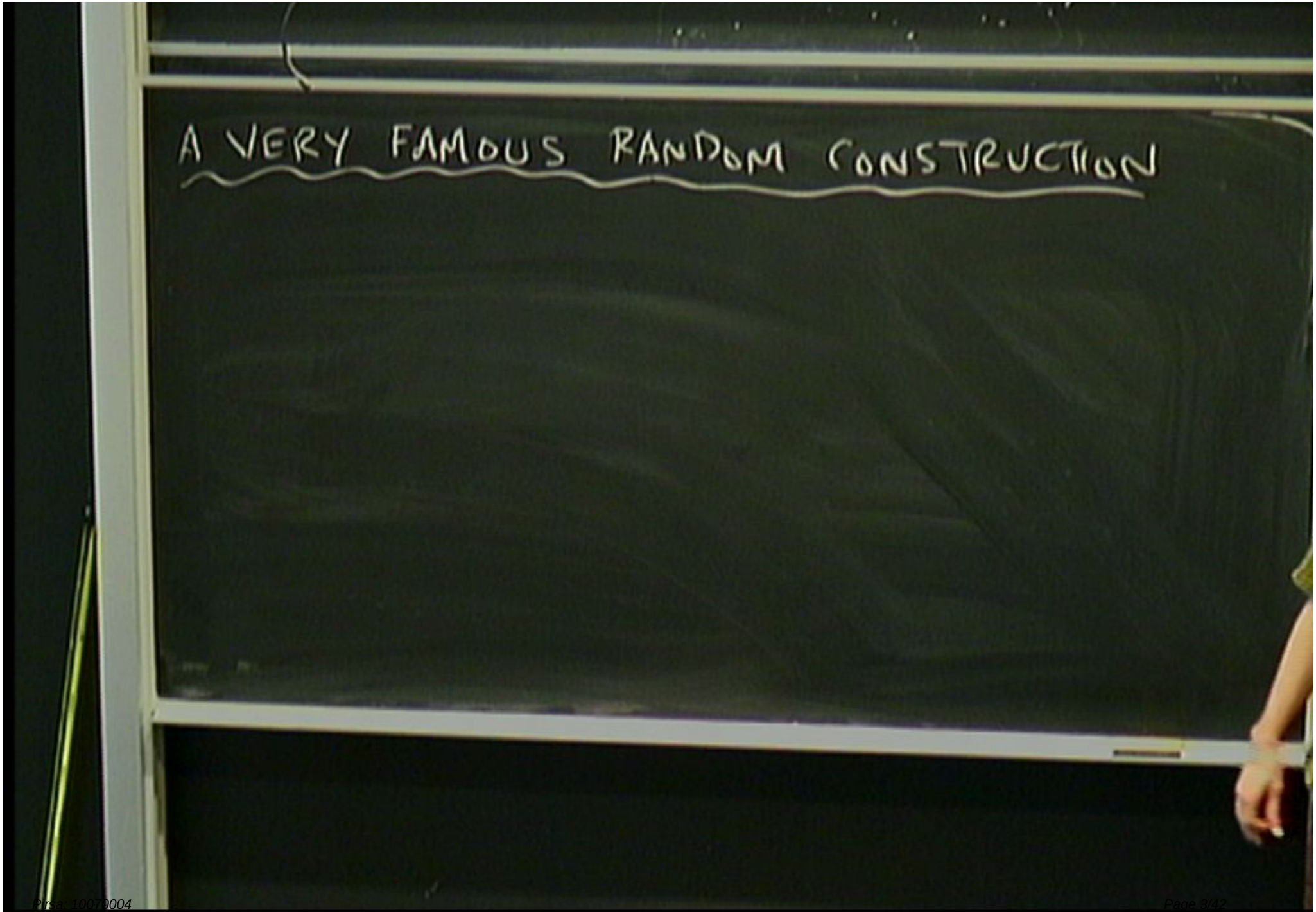
Title: Random constructions in Quantum Information Theory

Date: Jul 04, 2010 09:15 AM

URL: http://pirsa.org/10070004

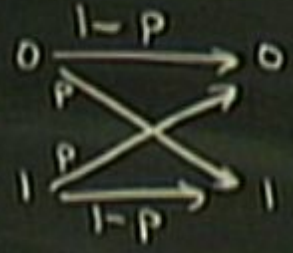
Abstract: TBA

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS


A VERY FAMOUS RANDOM CONSTRUCTION

A VERY FAMOUS RANDOM CONSTRUCTION

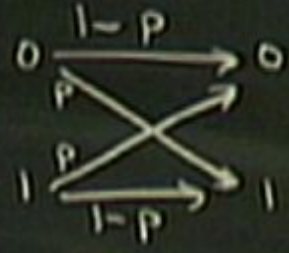
BINARY
SYMMETRIC
CHANNEL



$: p(y|x)$

A VERY FAMOUS RANDOM CONSTRUCTION

BINARY SYMMETRIC CHANNEL



$: p(y|x)$

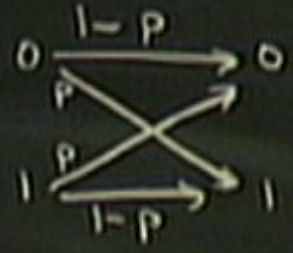
MANY USES $p^{\wedge}(y_1 \cdots y_n | x_1 \cdots x_n) = \prod_{i=1}^{n} p(y_i|x_i)$

$y^{\wedge}$ $x^{\wedge}$

$p^{\wedge}$

A VERY FAMOUS RANDOM CONSTRUCTION

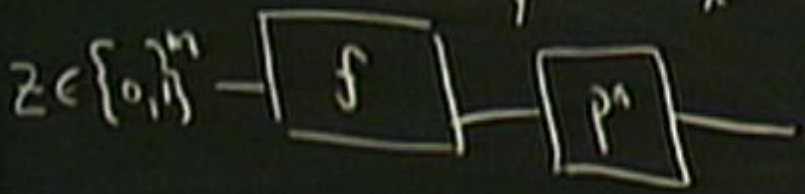
BINARY SYMMETRIC CHANNEL



$: p(y|x)$

MANY USES $p^{\wedge}(y_1 \cdots y_n | x_1 \cdots x_n) = \prod_{i=1}^{n} p(y_i|x_i)$

$y^{\wedge}$ $x^{\wedge}$



A VERY FAMOUS RANDOM CONSTRUCTION

BINARY SYMMETRIC CHANNEL

$: p(y|x)$

MANY USES $p^n(y_1 \cdots y_n | x_1 \cdots x_n) = \prod_{i=1}^{n} p(y_i|x_i)$

y^n x^n

$z \in \{0,1\}^m$ — f — p^n — g — $\hat{z}$

A VERY FAMOUS RANDOM CONSTRUCTION

BINARY SYMMETRIC CHANNEL

$: p(y|x)$

MANY USES $p^n(y_1 \cdots y_n | x_1 \cdots x_n) = \prod_{i=1}^{n} p(y_i|x_i)$

y^n x^n

$z \in \{0,1\}^m$ — [f] — [p^n] — [g] — $\hat{z}$ $\quad \Pr\{z \neq \hat{z}\} \xrightarrow{n \to \infty} 0$

HOW TO FIND NEAR-OPTIMAL f?

ie $\frac{m}{n} \longrightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p)\log(1-p)$

HOW TO FIND NEAR-OPTIMAL f?

