Title: Quantum Error Correction 5B

Date: Feb 06, 2007 05:00 PM

URL: http://pirsa.org/07020018

Abstract: Weight enumerators, quantum MacWilliams identity, quantum shadow enumerator, higher-dimensional Pauli group, stabilizer codes for qudits

Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j$$

A_j = # elements of wt j in S

Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j$$

A_j = # elements of wt j in S

The dual enumerator is

$$B(x) = \sum_{j=0}^{n} B_j x^j$$

B_j = # elements of wt j in $N(S)$.

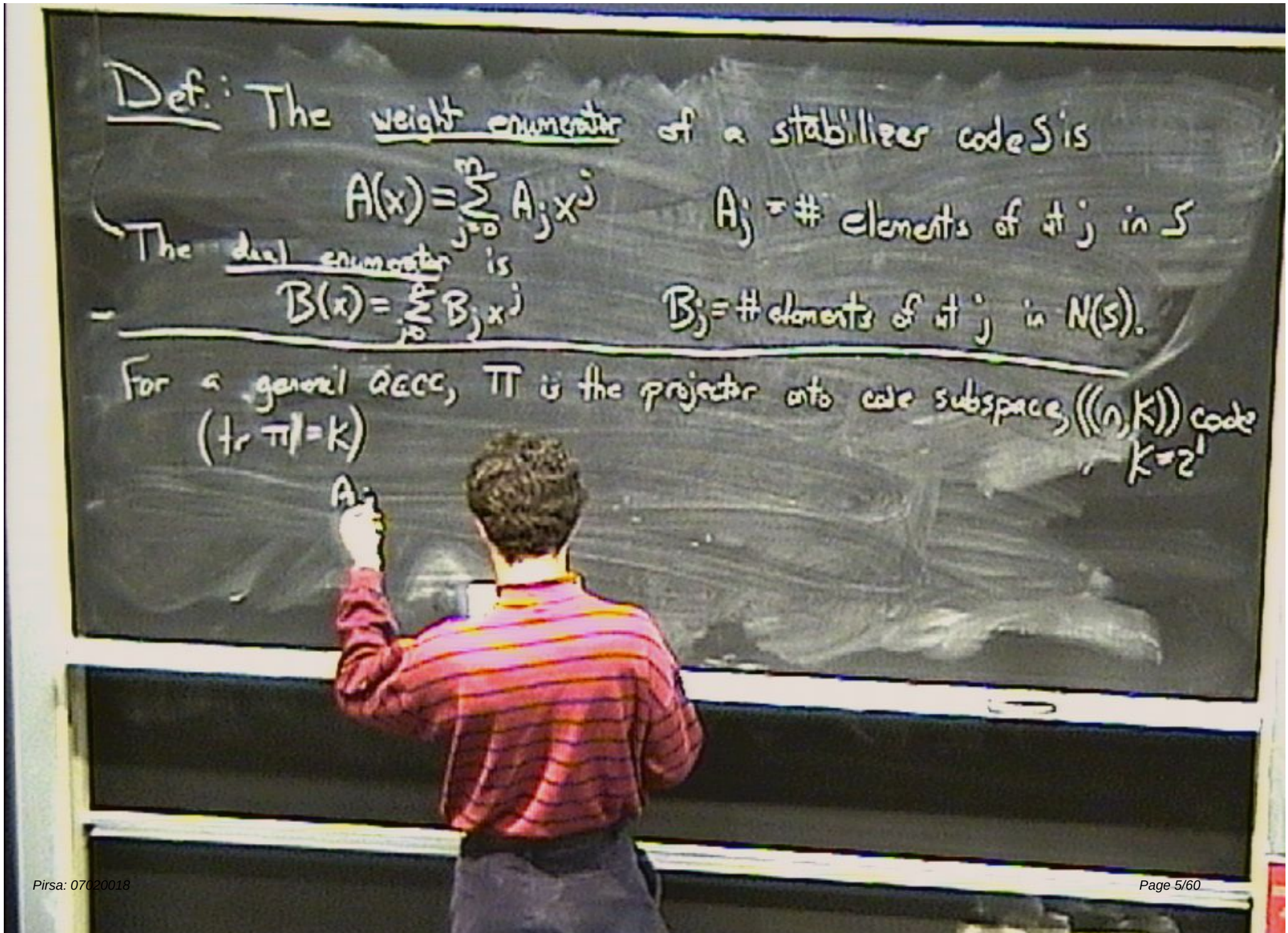
Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j \qquad A_j = \#\text{ elements of wt } j \text{ in } S$$

The dual enumerator is

$$B(x) = \sum_{j=0}^{n} B_j x^j \qquad B_j = \#\text{ elements of wt } j \text{ in } N(S).$$

For a general QECC, Π is the projector onto code subspace, $((n,K))$ code, $K = 2^k$


Def: The weight enumerator of a stabilizer code S is
$A(x) = \sum_{j=0}^{n} A_j x^j$
A_j = # elements of wt j in S
The dual enumerator is
$B(x) = \sum_{j=0}^{n} B_j x^j$
B_j = # elements of wt j in N(S).
For a general QECC, Π is the projector onto code subspace, ((n,K)) code
$(\mathrm{tr}\,\Pi = K)$
$K = 2^l$
A_i

Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j \qquad A_j = \#\text{ elements of wt } j \text{ in } S$$

The dual enumerator is

$$B(x) = \sum_{j=0}^{n} B_j x^j \qquad B_j = \#\text{ elements of wt } j \text{ in } N(S).$$

For a general QECC, Π is the projector onto code subspace, $((n,K))$ code, $K = 2^l$ $(\mathrm{tr}\,\Pi = K)$

$$A_j = \frac{1}{K^2} \sum \left[\mathrm{tr}(P\Pi)\right]^2 \qquad \overline{P_n} = P_n / \{\pm 1, \pm i\}$$

Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j \qquad A_j = \#\text{ elements of wt } j \text{ in } S$$

The dual enumerator is

$$B(x) = \sum_{j=0}^{n} B_j x^j \qquad B_j = \#\text{ elements of wt } j \text{ in } N(S).$$

For a general QECC, Π is the projector onto code subspace, $((n,K))$ code, $K = 2^l$ $(\mathrm{tr}\,\Pi = K)$

$$A_j = \frac{1}{K^2} \sum_{P \in \overline{P}_n,\ \mathrm{wt}\,P = j} \left[\mathrm{tr}\,(P\Pi)\right]^2 \qquad \overline{P}_n = P_n / \{\pm 1, \pm i\}$$

Def: The weight enumerator of a stabilizer code S is

$$A(x) = \sum_{j=0}^{n} A_j x^j \qquad A_j = \#\text{ elements of wt } j \text{ in } S$$

The dual enumerator is

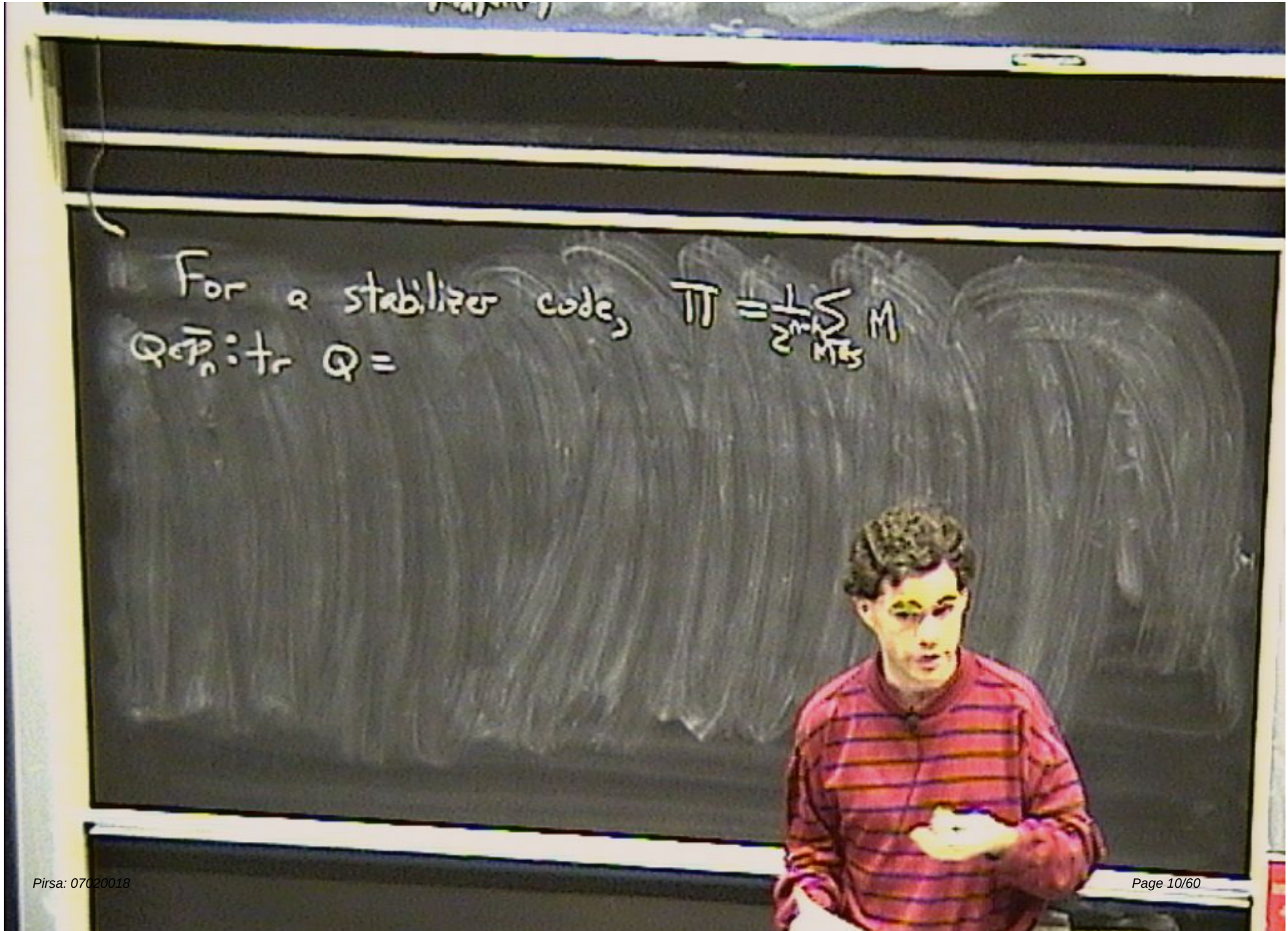
$$B(x) = \sum_{j=0}^{n} B_j x^j \qquad B_j = \#\text{ elements of wt } j \text{ in } N(S).$$

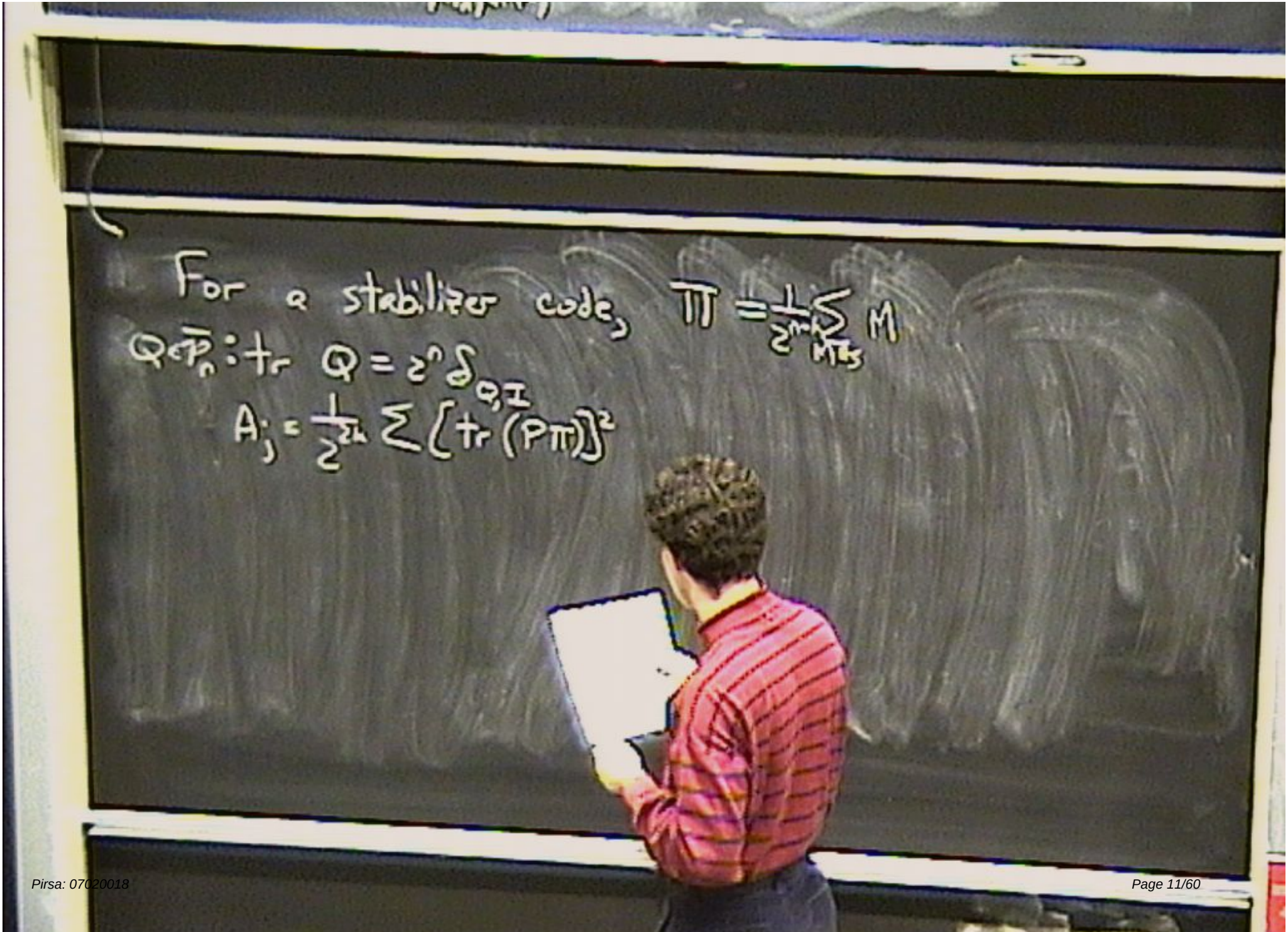
For a general QECC, Π is the projector onto code subspace, $((n,K))$ code, $K = 2^l$ $(\mathrm{tr}\,\Pi = K)$

