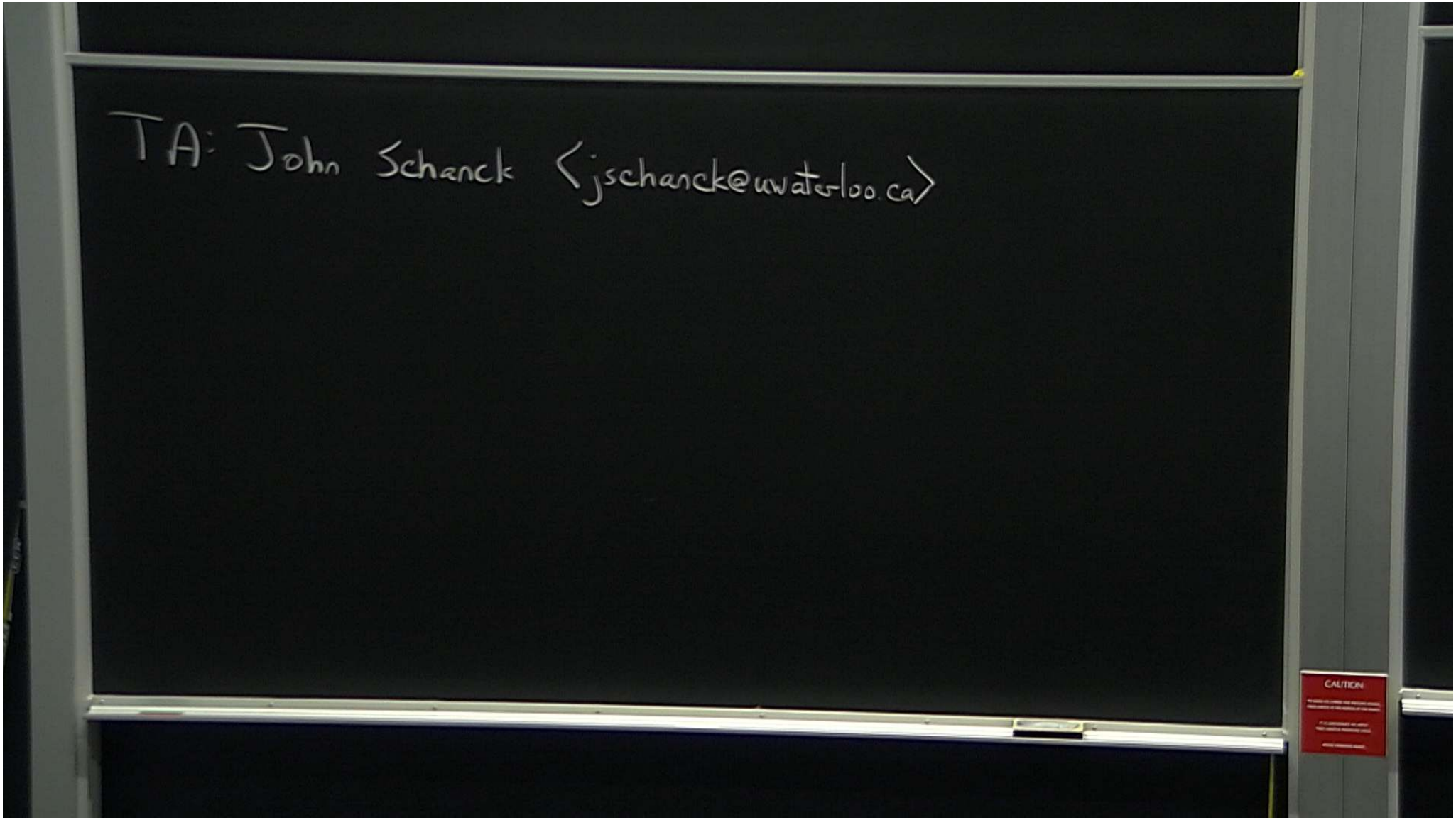
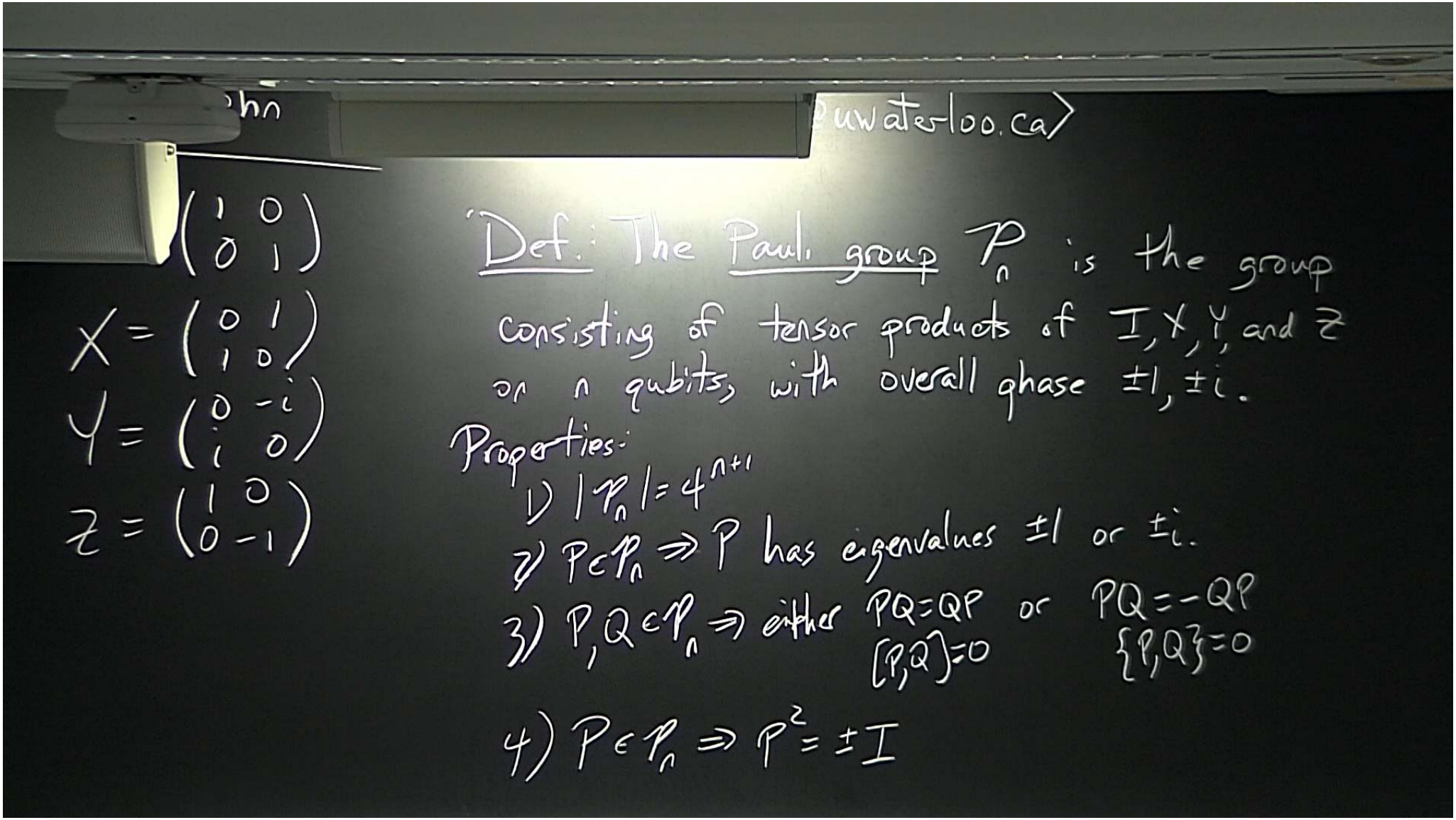
Title: IQC - Quantum Error Correction - Lecture 2

