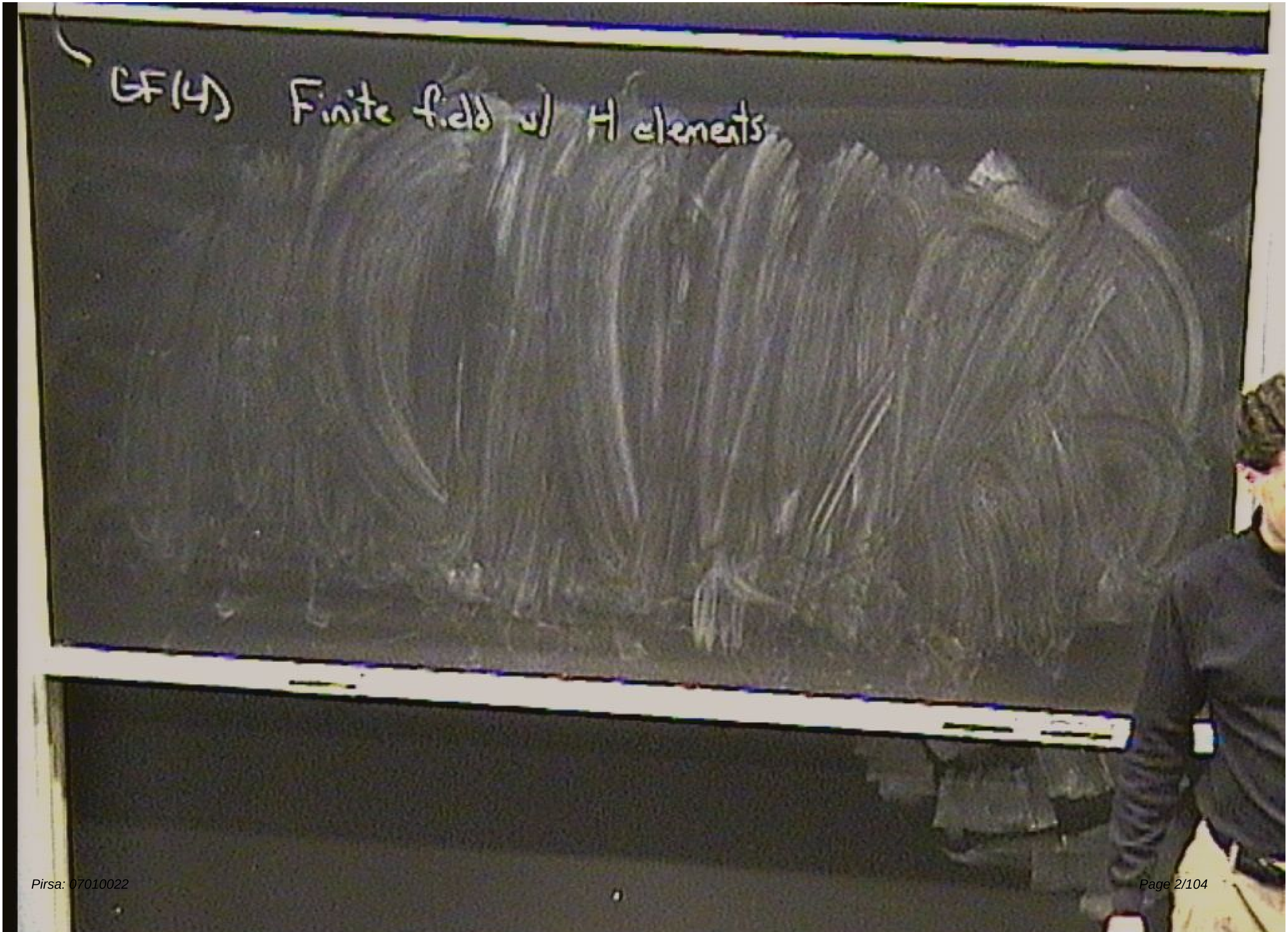
Title: Quantum Error Correction 3A

Date: Jan 23, 2007 03:30 PM

URL: http://pirsa.org/07010022

Abstract: Finite field GF(4), stabilizer codes as GF(4) codes, perfect quantum codes, definition of Clifford group, sample elements of Clifford group


GF(4) Finite field w/ 4 elements

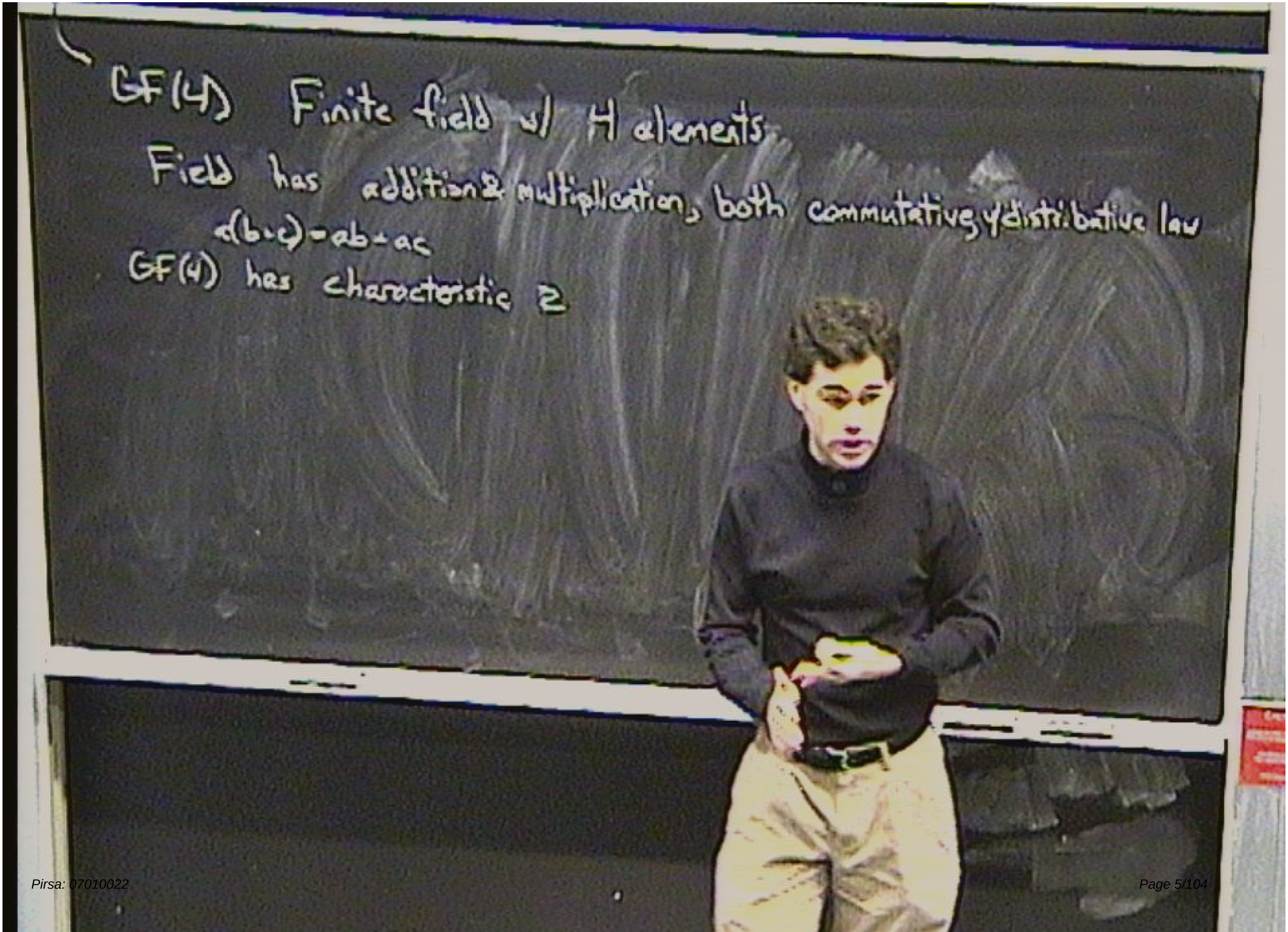
GF(4) Finite field w/ 4 elements.

Field has addition & multiplication

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative & distributive law

$a(b+c) = ab + ac$

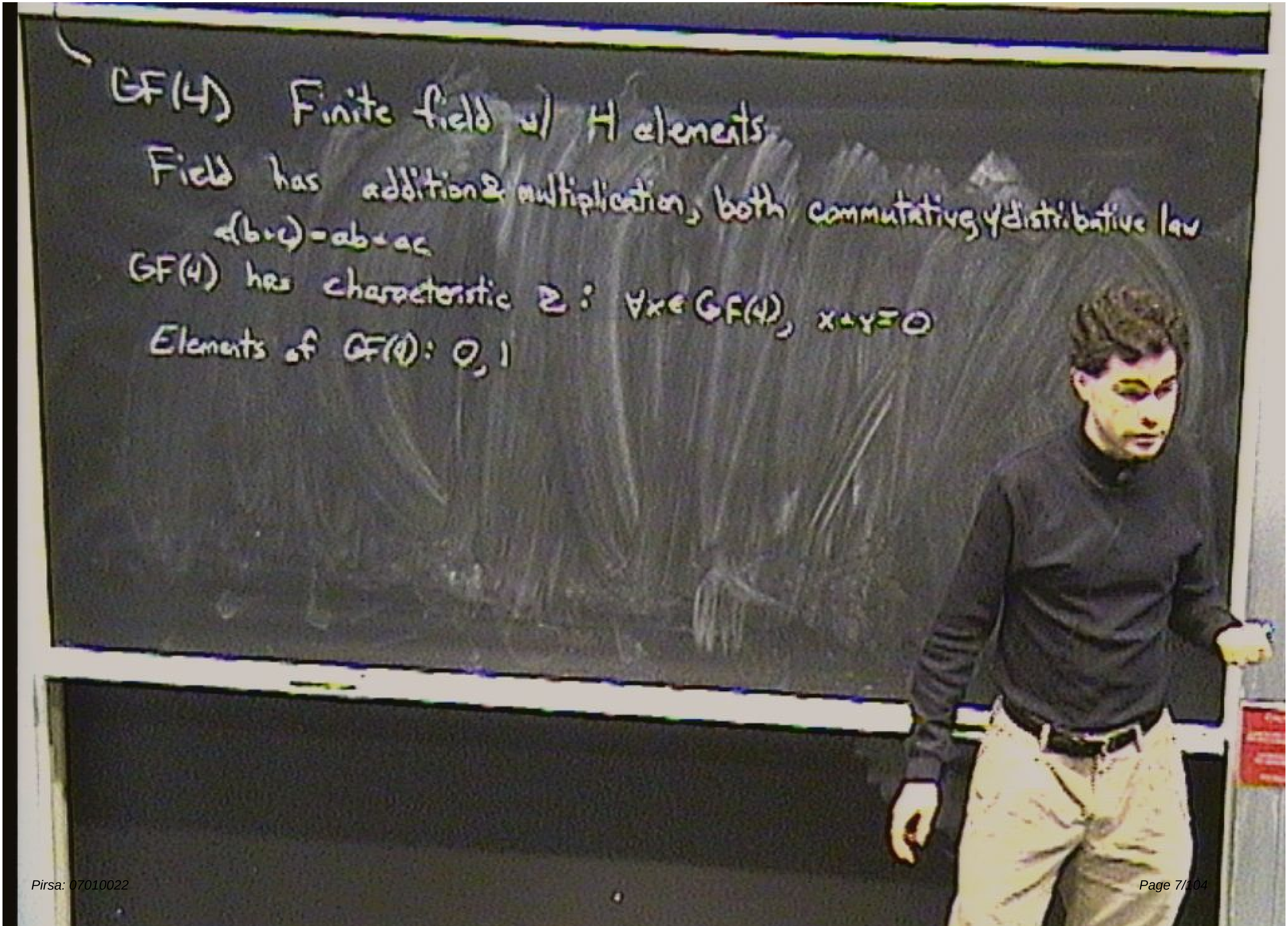

GF(4) Finite field w/ 4 elements
Field has addition & multiplication, both commutative, distributive law
a(b+c) = ab + ac
GF(4) has characteristic 2

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative, distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x+x=0$


GF(4) Finite field w/ 4 elements
Field has addition & multiplication, both commutative & distributive law
a(b+c) = ab+ac
GF(4) has characteristic 2: ∀x∈GF(4), x+x=0
Elements of GF(4): 0, 1

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative, & distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative, & distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4),\ x + x = 0$

Elements of GF(4): $0, 1, \omega, \omega^2$

$1 + \omega = \omega^2$

$\omega^3 = 1$

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative, distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dim vector space over $\mathbb{Z}_2$

$1+\omega=\omega^2$

$\omega^3=1$

GF(4) Finite field w/ 4 elements

Field has addition & multiplication, both commutative, & distributive law

$a(b+c) = ab + ac$

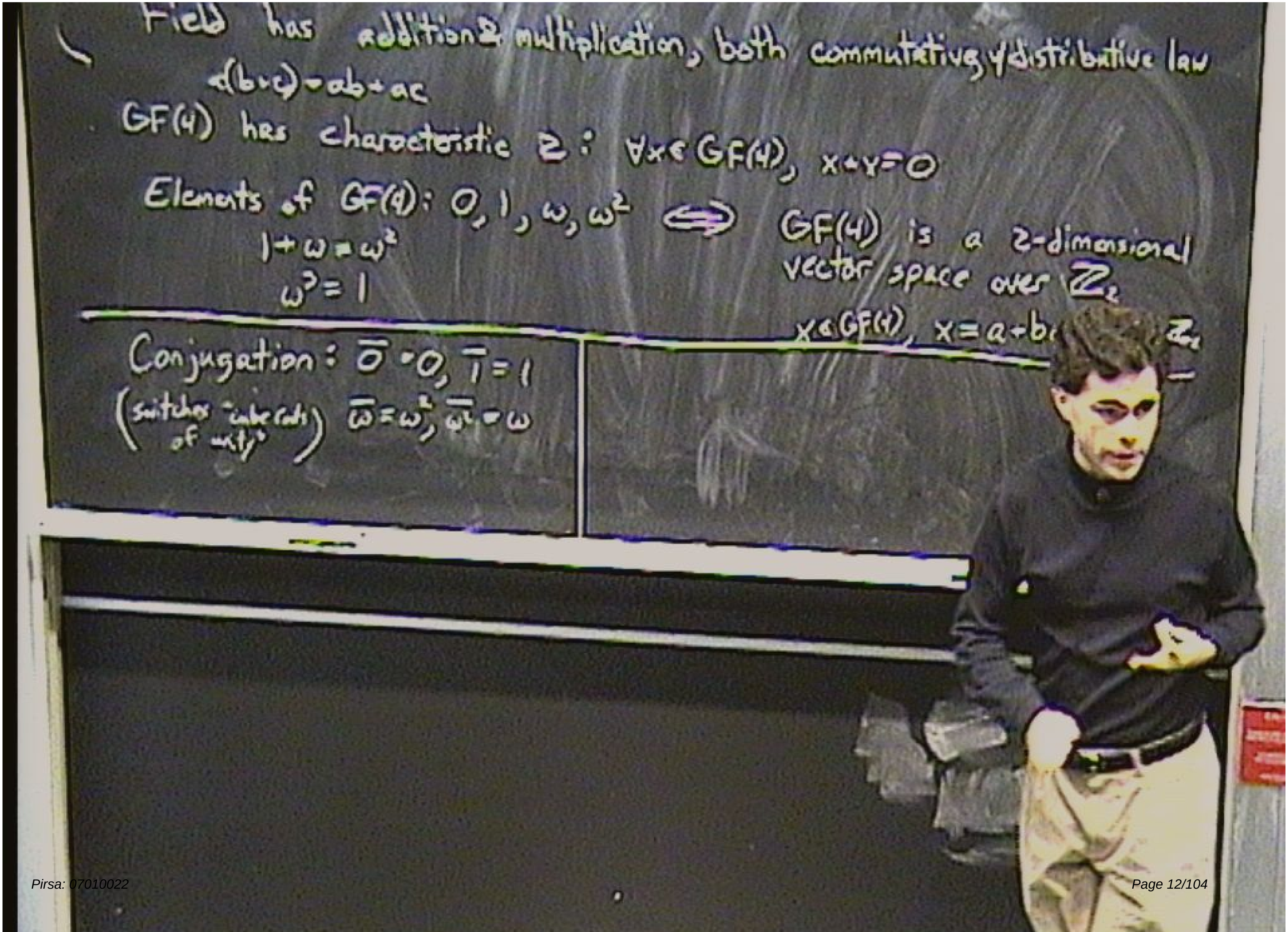
GF(4) has characteristic 2: $\forall x \in GF(4)$, $x + x = 0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1 + \omega = \omega^2$

$\omega^3 = 1$

$x \in GF(4)$, $x = a + b\omega$, $a, b \in \mathbb{Z}_2$


Field has addition & multiplication, both commutative & distributive law
a(b+c) = ab+ac
GF(4) has characteristic 2: ∀x∈GF(4), x+x=0
Elements of GF(4): 0, 1, ω, ω² ⟺ GF(4) is a 2-dimensional vector space over ℤ₂
1+ω=ω²
ω³=1
x∈GF(4), x=a+b
Conjugation: 0̄=0, 1̄=1
(switches "cube roots of unity") ω̄=ω², ω̄²=ω

Field has addition & multiplication, both commutative, distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4),\ x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1+\omega=\omega^2$

$\omega^3=1$

$x \in GF(4),\ x = a + b\omega,\ a,b \in \mathbb{Z}_2$

Conjugation: $\bar{0}=0,\ \bar{1}=1$

(switches "cube roots of unity") $\bar{\omega}=\omega^2,\ \overline{\omega^2}=\omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x

Field has addition & multiplication, both commutative, distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x + x = 0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1 + \omega = \omega^2$

$\omega^3 = 1$

$x \in GF(4)$, $x = a + b\omega$, $a, b \in \mathbb{Z}_2$

Conjugation: $\bar{0} = 0$, $\bar{1} = 1$

(switches "cube roots of unity") $\bar{\omega} = \omega^2$, $\overline{\omega^2} = \omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x

Field has addition & multiplication, both commutative, distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x + x = 0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1 + \omega = \omega^2$

$\omega^3 = 1$

$x \in GF(4)$, $x = a + b\omega$, $a, b \in \mathbb{Z}_2$

Conjugation: $\bar{0} = 0$, $\bar{1} = 1$

(switches "cube roots of unity") $\bar{\omega} = \omega^2$, $\overline{\omega^2} = \omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x E.g. $M_\omega = ($

Field has addition & multiplication, both commutative, & distributive law

$a(b+c)=ab+ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1+\omega=\omega^2$

$\omega^3=1$

$x \in GF(4)$, $x=a+b\omega$, $a,b \in \mathbb{Z}_2$

Conjugation: $\bar{0}=0$, $\bar{1}=1$

(switches "cube roots of unity") $\bar{\omega}=\omega^2$, $\overline{\omega^2}=\omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x. E.g. $M_\omega=\begin{pmatrix}0&1\\1&1\end{pmatrix}$

<u>Trace</u>: $\mathrm{tr}\,x=\mathrm{tr}\,M_x$

Field has addition & multiplication, both commutative, & distributive law

$a(b+c) = ab + ac$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x + x = 0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1 + \omega = \omega^2$

$\omega^3 = 1$

$x \in GF(4)$, $x = a + b\omega$, $a, b \in \mathbb{Z}_2$

Conjugation: $\bar{0} = 0$, $\bar{1} = 1$

(switches "cube roots of unity") $\bar{\omega} = \omega^2$, $\overline{\omega^2} = \omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x. E.g. $M_\omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

<u>Trace</u>: $\mathrm{tr}\, x = \mathrm{tr}\, M_x = x + x^2$

GF(4) has characteristic 2: $\forall x \in GF(4)$, $x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1+\omega=\omega^2$

$\omega^3=1$

$x \in GF(4)$, $x = a+b\omega$, $a,b \in \mathbb{Z}_2$

Conjugation: $\bar{0}=0$, $\bar{1}=1$

(switches "cube roots of unity") $\bar{\omega}=\omega^2$, $\overline{\omega^2}=\omega$

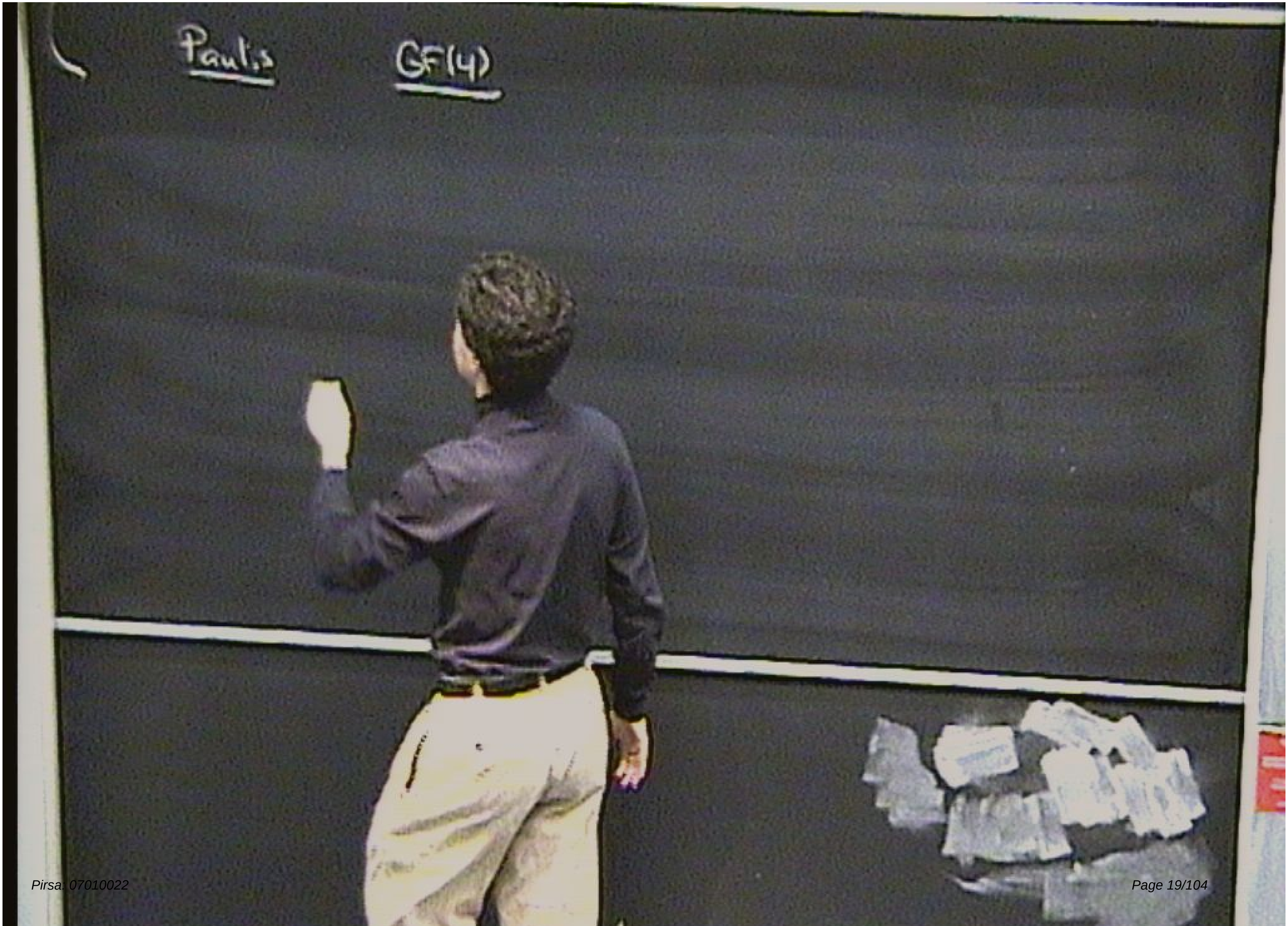
Multiplication by $x \in GF(4)$ corresponds to some matrix M_x Eg. $M_\omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