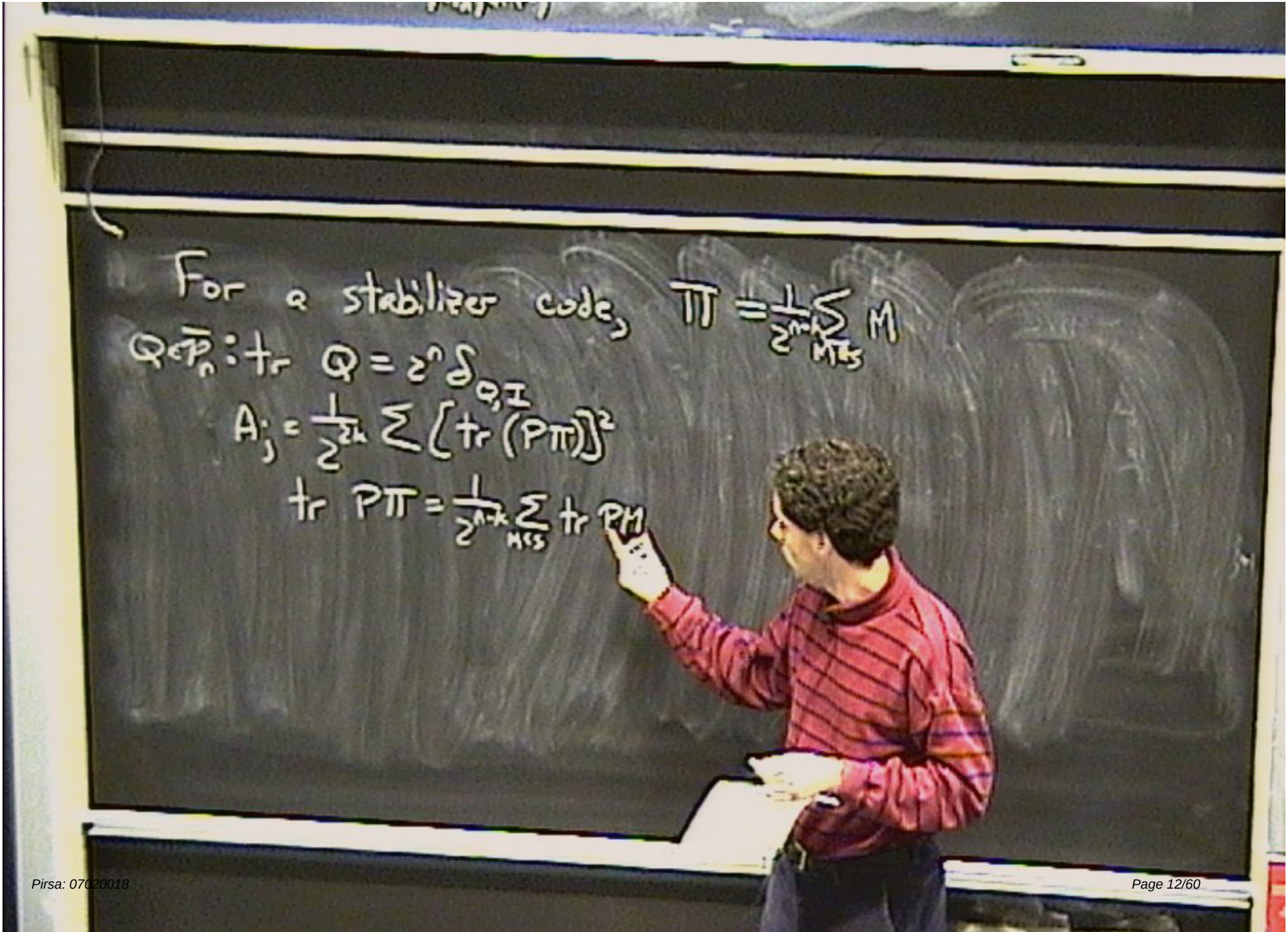
$$A_j = \frac{1}{K^2} \sum_{P \in P_n,\ \mathrm{wt}\, P = j} [\mathrm{tr}(P\Pi)]^2 \qquad \overline{P_n} = P_n / \{\pm 1, \pm i\}$$

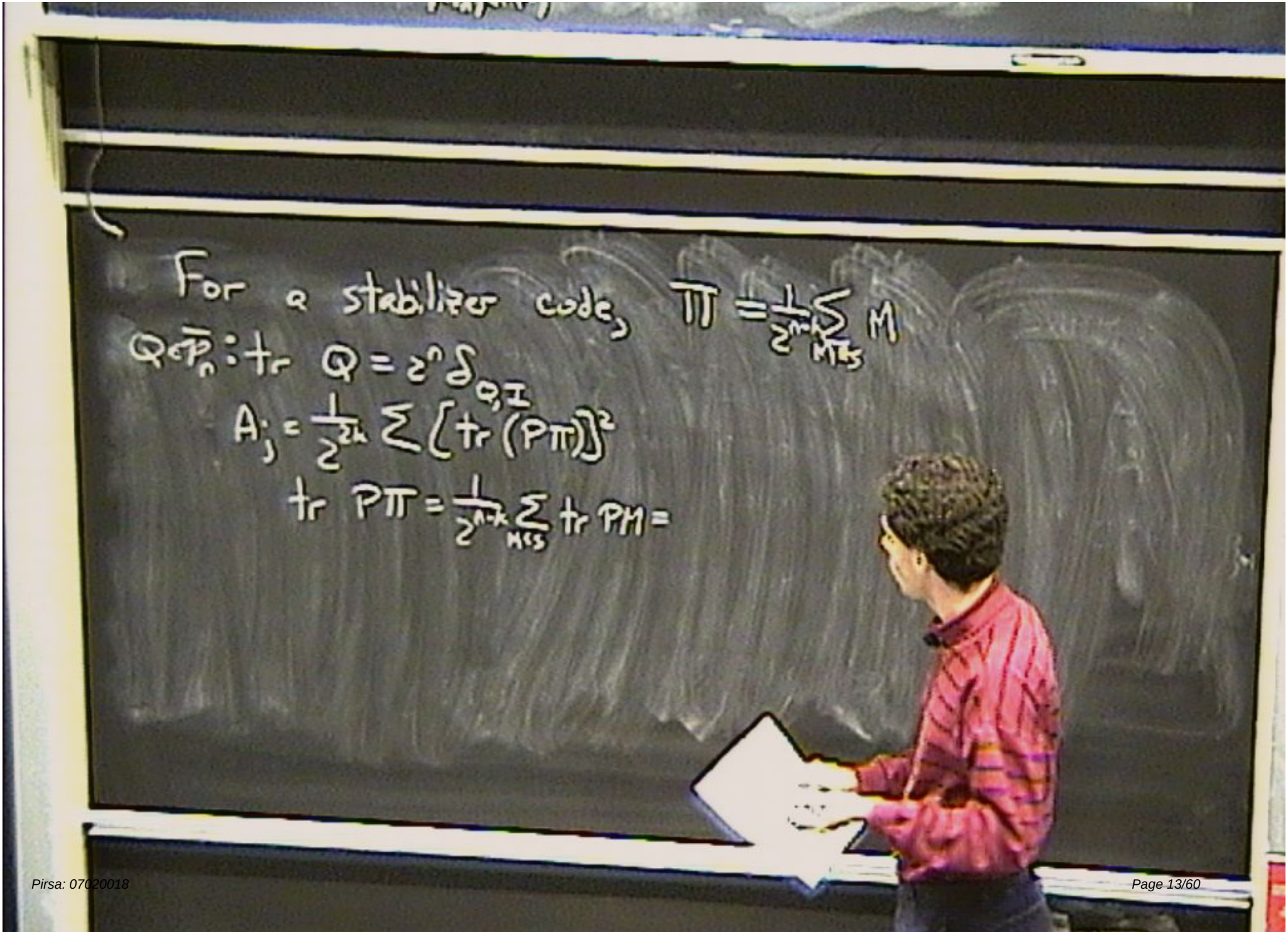
$$B_j = \frac{1}{K} \sum_{P \in P_n,\ \mathrm{wt}\, P = j} \mathrm{tr}(P\Pi P\Pi)$$

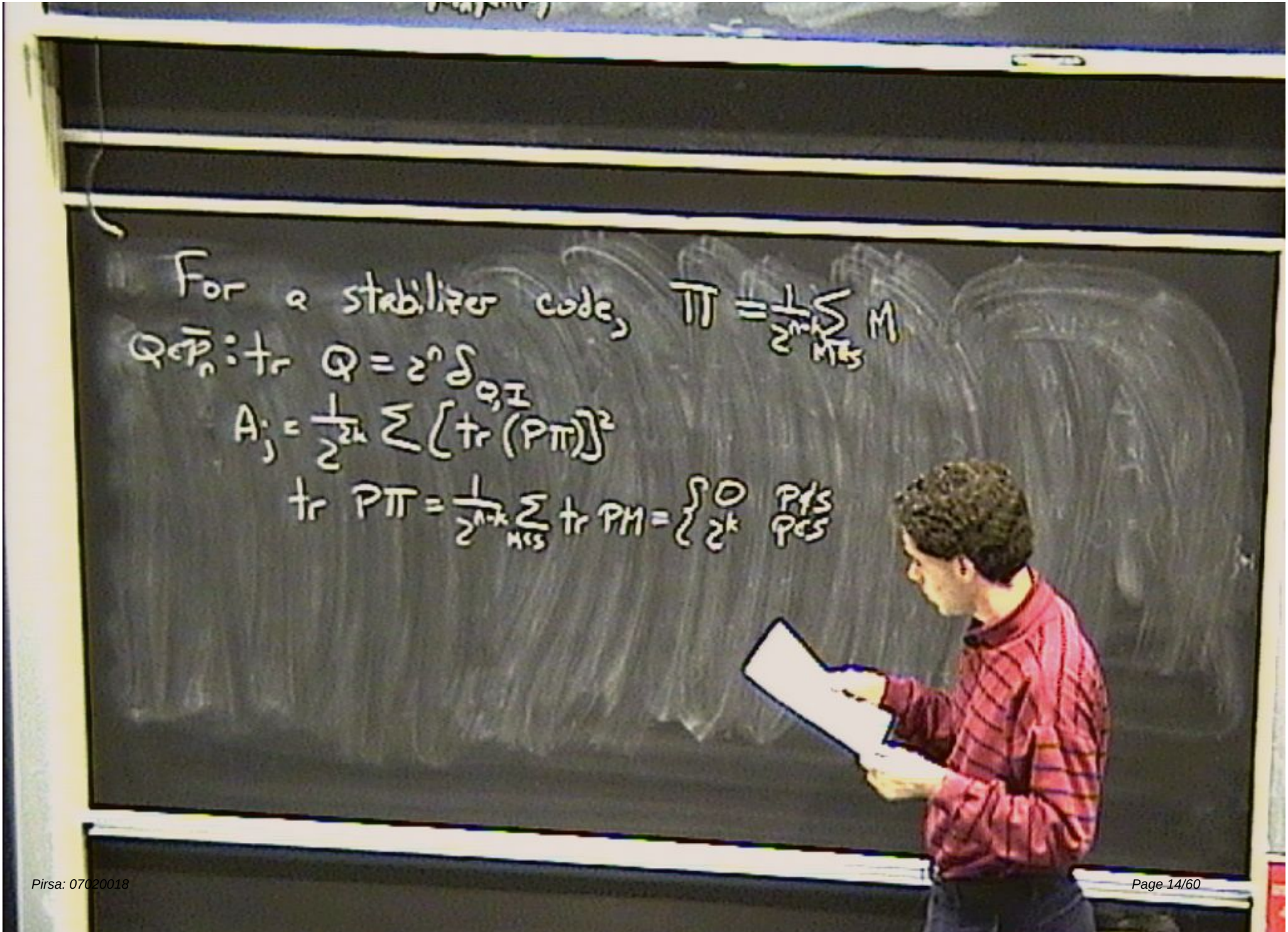
For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \overline{P}_n$: $tr\ Q =$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \bar{P}_n : \mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2n}} \sum [\mathrm{tr}(P\Pi)]^2$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \overline{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2$
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2$
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM =$