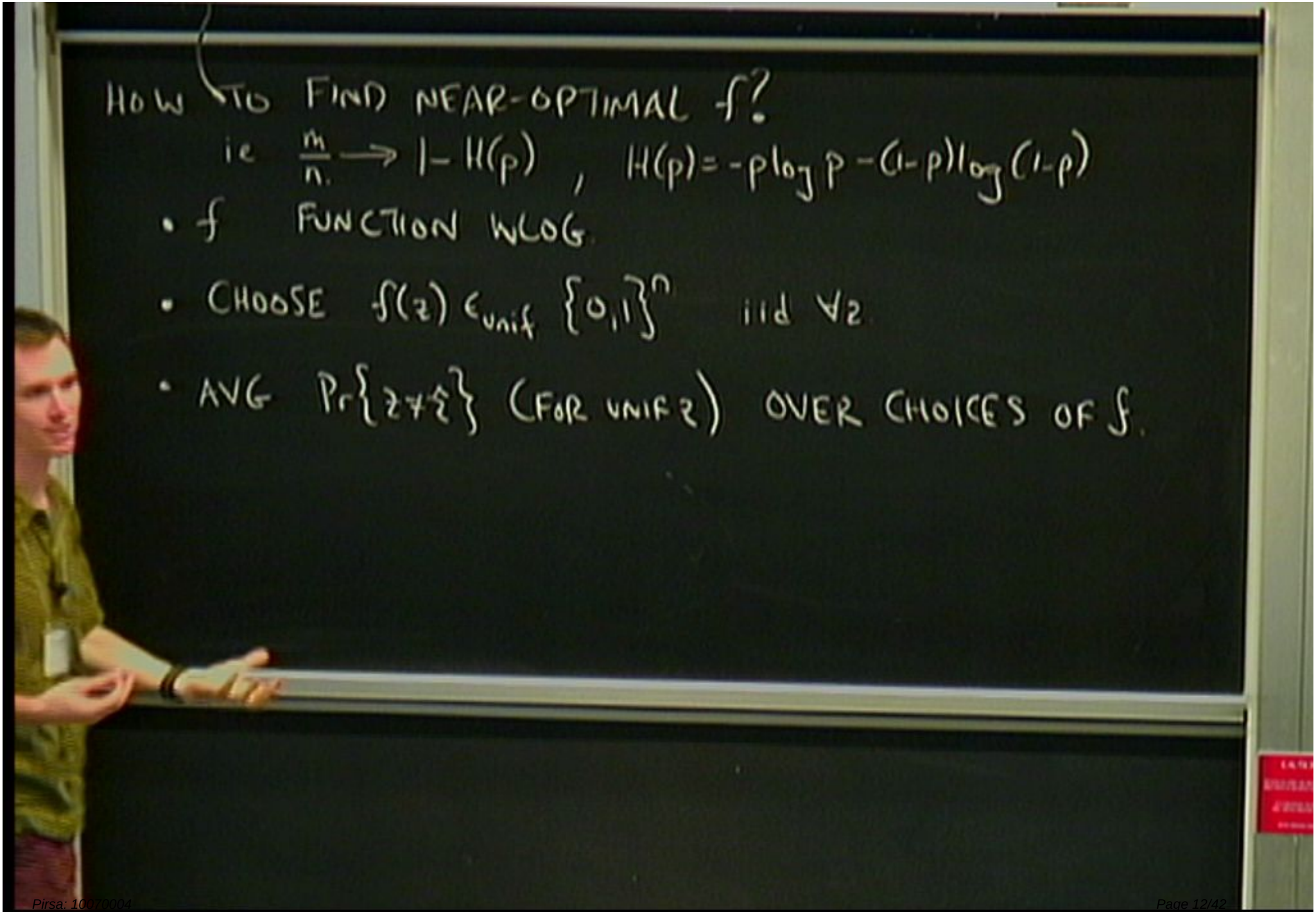
ie $\frac{m}{n} \longrightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p)\log(1-p)$

- f FUNCTION WLOG.

HOW TO FIND NEAR-OPTIMAL f?

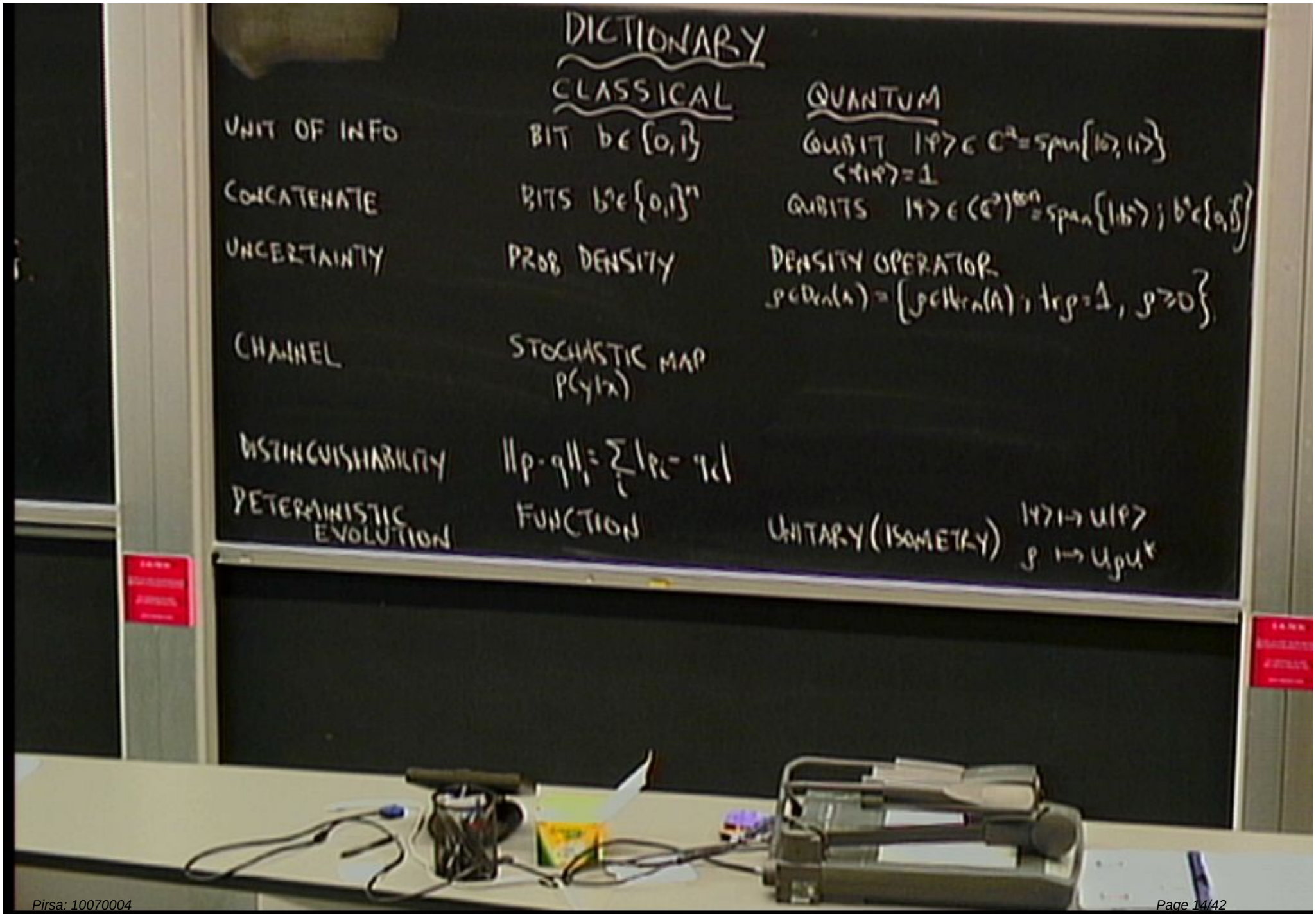
ie $\frac{m}{n} \longrightarrow 1 - H(p)$, $H(p) = -p \log p - (1-p)\log(1-p)$

