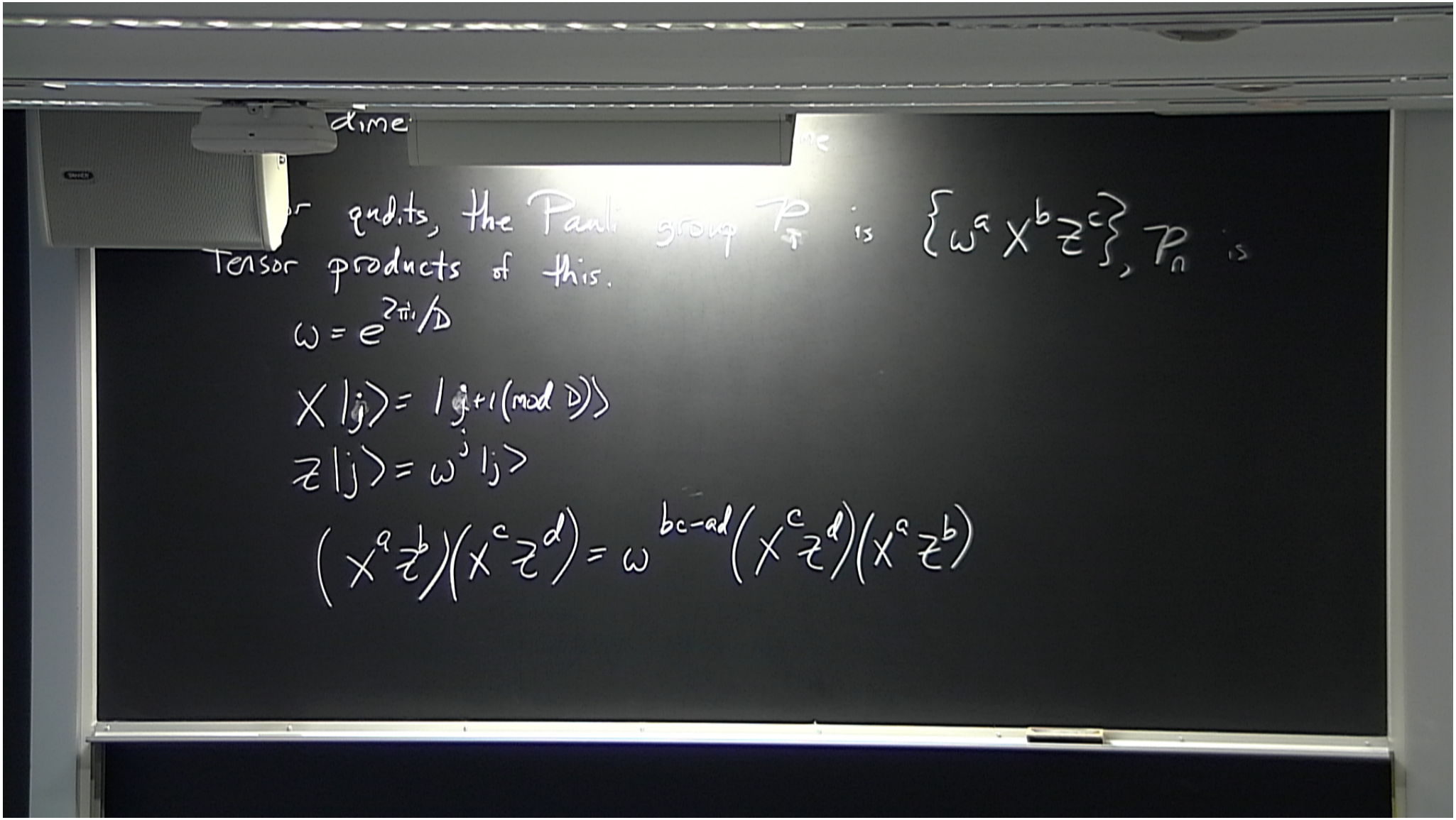
Title: IQC - Quantum Error Correction - Lecture 3

Date: Jan 18, 2018 02:00 PM

URL: http://pirsa.org/18010049

Abstract:


dime
qudits, the Pauli group P_1 is $\{\omega^a X^b Z^c\}$, P_n is
Tensor products of this.
$\omega = e^{2\pi i/D}$
$X|j\rangle = |j+1 \pmod D\rangle$
$Z|j\rangle = \omega^j |j\rangle$
$(X^a Z^b)(X^c Z^d) = \omega^{bc-ad}(X^c Z^d)(X^a Z^b)$

Def: Given subspace Q of $\mathcal{H}_p^{\otimes n}$,

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

If S is an Abelian subgroup of $\mathcal{P}_n$, $\omega I \notin S$,

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

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

Weight is # of non-trivial tensor factors of an operator.

(Non-stabilizer) QECC with n physical qudits, logical Hilbert space of dim K, distance d,

; it is a $((n,K,d))_D$ code.

A stabilizer code with $K = D^k$ is a $[[n,k,d]]_D$ code.

Qudit dimension $D = p$ odd prime

Def: For qudits, the Pauli group $\mathcal{P}_1$ is $\{\omega^a X^b Z^c\}$, $\mathcal{P}_n$ is tensor products of this.

$\omega = e^{2\pi i/D}$

$X|j\rangle = |j+1 \pmod D\rangle$

$Z|j\rangle = \omega^j |j\rangle$

$(X^a Z^b)(X^c Z^d) = \omega^{bc-ad}(X^c Z^d)(X^a Z^b)$

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

Qudit dimension $D = p$ odd prime

Def: For qudits, the Pauli group $\mathcal{P}_1$ is $\{\omega^a X^b Z^c\}$, $\mathcal{P}_n$ is tensor products of this.

$a, b, c \in \{0, 1, \ldots, D-1\}$

$\omega = e^{2\pi i/D}$

$X|j\rangle = |j+1 \pmod D\rangle$

$Z|j\rangle = \omega^j |j\rangle$

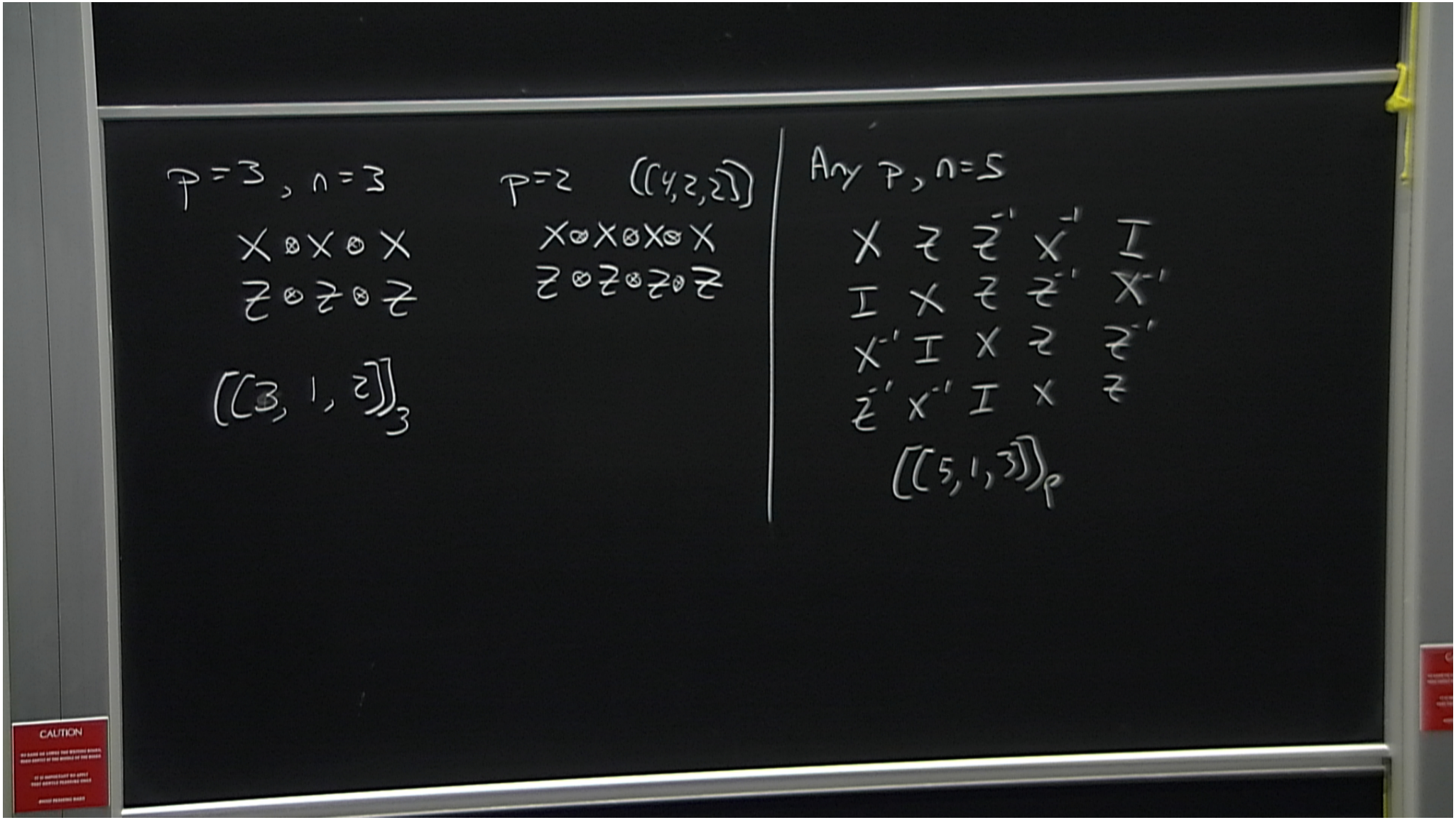
$(X^a Z^b)(X^c Z^d) = \omega^{bc-ad}(X^c Z^d)(X^a Z^b)$

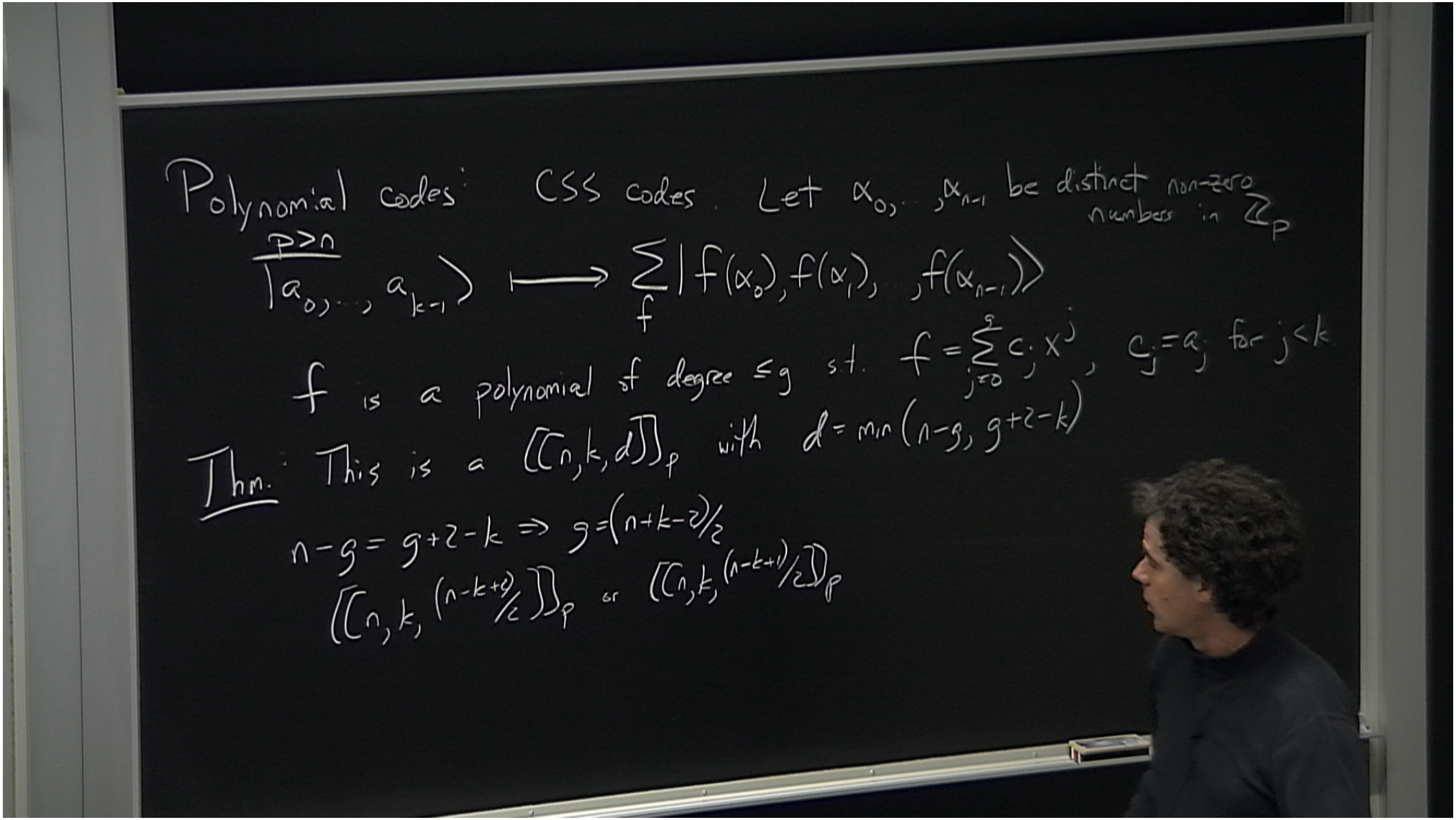
a) If S has r generators [illegible] encodes $n-r$ logical qudits

b) The distance of S is the minimum weight of $M \in N(S) \setminus S$.