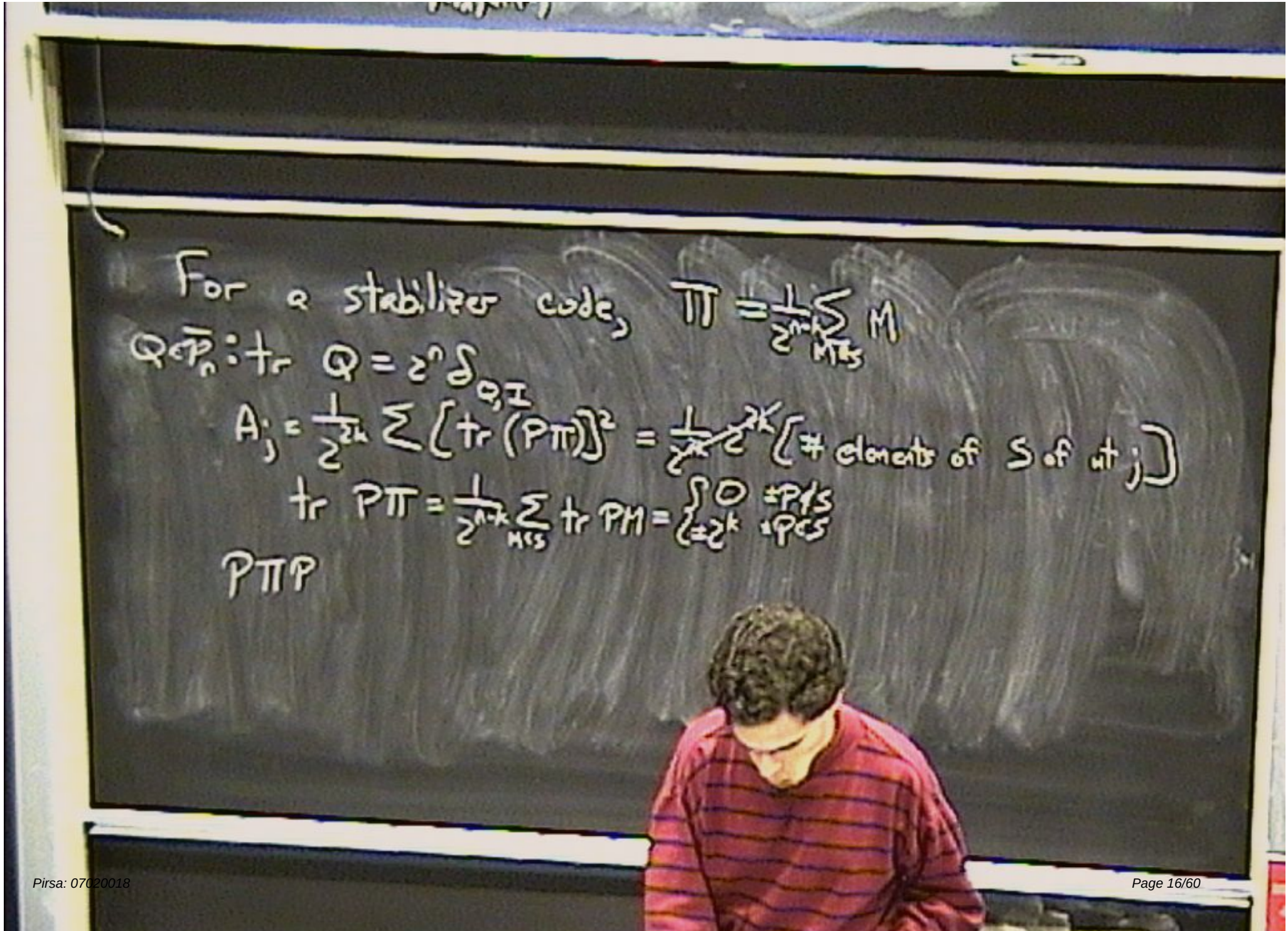

For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \overline{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2$
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & P \notin S \\ 2^k & P \in S \end{cases}$

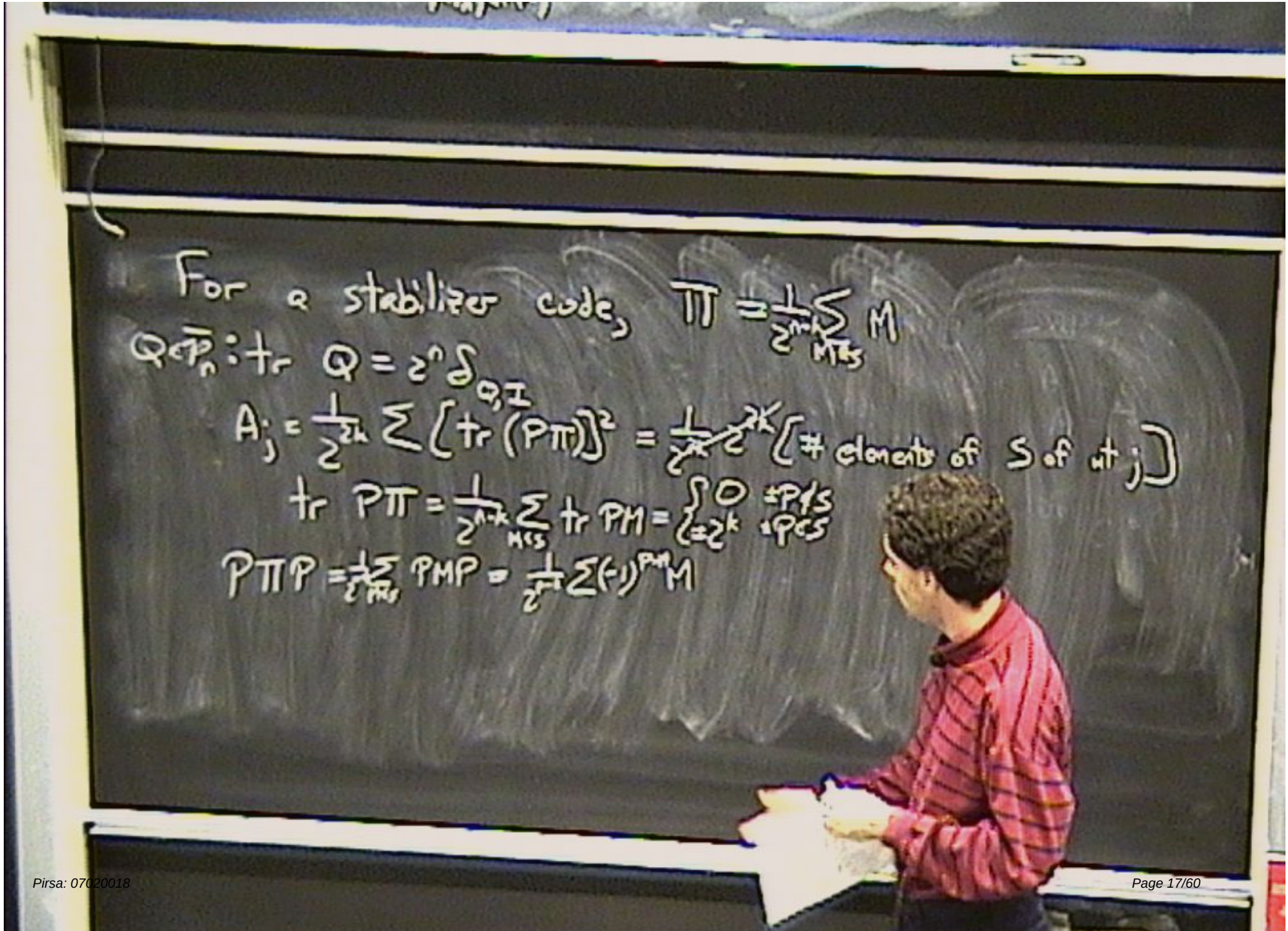
For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$

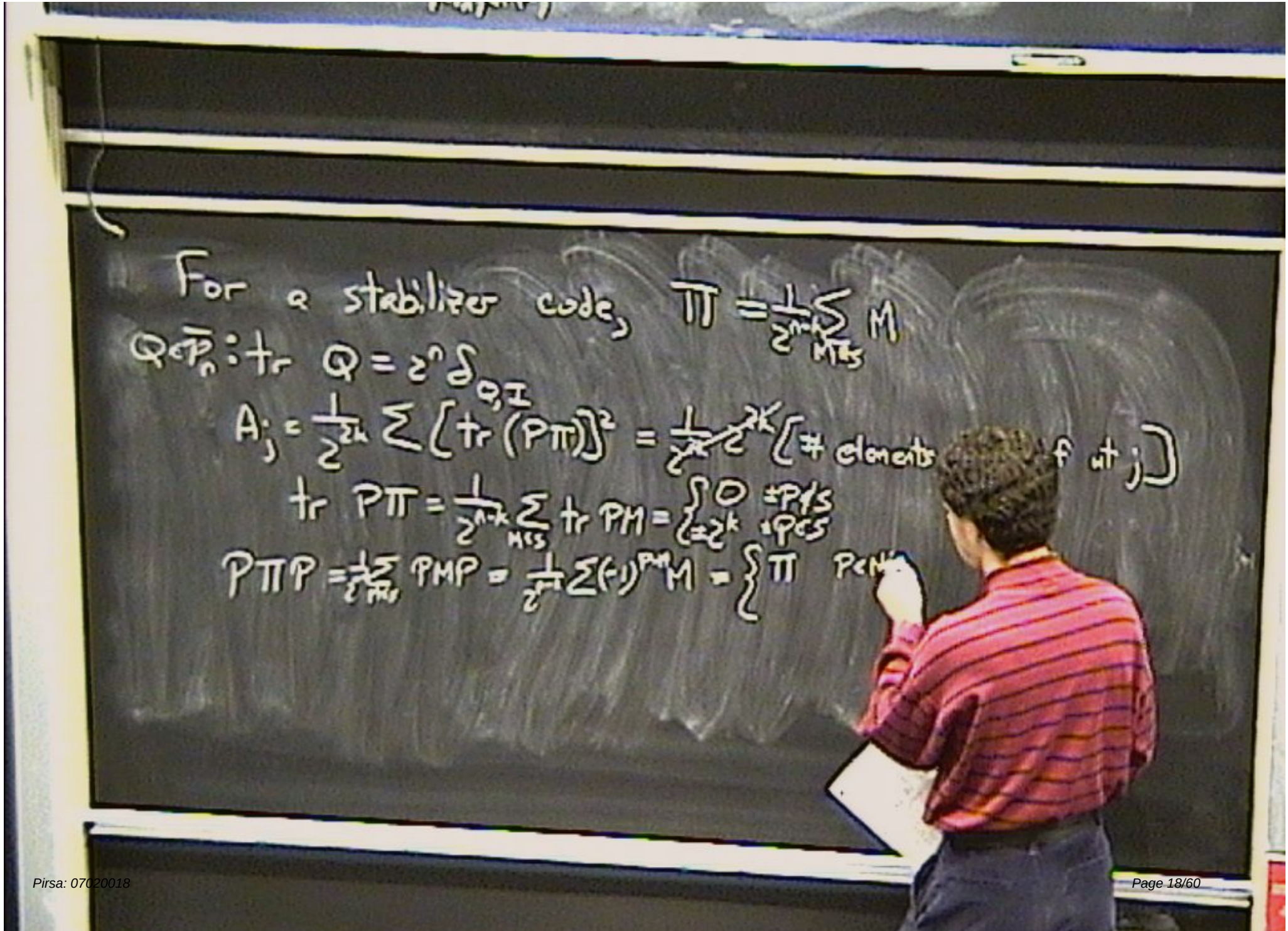
$Q \in \overline{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$

$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2 = \frac{1}{2^{2k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$

$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum [\mathrm{tr}(P\Pi)]^2 = \frac{1}{2^{2k}} 2^{2k} [\#\text{ elements of } S \text{ of wt } j]$
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \text{if } P \notin S \\ \pm 2^k & \text{if } P \in S \end{cases}$
$P\Pi P$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}(P\Pi)\right]^2 = \frac{1}{2^{n-k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$
$P\Pi P = \frac{1}{2^{n-k}} \sum_{PMP = \pm M} PMP = \frac{1}{2^{n-k}} \sum (-1)^{P,M} M$


For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$
$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$
$A_j = \frac{1}{2^{2k}} \sum [\mathrm{tr}(P\Pi)]^2 = \frac{1}{2^{2k}} 2^{2k} [\#$ elements
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$
$P\Pi P = \frac{1}{2^{n-k}} \sum_{M \in S} PMP = \frac{1}{2^{n-k}} \sum (-1)^{PM} M = \begin{cases} \Pi & P \in$

For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$

$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$

$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2 = \frac{1}{2^{2k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$

$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$

$P\Pi P = \frac{1}{2^{n-k}} \sum_{PM} PMP = \frac{1}{2^{n-k}} \sum (-1)^{PM} M = \begin{cases} \Pi & P \in N(G) \end{cases}$

For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$

$Q \in \overline{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$

$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}\,(P\Pi)\right]^2 = \frac{1}{2^{2k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$

$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & P \notin S \\ \pm 2^k & P \in S \end{cases}$

$P\Pi P = \frac{1}{2^{n-k}} \sum_{M \in S} PMP = \frac{1}{2^{n-k}} \sum (-1)^{P \# M} M = \begin{cases} \Pi & P \in N(G) \\ \Pi_- & P \notin N(G) \end{cases}$ $\qquad \Pi_- \Pi = 0$