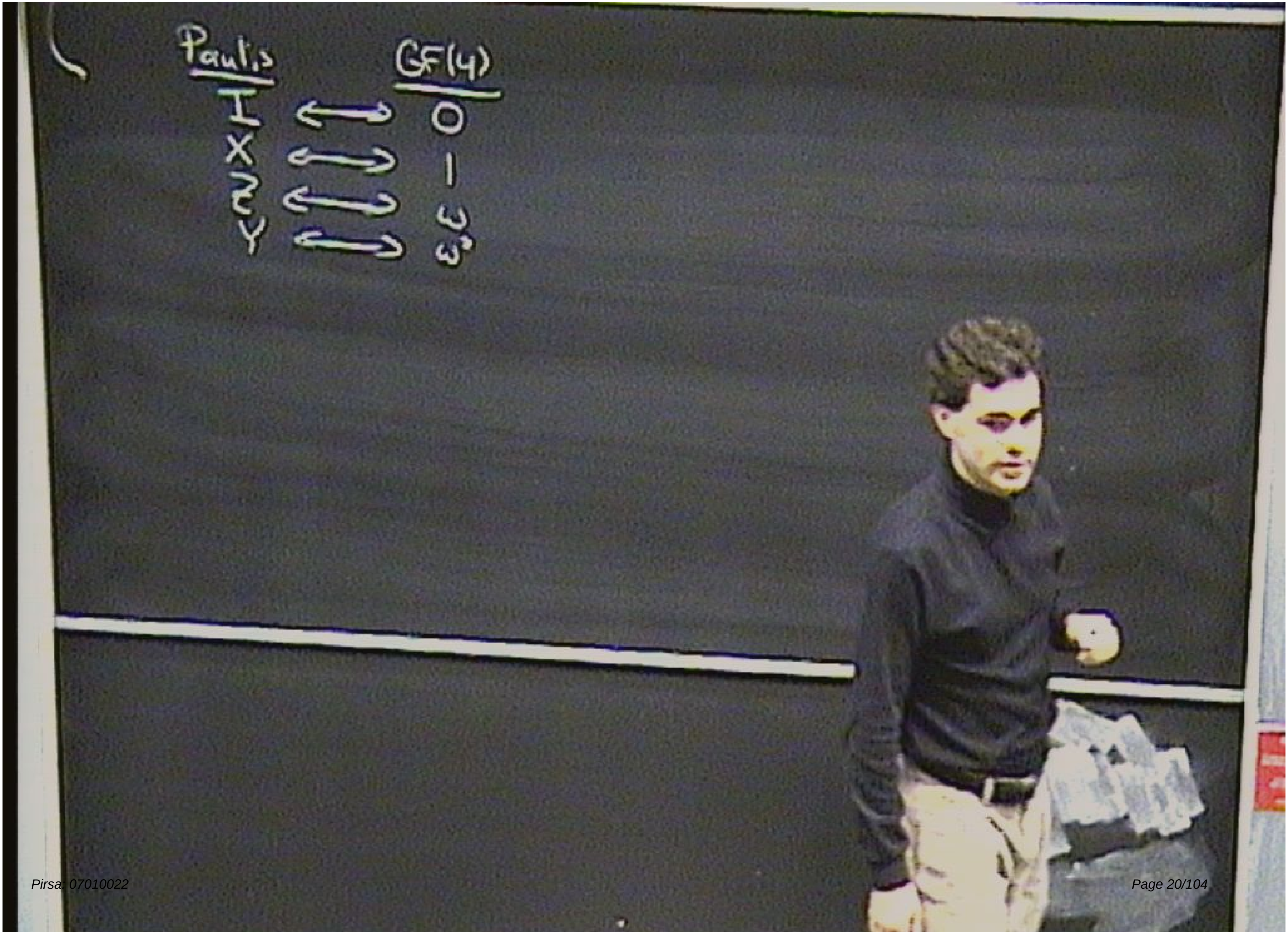
Trace: $\mathrm{tr}\, x = \mathrm{tr}\, M_x = x + x^2$

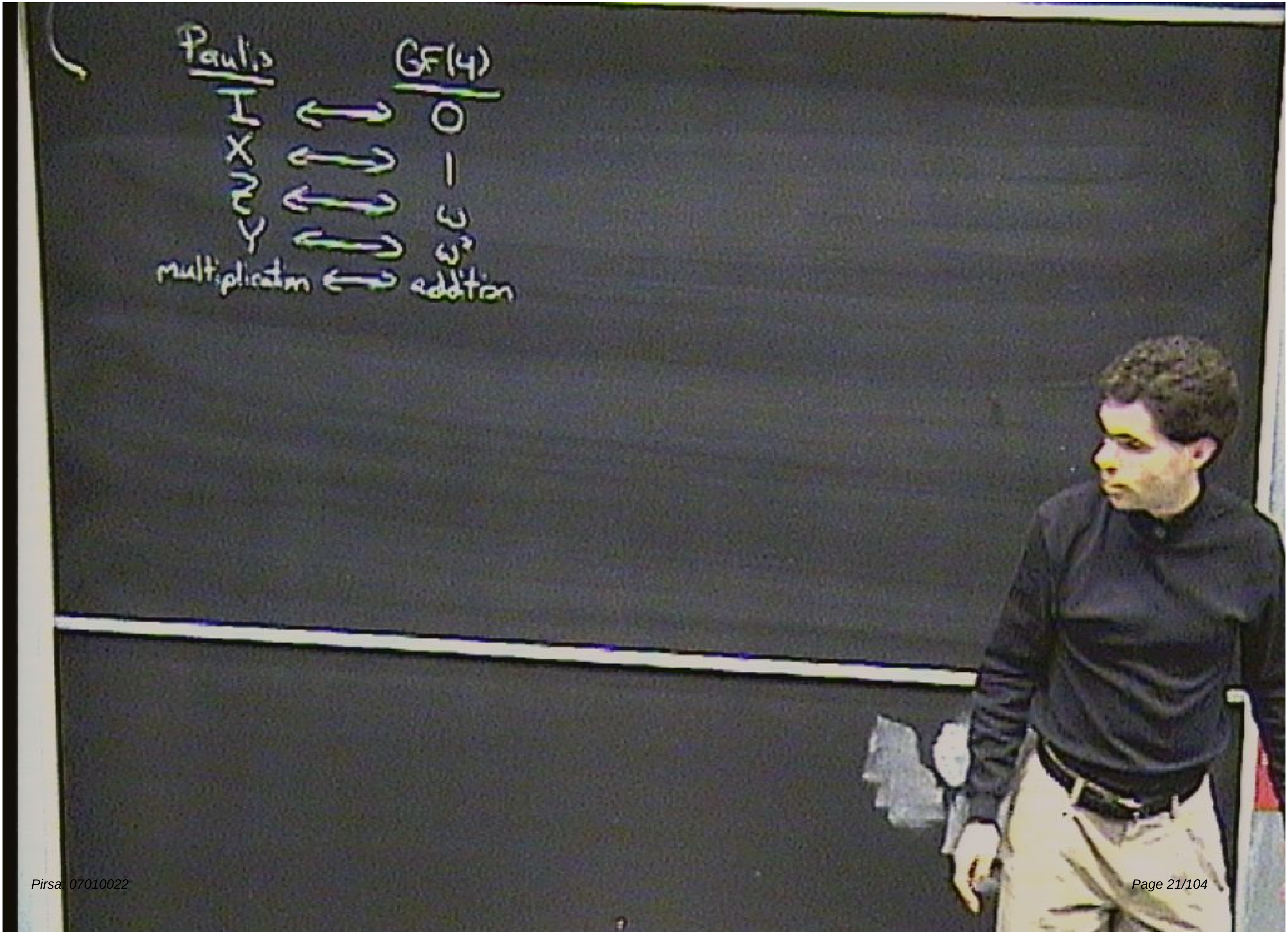
$\mathrm{tr}\, x \in \mathbb{Z}_2$

$\mathrm{tr}\, 0 = \mathrm{tr}\, 1 = 0$

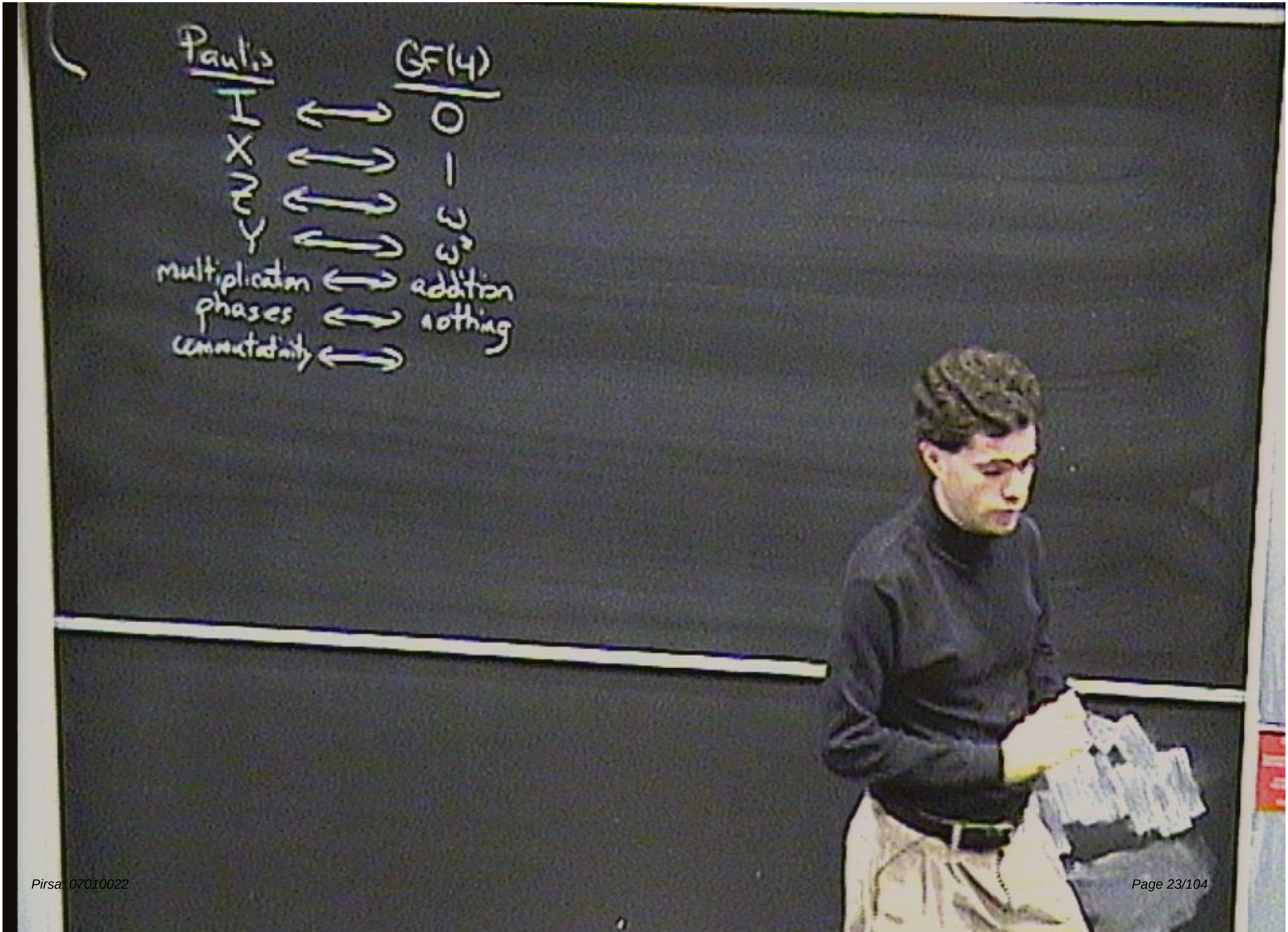
$\mathrm{tr}\, \omega = \mathrm{tr}\, \omega^2 = 1$

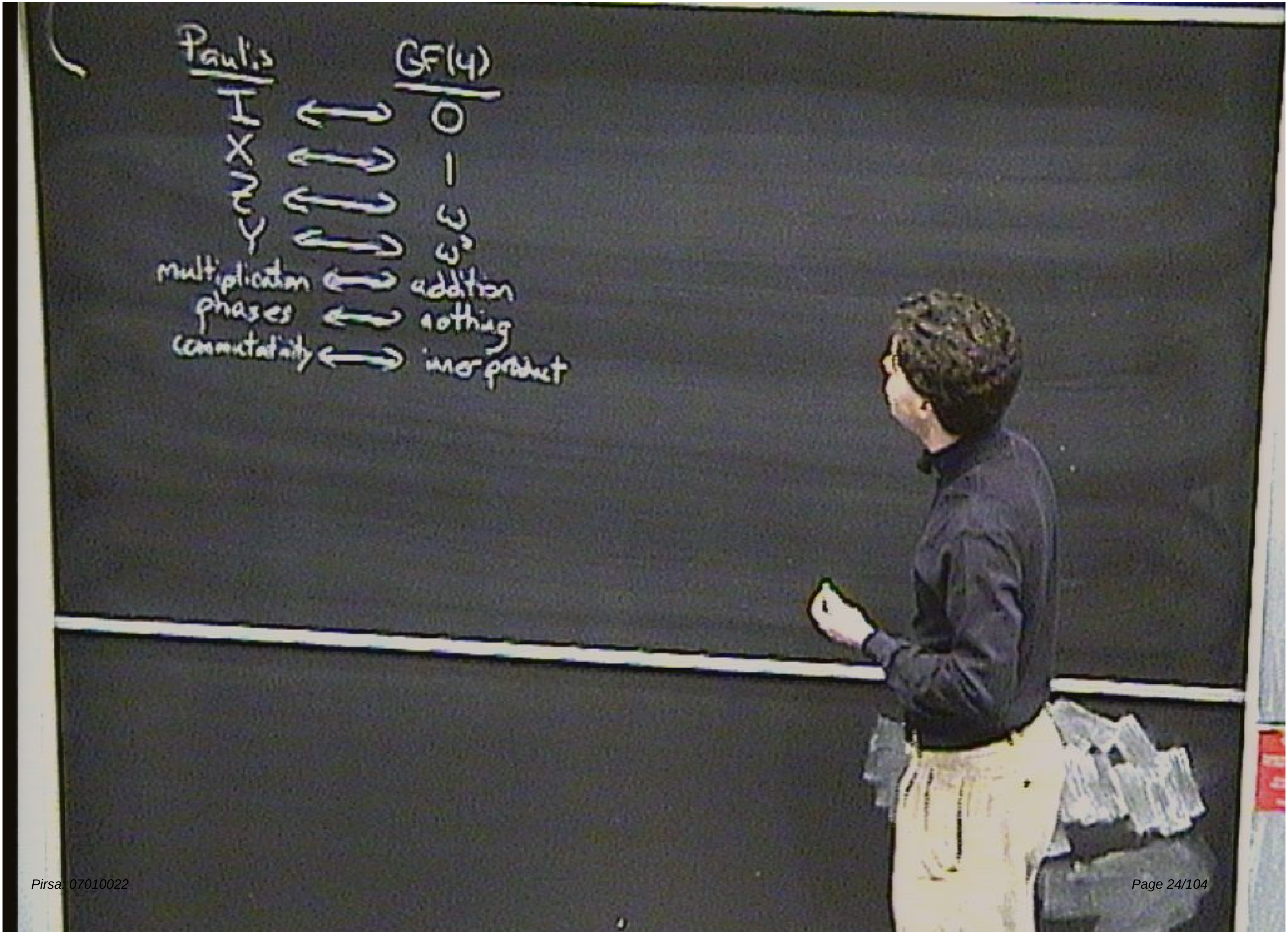

Paulis
GF(4)


Paulis GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²


Paulis
GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²
multiplication ⟷ addition

Paulis		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition
phases	$\longleftrightarrow$	nothing


Paulis
GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²
multiplication ⟷ addition
phases ⟷ nothing
commutativity ⟷


Paulis
GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²
multiplication ⟷ addition
phases ⟷ nothing
commutativity ⟷ inner product

Paulis		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition
phases	$\longleftrightarrow$	nothing
commutativity	$\longleftrightarrow$	inner product

$$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$$

Paulis		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition
phases	$\longleftrightarrow$	nothing
commutativity	$\longleftrightarrow$	inner product

$$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$$

$$[P,Q]=0 \Leftrightarrow tr(\vec{u} \cdot \overline{\vec{v}}) = 0$$

GF(4) has characteristic 2 : $\forall x \in GF(4),\ x+x=0$

Elements of GF(4): $0, 1, \omega, \omega^2$ $\Longleftrightarrow$ GF(4) is a 2-dimensional vector space over $\mathbb{Z}_2$

$1+\omega=\omega^2$

$\omega^3=1$

$x \in GF(4),\ x = a+b\omega,\ a,b \in \mathbb{Z}_2$

Conjugation: $\bar{0}=0,\ \bar{1}=1$

(switches "cube roots of unity") $\bar{\omega}=\omega^2,\ \overline{\omega^2}=\omega$

Multiplication by $x \in GF(4)$ corresponds to some matrix M_x. E.g. $M_\omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

Trace: $\mathrm{tr}\, x = \mathrm{tr}\, M_x = x + x^2$

$\mathrm{tr}\, x \in \mathbb{Z}_2$

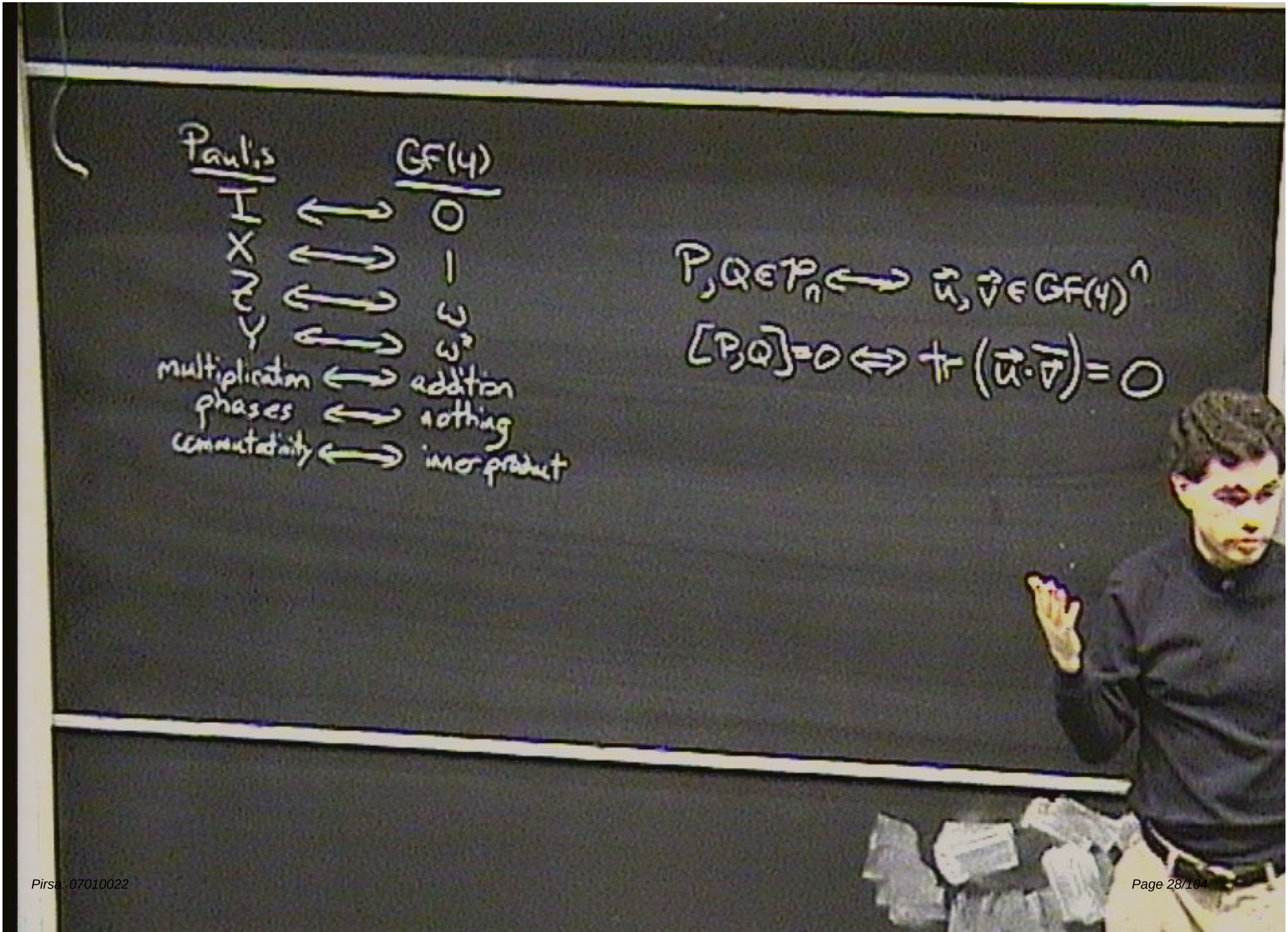
$\mathrm{tr}\, 0 = \mathrm{tr}\, 1 = 0$

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

Paulis		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition

$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$

$[P,Q]=0 \Leftrightarrow \mathrm{tr}\left(\vec{u} \cdot \bar{\vec{v}}\right) = 0$


Paulis
GF(4)
$I \longleftrightarrow 0$
$X \longleftrightarrow 1$
$Z \longleftrightarrow \omega$
$Y \longleftrightarrow \omega^2$
multiplication $\longleftrightarrow$ addition
phases $\longleftrightarrow$ nothing
commutativity $\longleftrightarrow$ inner product
$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$
$[P, Q] = 0 \Leftrightarrow \mathrm{tr}(\vec{u} \cdot \bar{\vec{v}}) = 0$

Pauli's		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition
phases	$\longleftrightarrow$	nothing
commutativity	$\longleftrightarrow$	inner product

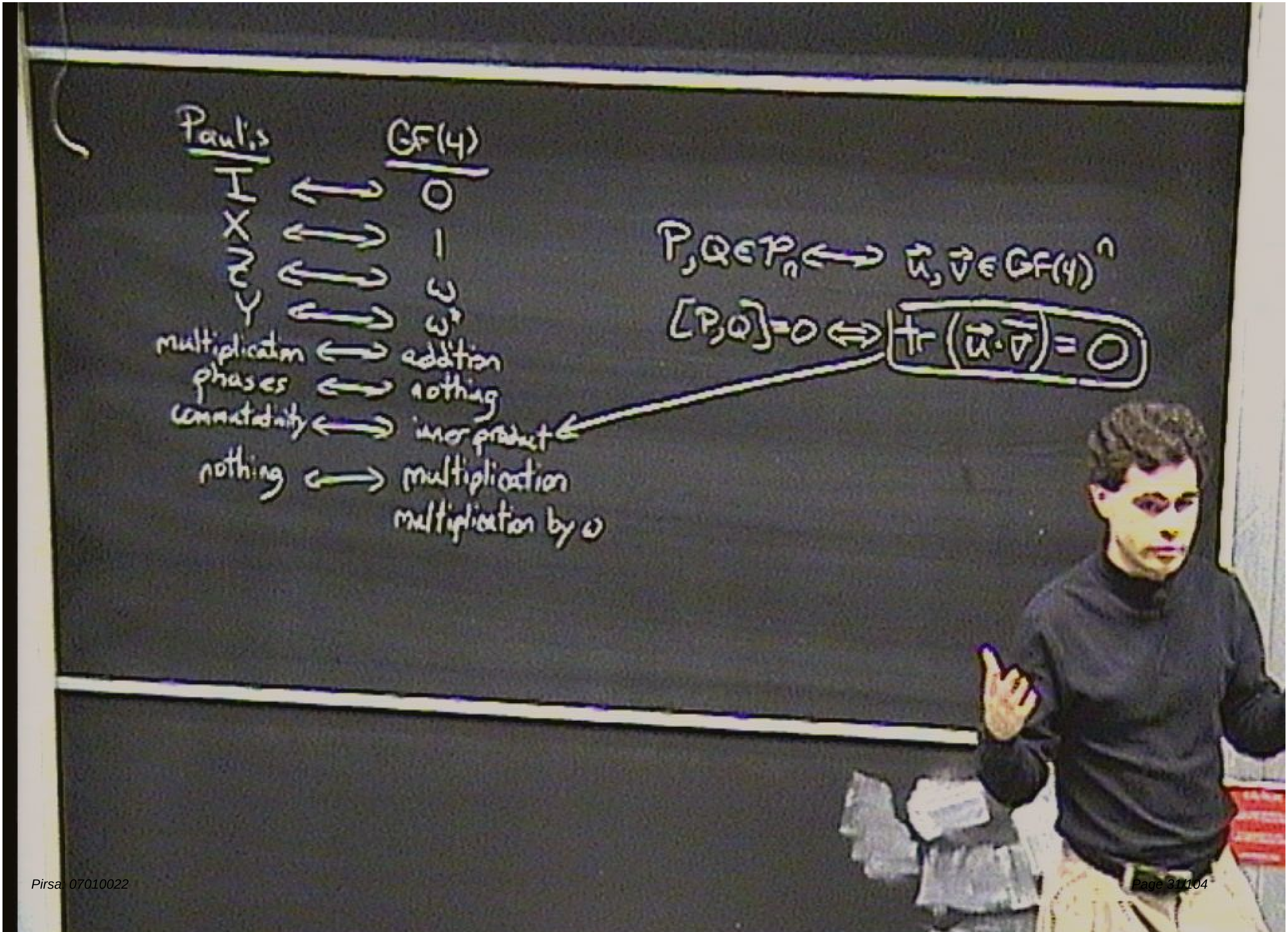
$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$