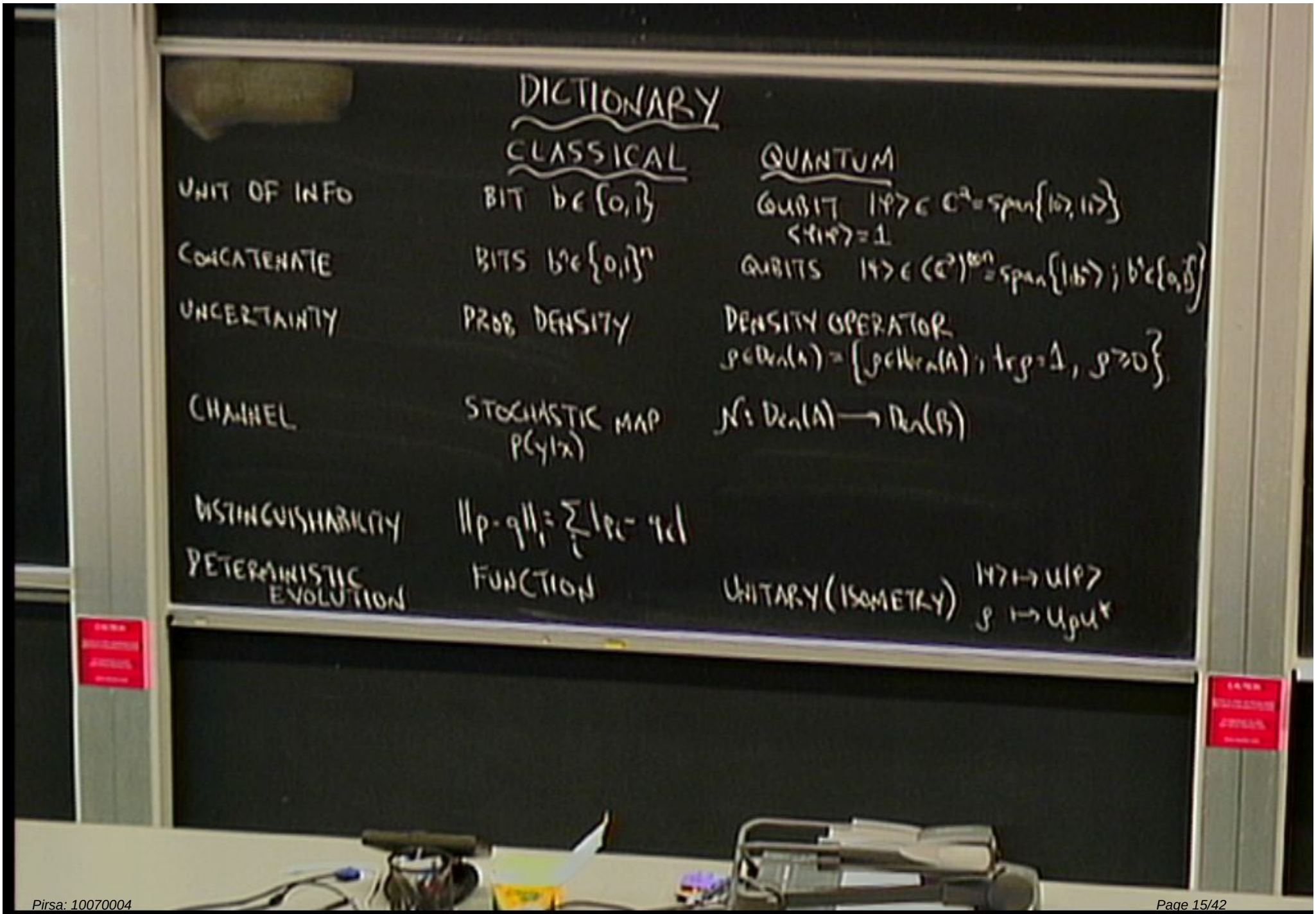
- f FUNCTION WLOG.
- CHOOSE $f(z) \in_{unif} \{0,1\}^n$ iid $\forall z$