For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$

$Q \in \bar{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$

$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}(P\Pi)\right]^2 = \frac{1}{2^{2k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$

$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$

$P\Pi P = \frac{1}{2^{n-k}} \sum_{M \in S} PMP = \frac{1}{2^{n-k}} \sum (-1)^{P,M} M = \begin{cases} \Pi & P \in N(G) \\ \Pi_- & P \notin N(G) \end{cases}$ $\qquad \Pi_- \Pi = 0$

$\mathrm{tr}\, P\Pi P\Pi = \begin{cases} 2^k & P \in N(G) \\ 0 & P \notin N(G) \end{cases}$

$B_j = \frac{1}{2^k} \sum \mathrm{tr}(P\Pi P\Pi) = \#\text{ elements of } N(S) \text{ of wt } j$

For a stabilizer code, $\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} M$

$Q \in \overline{P}_n$: $\mathrm{tr}\, Q = 2^n \delta_{Q,I}$

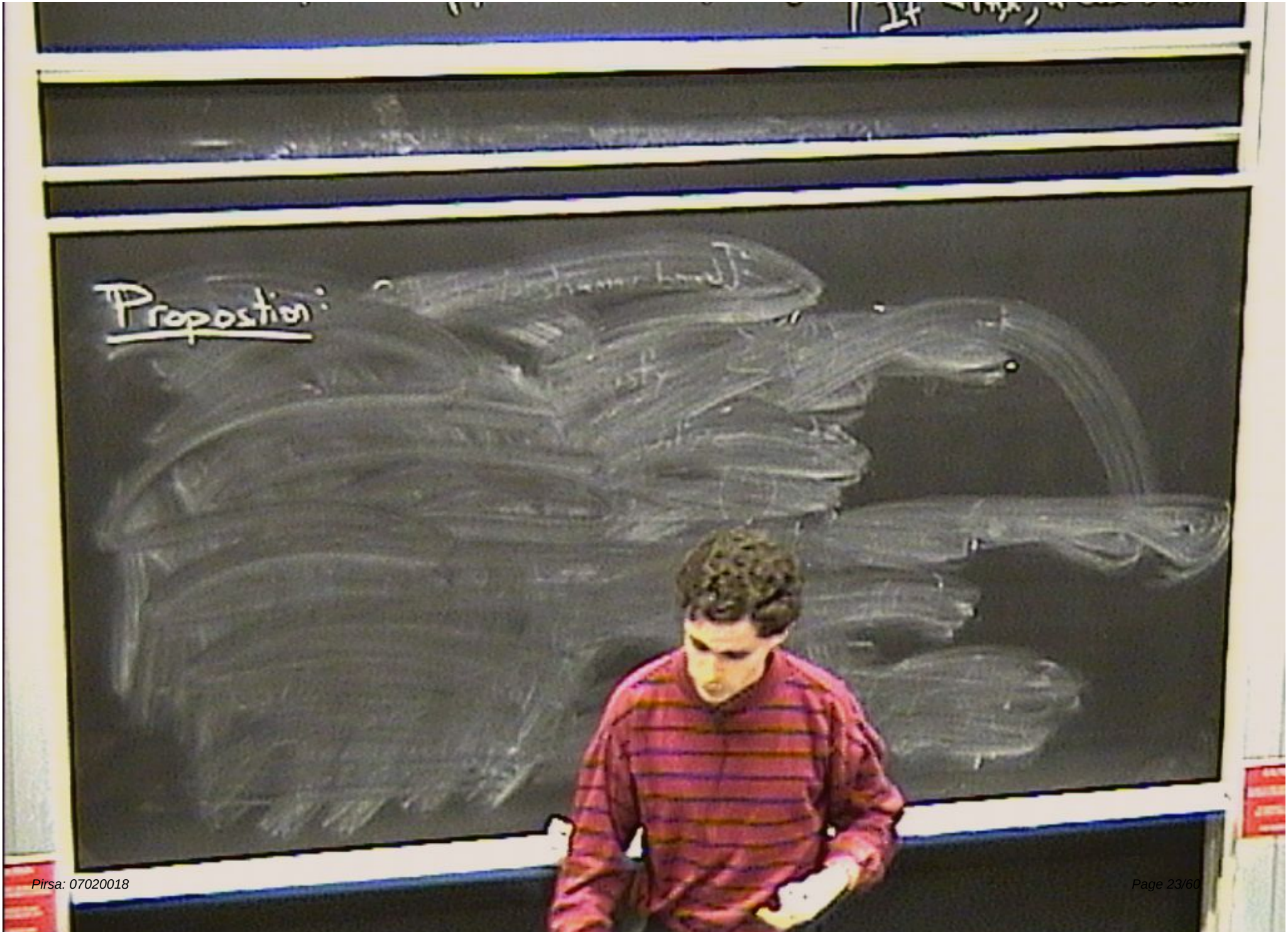
$A_j = \frac{1}{2^{2k}} \sum \left[\mathrm{tr}(P\Pi)\right]^2 = \frac{1}{2^{2k}} 2^{2k} \left[\#\text{ elements of } S \text{ of wt } j\right]$

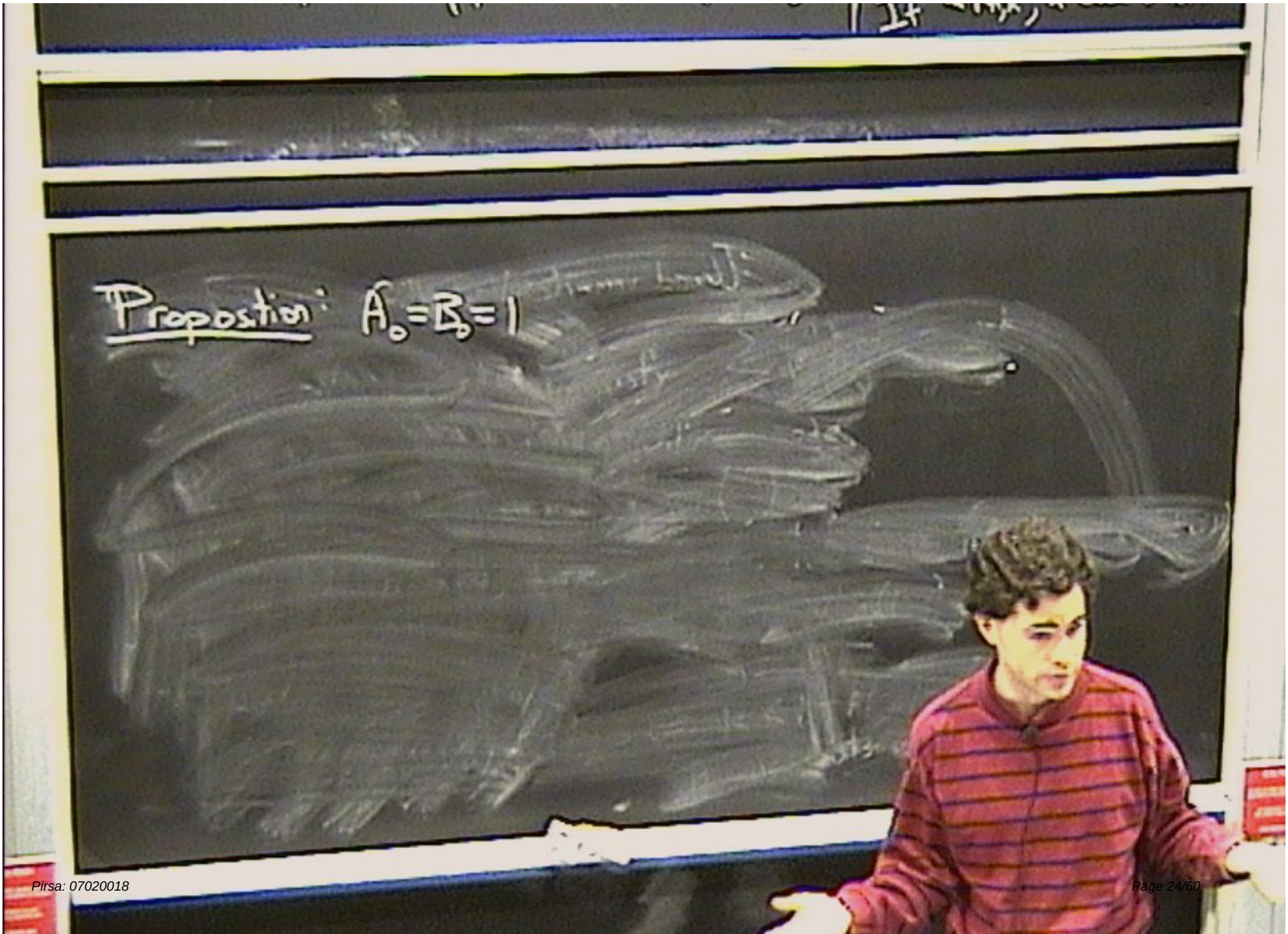
$\mathrm{tr}\, P\Pi = \frac{1}{2^{n-k}} \sum_{M \in S} \mathrm{tr}\, PM = \begin{cases} 0 & \pm P \notin S \\ \pm 2^k & \pm P \in S \end{cases}$

$P\Pi P = \frac{1}{2^{n-k}} \sum_{M \in S} PMP = \frac{1}{2^{n-k}} \sum (-1)^{PM} M = \begin{cases} \Pi & P \in N(G) \\ \Pi_- & P \notin N(G) \end{cases}$ $\qquad \Pi_- \Pi = 0$

$\mathrm{tr}\, P\Pi P\Pi = \begin{cases} 2^k & P \in N(G) \\ 0 & P \notin N(G) \end{cases}$

$B_j = \frac{1}{2^k} \sum \mathrm{tr}(P\Pi P\Pi) = \#\text{ elements of } N(S) \text{ of wt } j$


Proposition:


Proposition: $A_0 = B_0 = 1$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate.

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate. degenerate $\Rightarrow$ impure

Thm. [quantum MacWilliams identity]: $B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate. degenerate $\Rightarrow$ impure

Thm. [quantum MacWilliams identity]: $B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate. degenerate $\Rightarrow$ impure

Thm. [quantum MacWilliams identity]: $B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate.

degenerate $\Rightarrow$ impure

Thm. [quantum MacWilliams identity]: $B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$

Def: The quantum shadow enumerator is $Sh(x) = \sum_j Sh_j x^j$

$Sh_j =$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate.

Thm. [quantum MacWilliams identity]: degenerate $\Rightarrow$ impure

$$B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$$

Def: The quantum shadow enumerator is $Sh(x) = \sum_{j=0}^{n} Sh_j x^j$ with

$$Sh_j = \frac{1}{K} \sum_{P \in \pi_{n,j}} \mathrm{tr}\left(P \Pi P Y^{\otimes n} \bar{\Pi} Y^{\otimes n}\right)$$

($\bar{\Pi}$ = complex conjugate of Π)

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def: A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate. degenerate $\Rightarrow$ impure

Thm. [quantum MacWilliams identity]: $\boxed{B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)}$

Def: The quantum shadow enumerator is $S_h(x) = \sum_{j=0}^{n} S_j x^j$ with

$$S_j = \frac{1}{K} \sum_{P \in \pi(n,d,n_j)} \operatorname{tr}\left(P \Pi P Y^{\otimes n} \bar{\Pi} Y^{\otimes n}\right) \qquad (\bar{\Pi} = \text{complex conjugate of } \Pi)$$

Thm: $S_j \geq 0$. $S_h(x) = \frac{K}{2^n}(1+3x) A\left(\frac{x-1}{1+3x}\right)$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

Note: impure $\neq$ degenerate.

Thm. [quantum MacWilliams identity]: degenerate $\Rightarrow$ impure

$$B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)$$

Def: The quantum shadow enumerator is $Sh(x) = \sum_{j=0}^{n} Sh_j x^j$ with

$$Sh_j = \frac{1}{K} \sum_{P \in \text{supp}_j} \operatorname{tr}\left(P \Pi P Y^{\otimes n} \bar{\Pi} Y^{\otimes n}\right) \qquad (\bar{\Pi} = \text{complex conjugate of } \Pi)$$

Thm: $Sh_j \geq 0$.

$$Sh(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{x-1}{1+3x}\right)$$

Proposition: $A_0 = B_0 = 1$, $B_j \geq A_j \geq 0$. A QECC of distance d has $A_j = B_j$ $j < d$.

Def. A code with $A_j = B_j = 0$ for $j < d$ is called pure; otherwise it is impure.