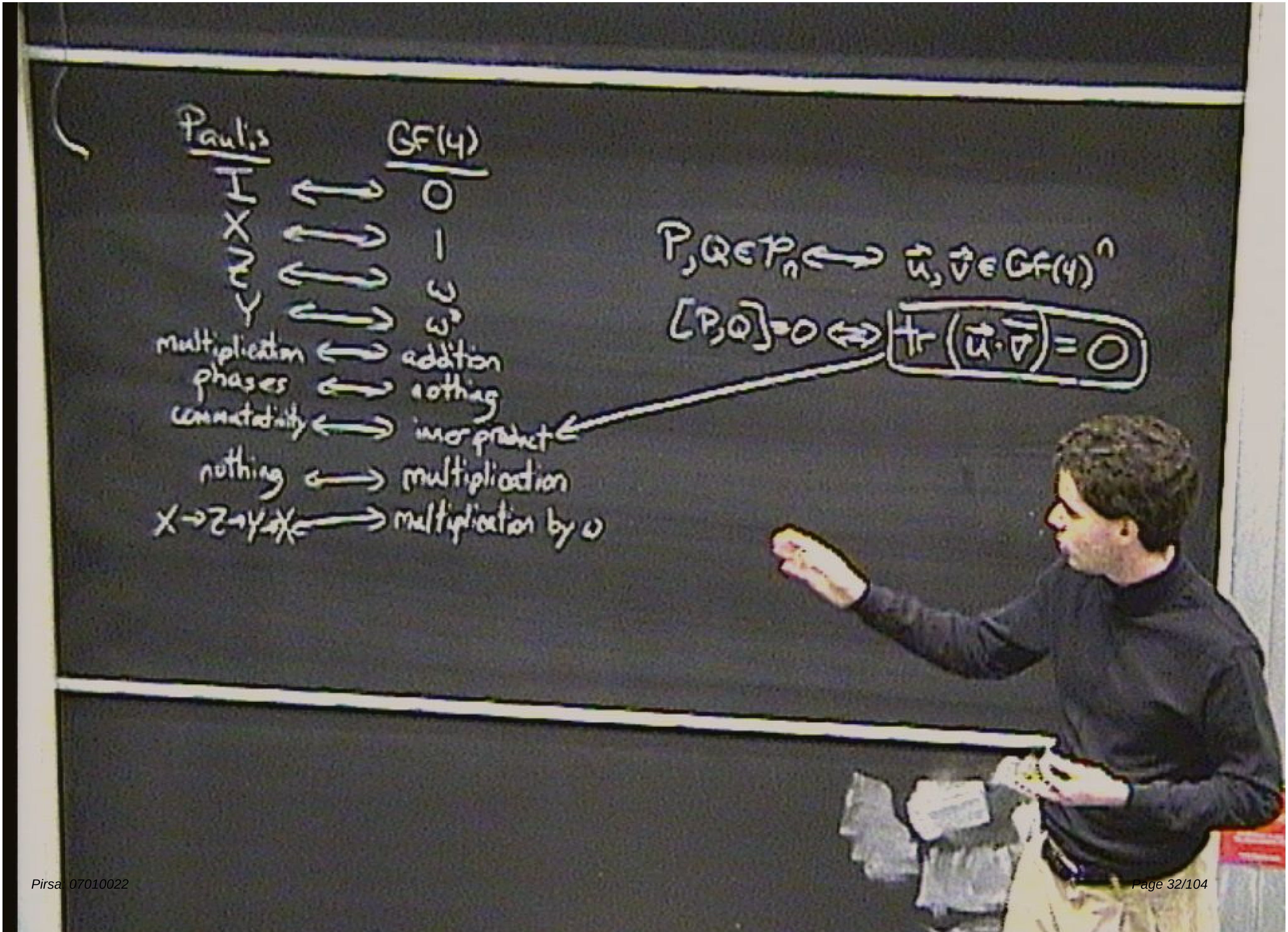
$[P, Q] = 0 \Leftrightarrow \mathrm{tr}(\vec{u} \cdot \overline{\vec{v}}) = 0$

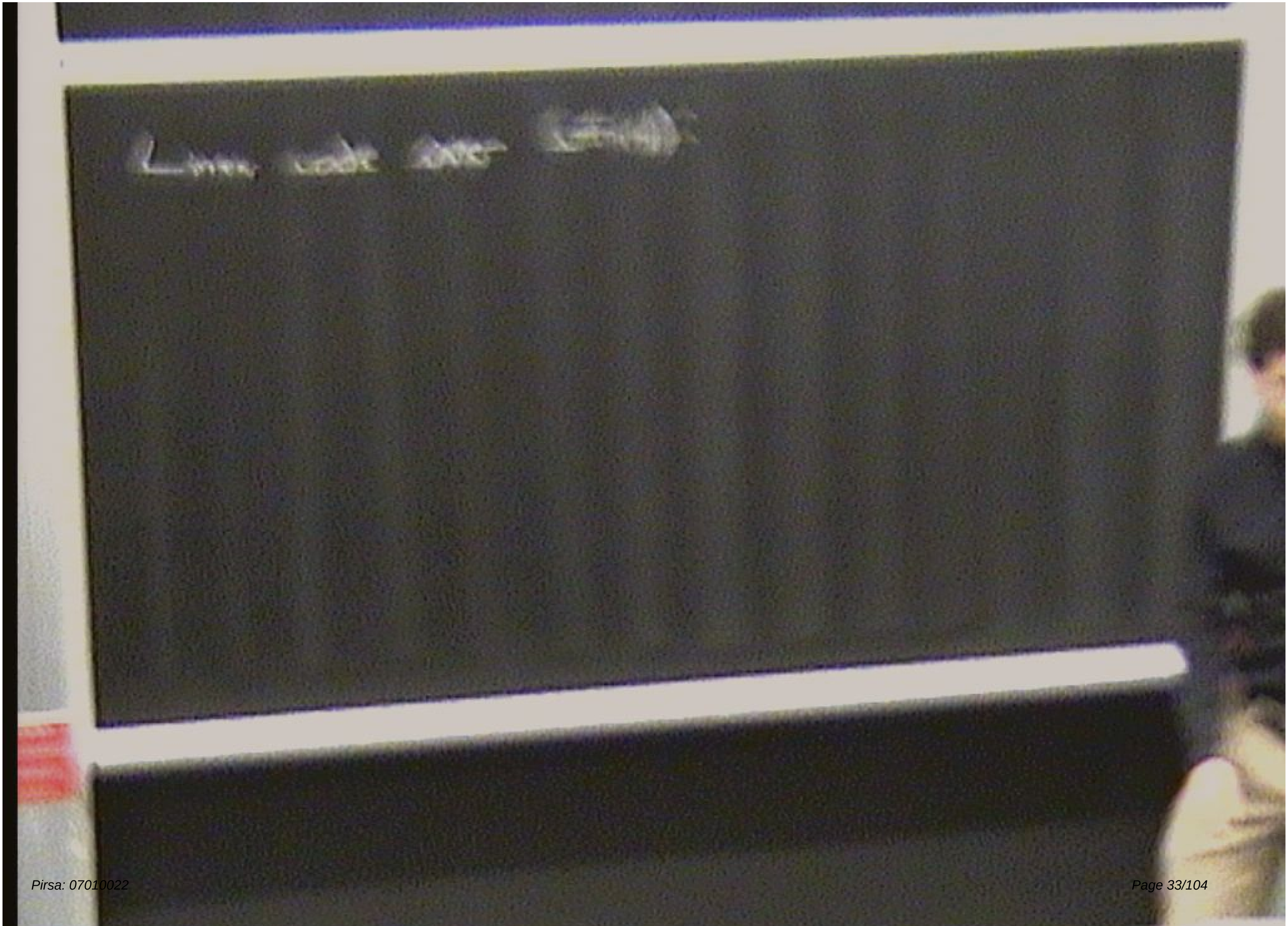
Paulis		GF(4)
I	$\longleftrightarrow$	0
X	$\longleftrightarrow$	1
Z	$\longleftrightarrow$	ω
Y	$\longleftrightarrow$	ω^2
multiplication	$\longleftrightarrow$	addition
phases	$\longleftrightarrow$	nothing
commutativity	$\longleftrightarrow$	inner product multiplication

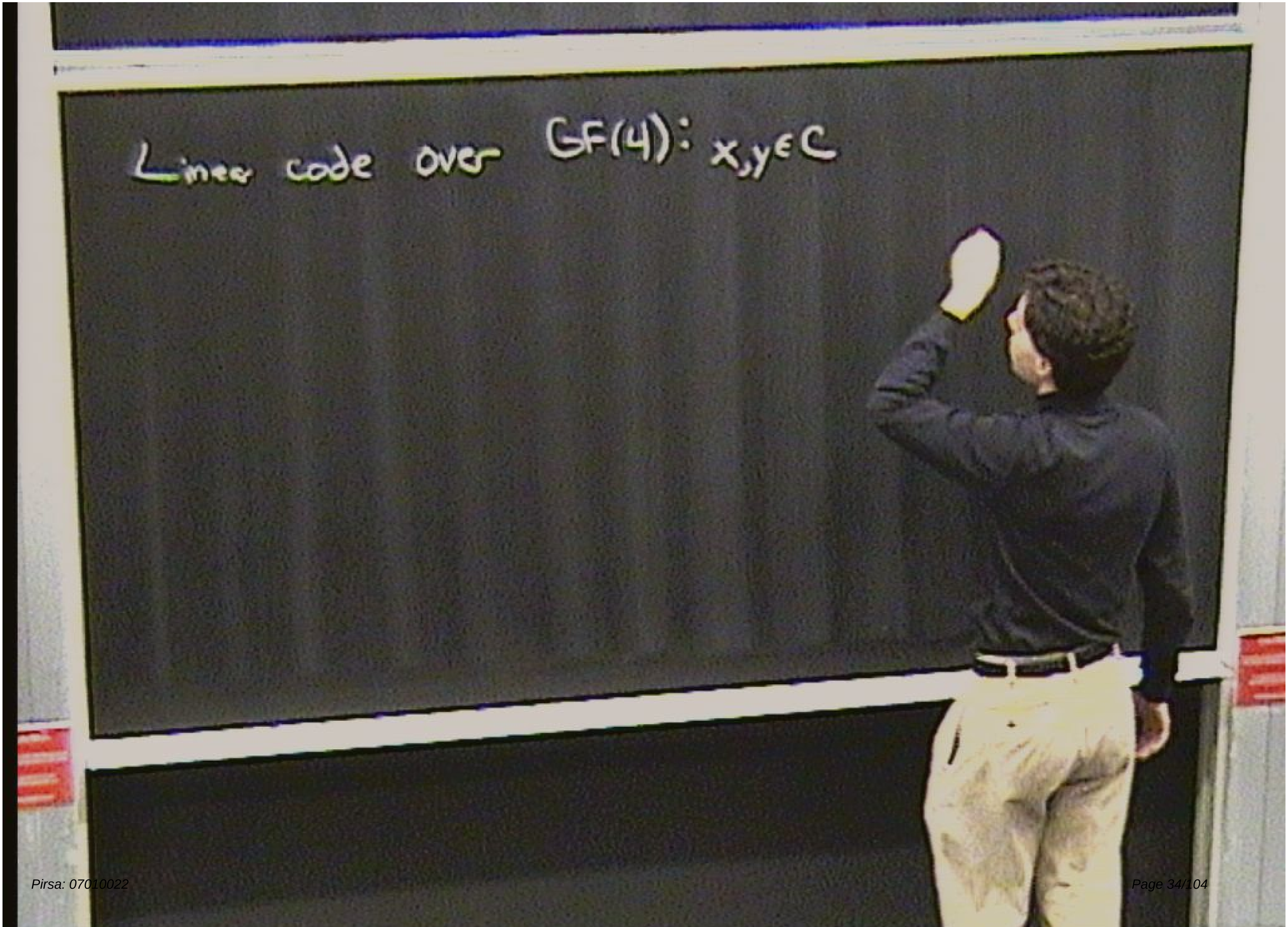
$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$

$[P,Q]=0 \Leftrightarrow \boxed{tr(\vec{u}\cdot\bar{\vec{v}}) = 0}$


Paulis
GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²
multiplication ⟷ addition
phases ⟷ nothing
commutativity ⟷ inner product
nothing ⟷ multiplication
multiplication by ω
$P, Q \in \mathcal{P}_n \longleftrightarrow \vec{u}, \vec{v} \in GF(4)^n$
$[P,Q]=0 \Leftrightarrow \mathrm{tr}(\vec{u}\cdot\vec{v}) = 0$


Paulis
GF(4)
I ⟷ 0
X ⟷ 1
Z ⟷ ω
Y ⟷ ω²
multiplication ⟷ addition
phases ⟷ nothing
commutativity ⟷ inner product
nothing ⟷ multiplication
X → Z → Y → X ⟷ multiplication by ω
P, Q ∈ 𝒫ₙ ⟷ u⃗, v⃗ ∈ GF(4)ⁿ
[P, Q] = 0 ⟷ tr(u⃗ · v⃗) = 0




Linear code over GF(4): x,y∈C

Linear code over $GF(4)$: $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \alpha \vec{y} \in C$, $\alpha \in GF(4)$

Linear code over $GF(4)$: $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \alpha \vec{y} \in C$, $\alpha \in GF(4)$

Additive code over $GF(4)$: $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \vec{y} \in C$

Linear code over $GF(4)$: $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C$, $\alpha\in GF(4)$

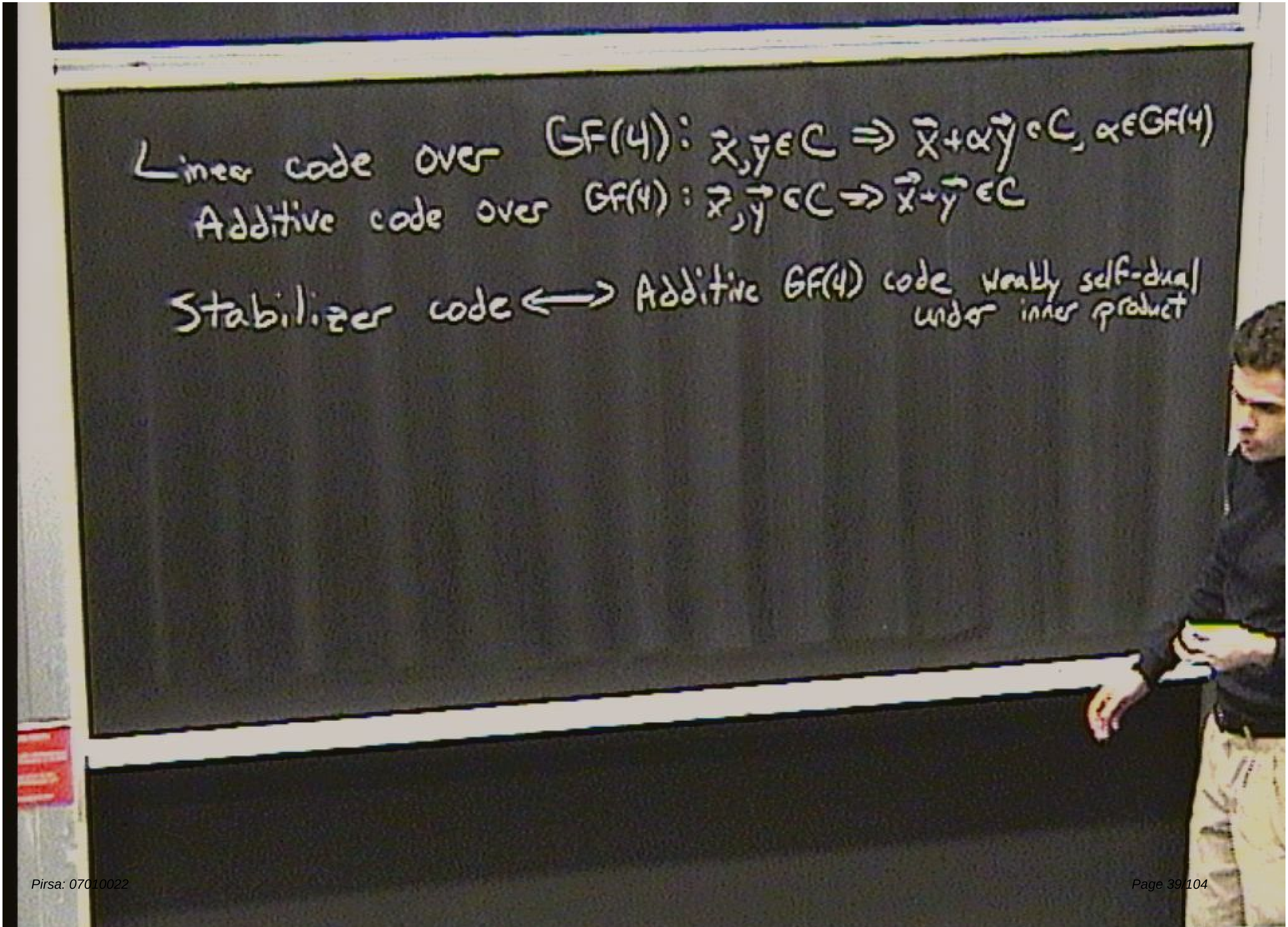
Additive code over $GF(4)$: $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

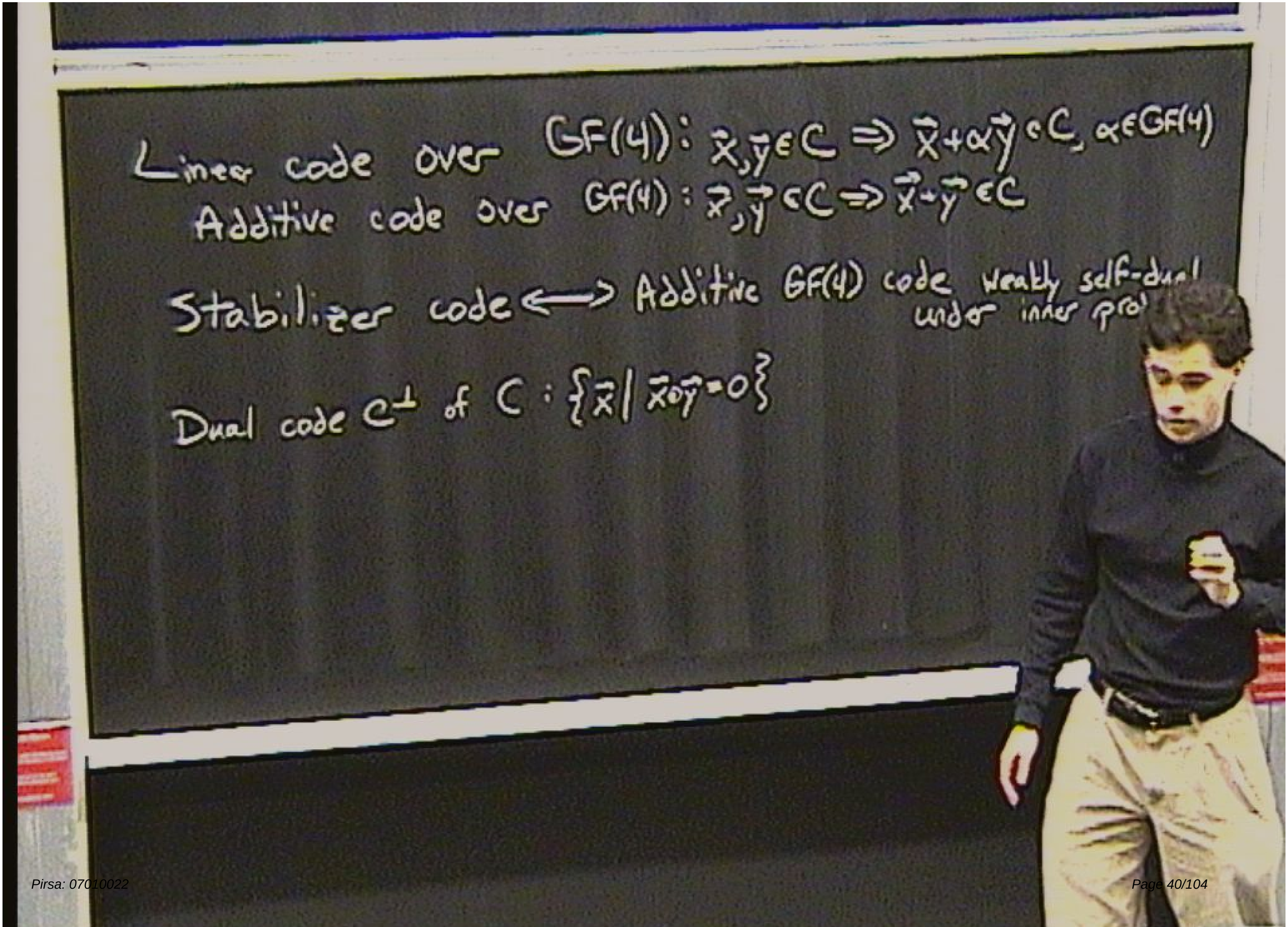
Stabilizer code $\longleftrightarrow$

Linear code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C,\ \alpha\in GF(4)$

Additive code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

Stabilizer code $\longleftrightarrow$ Additive GF(4) code


Linear code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C$, $\alpha\in GF(4)$
Additive code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$
Stabilizer code $\longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product


Linear code over GF(4): $\vec{x},\vec{y} \in C \Rightarrow \vec{x}+\alpha\vec{y} \in C$, $\alpha \in GF(4)$
Additive code over GF(4): $\vec{x},\vec{y} \in C \Rightarrow \vec{x}+\vec{y} \in C$
Stabilizer code $\longleftrightarrow$ Additive GF(4) code weakly self-dual under inner pro
Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x} \circ \vec{y} = 0\}$

Linear code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C$, $\alpha\in GF(4)$

Additive code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x}\odot\vec{y}=0 \ \forall \vec{y}\in C\}$, $\vec{x}\odot\vec{y} = tr(\vec{x}\cdot\bar{\vec{y}})$

Linear code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \alpha \vec{y} \in C$, $\alpha \in GF(4)$

Additive code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \vec{y} \in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x} \odot \vec{y} = 0 \ \forall \vec{y} \in C\}$, $\vec{x} \odot \vec{y} = \mathrm{tr}(\vec{x} \cdot \bar{\vec{y}})$

Weakly self-dual: $C \subseteq C^{\perp}$

Linear code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C$, $\alpha\in GF(4)$

Additive code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x}\circledast\vec{y}=0\ \forall \vec{y}\in C\}$, $\vec{x}\circledast\vec{y}=\mathrm{tr}(\vec{x}\cdot\bar{\vec{y}})$

Weakly self-dual: $C\subseteq C^{\perp}$ $\Leftrightarrow$ stabilizer Abelian

Linear code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \alpha \vec{y} \in C$, $\alpha \in GF(4)$

Additive code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \vec{y} \in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x} \circ \vec{y} = 0 \ \forall \vec{y} \in C\}$, $\vec{x} \circ \vec{y} = tr(\vec{x} \cdot \bar{\vec{y}})$

Weakly self-dual: $C \subseteq C^{\perp} \Leftrightarrow$ Stabilizer Abelian

$N(S) \Leftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Linear code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \alpha \vec{y} \in C$, $\alpha \in GF(4)$

Additive code over GF(4): $\vec{x}, \vec{y} \in C \Rightarrow \vec{x} + \vec{y} \in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x} \mid \vec{x} \circ \vec{y} = 0 \ \forall \vec{y} \in C\}$, $\vec{x} \circ \vec{y} = \mathrm{tr}(\vec{x} \cdot \bar{\vec{y}})$

Weakly self-dual: $C \subseteq C^{\perp} \Leftrightarrow$ Stabilizer Abelian

$N(S) \Longleftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Note:

Linear code over $GF(4)$: $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C$, $\alpha\in GF(4)$

Additive code over $GF(4)$: $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

Stabilizer code $\Longleftrightarrow$ Additive $GF(4)$ code weakly self-dual under inner product

Dual code $C^{\perp}$ of C: $\{\vec{x}\,|\,\vec{x}\odot\vec{y}=0\ \forall\vec{y}\in C\}$, $\vec{x}\odot\vec{y}=\mathrm{tr}(\vec{x}\cdot\vec{\bar{y}})$

Weakly self-dual: $C\subseteq C^{\perp}$ $\Longleftrightarrow$ Stabilizer Abelian

$N(S)\Longleftrightarrow C^{\perp}$ Distance = min wt. $x\,|\,x\in C^{\perp}\setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy

$N(S) \longleftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy.

Hamming codes over GF(4):

$N(S) \longleftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy.