Elements of S are form (with generators $M_1, \dots, M_r$)

$$\prod_{i=1}^{r} M_i^{a_i}, \quad a_i \in \{0, 1, \dots, p-1\}$$


p=3, n=3
X⊗X⊗X
Z⊗Z⊗Z
[[3, 1, 2]]3
p=2 ([4,2,2])
X⊗X⊗X⊗X
Z⊗Z⊗Z⊗Z
Any p, n=5
X Z Z⁻¹ X⁻¹ I
I X Z Z⁻¹ X⁻¹
X⁻¹ I X Z Z⁻¹
Z⁻¹ X⁻¹ I X Z
([5,1,3])p
CAUTION


Polynomial codes: CSS codes. Let $\alpha_0, \ldots, \alpha_{n-1}$ be distinct non-zero numbers in $\mathbb{Z}_p$
$p > n$
$|a_0, \ldots, a_{k-1}\rangle \longmapsto \sum_f |f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})\rangle$
f is a polynomial of degree $\leq g$ s.t. $f = \sum_{j=0}^{g} c_j x^j$, $c_j = a_j$ for $j < k$
Thm. This is a $[[n, k, d]]_p$ with $d = \min(n-g, g+2-k)$
$n - g = g + 2 - k \Rightarrow g = (n+k-2)/2$
$[[n, k, (n-k+2)/2]]_p$ or $[[n, k, (n-k+1)/2]]_p$

Polynomial codes: CSS codes. Let $\alpha_0, \ldots, \alpha_{n-1}$ be distinct non-zero numbers in $\mathbb{Z}_p$

$p > n$

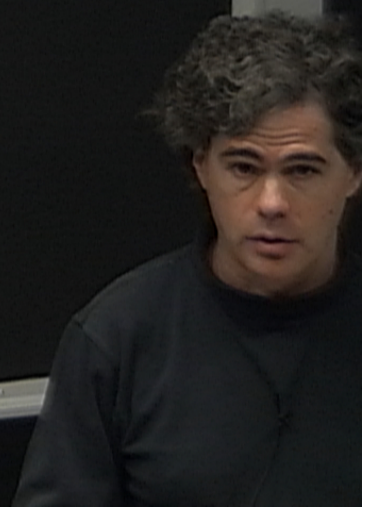
$$|a_0, \ldots, a_{k-1}\rangle \longmapsto \sum_f |f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})\rangle$$

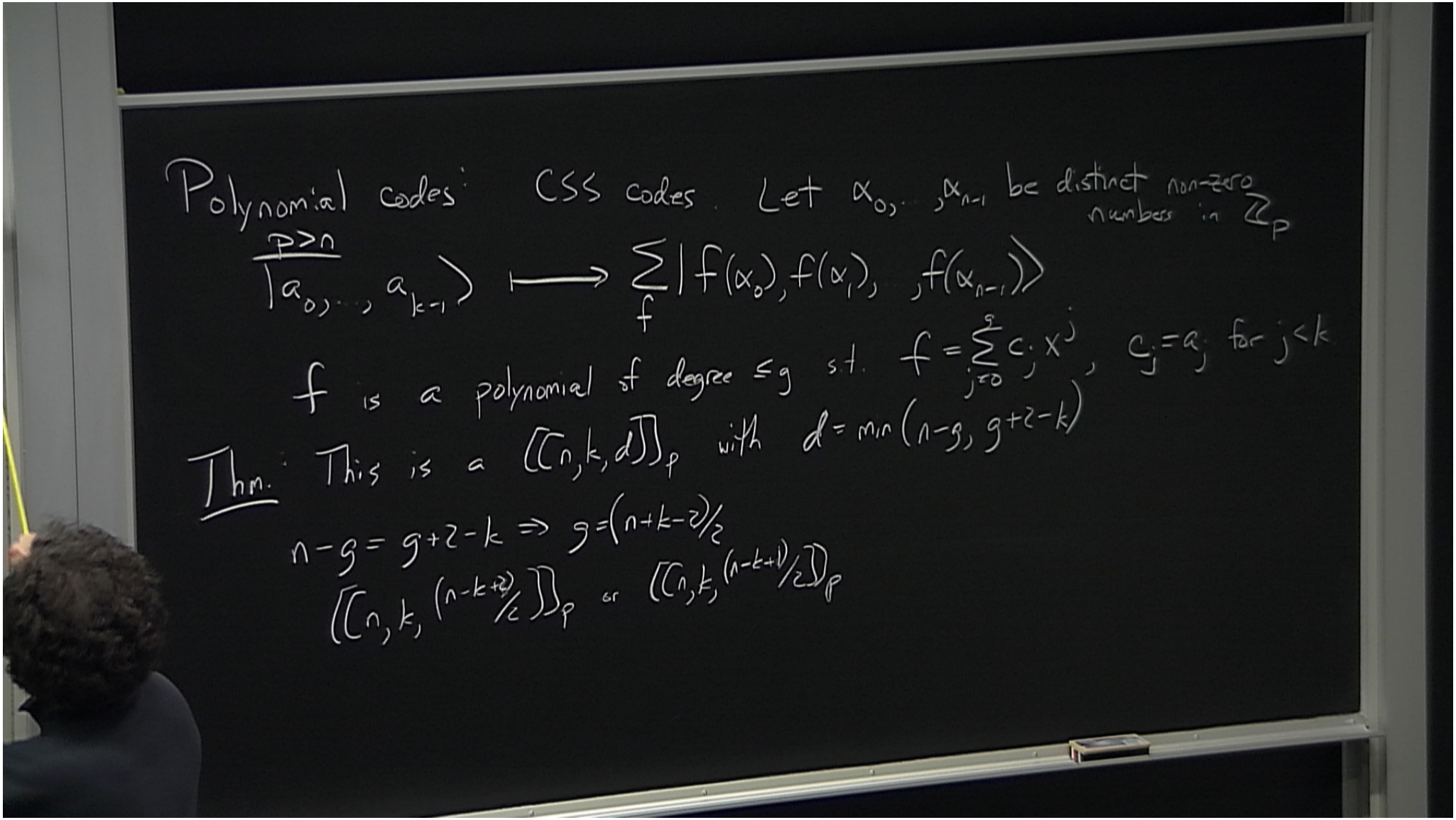
f is a polynomial of degree $\leq g$ s.t. $f = \sum_{j=0}^{g} c_j x^j$, $c_j = a_j$ for $j < k$

Thm. This is a $[[n, k, d]]_p$ with $d = \min(n-g, g+2-k)$

$n - g = g + 2 - k \Rightarrow g = (n+k-2)/2$

$[[n, k, (n-k+2)/2]]_p$ or $[[n, k, (n-k+1)/2]]_p$




Polynomial codes: CSS codes. Let $\alpha_0, \ldots, \alpha_{n-1}$ be distinct non-zero numbers in $\mathbb{Z}_p$
$p > n$
$(a_0, \ldots, a_{k-1}) \longmapsto \sum_f |f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})\rangle$
f is a polynomial of degree $\leq g$ s.t. $f = \sum_{j=0}^{g} c_j x^j$, $c_j = a_j$ for $j < k$
Thm. This is a $[[n, k, d]]_p$ with $d = \min(n-g, g+2-k)$
$n - g = g + 2 - k \Rightarrow g = (n+k-2)/2$
$[[n, k, (n-k+2)/2]]_p$ or $[[n, k, (n-k+1)/2]]_p$

Thm When $D=p$ is prime,

a) If S has r generators, $T(S)$ encodes $n-r$ logical qudits

b) The distance of S is the minimum weight of $M \in N(S) \setminus S$.

Elements of S are form (with generators $M_1, \ldots, M_r$)

$$\prod_{i=1}^{r} M_i^{a_i}, \quad a_i \in \{0, 1, \ldots, p-1\}$$

Symplectic representation

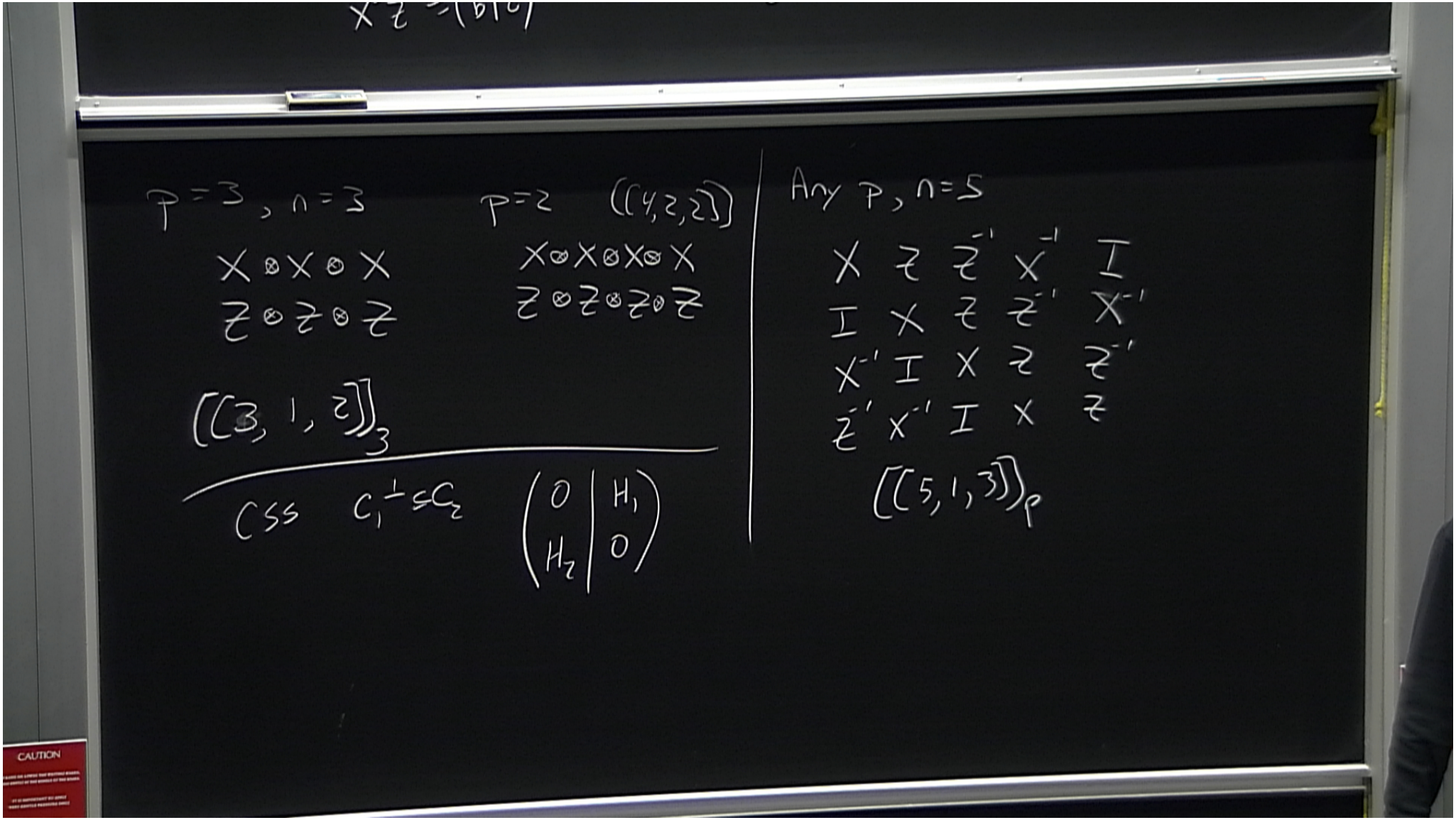
$X = (1|0)$, $Z = (0|1)$

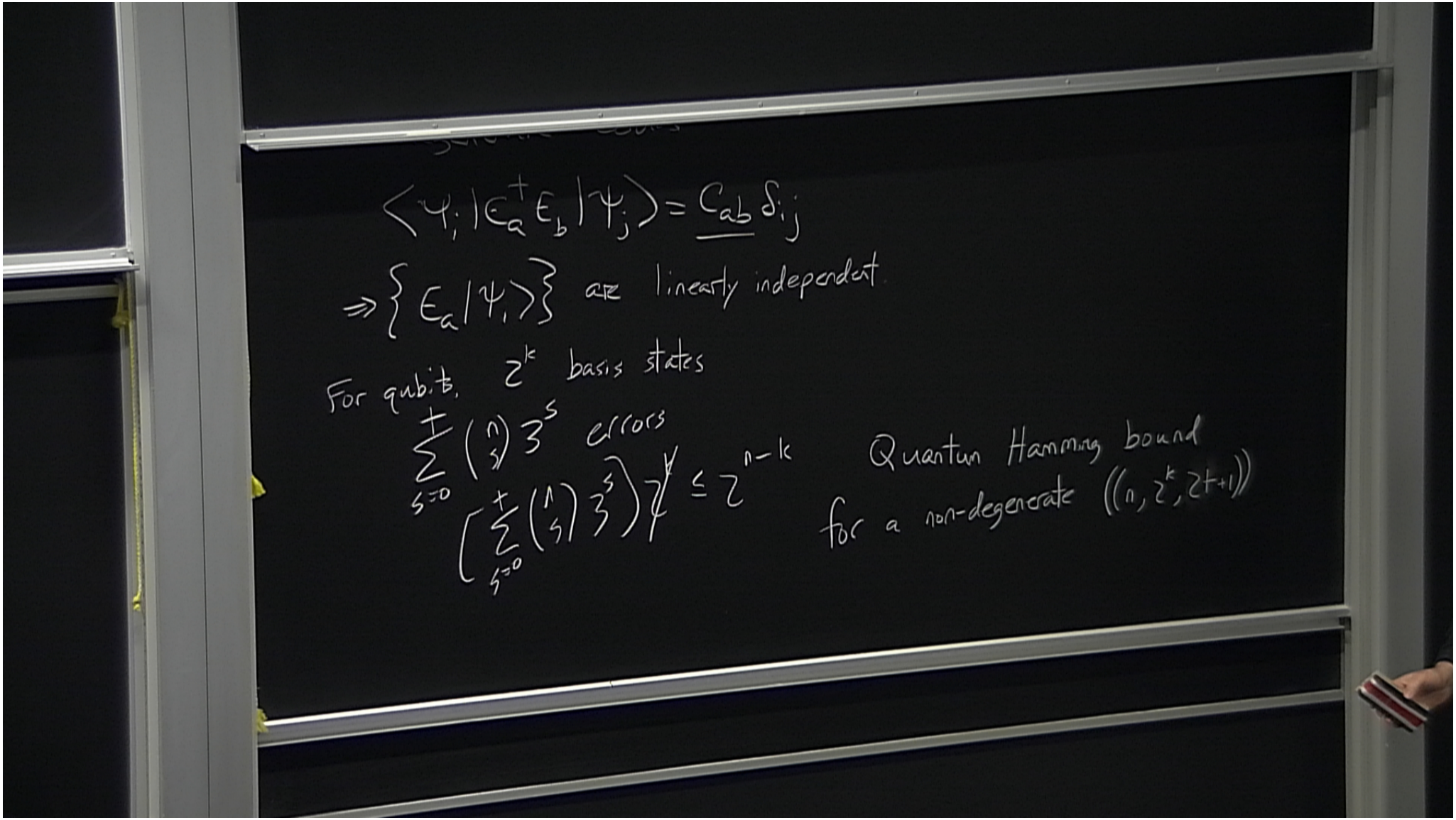
$X^b Z^c = (b|c)$

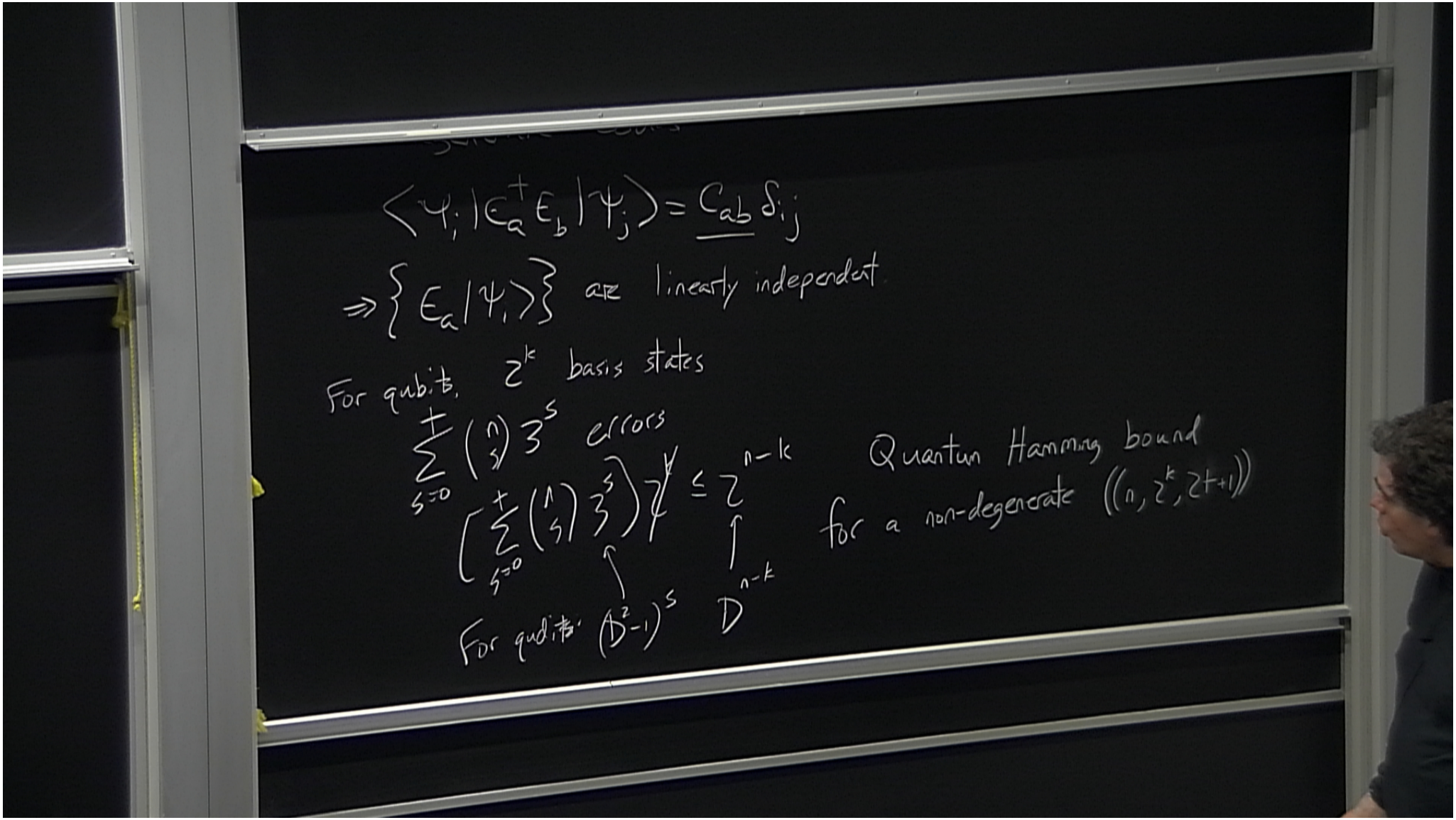
Symplectic form $(\vec{a}|\vec{b}) \odot (\vec{c}|\vec{d})$

