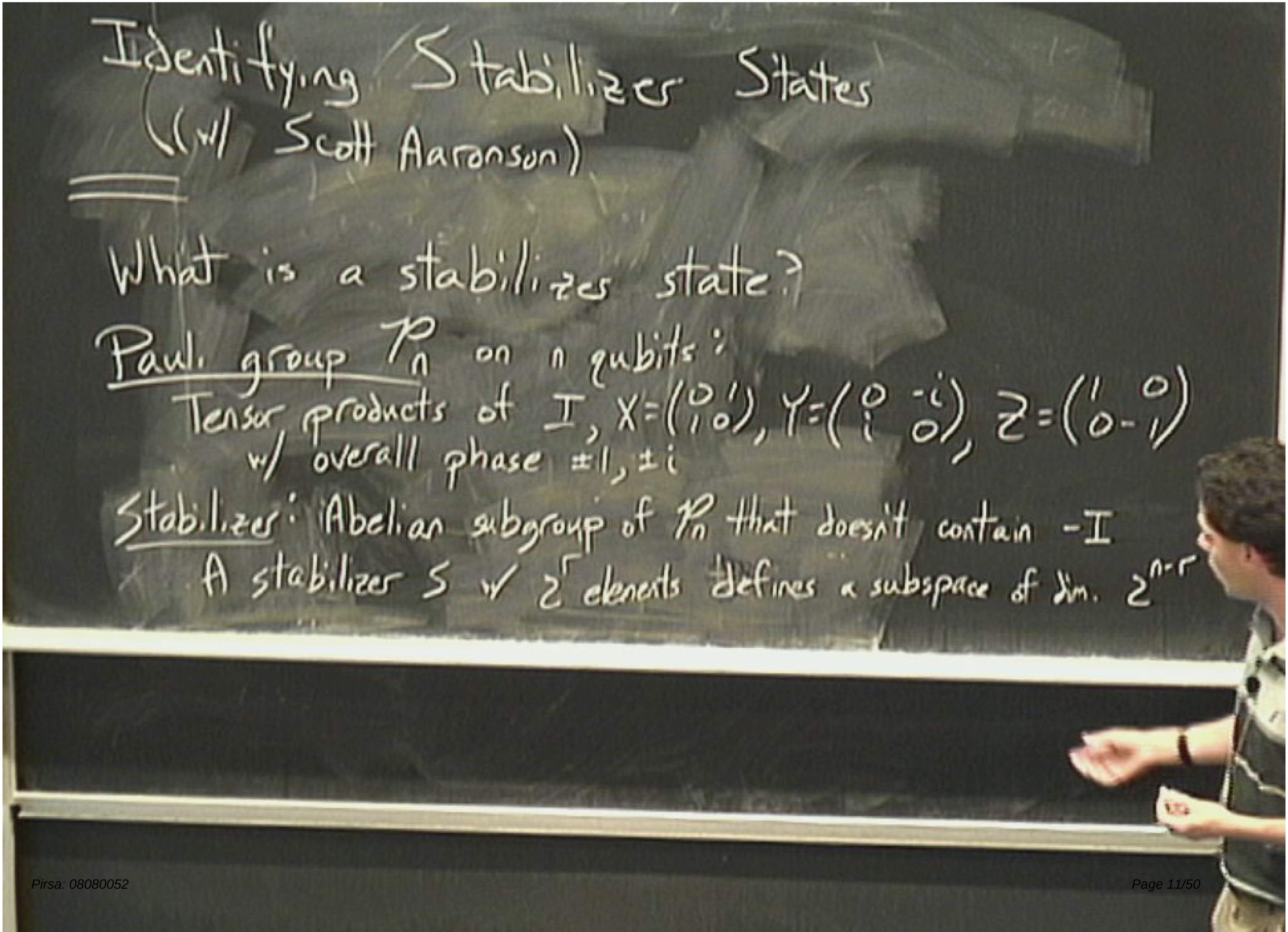
What is a stabilizer state?

<u>Pauli group</u> $\mathcal{P}_n$ on n qubits:

Tensor products of I, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

w/ overalll phase $\pm 1, \pm i$

<u>Stabilizer</u>: Abelian subgroup of $\mathcal{P}_n$ that doesn't contain $-I$


Identifying Stabilizer States
((w/ Scott Aaronson)
What is a stabilizer state?
Pauli group $\mathcal{P}_n$ on n qubits:
Tensor products of I, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$
w/ overalll phase $\pm1, \pm i$
Stabilizer: Abelian subgroup of $\mathcal{P}_n$ that doesn't contain $-I$
A stabilizer S w/ 2^r elements defines a subspace of dim. 2^{n-r}

Identifying Stabilizer States
(w/ Scott Aaronson)

What is a stabilizer state?

Pauli group $\mathcal{P}_n$ on n qubits:

Tensor products of I, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

w/ overalll phase $\pm 1, \pm i$

Stabilizer: Abelian subgroup of $\mathcal{P}_n$ that doesn't contain $-I$

A stabilizer S w/ 2^r elements defines a subspace of dim. 2^{n-r}

The s

The subspace associated w/ S is

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

The subspace associated w/ S is

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

When $r = n$, $T(S)$ is a single state. ("Stabilizer state")

The subspace associated w/ S is

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

When $r = n$, $T(S)$ is a single state. ("Stabilizer state")

Describe S by giving its generators (there are r)

The subspace associated w/ S is

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

When $r = n$, $T(S)$ is a single state. ("<u>Stabilizer state</u>")

Describe S by giving its generators (there are r)

There are $2^{O(n^2)}$ stabilizer states

- We can describe one w/ $O(n^2)$ bits

The subspace associated w/ S is

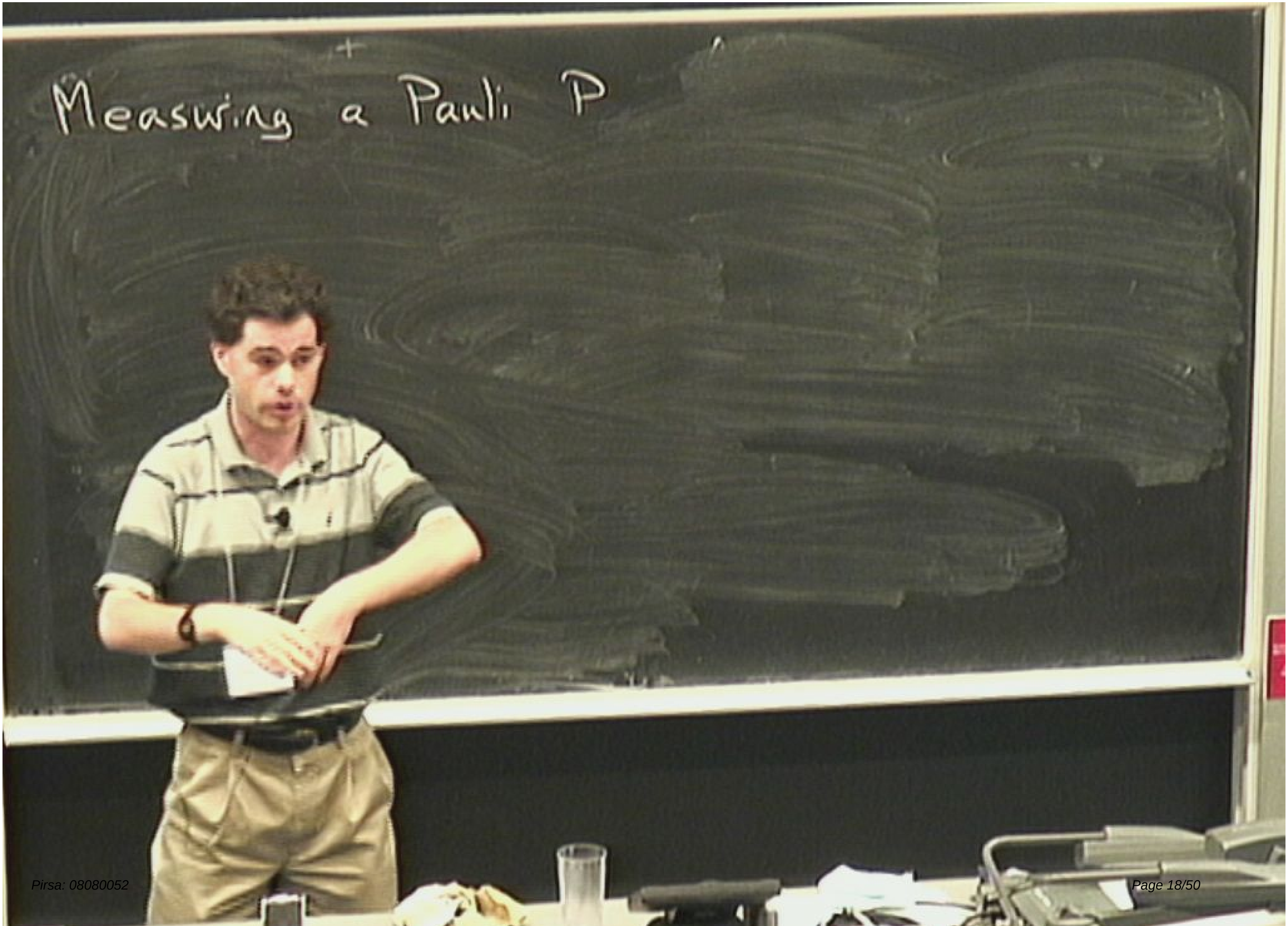
$$T(S) = \{ |\psi\rangle \mid M|\psi\rangle = |\psi\rangle \;\; \forall M \in S \}$$

When $r = n$, $T(S)$ is a single state. ("<u>Stabilizer state</u>")

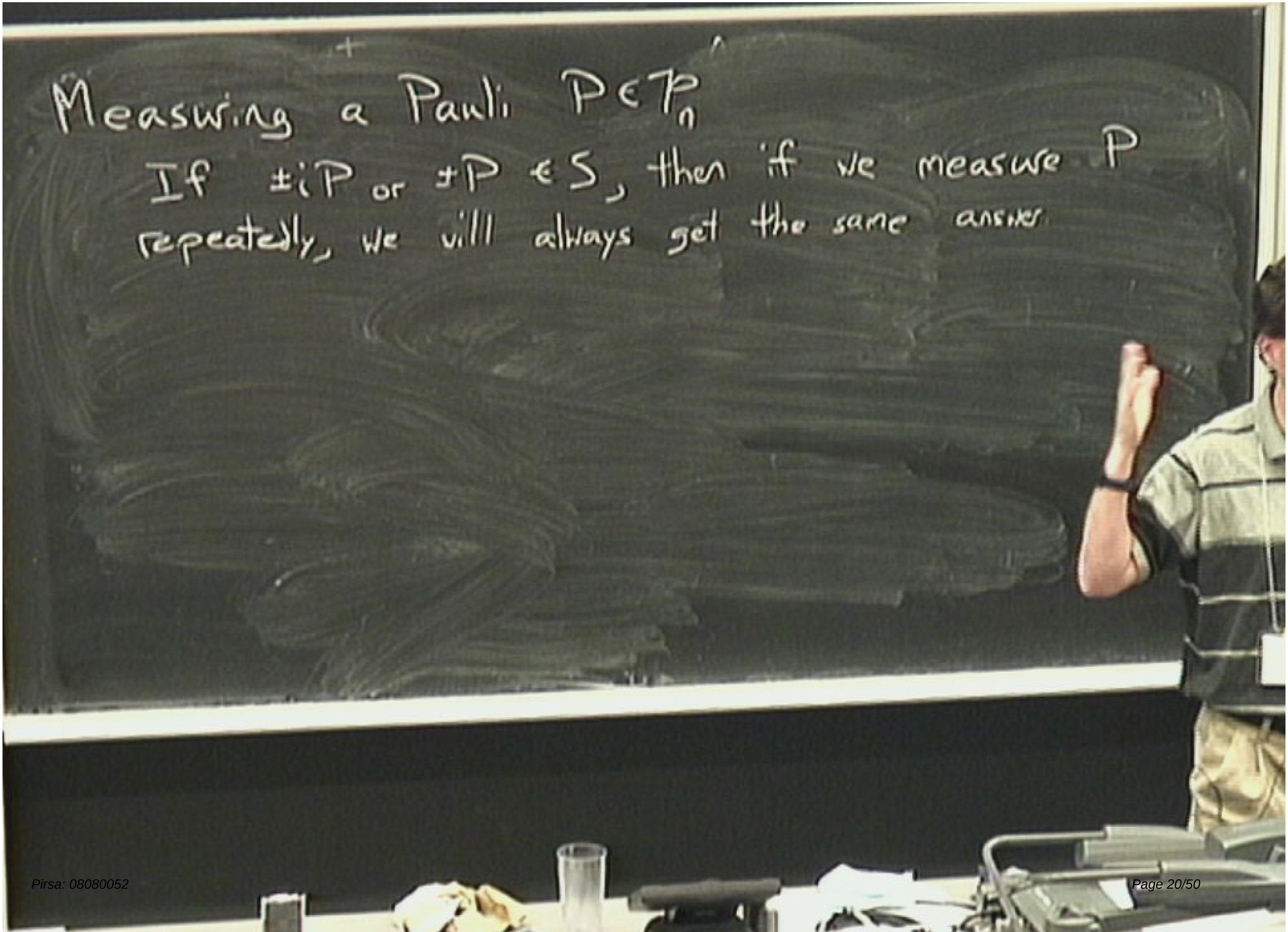
Describe S by giving its generators (there are r)