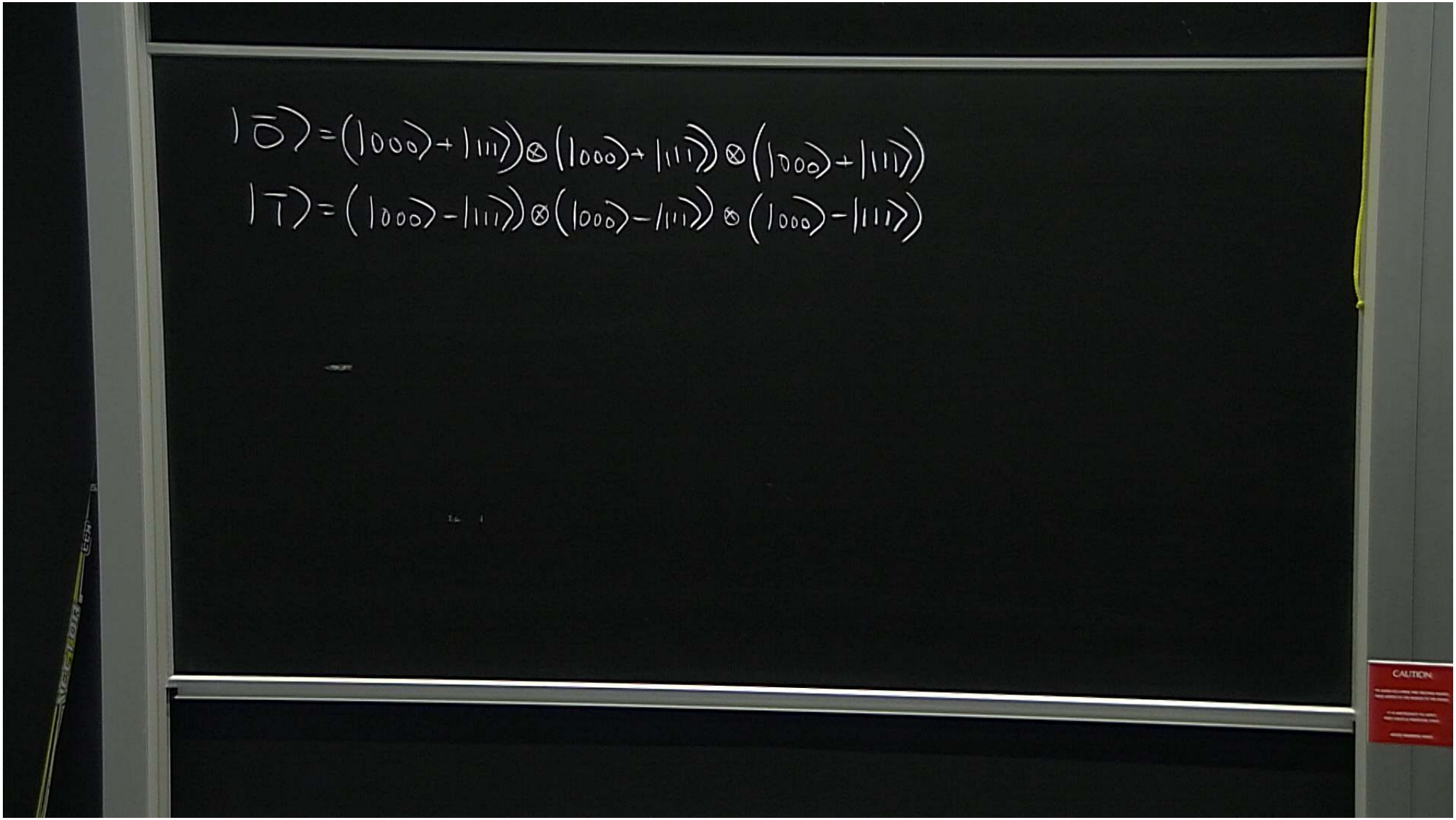
Date: Jan 11, 2018 02:00 PM

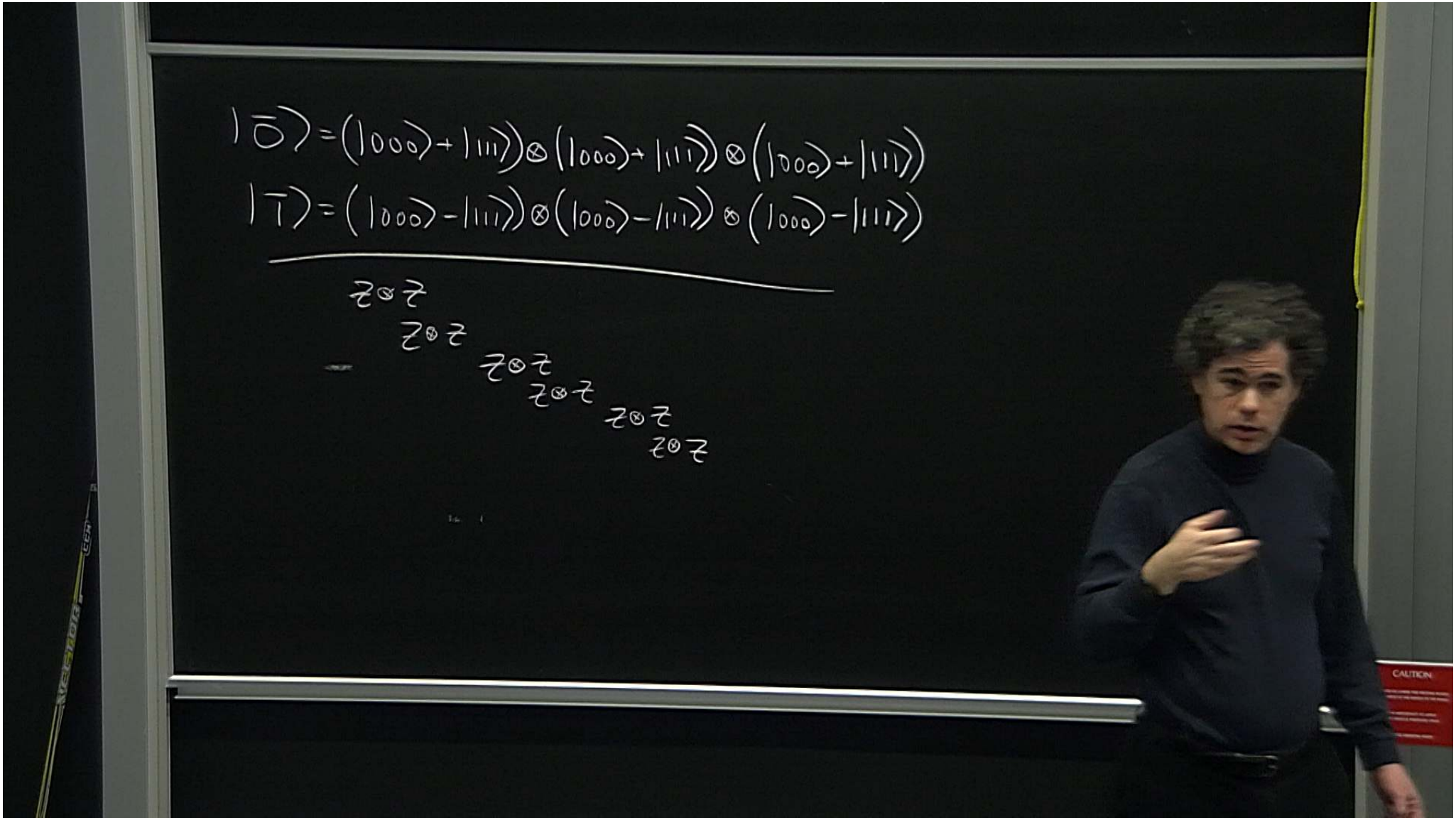
URL: http://pirsa.org/18010048

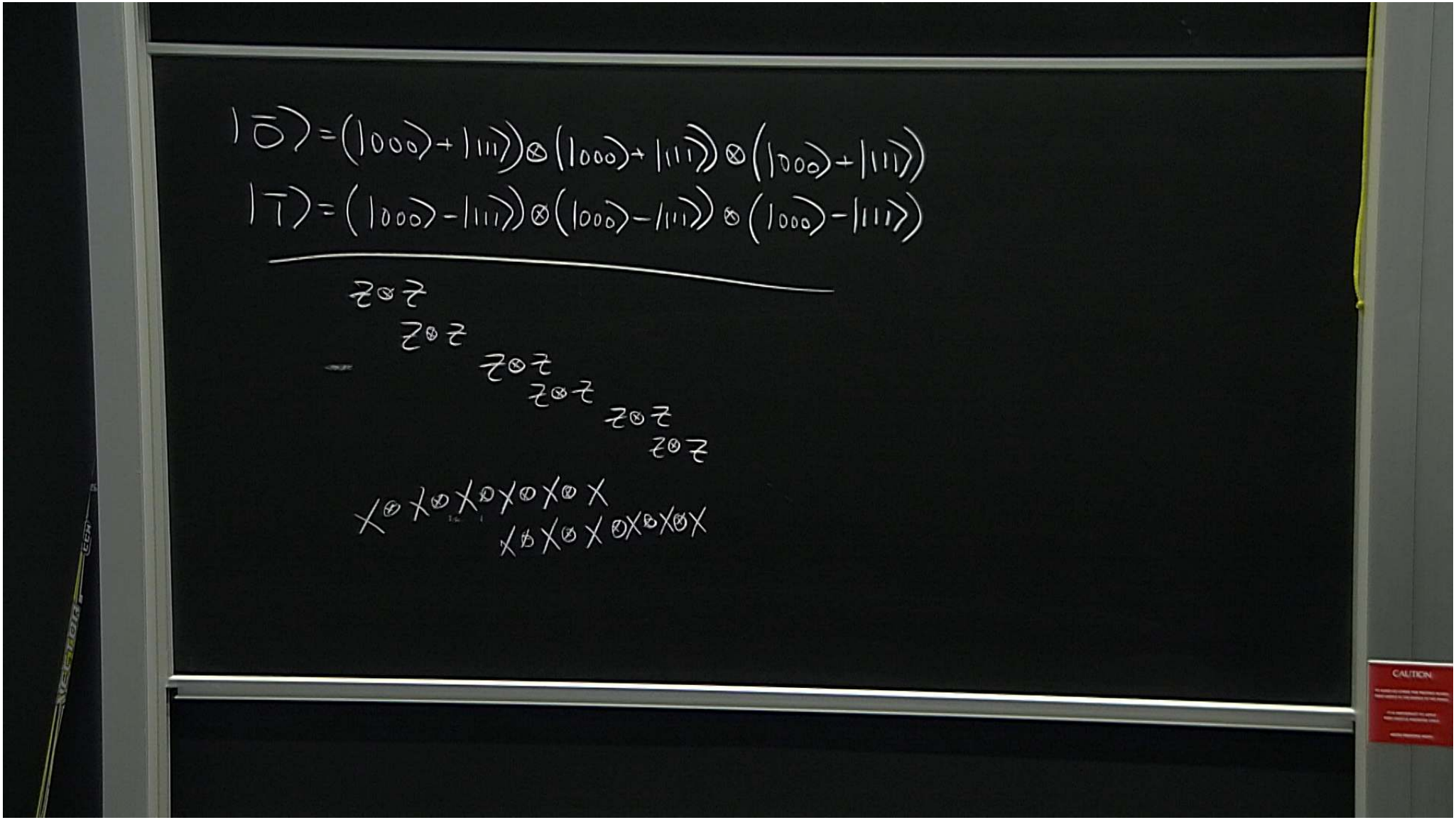
Abstract:


TA: John Schanck <jschanck@uwaterloo.ca>
CAUTION


hn
uwaterloo.ca
$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Def: The Pauli group $\mathcal{P}_n$ is the group consisting of tensor products of I, X, Y, and Z on n qubits, with overall phase $\pm 1, \pm i$.
Properties:
1) $|\mathcal{P}_n| = 4^{n+1}$
2) $P \in \mathcal{P}_n \Rightarrow P$ has eigenvalues ± 1 or $\pm i$.
3) $P, Q \in \mathcal{P}_n \Rightarrow$ either $PQ = QP$ or $PQ = -QP$
$[P,Q] = 0$ $\{P,Q\} = 0$
4) $P \in \mathcal{P}_n \Rightarrow P^2 = \pm I$


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


$|\bar{0}\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$
$|\bar{1}\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$
$z \otimes z$
$z \otimes z$
$z \otimes z$
$z \otimes z$
$z \otimes z$
$z \otimes z$
CAUTION


$|\bar{0}\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$
$|\bar{1}\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$
Z⊗Z
Z⊗Z
Z⊗Z
Z⊗Z
Z⊗Z
Z⊗Z
X⊗X⊗X⊗X⊗X⊗X
X⊗X⊗X⊗X⊗X⊗X
CAUTION

Def. Given code Q, let the stabilizer of Q be

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

Properties of stabilizers:

1) $-I \notin S(Q)$

2) $S(Q)$ is a group $\longrightarrow$ $M, N \in S(Q)$, $MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$

3) $S(Q)$ is Abelian $\longrightarrow$ $M, N \in S(Q)$, $(MN - NM)|\psi\rangle = 0$

Def: Given code Q, let the **stabilizer** of Q be

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

Properties of stabilizers:

1) $-I \notin S(Q)$

2) $S(Q)$ is a group $\longrightarrow$ $M, N \in S(Q)$
$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$

3) $S(Q)$ is Abelian $\longrightarrow$ $M, N \in S(Q)$
$(MN - NM)|\psi\rangle = 0$
$M, N \in \mathcal{P}_n \Rightarrow (M,N) = 0$ or $\{M,N\} = 0$
$\Downarrow$
$(M,N) = 0$
$MN - NM \neq 2MN$

Def. Given code Q, let the **stabilizer** of Q be

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

Properties of stabilizers:

1) $-I \notin S(Q)$

2) $S(Q)$ is a group $\longrightarrow$ $M, N \in S(Q)$
$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$

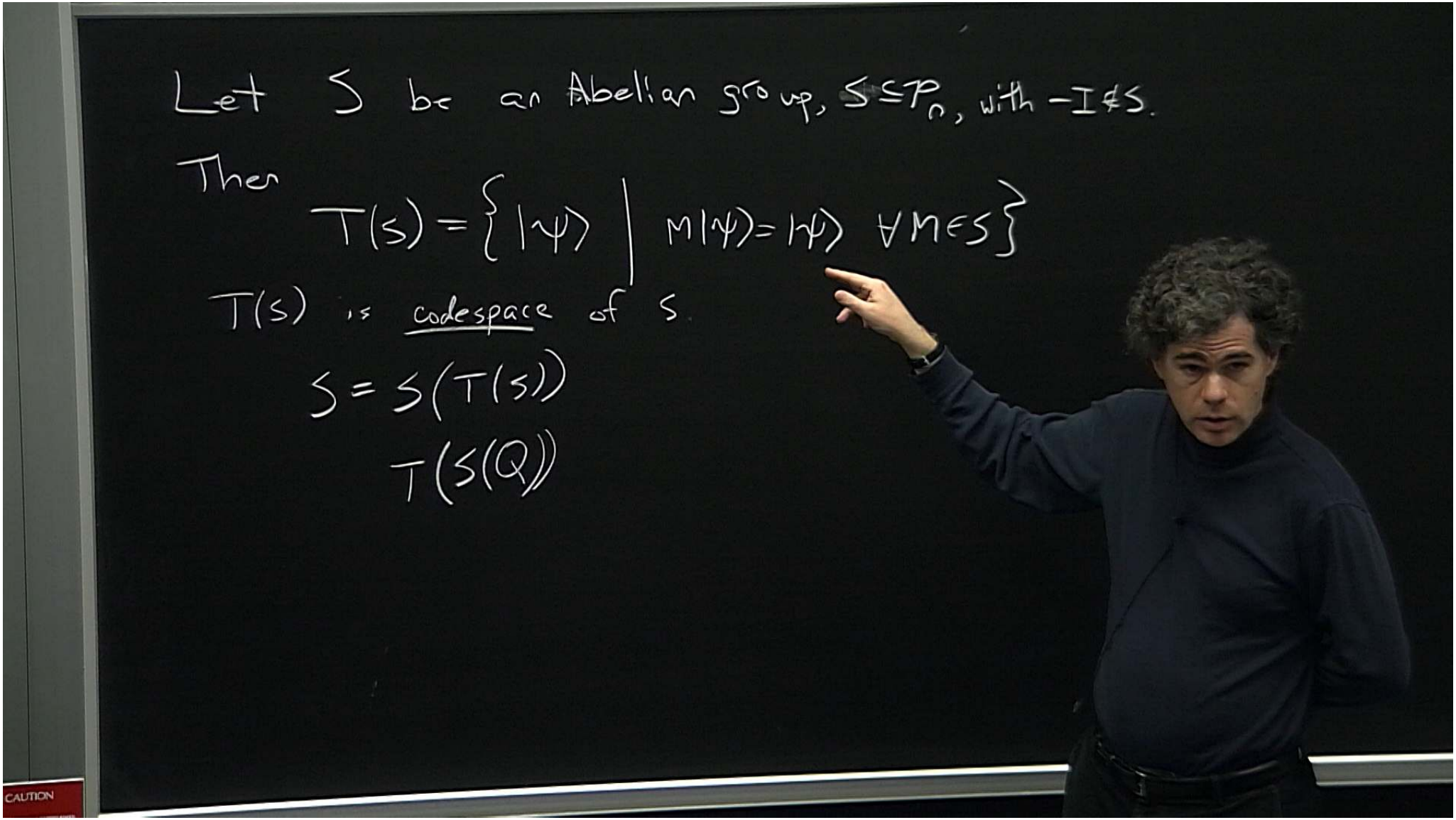
3) $S(Q)$ is Abelian $\longrightarrow$ $M, N \in S(Q)$
$(MN - NM)|\psi\rangle = 0$
$M, N \in \mathcal{P}_n \Rightarrow (M,N) = 0$ or $\{M,N\} = 0$
$\Downarrow$ $\quad\quad$ $\downarrow$
$(M,N) = 0$ $\quad\quad$ $MN - NM \neq 2MN$

---

r generators $M_1, \ldots, M_r$; $M_i^2 = I$

$M_1^{a_1} M_2^{a_2} \cdots M_r^{a_r}$ $\quad\quad$ $|S(Q)| = 2^r$

$a_1, \ldots a_r \in \{0,1\}$


Let S be an Abelian group, $S \subseteq \mathcal{P}_n$, with $-I \notin S$.
Then
$T(S) = \{ |\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S \}$
$T(S)$ is codespace of S.
$S = S(T(S))$
$T(S(Q))$
CAUTION

Let S be an Abelian group, $S \subseteq \mathcal{P}_n$, with $-I \notin S$.

Then

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

$T(S)$ is <u>codespace</u> of S.

$$S = S(T(S))$$

If $Q = T(S(Q))$, then Q is a <u>stabilizer code</u>.

Let S be an Abelian group, $S \subseteq \mathcal{P}_n$, with $-I \notin S$.