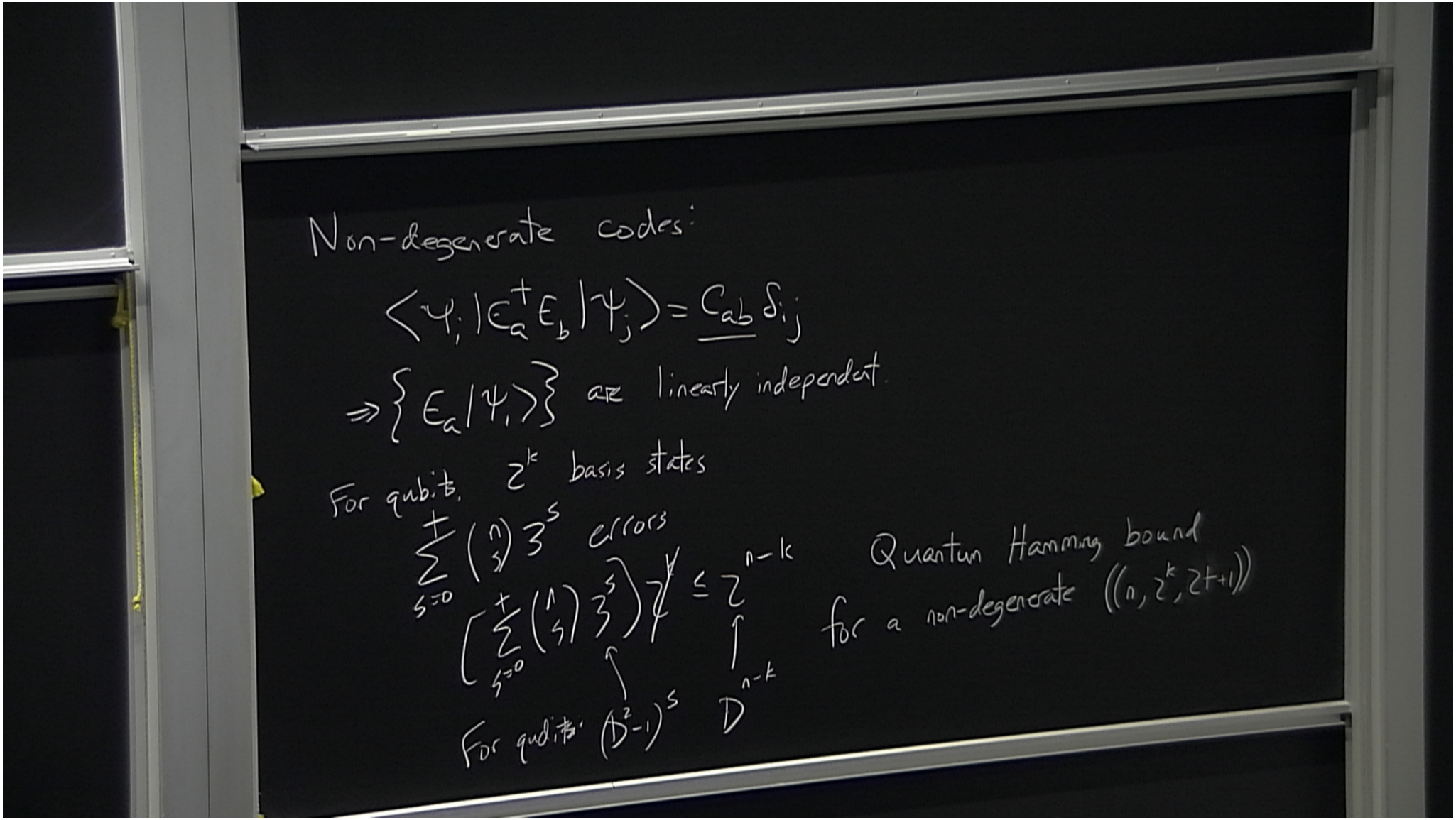
$= \vec{b}\cdot\vec{c} - \vec{a}\cdot\vec{d}$

$= 0$ iff corresponding Paulis commute


p=3, n=3
X⊗X⊗X
Z⊗Z⊗Z
[[3, 1, 2]]3
p=2 [[4,2,2]]
X⊗X⊗X⊗X
Z⊗Z⊗Z⊗Z
Any p, n=5
X Z Z⁻¹ X⁻¹ I
I X Z Z⁻¹ X⁻¹
X⁻¹ I X Z Z⁻¹
Z⁻¹ X⁻¹ I X Z
[[5,1,3]]p
CSS C1⊥ ⊆ C2
(0 | H1 / H2 | 0)


$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$
$\Rightarrow \{ E_a | \psi_i \rangle \}$ are linearly independent
For qubits, 2^k basis states
$\sum_{s=0}^{t} \binom{n}{s} 3^s$ errors
$\left[\sum_{s=0}^{t} \binom{n}{s} 3^s \right] 2^k \leq 2^{n-k}$
Quantum Hamming bound
for a non-degenerate $((n, 2^k, 2t+1))$

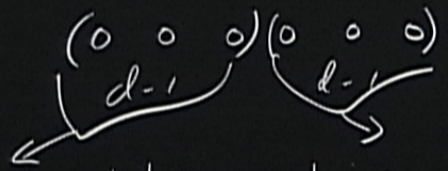

$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$
$\Rightarrow \{ E_a | \psi_i \rangle \}$ are linearly independent
For qubits, 2^k basis states
$\sum_{s=0}^{t} \binom{n}{s} 3^s$ errors
$\left[\sum_{s=0}^{t} \binom{n}{s} 3^s \right] 2^k \leq 2^{n-k}$
Quantum Hamming bound
for a non-degenerate $((n, 2^k, 2t+1))$
For qudits, $(D^2-1)^s$
D^{n-k}


Non-degenerate codes:
$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$
$\Rightarrow \{ E_a | \psi_i \rangle \}$ are linearly independent
For qubits: 2^k basis states
$\sum_{s=0}^{t} \binom{n}{s} 3^s$ errors
$\left[\sum_{s=0}^{t} \binom{n}{s} 3^s \right] 2^k \leq 2^{n-k}$ Quantum Hamming bound
for a non-degenerate $((n, 2^k, 2t+1))$
For qudits: $(D^2-1)^s$ D^{n-k}

Thm (Quantum Singleton bound): An $((n, 2^k, d))$ must satisfy $k \leq n - 2(d-1)$.

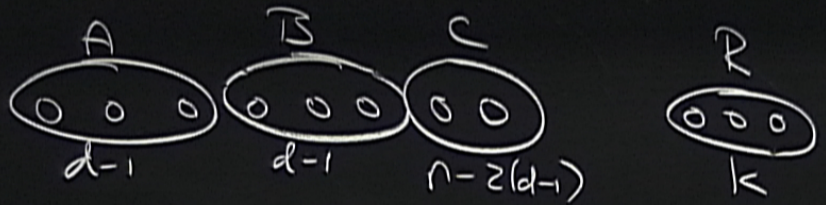
$(k=1 \Rightarrow n \geq 2d-1)$

Proof: $k=1$



violates no-cloning

Proves $k=1$ case



Maximally entangled state between R and code space

$\rho_{AR} = \rho_A \otimes \rho_R$, $\rho_{BR} = \rho_B \otimes \rho_R$

$S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$

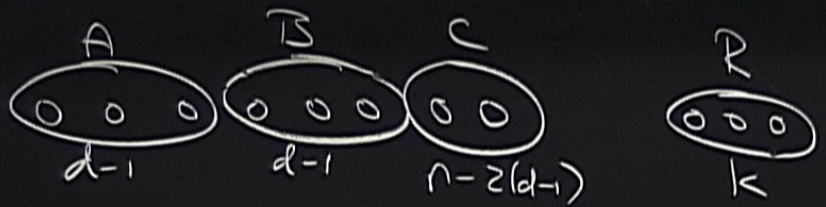
$S(AR) = S(BC) \leq S(B) + S(C)$

$= S(A) + S(R)$

k

$k \leq S(C) + S(B) - S(A)$

$k \leq S(C) + S(A) - S(B)$



Maximally entangled state between R and code space

$\rho_{AR} = \rho_A \otimes \rho_R$, $\rho_{BR} = \rho_B \otimes \rho_R$

$S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$

$S(AR) = S(BC) \leq S(B) + S(C)$

$= S(A) + S(R)$

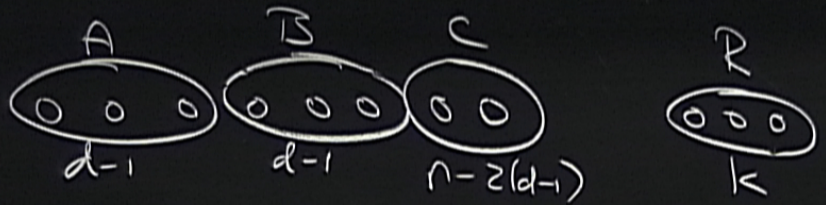
k

$k \leq S(C) + \{S(B) - S(A)\}$

$k \leq S(C) + \{S(A) - S(B)\}$

$\Downarrow$

$k \leq S(C)$



Maximally entangled state between R and code space

$\rho_{AR} = \rho_A \otimes \rho_R$, $\rho_{BR} = \rho_B \otimes \rho_R$

$S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$

$S(AR) = S(BC) \leq S(B) + S(C)$

$= S(A) + S(R)$

k

$k \leq S(C) + \{S(B) - S(A)\}$

$k \leq S(C) + \{S(A) - S(B)\}$

$\Downarrow$

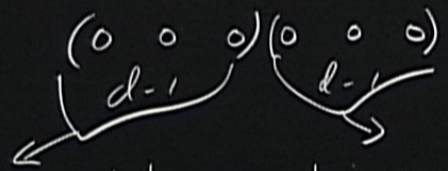
$k \leq S(C) \leq n - 2(d-1)$

Thm (Quantum Singleton bound): An $((n, 2^k, d))$ must satisfy $k \leq n - 2(d-1)$.

($k = 1 \Rightarrow n \geq 2d - 1$)

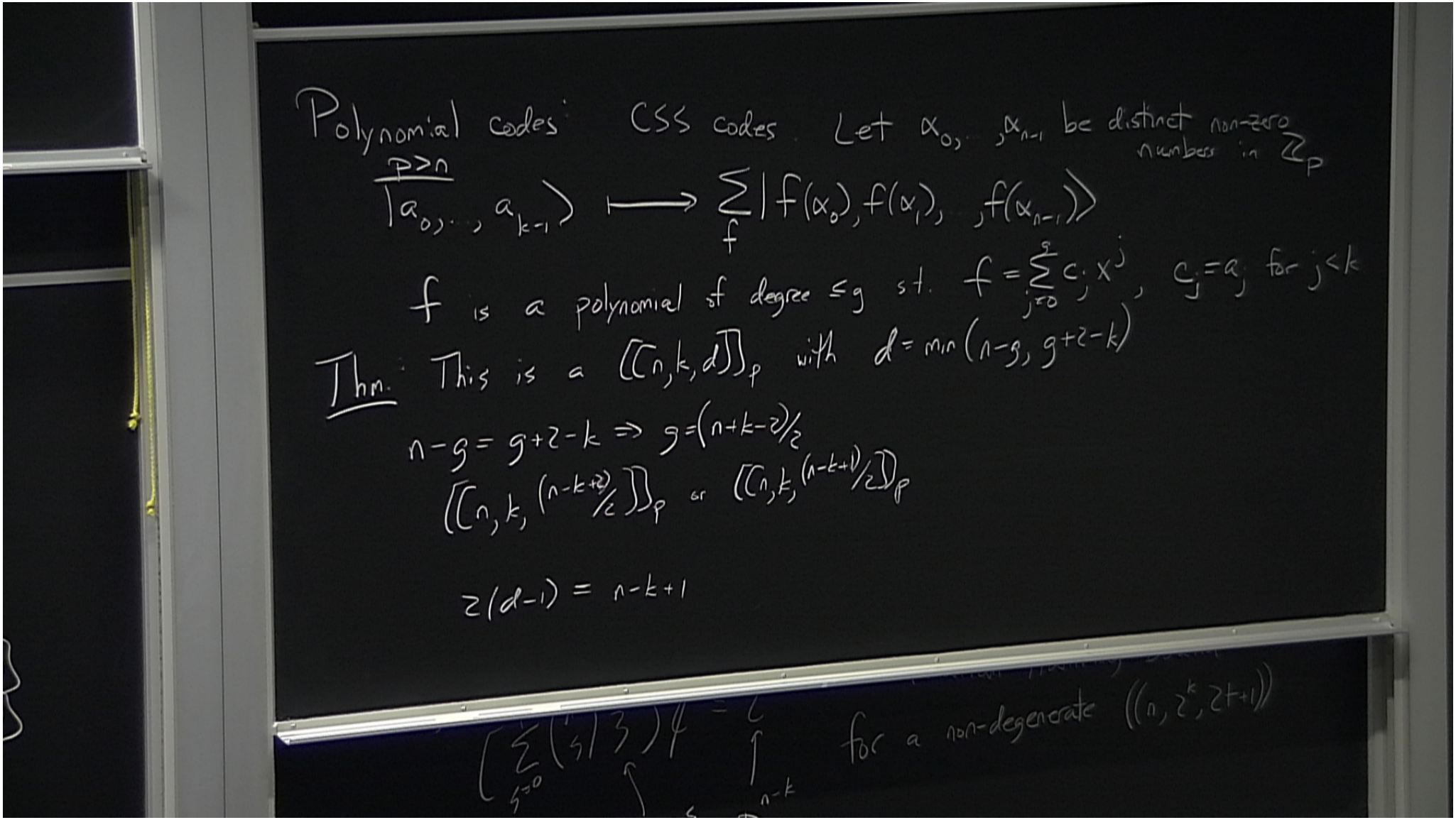
A code for which $k = n - 2(d-1)$ is a quantum MDS code

Proof: $k = 1$



violates no-cloning

Proves $k = 1$ case


Polynomial codes CSS codes Let $\alpha_0, \ldots, \alpha_{n-1}$ be distinct non-zero numbers in $\mathbb{Z}_p$
$p \geq n$
$(a_0, \ldots, a_{k-1}) \longmapsto \sum_f |f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})\rangle$
f is a polynomial of degree $\leq g$ s.t. $f = \sum_{j=0}^{g} c_j x^j$, $c_j = a_j$ for $j < k$
Thm. This is a $[[n, k, d]]_p$ with $d = \min(n-g, g+2-k)$
$n - g = g + 2 - k \Rightarrow g = (n+k-2)/2$
$[[n, k, (n-k+2)/2]]_p$ or $[[n, k, (n-k+1)/2]]_p$
$2(d-1) = n-k+1$
for a non-degenerate $((n, 2^k, 2t+1))$

Thm: (Quantum Gilbert-Varshamov bound)

Suppose n, k, d s.t.

$$\sum_{s=0}^{d-1} \binom{n}{s} 3^s \leq 2^{n-k}$$

Then $\exists$ $[[n, k, d]]$ code.