Hamming codes over GF(4): Linear codes

$N(S) \longleftrightarrow C^\perp$ Distance = min wt. $x \mid x \in C^\perp \setminus C$

Note: Distance can be larger than distance of $C^\perp$ because of degeneracy

Hamming codes over GF(4): Linear codes

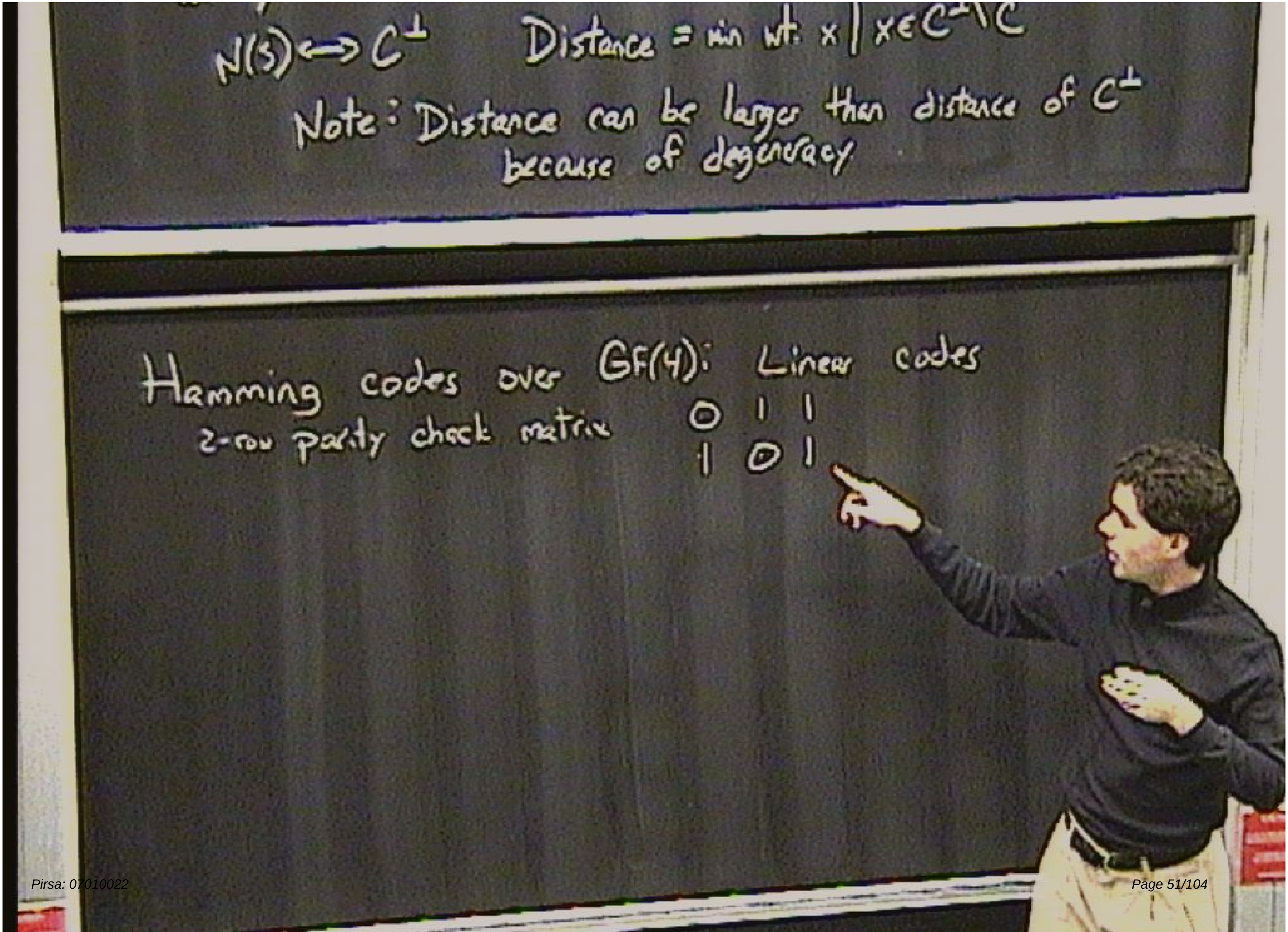
2-row parity check matrix

$N(S) \longleftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy.

Hamming codes over GF(4): Linear codes

2-row parity check matrix
$$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$$


$N(S) \Longleftrightarrow C^{\perp}$
Distance = min wt. $x \mid x \in C^{\perp} \setminus C$
Note: Distance can be larger than distance of $C^{\perp}$
because of degeneracy
Hamming codes over GF(4): Linear codes
2-row parity check matrix
0 1 1
1 0 1

$N(S) \longleftrightarrow C^{\perp}$ Distance $=$ min wt. $x \mid x \in C^{\perp} \setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy.

Hamming codes over $GF(4)$: Linear codes

2-row parity check matrix
$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix}$$

$N(S) \longleftrightarrow C^\perp$ Distance = min wt. $x \mid x \in C^\perp \setminus C$

Note: Distance can be larger than distance of $C^\perp$ because of degeneracy

Hamming codes over GF(4): Linear codes

2-row parity check matrix

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix} \qquad [5,3,3]_4$$

$N(S) \Longleftrightarrow C^{\perp}$ Distance = min wt. $x \mid x \in C^{\perp} \setminus C$

Note: Distance can be larger than distance of $C^{\perp}$ because of degeneracy.

Hamming codes over GF(4): Linear codes

2-row parity check matrix

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix} \qquad [5,3,3]_4$$

Convert to stabilizer code

$N(S) \Longleftrightarrow C^\perp$ Distance = min wt. $x \mid x \in C^\perp \setminus C$

Note: Distance can be larger than distance of $C^\perp$ because of degeneracy

Hamming codes over GF(4): Linear codes

2-row parity check matrix $\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix}$ $[5,3,3]_4$

Convert to stabilizer code linear $\rightarrow$ additive

Linear code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\alpha\vec{y}\in C,\ \alpha\in GF(4)$

Additive code over GF(4): $\vec{x},\vec{y}\in C \Rightarrow \vec{x}+\vec{y}\in C$

Stabilizer code $\Longleftrightarrow$ Additive GF(4) code weakly self-dual under inner product

Dual code $C^\perp$ of C: $\{\vec{x} \mid \vec{x}\circ\vec{y}=0\ \forall \vec{y}\in C\}$, $\vec{x}\circ\vec{y}=\mathrm{tr}(\vec{x}\cdot\bar{\vec{y}})$

Weakly self-dual: $C\subseteq C^\perp \Longleftrightarrow$ Stabilizer Abelian

$N(S)\Longleftrightarrow C^\perp$ Distance = min wt. $x \mid x\in C^\perp\setminus C$

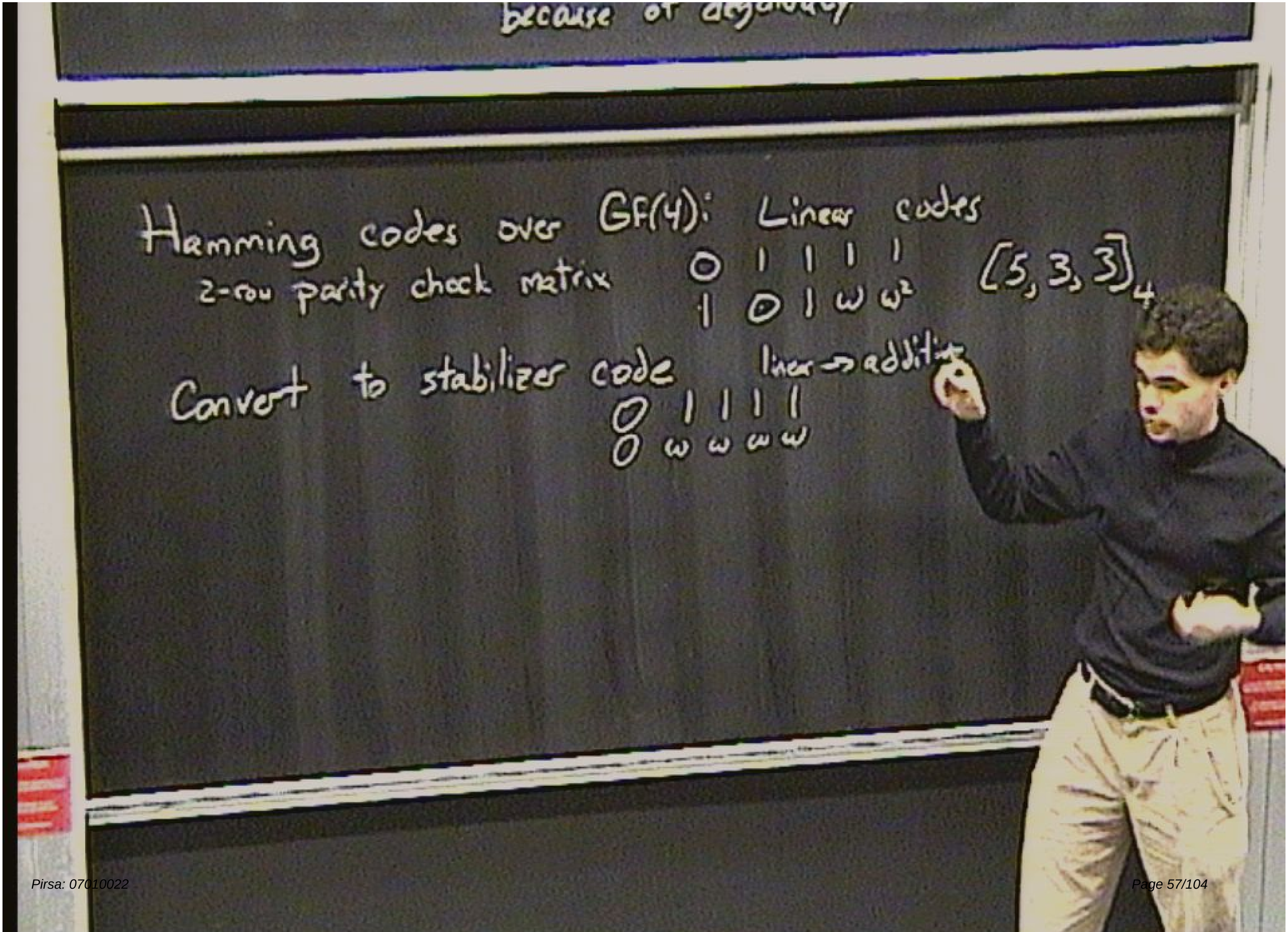
Note: Distance can be larger than distance of $C^\perp$ because of degeneracy

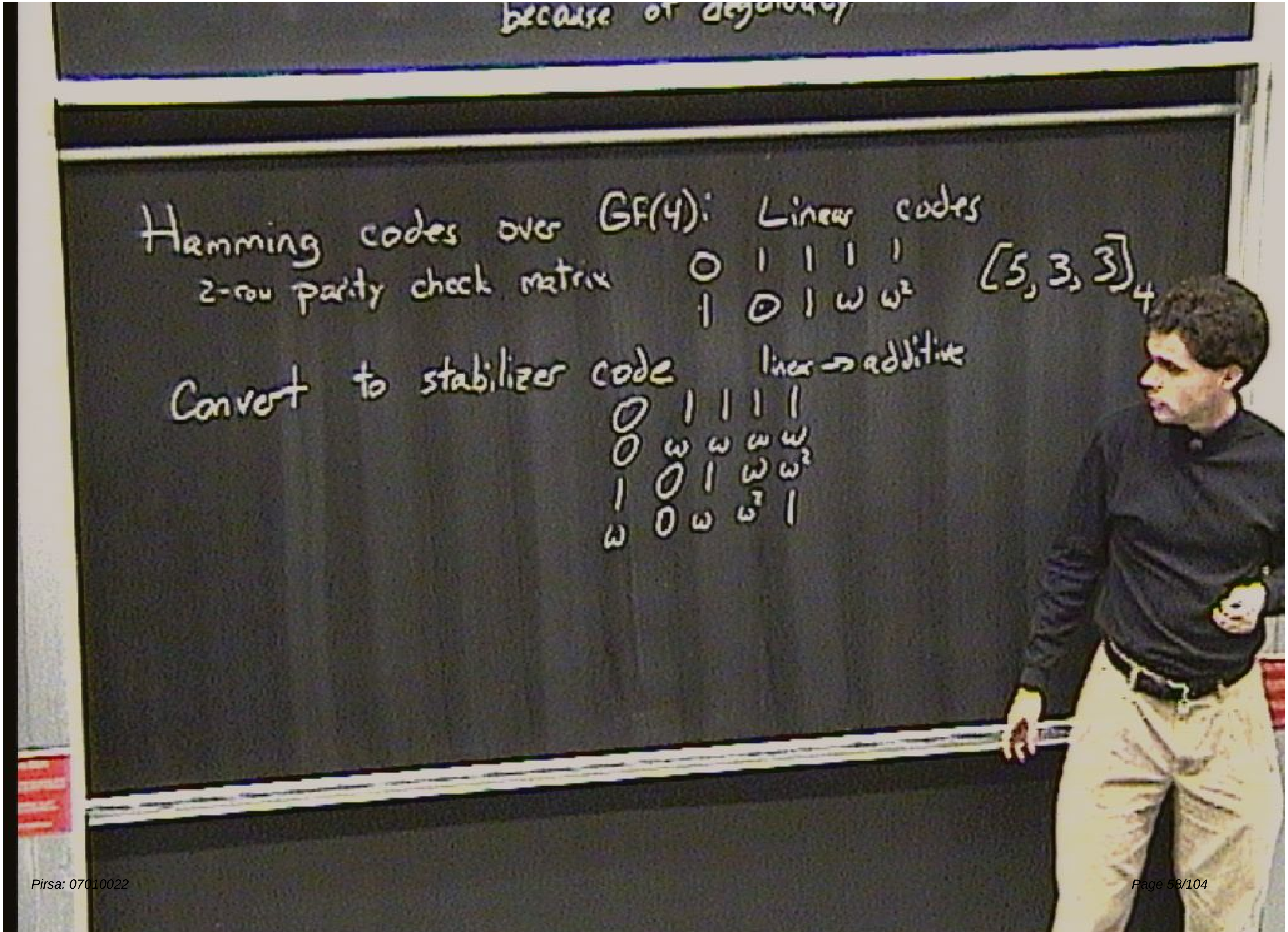
Hamming codes over GF(4): Linear codes

2-row parity check matrix $\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix}$ $[5,3,3]_4$

linear $\Rightarrow$ additive

Convert to stabilizer code


because of
Hamming codes over GF(4): Linear codes
2-row parity check matrix
0 1 1 1 1
1 0 1 ω ω²
[5, 3, 3]₄
Convert to stabilizer code
linear → additi
0 1 1 1 1
0 ω ω ω ω


because of
Hamming codes over GF(4): Linear codes
2-row parity check matrix
0 1 1 1 1
1 0 1 ω ω²
[5, 3, 3]₄
Convert to stabilizer code
linear → additive
0 1 1 1 1
0 ω ω ω ω
1 0 1 ω ω²
ω 0 ω ω² 1

because of degeneracy

Hamming codes over GF(4): Linear codes

2-row parity check matrix

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix} \qquad [5,3,3]_4$$

Convert to stabilizer code

linear → additive

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 0 & \omega & \omega & \omega & \omega \\ 0 & 0 & 1 & \omega & \omega^2 \\ 1 & 0 & 1 & \omega^2 & 1 \\ \omega & 0 & \omega & \omega^2 & 1 \end{matrix} \longleftrightarrow \begin{matrix} I X X X X \\ I Z Z Z Z \\ X I X Z Y \\ Z I Z Y I \end{matrix}$$

because of degeneracy

Hamming codes over GF(4): Linear codes

2-row parity check matrix

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix} \qquad [5,3,3]_4$$

Convert to stabilizer code   linear → additive

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 0 & \omega & \omega & \omega & \omega \\ 1 & 0 & 1 & \omega & \omega^2 \\ \omega & 0 & \omega & \omega^2 & 1 \end{matrix} \longleftrightarrow \begin{matrix} I & X & X & X & X \\ I & Z & Z & Z & Z \\ X & I & X & Z & Y \\ Z & I & Z & Y & X \end{matrix}$$

$[[5,1,$

because of degeneracy

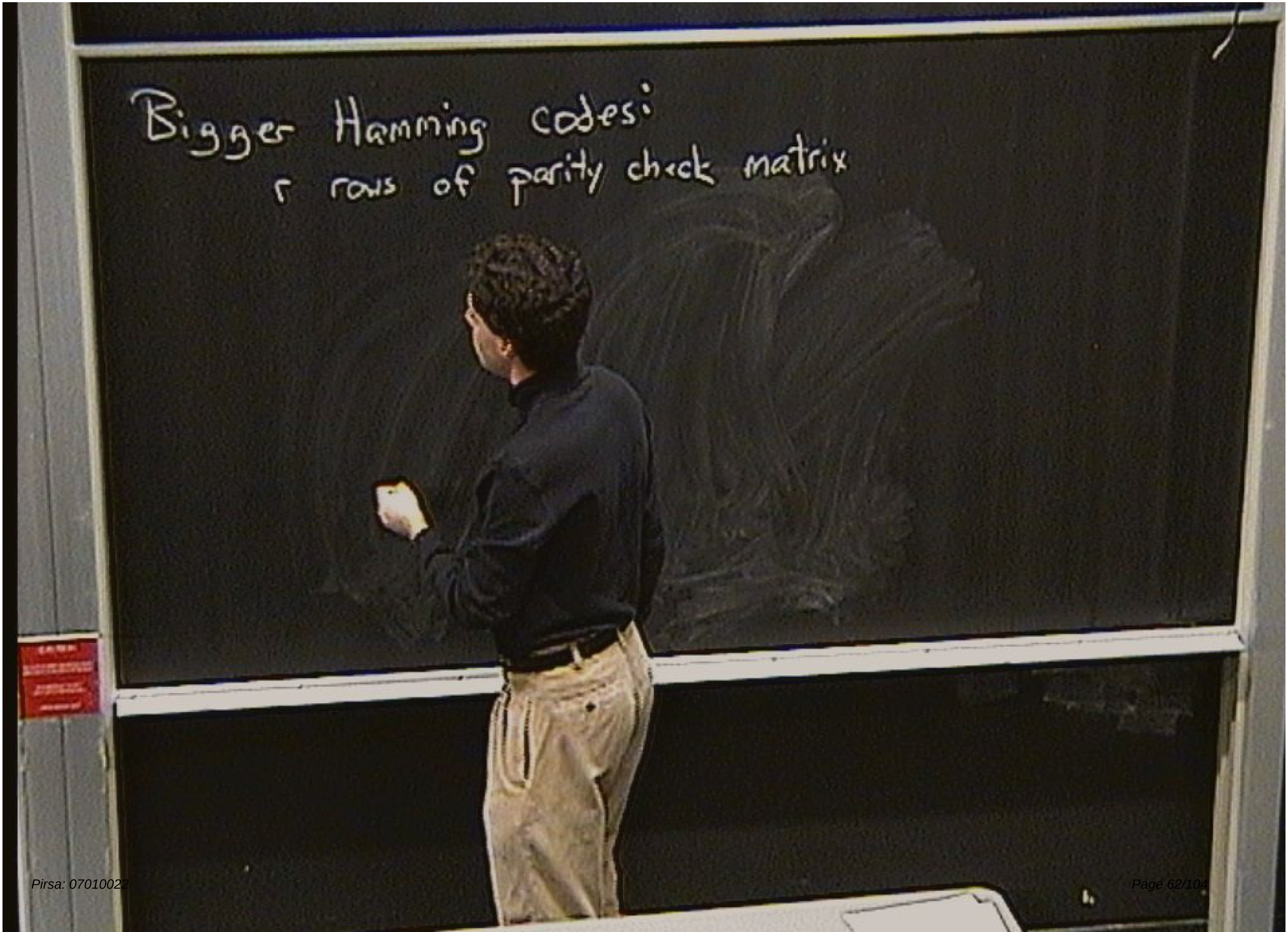
Hamming codes over GF(4): Linear codes

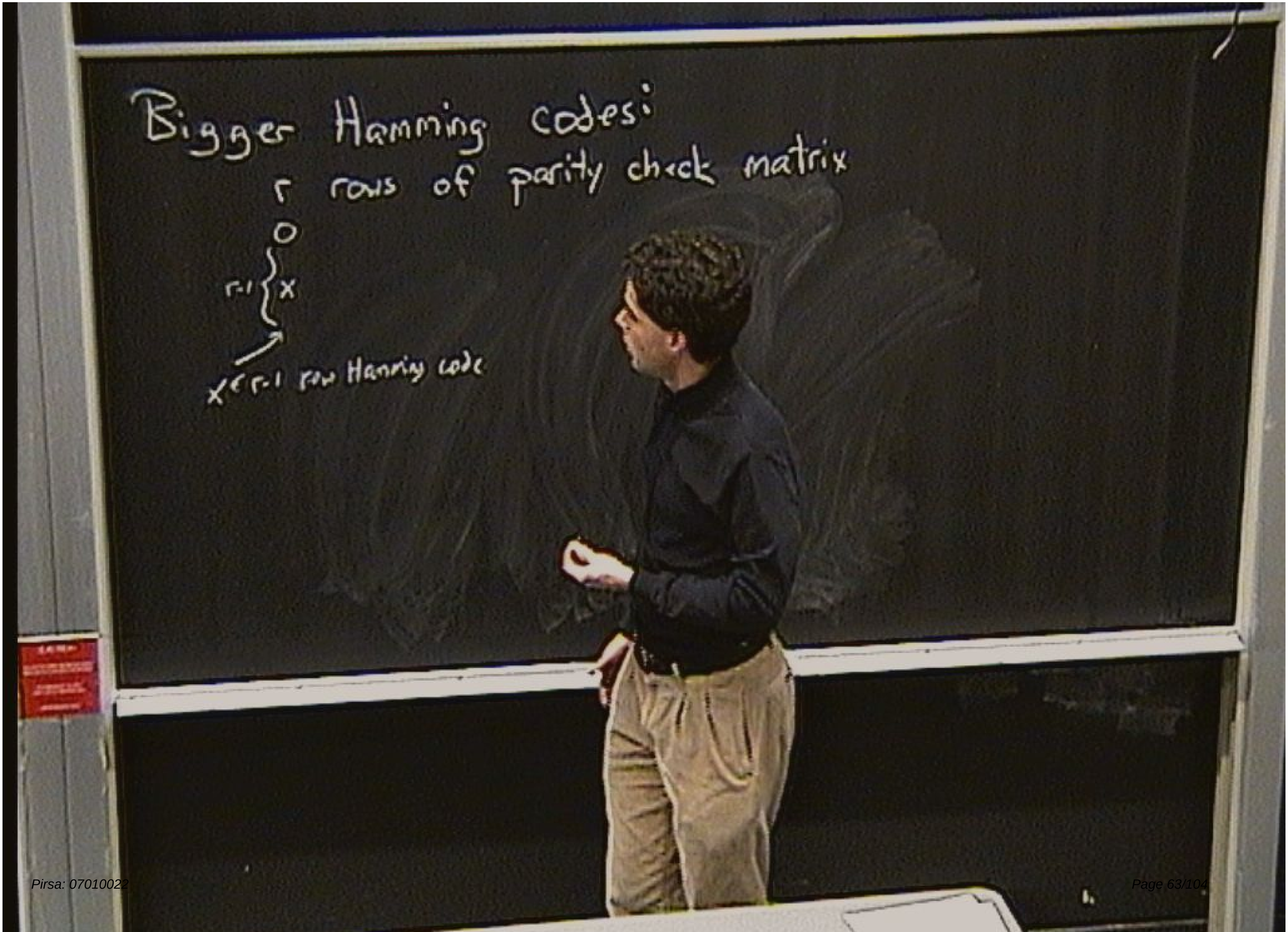
2-row parity check matrix
$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{matrix} \qquad [5,3,3]_4$$