Then

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

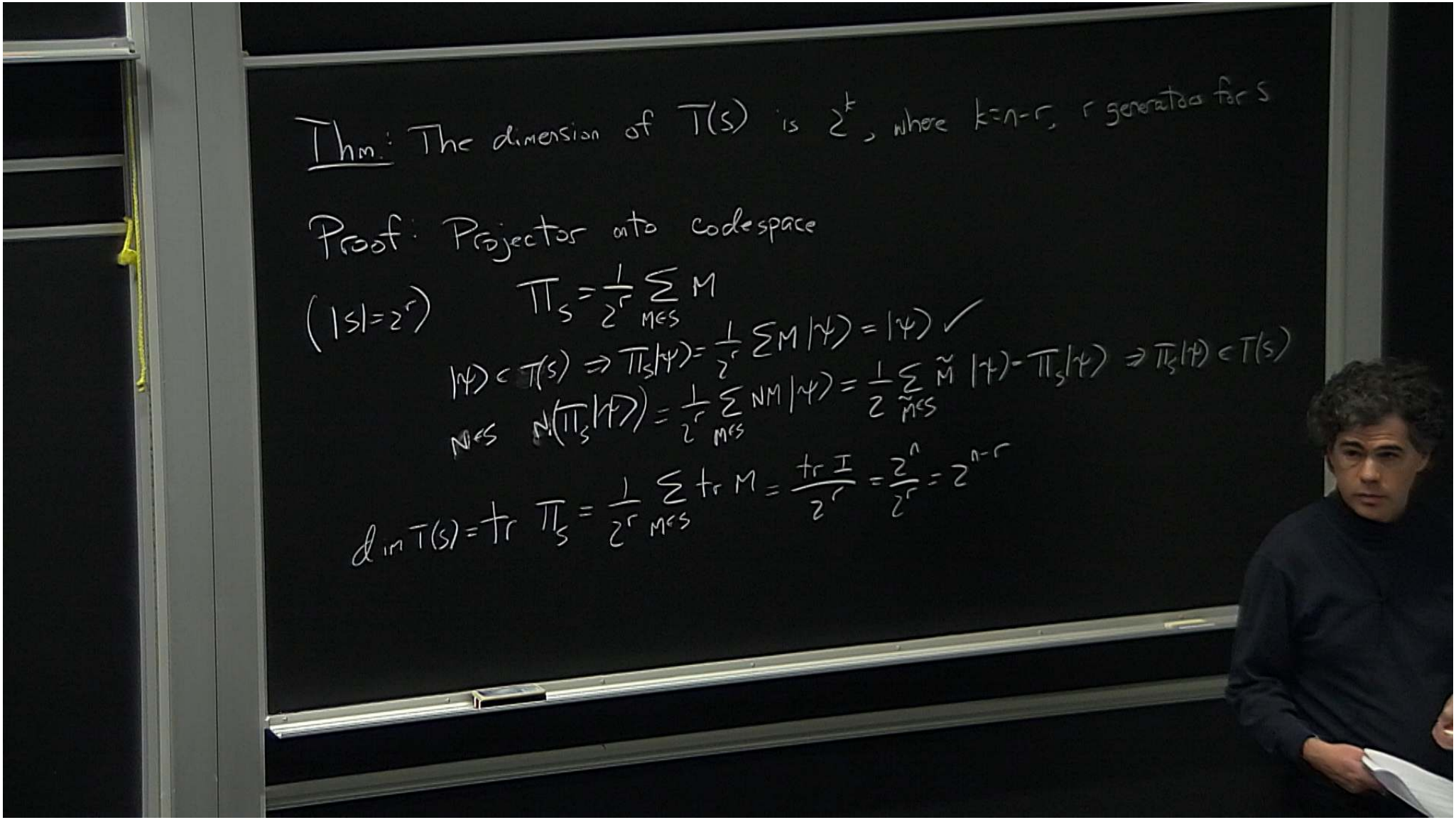
$T(S)$ is <u>codespace</u> of S.

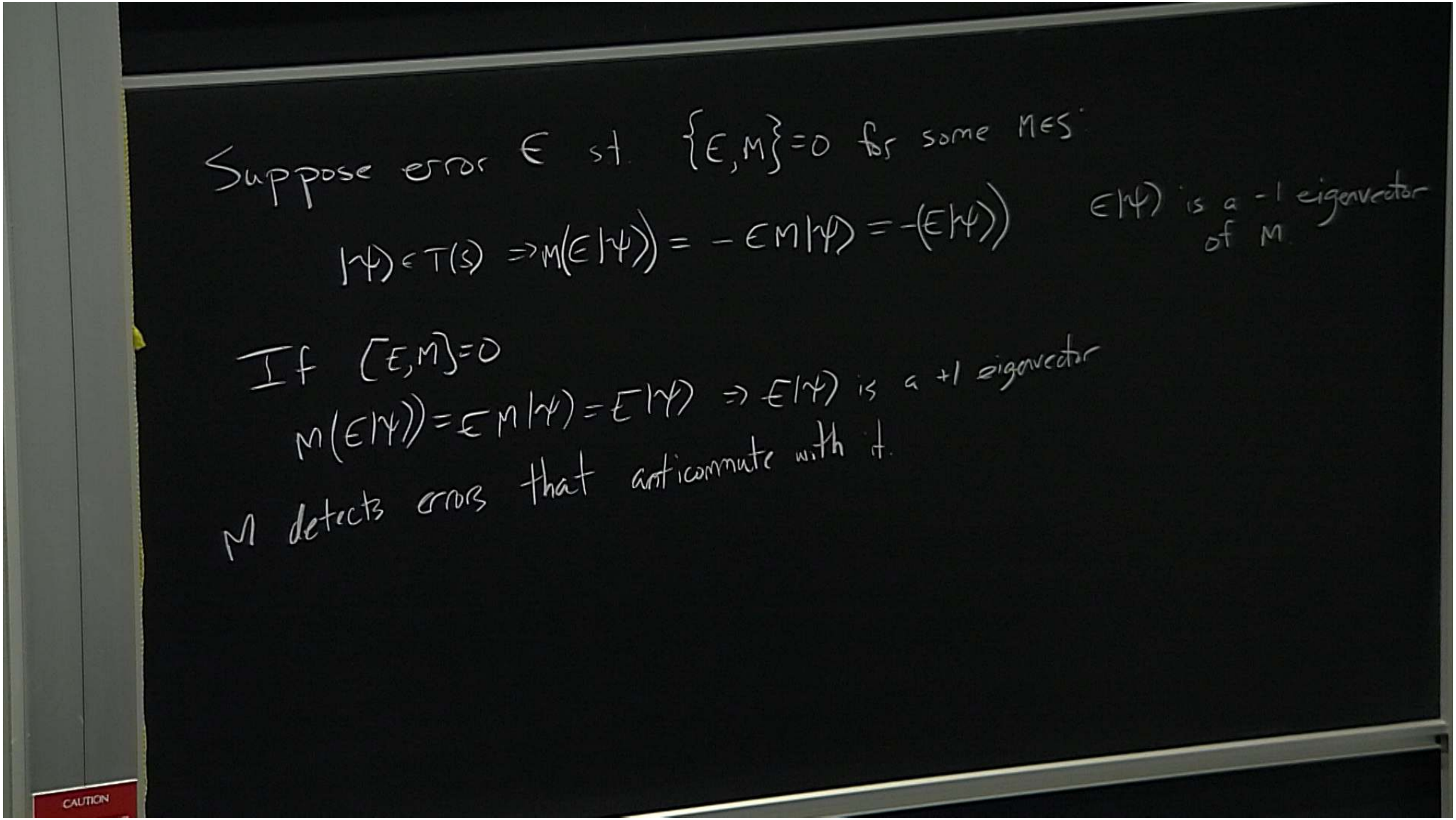
$$S = S(T(S))$$

If $Q = T(S(Q))$, then Q is a <u>stabilizer code</u>.

E.g. non-stabilizer code $|\bar{0}\rangle = |00\rangle$

$|\bar{1}\rangle = |01\rangle + |10\rangle$


Thm: The dimension of T(S) is 2^k, where $k=n-r$, r generators for S
Proof: Projector onto codespace
$(|S|=2^r)$ $\Pi_S = \frac{1}{2^r}\sum_{M\in S} M$
$|\psi\rangle \in T(S) \Rightarrow \Pi_S|\psi\rangle = \frac{1}{2^r}\sum M|\psi\rangle = |\psi\rangle$ ✓
$N\in S$ $N(\Pi_S|\psi\rangle) = \frac{1}{2^r}\sum_{M\in S} NM|\psi\rangle = \frac{1}{2}\sum_{\tilde{M}\in S} \tilde{M}|\psi\rangle - \Pi_S|\psi\rangle \Rightarrow \Pi_S|\psi\rangle \in T(S)$
$\dim T(S) = \mathrm{tr}\,\Pi_S = \frac{1}{2^r}\sum_{M\in S}\mathrm{tr}\,M = \frac{\mathrm{tr}\,I}{2^r} = \frac{2^n}{2^r} = 2^{n-r}$


Suppose error E s.t. $\{E,M\}=0$ for some $M \in S$
$|\psi\rangle \in T(S) \Rightarrow M(E|\psi\rangle) = -EM|\psi\rangle = -(E|\psi\rangle)$
$E|\psi\rangle$ is a -1 eigenvector of M
If $[E,M]=0$
$M(E|\psi\rangle) = EM|\psi\rangle = E|\psi\rangle \Rightarrow E|\psi\rangle$ is a $+1$ eigenvector
M detects errors that anticommute with it.
CAUTION

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

Set of undetectable errors: $N(S) \setminus S$

Note that $S \subseteq N(S)$

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

Set of undetectable errors: $N(S) \setminus S$

Note that $S \subseteq N(S)$

Correct errors

E & F have ~~different~~ same syndromes error $\Leftrightarrow$ E & F commute w/ same elements of S

$\Leftrightarrow [E^\dagger F, M] = 0 \ \forall M \in S$

$\Leftrightarrow E^\dagger F \in N(S)$

Thm: S can correct a set $\mathcal{E} \subseteq \mathcal{P}_n$ iff $\forall E, F \in \mathcal{E}$ $E^\dagger F \notin N(S) \setminus S$

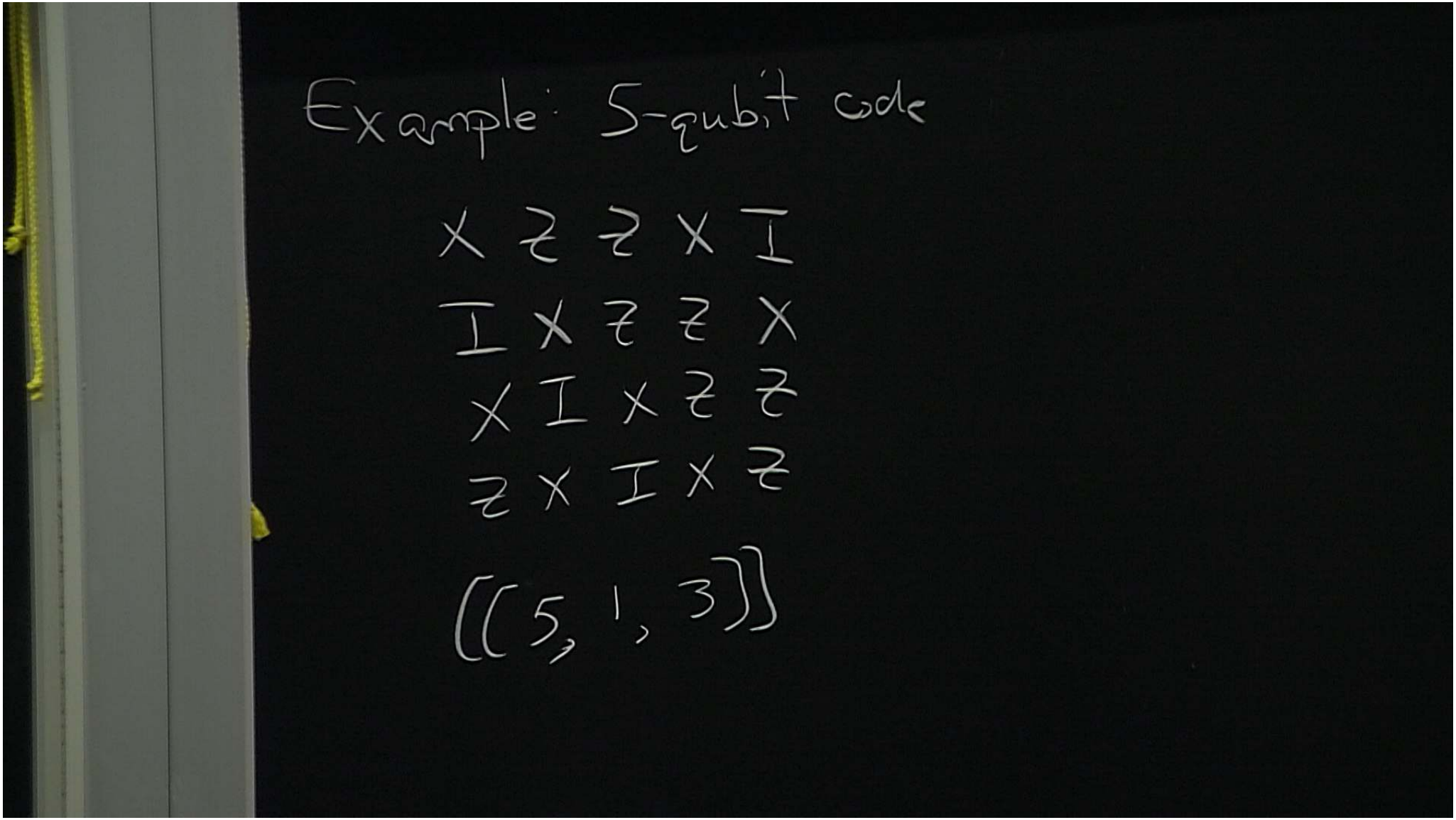
Cor: The distance of S is minimum weight of $N \in N(S) \setminus S$. The code is degenerate if this is no.