There are $2^{O(n^2)}$ stabilizer states

- We can describe one w/ $O(n^2)$ bits


Measuring a Pauli P

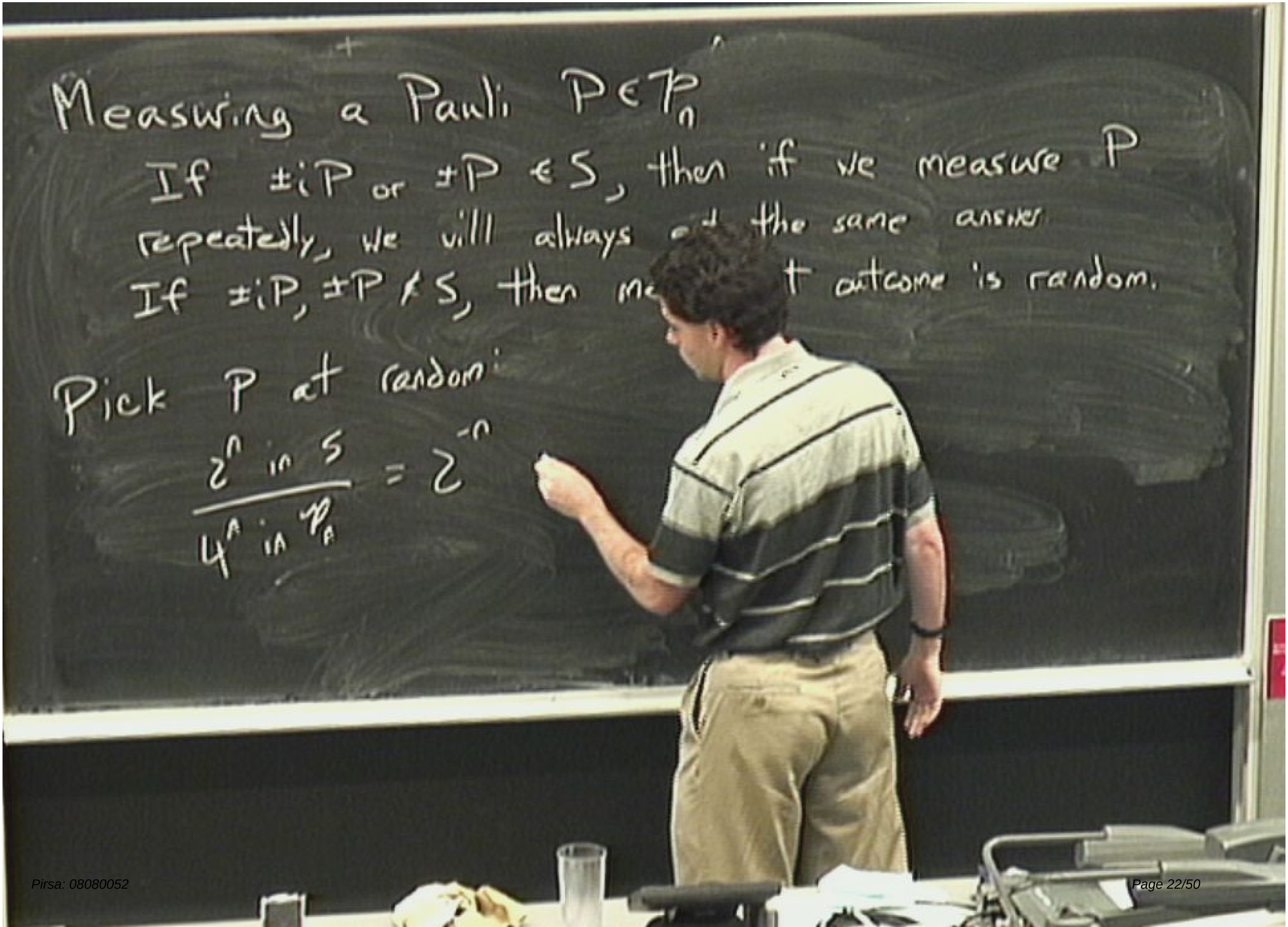
Measuring a Pauli $P \in \mathcal{P}_n$

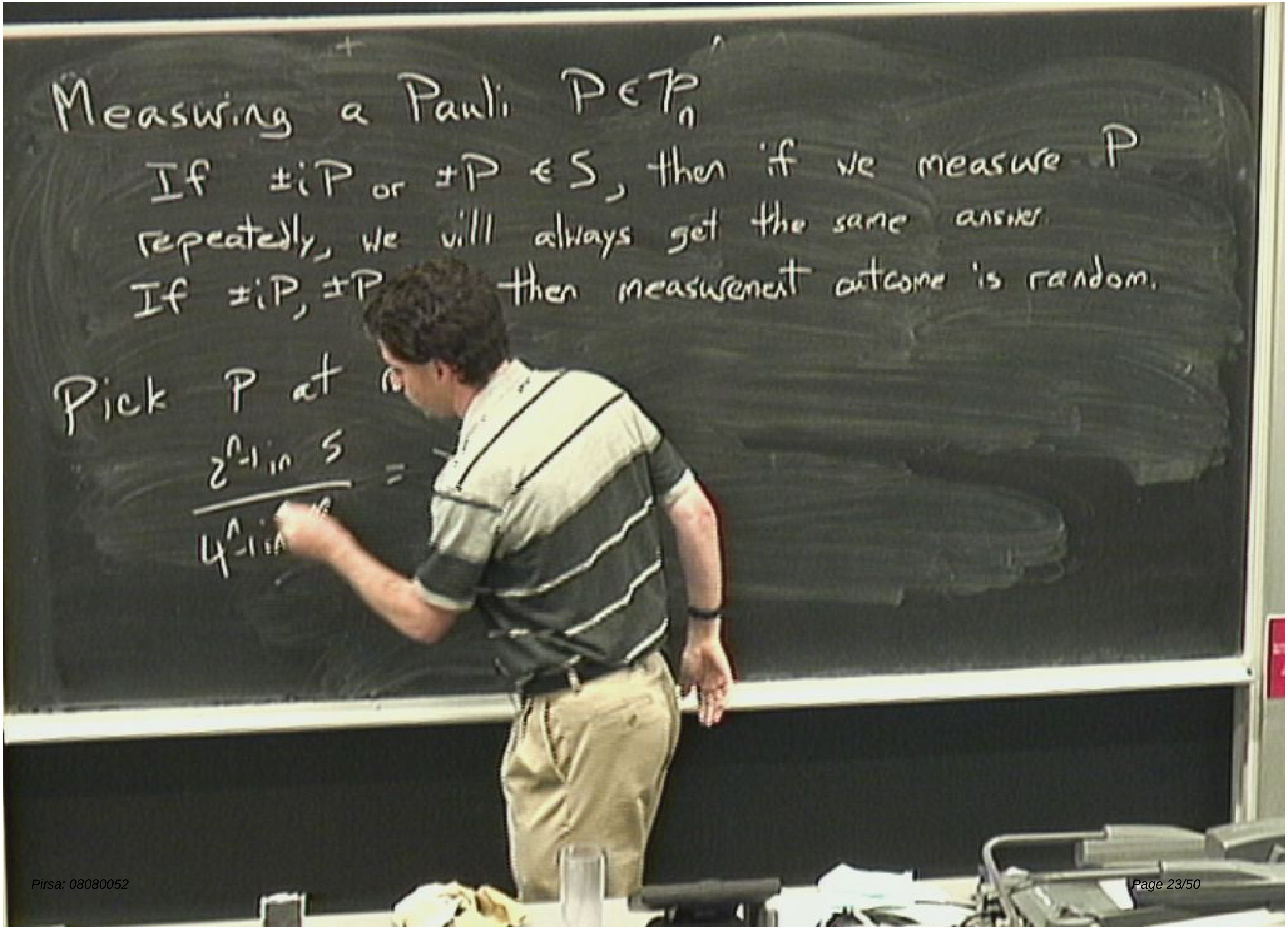

Measuring a Pauli $P \in \mathcal{P}_n$
If $\pm iP$ or $\pm P \in S$, then if we measure P
repeatedly, we will always get the same answer

Measuring a Pauli $P \in \mathcal{P}_n$

If $\pm iP$ or $\pm P \in S$, then if we measure P repeatedly, we will always get the same answer

If $\pm iP, \pm P \notin S$, then measurement outcome is random.


Measuring a Pauli $P \in \mathcal{P}_n$
If $\pm iP$ or $\pm P \in S$, then if we measure P
repeatedly, we will always
the same answer
If $\pm iP, \pm P \notin S$, then
outcome is random.
Pick P at random:
$\frac{2^n \text{ in } S}{4^n \text{ in } \mathcal{P}_n} = 2^{-n}$


Measuring a Pauli P ∈ 𝒫n
If ±iP or ±P ∈ S, then if we measure P
repeatedly, we will always get the same answer
If ±iP, ±P
then measurement outcome is random.
Pick P at
2^n-1 in S
4^n-1 in
=