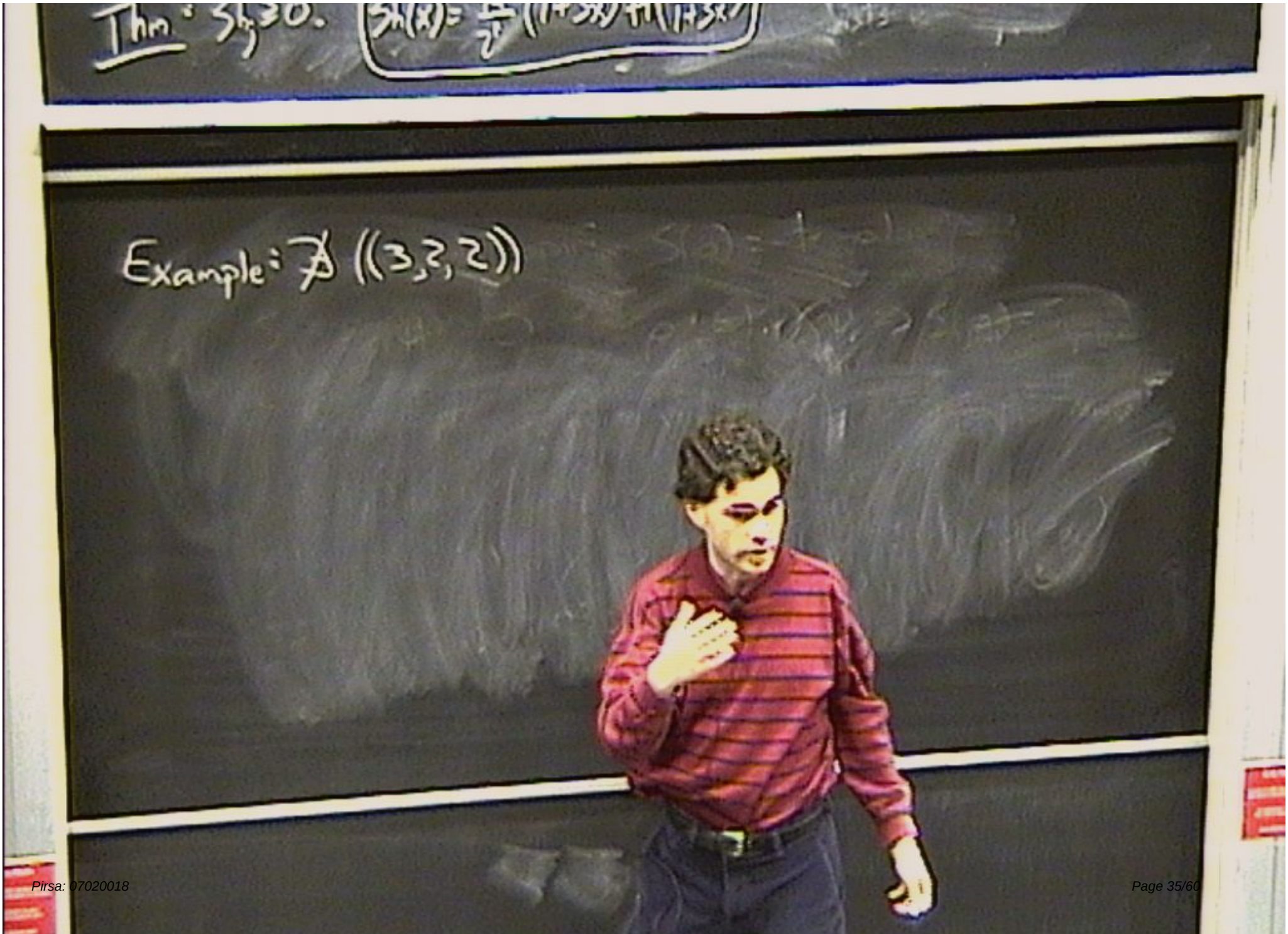
Note: impure $\neq$ degenerate. degenerate $\Rightarrow$ impure

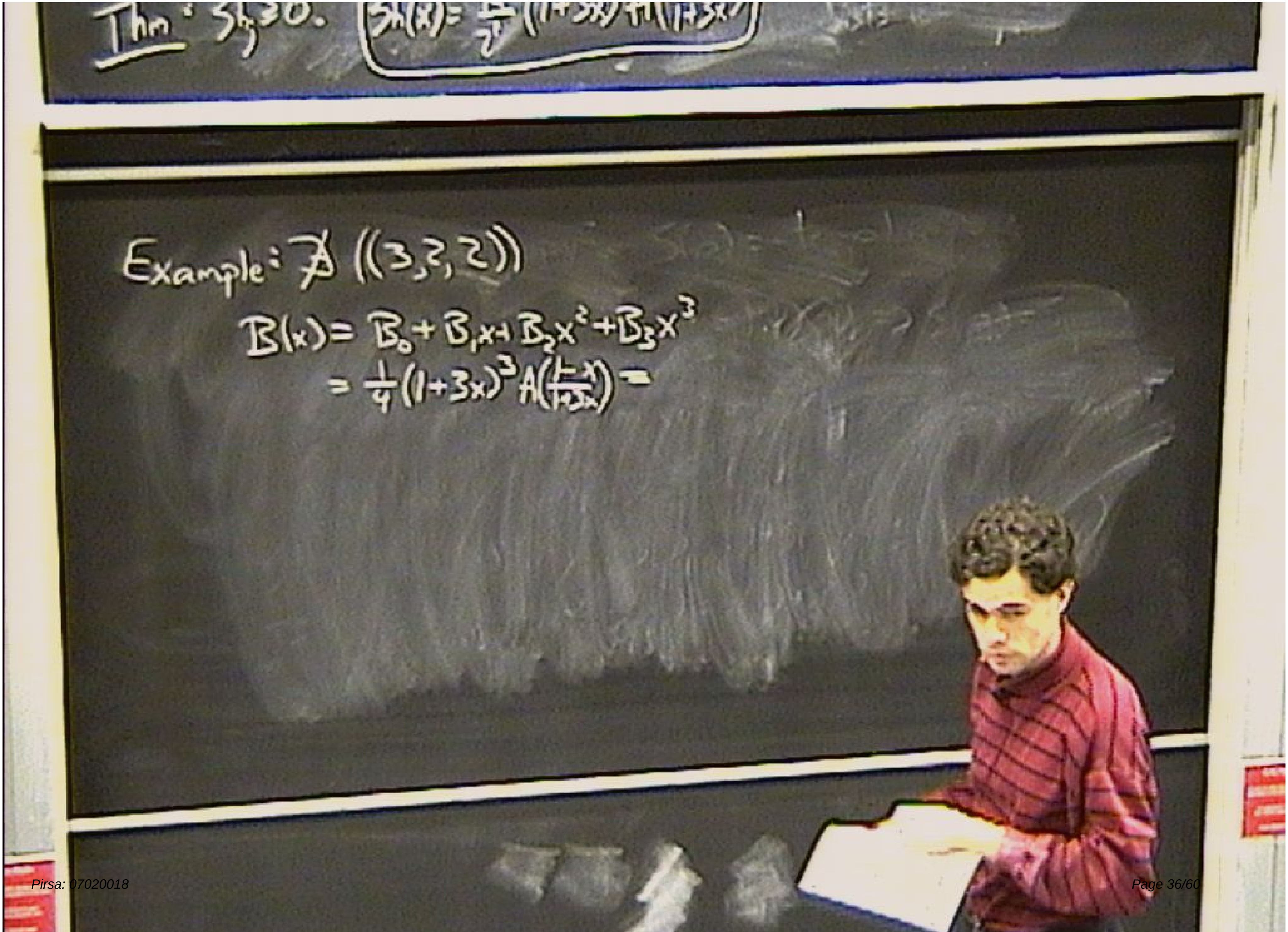
Thm. [quantum MacWilliams identity]: $\boxed{B(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{1-x}{1+3x}\right)}$

Def: The quantum shadow enumerator is $Sh_j = \frac{1}{K} \sum_{\text{wt } E = j} \text{tr}(P \Pi P Y^{a_1} \Pi^* Y^{a_2})$ $(\Pi^*$ complex conjugate of $\Pi)$

$Sh(x) = \sum_{j=0}^{n} Sh_j x^j$ with

Thm: $Sh_j \geq 0$. $\boxed{Sh(x) = \frac{K}{2^n}(1+3x)^n A\left(\frac{x-1}{1+3x}\right)}$


Thm: 5.3.30.
Example: $\mathcal{B}((3,3,2))$


Thm: $S_k \geq 0$.
Example: ∄ ((3,2,2))
$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$
$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) =$

Thm: $S_{n,3}$ ⊃.

Example: $\mathcal{B}((3,2,2))$

$$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$$

$$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) = \frac{1}{4}\left[(1+3x)^3 A_0 + (1+3x)^2(1-x)A_1 + (1+3x)(1-x)^2 A_2 + (1-x)^3 A_3\right]$$

$$4B_0 =$$

Thm: $S_{4,3}(0)$. $S_n(x) = \frac{1}{2^n}((1+3x)^n + (1-x)^n)$

Example: $\mathcal{B}((3,2,2))$

$$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$$

$$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) = \frac{1}{4}\left[(1+3x)^3 A_0 + (1+3x)^2(1-x)A_1 + (1+3x)(1-x)^2 A_2 + (1-x)^3 A_3\right]$$

$B_0 = 1$ $\quad A_0 = 1$

$$4 = 4B_0 = 1 + A_1 + A_2 + A_3$$

$$4B_1 = 9 + 5A_1 + A_2 - 3A_3$$

$$4B_2 = 27 + 3A_1 - 5A_2 + 3A_3$$

$$4B_3 = 27 - 9A_1 + 3A_2 - A_3$$

Thm: $S_n \geq 0$. $\mathcal{B}_n(x) = \frac{1}{2^n}((1+3x)^n + (1-x)^n)$

Example: $\mathcal{B}((3,2,2))$

$$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$$

$$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) = \frac{1}{4}\left[(1+3x)^3 A_0 + (1+3x)^2(1-x)A_1 + (1+3x)(1-x)^2 A_2 + (1-x)^3 A_3\right]$$

$A_0 = 1$, $B_0 = 1$

$$4 = 4B_0 = 1 + A_1 + A_2 + A_3 \Rightarrow A_1 + A_2 + A_3 = 3$$

$$4B_1 = 9 + 5A_1 + A_2 - 3A_3 \Rightarrow A_1 + A_2 - 3A_3 = -9$$

$$4B_2 = 27 + 3A_1 - 5A_2 + 3A_3 \Rightarrow 3A_1 - 9A_2 + 3A_3 = -27 \checkmark$$

$$4B_3 = 27 - 9A_1 + 3A_2 - A_3 \Rightarrow -9A_1 + 3A_2 - 5A_3 = -27 \checkmark$$

$A_3 = 3$

$A_1 = A_2 = 0$

$A(x) = 1 + 3x^3$

Thm. (quantum Hamming bou[redacted],2^k, d)) non-degenerate code must satisfy $\left[\sum_{j=0}^{t}\binom{n}{j}3^j\right]2^k \le 2^n$ $(d=2t+1)$

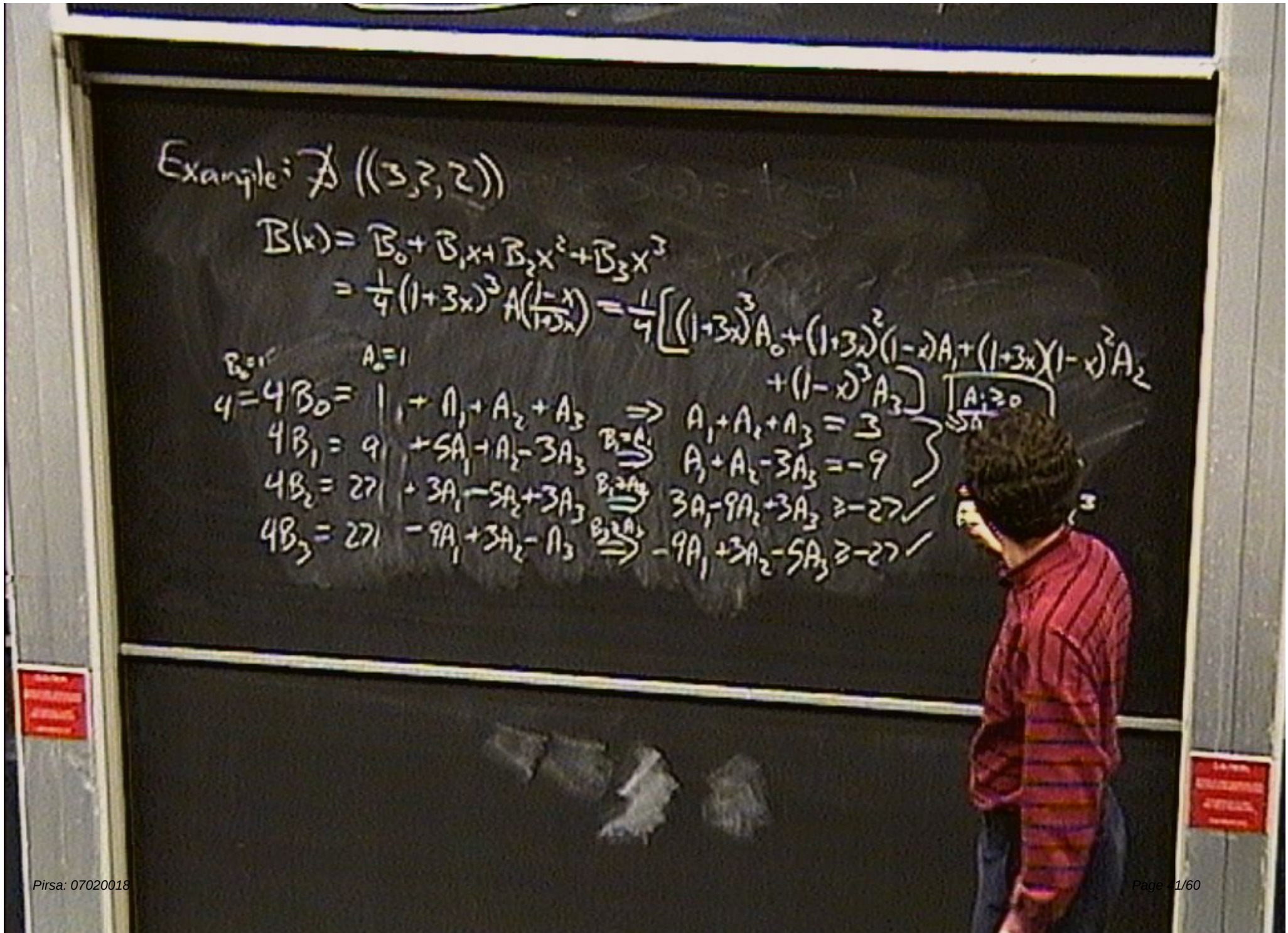
Proof: For a non-degenerate code, different errors produce linearly independent states $\Rightarrow$ (# errors)(# basis codewords) $\le$ dim. Hilbert space.