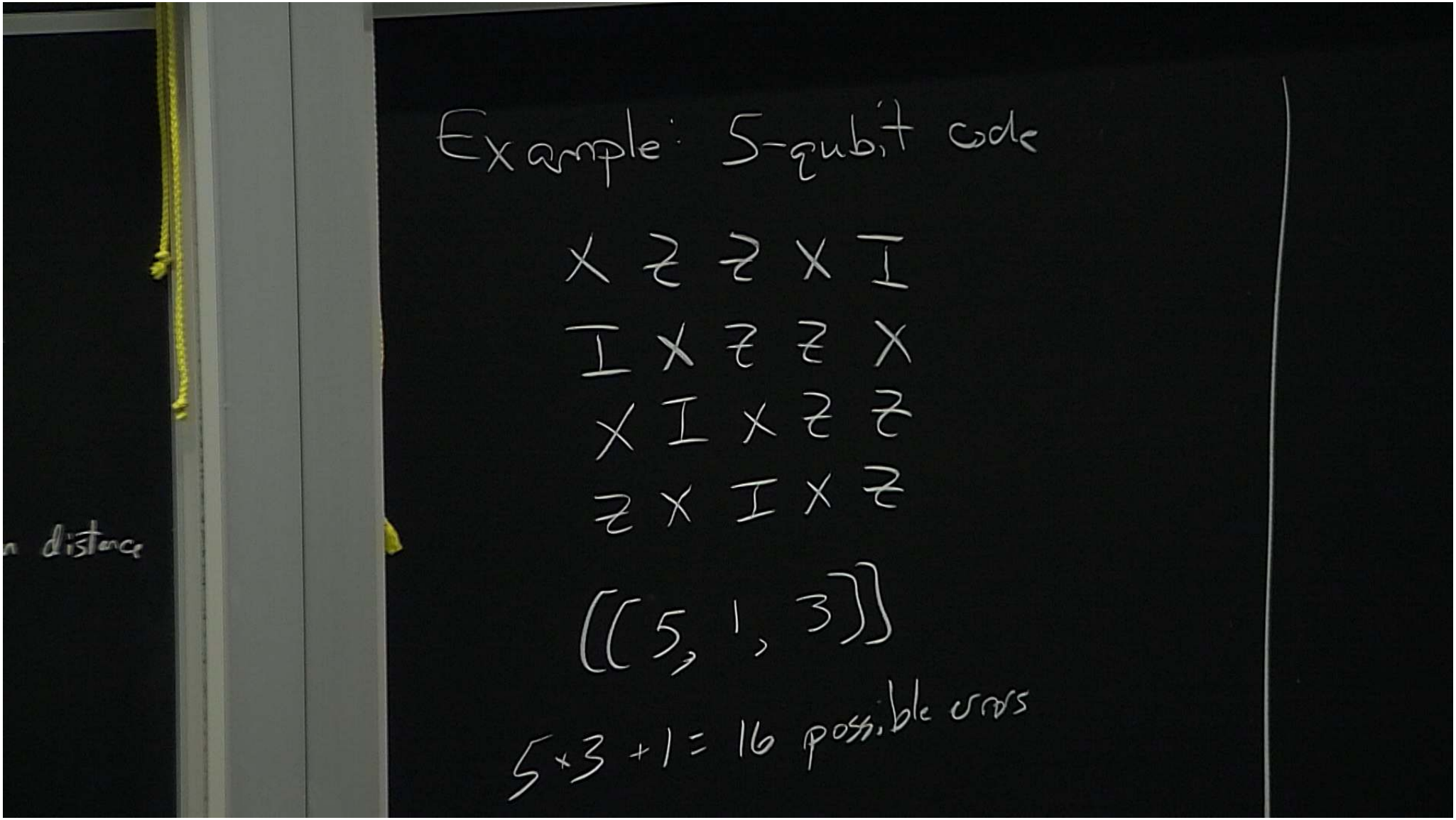
CAUTION

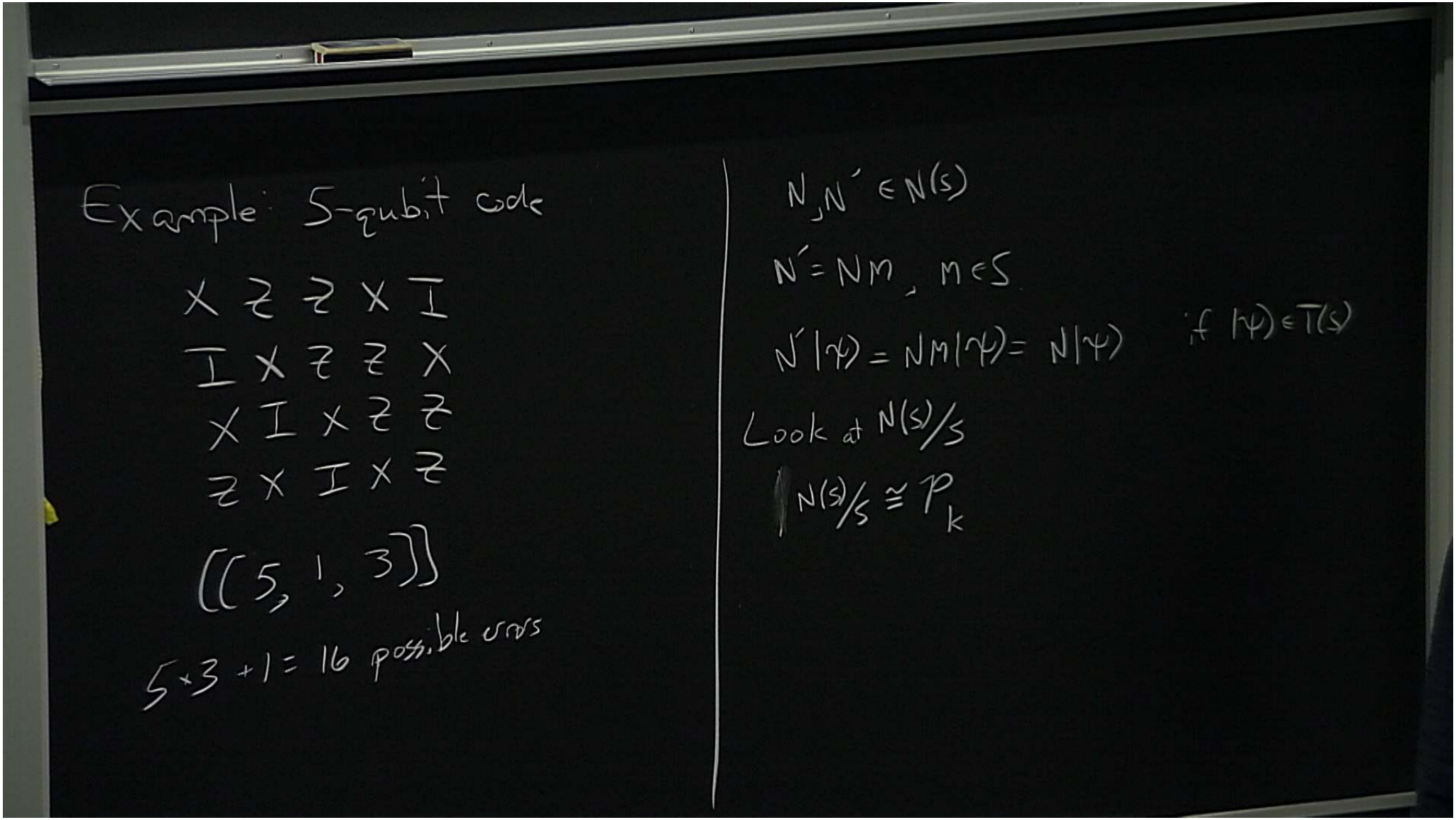
Thm: S can correct a set $\mathcal{C} \subseteq \mathcal{P}_n$ iff $E^\dagger F \notin N(S) \setminus S$ $\forall E, F \in \mathcal{C}$.

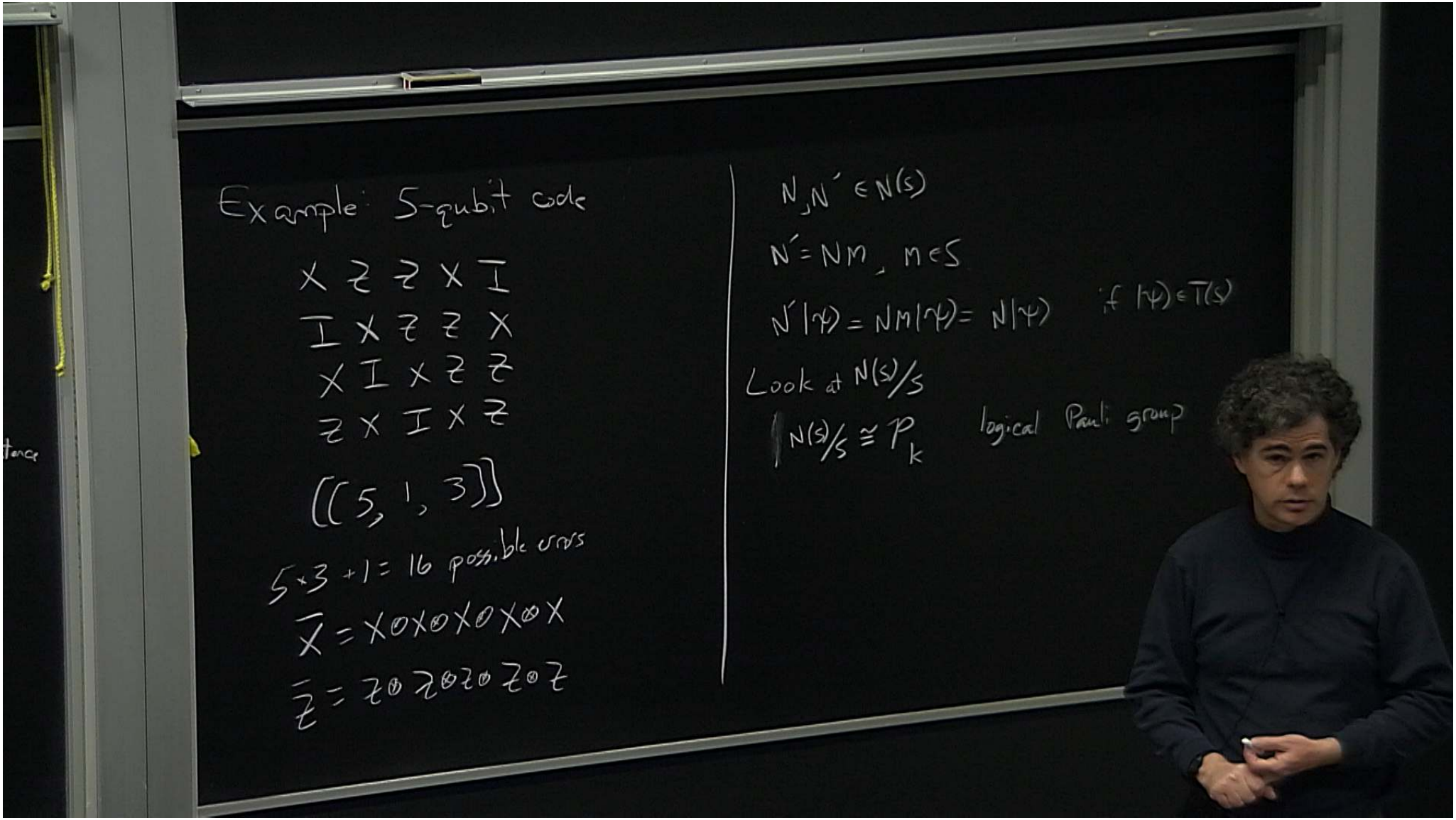
Cor: The distance of S is minimum weight of $N \in N(S) \setminus S$. The code is degenerate if S contains an element of lower weight.

Def: For a stabilizer code, if we have n physical qubits, k logical qubits and distance d, it is a $[[n, k, d]]$ code.