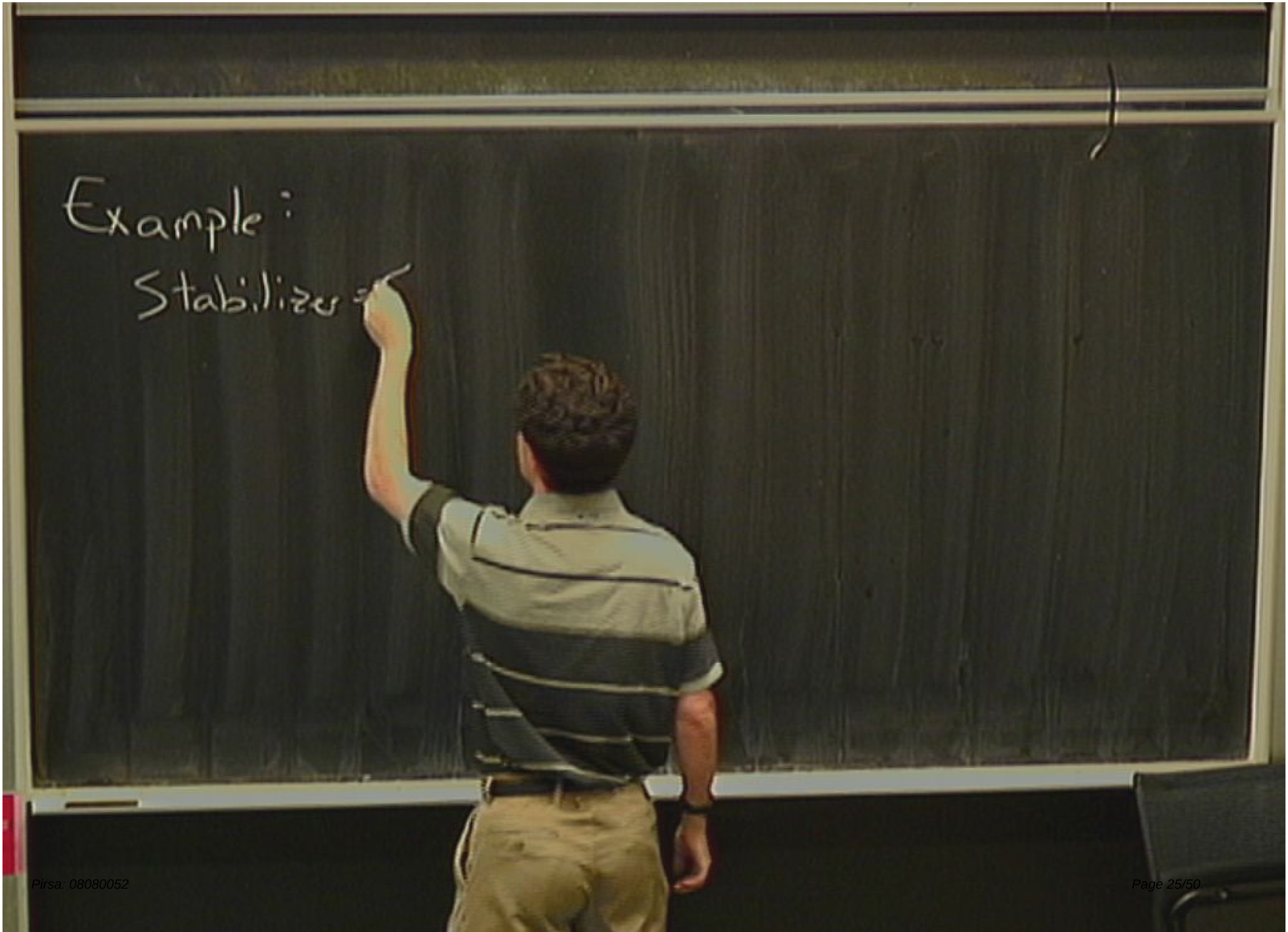
Measuring a Pauli $P \in \mathcal{P}_n$

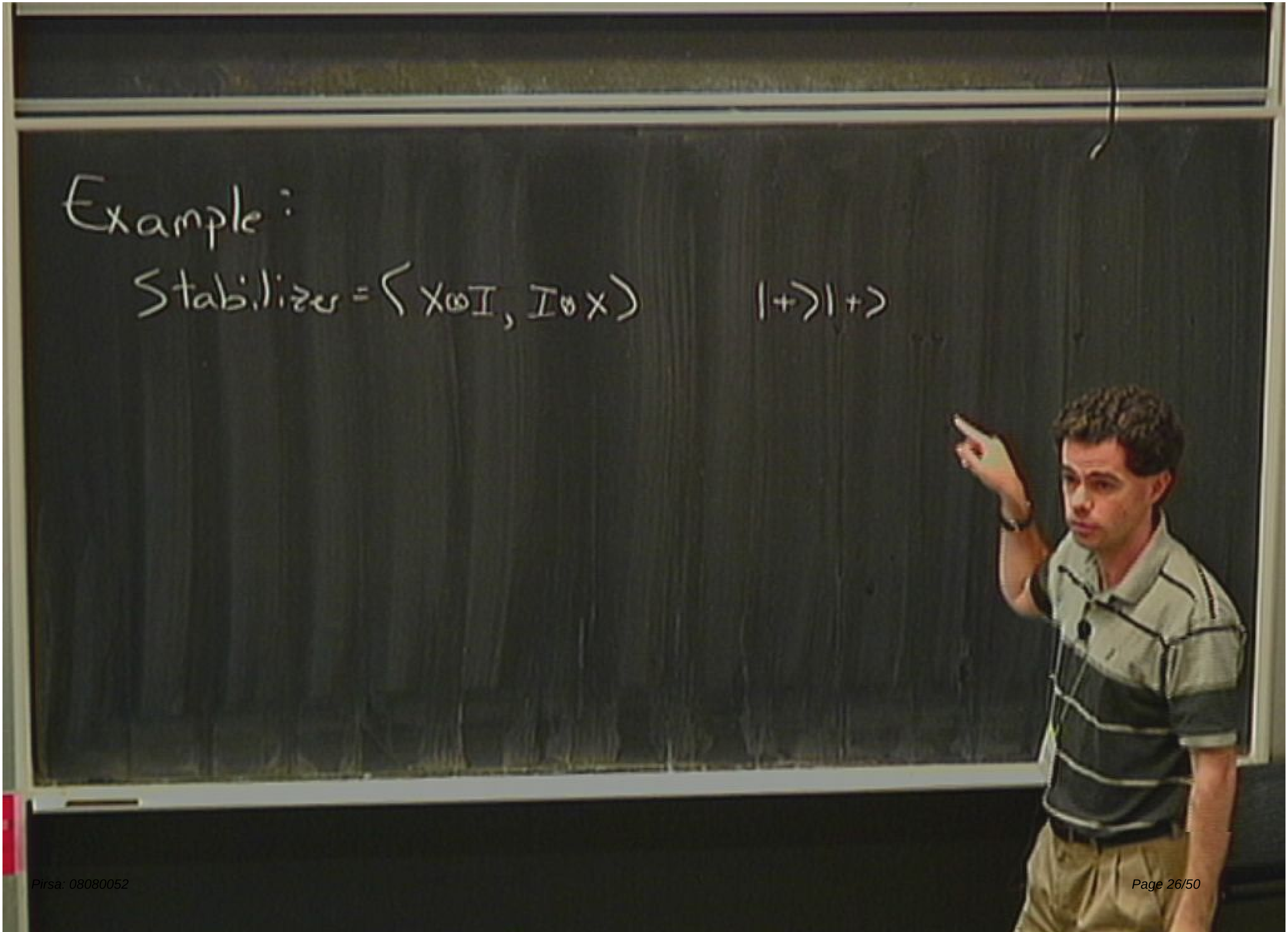
If $\pm iP$ or $\pm P \in S$, then if we measure P repeatedly, we will always get the same answer

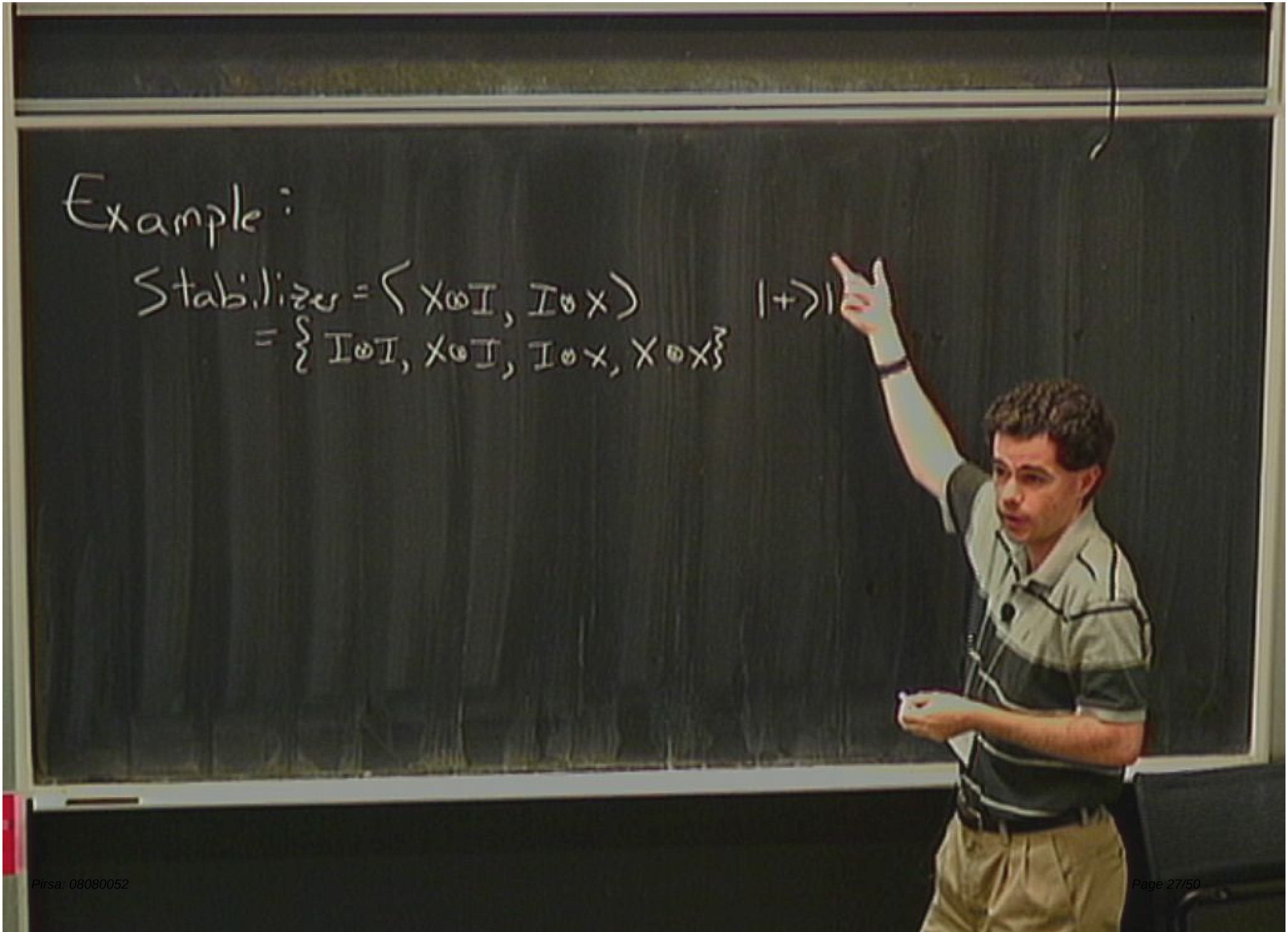
If $\pm iP, \pm P \notin S$, then measurement outcome is random.

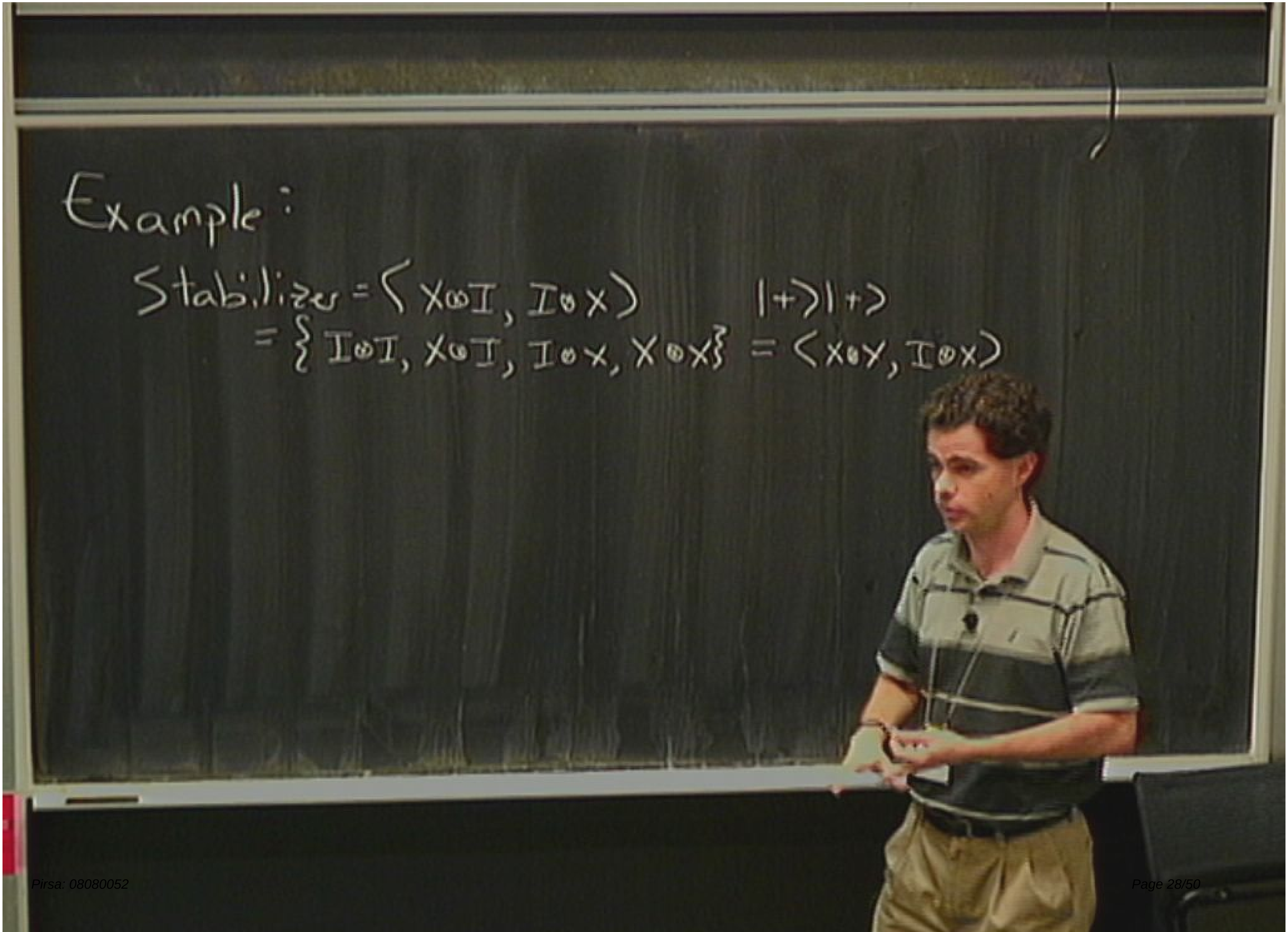
Pick P at random:

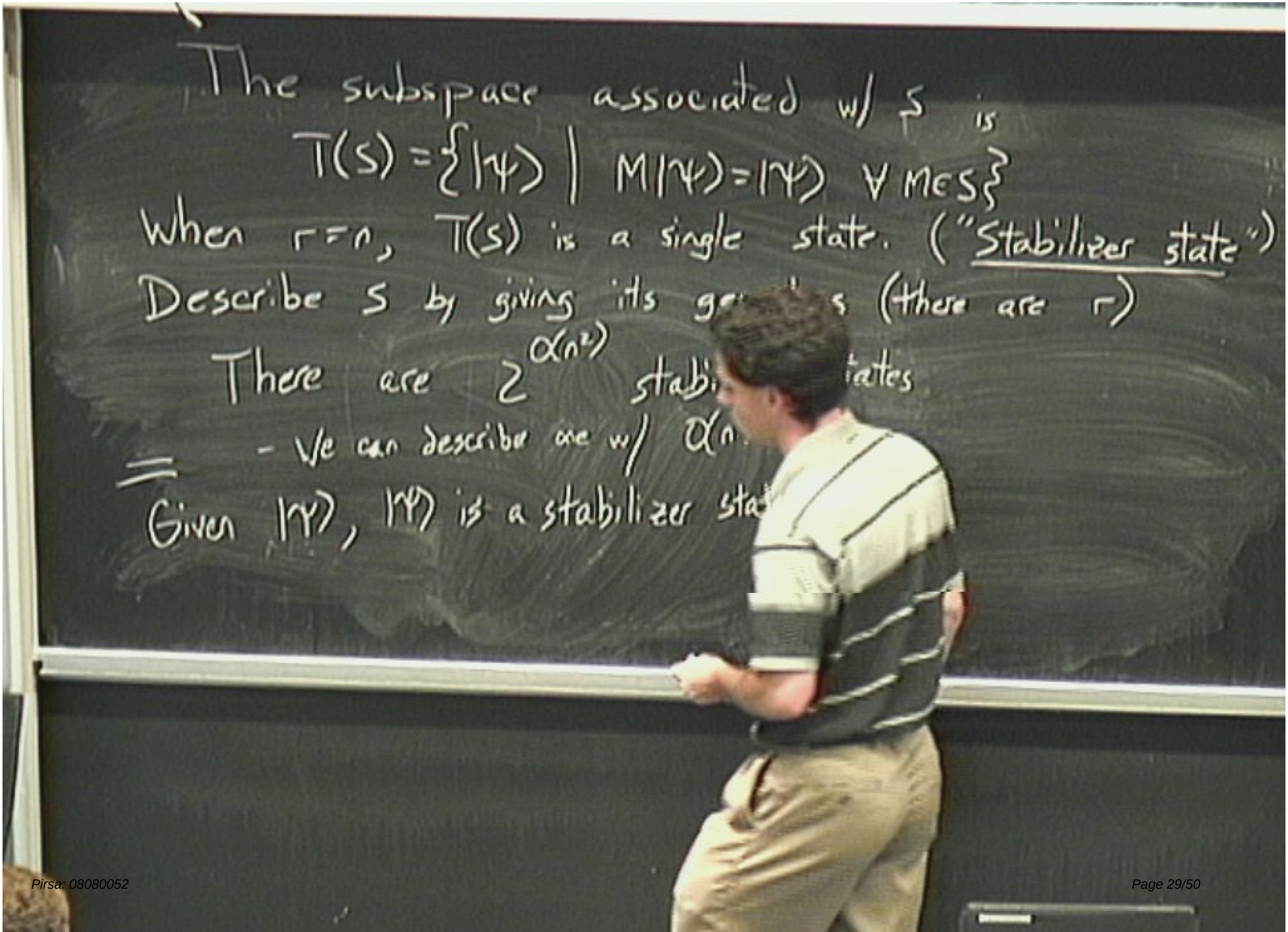
$$\frac{2^n - 1 \text{ in } S - \{I\}}{4^n - 1 \text{ in } \mathcal{P}_n - \{I\}} \approx 2^{-n} \quad (\text{Prob. of choosing } P \in S)$$


Example:
Stabilizer =


Example:
Stabilizer = ⟨X⊗I, I⊗X⟩
|+⟩|+⟩


Example:
Stabilizer = ⟨X⊗I, I⊗X⟩
|+⟩|
= {I⊗I, X⊗I, I⊗X, X⊗X}


Example:
Stabilizer = $\langle X\otimes I, I\otimes X\rangle$
$|+\rangle|+\rangle$
$= \{I\otimes I, X\otimes I, I\otimes X, X\otimes X\} = \langle X\otimes X, I\otimes X\rangle$


The subspace associated w/ S is
$T(S) = \{ |\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S \}$
When r = n, T(S) is a single state. ("Stabilizer state")
Describe S by giving its ge[...]s (there are r)
There are $2^{O(n^2)}$ stabi[...]tates
- We can describe one w/ $O(n$
Given $|\psi\rangle$, $|\psi\rangle$ is a stabilizer sta

The subspace associated w/ S is

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

When $r = n$, $T(S)$ is a single state. ("Stabilizer state")

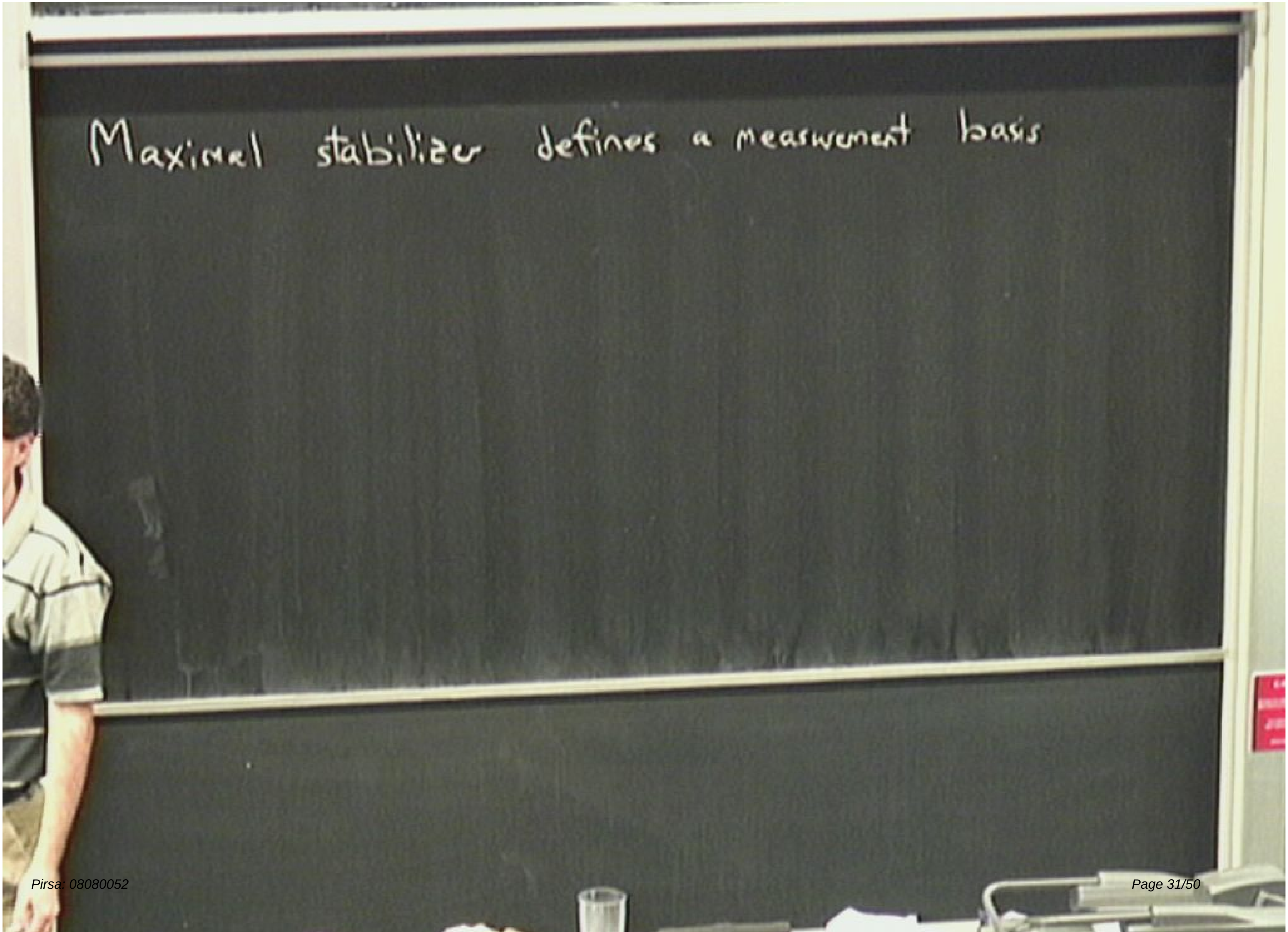
Describe S by giving its generators (there are r)

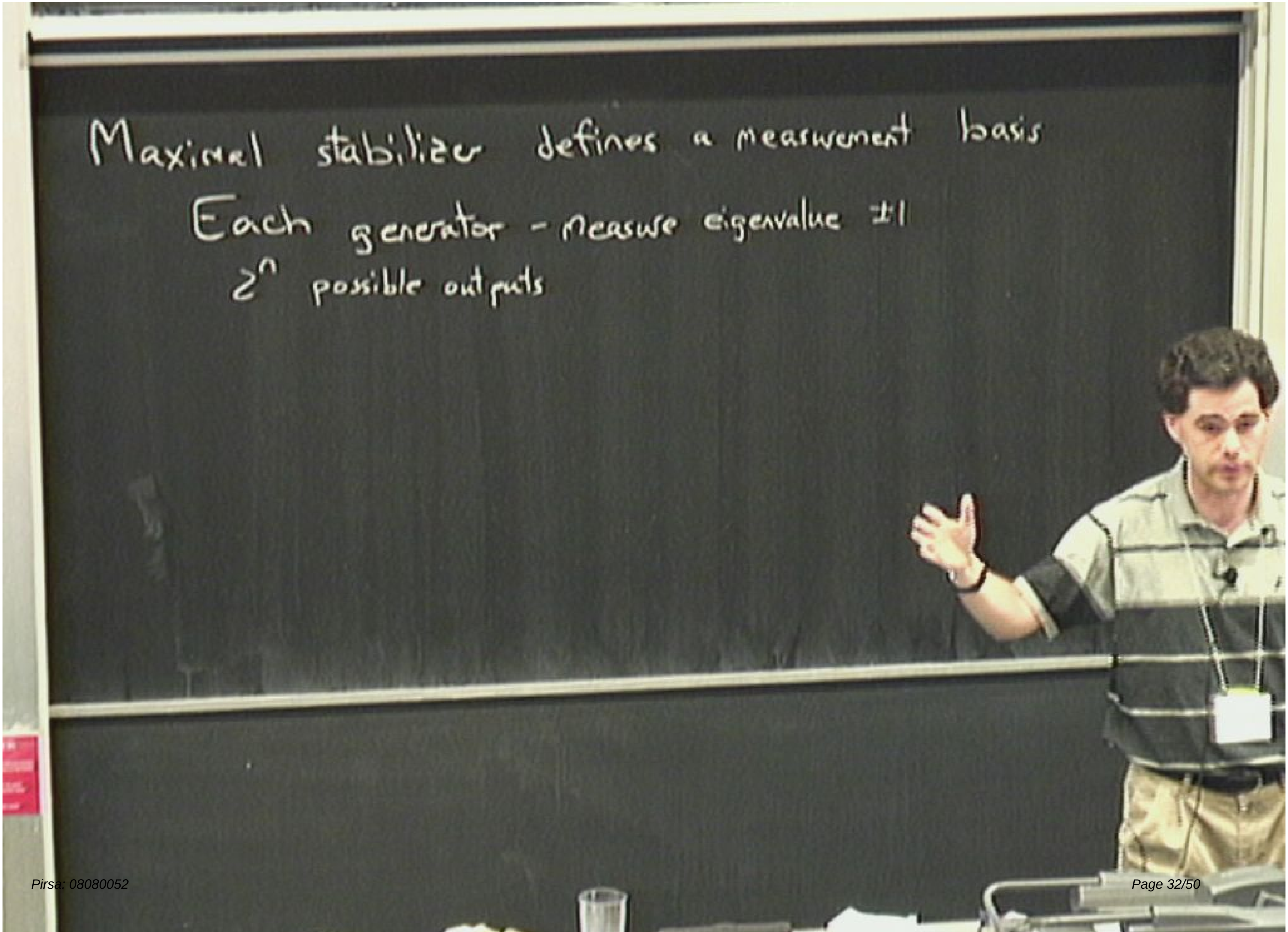
There are $2^{O(n^2)}$ stabilizer states