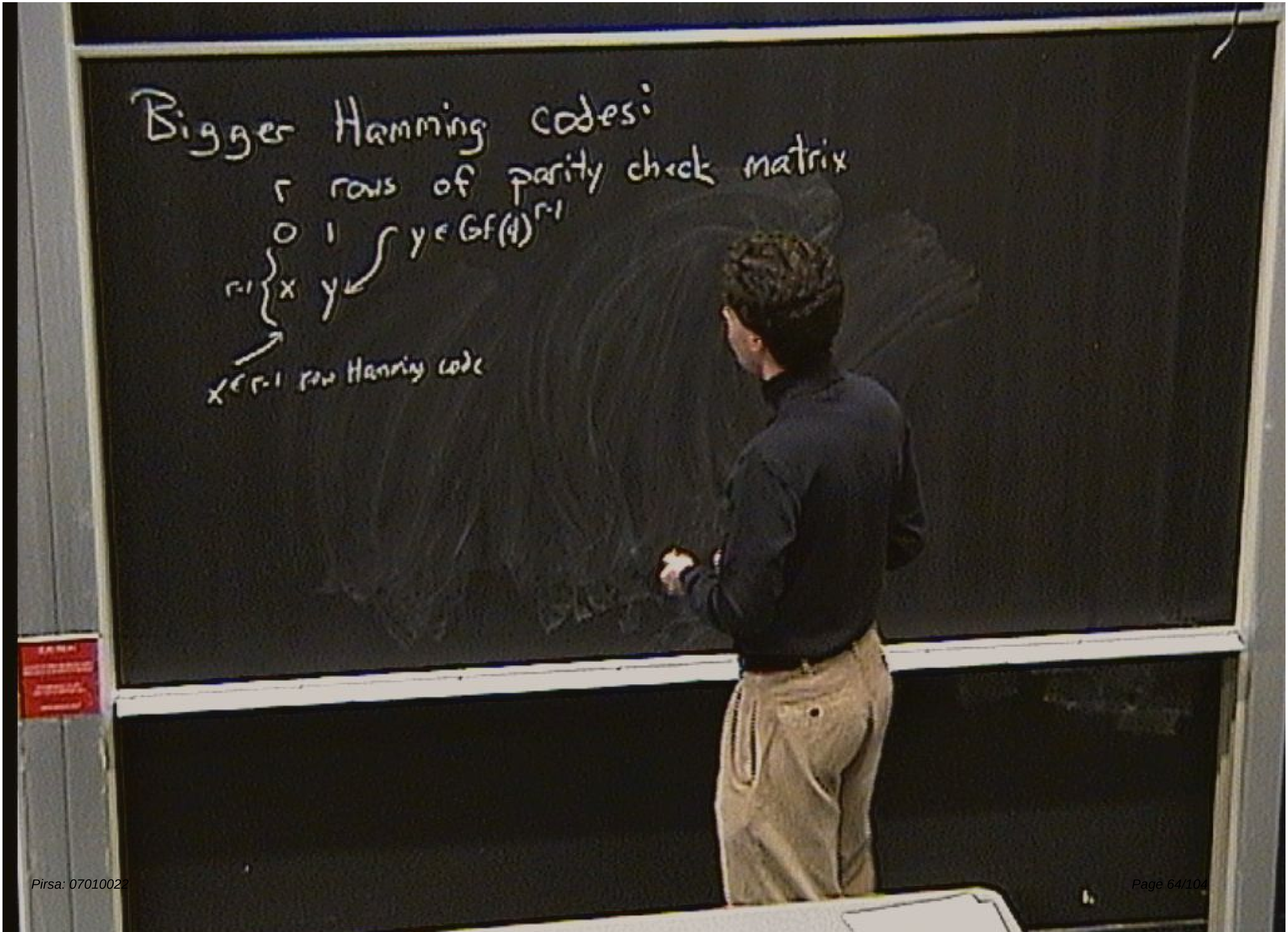
Convert to stabilizer code   linear $\Rightarrow$ additive

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 0 & \omega & \omega & \omega & \omega \\ 1 & 0 & 1 & \omega & \omega^2 \\ \omega & 0 & \omega & \omega^2 & 1 \end{matrix} \longleftrightarrow \begin{matrix} I & X & X & X & X \\ I & Z & Z & Z & Z \\ X & I & X & Z & Y \\ Z & I & Z & Y & X \end{matrix}$$

$[[5,1,3]]$


Bigger Hamming codes:
r rows of parity check matrix


Bigger Hamming codes:
r rows of parity check matrix
0
r-1 { x
x ∈ r-1 row Hamming code


Bigger Hamming codes:
r rows of parity check matrix
0 1 y ∈ GF(q)^{r-1}
r-1 { x y
x ∈ r-1 row Hamming code

Bigger Hamming codes:

r rows of parity check matrix

$$\begin{array}{c} \\ r-1\left\{\begin{array}{c}\\ \\ \end{array}\right. \end{array} \begin{array}{cc} 0 & 1 \\ x & y \end{array} \qquad y \in GF(4)^{r-1}$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 \ldots + 4^{r-1}$$

$$= \frac{4^r - 1}{3}$$

Bigger Hamming codes:

r rows of parity check matrix

$$\begin{array}{cc} & \begin{matrix} 0 & 1 \end{matrix} \\ r-1\left\{\right. & \begin{matrix} x & y \end{matrix} \end{array} \qquad y \in GF(4)^{r-1}$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$$

$$= \boxed{\frac{4^r - 1}{3}}$$

$$[(4^r-1)/3,\ (4^r-1)/3 - r]$$

Bigger Hamming codes:

r rows of parity check matrix

$$\begin{array}{c} \\ r-1\left\{\right. \end{array}\begin{array}{cc} 0 & 1 \\ x & y \end{array} \qquad y \in GF(4)^{r-1}$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1} = \boxed{\frac{4^r - 1}{3}}$$

$$[(4^r-1)/3,\ (4^r-1)/3 - r,\ 3]_4$$

Bigger Hamming codes:

r rows of parity check matrix

$$r-1\left\{\begin{array}{cc} 0 & 1 \\ x & y \end{array}\right. \qquad y \in GF(4)^{r-1}$$

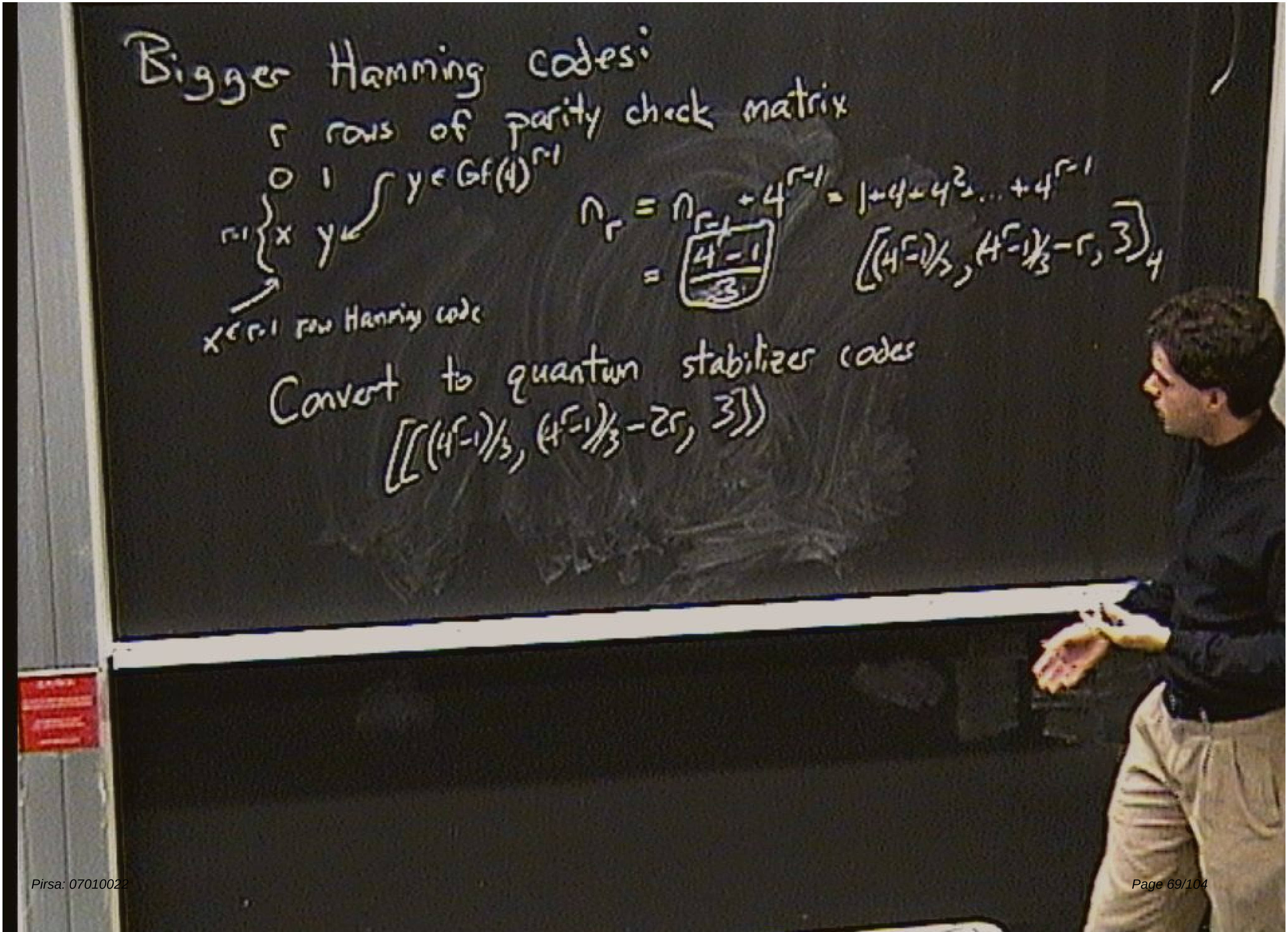
$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$$
$$= \boxed{\frac{4^r - 1}{3}}$$

$$[(4^r-1)/3,\ (4^r-1)/3 - r,\ 3]_4$$

Convert to quantum stabilizer codes

$$[[(4^r-1)/3,$$


Bigger Hamming codes:
r rows of parity check matrix
0 1 y ∈ GF(4)^(r-1)
r-1 {x y
x ∈ r-1 row Hamming code
n_r = n_(r-1) + 4^(r-1) = 1+4+4^2 ... +4^(r-1)
= (4^r - 1)/3
[(4^r-1)/3, (4^r-1)/3 - r, 3]_4
Convert to quantum stabilizer codes
[[(4^r-1)/3, (4^r-1)/3 - 2r, 3]]

$r-1\{x \quad y$

$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$

$= \boxed{\frac{4^r - 1}{3}}$

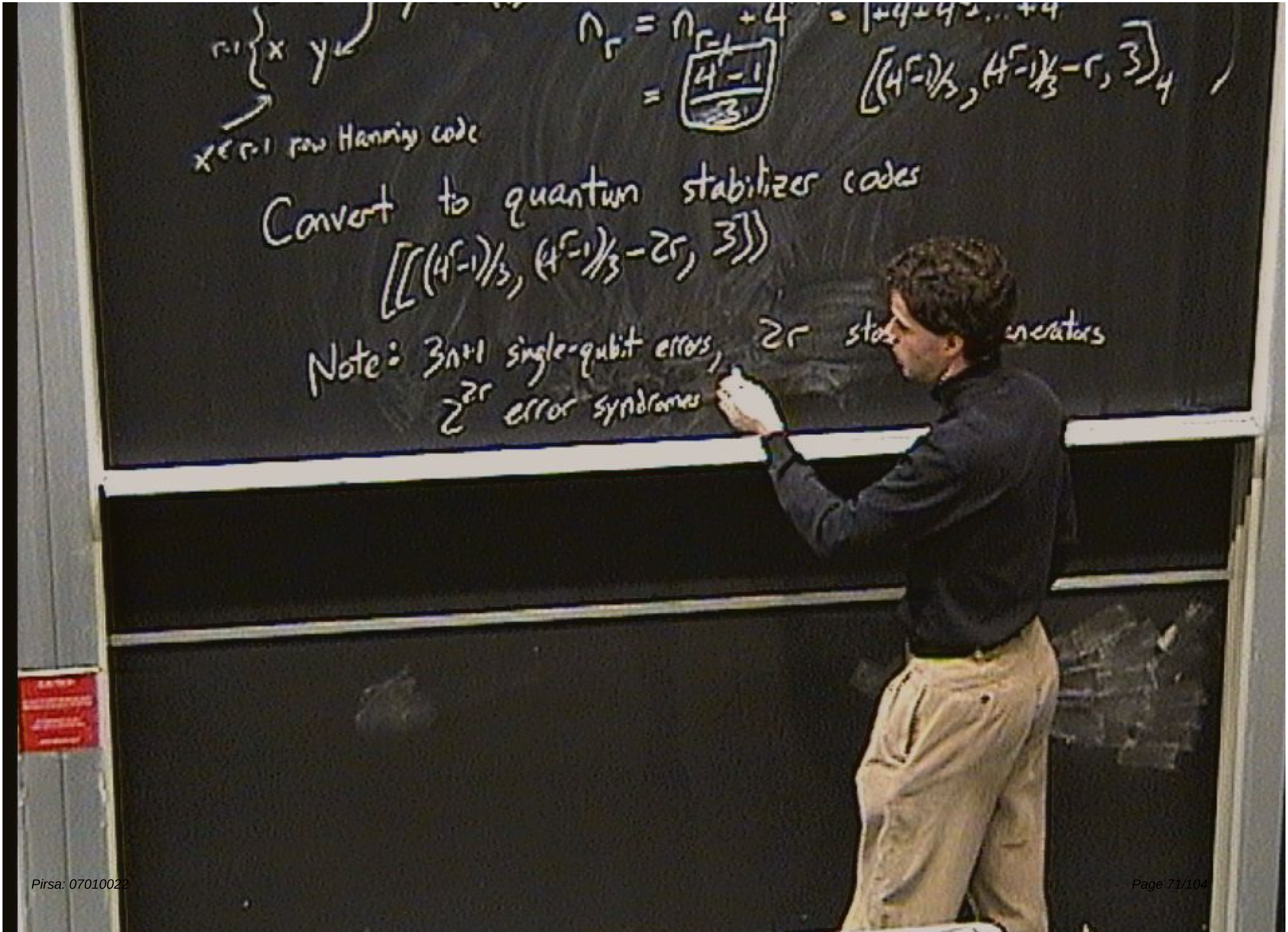
$[(4^r-1)/3, (4^r-1)/3 - r, 3]_4$

$x \in r-1$ row Hamming code

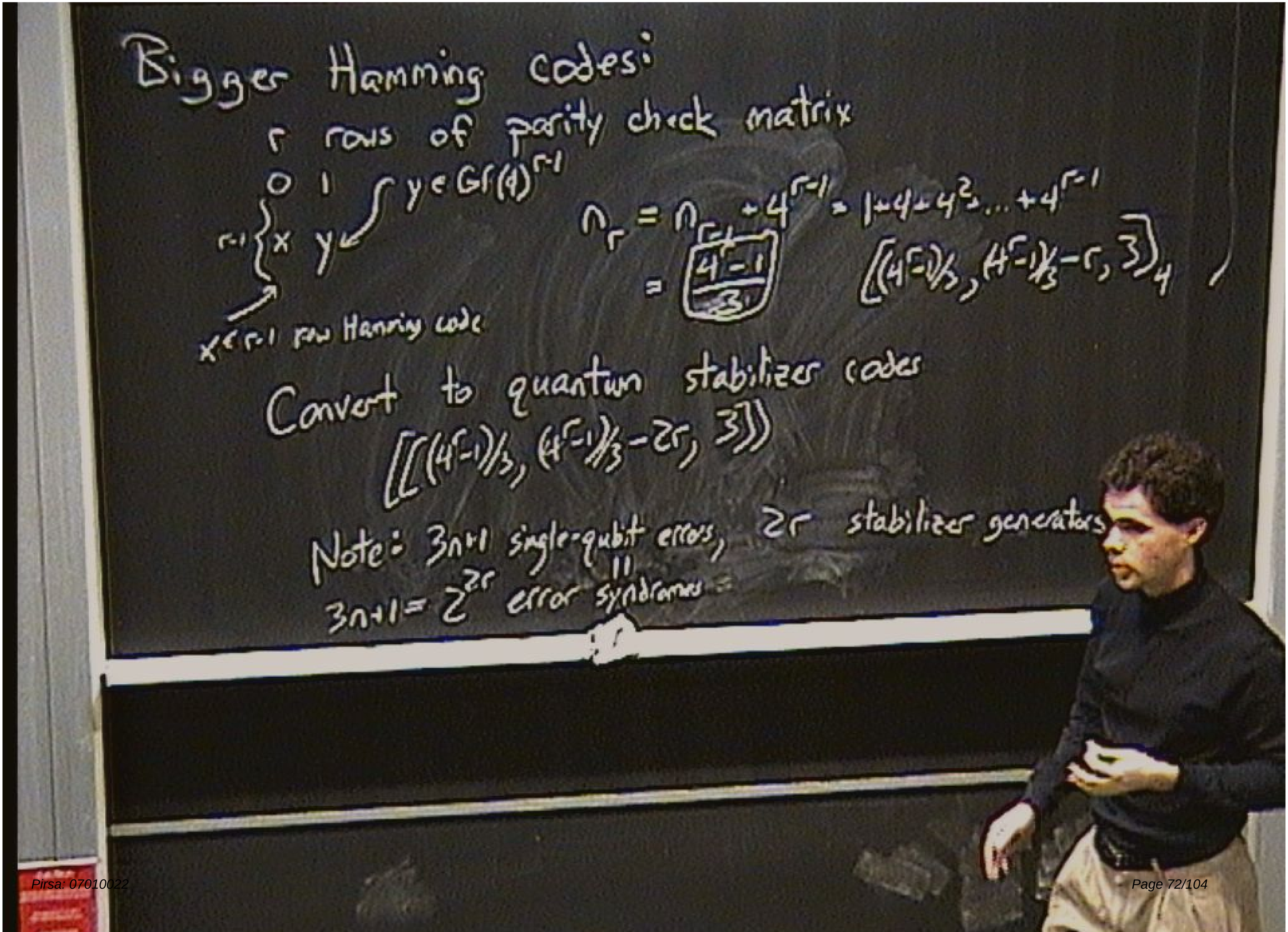
Convert to quantum stabilizer codes

$[[(4^r-1)/3, (4^r-1)/3 - 2r, 3]]$

Note: $3n+1$ single-qubit errors, 2^k encoded states



r-1 {x y
n_r = n_{r-1} + 4^{r-1} = 1+4+4^2...+4
= (4^r - 1)/3
((4^r-1)/3, (4^r-1)/3 - r, 3)_4
x ∈ r-1 row Hamming code
Convert to quantum stabilizer codes
[[(4^r-1)/3, (4^r-1)/3 - 2r, 3]]
Note: 3n+1 single-qubit errors, 2r sta enerators
2^{2r} error syndromes


Bigger Hamming codes:
r rows of parity check matrix
0 1 y ∈ GF(4)^(r-1)
r-1 { x y
x ∈ r-1 row Hamming code
n_r = n_(r-1) + 4^(r-1) = 1+4+4^2+...+4^(r-1)
= (4^r - 1)/3
[(4^r-1)/3, (4^r-1)/3 - r, 3]_4
Convert to quantum stabilizer codes
[[(4^r-1)/3, (4^r-1)/3 - 2r, 3]]
Note: 3n+1 single-qubit errors, 2r stabilizer generators
3n+1 = 2^(2r) error syndromes

Bigger Hamming codes:

r rows of parity check matrix

$$
\begin{array}{c}
\\
{\scriptstyle r-1}\left\{\begin{array}{cc} 0 & 1 \\ x & y \end{array}\right.
\end{array}
\qquad y \in GF(4)^{r-1}
$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$$

$$= \boxed{\frac{4^r - 1}{3}}$$

$[(4^r-1)/3,\ (4^r-1)/3 - r,\ 3]_4$

$r=2$ $[[5,1,3]]$

$r=3$ $[[21,15,3]]$

Convert to quantum stabilizer codes

$[[(4^r-1)/3,\ (4^r-1)/3 - 2r,\ 3]]$

Note: $3n+1$ single-qubit errors, $2r$ stabilizer generators

$3n+1 = 2^{2r}$ error syndromes "Perfect code"

Bigger Hamming codes:

r rows of parity check matrix

$$\begin{array}{c} \\ r-1\left\{\begin{array}{cc} 0 & 1 \\ x & y \end{array}\right. \end{array} \qquad y \in GF(4)^{r-1}$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$$

$$= \boxed{\frac{4^r - 1}{3}}$$

$[(4^r-1)/3,\ (4^r-1)/3 - r,\ 3]_4$

$r=2$ $[[5,1,3]]$

$r=3$ $[[21,15,3]]$

$r=4$ $[[$

Convert to quantum stabilizer codes

$[[(4^r-1)/3,\ (4^r-1)/3 - 2r,\ 3]]$

Note: $3n+1$ single-qubit errors, $2r$ stabilizer generators

$3n+1 = 2^{2r}$ error syndromes "Perfect code"

Bigger Hamming codes:

r rows of parity check matrix

$$r-1\left\{\begin{matrix} 0 & 1 \\ x & y \end{matrix}\right. \qquad y \in GF(4)^{r-1}$$