$n \to \infty$ $\frac{s}{n}$ constant

$$\binom{n}{s} \to 2^{n h(s/n)}$$

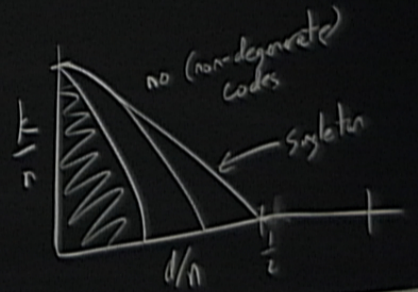
$$h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

Hamming bound

$$\frac{k}{n} \leq 1 - \frac{t}{n} \log_2 3 - h\left(\frac{t}{n}\right)$$

GV bound

$$\frac{k}{n} \leq 1 - \frac{d}{n} \log_2 3 - h\left(\frac{d}{n}\right)$$



Thm: (Quantum Gilbert-Varshamov bound)

Suppose n, k, d s.t.

$$\sum_{s=0}^{d-1} \binom{n}{s} 3^s \leq 2^{n-k}$$

Then $\exists$ $[[n, k, d]]$ code.

$n \to \infty$ $\frac{s}{n}$ constant

$$\binom{n}{s} \to 2^{n\, h(s/n)}$$

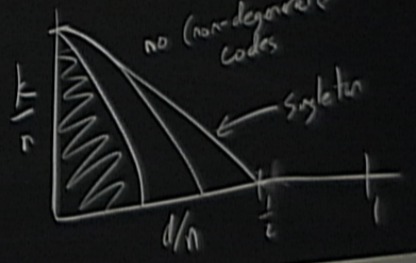
$$h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

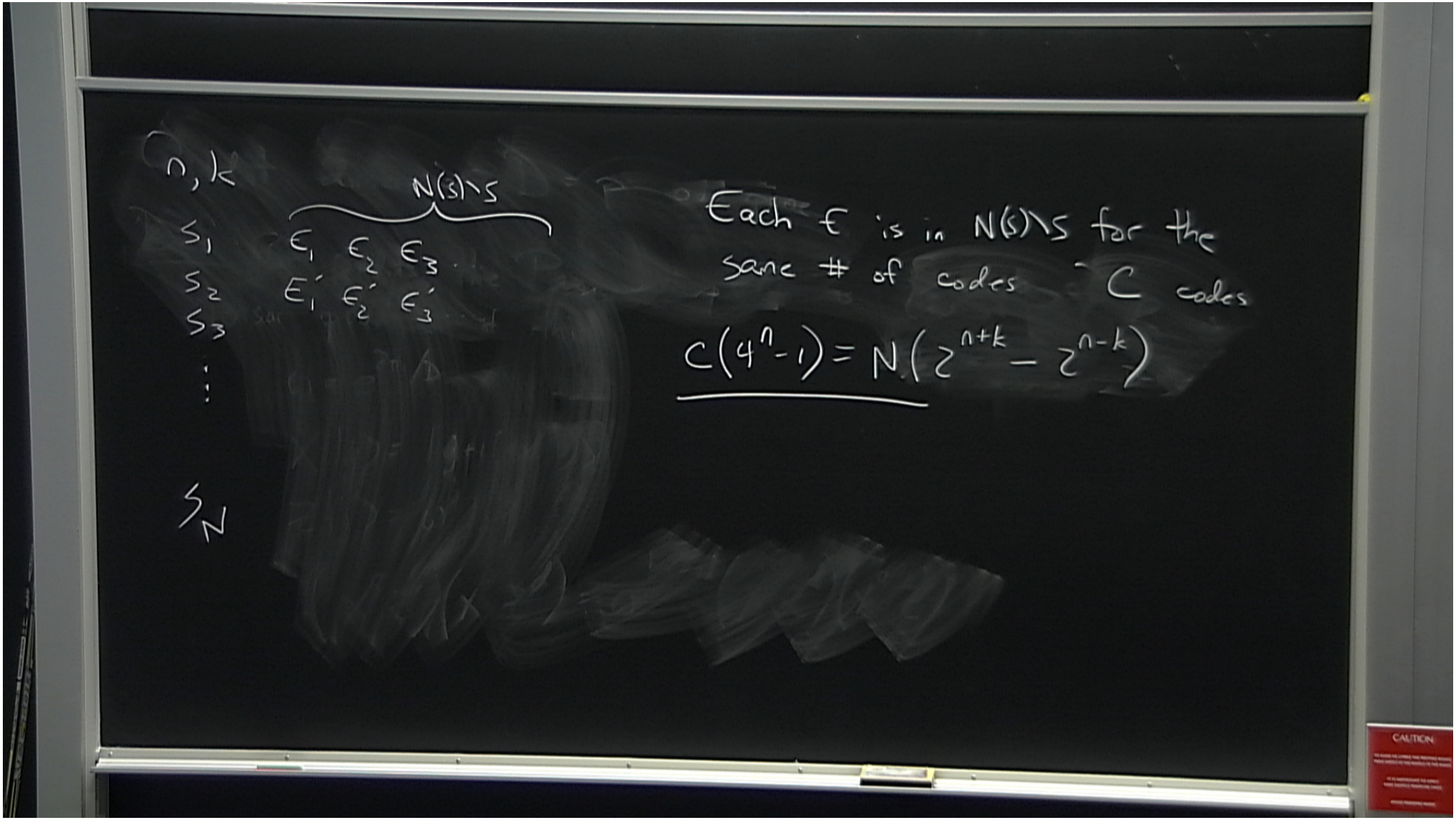
Hamming bound

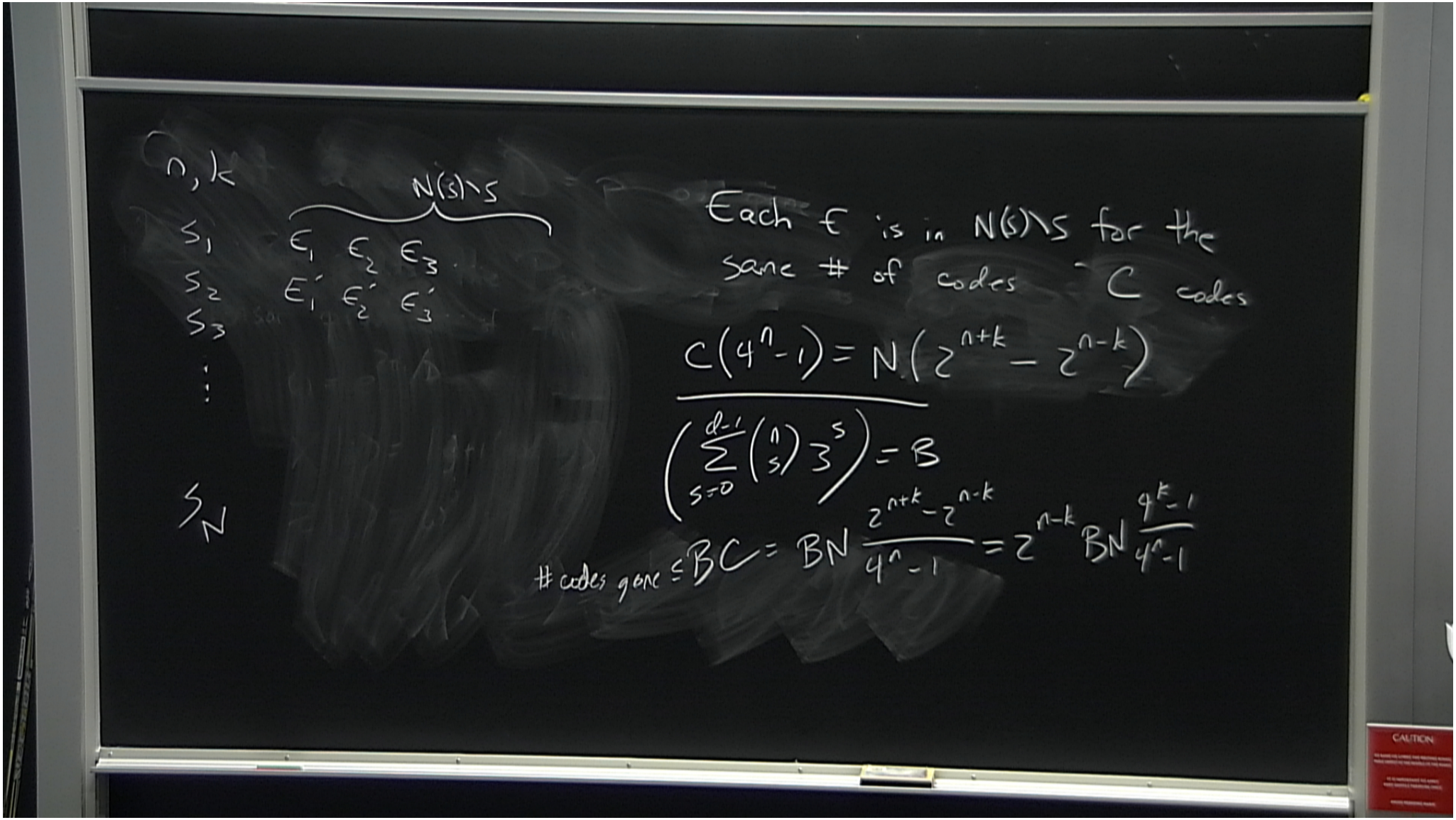
$$\frac{k}{n} \leq 1 - \frac{t}{n} \log_2 3 - h\left(\frac{t}{n}\right)$$

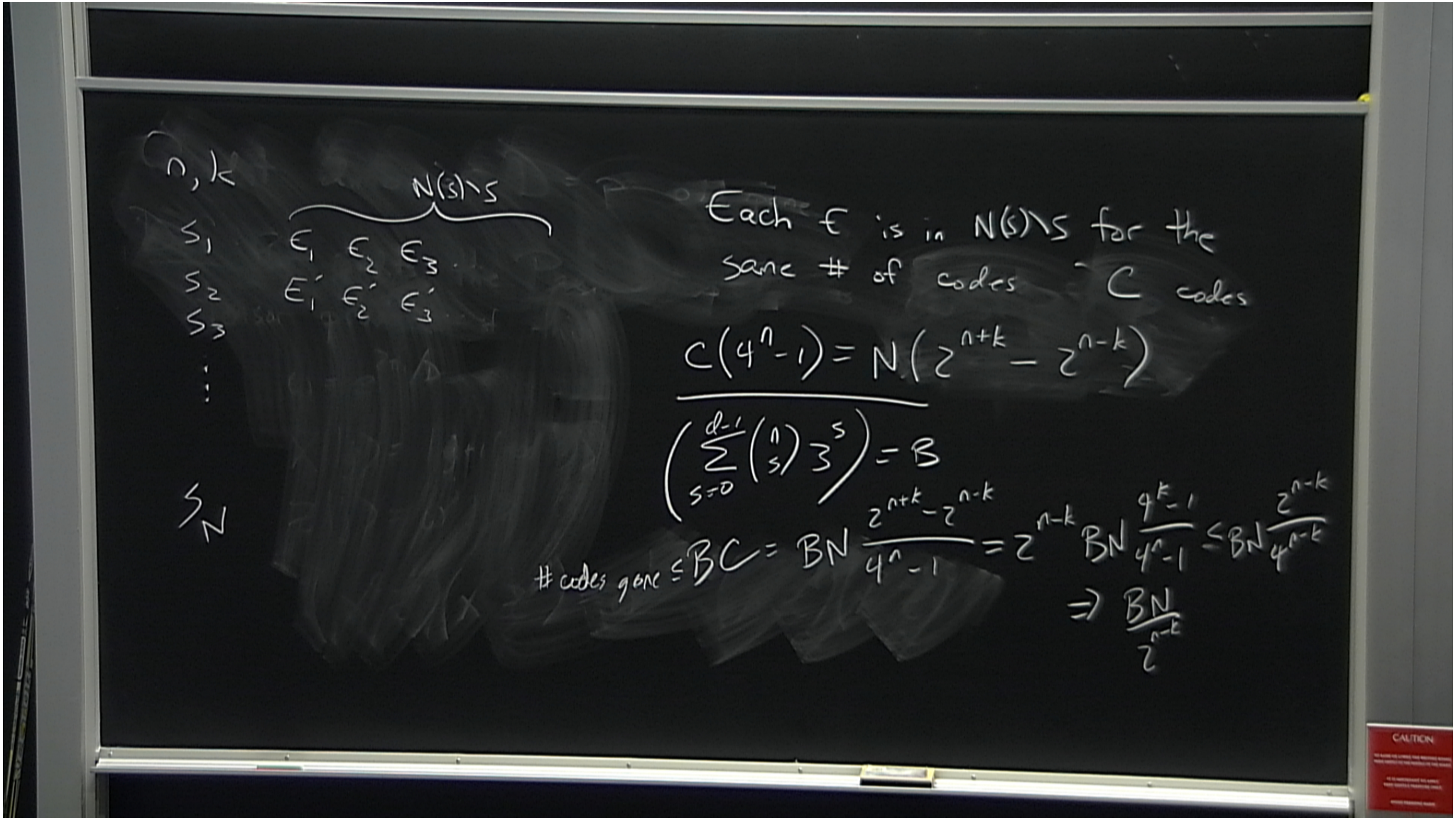
GV bound

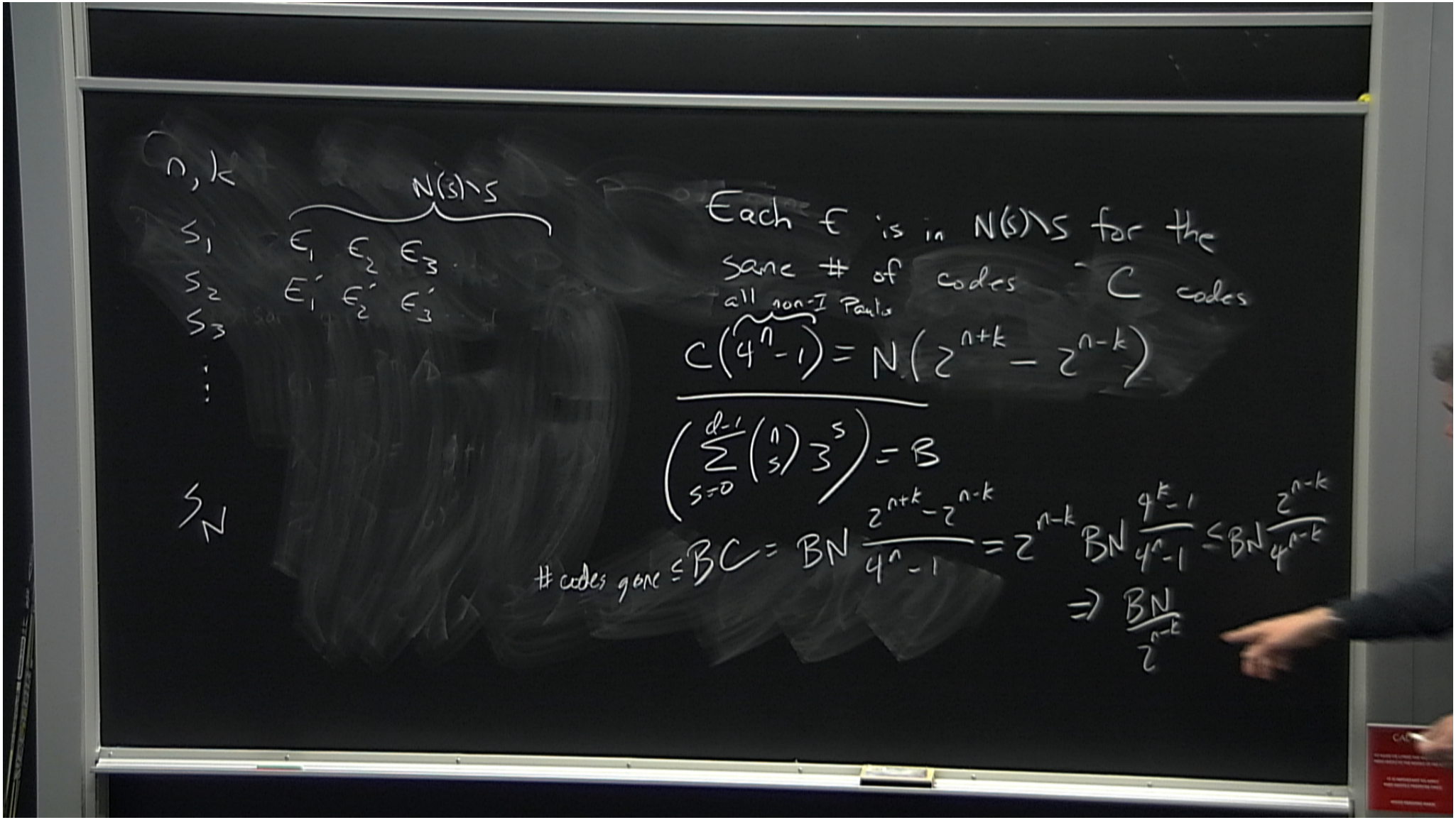
$$\frac{k}{n} \leq 1 - \frac{d}{n} \log_2 3 - h\left(\frac{d}{n}\right)$$