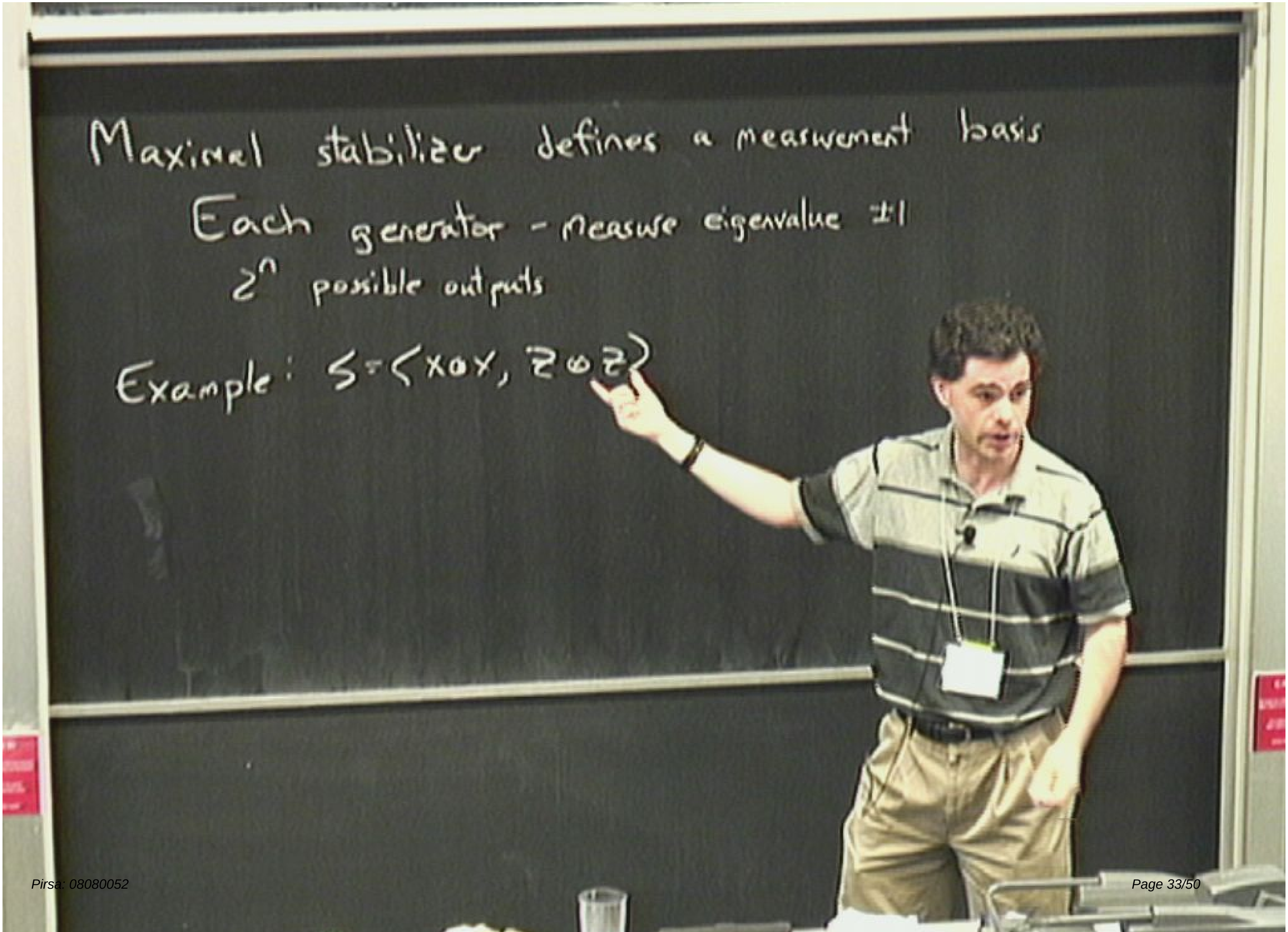
- We can describe one w/ $O(n^2)$ bits

Given $|\psi\rangle^{\otimes M}$, $|\psi\rangle$ is a stabilizer state

Find S, with $T(S) = \{|\psi\rangle\}$


Maximal stabilizer defines a measurement basis


Maximal stabilizer defines a measurement basis
Each generator - measure eigenvalue ±1
2^n possible outputs

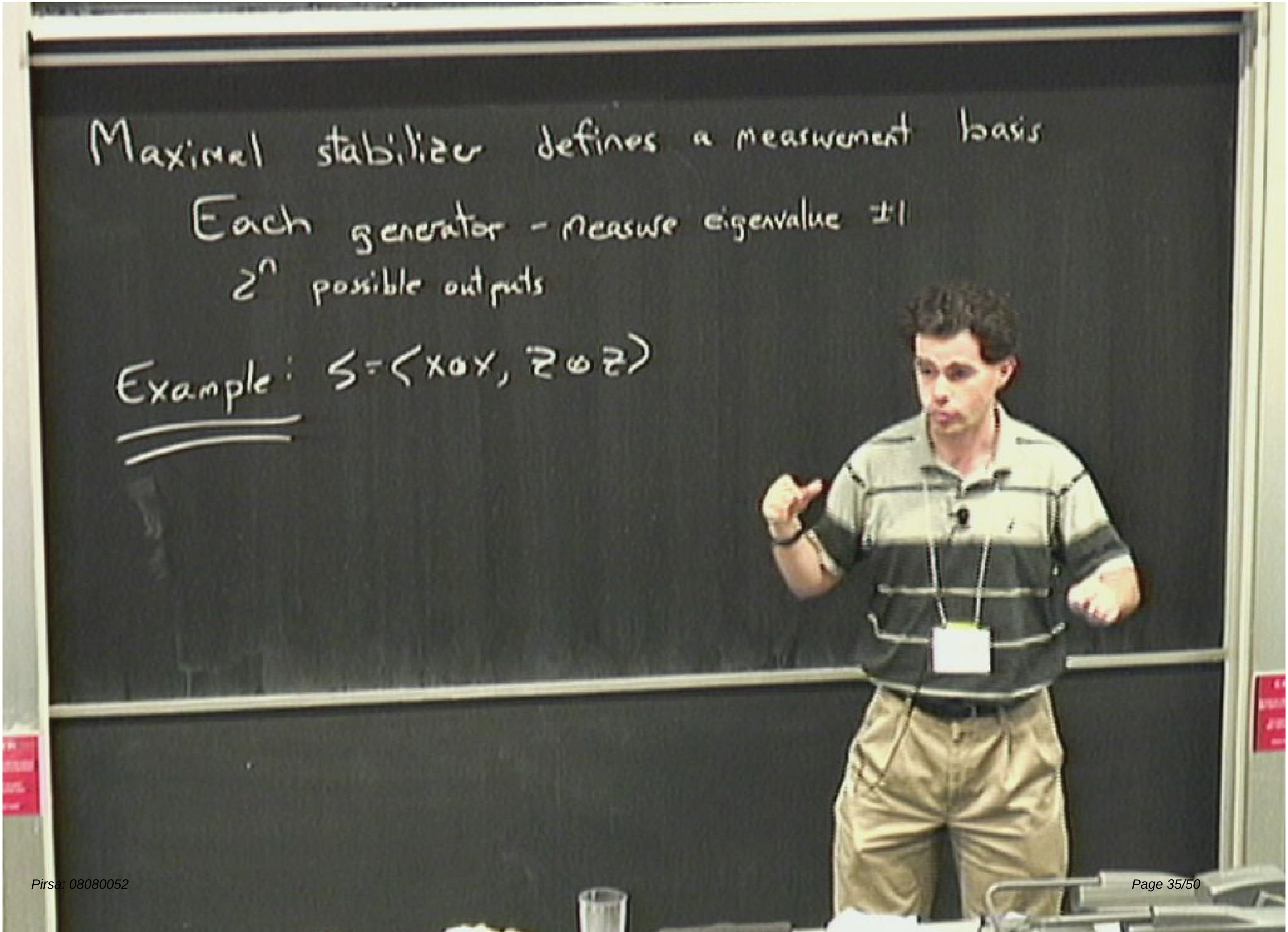

Maximal stabilizer defines a measurement basis
Each generator - measure eigenvalue ± 1
2^n possible outputs
Example: $S = \langle X \otimes X, Z \otimes Z \rangle$

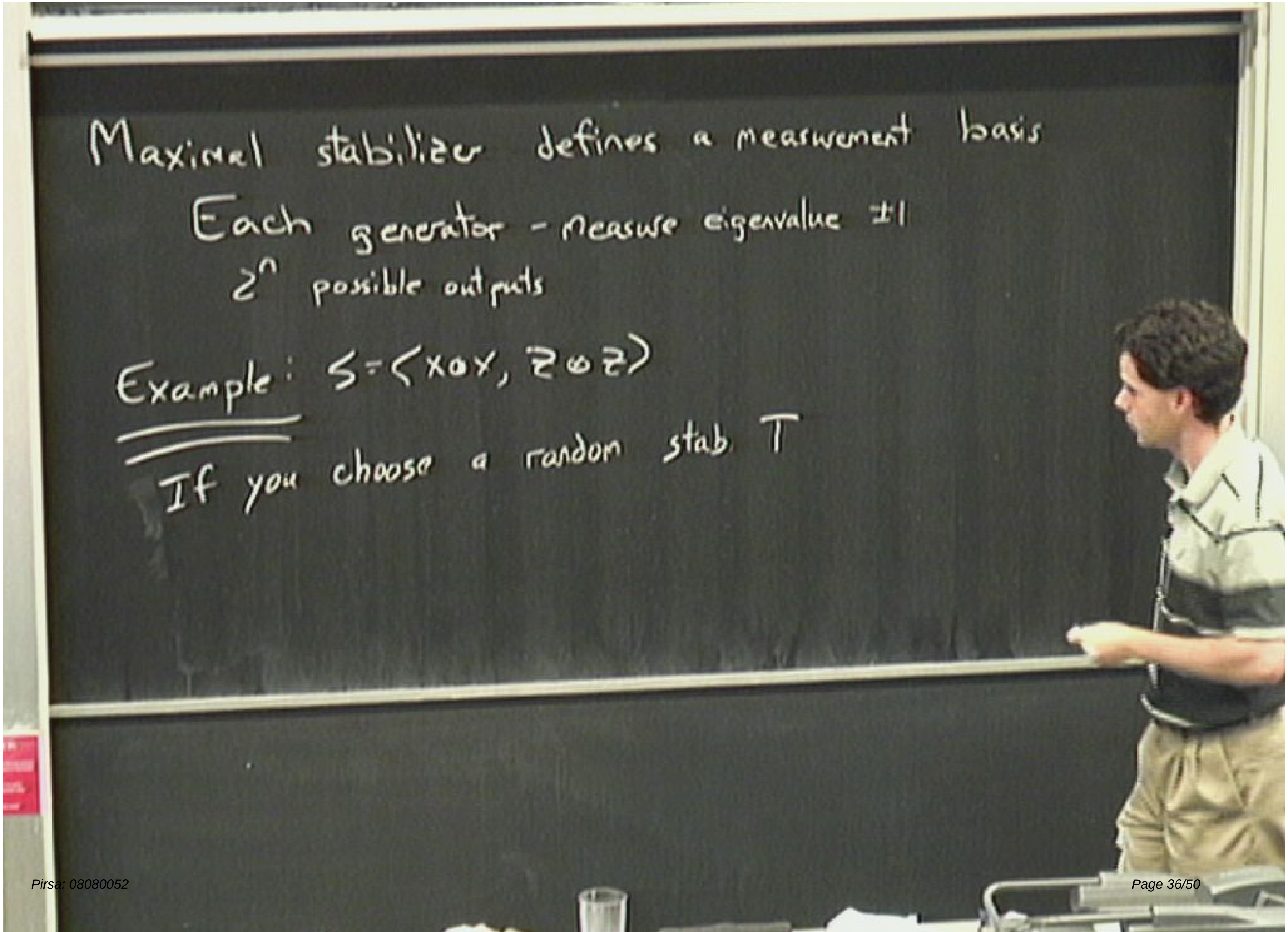
Maximal stabilizer defines a measurement basis