$x \in r-1$ row Hamming code

$$n_r = n_{r-1} + 4^{r-1} = 1 + 4 + 4^2 + \dots + 4^{r-1}$$

$$= \boxed{\frac{4^r - 1}{3}}$$

$$[(4^r-1)/3,\ (4^r-1)/3 - r,\ 3]_4$$

$r=2$ $[[5,1,3]]$

$r=3$ $[[21,15,3]]$

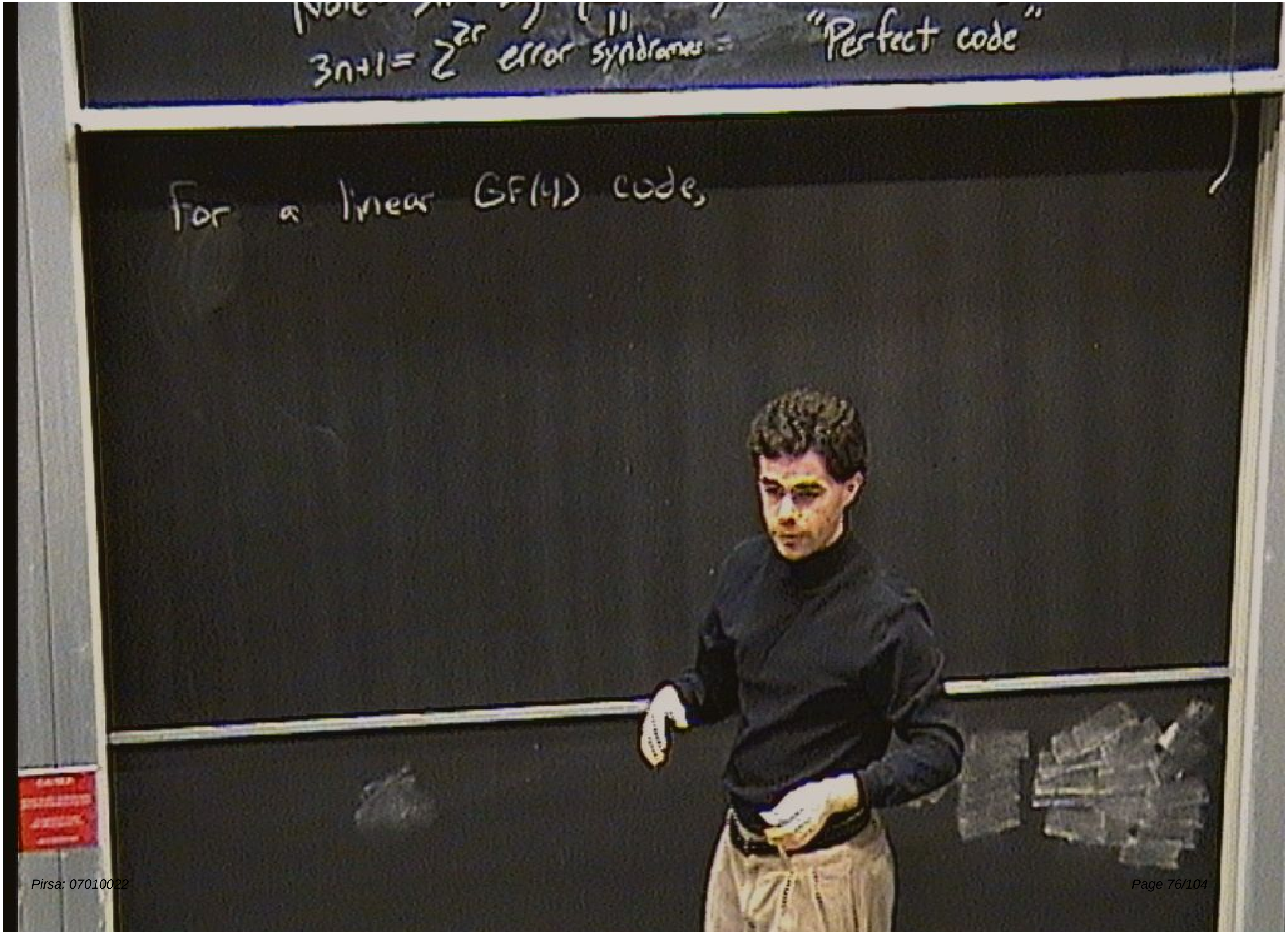
$r=4$ $[[85,77,3]]$

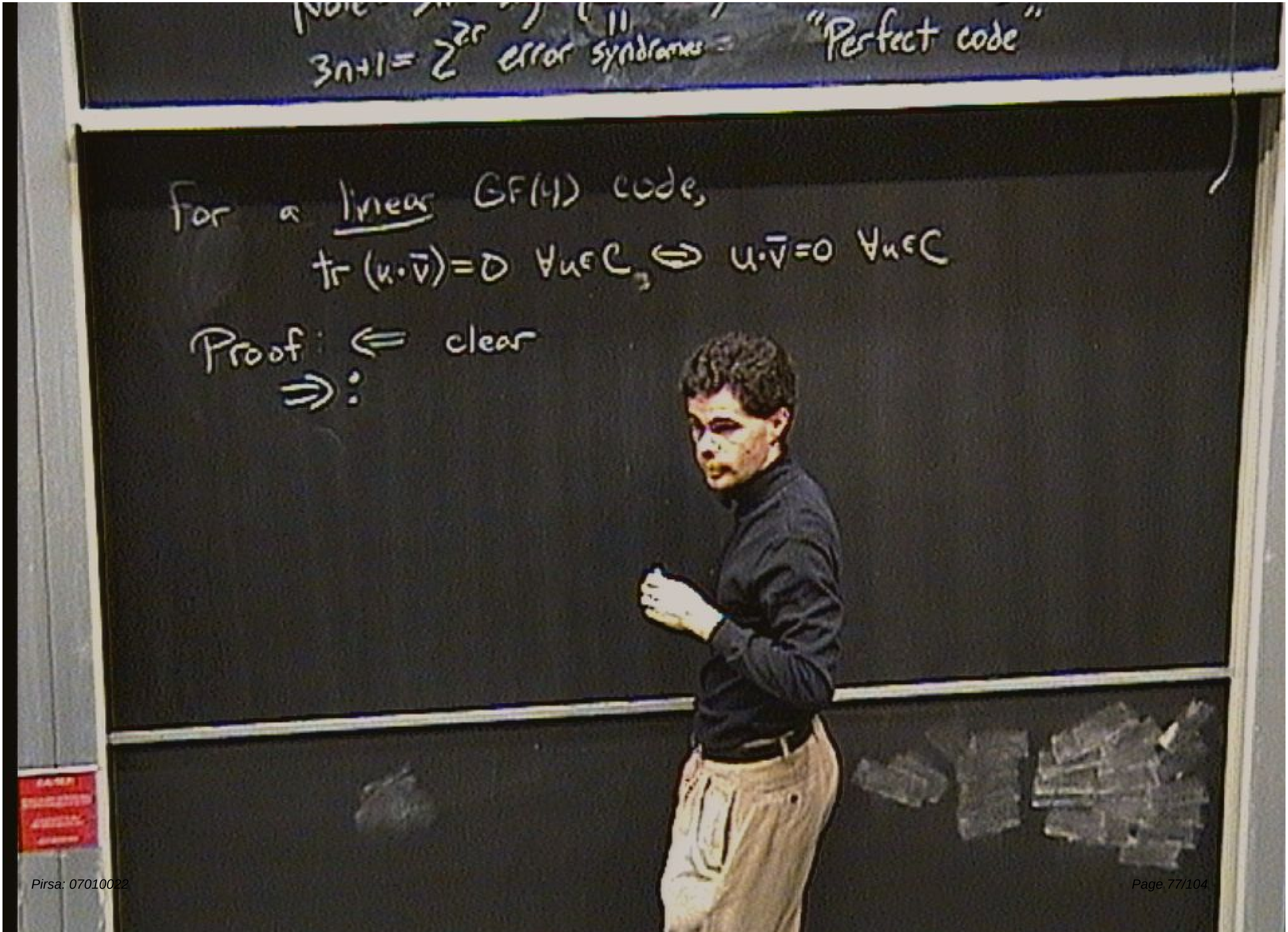
Convert to quantum stabilizer codes

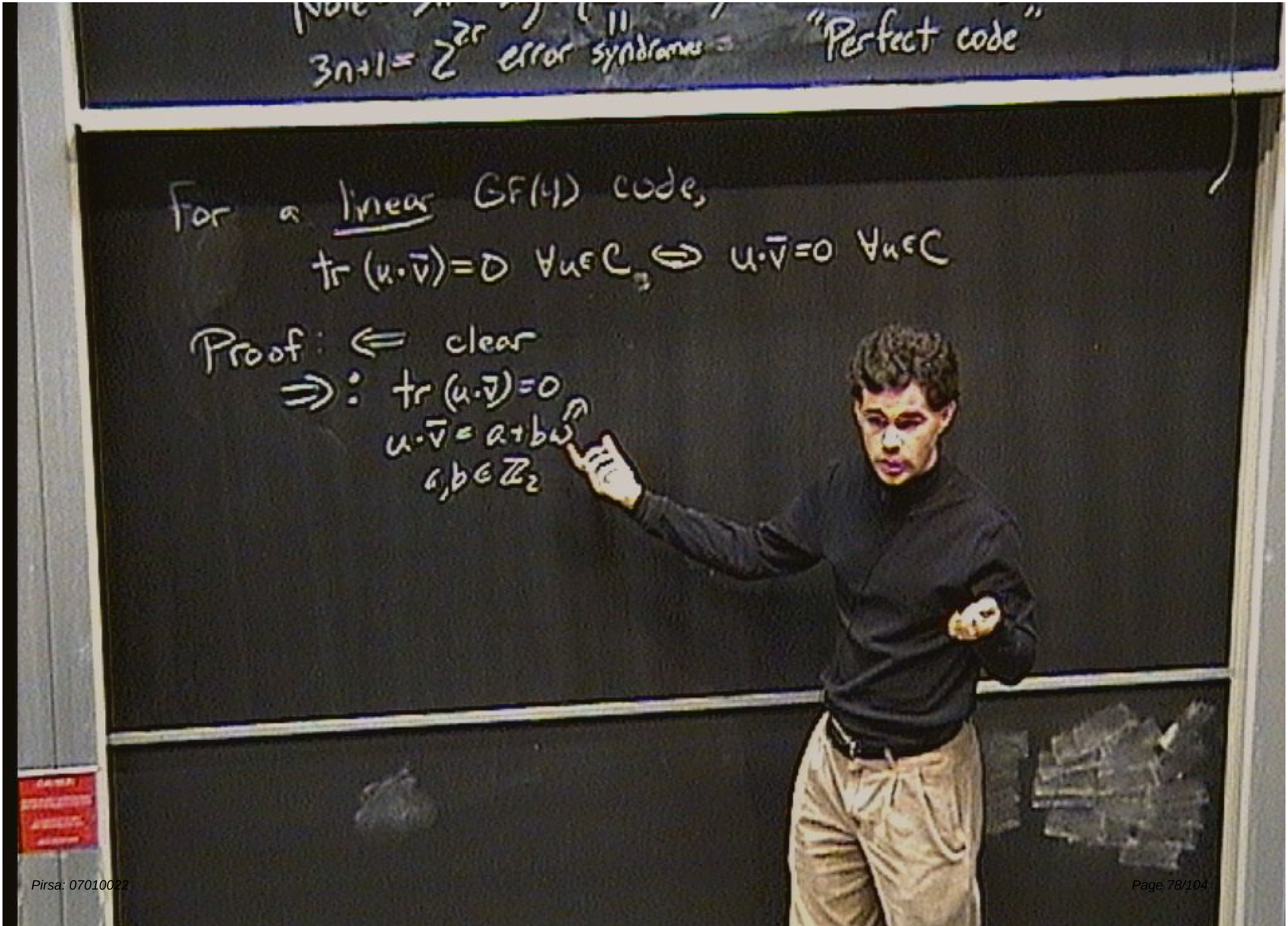
$$[[(4^r-1)/3,\ (4^r-1)/3 - 2r,\ 3]]$$

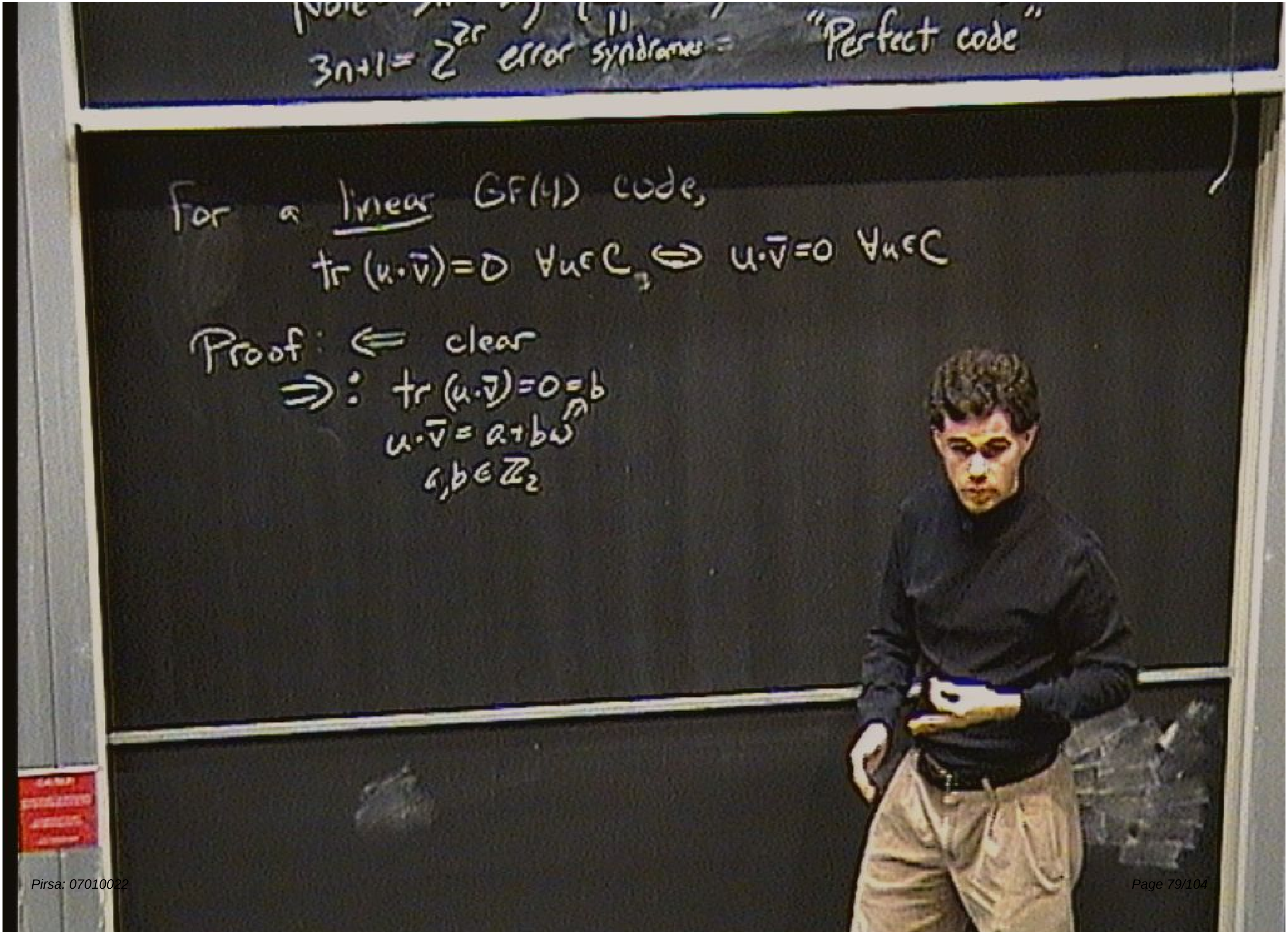
Note: $3n+1$ single-qubit errors, $2r$ stabilizer generators

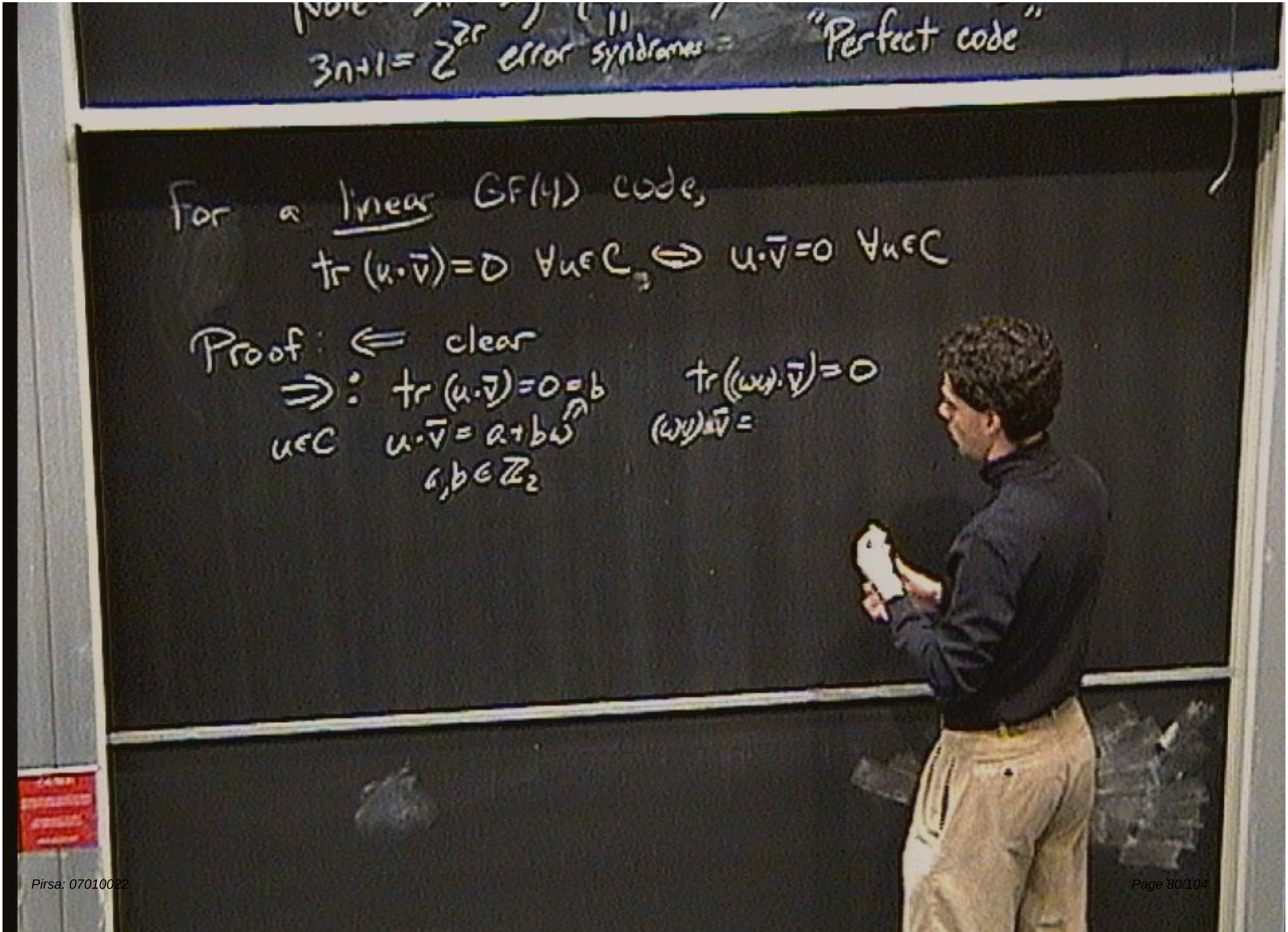
$3n+1 = 2^{2r}$ error syndromes. "Perfect code"


3n+1 = 2^2r error syndromes = "Perfect code"
For a linear GF(4) code,

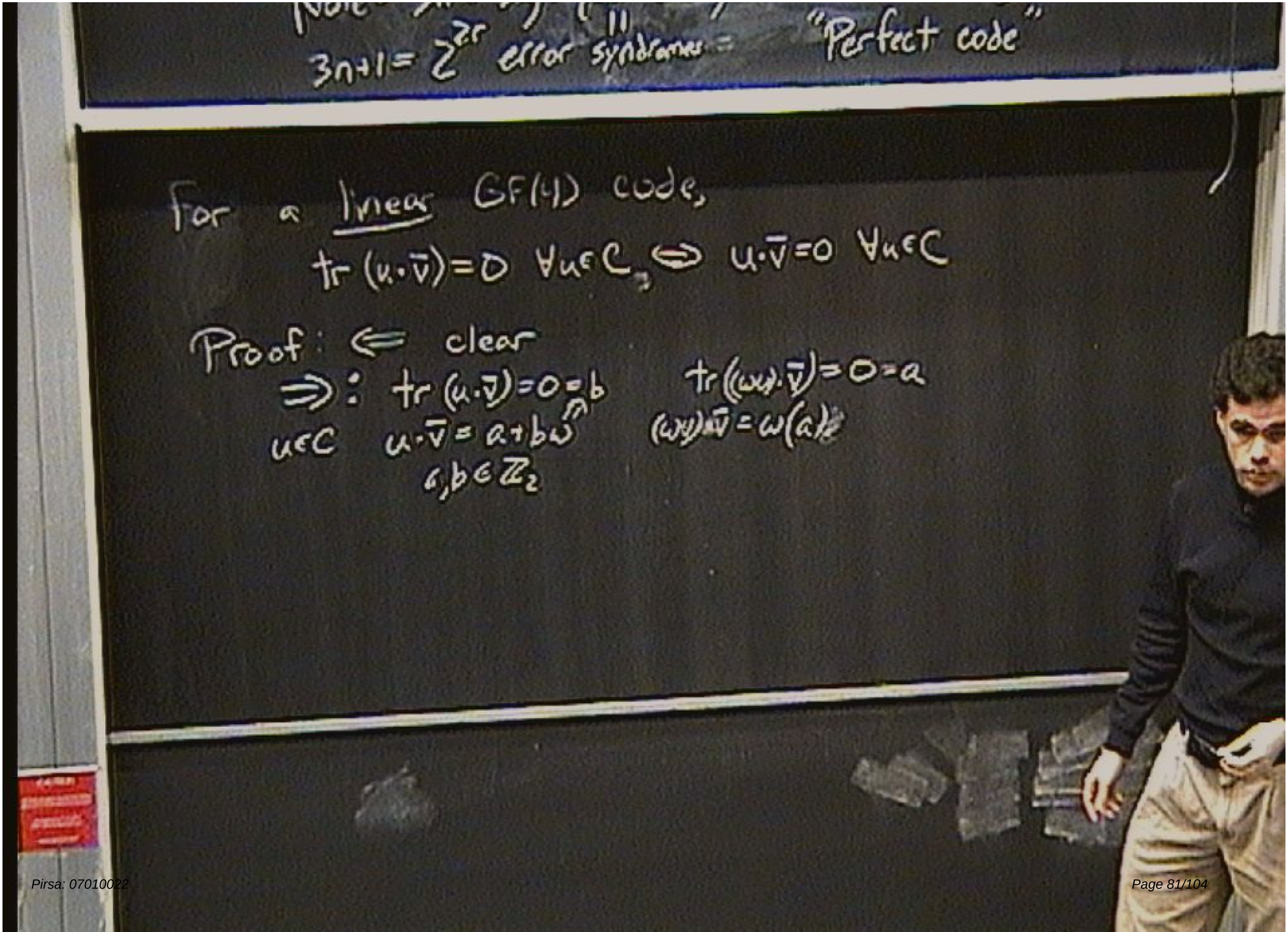

3n+1 = 2^2r error syndromes
"Perfect code"
For a linear GF(4) code,
tr (u·v̄)=0 ∀u∈C_2 ⟺ u·v̄=0 ∀u∈C
Proof: ⟸ clear
⟹:

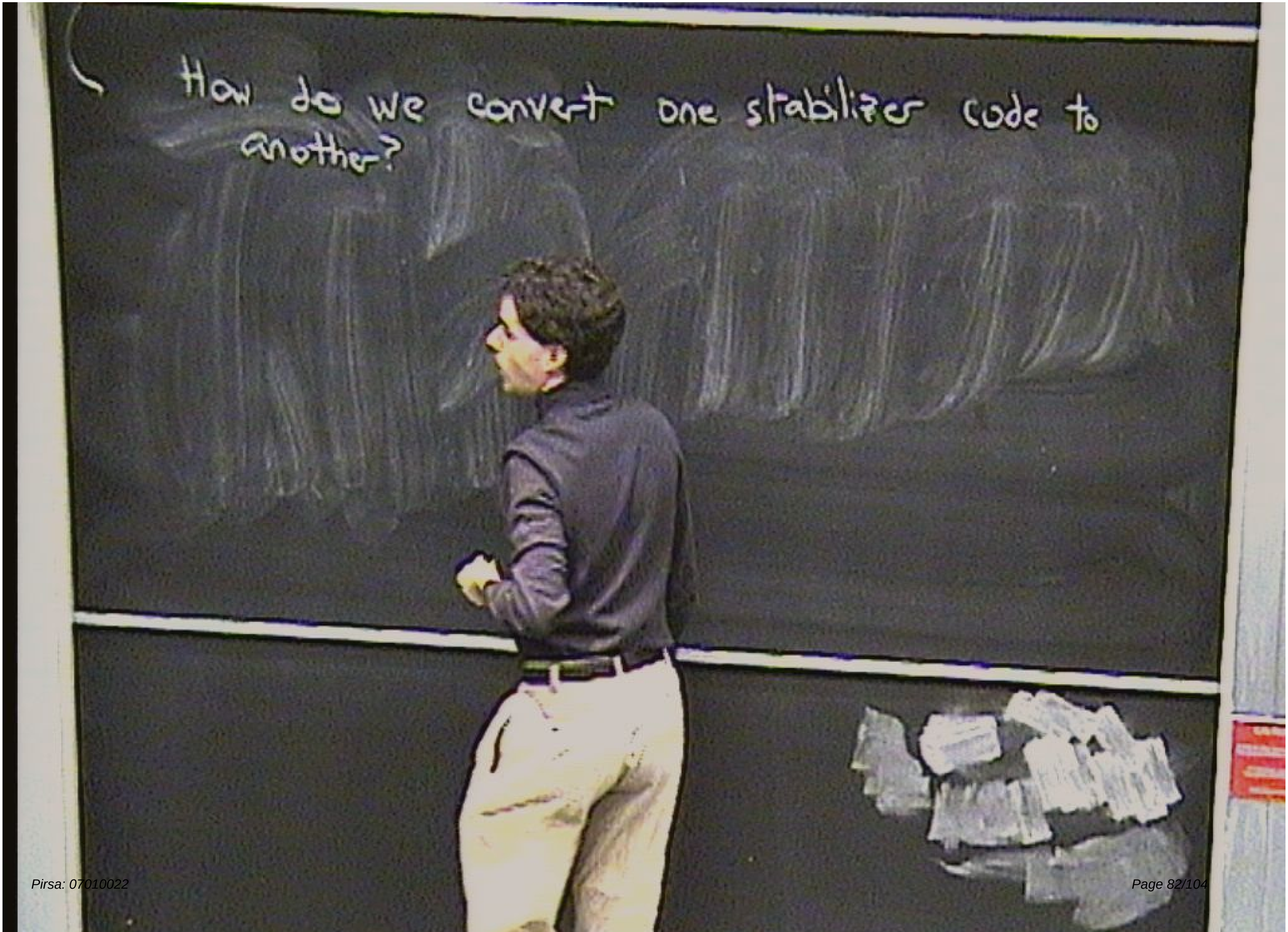

3n+1 = 2^2r error syndromes
"Perfect code"
For a linear GF(4) code,
tr(u·v̄)=0 ∀u∈C ⟺ u·v̄=0 ∀u∈C
Proof: ⟸ clear
⟹: tr(u·v̄)=0
u·v̄ = a+bω
a,b ∈ ℤ2

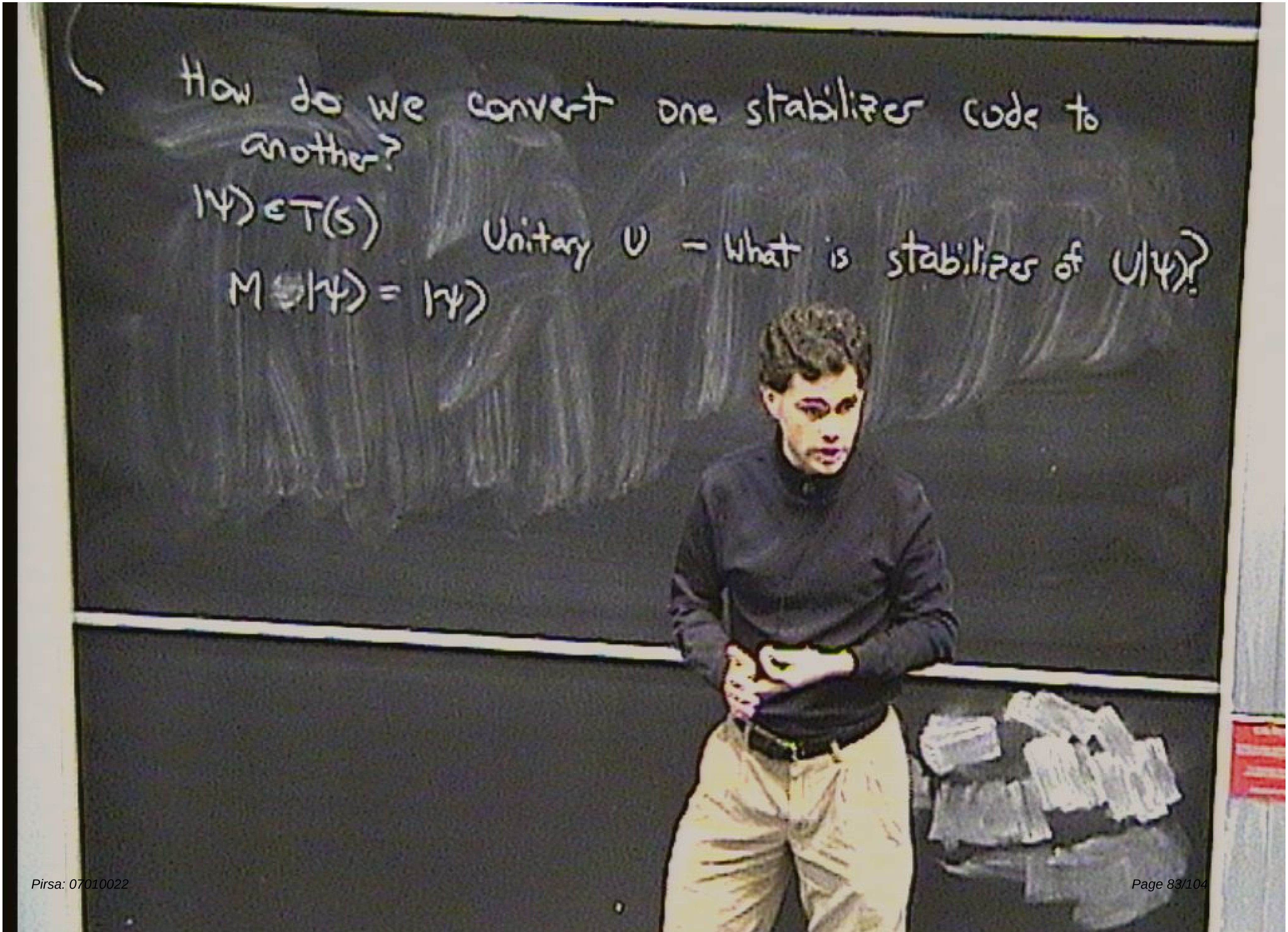

3n+1 = 2^2r error syndromes = "Perfect code"
For a linear GF(4) code,
tr(u·v̄)=0 ∀u∈C ⟺ u·v̄=0 ∀u∈C
Proof: ⟸ clear
⟹: tr(u·v̄)=0=b
u·v̄ = a+bω
a,b ∈ ℤ2