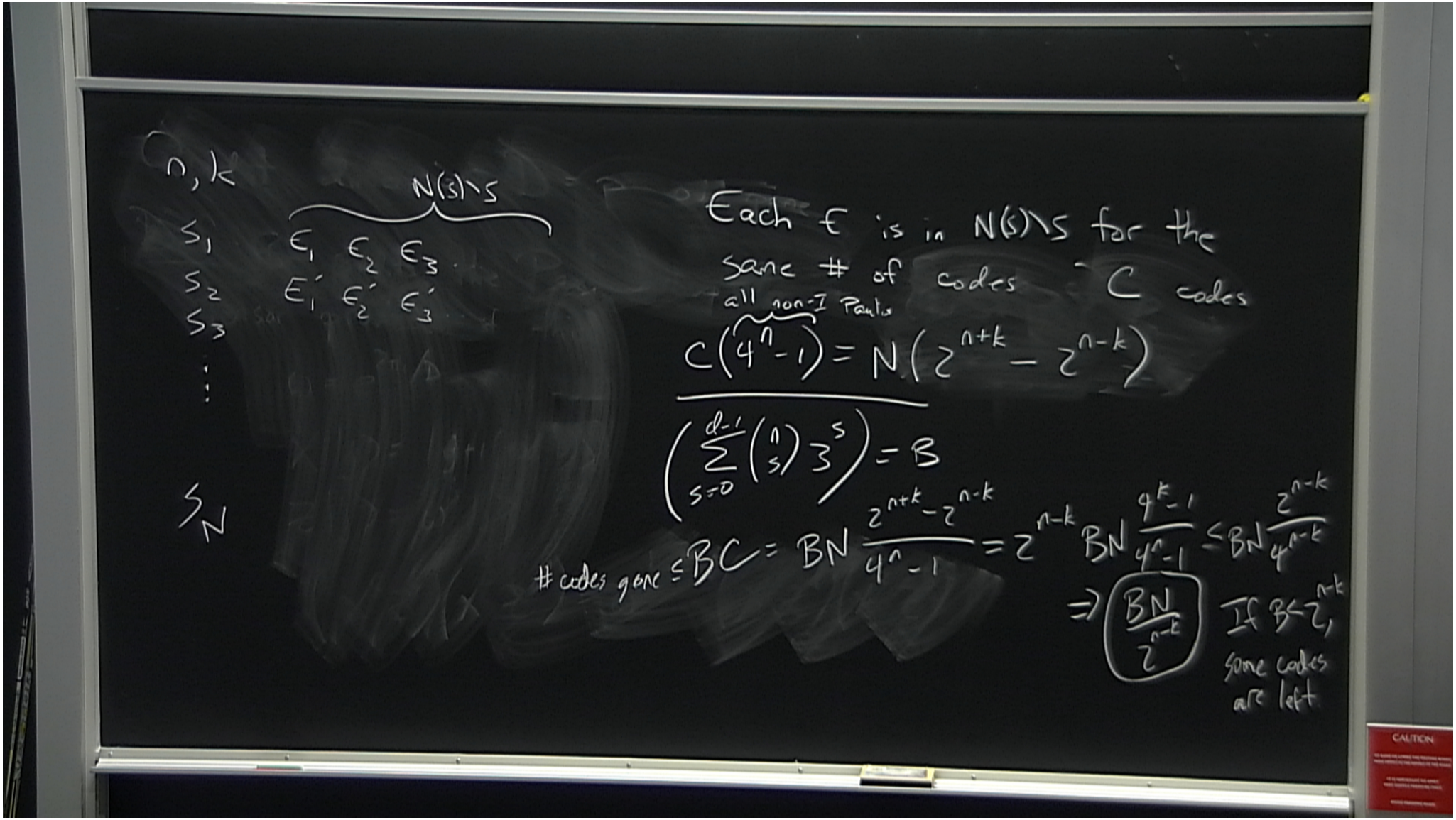


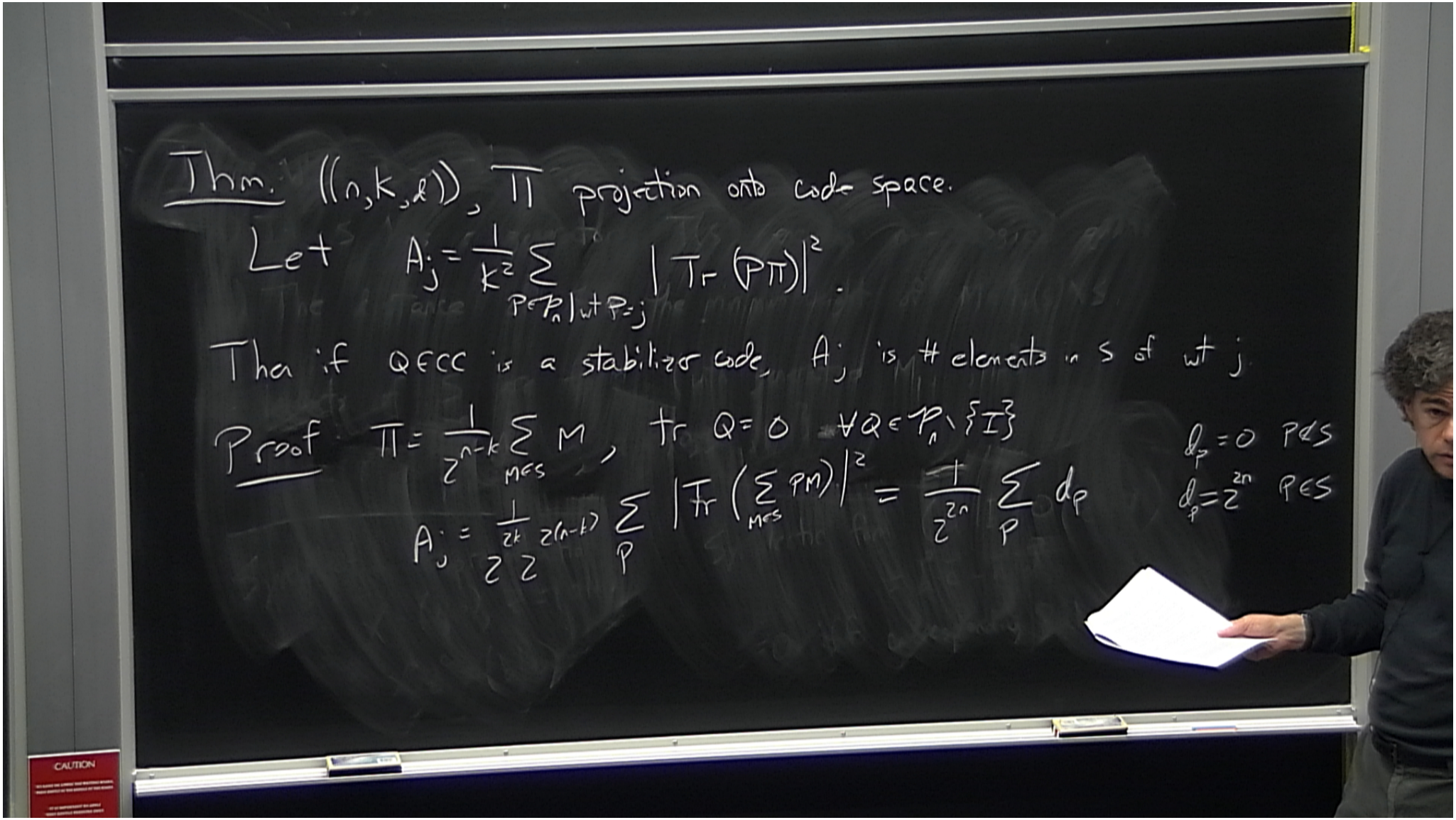

n, k
N(S)\S
S_1 ϵ_1 ϵ_2 ϵ_3
S_2 ϵ_1' ϵ_2' ϵ_3'
S_3
S_N
Each ϵ is in N(S)\S for the same # of codes C codes
$C(4^n - 1) = N(2^{n+k} - 2^{n-k})$
CAUTION

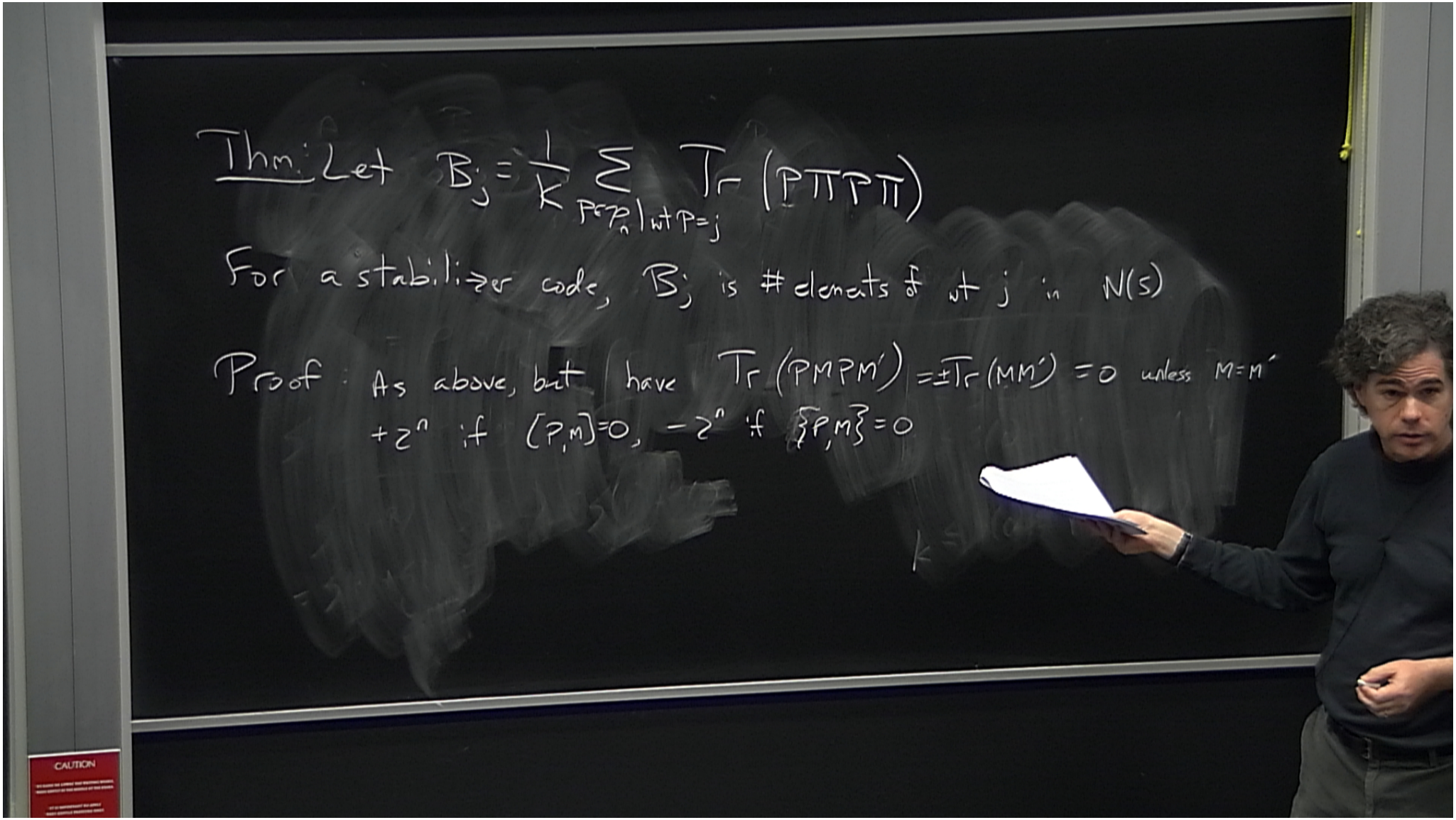

n, k
N(S)\S
S_1 ϵ_1 ϵ_2 ϵ_3
S_2 ϵ_1' ϵ_2' ϵ_3'
S_3
S_N
Each ϵ is in N(S)\S for the same # of codes C codes
$C(4^n-1) = N(2^{n+k} - 2^{n-k})$
$\left(\sum_{s=0}^{d-1} \binom{n}{s} 3^s\right) = B$
codes gone $\leq BC = BN \frac{2^{n+k}-2^{n-k}}{4^n-1} = 2^{n-k} BN \frac{4^k-1}{4^n-1}$


n, k
N(s)\S
S_1 E_1 E_2 E_3
S_2 E_1' E_2' E_3'
S_3
S_N
Each E is in $N(S)\backslash S$ for the same # of codes
C codes
$C(4^n-1) = N(2^{n+k} - 2^{n-k})$
$\left(\sum_{s=0}^{d-1} \binom{n}{s} 3^s\right) = B$
codes gone $\leq BC = BN \frac{2^{n+k}-2^{n-k}}{4^n-1} = 2^{n-k} BN \frac{4^k-1}{4^n-1} \leq BN \frac{2^{n-k}}{4^{n-k}}$
$\Rightarrow \frac{BN}{2^{n-k}}$


n, k
N(S)\S
S_1 ϵ_1 ϵ_2 ϵ_3
S_2 ϵ_1' ϵ_2' ϵ_3'
S_3
S_N
Each ϵ is in N(S)\S for the same # of codes C codes
all non-I Paulis
$C(4^n - 1) = N(2^{n+k} - 2^{n-k})$
$\left(\sum_{s=0}^{d-1} \binom{n}{s} 3^s\right) = B$
codes gone $\leq BC = BN \frac{2^{n+k} - 2^{n-k}}{4^n - 1} = 2^{n-k} BN \frac{4^k - 1}{4^n - 1} \leq BN \frac{2^{n-k}}{4^{n-k}}$
$\Rightarrow \frac{BN}{2^{n-k}}$


n, k
N(S)\S
S_1 ϵ_1 ϵ_2 ϵ_3
S_2 ϵ_1' ϵ_2' ϵ_3'
S_3
S_N
Each ϵ is in N(S)\S for the same # of codes C codes
all non-I Paulis
$C(4^n-1) = N(2^{n+k} - 2^{n-k})$
$\left(\sum_{s=0}^{d-1} \binom{n}{s} 3^s\right) = B$
codes gone $\leq BC = BN \frac{2^{n+k}-2^{n-k}}{4^n-1} = 2^{n-k} BN \frac{4^k-1}{4^n-1} \leq BN \frac{2^{n-k}}{4^{n-k}}$
$\Rightarrow \frac{BN}{2^{n-k}}$
If $B < 2^{n-k}$, some codes are left


Thm. $((n,k,d))$, Π projection onto code space.
Let $A_j = \frac{1}{k^2} \sum_{P \in \mathcal{P}_n \mid wt\, P = j} |Tr(P\Pi)|^2$.
Then if $Q \in CC$ is a stabilizer code, A_j is # elements in S of wt j.
Proof $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$, $tr\, Q = 0 \quad \forall Q \in \mathcal{P}_n \setminus \{I\}$
$A_j = \frac{1}{2^k 2^{(n-k)}} \sum_P \left| Tr\left(\sum_{M \in S} PM\right)\right|^2 = \frac{1}{2^{2n}} \sum_P d_P$
$d_P = 0$ $P \notin S$
$d_P = 2^{2n}$ $P \in S$
CAUTION