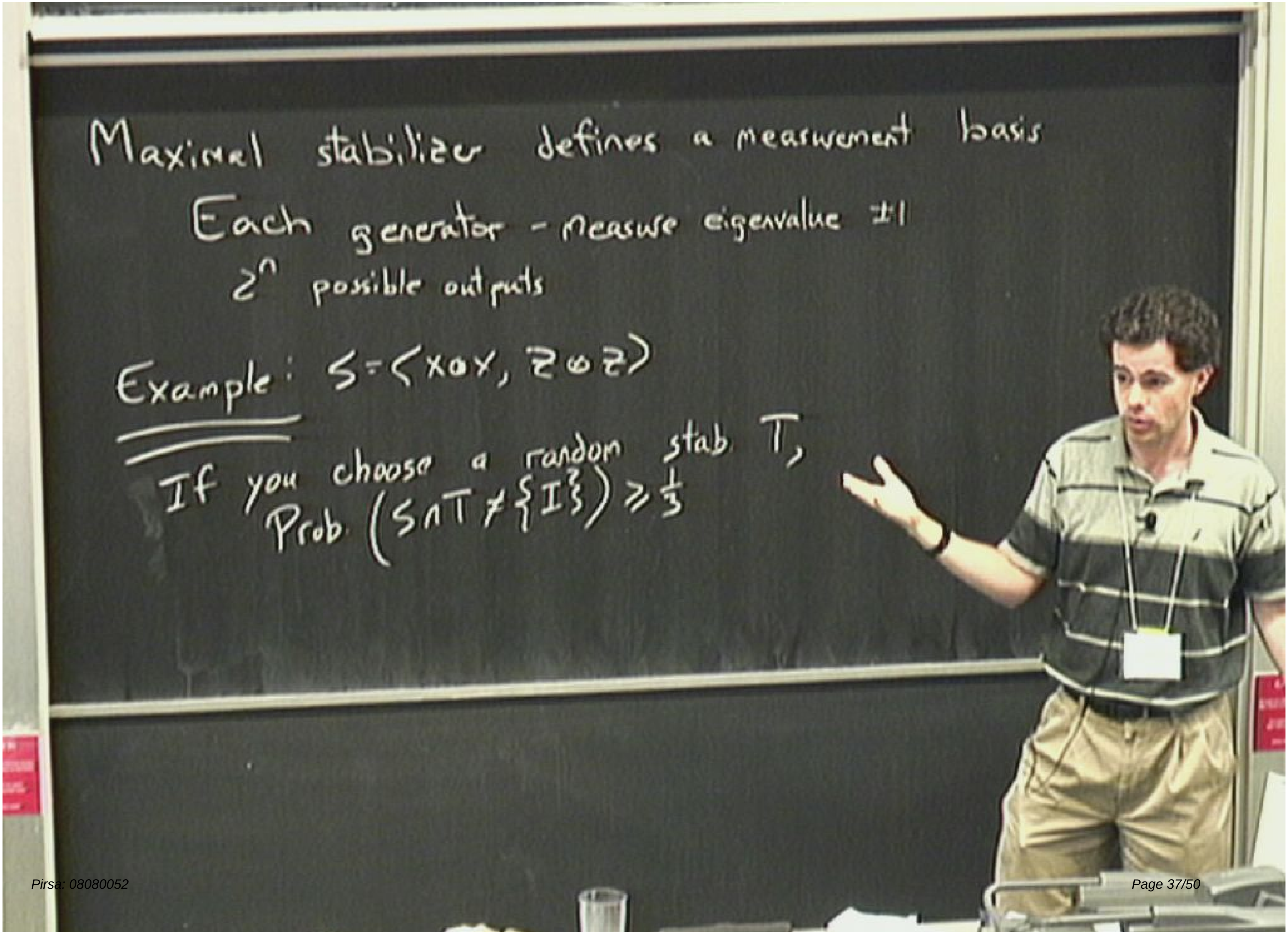
Each generator - measure eigenvalue ± 1

2^n possible outputs

Example: $S = \langle X \otimes X, Z \otimes Z \rangle$


Maximal stabilizer defines a measurement basis
Each generator - measure eigenvalue ± 1
2^n possible outputs
Example: $S = \langle X \otimes X, Z \otimes Z \rangle$


Maximal stabilizer defines a measurement basis
Each generator - measure eigenvalue ± 1
2^n possible outputs
Example: $S = \langle X \otimes X, Z \otimes Z \rangle$
If you choose a random stab T


Maximal stabilizer defines a measurement basis
Each generator - measure eigenvalue ±1
2^n possible outputs
Example: $S = \langle X \otimes X, Z \otimes Z \rangle$
If you choose a random stab. T,
Prob $(S \cap T \neq \{I\}) \geq \frac{1}{3}$