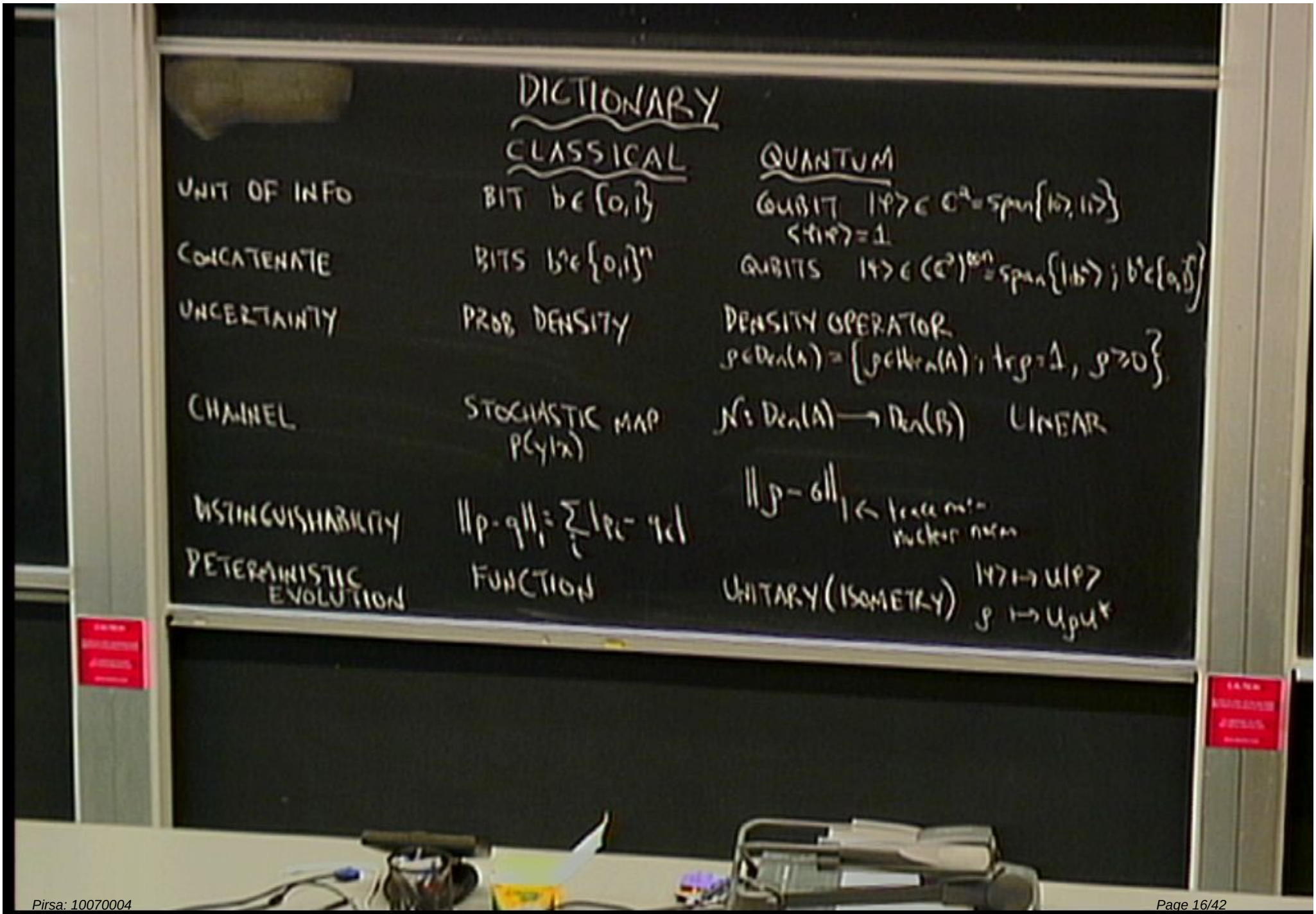

HOW TO FIND NEAR-OPTIMAL f?
ie $\frac{m}{n} \to 1 - H(p)$, $H(p) = -p \log p - (1-p)\log(1-p)$
• f FUNCTION WLOG
• CHOOSE $f(z) \in_{unif} \{0,1\}^n$ iid $\forall z$
• AVG $\Pr\{z \to \xi\}$ (FOR UNIF z) OVER CHOICES OF f.