Thm: Let $B_j = \frac{1}{K} \sum_{P \in \mathcal{P}_n \text{ wt } P = j} \mathrm{Tr}(P \Pi P \Pi)$
For a stabilizer code, B_j is # elements of wt j in $N(S)$
Proof: As above, but have $\mathrm{Tr}(PMPM') = \pm \mathrm{Tr}(MM') = 0$ unless $M = M'$
$+2^n$ if $[P,M]=0$, -2^n if $\{P,M\}=0$
CAUTION

Thm: Let $B_j = \frac{1}{K} \sum_{P \in \mathcal{P}_n \text{ wt } P = j} \mathrm{Tr}(\Pi P \Pi P)$

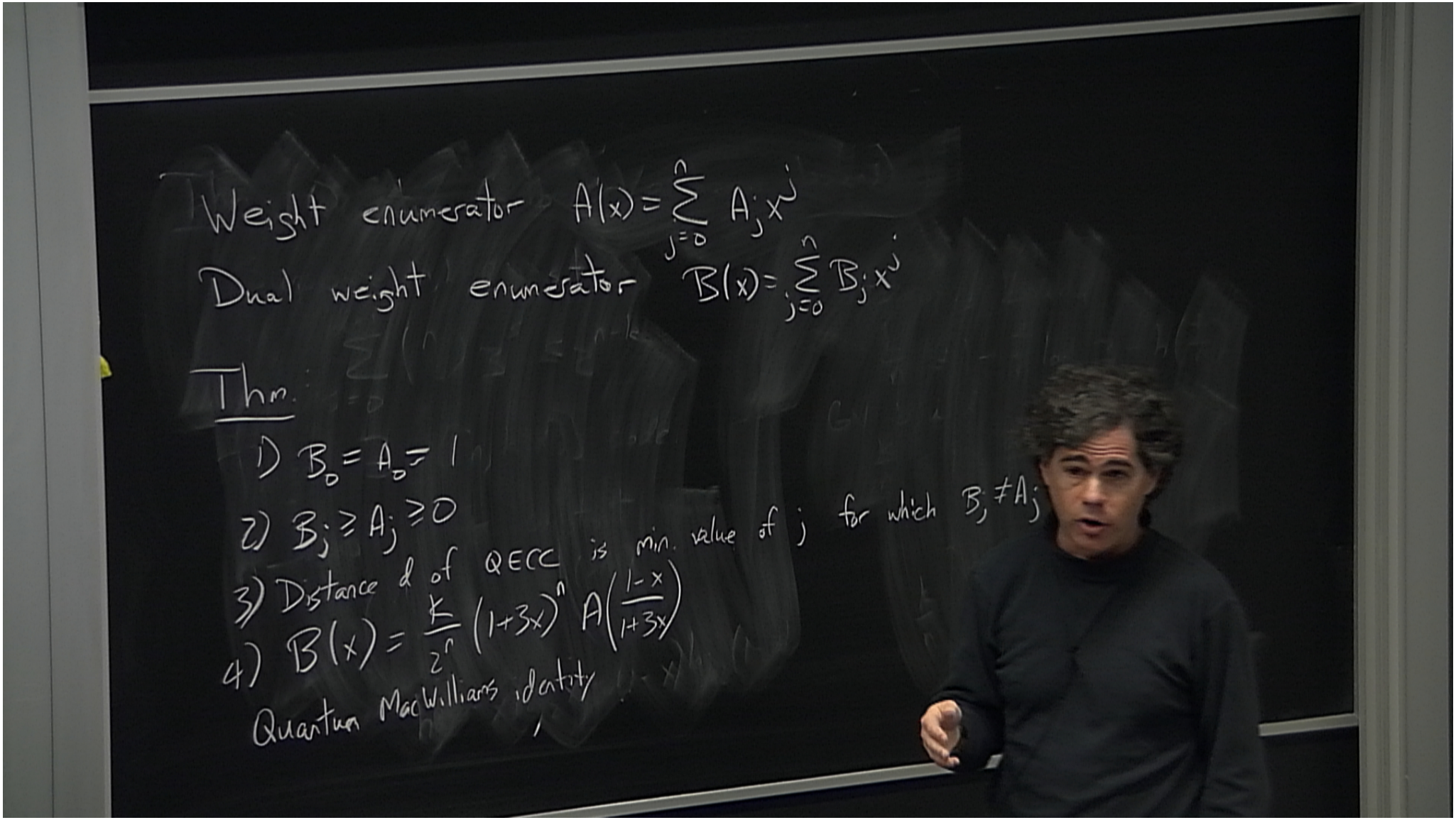
For a stabilizer code, B_j is # elements of wt j in $N(S)$

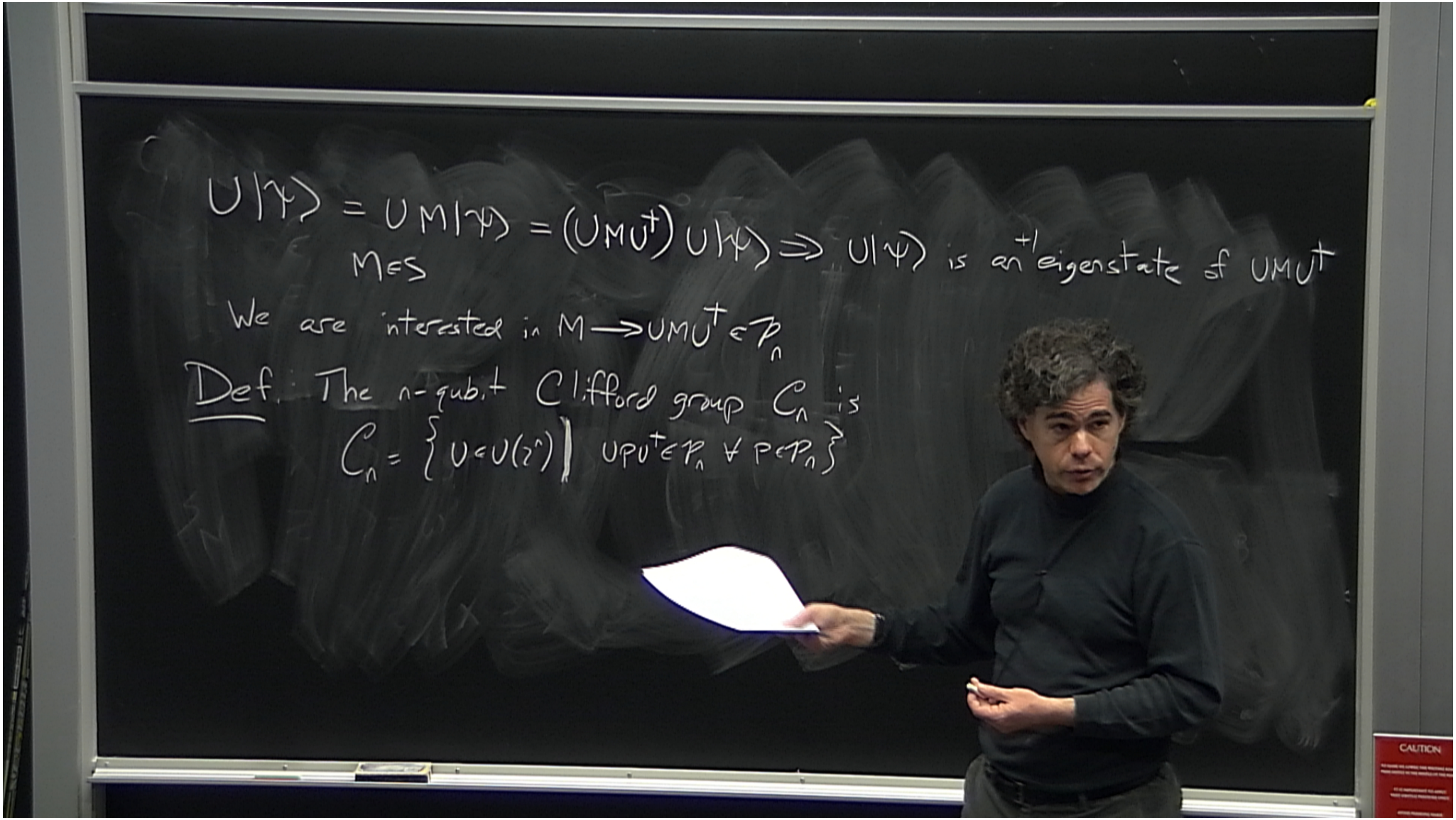
Proof: As above, but have $\mathrm{Tr}(PMPM') = \pm \mathrm{Tr}(MM') = 0$ unless $M = M'$

$+2^n$ if $[P,M]=0$, -2^n if $\{P,M\}=0$

If $P \in N(S)$ only $+$

If $P \notin N(S)$, $+$ & $-$ Cancel $\Rightarrow$ get 0.


Weight enumerator $A(x) = \sum_{j=0}^{n} A_j x^j$
Dual weight enumerator $B(x) = \sum_{j=0}^{n} B_j x^j$
Thm:
1) $B_0 = A_0 = 1$
2) $B_j \geq A_j \geq 0$
3) Distance d of QECC is min. value of j for which $B_j \neq A_j$
4) $B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$
Quantum MacWilliams identity


$U|\psi\rangle = UM|\psi\rangle = (UMU^\dagger)U|\psi\rangle \Rightarrow U|\psi\rangle$ is an ± 1 eigenstate of $UMU^\dagger$
$M \in S$
We are interested in $M \longrightarrow UMU^\dagger \in \mathcal{P}_n$
Def: The n-qubit Clifford group C_n is
$C_n = \{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
CAUTION

$U|\psi\rangle = UM|\psi\rangle = (UMU^\dagger)U|\psi\rangle \Rightarrow U|\psi\rangle$ is an ± 1 eigenstate of $UMU^\dagger$

$M \in S$

We are interested in $M \longrightarrow UMU^\dagger \in \mathcal{P}_n$

Def: The n-qubit Clifford group C_n is

$$C_n = \{ U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n \}$$

$(UV)P(V^\dagger U^\dagger) = U(\underbrace{VPV^\dagger}_{\in \mathcal{P}_n})U^\dagger \in \mathcal{P}_n$

$U|\psi\rangle = UM|\psi\rangle = (UMU^\dagger)U|\psi\rangle \Rightarrow U|\psi\rangle$ is an $+1$ eigenstate of $UMU^\dagger$

$M \in S$

We are interested in $M \longrightarrow UMU^\dagger \in \mathcal{P}_n$

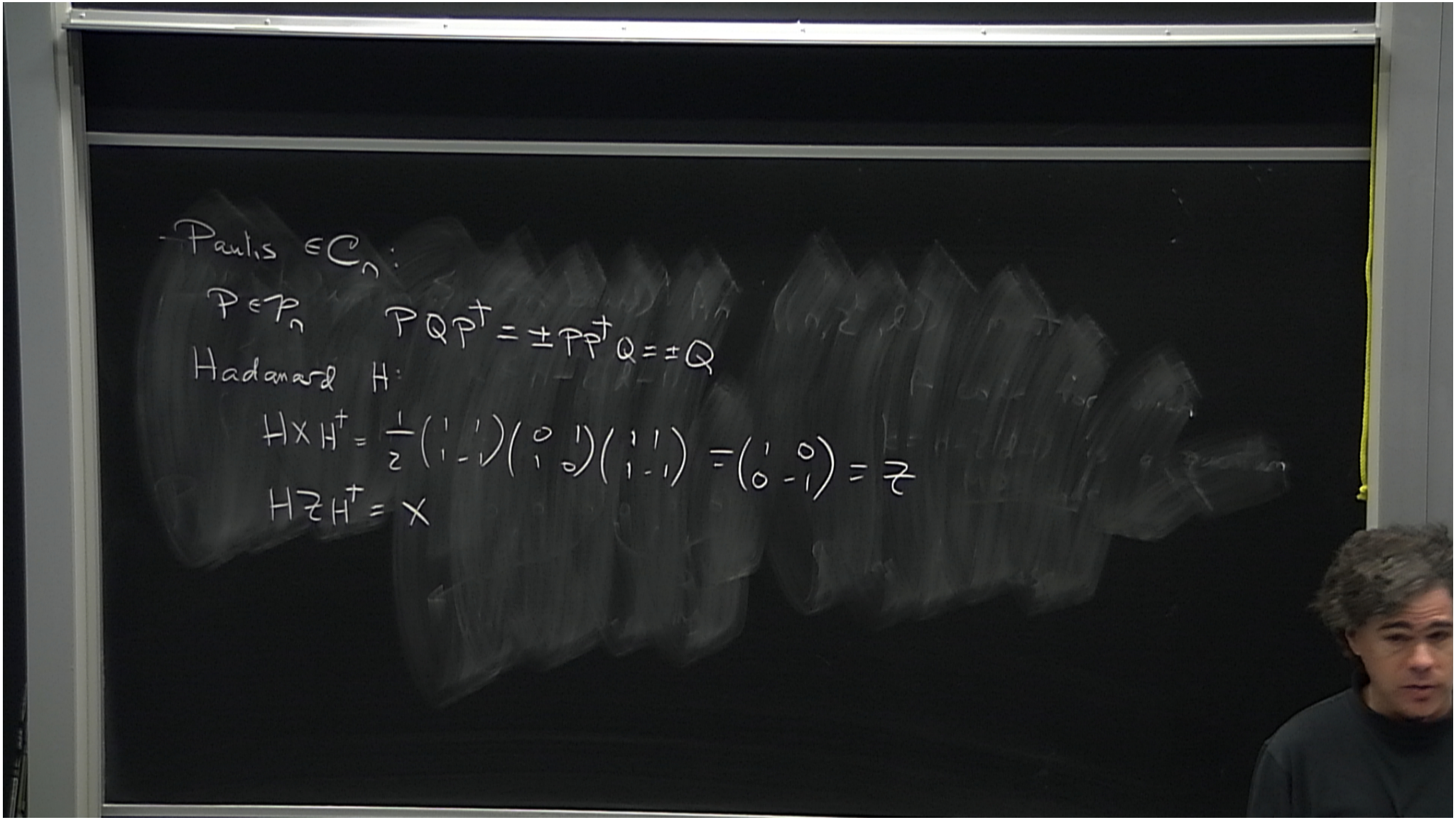
Def: The n-qubit Clifford group C_n is

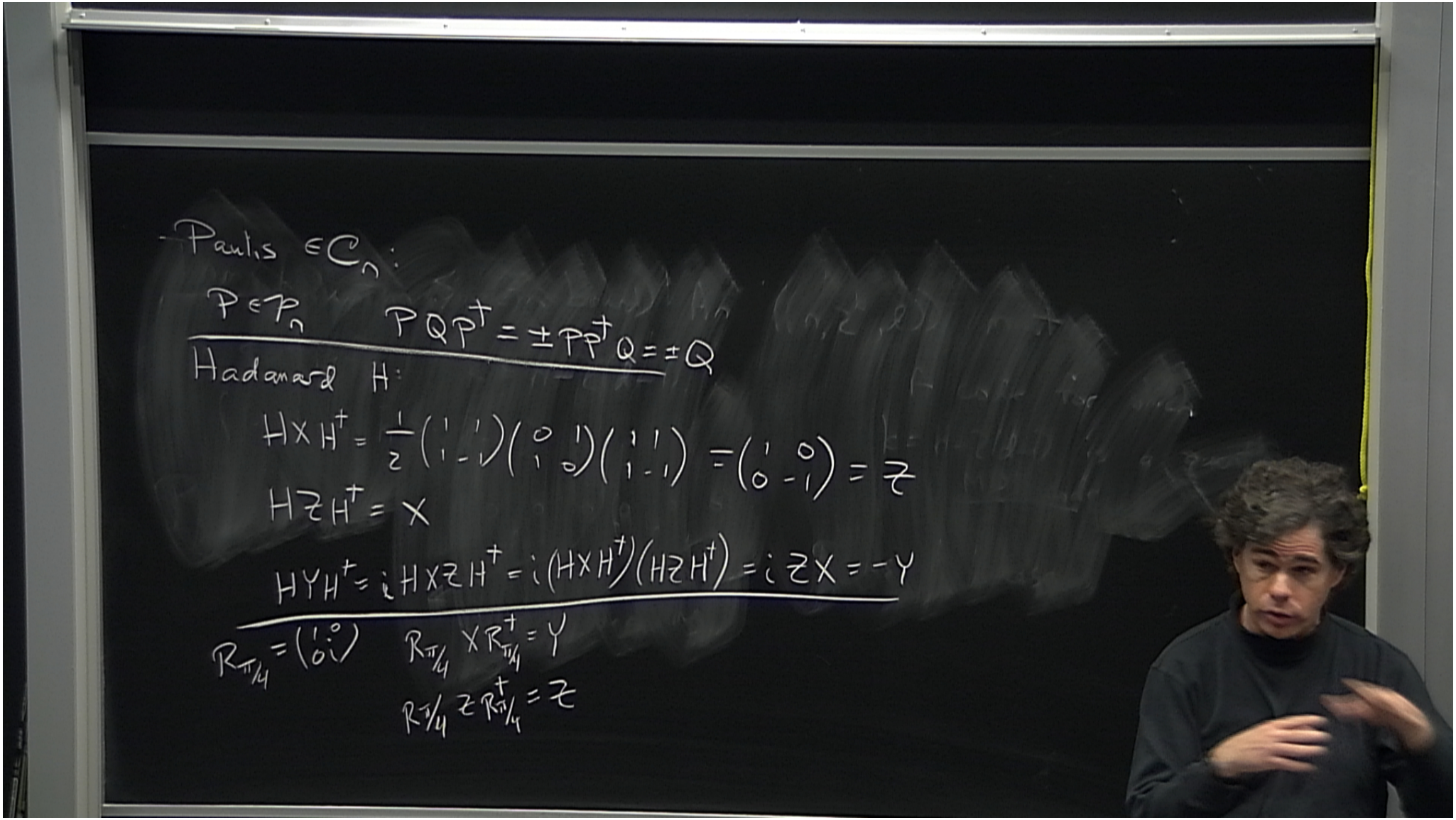
$$C_n = \{ U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall\, P \in \mathcal{P}_n \}$$