Maximal stabilizer defines a measurement basis

Each generator - measure eigenvalue ± 1

2^n possible outputs

Example: $S = \langle X \otimes X, Z \otimes Z \rangle$

If you choose a random stab T,

$\text{Prob}\left(S \cap T \neq \{I\} \right) \geq \frac{1}{3}$

Maximal stabilizer defines a measurement basis

Each generator - measure eigenvalue ± 1

2^n possible outputs

Example: $S = \langle X \otimes X, Z \otimes Z \rangle$

If you choose a random stab T,

Prob $\left(S \cap T \neq \{I\}\right) \geq \frac{1}{3}$

Maximal stabilizer defines a measurement basis

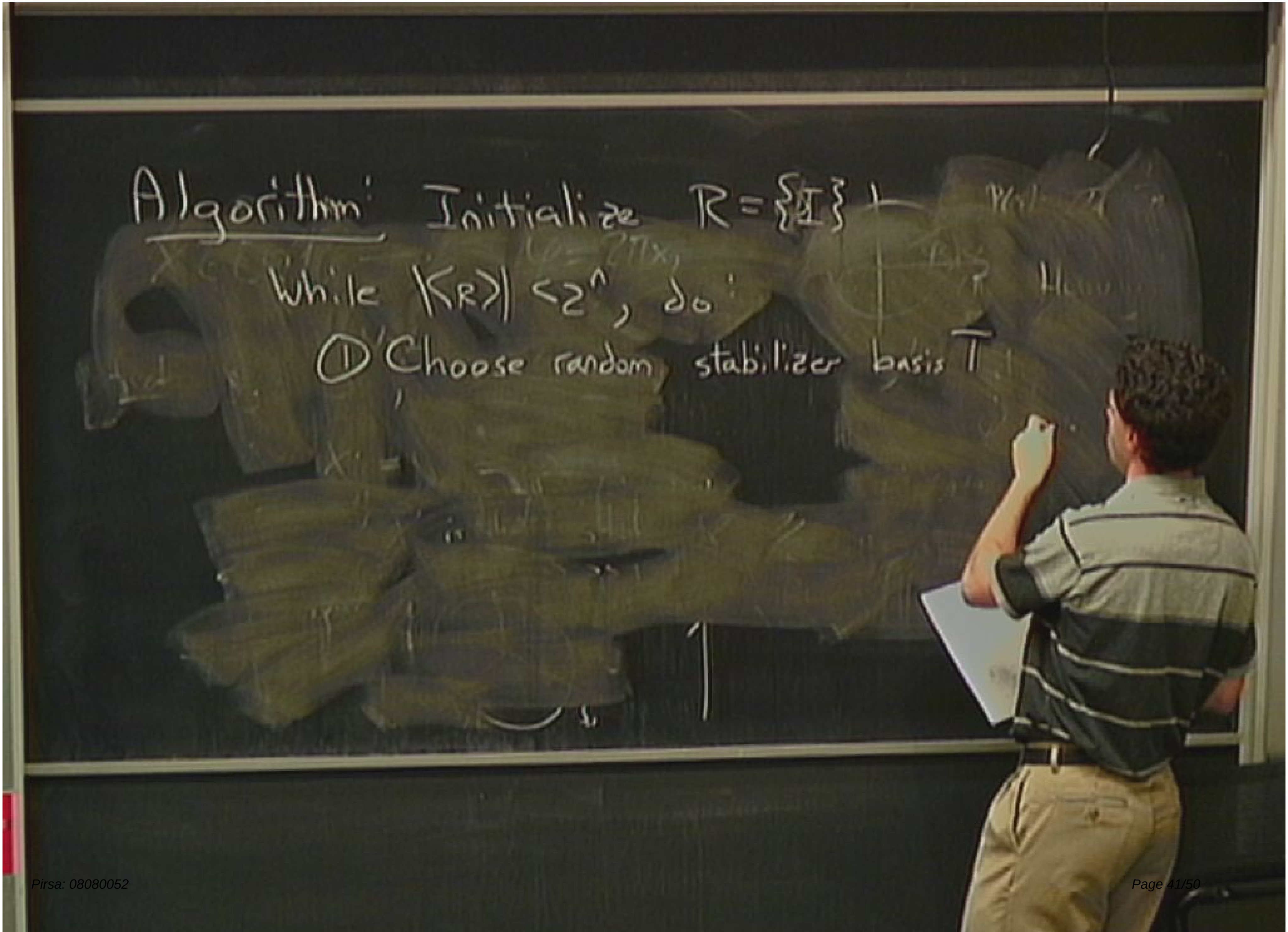
Each generator - measure eigenvalue ± 1

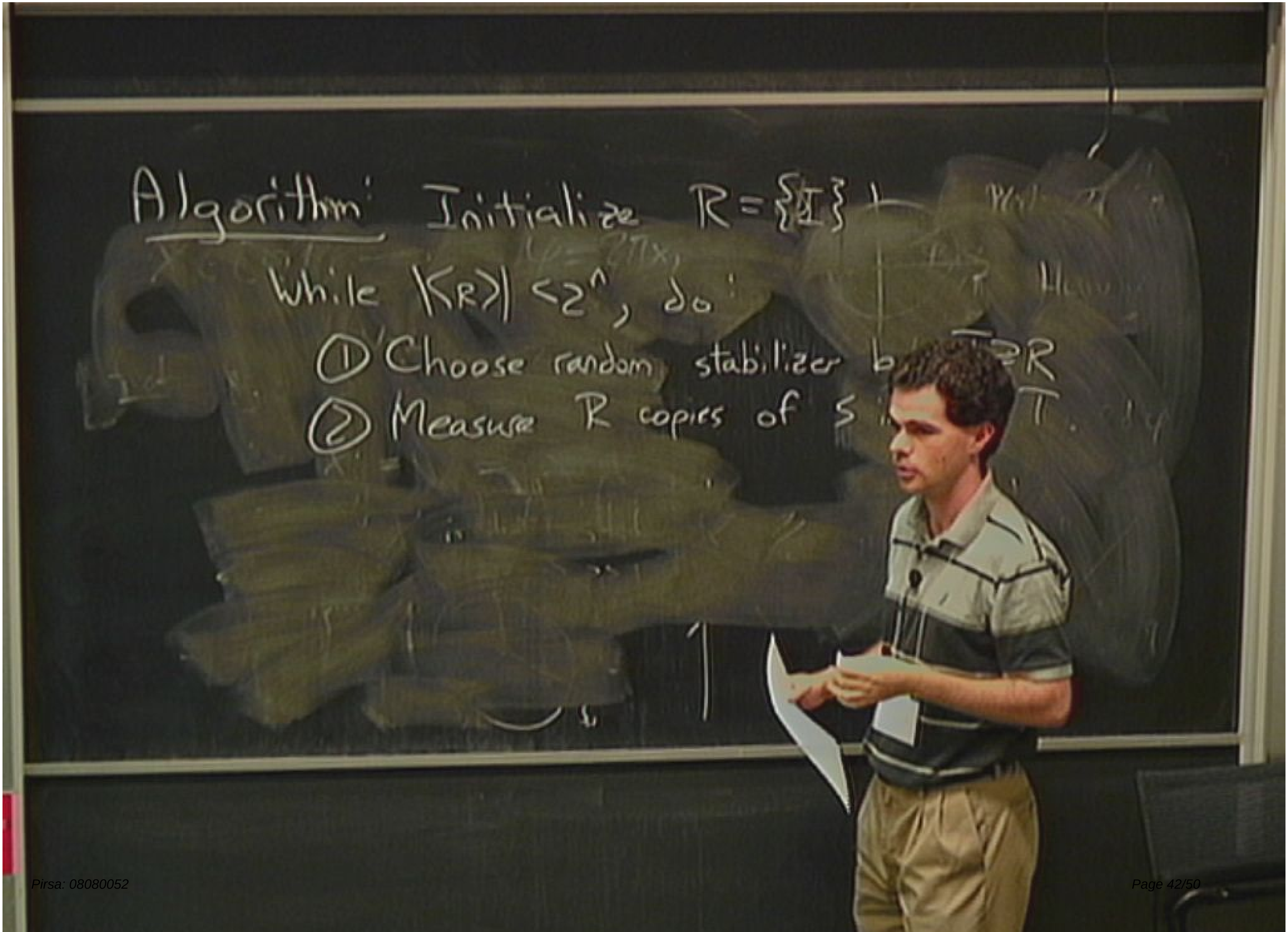
2^n possible outputs

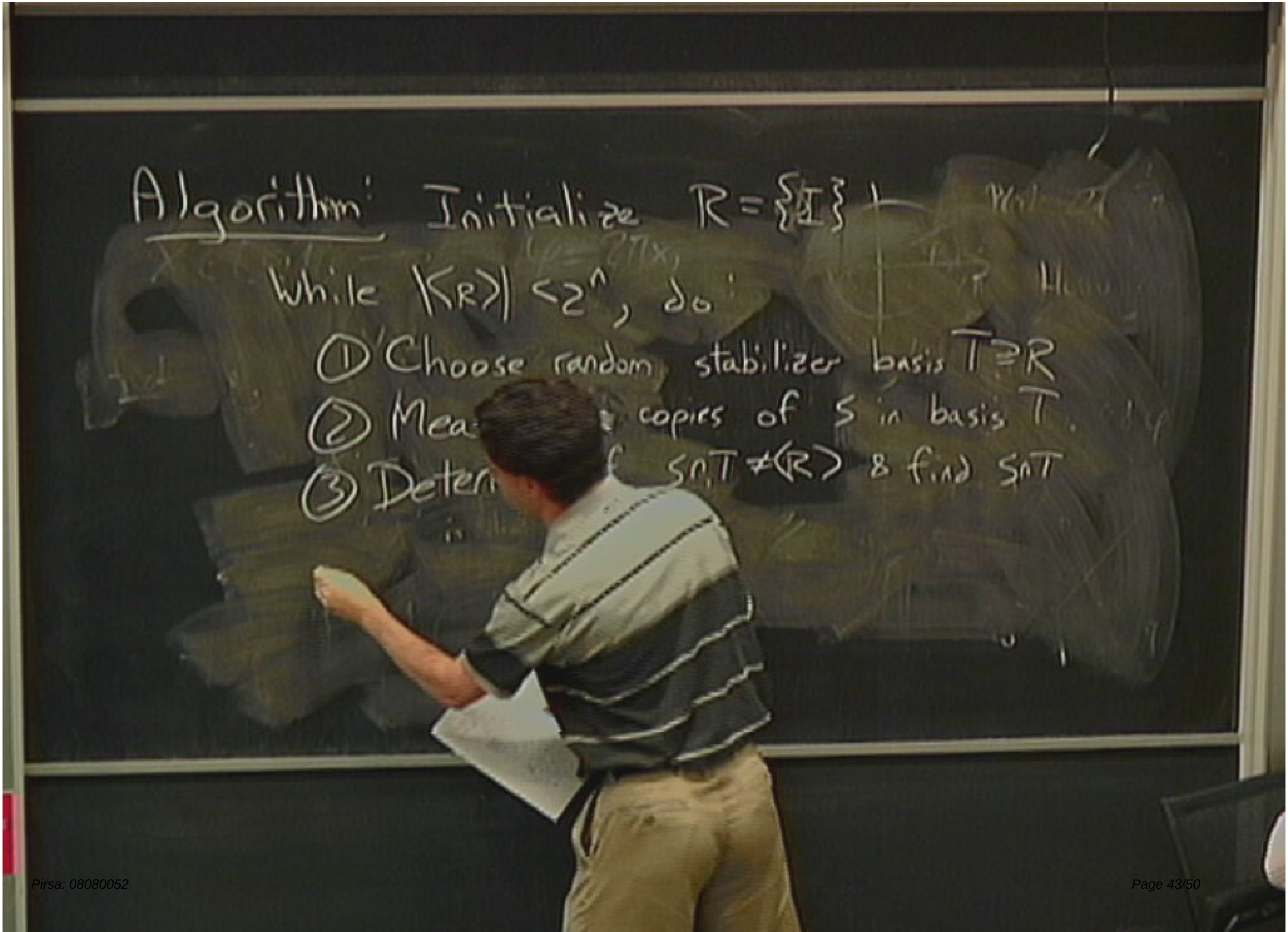
Example: $S = \langle X \otimes X, Z \otimes Z \rangle$

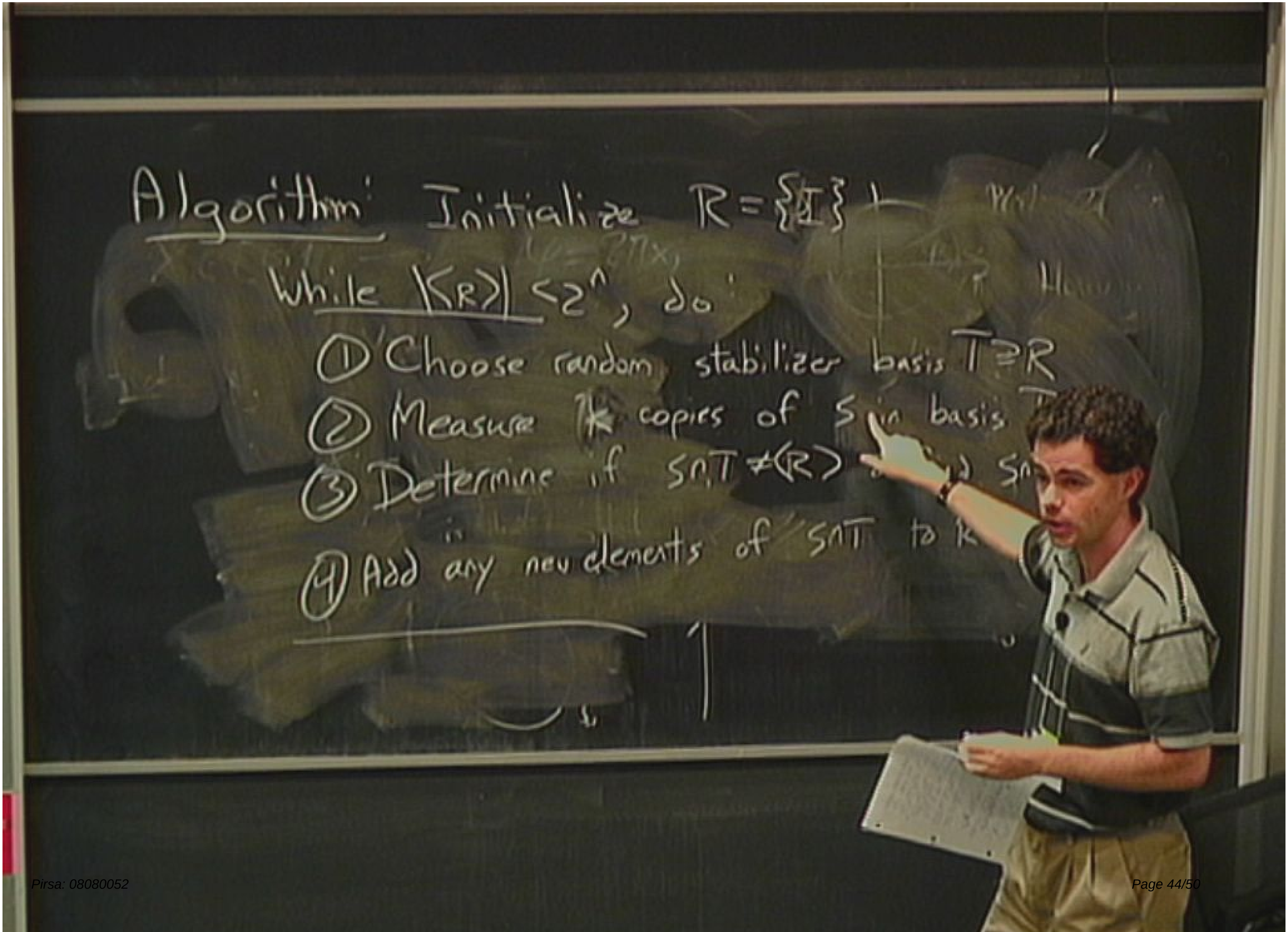
If you choose a random stab T,

Prob $\left(S \cap T \neq \{I\} \right) \geq \frac{1}{3}$


Algorithm: Initialize R = {I}
While |⟨R⟩| < 2^n, do:
① Choose random stabilizer basis T


Algorithm: Initialize R = {I}
While |⟨R⟩| < 2^n, do:
① Choose random stabilizer
② Measure R copies of S


Algorithm: Initialize $R = \{I\}$
While $|\langle R \rangle| < 2^n$, do:
① Choose random stabilizer basis $T \supseteq R$
② Mea copies of S in basis T.
③ Deter $S \cap T \neq \langle R \rangle$ & find $S \cap T$


Algorithm: Initialize R = {I}
While |⟨R⟩| < 2^n, do:
① Choose random stabilizer basis T ⊇ R
② Measure k copies of S in basis
③ Determine if S∩T ≠ ⟨R⟩
④ Add any new elements of S∩T to

Algorithm: Initialize $R = \{I\}$

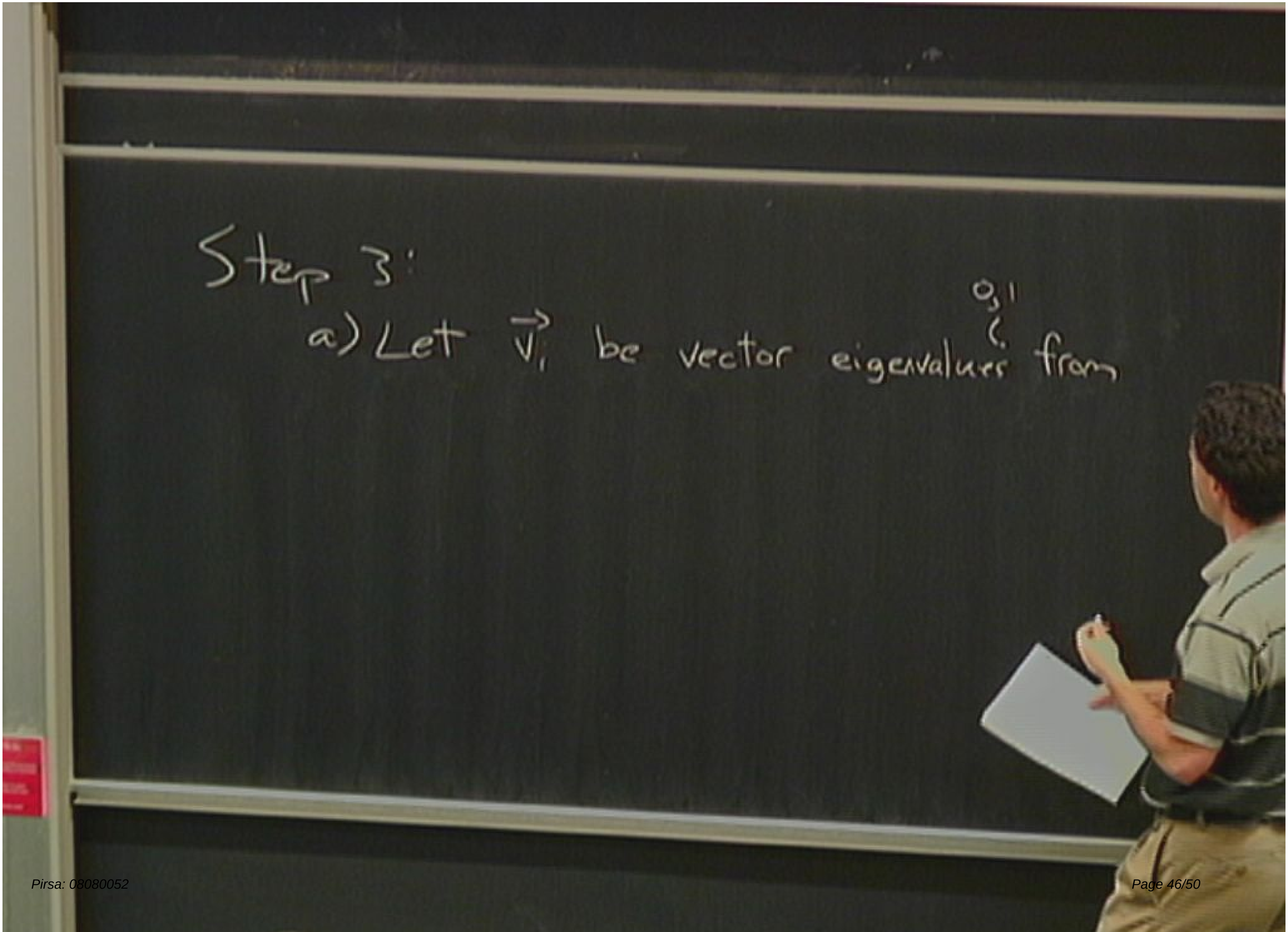
While $|\langle R \rangle| < 2^n$, do:

① Choose random stabilizer basis $T \supseteq R$

② Measure $k = O(n)$ copies of S in basis T.