Example: 5-qubit code
X Z Z X I
I X Z Z X
X I X Z Z
Z X I X Z
[[5, 1, 3]]


Example: 5-qubit code
X Z Z X I
I X Z Z X
X I X Z Z
Z X I X Z
[[5, 1, 3]]
5×3+1=16 possible errors
distance


Example: 5-qubit code
X Z Z X I
I X Z Z X
X I X Z Z
Z X I X Z
[[5, 1, 3]]
5×3 + 1 = 16 possible errors
N, N' ∈ N(S)
N' = NM, M ∈ S
N'|ψ⟩ = NM|ψ⟩ = N|ψ⟩ if |ψ⟩ ∈ T(S)
Look at N(S)/S
N(S)/S ≅ P_k


Example: 5-qubit code
X Z Z X I
I X Z Z X
X I X Z Z
Z X I X Z
[[5, 1, 3]]
5×3+1 = 16 possible errors
$\bar{X} = X \otimes X \otimes X \otimes X \otimes X$
$\bar{Z} = Z \otimes Z \otimes Z \otimes Z \otimes Z$
$N, N' \in N(S)$
$N' = NM, \; M \in S$
$N'|\psi\rangle = NM|\psi\rangle = N|\psi\rangle$ if $|\psi\rangle \in T(S)$
Look at $N(S)/S$
$N(S)/S \cong \mathcal{P}_k$ logical Pauli group

Linear codes

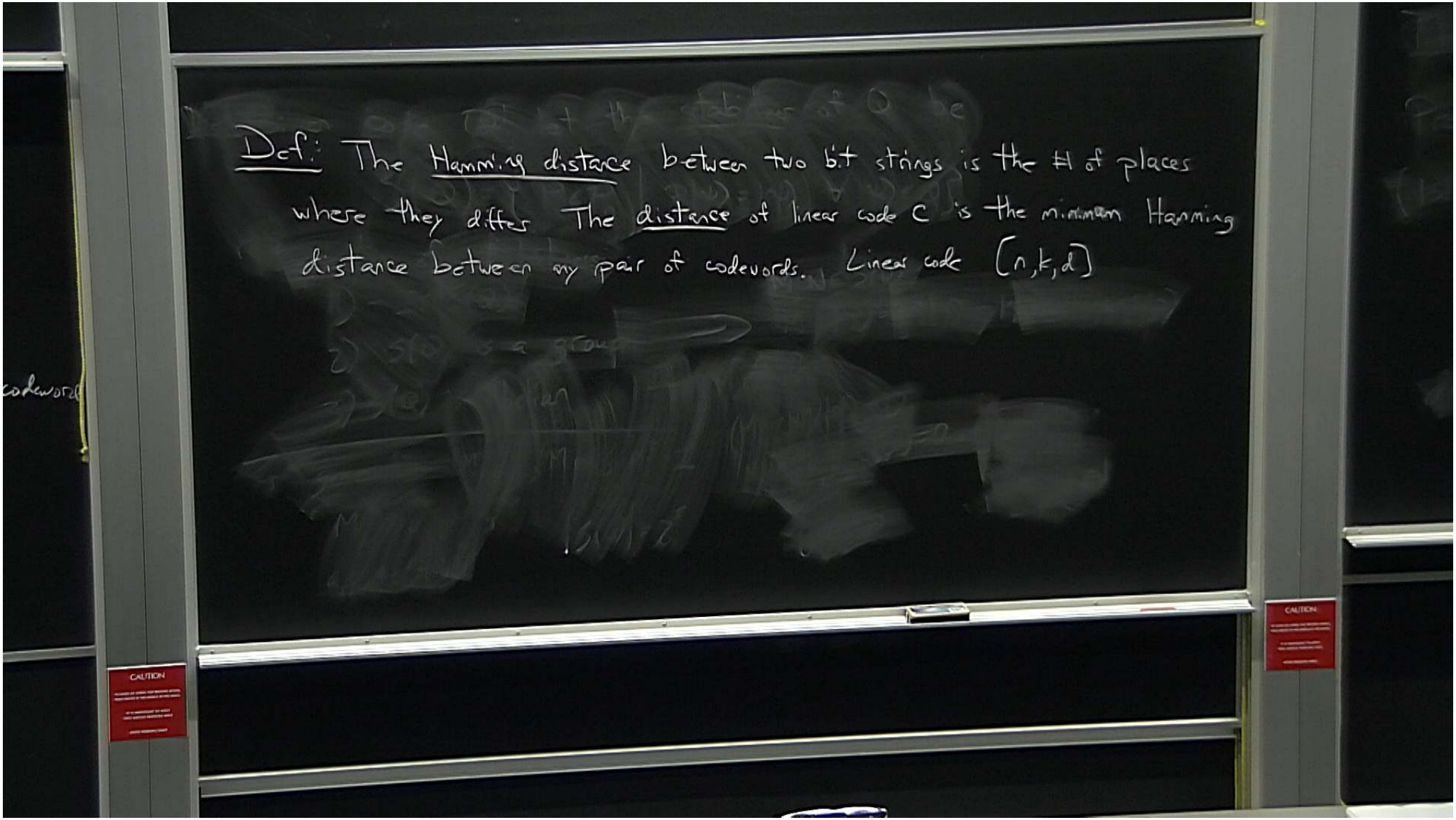
Def: A classical code C is a set of bit strings. C is a **linear code** if $x, y \in C \Rightarrow x+y \in C$

Define via **generator matrix**, $k \times n$ binary matrix (k = # logical bits, n = # physical bits). Each row is a basis codeword.

General codeword - given logical v, encoded as $G^T v$.

E.g. Hamming code

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


Def: The Hamming distance between two bit strings is the # of places where they differ. The distance of linear code C is the minimum Hamming distance between any pair of codewords. Linear code [n,k,d]
CAUTION

Def: The Hamming distance between two bit strings is the # of places where they differs. The distance of ~~Linear~~ code C is the minimum Hamming distance between any pair of codewords.

Linear code $[n, k, d]$

General code (n, K, d)

Hamming distance = $wt(x, y)$

$\Rightarrow$ Linear code: distance = lowest wt nontrivial codeword

Thm: S can correct a set $\mathcal{E} \subseteq \mathcal{P}_n$ iff $\forall E, F \in \mathcal{E}$ $E^\dagger F \notin N(S) \setminus S$

Def: For a linear code, the parity check matrix H is a matrix of maximal rank s.t. $HG^T = 0$

$$H(G^T v) = 0$$

maximal rank st $HG^T = 0$

$$H(G^T v) = 0$$

Error e, codeword $x \longmapsto x+e$

$H(x+e) = Hx + He = He$ error syndrome

Hamming code $H = \begin{pmatrix} 1111000 \\ 1100110 \\ 1010101 \end{pmatrix}$

single-bit errors have syndromes which are ith column of H

Def: For a linear code, the parity check matrix H is a matrix of maximal rank s.t. $HG^T = 0$

$$H(G^T v) = 0$$

Error e, codeword $x \longmapsto x+e$

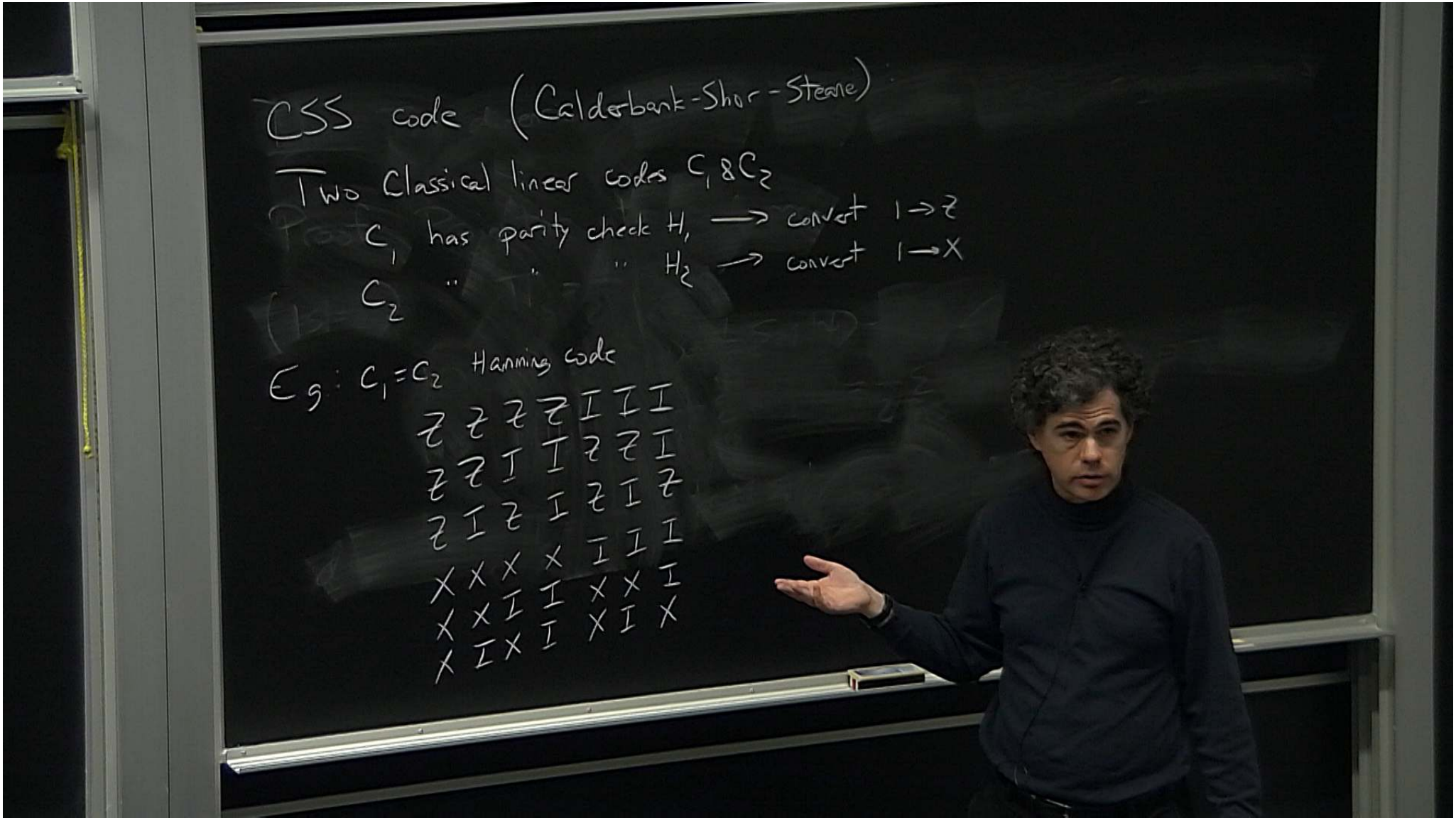
$H(x+e) = Hx + He = He$ error syndrome

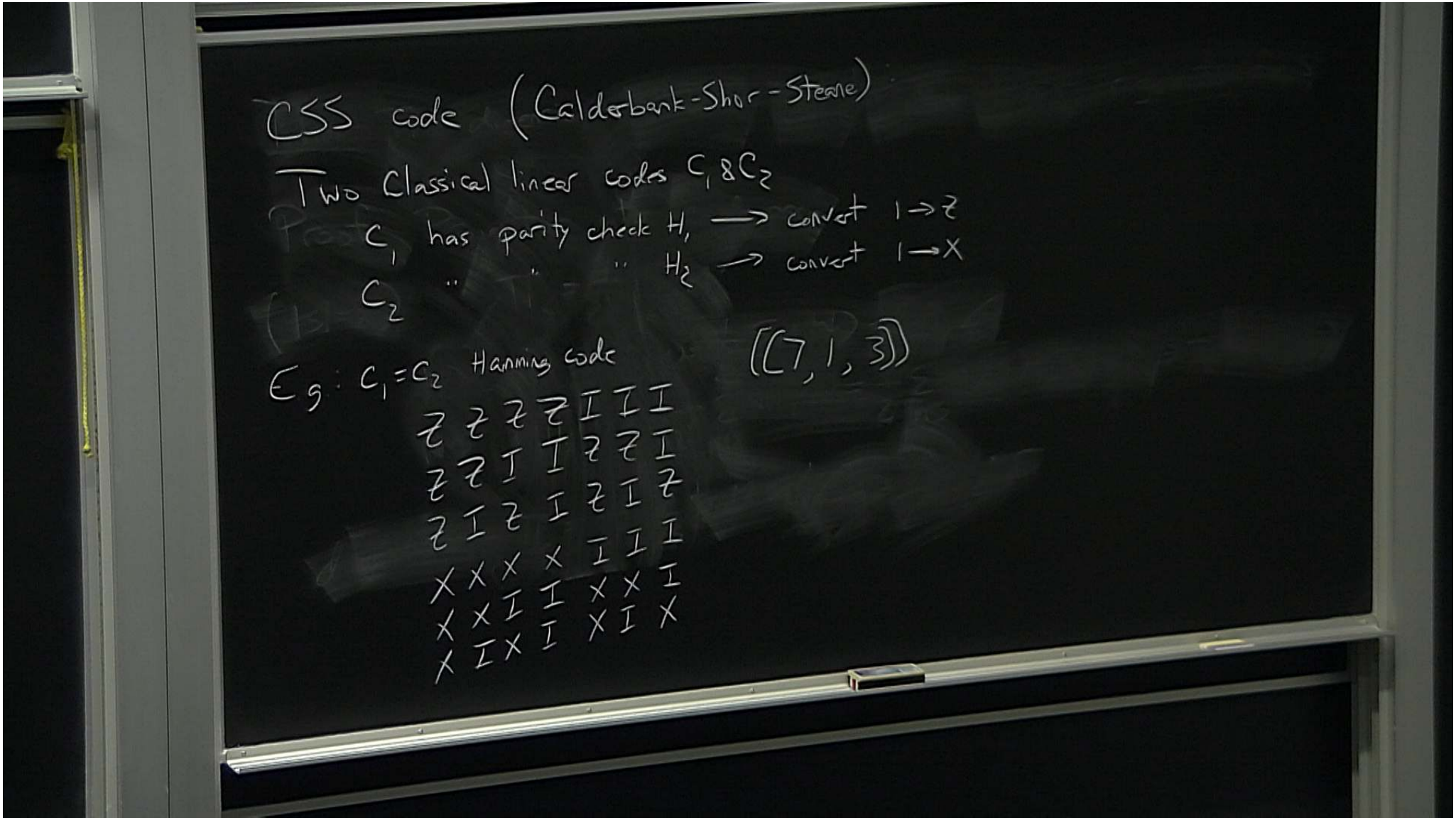
Hamming code $H = \begin{pmatrix} 1111000 \\ 1100110 \\ 1010101 \end{pmatrix} \longrightarrow$