Asymptotic limit: $\frac{t}{n}=p$ $R<1-h(p)-p\log 3$

Thm. [quantum Singleton bound (Knill-Laflamme bound)]: $n-k \ge 2(d-1)$ (Note: this applies to non-binary registers)

Note: Saturated by $[[5,1,3]]$ and $[[4,2,2]]$ ($\in [[2n, 2n-2, 2]]$)

Apply shadow enumerator


Example: $\mathcal{A}((3,2,2))$
$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$
$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) = \frac{1}{4}\left[(1+3x)^3 A_0 + (1+3x)^2(1-x)A_1 + (1+3x)(1-x)^2 A_2 + (1-x)^3 A_3\right]$
$B_0=1$ $A_0=1$
$4 = 4B_0 = 1 + A_1 + A_2 + A_3 \Rightarrow A_1 + A_2 + A_3 = 3$
$4B_1 = 9 + 5A_1 + A_2 - 3A_3 \Rightarrow A_1 + A_2 - 3A_3 = -9$
$4B_2 = 27 + 3A_1 - 5A_2 + 3A_3 \Rightarrow 3A_1 - 9A_2 + 3A_3 \geq -27$
$4B_3 = 27 - 9A_1 + 3A_2 - A_3 \Rightarrow -9A_1 + 3A_2 - 5A_3 \geq -27$
$A_i \geq 0$

Example: $\mathcal{B}((3,2,2))$

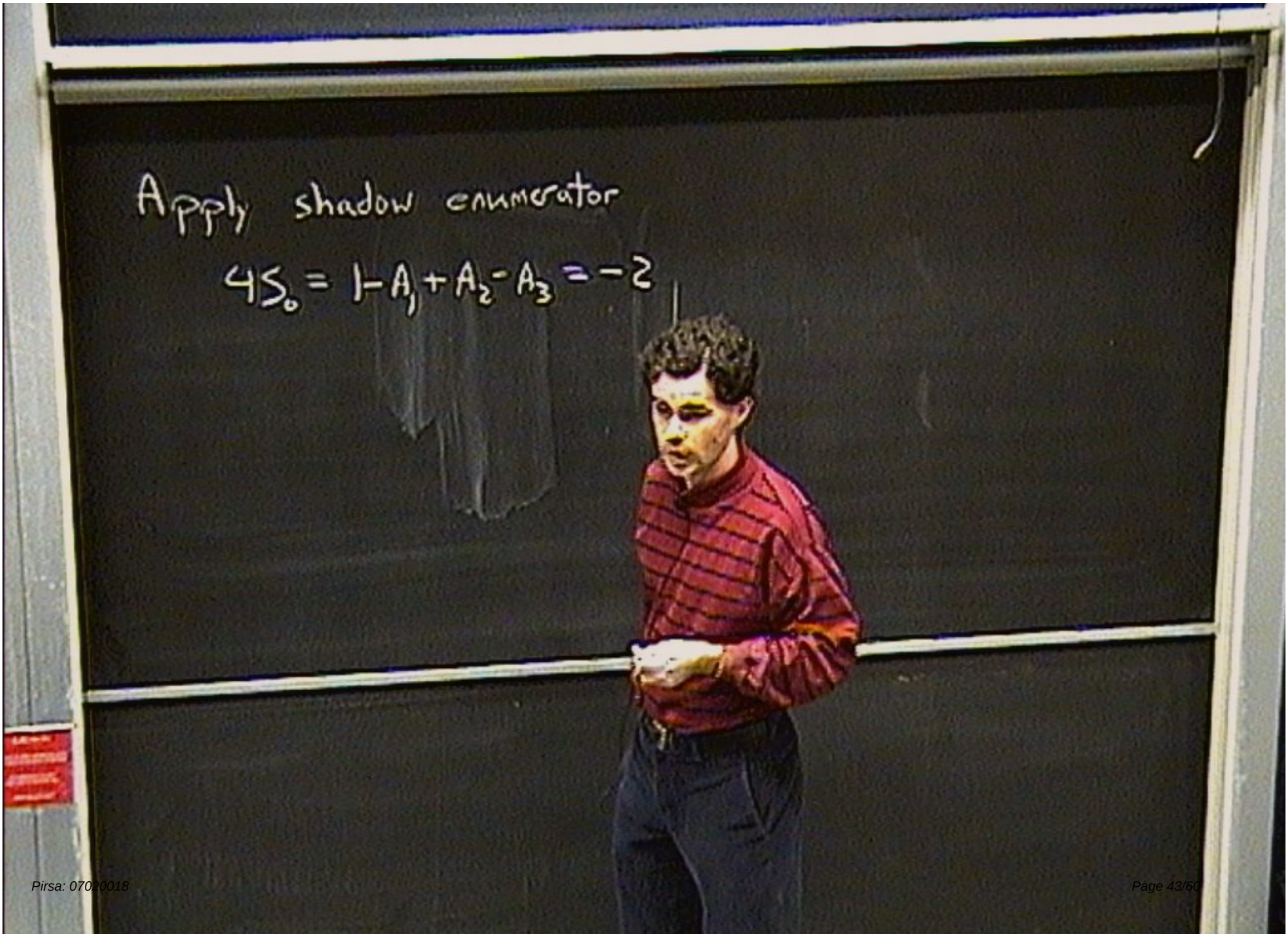
$$B(x) = B_0 + B_1 x + B_2 x^2 + B_3 x^3$$
$$= \frac{1}{4}(1+3x)^3 A\left(\frac{1-x}{1+3x}\right) = \frac{1}{4}\Big[(1+3x)^3 A_0 + (1+3x)^2(1-x)A_1 + (1+3x)(1-x)^2 A_2 + (1-x)^3 A_3\Big]$$

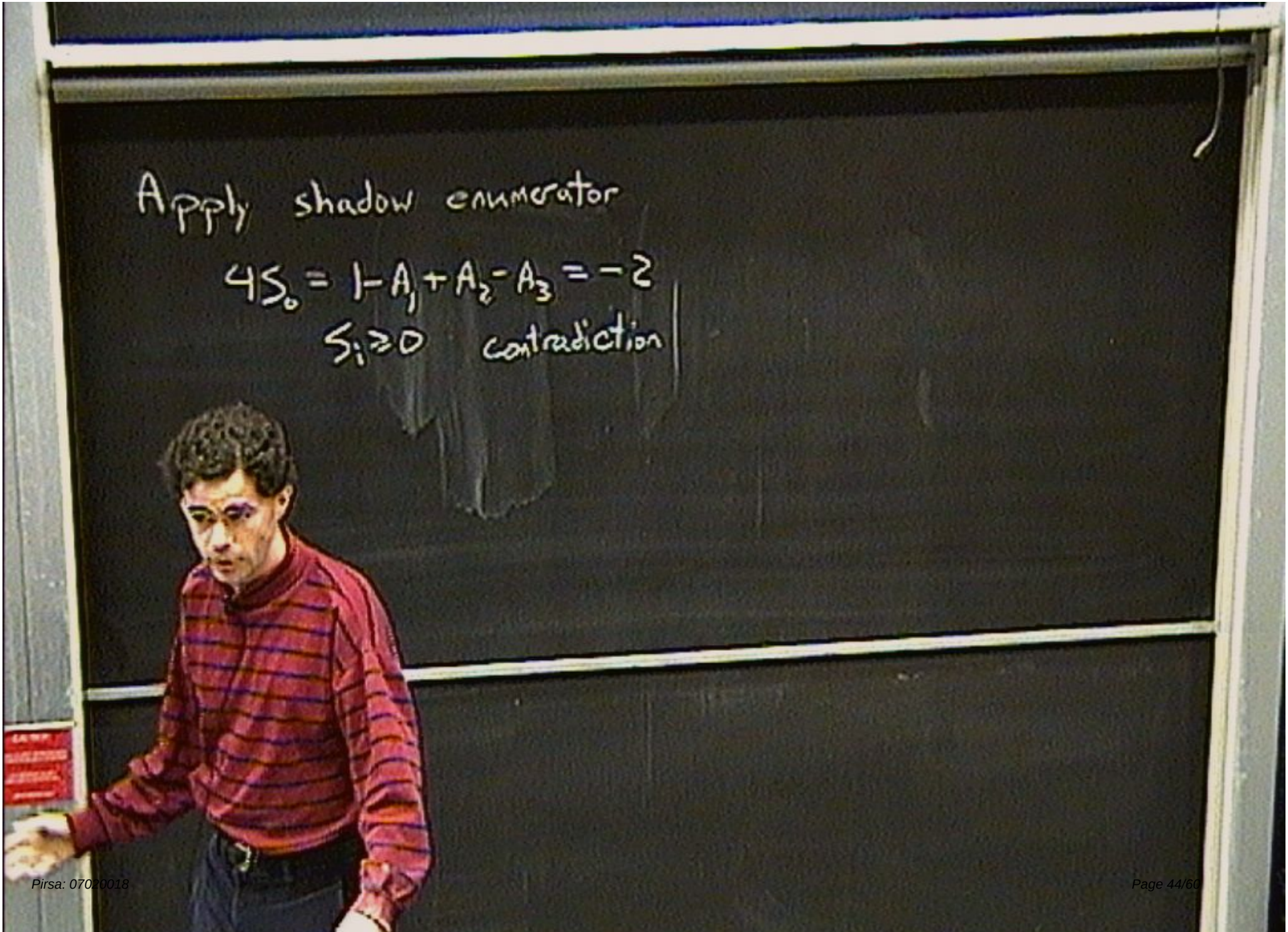
$B_0 = 1$, $A_0 = 1$

$$4 = 4B_0 = 1 + A_1 + A_2 + A_3 \Rightarrow A_1 + A_2 + A_3 = 3$$
$$4B_1 = 9 + 5A_1 + A_2 - 3A_3 \quad B_2 = A_3 \Rightarrow A_1 + A_2 - 3A_3 = -9$$
$$4B_2 = 27 + 3A_1 - 5A_2 + 3A_3 \quad B_3 = A_2 \Rightarrow 3A_1 - 9A_2 + 3A_3 = -27 \checkmark$$
$$4B_3 = 27 - 9A_1 + 3A_2 - A_3 \quad B_3 = A_2 \Rightarrow -9A_1 + 3A_2 - 5A_3 = -27 \checkmark$$

$A_0 = 1$, $A_3 = 3$ $\Rightarrow$ $A_1 = A_2 = 0$

$A(x) = 1 + 3x^3$


Apply shadow enumerator
$4S_0 = 1 - A_1 + A_2 - A_3 = -2$


Apply shadow enumerator
$4S_0 = 1 - A_1 + A_2 - A_3 = -2$
$S_1 \geq 0$ contradiction

Similarly, $k \leq S(C) + (S(A) - S(B)) \Rightarrow [k = S(C) = n - (d - \ldots)]$

Def.: For D-dimensional registers (qudits), $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, X

Similarly, $k \leq \chi(C) + (\chi(A) - \chi(B)) \Rightarrow \boxed{k = \chi(C) = n - (d-1)}$

Def.: For D-dimensional registers (qudits), $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, $X|j\rangle = |j+1 \bmod D\rangle$, $Z|j\rangle = \omega^j |j\rangle$

(For even dimensions, sometimes $\mathcal{P}_1 = \{\sqrt{\omega}^a X^b Z^c\}$)

n-qudit Pauli group $\mathcal{P}_n$ is tensor product of n $\mathcal{P}_1$'s (i.e. $\{\omega^a X^{b_1} Z^{c_1} \otimes X^{b_2} Z^{c_2} \otimes \cdots X^{b_n} Z^{c_n}\}$

Similarly, $k \leq \chi(C) + (\chi(A) - \chi(B)) \Rightarrow k = \chi(C) = n - 2(g-1)$

Def.: For D-dimensional registers (qudits), $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, $X|j\rangle = |j+1 \pmod D\rangle$, $Z|j\rangle = \omega^j |j\rangle$

(For even dimensions, sometimes $\mathcal{P}_1 = \{\sqrt{\omega}^a X^b Z^c\}$)

n-qudit Pauli group $\mathcal{P}_n$ is tensor product of n $\mathcal{P}_1$'s (i.e. $\{\omega^a X^{b_1} Z^{c_1} \otimes X^{b_2} Z^{c_2} \otimes \cdots \otimes X^{b_n} Z^{c_n}\}$)

$XZ = \omega^{-1} ZX$, $(X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \omega^{bc-ad} (X^c Z^d)(X^a Z^b)$

Similarly, $k \leq s(C) \Rightarrow (S(A) \to S(B)) \Rightarrow k \leq s(C) = n - \dim(A)$