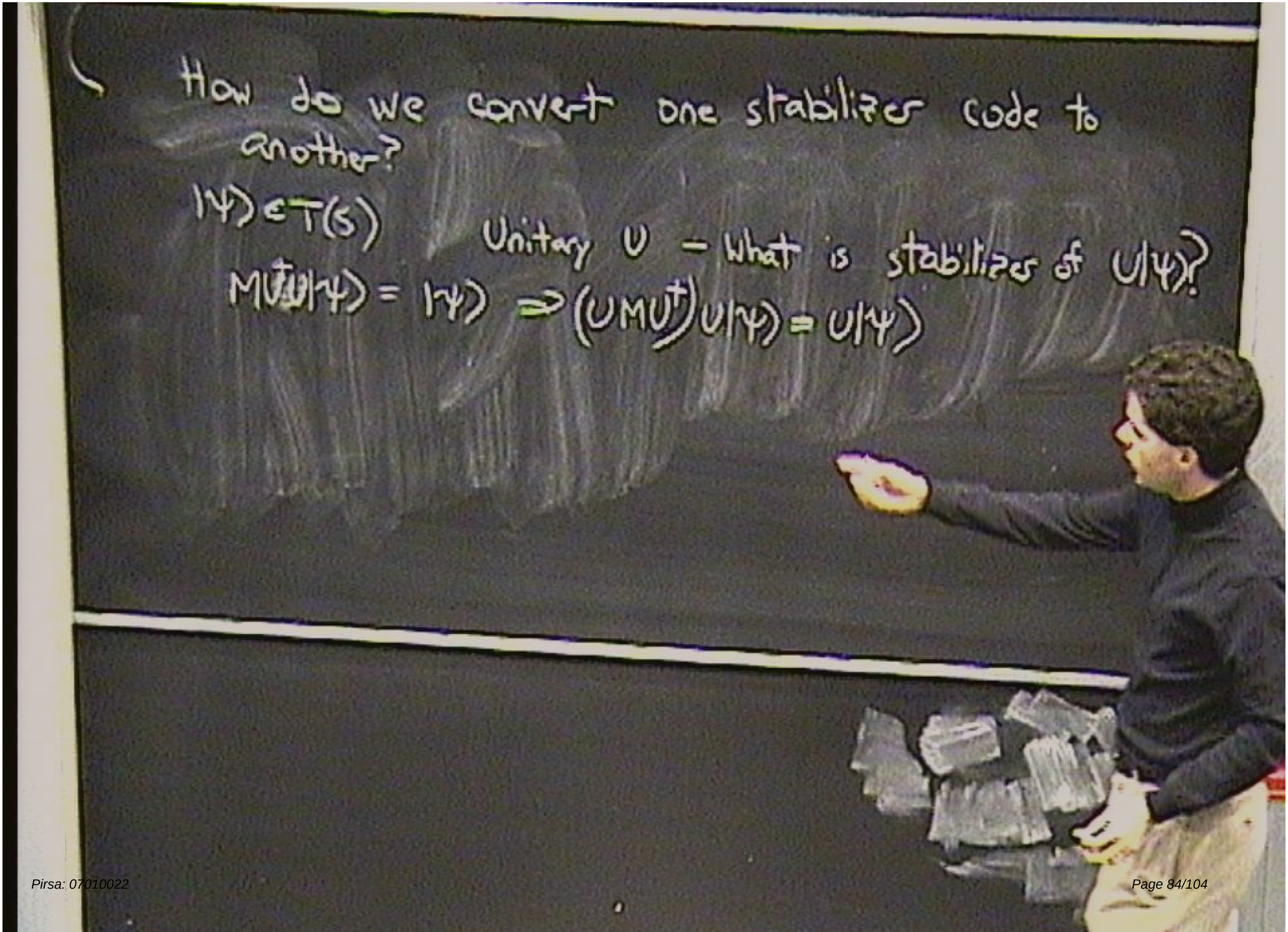


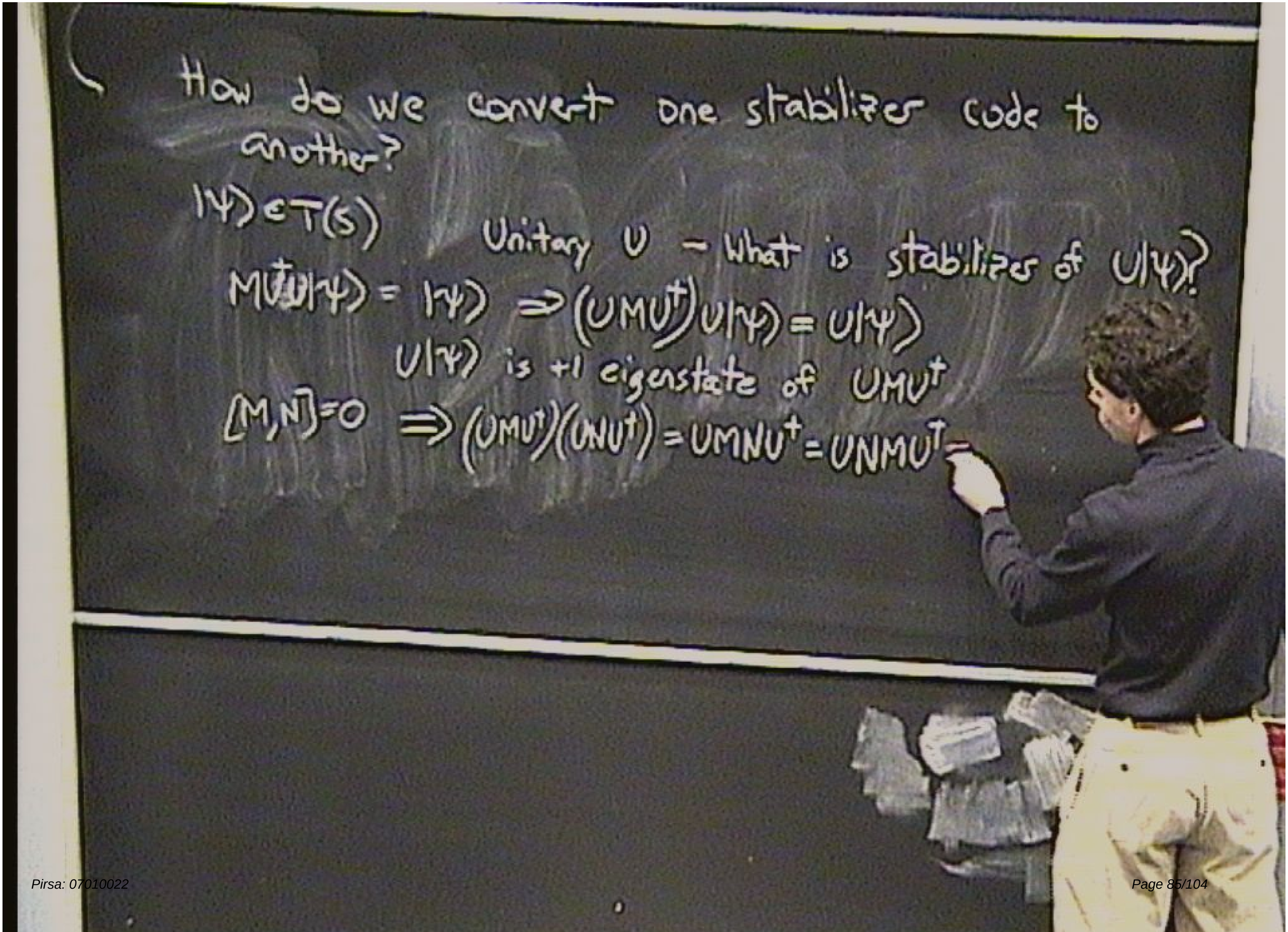
3n+1 = 2^2r error syndromes = "Perfect code"
For a linear GF(4) code,
tr(u·v̄)=0 ∀u∈C ⟺ u·v̄=0 ∀u∈C
Proof: ⟸ clear
⟹: tr(u·v̄)=0=b
tr((ωu)·v̄)=0
u∈C
u·v̄ = a+bω
(ωu)·v̄ =
a,b ∈ ℤ2


3n+1 = 2^2r error syndromes = "Perfect code"
For a linear GF(4) code,
tr(u·v̄)=0 ∀u∈C ⟺ u·v̄=0 ∀u∈C
Proof: ⟸ clear
⟹: tr(u·v̄)=0=b tr((ωu)·v̄)=0=a
u∈C u·v̄ = a+bω̂ (ωu)·v̄ = ω(a)
a,b ∈ Z2


How do we convert one stabilizer code to another?


How do we convert one stabilizer code to another?
|ψ⟩ ∈ T(S)
Unitary U – What is stabilizer of U|ψ⟩?
M |ψ⟩ = |ψ⟩


How do we convert one stabilizer code to another?
|ψ⟩ ∈ T(S)
Unitary U – what is stabilizer of U|ψ⟩?
MU†U|ψ⟩ = |ψ⟩ ⇒ (UMU†)U|ψ⟩ = U|ψ⟩


How do we convert one stabilizer code to another?
$|\psi\rangle \in T(S)$
Unitary U – what is stabilizer of $U|\psi\rangle$?
$M(U^\dagger U)|\psi\rangle = |\psi\rangle \Rightarrow (UMU^\dagger)U|\psi\rangle = U|\psi\rangle$
$U|\psi\rangle$ is +1 eigenstate of $UMU^\dagger$
$[M,N]=0 \Rightarrow (UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = UNMU^\dagger$

How do we convert one stabilizer code to another?

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

Unitary U – what is stabilizer of $U|\psi\rangle$?

$$M U^\dagger U|\psi\rangle = |\psi\rangle \Rightarrow (UMU^\dagger)U|\psi\rangle = U|\psi\rangle$$

$U|\psi\rangle$ is +1 eigenstate of $UMU^\dagger$

$$[M,N]=0 \Leftrightarrow (UMU^\dagger)(UNU^\dagger) = UMNU^\dagger = UNMU^\dagger = (UNU^\dagger)(UMU^\dagger)$$

$$[UMU^\dagger, UNU^\dagger]=0$$

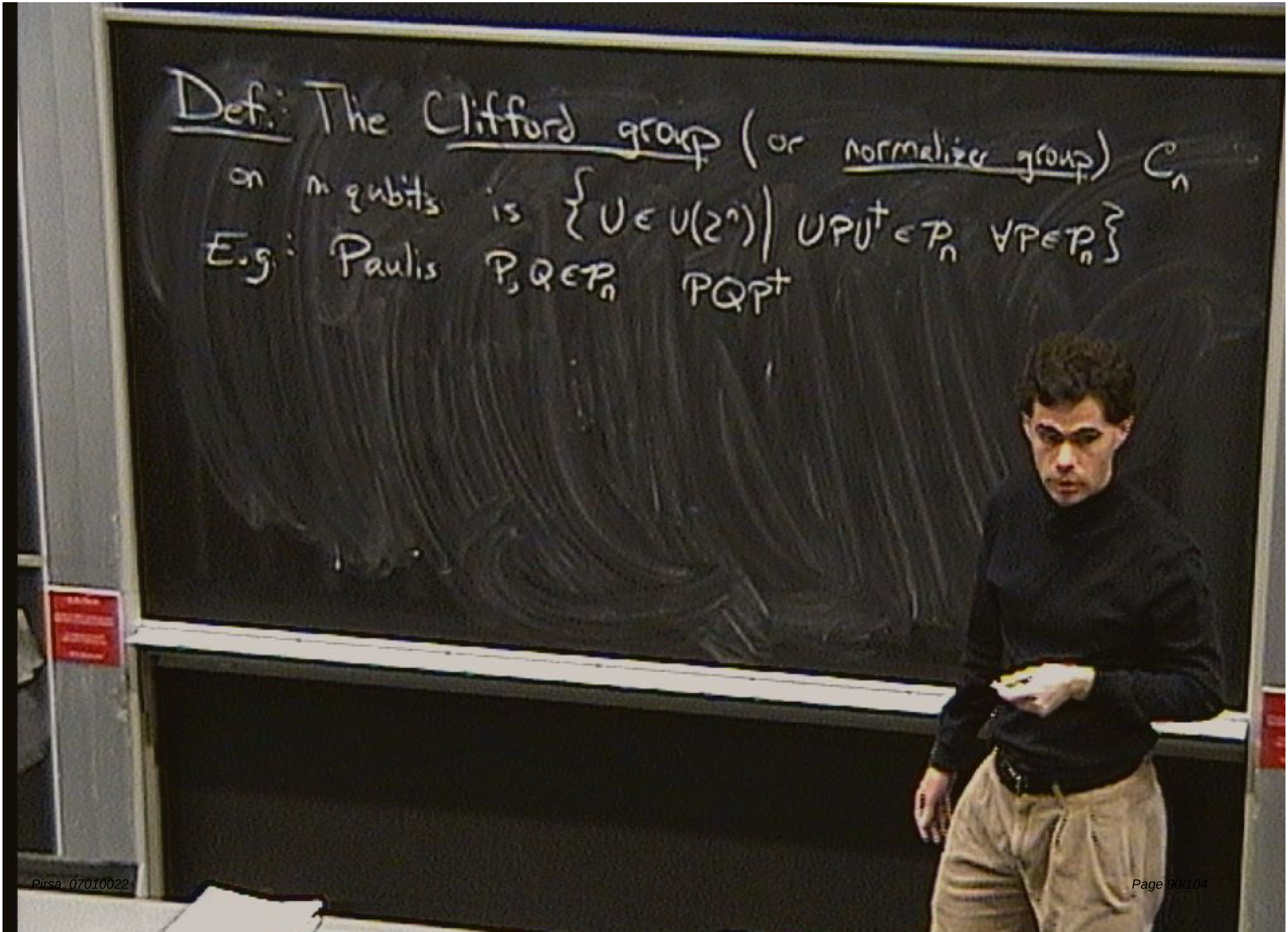
Def.: The **Clifford group** (or **normalizer group**) $\mathcal{C}_n$

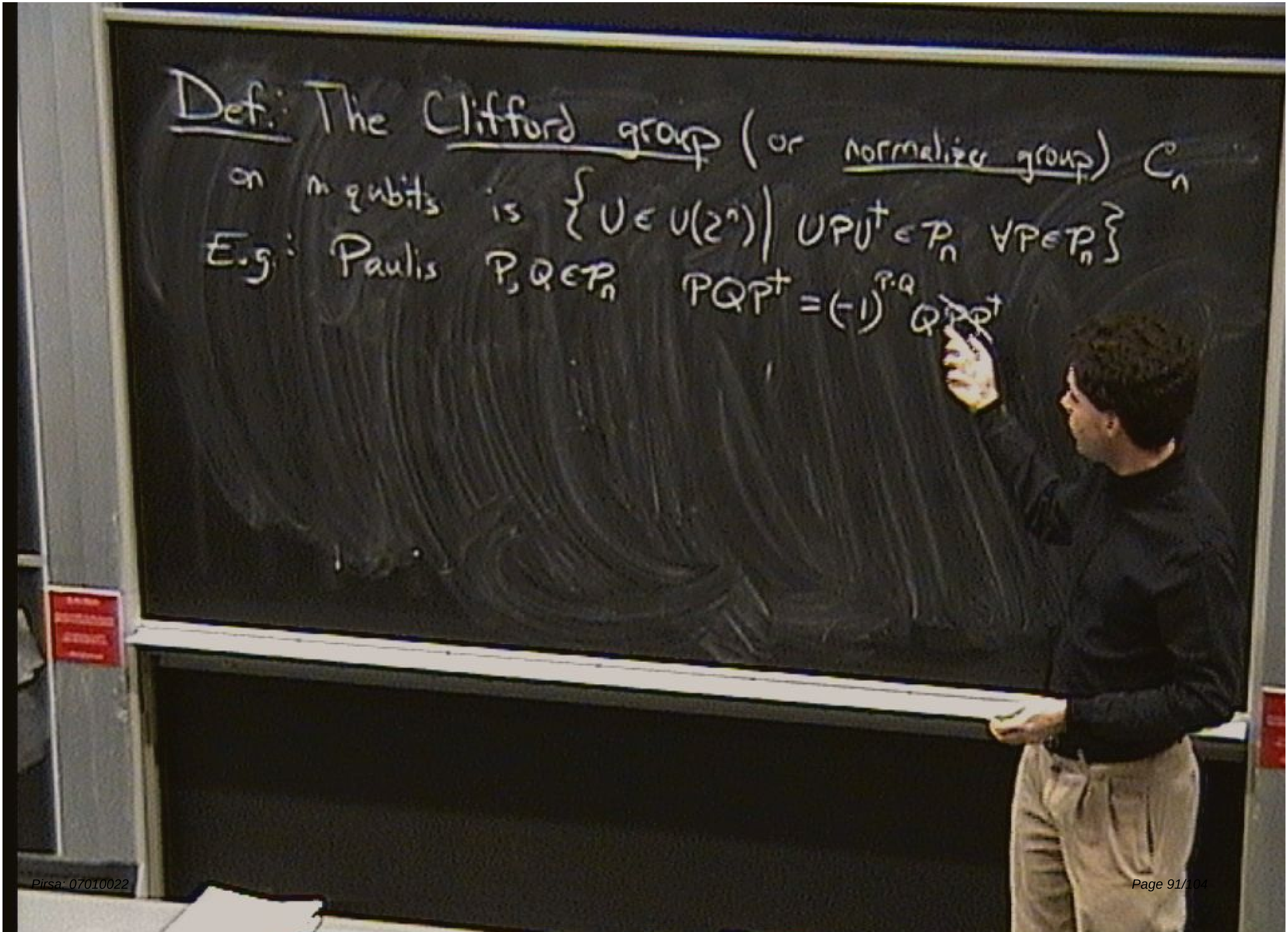
on n qubits is $\{$

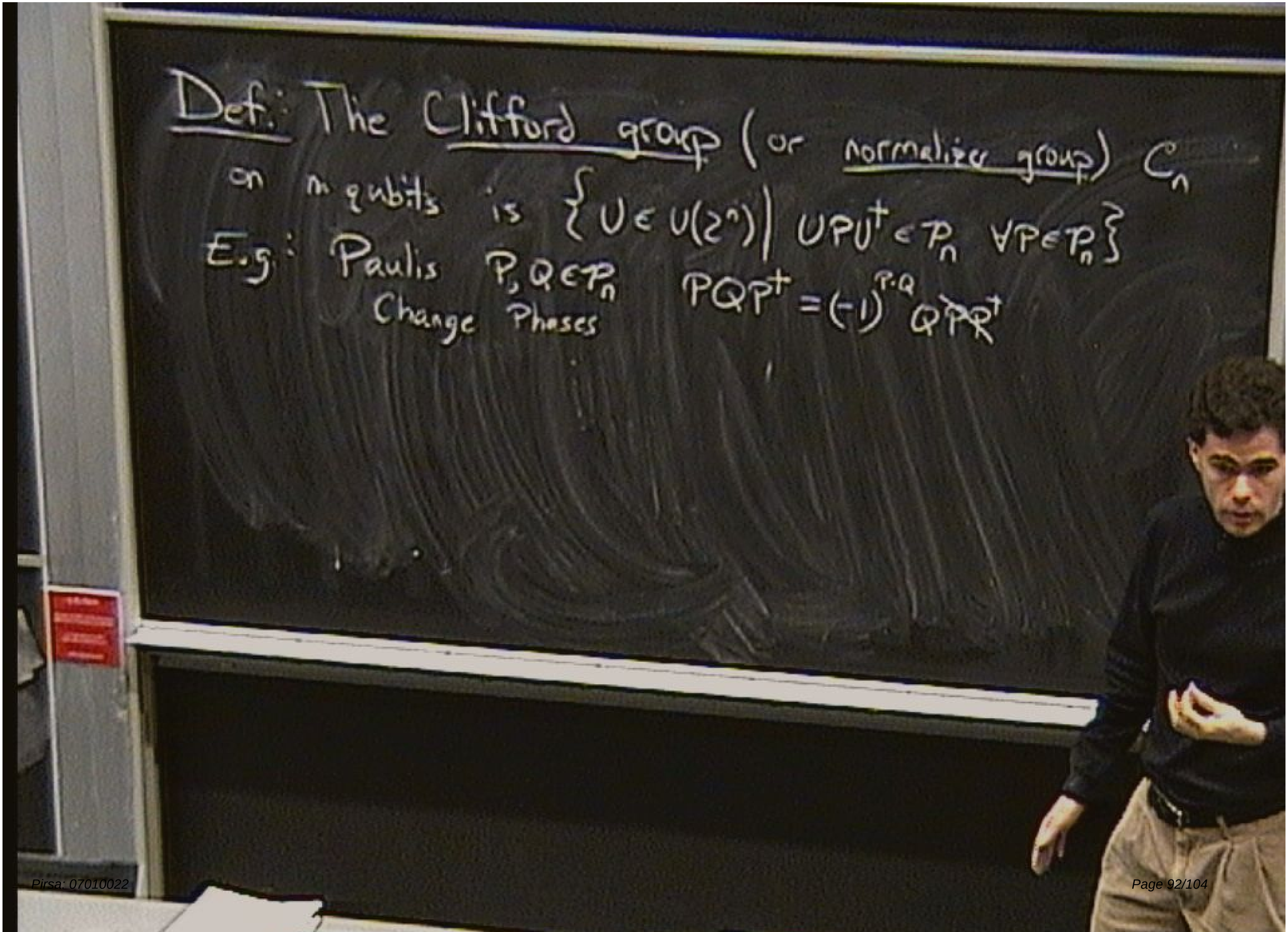
Def.: The **Clifford group** (or **normalizer group**) $\mathcal{C}_n$ on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$