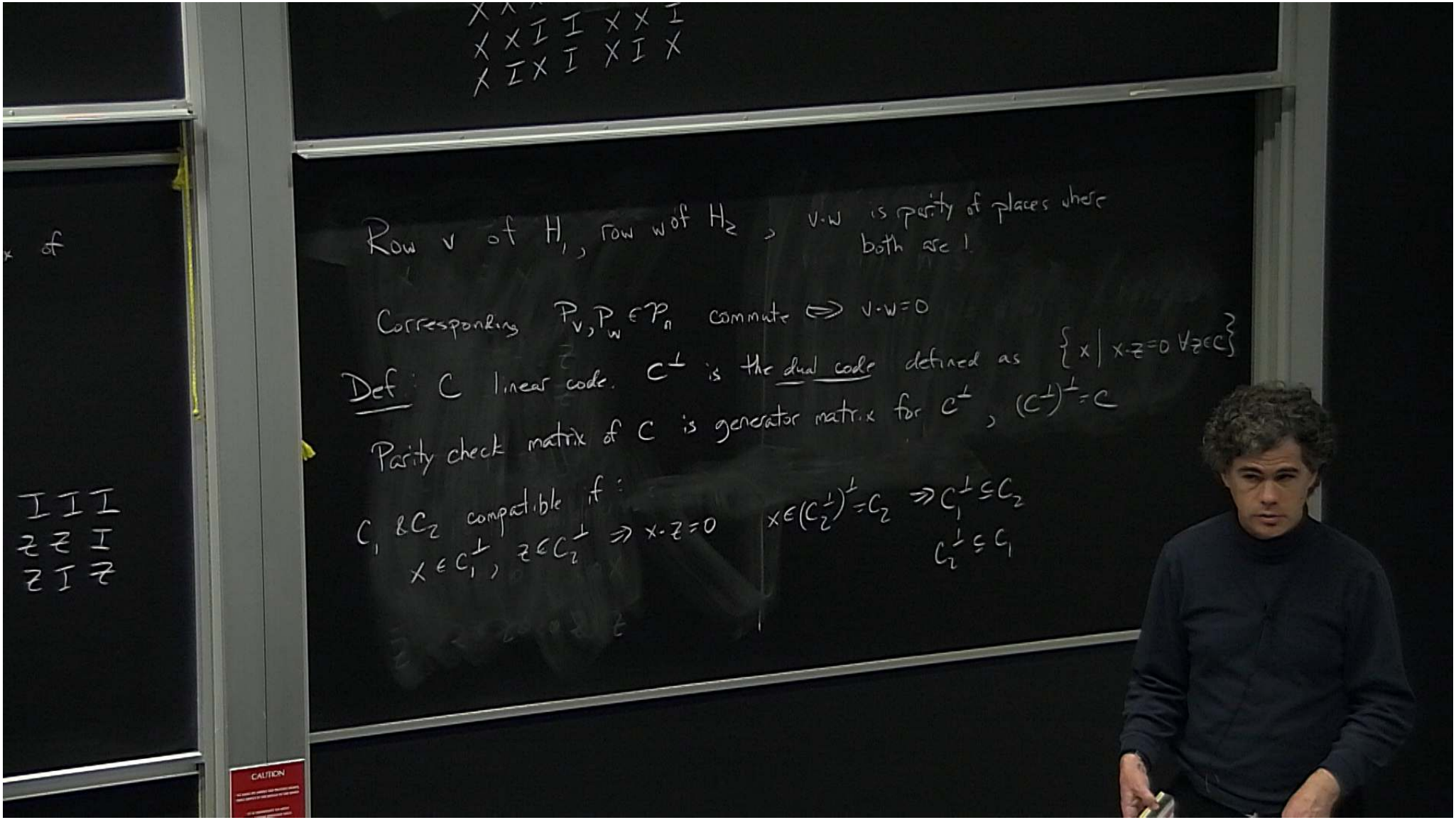
$$\begin{matrix} Z & Z & Z & Z & I & I & I \\ Z & Z & I & I & Z & Z & I \\ Z & I & Z & I & Z & I & Z \end{matrix}$$

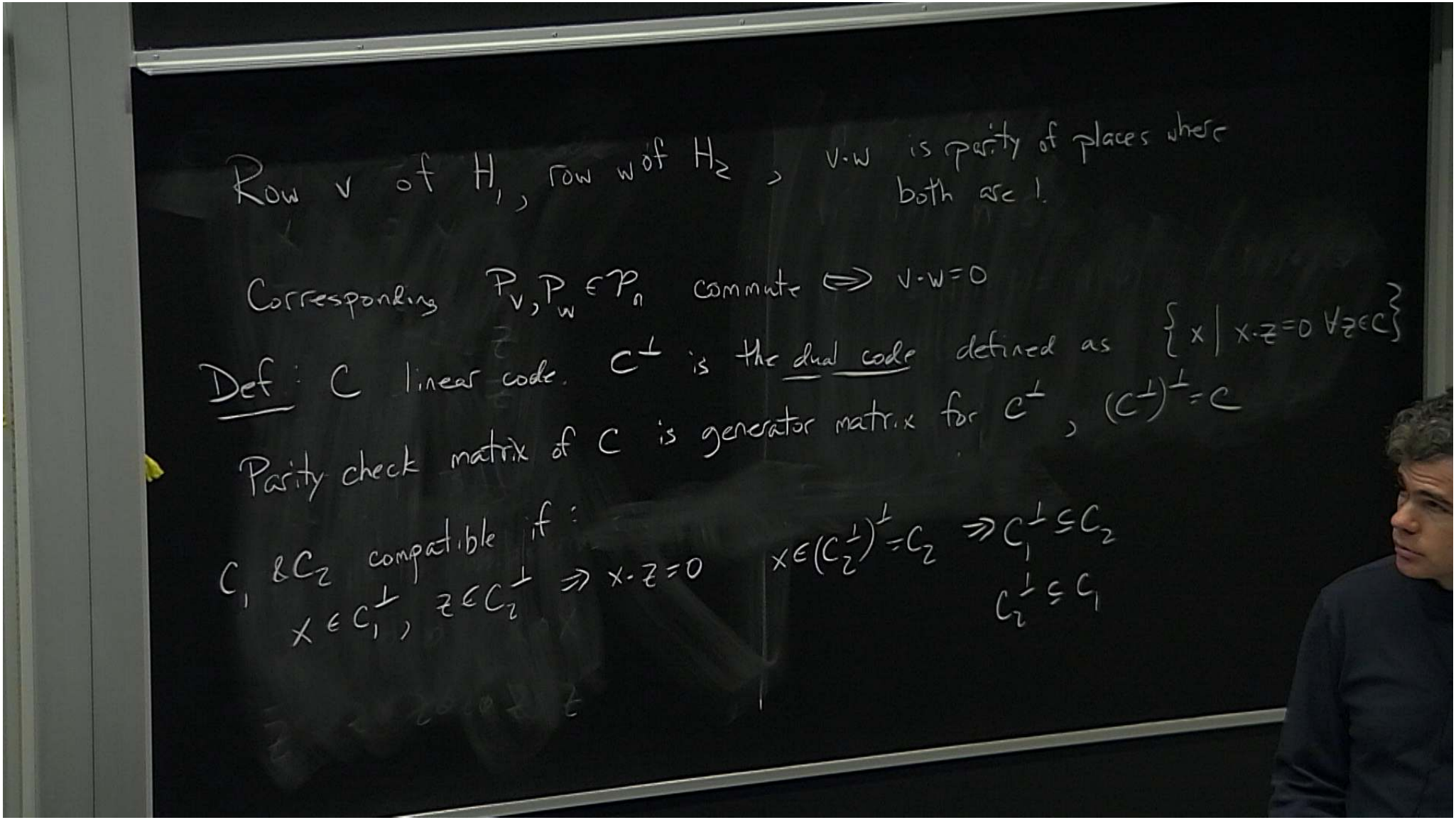
single-bit errors have syndromes which are ith column of H

$[7, 4, 3]$ code


CSS code (Calderbank-Shor-Steane)
Two Classical linear codes C_1 & C_2
C_1 has parity check H_1 → convert 1→Z
C_2 " " " H_2 → convert 1→X
Eg: $C_1 = C_2$ Hanning code
Z Z Z Z I I I
Z Z I I Z Z I
Z I Z I Z I Z
X X X X I I I
X X I I X X I
X I X I X I X


CSS code (Calderbank-Shor-Steane)
Two Classical linear codes C_1 & C_2
C_1 has parity check H_1 → convert 1→Z
C_2 " " " H_2 → convert 1→X
Eg: $C_1 = C_2$ Hanning code ([7, 1, 3])
Z Z Z Z I I I
Z Z I I Z Z I
Z I Z I Z I Z
X X X X I I I
X X I I X X I
X I X I X I X


Row v of H_1, row w of H_2, $v \cdot w$ is parity of places where both are 1
Corresponding $P_v, P_w \in \mathcal{P}_n$ commute $\Leftrightarrow v \cdot w = 0$
Def: C linear code. $C^\perp$ is the dual code defined as $\{x \mid x \cdot z = 0 \ \forall z \in C\}$
Parity check matrix of C is generator matrix for $C^\perp$, $(C^\perp)^\perp = C$
C_1 & C_2 compatible if:
$x \in C_1^\perp$, $z \in C_2^\perp \Rightarrow x \cdot z = 0$
$x \in (C_2^\perp)^\perp = C_2 \Rightarrow C_1^\perp \subseteq C_2$
$C_2^\perp \subseteq C_1$
CAUTION


Row v of H_1, row w of H_2, $v \cdot w$ is parity of places where both are 1.
Corresponding $P_v, P_w \in \mathcal{P}_n$ commute $\Leftrightarrow v \cdot w = 0$
Def: C linear code. $C^\perp$ is the dual code defined as $\{x \mid x \cdot z = 0 \ \forall z \in C\}$
Parity check matrix of C is generator matrix for $C^\perp$, $(C^\perp)^\perp = C$
C_1 & C_2 compatible if:
$x \in C_1^\perp$, $z \in C_2^\perp \Rightarrow x \cdot z = 0$
$x \in (C_2^\perp)^\perp = C_2 \Rightarrow C_1^\perp \subseteq C_2$
$C_2^\perp \subseteq C_1$

TA: John Schanck <jschanck@uwaterloo.ca>

Thm: Let $C_1^{\perp} \subseteq C_2$, C_1, C_2 linear codes C_1 is $[n, k_1, d_1]$, C_2 is $[n, k_2, d_2]$.

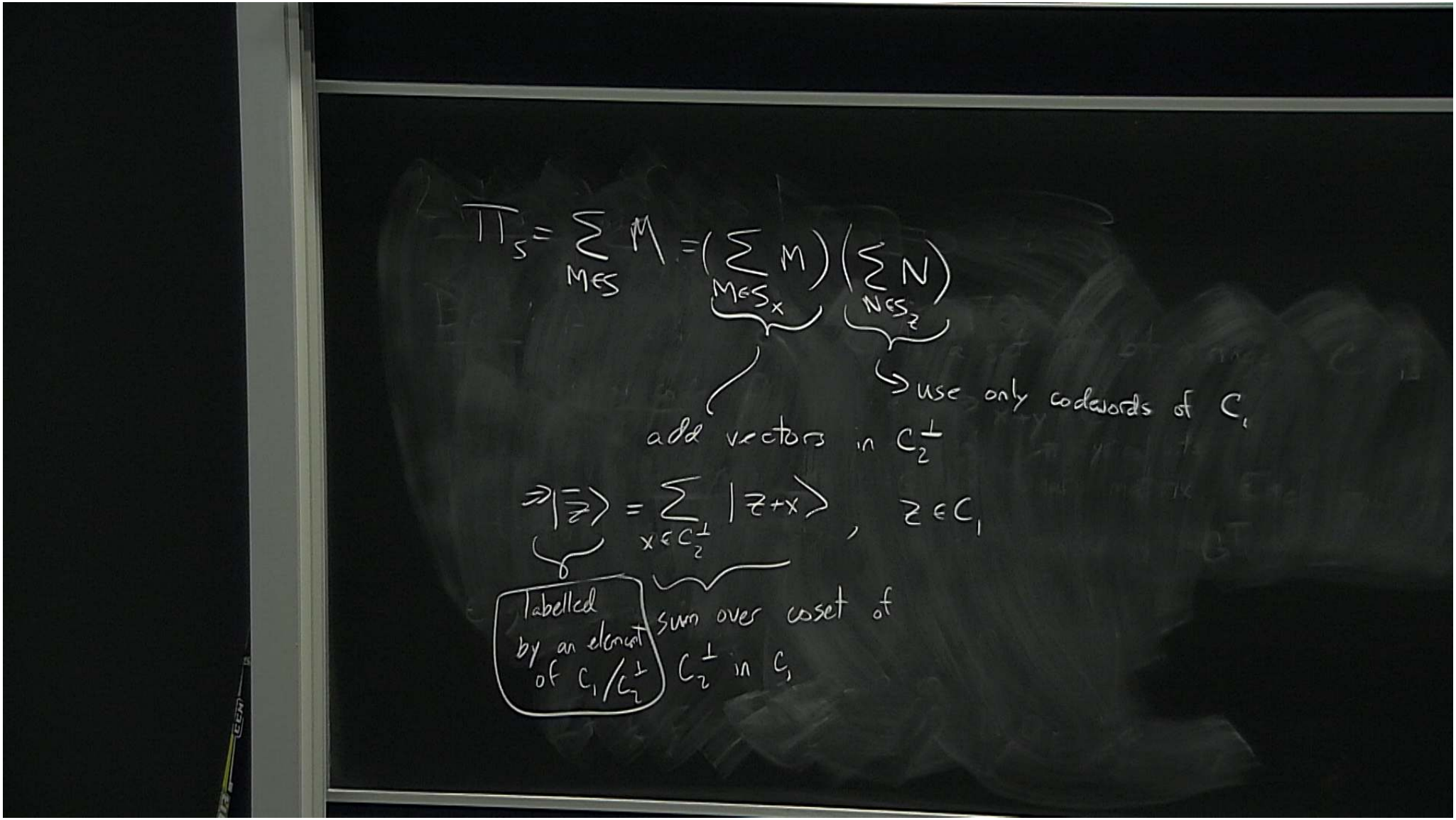
Then $\exists$ quantum code (CSS code) which is $[[n, k_1 + k_2 - n, d]]$, with