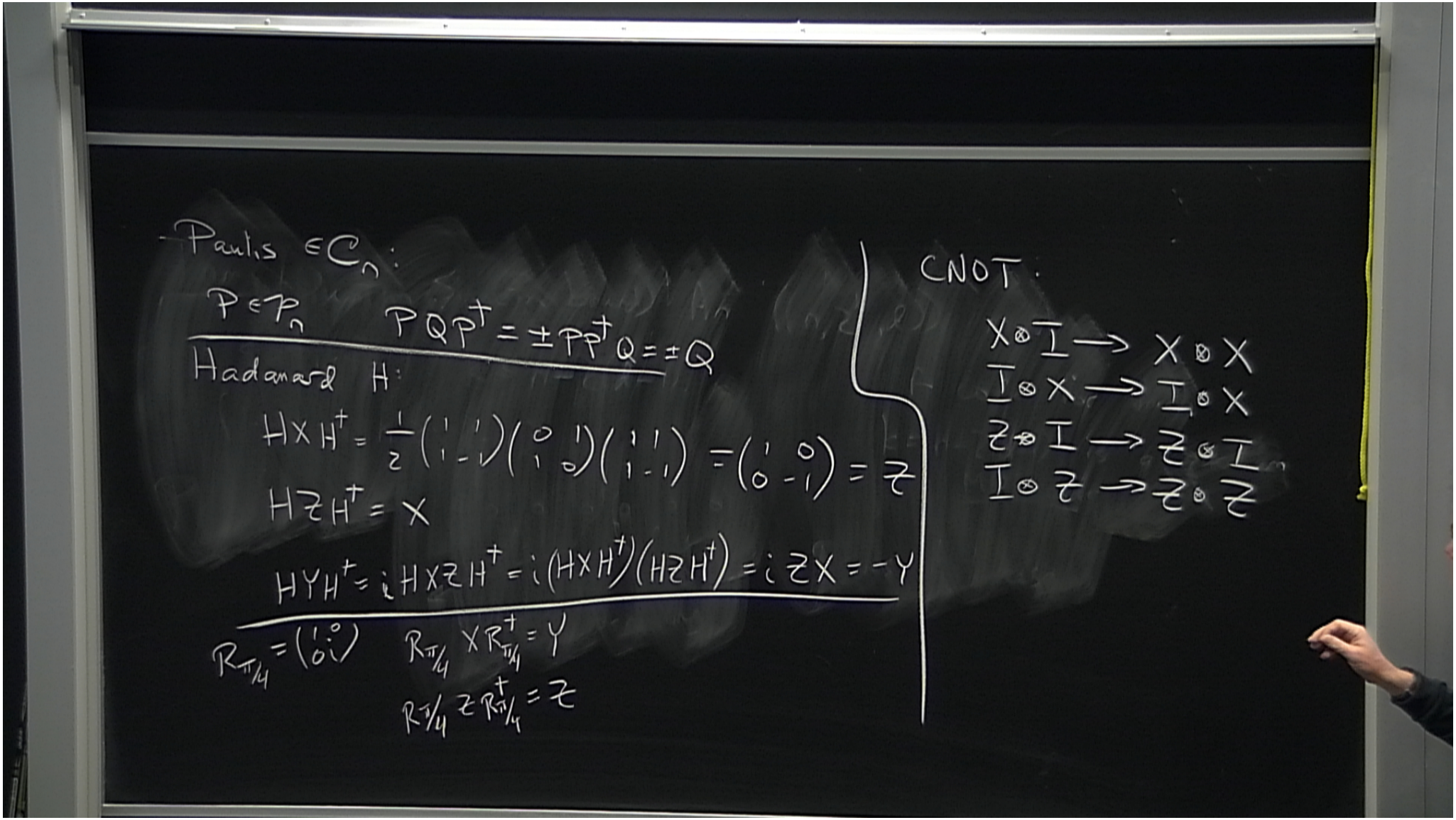
$(UV)P(V^\dagger U^\dagger) = U(VPV^\dagger)U^\dagger \in \mathcal{P}_n$

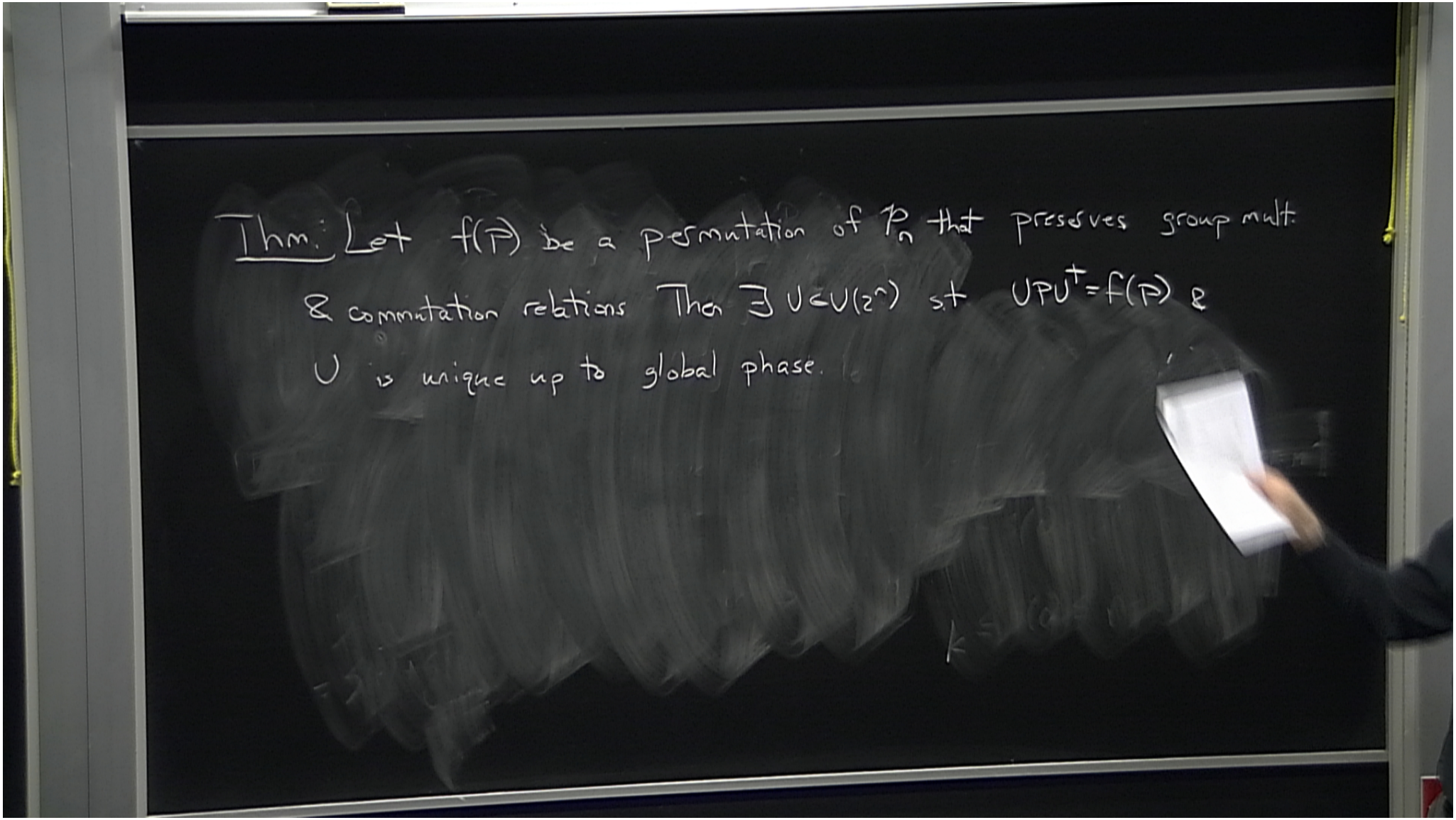
$UPU^\dagger = Q \Rightarrow U^\dagger QU = P \in \mathcal{P}_n$

$[P,Q] = 0 \iff [UPU^\dagger, UQU^\dagger] = UPQU^\dagger - UQPU^\dagger = U[P,Q]U^\dagger = 0$


Paulis $\in \mathcal{C}_n$:
$P \in \mathcal{P}_n$ $PQP^\dagger = \pm PP^\dagger Q = \pm Q$
Hadamard H:
$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = Z$
$HZH^\dagger = X$


Paulis $\in \mathbb{C}_n$:
$P \in \mathcal{P}_n \quad PQP^\dagger = \pm PP^\dagger Q = \pm Q$
Hadamard H:
$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = Z$
$HZH^\dagger = X$
$HYH^\dagger = iHXZH^\dagger = i(HXH^\dagger)(HZH^\dagger) = iZX = -Y$
$R_{\pi/4} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} \quad R_{\pi/4} X R_{\pi/4}^\dagger = Y$
$R_{\pi/4} Z R_{\pi/4}^\dagger = Z$


Paulis $\in \mathbb{C}_n$:
$P \in \mathcal{P}_n \quad PQP^\dagger = \pm PP^\dagger Q = \pm Q$
Hadamard H:
$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = Z$
$HZH^\dagger = X$
$HYH^\dagger = iHXZH^\dagger = i(HXH^\dagger)(HZH^\dagger) = iZX = -Y$
$R_{\pi/4} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$
$R_{\pi/4} X R_{\pi/4}^\dagger = Y$
$R_{\pi/4} Z R_{\pi/4}^\dagger = Z$
CNOT:
$X \otimes I \to X \otimes X$
$I \otimes X \to I \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes Z \to Z \otimes Z$


Thm: Let f(P) be a permutation of $\mathcal{P}_n$ that preserves group mult.
& commutation relations Then ∃ U∈U(2^n) s.t UPU† = f(P) &
U is unique up to global phase.

Thm: Let $f(P)$ be a permutation of $\mathcal{P}_n$ that preserves group mult. & commutation relations. Then $\exists\, U \in U(2^n)$ s.t. $UPU^\dagger = f(P)$ & U is unique up to global phase. $U \in C_n$

Proof: $|0\ldots0\rangle$ has stabilizer $\langle Z_1, Z_2, \ldots Z_n \rangle$

$\Leftarrow$ stabilizer $\langle f(Z_1), f(Z_2), \ldots f(Z_n) \rangle$

$U|0\rangle$

$|10\ldots0\rangle = X_1|0\ldots0\rangle \rightarrow U|10\ldots0\rangle = \underbrace{UX_1U^\dagger}_{f(X)} U|0\ldots0\rangle = f(X_1)\, U|0\ldots0\rangle$

Thm: Let $f(P)$ be a permutation of $\mathcal{P}_n$ that preserves group mult. & commutation relations. Then $\exists\, U \in U(2^n)$ s.t. $UPU^\dagger = f(P)$ & U is unique up to global phase. $U \in C_n$

Proof: $|0\ldots0\rangle$ has stabilizer $\langle Z_1, Z_2, \ldots Z_n \rangle$

$\downarrow$

stabilizer $\langle f(Z_1), f(Z_2), \ldots f(Z_n) \rangle$

$U|0\rangle \Leftarrow$ stabilizer

$|10\ldots0\rangle = X_1|0\ldots0\rangle \rightarrow U|10\ldots0\rangle = \underbrace{UX_1U^\dagger}_{f(X_1)} U|0\ldots0\rangle = f(X_1)\, U|0\ldots0\rangle$

$|11\ldots10\rangle = X_2|0\ldots0\rangle \rightarrow$ $\qquad\qquad f(X_2)\, U|0\ldots0\rangle$

Thm: Let $f(P)$ be a permutation of $\mathcal{P}_n$ that preserves group mult. & commutation relations. Then $\exists\, U \in U(2^n)$ s.t. $UPU^\dagger = f(P)$ & U is unique up to global phase. $U \in C_n$