Def.: For D-dimensional registers (qudits), $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, $X|j\rangle = |j+1 \bmod D\rangle$, $Z|j\rangle = \omega^j |j\rangle$

(For even dimensions, sometimes $\mathcal{P}_1 = \{\sqrt{\omega}^a X^b Z^c\}$)

n-qudit Pauli group $\mathcal{P}_n$ is tensor product of n $\mathcal{P}_1$'s (i.e. $\{\omega^a X^{b_1} Z^{c_1} \otimes X^{b_2} Z^{c_2} \otimes \cdots X^{b_n} Z^{c_n}\}$)

$XZ = \omega^{-1} ZX$, $(X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \omega^{bc-ad} (X^c Z^d)(X^a Z^b)$

Map $\rightarrow$ vector (length $2n$) $P \to (\vec{a}|\vec{b})$ $(P = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n})$

Similarly, $k \leq \chi(C) - (\chi(A) - \chi(B)) \Rightarrow k = \chi(C) = n - (d-1)$

Def.: For D-dimensional registers (qudits), $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, $X|j\rangle = |j+1 \bmod D\rangle$, $Z|j\rangle = \omega^j |j\rangle$

(For even dimensions, sometimes $\mathcal{P}_1 = \{\sqrt{\omega}^a X^b Z^c\}$)

n-qudit Pauli group $\mathcal{P}_n$ is tensor product of n $\mathcal{P}_1$s (i.e. $\{\omega^a X^{b_1} Z^{c_1} \otimes X^{b_2} Z^{c_2} \otimes \cdots \otimes X^{b_n} Z^{c_n}\}$)

$XZ = \omega^{-1} ZX$, $(X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \boxed{\omega^{bc-ad}} (X^c Z^d)(X^a Z^b)$

Map $\rightarrow$ vector (length $2n$) $P \rightarrow (\vec{a}|\vec{b})$ $(P = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n})$

Symplectic inner product $P \cdot Q = (\vec{a}|\vec{b}) \cdot (\vec{c}|\vec{d}) = \vec{b} \cdot \vec{c} - \vec{a} \cdot \vec{d}$

Def: For D-dimensional r[redacted], $D \geq 2$, let the Pauli group $\mathcal{P}_1 = \{\omega^a X^b Z^c\}$, where $\omega = e^{2\pi i/D}$, $X|j\rangle = |j+1 \pmod D\rangle$, $Z|j\rangle = \omega^j |j\rangle$

(For even dimensions, sometimes $\mathcal{P}_1 = \{\sqrt{\omega}^a X^b Z^c\}$)

n-qudit Pauli group $\mathcal{P}_n$ is tensor product of n $\mathcal{P}_1$'s (i.e. $\{\omega^a X^{b_1} Z^{c_1} \otimes X^{b_2} Z^{c_2} \otimes \cdots \otimes X^{b_n} Z^{c_n}\}$)

$XZ = \omega^{-1} ZX$, $(X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \boxed{\omega^{bc-ad}} (X^c Z^d)(X^a Z^b)$

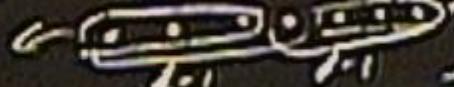
Mod d vector (length $2n$) $P \to (\vec{a}|\vec{b})$ $(P = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n})$

Symplectic inner product $P \cdot Q = (\vec{a}|\vec{b}) \cdot (\vec{c}|\vec{d}) = \vec{b}\cdot\vec{c} - \vec{a}\cdot\vec{d}$

$PQ = \omega^{P \cdot Q} QP$

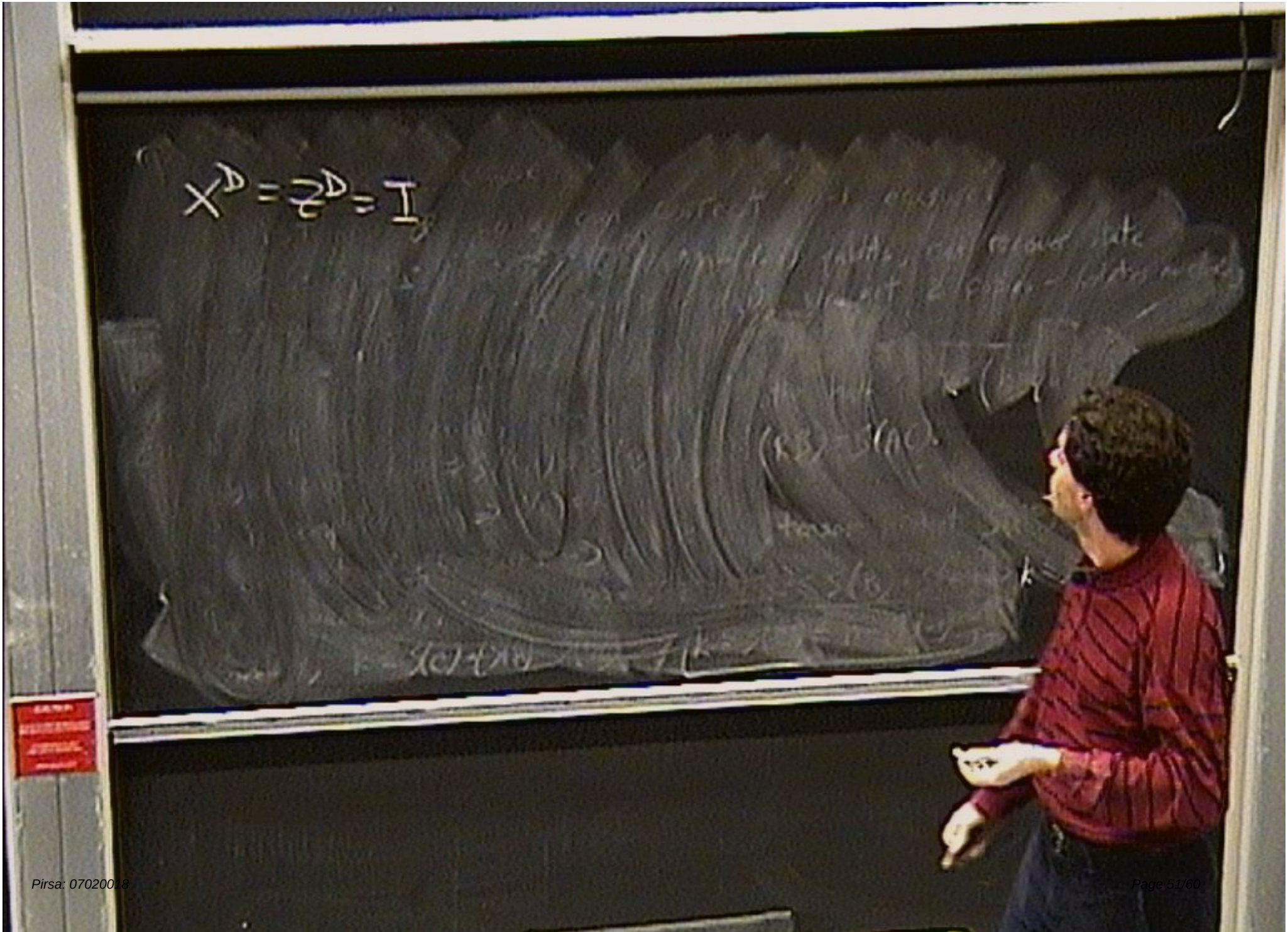
Proof: $k=1$ case

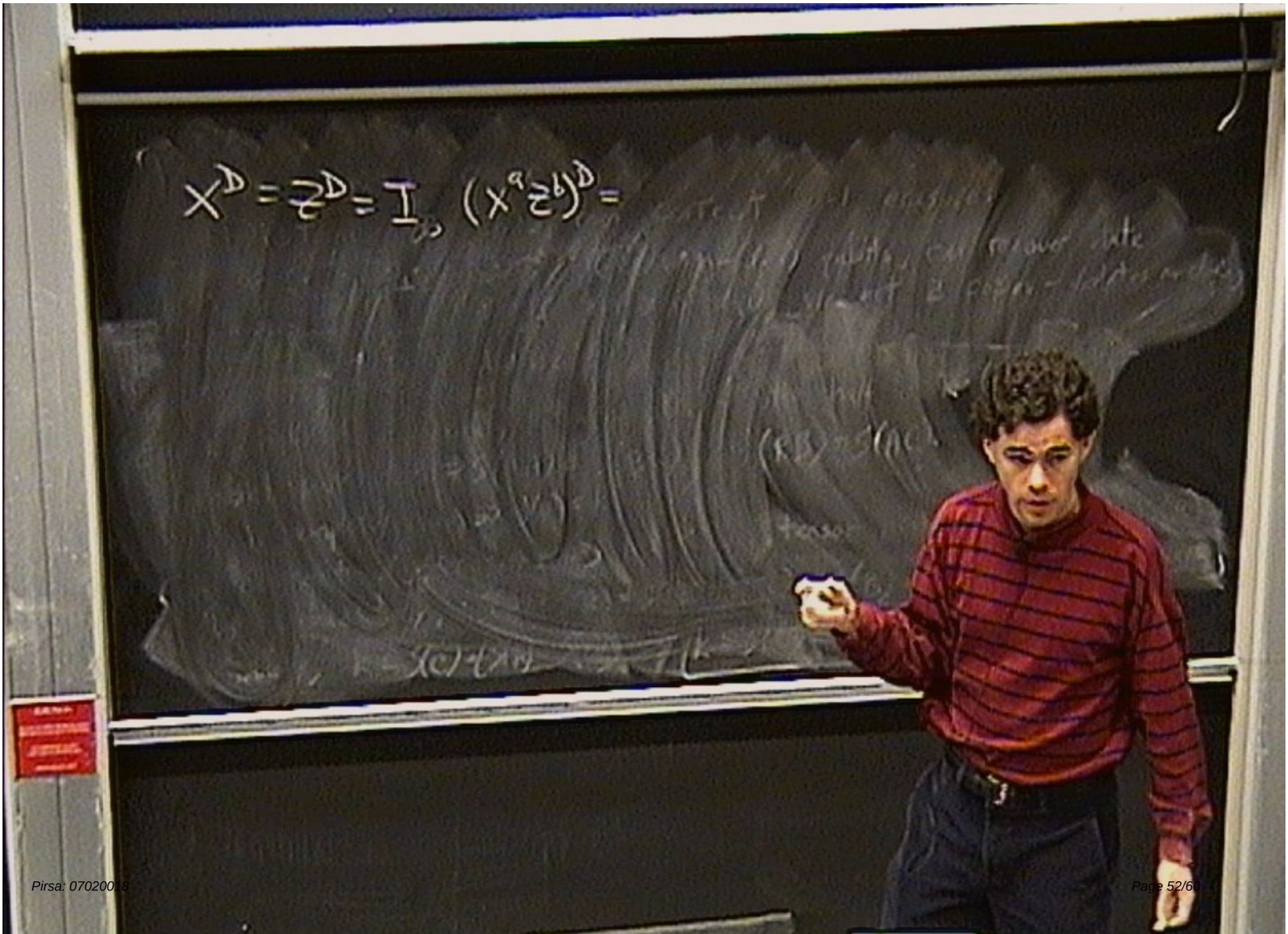
Distance d code can correct $d-1$ erasures