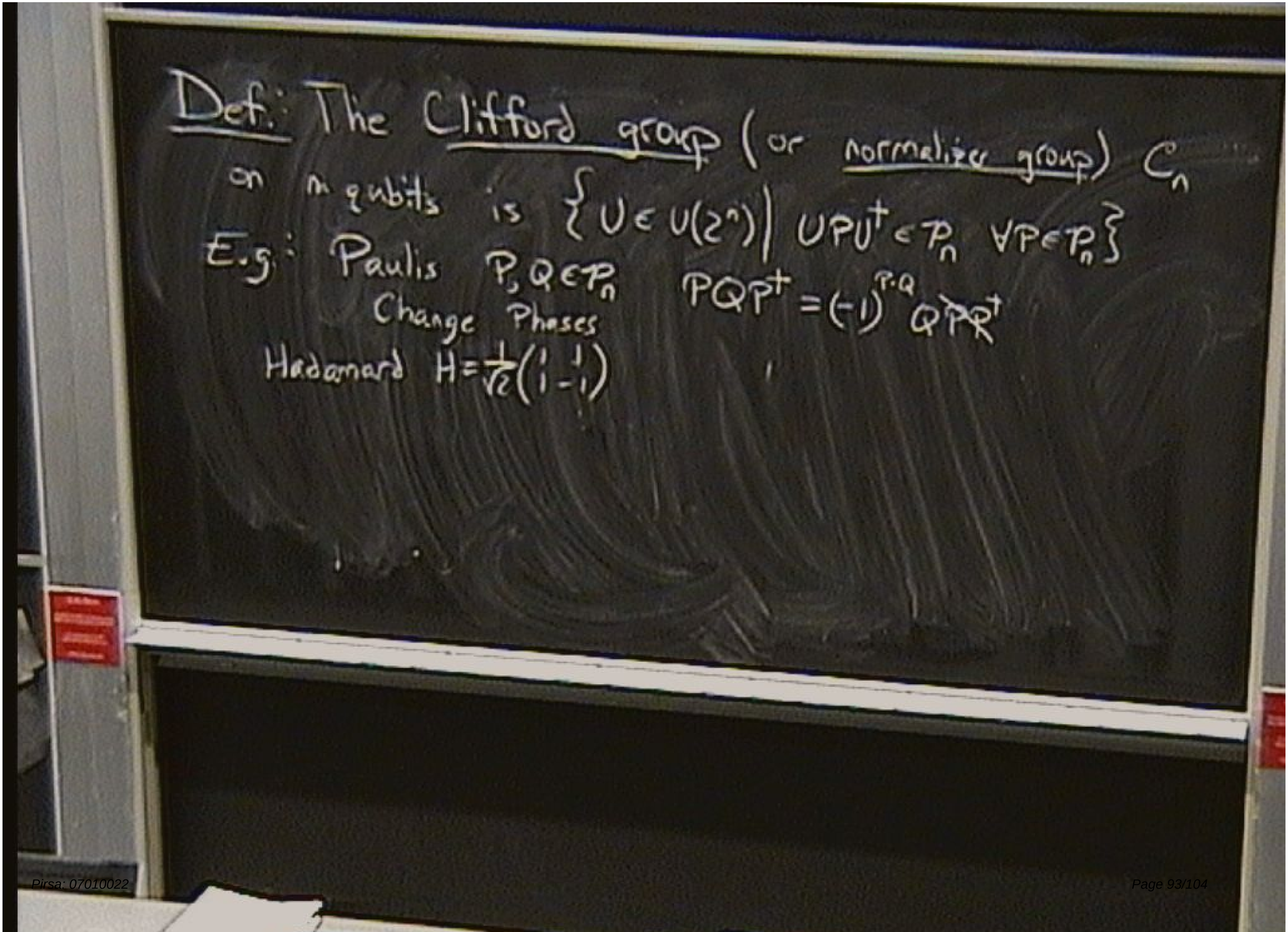
Def: The <u>Clifford group</u> (or <u>normalizer group</u>) $\mathcal{C}_n$ on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$

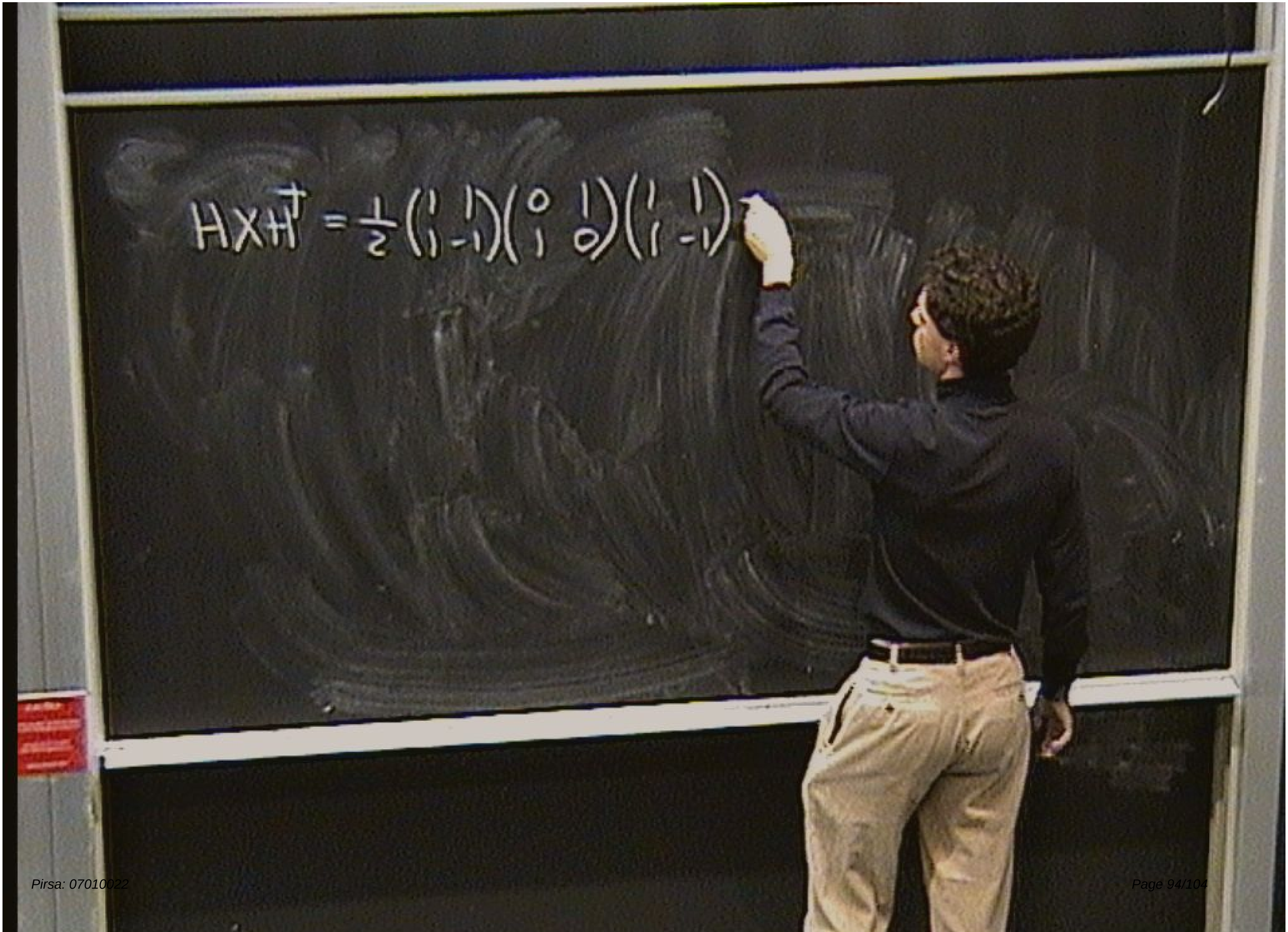
E.g.:


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger$

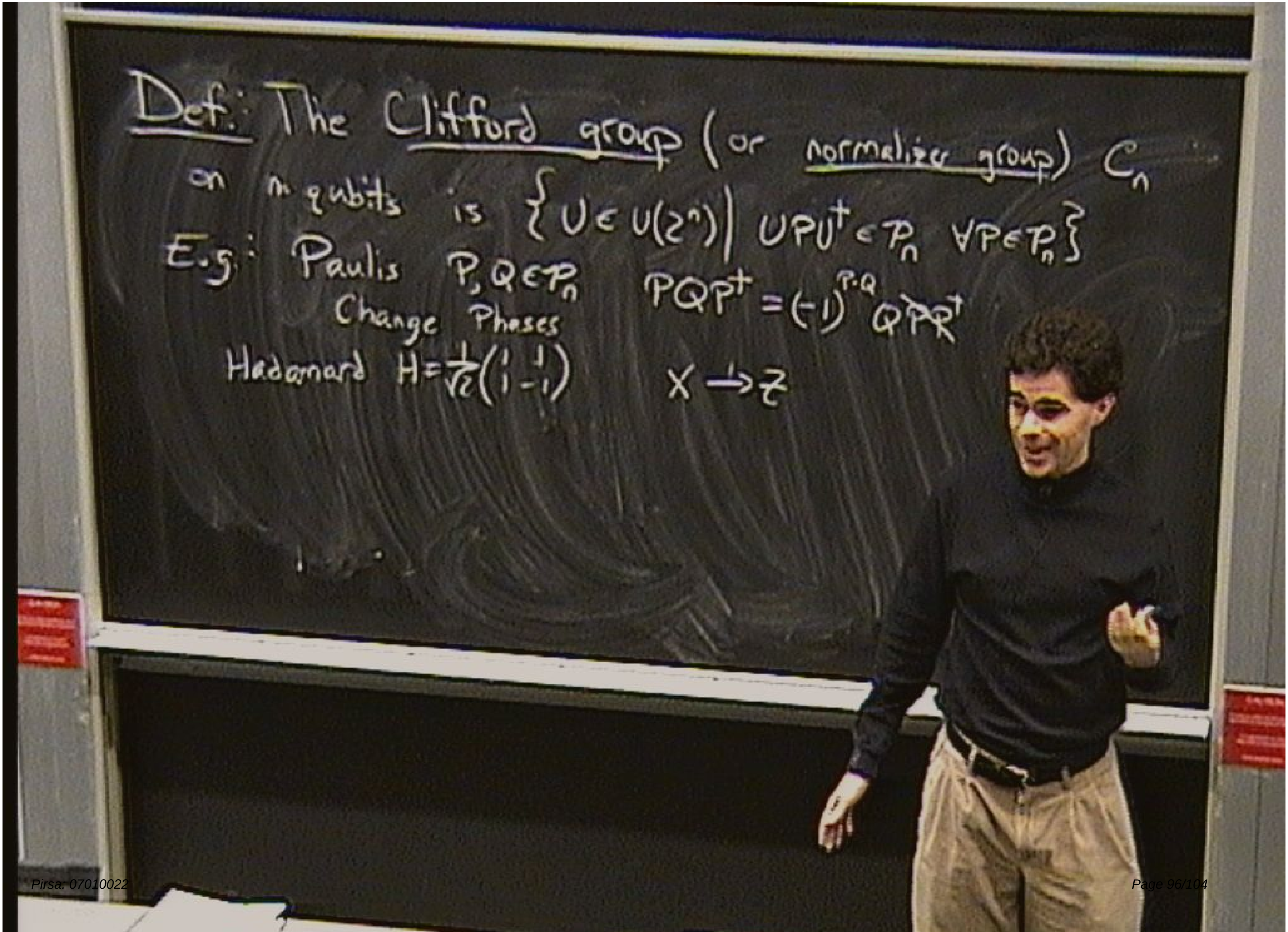

Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger = (-1)^{P \cdot Q} QPP^\dagger$


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger = (-1)^{P\cdot Q} Q\cancel{PP^\dagger}$
Change Phases


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger = (-1)^{P \cdot Q} Q\cancel{PP^\dagger}$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$


$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = Z$$


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in P_n \ \forall P \in P_n\}$
E.g.: Paulis $P, Q \in P_n$ $PQP^\dagger = (-1)^{P\cdot Q} QPP^\dagger$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $X \rightarrow Z$

Def: The Clifford group (or normalizer group) $\mathcal{C}_n$ on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$

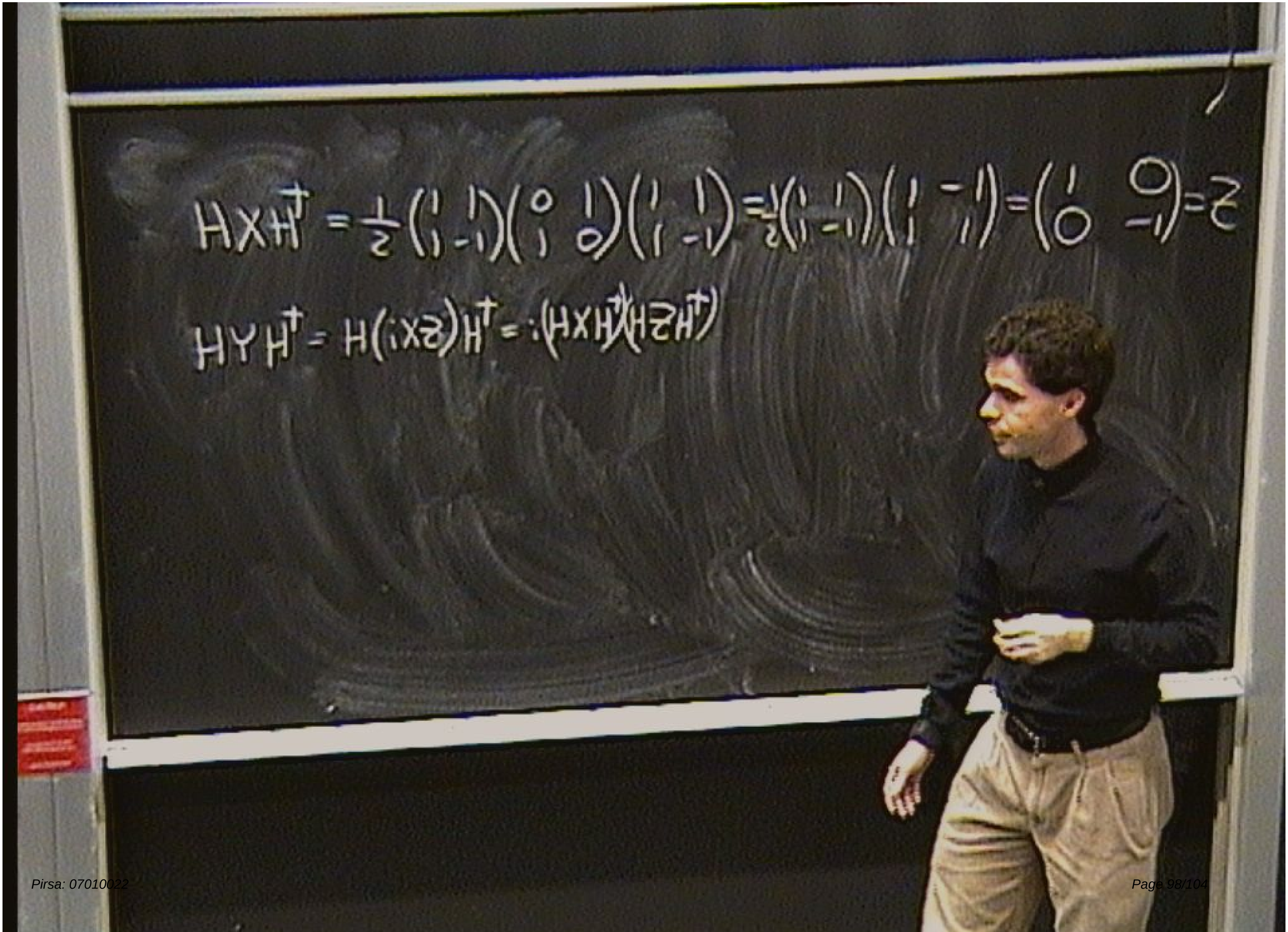
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $\quad PQP^\dagger = (-1)^{P\cdot Q}\, QPP^\dagger$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$X \to Z$

$Z \to X$

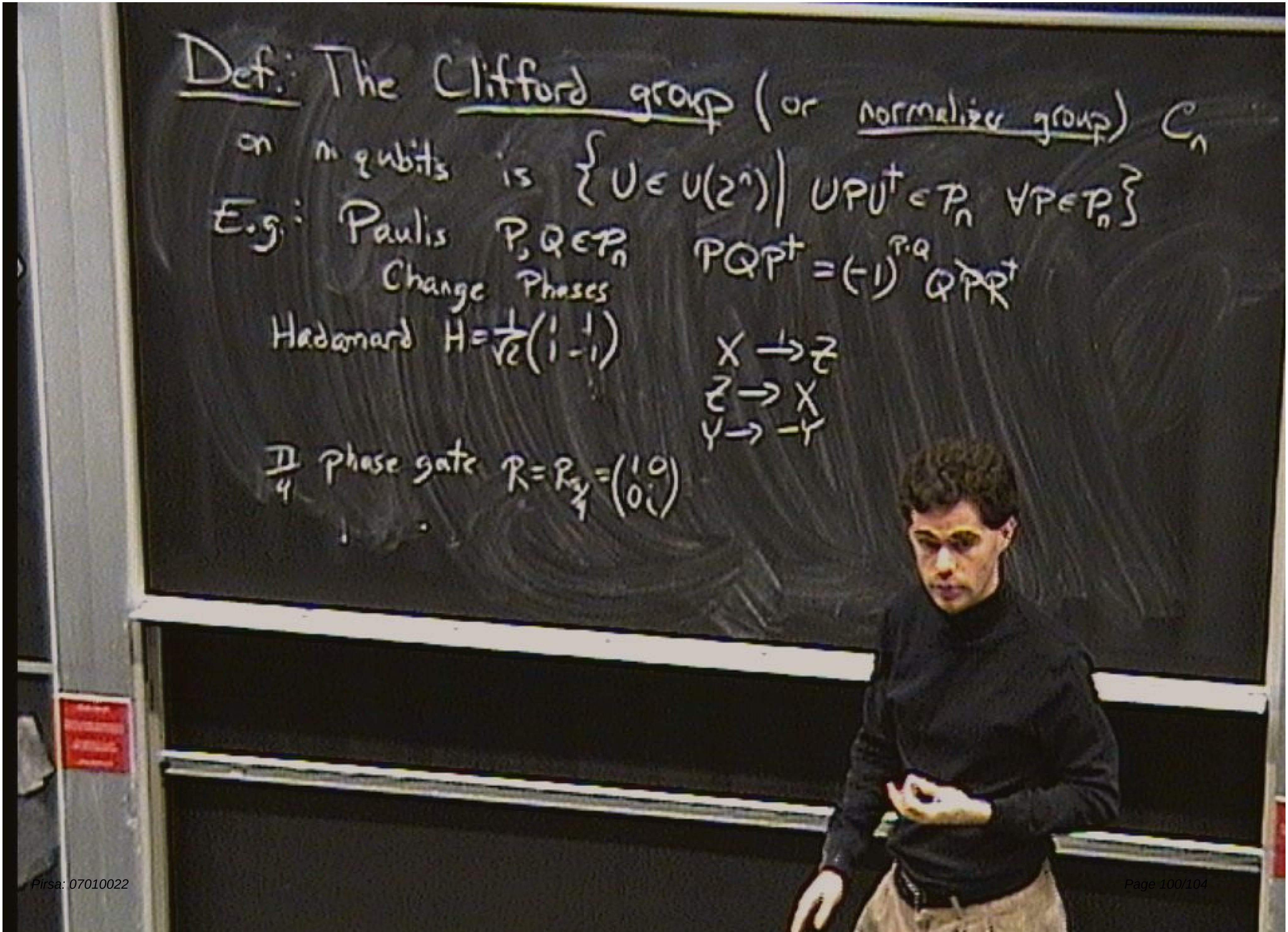


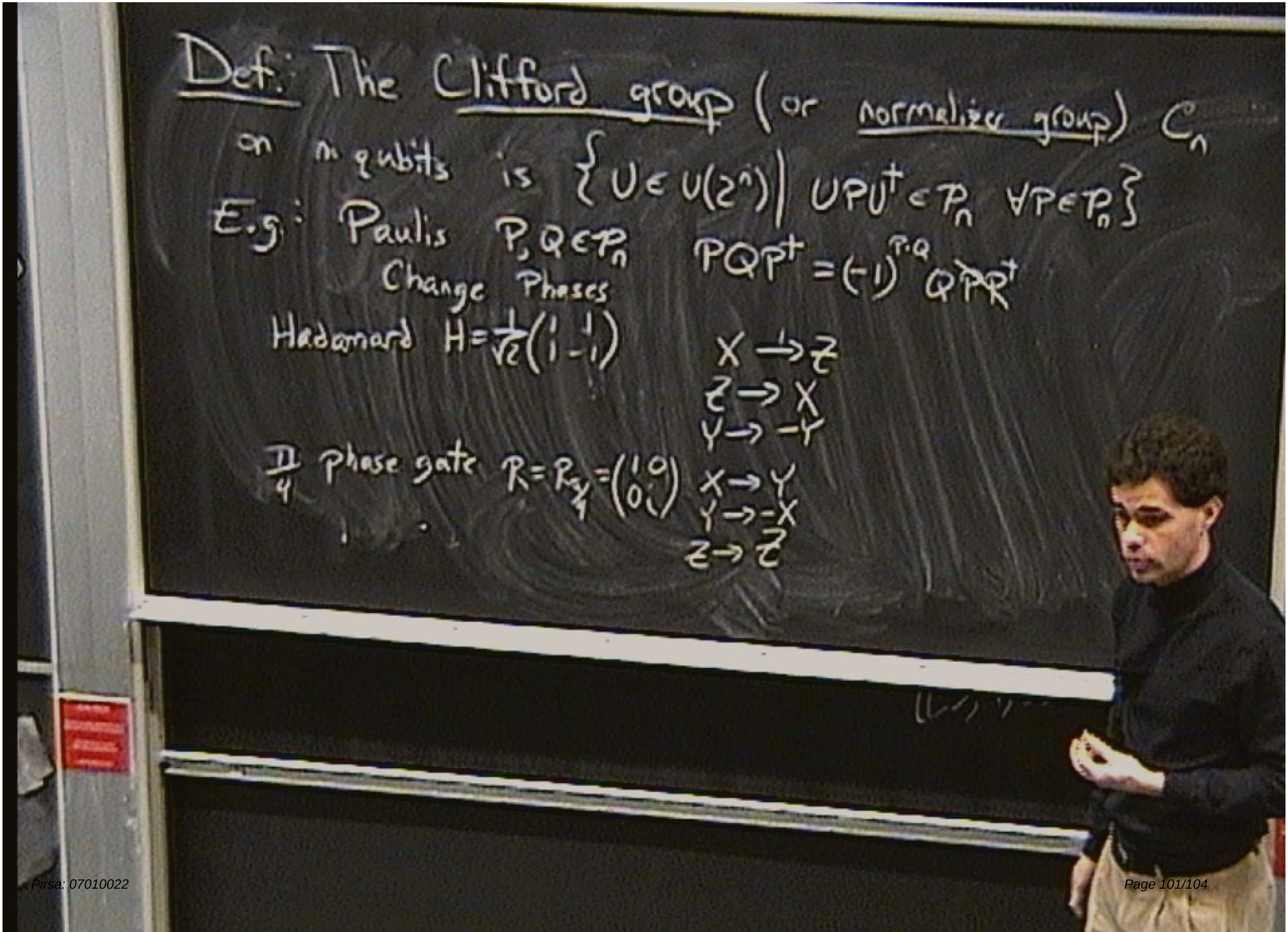
$HXH^\dagger = \frac{1}{2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&-1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&-1\\1&1\end{pmatrix} = \begin{pmatrix}1&0\\0&-1\end{pmatrix} = Z$
$HYH^\dagger = H(iXZ)H^\dagger = i(HXH^\dagger)(HZH^\dagger)$

$$HXH^{\dagger} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z$$

$$HYH^{\dagger} = H(iXZ)H^{\dagger} = i(HXH^{\dagger})(HZH^{\dagger}) = iZX = -Y$$

Sufficient to check $UPU^{\dagger} \in \mathcal{P}_n$ for generating set of $\mathcal{P}_1$ (for $\mathcal{P}_n$)


Def: The Clifford group (or normalizer group) C_n
on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger = (-1)^{P \cdot Q} Q P P^\dagger$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$X \to Z$
$Z \to X$
$Y \to -Y$
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$


Def: The Clifford group (or normalizer group) $\mathcal{C}_n$
on n qubits is $\{ U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n \}$
E.g.: Paulis $P, Q \in \mathcal{P}_n$ $PQP^\dagger = (-1)^{P \cdot Q} QPP^\dagger$
Change Phases
Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$X \to Z$
$Z \to X$
$Y \to -Y$
$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$X \to Y$
$Y \to -X$
$Z \to Z$

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$

E.g.: Paulis $P, Q \in \mathcal{P}_n$ $\quad PQP^\dagger = (-1)^{P\cdot Q} QPP^\dagger$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$X \rightarrow Z$
$Z \rightarrow X$
$Y \rightarrow -Y$

$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

$X \rightarrow Y$
$Y \rightarrow -X$
$Z \rightarrow Z$

CNOT: $X \otimes I \rightarrow X \otimes X$
$Z \otimes I \rightarrow Z \otimes I$
$I \otimes X \rightarrow I \otimes X$
$I \otimes Z \rightarrow Z \otimes Z$

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$

E.g.: Paulis $P, Q \in \mathcal{P}_n$ $\quad PQP^\dagger = (-1)^{P\cdot Q} QPP^\dagger$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$X \rightarrow Z$

$Z \rightarrow X$

$Y \rightarrow -Y$

$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$

$X \rightarrow Y$

$Y \rightarrow -X$

$Z \rightarrow Z$

CNOT: $X \otimes I \rightarrow X \otimes X$

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

$I \otimes X \rightarrow I \otimes X$

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

Permutations of qubits

Def: The Clifford group (or normalizer group) C_n on n qubits is $\{U \in U(2^n) \mid UPU^\dagger \in \mathcal{P}_n \ \forall P \in \mathcal{P}_n\}$ or $C_n / \{e^{i\theta} I\}$

E.g.: Paulis $P, Q \in \mathcal{P}_n$ $\quad PQP^\dagger = (-1)^{P\cdot Q} QPP^\dagger$

Change Phases

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$X \to Z$
$Z \to X$
$Y \to -Y$

$\frac{\pi}{4}$ phase gate $R = R_{\frac{\pi}{4}} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$

$X \to Y$
$Y \to -X$
$Z \to Z$

CNOT: $X\otimes I \to X \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes X \to I \otimes X$
$I \otimes Z \to Z \otimes Z$

Permutations of qubits