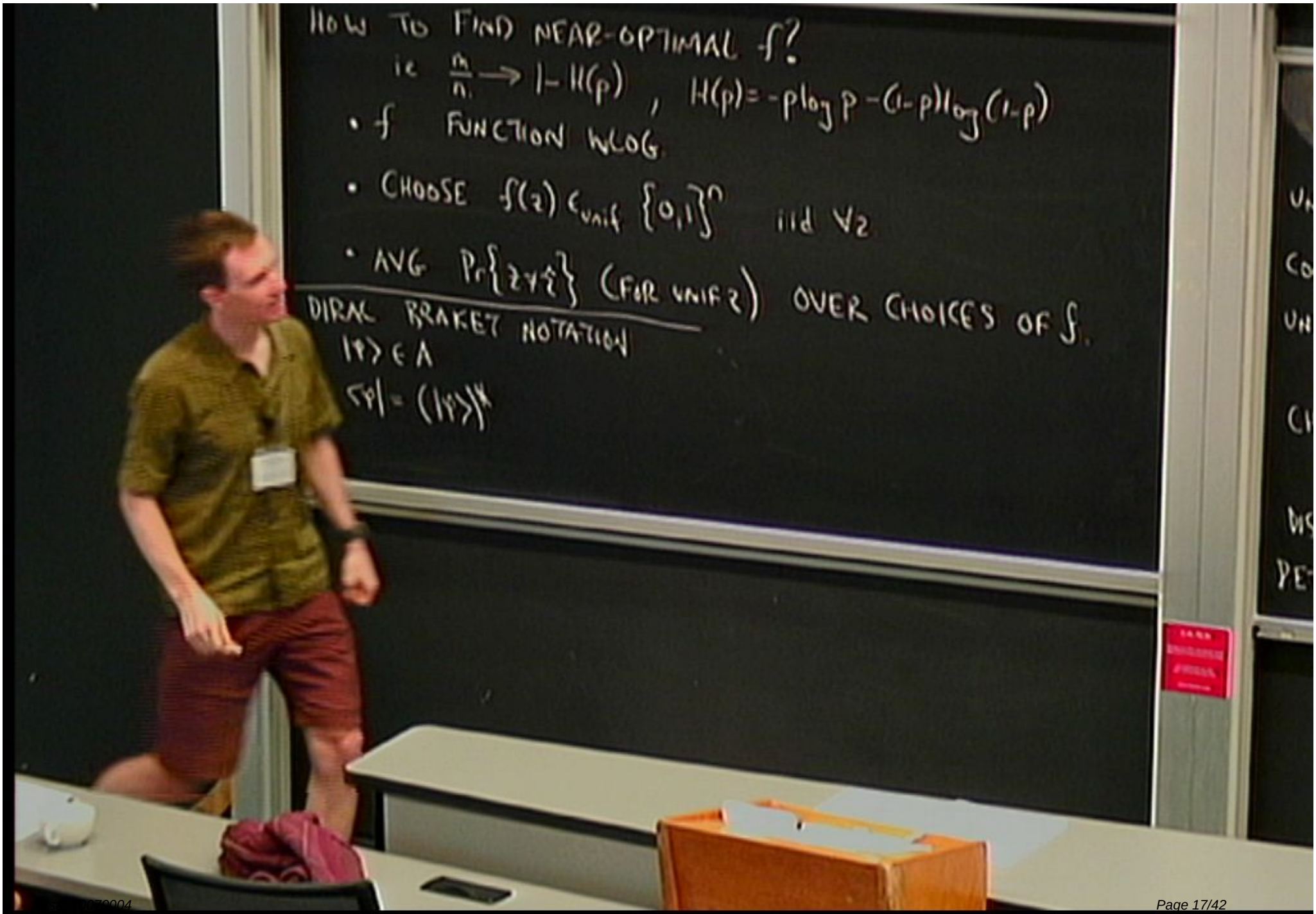
DICTIONARY

	CLASSICAL	QUANTUM
UNIT OF INFO	BIT $b \in \{0,1\}$	QUBIT $\|\psi\rangle \in \mathbb{C}^2 = \mathrm{span}\{\|0\rangle, \|1\rangle\}$ $\langle\psi\|\psi\rangle = 1$
CONCATENATE	BITS $b^n \in \{0,1\}^n$	QUBITS $\|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} = \mathrm{span}\{\|b\rangle : b^n \in \{0,1\}^n\}$
UNCERTAINTY	PROB DENSITY	
CHANNEL	STOCHASTIC MAP $P(y\|x)$	
DISTINGUISHABILITY	$\|p - q\|_1 = \sum_i \|p_i - q_i\|$	
DETERMINISTIC EVOLUTION	FUNCTION	UNITARY (ISOMETRY) $\|\psi\rangle \mapsto U\|\psi\rangle$ $\rho \mapsto U\rho U^*$


DICTIONARY
CLASSICAL
QUANTUM
UNIT OF INFO
BIT $b \in \{0,1\}$
QUBIT $|\psi\rangle \in \mathbb{C}^2 = \mathrm{span}\{|0\rangle, |1\rangle\}$
$\langle\psi|\psi\rangle = 1$
CONCATENATE
BITS $b^n \in \{0,1\}^n$
QUBITS $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} = \mathrm{span}\{|b\rangle\}; b^n \in \{0,1\}^n$
UNCERTAINTY
PROB DENSITY
DENSITY OPERATOR
$\rho \in \mathrm{Den}(A) = \{\rho \in \mathrm{Herm}(A); \mathrm{tr}\rho = 1, \rho \geq 0\}$
CHANNEL
STOCHASTIC MAP
$P(y|x)$
DISTINGUISHABILITY
$\|p - q\|_1 = \sum |p_x - q_x|$
DETERMINISTIC EVOLUTION
FUNCTION
UNITARY (ISOMETRY)
$|\psi\rangle \mapsto U|\psi\rangle$
$\rho \mapsto U\rho U^\dagger$


DICTIONARY
CLASSICAL
QUANTUM
UNIT OF INFO
BIT $b \in \{0,1\}$
QUBIT $|\psi\rangle \in \mathbb{C}^2 = \mathrm{span}\{|0\rangle, |1\rangle\}$
$\langle\psi|\psi\rangle = 1$
CONCATENATE
BITS $b^n \in \{0,1\}^n$
QUBITS $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} = \mathrm{span}\{|b\rangle\ ;\ b^n \in \{0,1\}^n\}$
UNCERTAINTY
PROB DENSITY
DENSITY OPERATOR
$\rho \in \mathrm{Den}(A) = \{\rho \in \mathrm{Herm}(A)\ ;\ \mathrm{tr}\rho = 1,\ \rho \geq 0\}$
CHANNEL
STOCHASTIC MAP
$p(y|x)$
$\mathcal{N}: \mathrm{Den}(A) \longrightarrow \mathrm{Den}(B)$
DISTINGUISHABILITY
$\|p - q\|_1 = \sum_x |p_x - q_x|$
DETERMINISTIC EVOLUTION
FUNCTION
UNITARY (ISOMETRY)
$|\psi\rangle \mapsto U|\psi\rangle$
$\rho \mapsto U\rho U^*$


DICTIONARY
CLASSICAL
QUANTUM
UNIT OF INFO
BIT $b \in \{0,1\}$
QUBIT $|\psi\rangle \in \mathbb{C}^2 = \mathrm{span}\{|0\rangle, |1\rangle\}$
$\langle\psi|\psi\rangle = 1$
CONCATENATE
BITS $b^n \in \{0,1\}^n$
QUBITS $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} = \mathrm{span}\{|b\rangle\,;\, b^n \in \{0,1\}^n\}$
UNCERTAINTY
PROB DENSITY
DENSITY OPERATOR
$\rho \in \mathrm{Den}(A) = \{\rho \in \mathrm{Herm}(A)\,;\, \mathrm{tr}\rho = 1,\ \rho \geq 0\}$
CHANNEL
STOCHASTIC MAP
$p(y|x)$
$\mathcal{N}: \mathrm{Den}(A) \longrightarrow \mathrm{Den}(B)$ LINEAR
DISTINGUISHABILITY
$\|p - q\|_1 = \sum_x |p_x - q_x|$
$\|\rho - \sigma\|_1$ ← trace norm
nuclear norm
DETERMINISTIC EVOLUTION
FUNCTION
UNITARY (ISOMETRY)
$|\psi\rangle \mapsto U|\psi\rangle$
$\rho \mapsto U\rho U^*$


HOW TO FIND NEAR-OPTIMAL f?
i.e. $\frac{n}{n} \to 1 - H(p)$, $H(p) = -p \log p - (1-p)\log(1-p)$
• f FUNCTION WLOG.
• CHOOSE $f(z) \in_{unif} \{0,1\}^n$ iid $\forall z$
• AVG $\Pr\{z \forall x\}$ (FOR UNIF z) OVER CHOICES OF f.
DIRAC BRAKET NOTATION
$|\psi\rangle \in A$
$\langle\psi| = (|\psi\rangle)^\dagger$