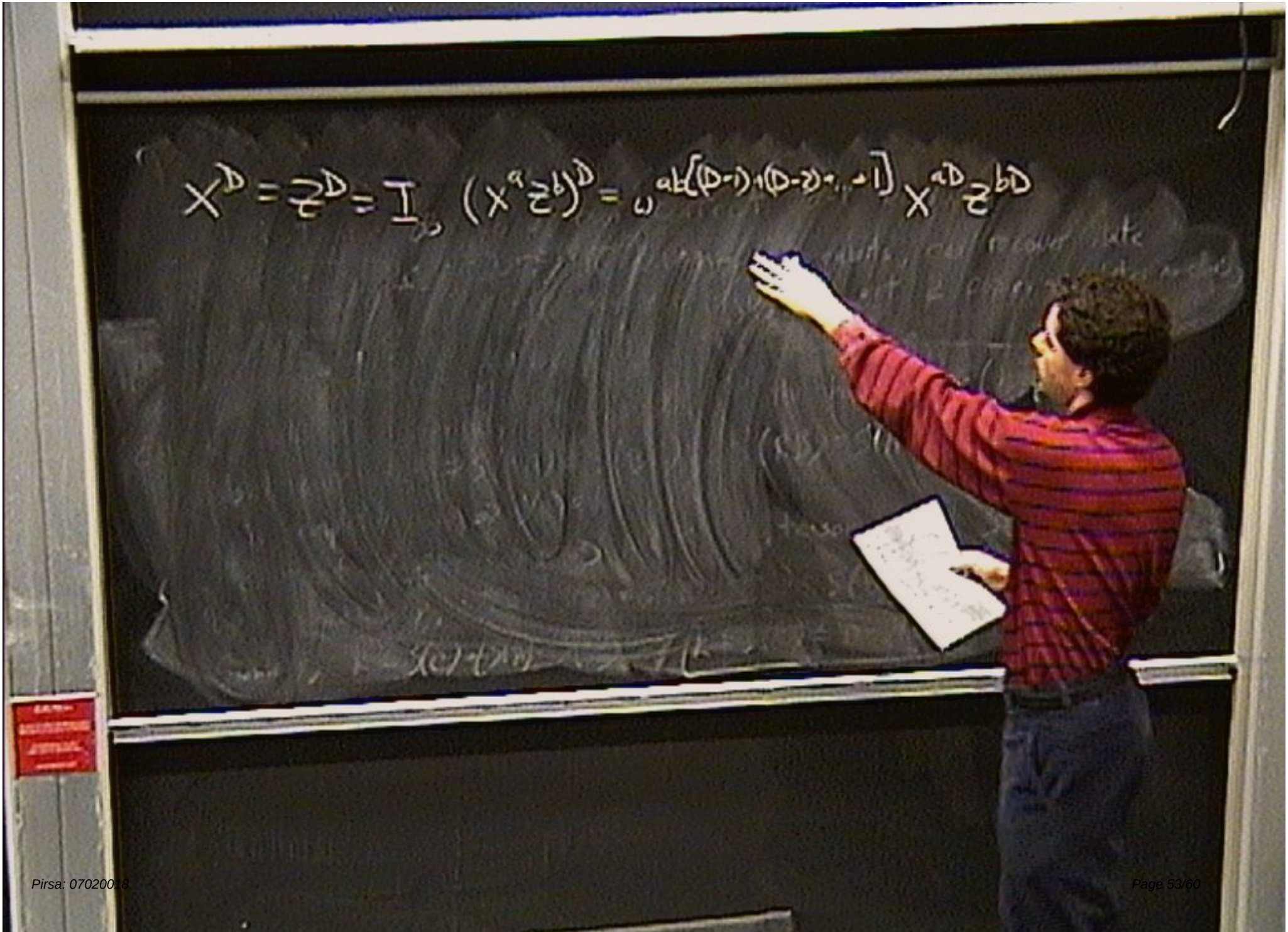


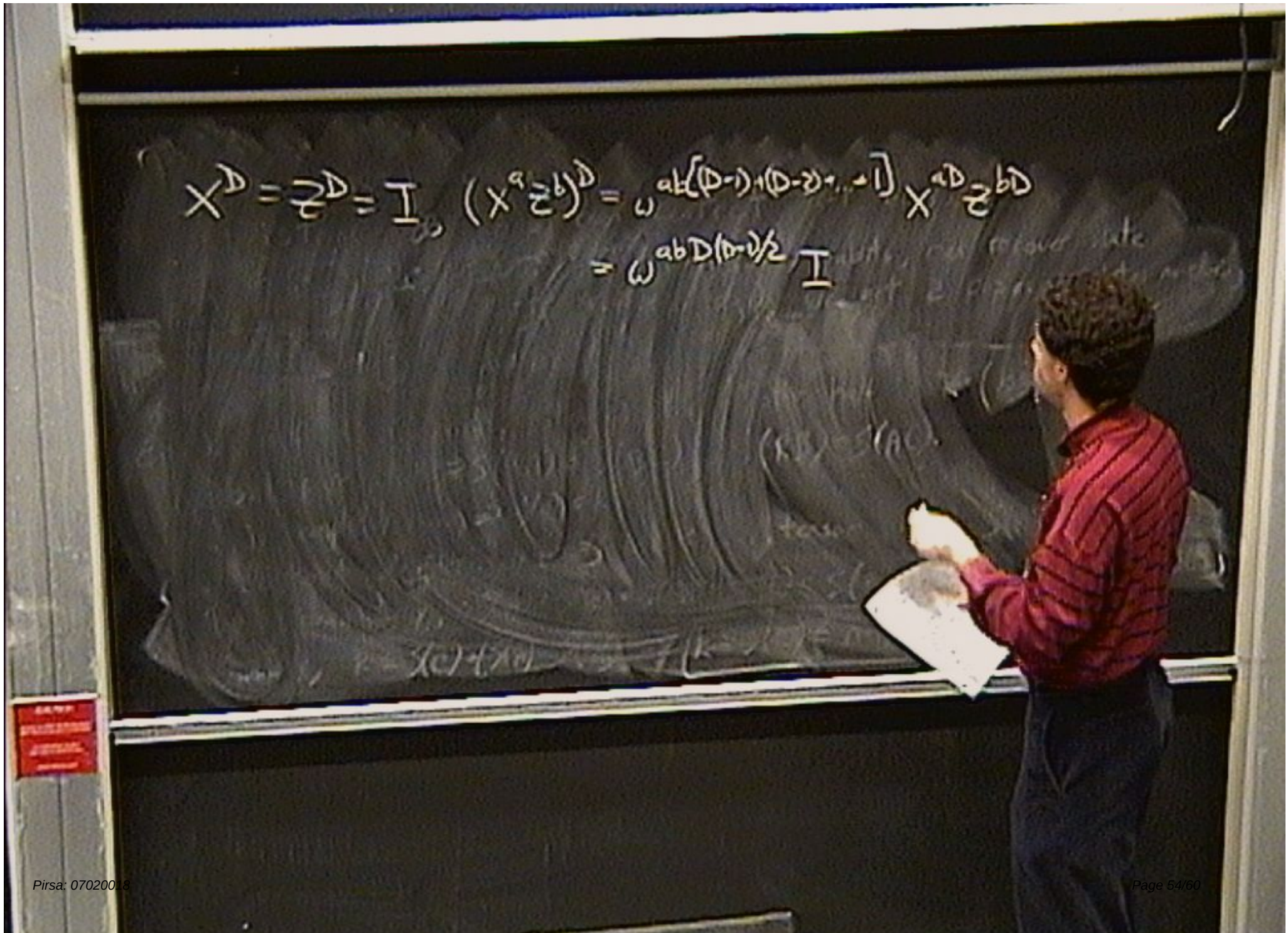
Given $n-(d-1)$ qubits, can recover state

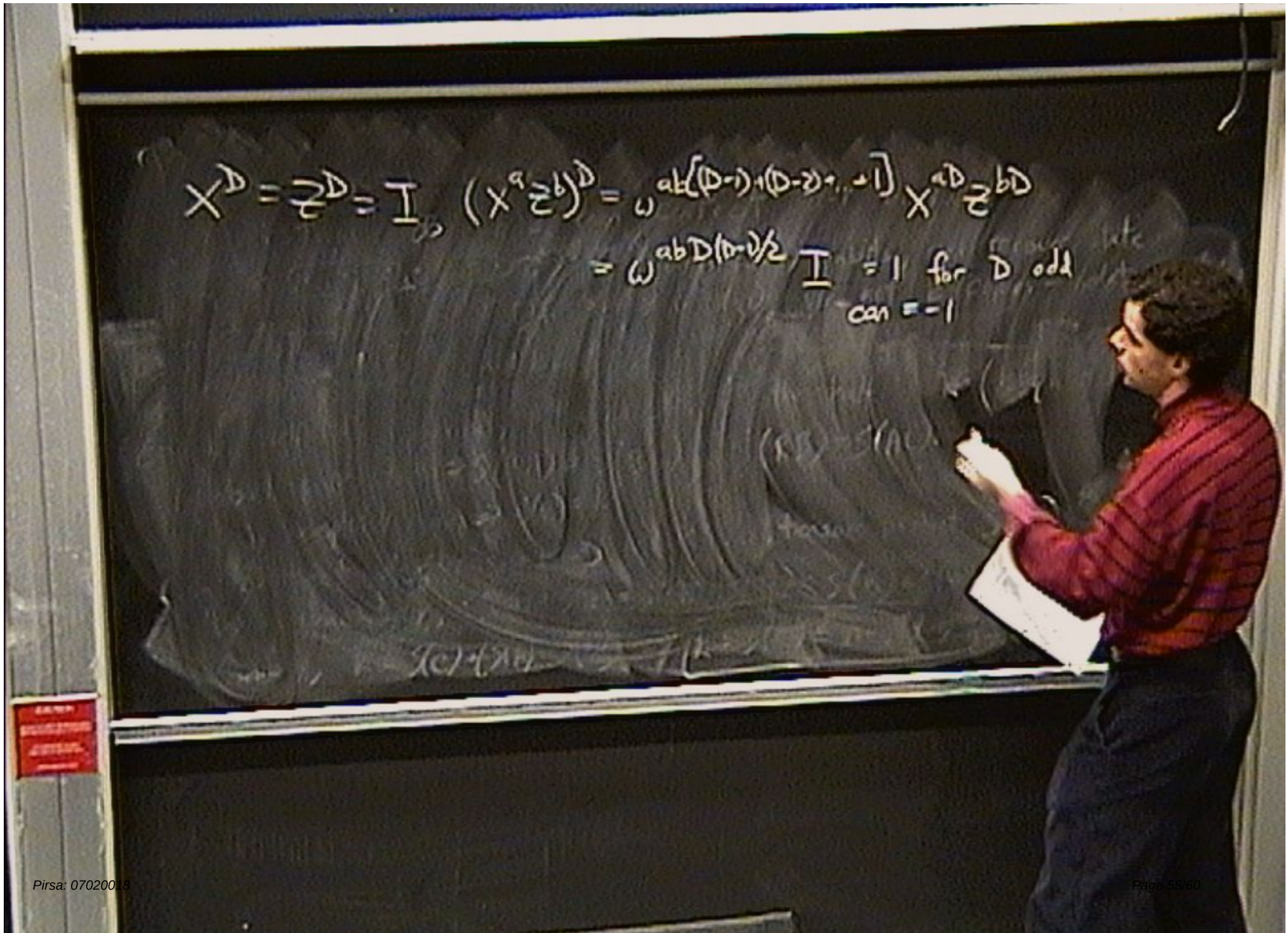
If $d-1 \geq n-(d-1)$, we get 2 copies – violates no-cloning


$X^D = Z^D = I$


$X^D = Z^D = \sum_{p_1} (X^q Z^b)^D =$




$X^D = Z^D = \mathbb{I}$, $(X^a Z^b)^D = \omega^{ab[(D-1)+(D-2)+\cdots+1]} X^{aD} Z^{bD}$
$= \omega^{abD(D-1)/2} \mathbb{I}$


$X^D = Z^D = \underline{I}_D$
$(X^a Z^b)^D = \omega^{ab[(D-1)+(D-2)+\cdots+1]} X^{aD} Z^{bD}$
$= \omega^{abD(D-1)/2}$
$\underline{I}$ = 1 for D odd
can = -1

$X^D = Z^D = I$, $(X^a Z^b)^D = \omega^{ab[(D-1)+(D-2)+\cdots+1]} X^{aD} Z^{bD}$

$= \omega^{abD(D-1)/2} I$ $= 1$ for D odd

$= -1$ for D even

P_n span $D^n \times D^n$ matrices $\Rightarrow$ can use as error bases

Specialize to $D = p$ prime (> 2)

Thm: Let S be an Abelian subgroup of P_n. $T(S) = \{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$

If S has r generators, $|S| = p^r$, $\dim T(S) = p^{k-r}$ $(k = n - r)$

$X^D = Z^D = I$, $(X^a Z^b)^D = \omega^{ab[(D-1)+(D-2)+\cdots+1]} X^{aD} Z^{bD}$

$= \omega^{abD(D-1)/2} I$ $= 1$ for D odd

can $= -1$ for D even

P_n span $D^n \times D^n$ matrices $\Rightarrow$ can use as error basis

Specialize to $D = p$ prime (> 2)

Thm: Let S be an Abelian subgroup of P_n, $T(S) = \{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$

If S has r generators, $|S| = p^r$, $\dim T(S) = p^{k-r}$ $(k = n-r)$

$= \omega^{abD(D-1)/2} \underline{I}$ $= 1$ for D odd

can $= -1$ for D even

$\mathcal{P}_n$ span $D^2 \times D^2$ matrices $\Rightarrow$ can use as error basis

Specialize to $D = p$ prime (> 2)

Thm: Let S be an Abelian subgroup of $\mathcal{P}_n$. $T(S) = \{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$

If S has r generators, $|S| = p^r$, $\dim T(S) = p^{k+r}$ $(k = n-r)$.

Let $N(S) = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$, and

$= \omega^{abD(D-1)/2} \underline{T} = 1$ for D odd

$\underline{T} = -1$ for D even

$\mathcal{P}_n$ span $D^n \times D^n$ matrices $\Rightarrow$ can use as error basis

Specialize to $D = p$ prime (> 2)

Thm: Let S be an Abelian subgroup of $\mathcal{P}_n$. $T(S) = \{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$.

If S has r generators, $|S| = p^r$, $\dim T(S) = p^{k-r}$ ($k = n-r$).

Let $N(S) = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$, and let $d = \min_{P \in N(S) \setminus S} w(P)$.

Then $T(S)$ has distance d as a qudit code.

$= \omega^{ab D(D-1)/2} \underline{T} = 1$ for D odd

can $= -1$ for D even

$\mathcal{P}_n$ span $D^n \times D^n$ matrices $\Rightarrow$ can use as error basis

Specialize to $D = p$ prime (> 2)

Thm: Let S be an Abelian subgroup of $\mathcal{P}_n$. $T(S) = \{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \ \forall M \in S\}$.

If S has r generators, $|S| = p^r$, $\dim T(S) = p^{k+r}$ ($k = n-r$).

Let $N(S) = \{P \in \mathcal{P}_n \mid PM = MP \ \forall M \in S\}$, and let $d = \min_{P \in N(S) \setminus S} \mathrm{wt}(P)$.

Then $T(S)$ has distance d as a qudit code.

We say it is $((n, k, d))_p$