③ Determine if $S \cap T \neq \langle R \rangle$ & find $S \cap T$

④ Add any new elements of $S \cap T$ to R

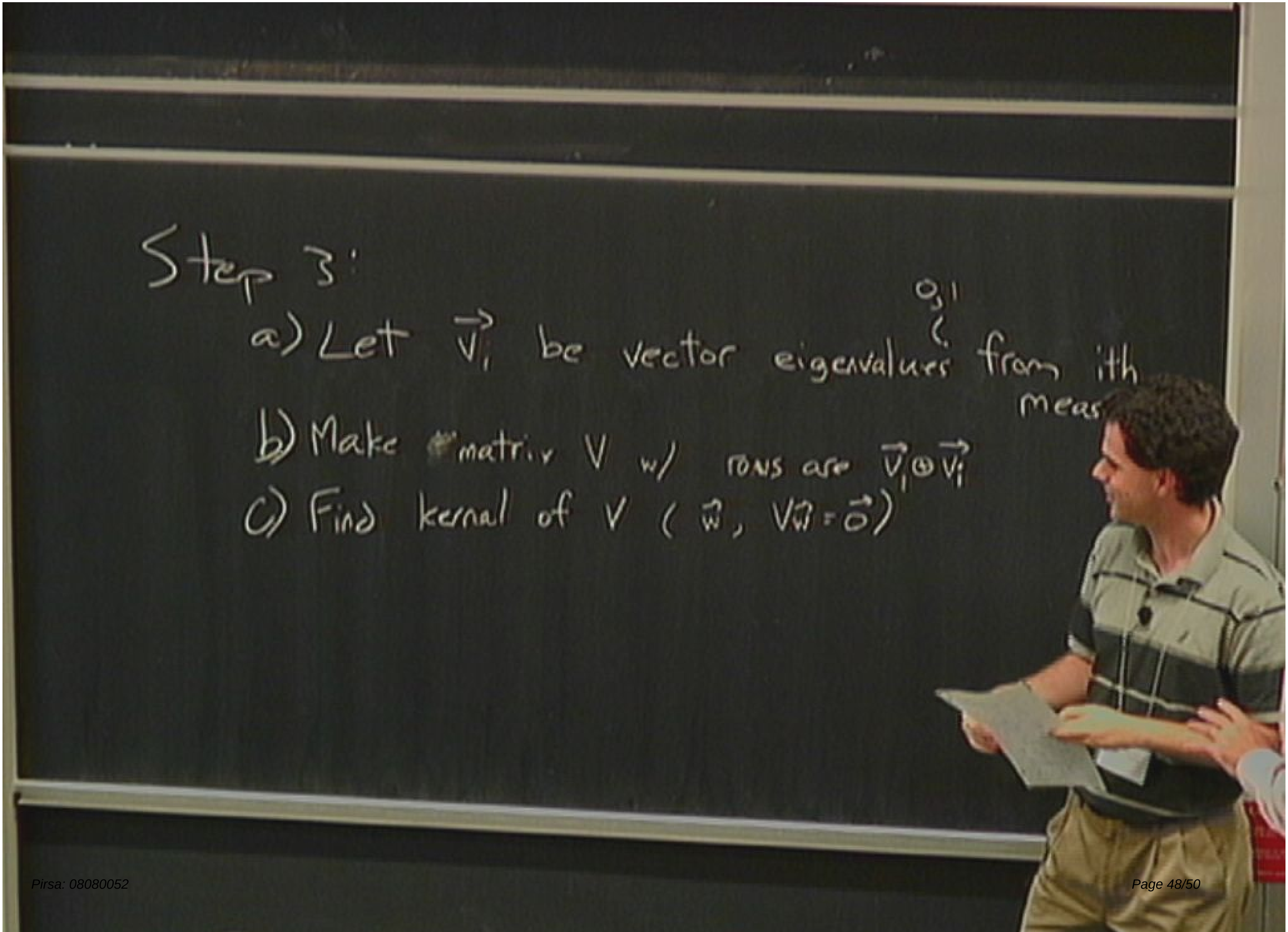

Step 3:
0,1
a) Let v⃗ᵢ be vector eigenvalues i from

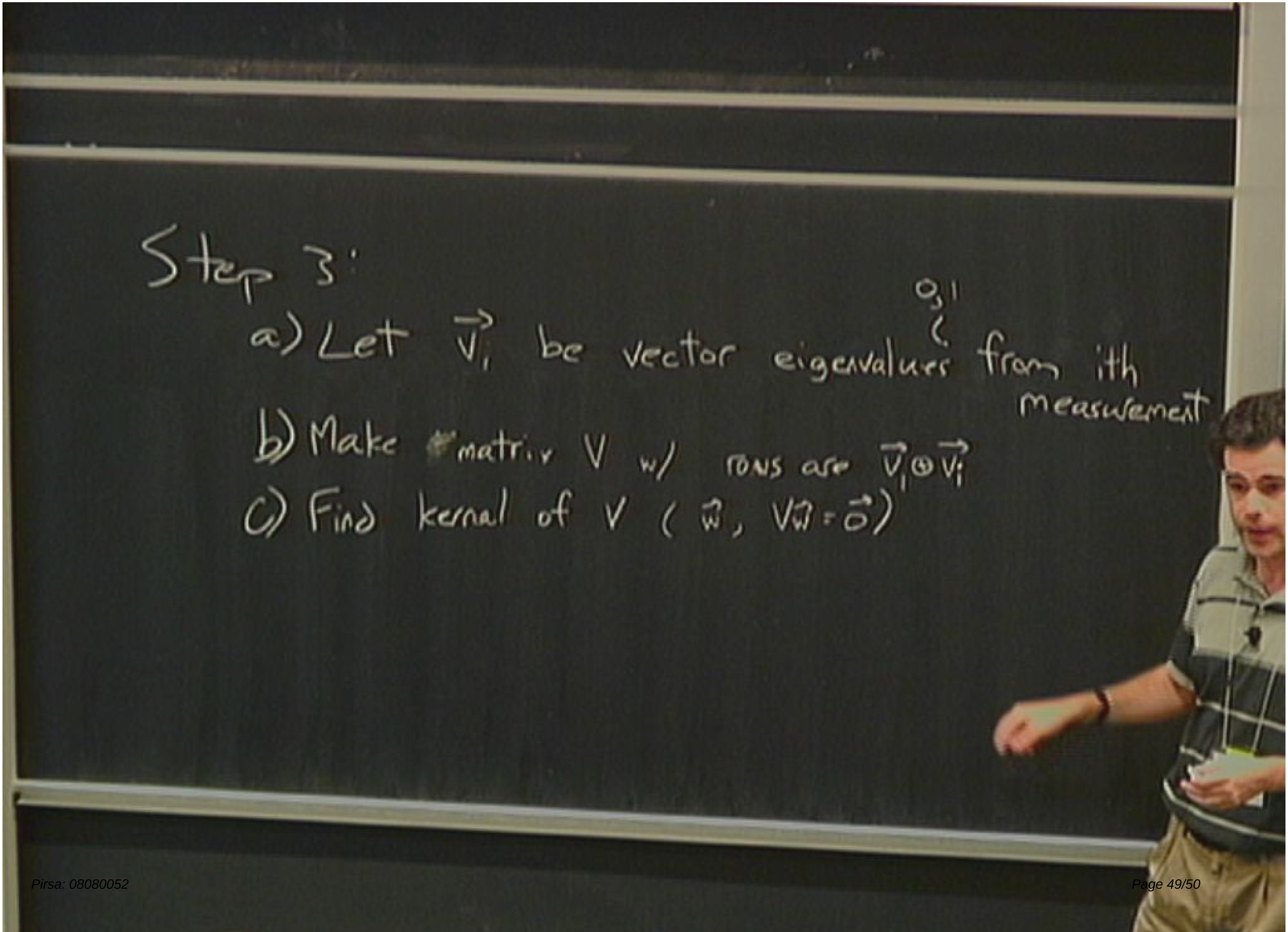
Step 3:

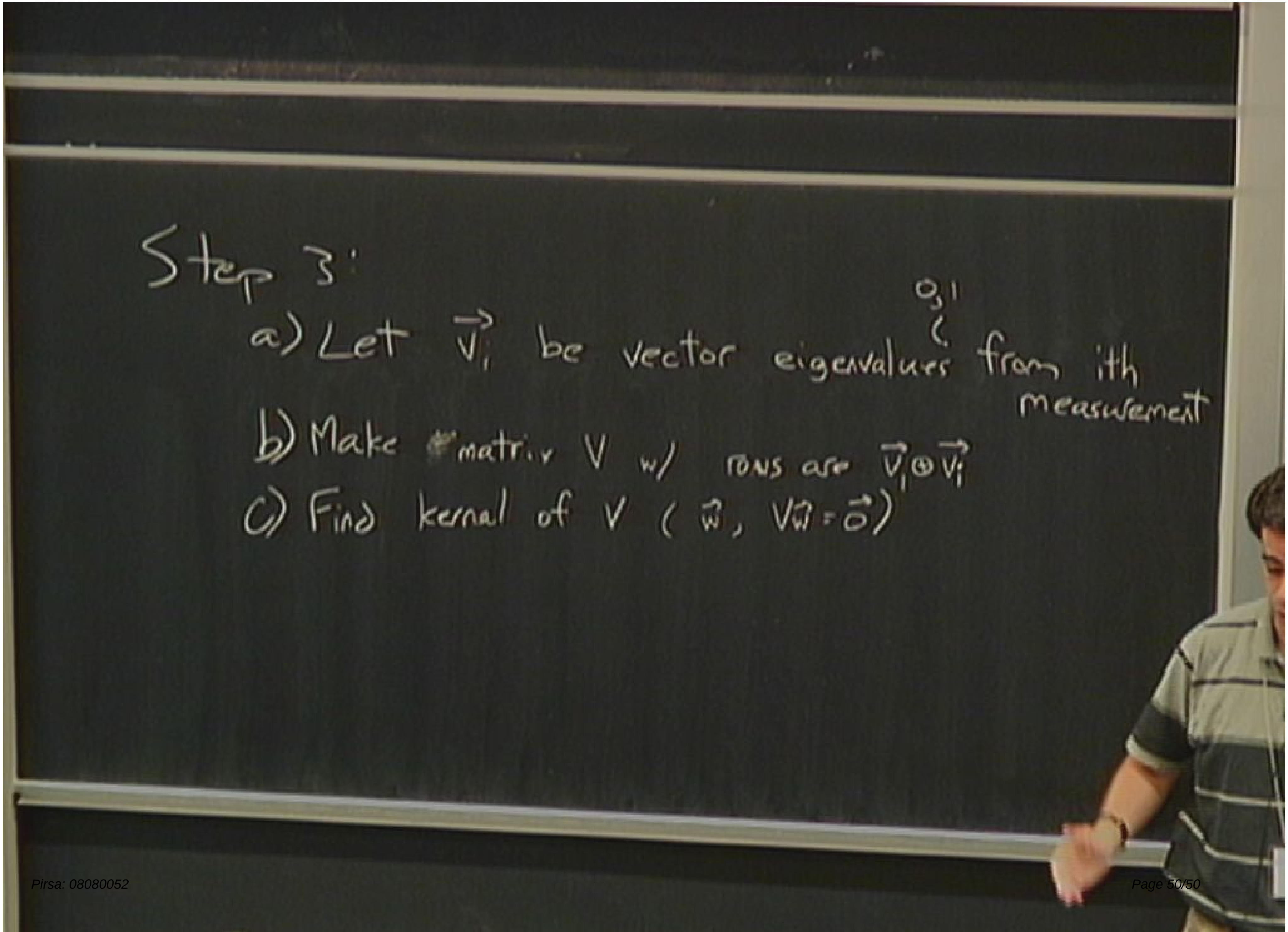
a) Let $\vec{v}_i$ be vector eigenvalues from ith measurem...

0,1

b) Make matrix V w/ rows are $\vec{v}_1 \oplus \vec{v}_i$


Step 3:
0,1
a) Let $\vec{v}_i$ be vector eigenvalues from ith meas
b) Make matrix V w/ rows are $\vec{v}_i \otimes \vec{v}_i$
c) Find kernal of V ($\vec{w}$, $V\vec{w} = \vec{0}$)


Step 3:
0,1
a) Let v⃗_i be vector eigenvalues from ith
measurement
b) Make matrix V w/ rows are v⃗_i ⊗ v⃗_i
c) Find kernal of V (w⃗, Vw⃗ = 0⃗)


Step 3:
0,1
a) Let $\vec{V}_i$ be vector eigenvalues from ith
measurement
b) Make matrix V w/ rows are $\vec{V}_i \otimes \vec{V}_i$
c) Find kernal of V ($\vec{w}$, $V\vec{w} = \vec{0}$)