• AVG $\Pr\{z \neq \xi\}$ (FOR UNIF z) OVE

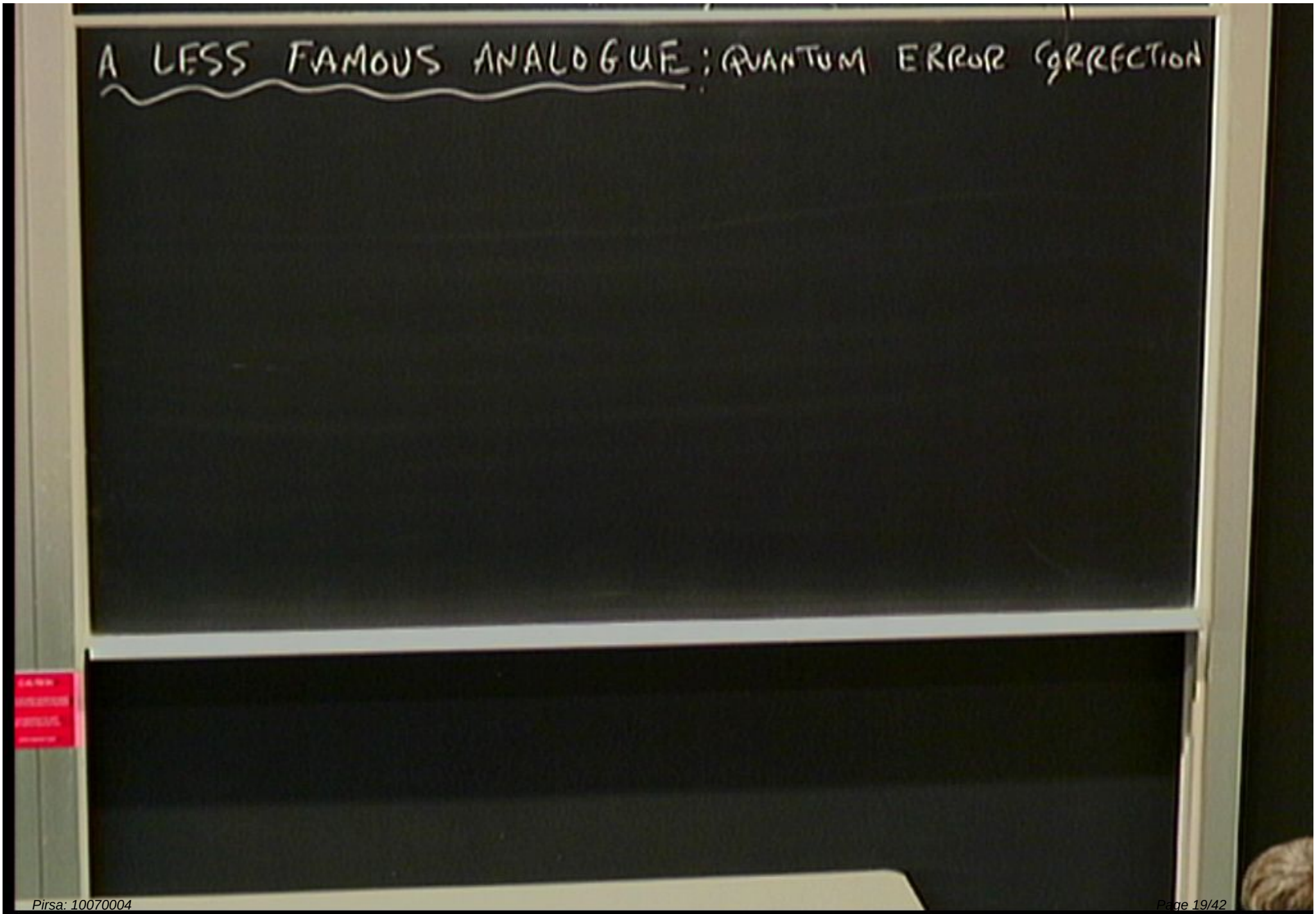
DIRAC BRAKET NOTATION

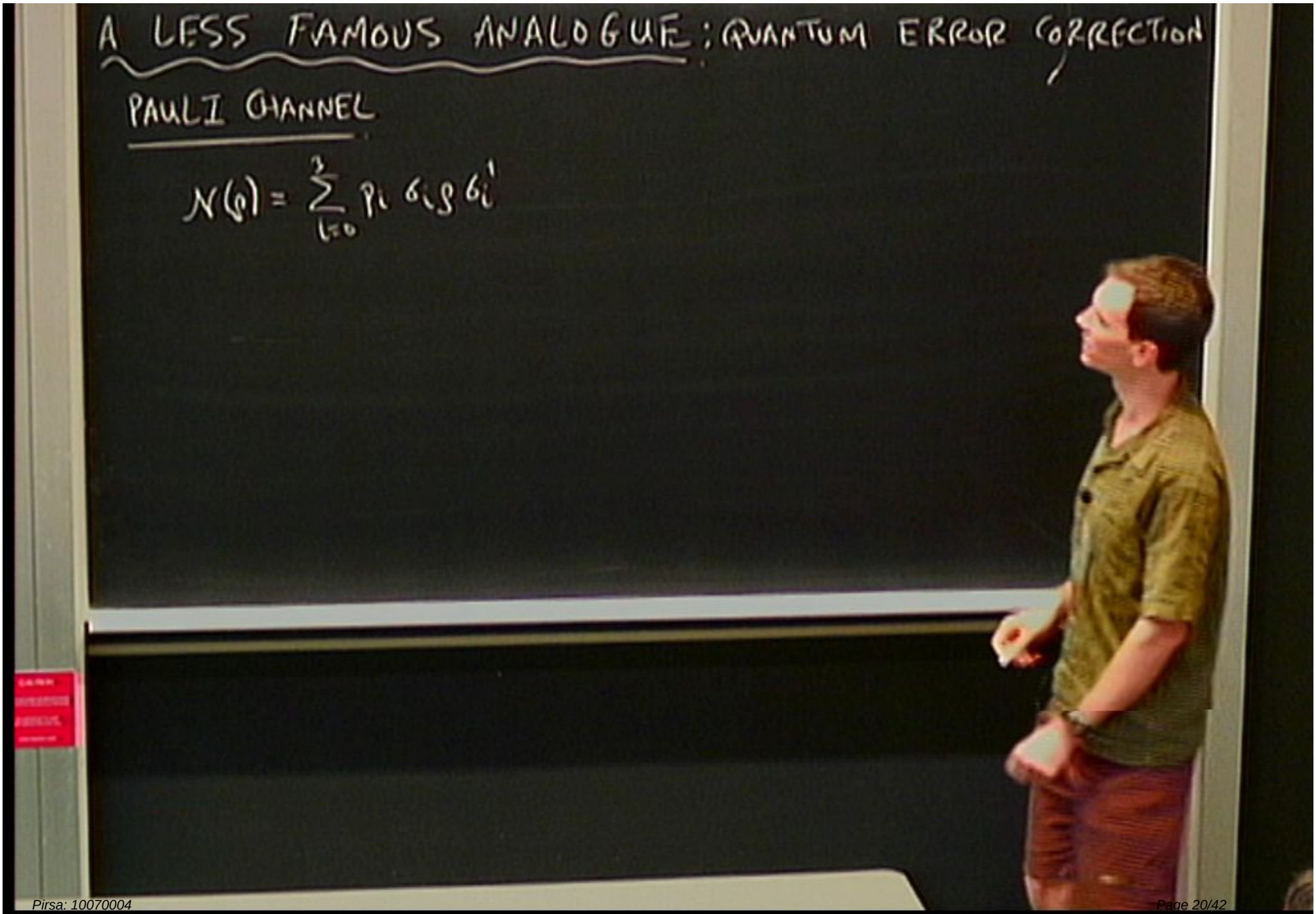
$|\varphi\rangle \in A$

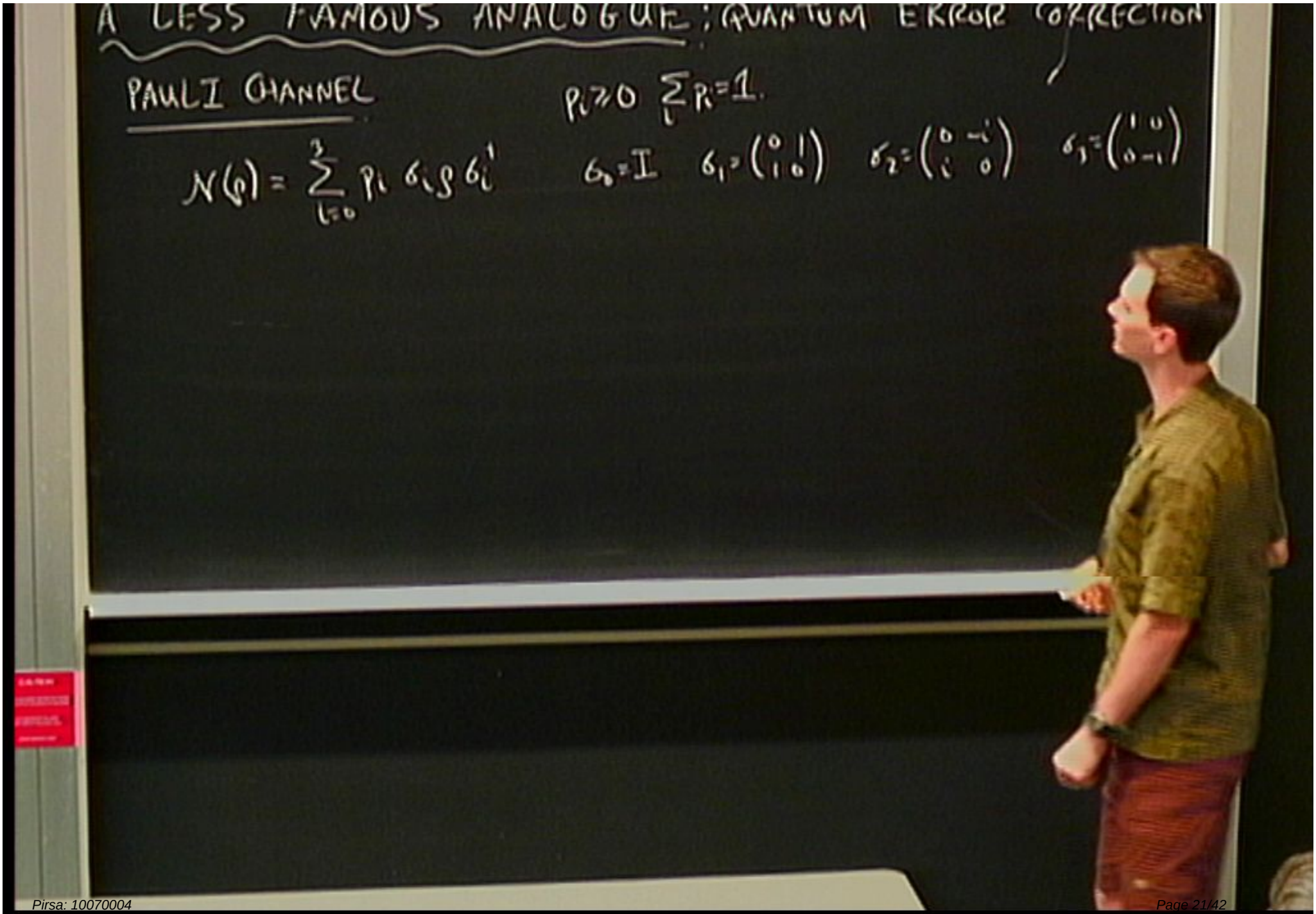
$\langle\varphi| = (|\varphi\rangle)^*$

$\langle\varphi|\psi\rangle$ INNER PRODUCT

$|\varphi\rangle\langle\varphi|$


A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION


A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION
PAULI CHANNEL
$N(\rho) = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i$


A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION
PAULI CHANNEL
$p_i \geq 0 \quad \sum_i p_i = 1.$
$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i^\dagger$
$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

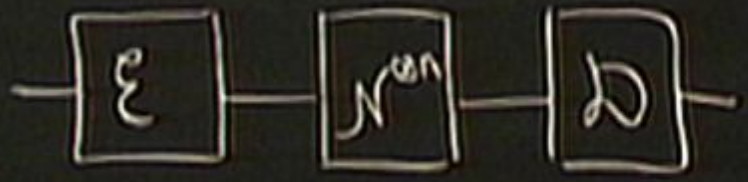