Proof: $|0\ldots0\rangle$ has stabilizer $\langle Z_1, Z_2, \ldots Z_n \rangle$

$\Leftarrow$ stabilizer $\langle f(Z_1), f(Z_2), \ldots f(Z_n) \rangle$

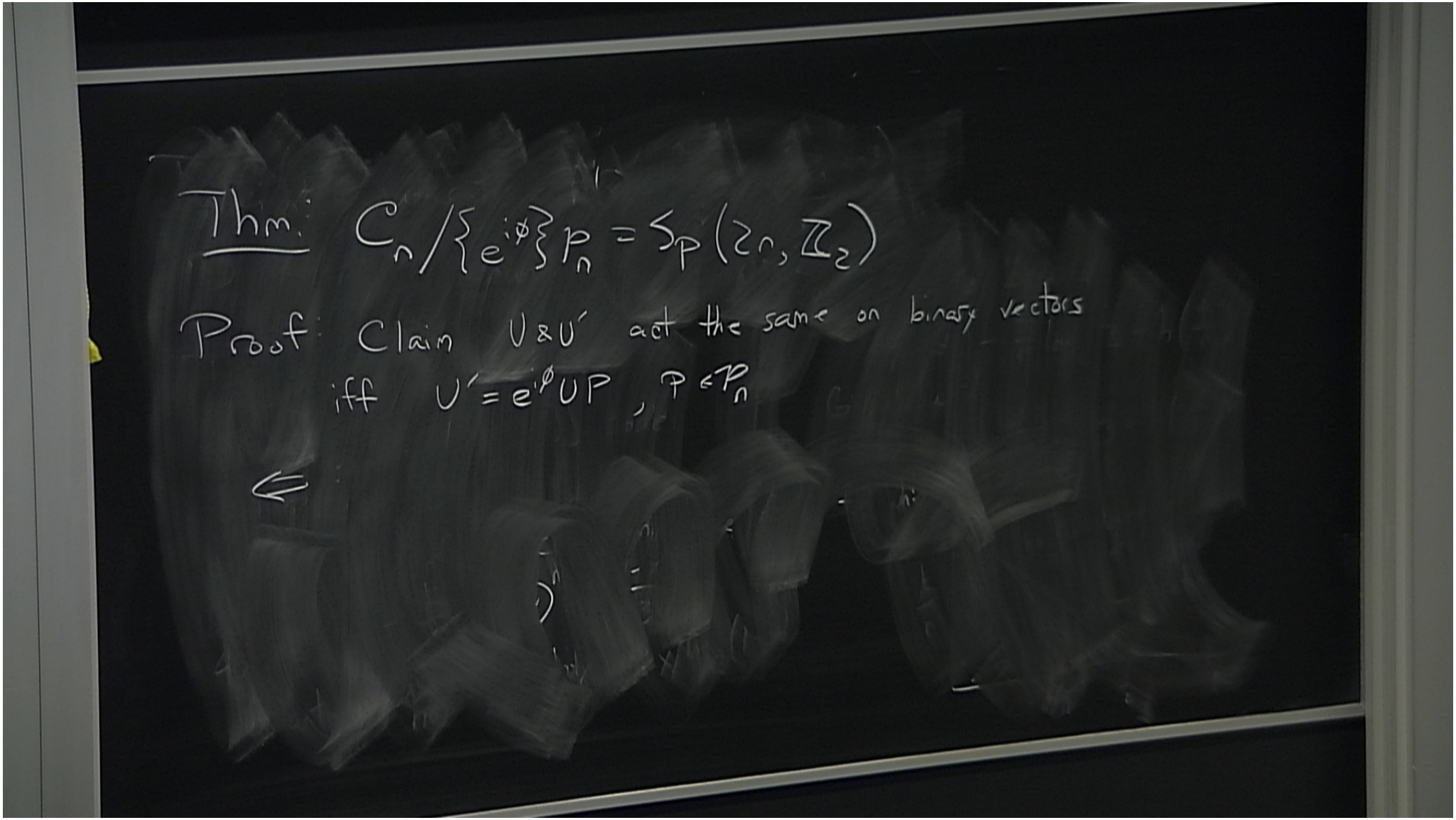
$U|0\rangle$

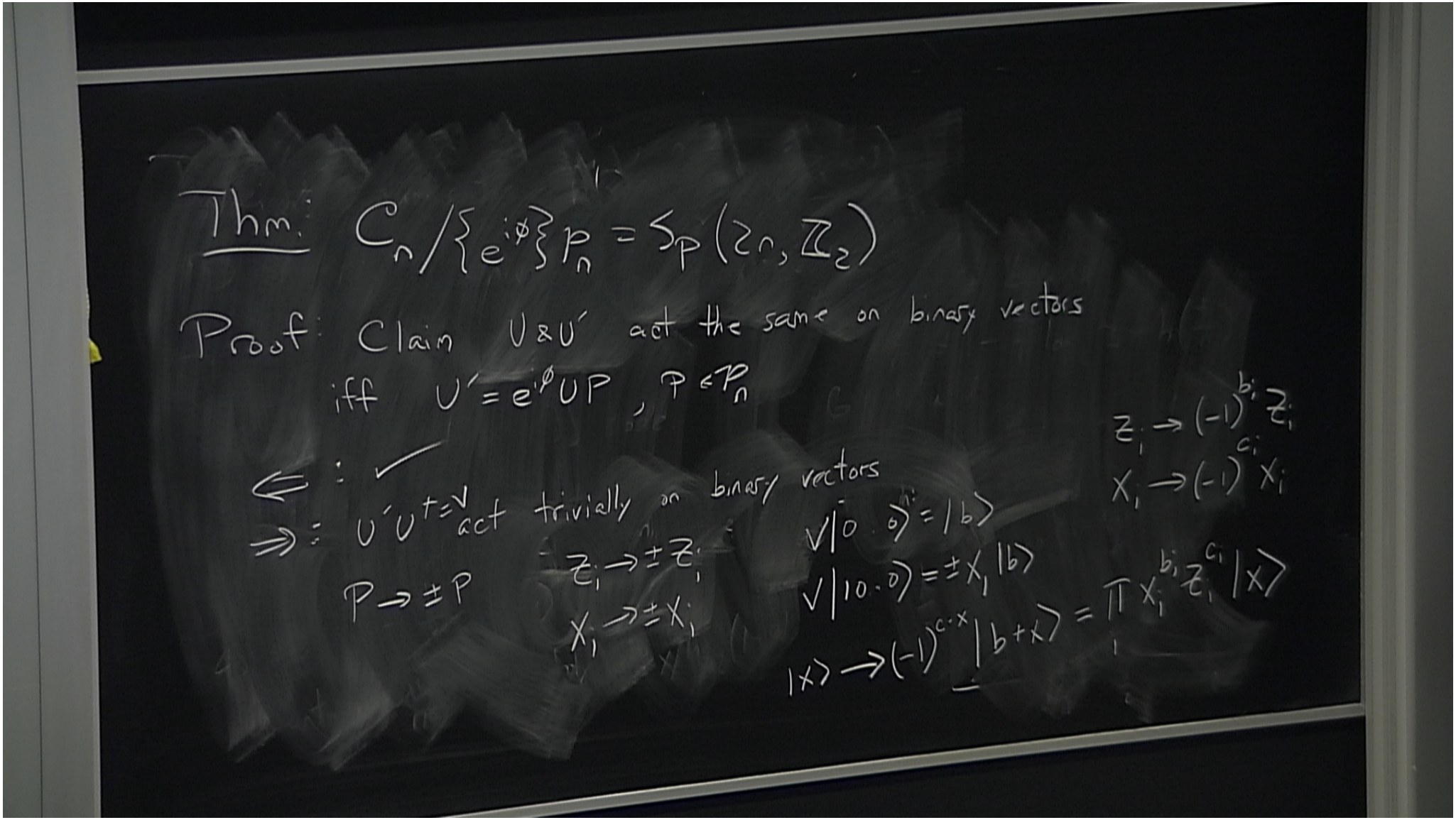
$|10\ldots0\rangle = X_1|0\ldots0\rangle \rightarrow U|10\ldots0\rangle = UX_1U^\dagger U|0\ldots0\rangle = f(X_1)\,U|0\ldots0\rangle$

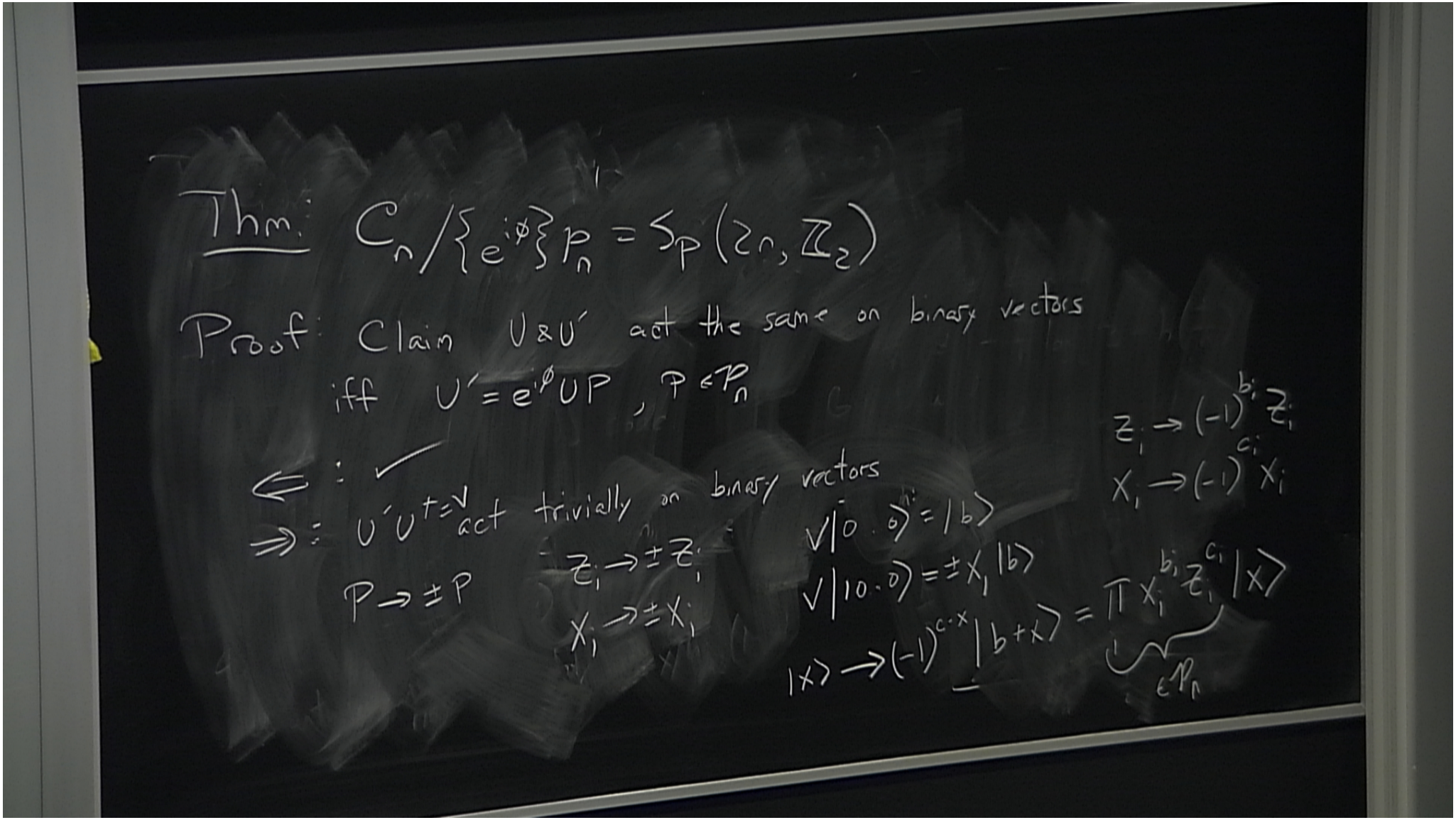
$|11\ldots10\rangle = X_2|0\ldots0\rangle \rightarrow$ $f(X_2)\,U|0\ldots0\rangle$

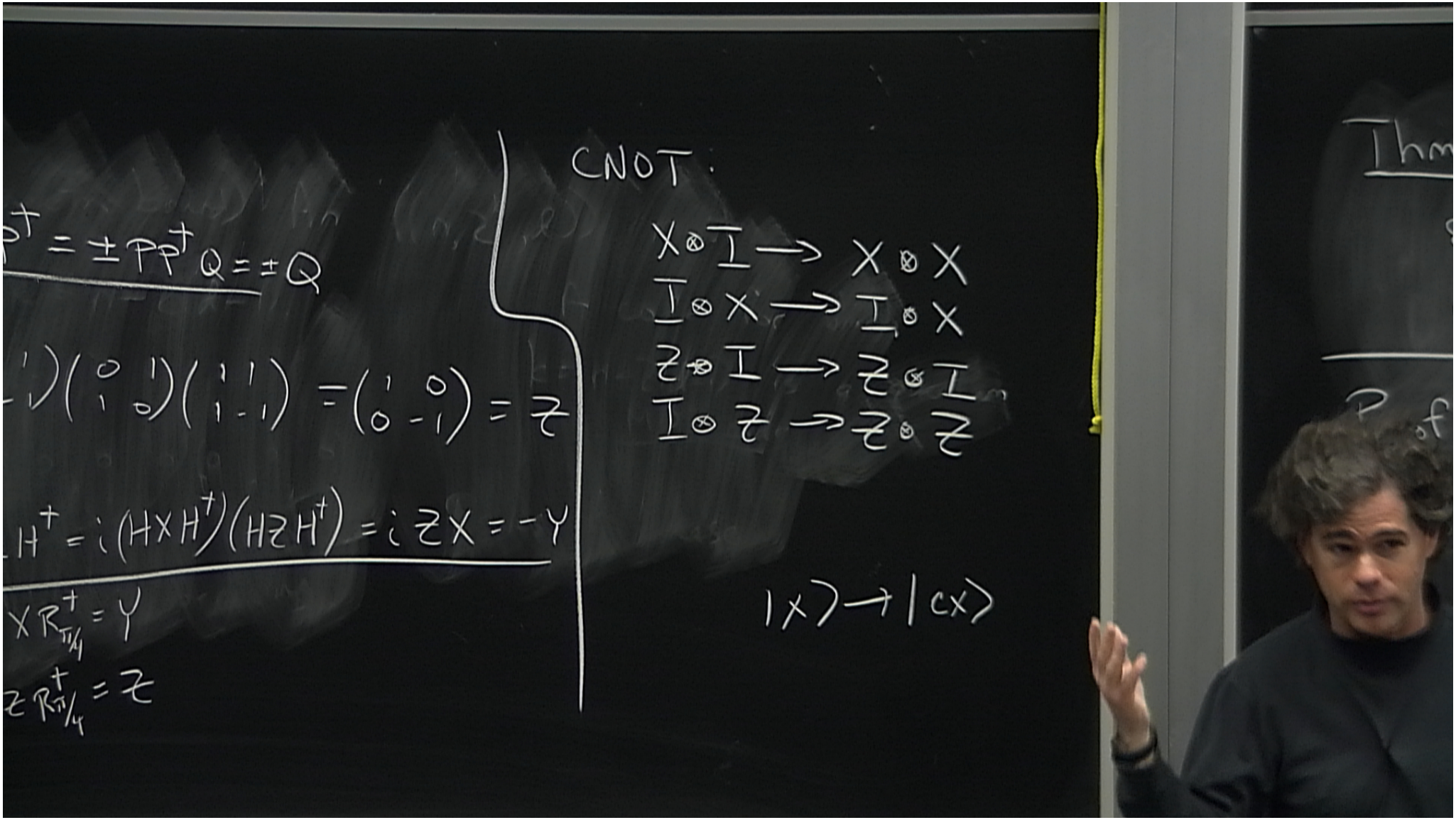
$(\langle 10\ldots0|U^\dagger)(U|0\ldots0\rangle) = \langle 0\ldots0|U^\dagger f(X_1 X_2)(U|0\ldots0\rangle) = 0$

$f(Z_2)^\dagger \quad f(Z_1)$


Thm: $C_n/\{e^{i\phi}\}P_n = S_p(2n, \mathbb{Z}_2)$
Proof: Claim U & U' act the same on binary vectors
iff $U' = e^{i\phi}UP$, $P \in P_n$
$\Leftarrow$


Thm: $C_n/\{e^{i\phi}\}P_n = S_p(2n, \mathbb{Z}_2)$
Proof: Claim U & U' act the same on binary vectors
iff $U' = e^{i\phi}UP$, $P \in P_n$
$\Leftarrow$: ✓
$\Rightarrow$: $U'U^\dagger = V$ act trivially on binary vectors
$P \to \pm P$
$Z_i \to \pm Z_i$
$X_i \to \pm X_i$
$V|0\ldots0\rangle = |b\rangle$
$V|10\ldots0\rangle = \pm X_i|b\rangle$
$|x\rangle \to (-1)^{c\cdot x}|b+x\rangle = \prod_i X_i^{b_i} Z_i^{c_i}|x\rangle$
$Z_i \to (-1)^{b_i} Z_i$
$X_i \to (-1)^{c_i} X_i$


Thm: $C_n/\{e^{i\phi}\}P_n = S_p(2n, \mathbb{Z}_2)$
Proof: Claim U & U' act the same on binary vectors
iff $U' = e^{i\phi}UP$, $P \in P_n$
$\Leftarrow$: ✓
$\Rightarrow$: $U'U^\dagger = V$ act trivially on binary vectors
$P \to \pm P$
$Z_i \to \pm Z_i$
$X_i \to \pm X_i$
$V|0\ldots0\rangle = |b\rangle$
$V|10\ldots0\rangle = \pm X_i|b\rangle$
$|x\rangle \to (-1)^{c\cdot x}|b+x\rangle = \prod X_i^{b_i} Z_i^{c_i}|x\rangle$
$\in P_n$
$Z_i \to (-1)^{b_i} Z_i$
$X_i \to (-1)^{c_i} X_i$


CNOT:
X⊗I → X⊗X
I⊗X → I⊗X
Z⊗I → Z⊗I
I⊗Z → Z⊗Z
|x⟩ → |cx⟩
Thm