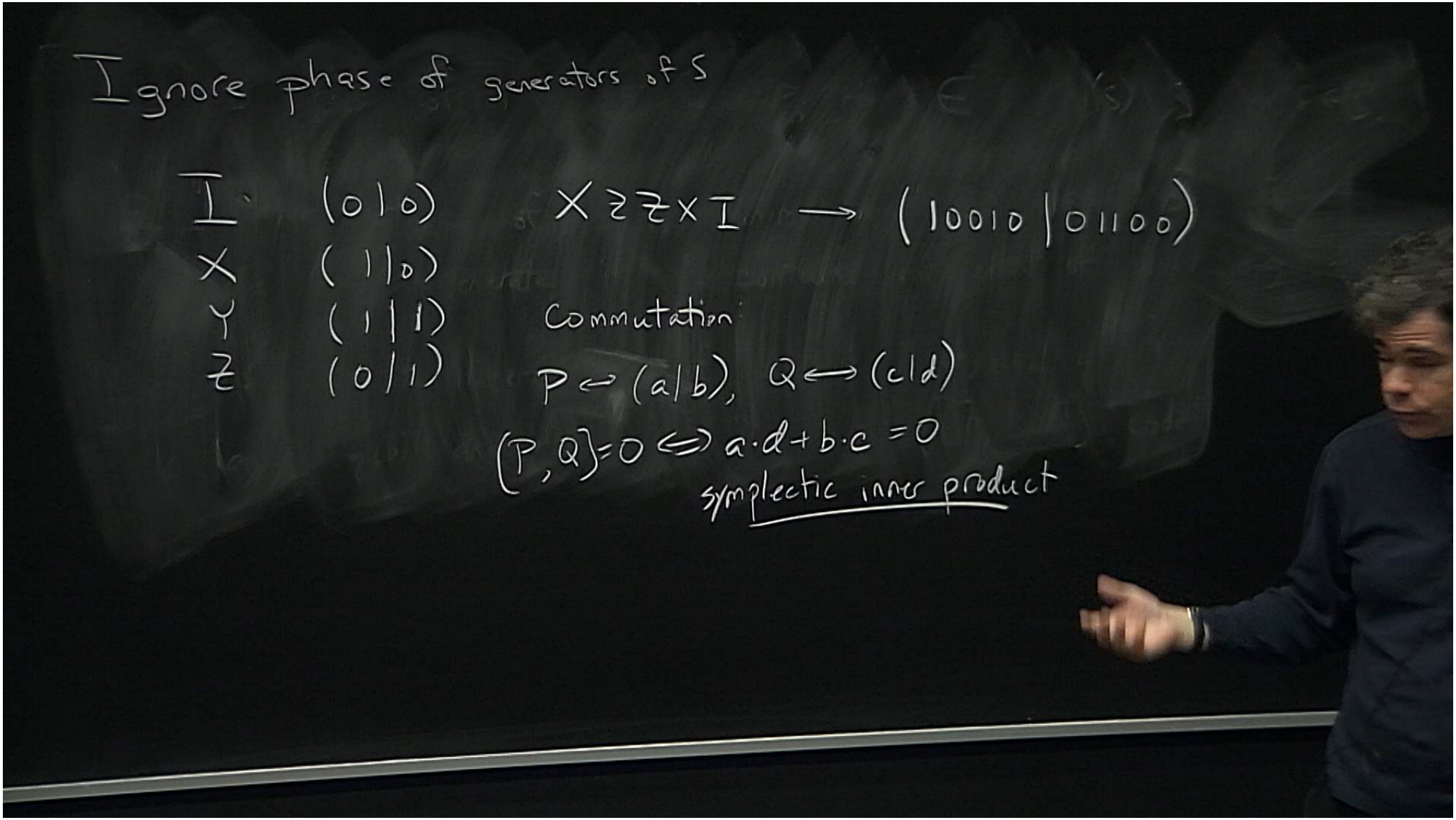
$d \geq \min(d_1, d_2)$

TA: John Schanck <jschanck@uwaterloo.ca>

Thm: Let $C_1^\perp \subseteq C_2$, C_1, C_2 linear codes. C_1 is $[n, k_1, d_1]$, C_2 is $[n, k_2, d_2]$.
Then $\exists$ quantum code (CSS code) which is $[[n, \underbrace{k_1+k_2-n}_{k}, d]]$, with
$d \geq \min(d_1, d_2)$

$k = n - \#\text{generators}$
$= n - (n-k_1) - (n-k_2) = k_1 + k_2 - n$


$\Pi_S = \sum_{M \in S} M = \left(\sum_{M \in S_X} M\right)\left(\sum_{N \in S_Z} N\right)$
add vectors in $C_2^\perp$
use only codewords of C_1
$\Rightarrow |\bar{z}\rangle = \sum_{x \in C_2^\perp} |z+x\rangle$, $z \in C_1$
labelled by an element of $C_1/C_2^\perp$
sum over coset of $C_2^\perp$ in C_1


Ignore phase of generators of S
I (0|0)
X (1|0)
Y (1|1)
Z (0|1)
XZZXI → (10010|01100)
Commutation
P ↔ (a|b), Q ↔ (c|d)
[P,Q]=0 ⇔ a·d+b·c=0
symplectic inner product

Ignore phase of generators of S

$I \quad (0|0)$

$X \quad (1|0)$

$Y \quad (1|1)$

$Z \quad (0|1)$

$XZZXI \longrightarrow (10010|01100)$

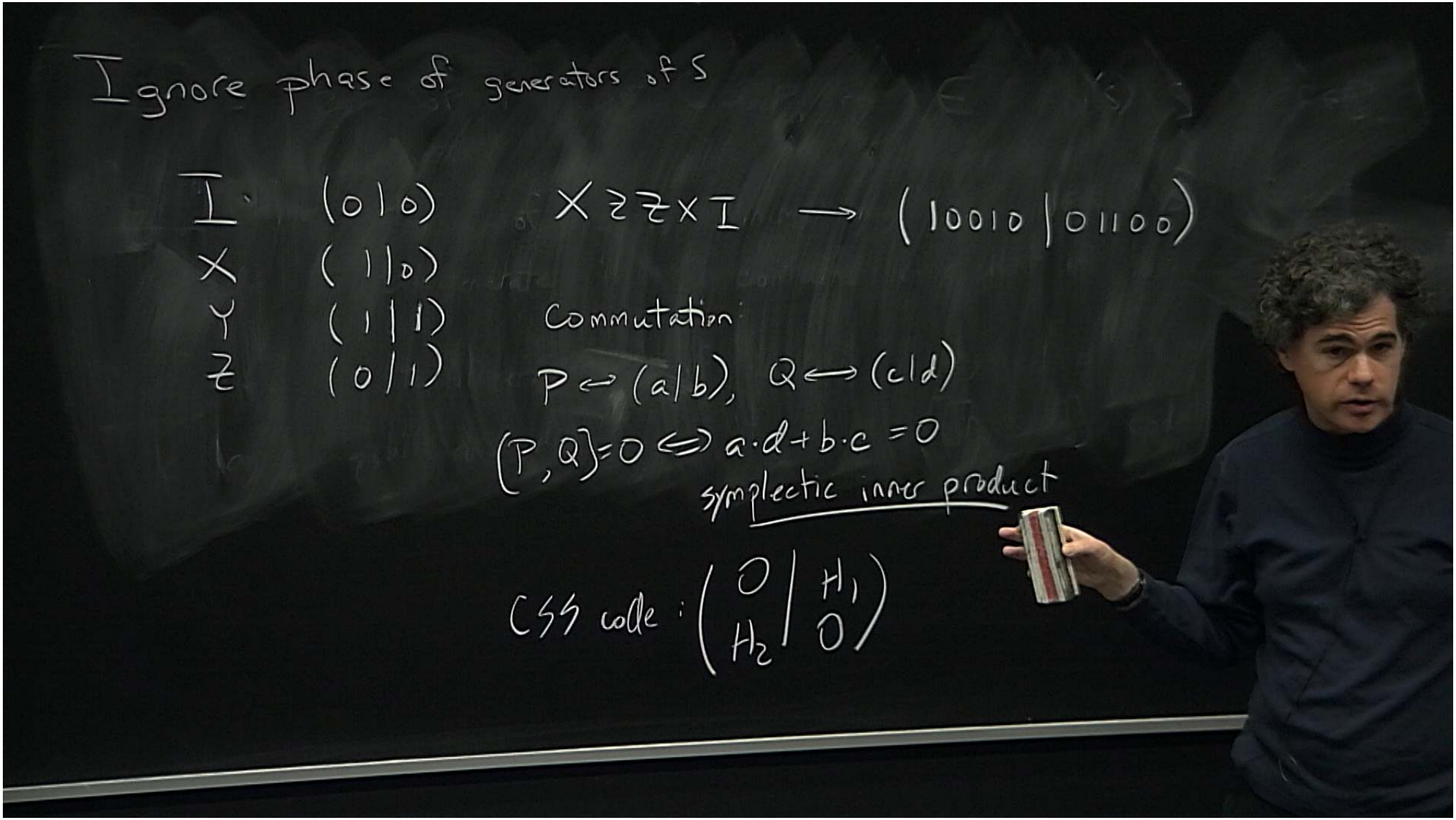
Commutation

$P \leftrightarrow (a|b), \quad Q \leftrightarrow (c|d)$

$[P,Q]=0 \Leftrightarrow a\cdot d + b\cdot c = 0$

symplectic inner product

CSS code : $\left(\quad | \quad \right)$


Ignore phase of generators of S
I (0|0)
X (1|0)
Y (1|1)
Z (0|1)
XZZXI → (10010|01100)
Commutation:
P ↔ (a|b), Q ↔ (c|d)
[P,Q]=0 ⇔ a·d+b·c=0
symplectic inner product
CSS code: (0 H1 / H2 0)

Ignore phase of generators of S

$I: (0|0)$ $\quad XZZXI \longrightarrow (10010|01100)$

$X: (1|0)$

$Y: (1|1)$

$Z: (0|1)$

Commutation:

$P \leftrightarrow (a|b)$, $Q \leftrightarrow (c|d)$

$[P,Q]=0 \Leftrightarrow a\cdot d + b\cdot c = 0$

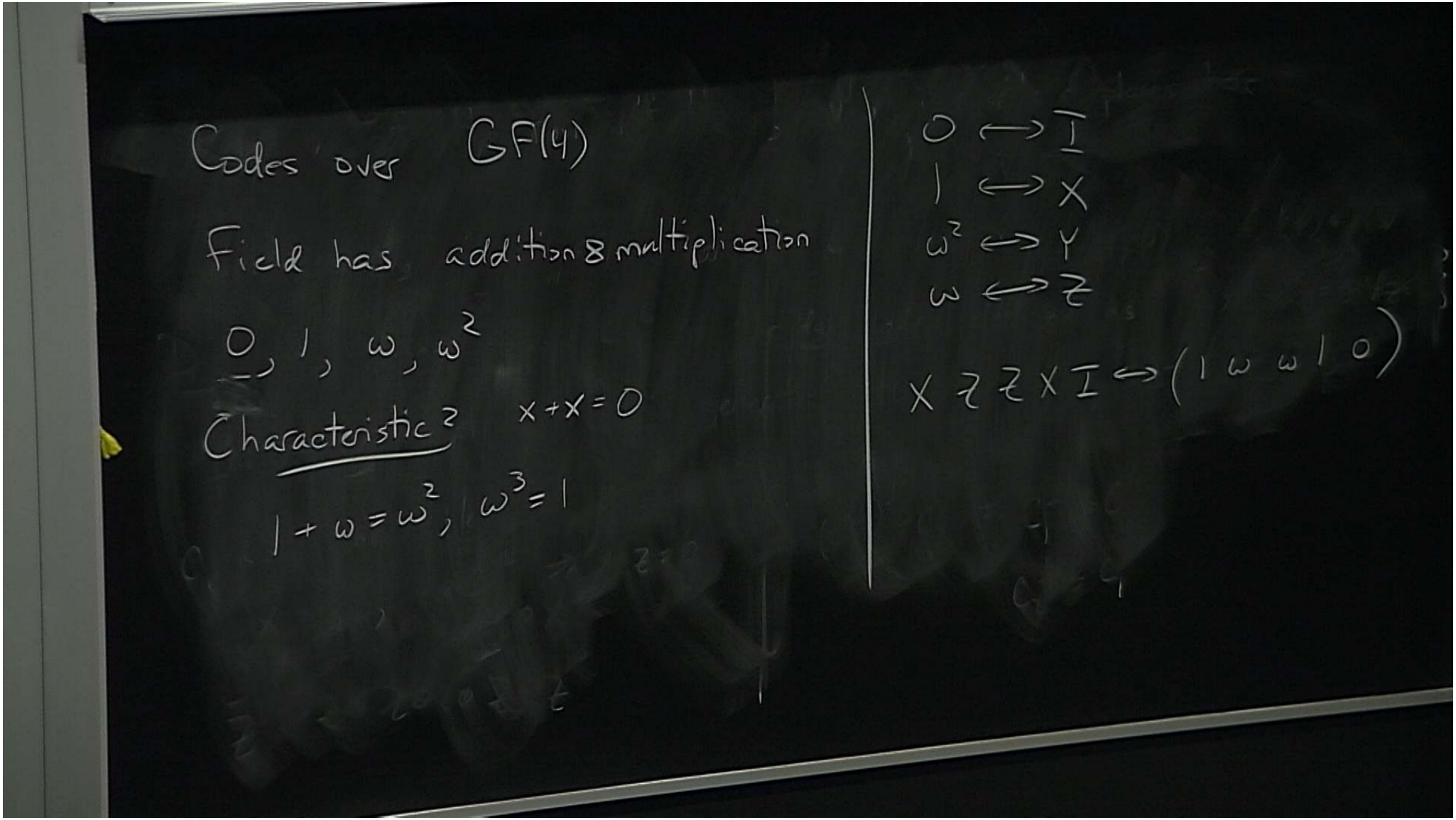
symplectic inner product

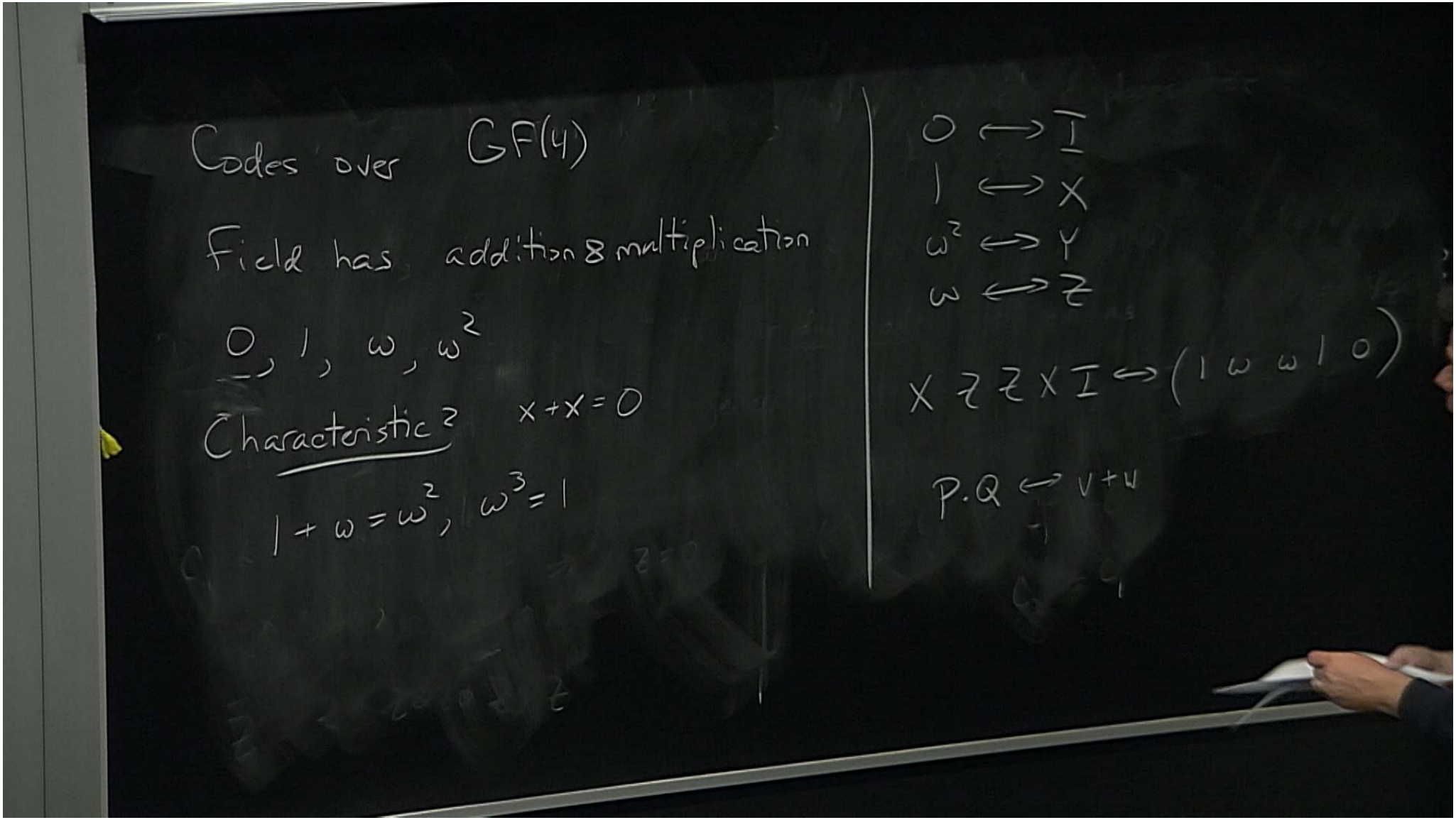
CSS code: $\left(\begin{array}{c|c} 0 & H_1 \\ H_2 & 0 \end{array}\right)$

P Q

{ {

v + w


Codes over GF(4)
Field has addition & multiplication
0, 1, ω, ω²
Characteristic 2 x+x=0
1+ω=ω², ω³=1
0 ⟷ I
1 ⟷ X
ω² ⟷ Y
ω ⟷ Z
XZZXI ⟷ (1 ω ω 1 0)


Codes over GF(4)
Field has addition & multiplication
0, 1, ω, ω²
Characteristic 2 x+x=0
1+ω=ω², ω³=1
0 ⟷ I
1 ⟷ X
ω² ⟷ Y
ω ⟷ Z
XZZXI ⟷ (1ωω|0)
P.Q ⟷ v+w

Codes over GF(4)

Field has addition & multiplication

$0, 1, \omega, \omega^2$

Characteristic 2 $\quad x + x = 0$

$1 + \omega = \omega^2, \quad \omega^3 = 1$

$\overline{0} = 0$
$\overline{1} = 1$
$\overline{\omega} = \omega^2$
$\overline{\omega^2} = \omega$

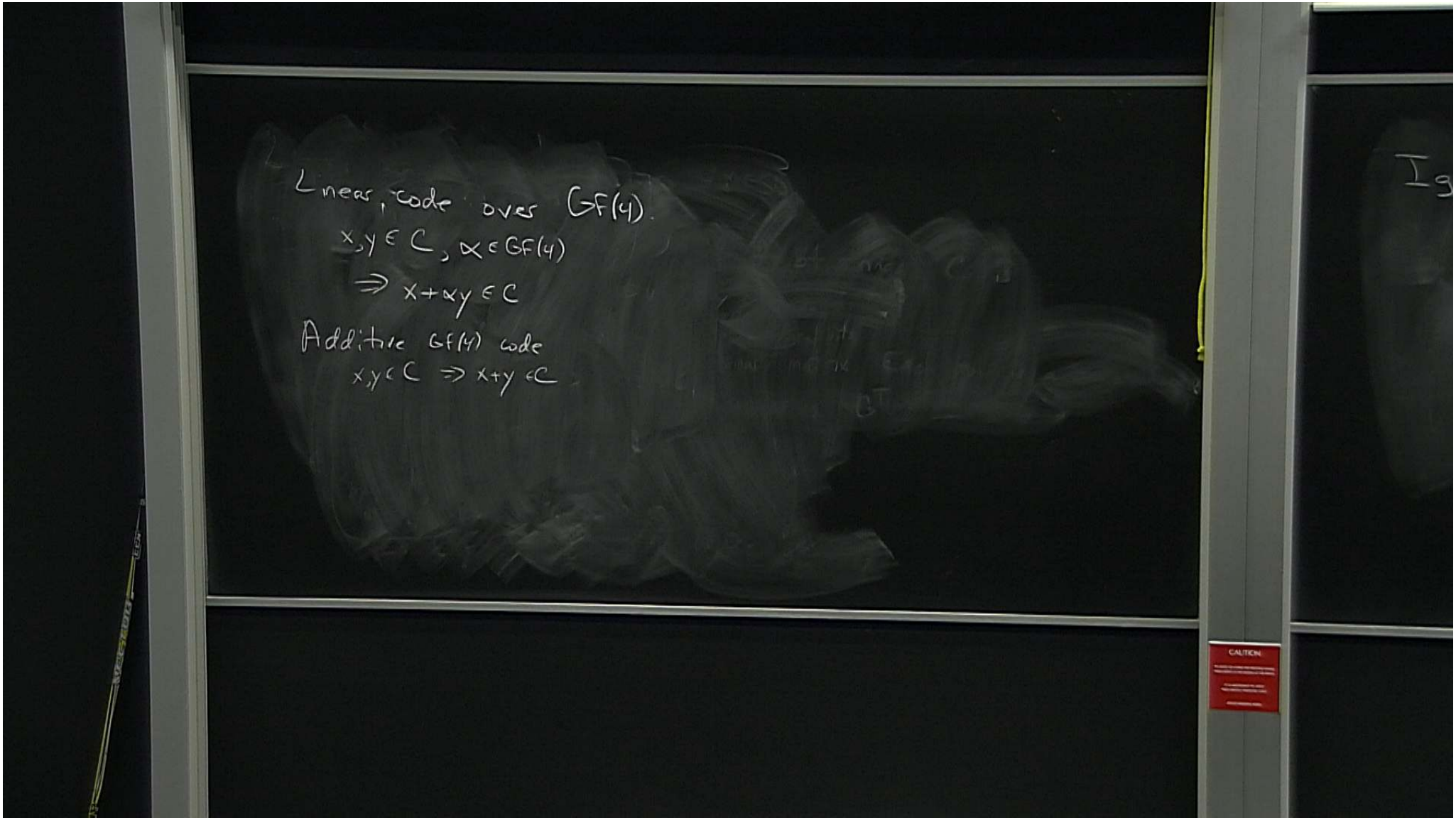
$\mathrm{tr}\, 0 = 0$
$\mathrm{tr}\, 1 = 0$
$\mathrm{tr}\, \omega = 1$
$\mathrm{tr}\, \omega^2 = 1$

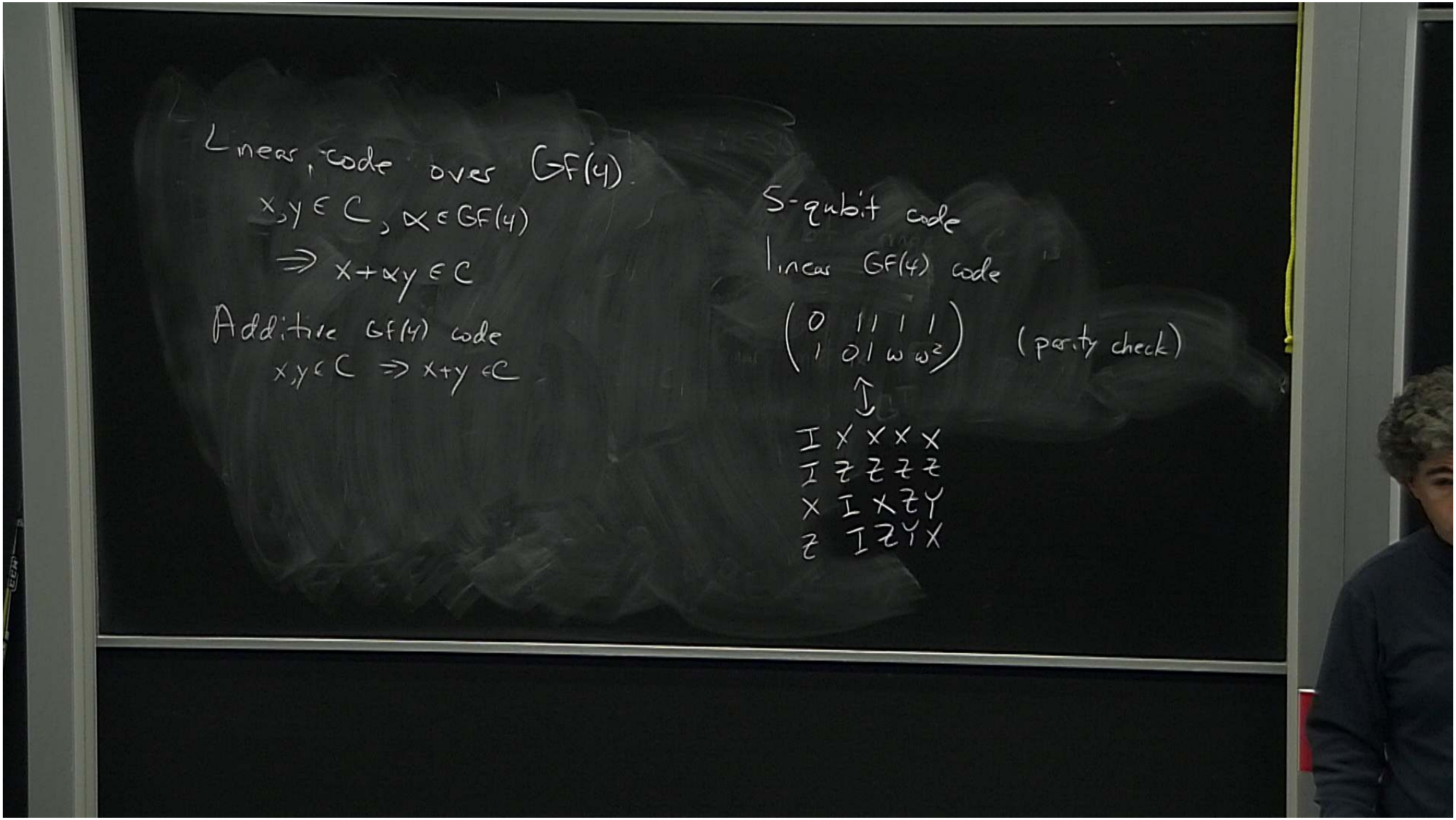
$0 \longleftrightarrow I$
$1 \longleftrightarrow X$
$\omega^2 \longleftrightarrow Y$
$\omega \longleftrightarrow Z$

$XZZXI \longleftrightarrow (1\ \omega\ \omega\ |\ 0)$

$P \cdot Q \longleftrightarrow v + w$

$(P, Q) = 0 \Leftrightarrow \mathrm{tr}(\bar{v} \cdot w) = 0$


Linear code over GF(4).
$x, y \in C, \alpha \in GF(4)$
$\Rightarrow x + \alpha y \in C$
Additive GF(4) code
$x, y \in C \Rightarrow x + y \in C$


Linear code over GF(4)
$x, y \in C, \alpha \in GF(4)$
$\Rightarrow x + \alpha y \in C$
Additive GF(4) code
$x, y \in C \Rightarrow x + y \in C$
5-qubit code
linear GF(4) code
$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{pmatrix}$ (parity check)
I X X X X
I Z Z Z Z
X I X Z Y
Z I Z Y X