A CLASS FAMOUS FOR ACRONYMS: QUANTUM ERROR CORRECTION

PAULI CHANNEL

$p_i \geq 0 \quad \sum_i p_i = 1.$

$$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \, \sigma_i \rho \sigma_i^\dagger$$

$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$



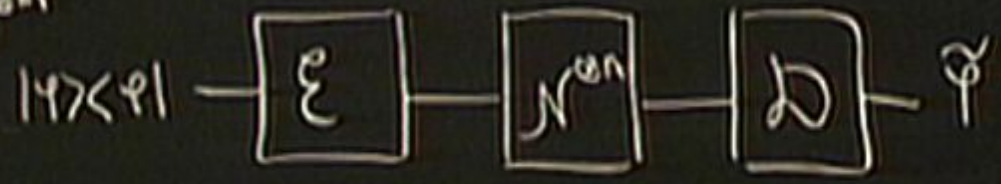
PAULI CHANNEL

$p_i \geq 0 \quad \sum_i p_i = 1$

$$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \, \sigma_i \rho \sigma_i^\dagger$$

$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|\psi\rangle \in (\mathbb{C}^2)^{\otimes m}$



PAULI CHANNEL

$p_i \geq 0 \quad \sum_i p_i = 1.$

$$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \, \sigma_i \rho \sigma_i^\dagger$$

$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\forall |\psi\rangle \quad \| |\psi\rangle\langle\psi| - \mathcal{D} \| < \epsilon$

$\epsilon \xrightarrow{n \to \infty} 0$

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

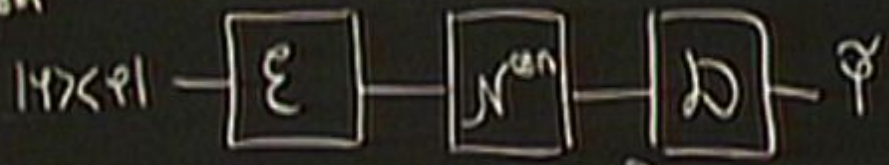
PAULI CHANNEL

$p_i \geq 0 \quad \sum_i p_i = 1$

$$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i^\dagger$$

$\sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$



$\forall |\psi\rangle \quad \| |\psi\rangle\langle\psi| - \rho \| < \epsilon$

$\epsilon \xrightarrow{n \to \infty} 0$

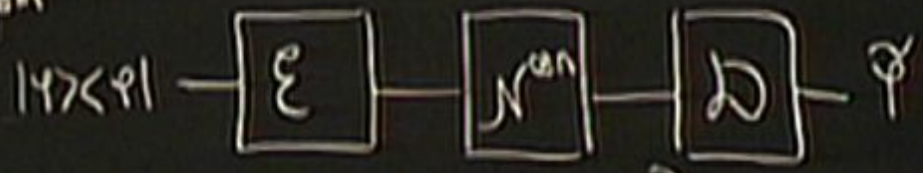
HOW TO FIND A GOOD $\mathcal{E}$?

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL $p_i \geq 0$ $\sum p_i = 1$

$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i^\dagger$ $\sigma_0 = I$ $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|\psi\rangle \in (\mathbb{C}^2)^{\otimes m}$



$\forall |\psi\rangle \quad \| |\psi\rangle\langle\psi| - \Psi \| < \epsilon$

$\epsilon \xrightarrow{n \to \infty} 0$

HOW TO FIND A GOOD $\mathcal{E}$?

• USE ISOMETRY $\mathcal{E}(\cdot) = E \cdot E^\dagger$

A LESS FAMOUS ANALOGUE: QUANTUM ERROR CORRECTION

PAULI CHANNEL $p_i \geq 0$ $\sum_i p_i = 1$

$$\mathcal{N}(\rho) = \sum_{i=0}^{3} p_i \sigma_i \rho \sigma_i^\dagger \qquad \sigma_0 = I \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

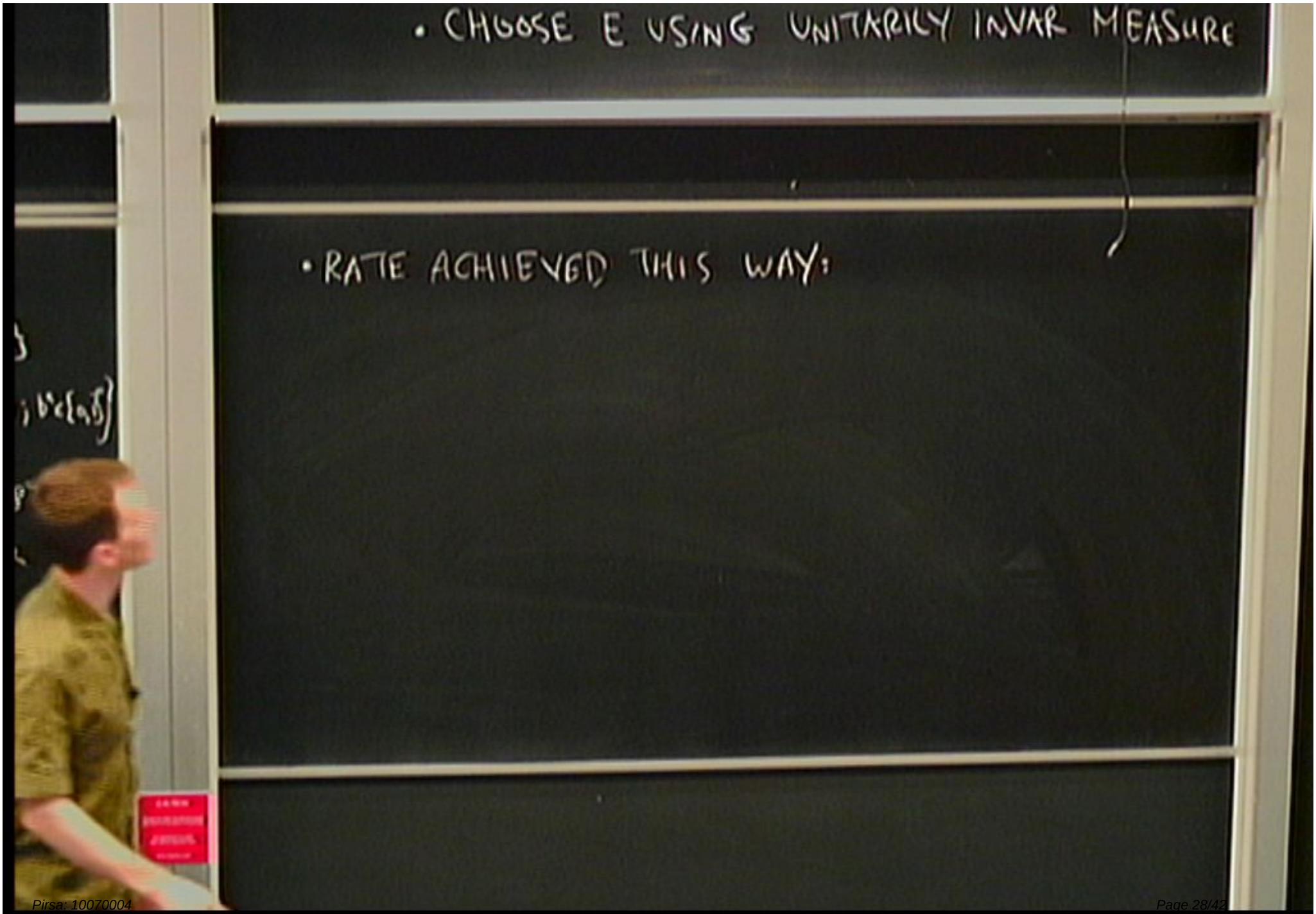
$|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

$\forall |\psi\rangle \quad \| |\psi\rangle\langle\psi| - \Psi \| < \epsilon$

$\epsilon \xrightarrow{n \to \infty} 0$

HOW TO FIND A GOOD $\mathcal{E}$?

- USE ISOMETRY $\mathcal{E}(\cdot) = E \cdot E^\dagger$
- CHOOSE E USING UNITARILY INVAR MEASURE


• CHOOSE E USING UNITARILY INVAR MEASURE
• RATE ACHIEVED THIS WAY:

- CHOOSE E USING UNITARILY INVAR MEASURE

- RATE ACHIEVED THIS WAY:

$$\frac{m}{n} \longrightarrow$$

- RATE ACHIEVED THIS WAY:

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) = -\sum_i p_i \log p_i$$

- RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) := -\sum_i p_i \log p_i$$

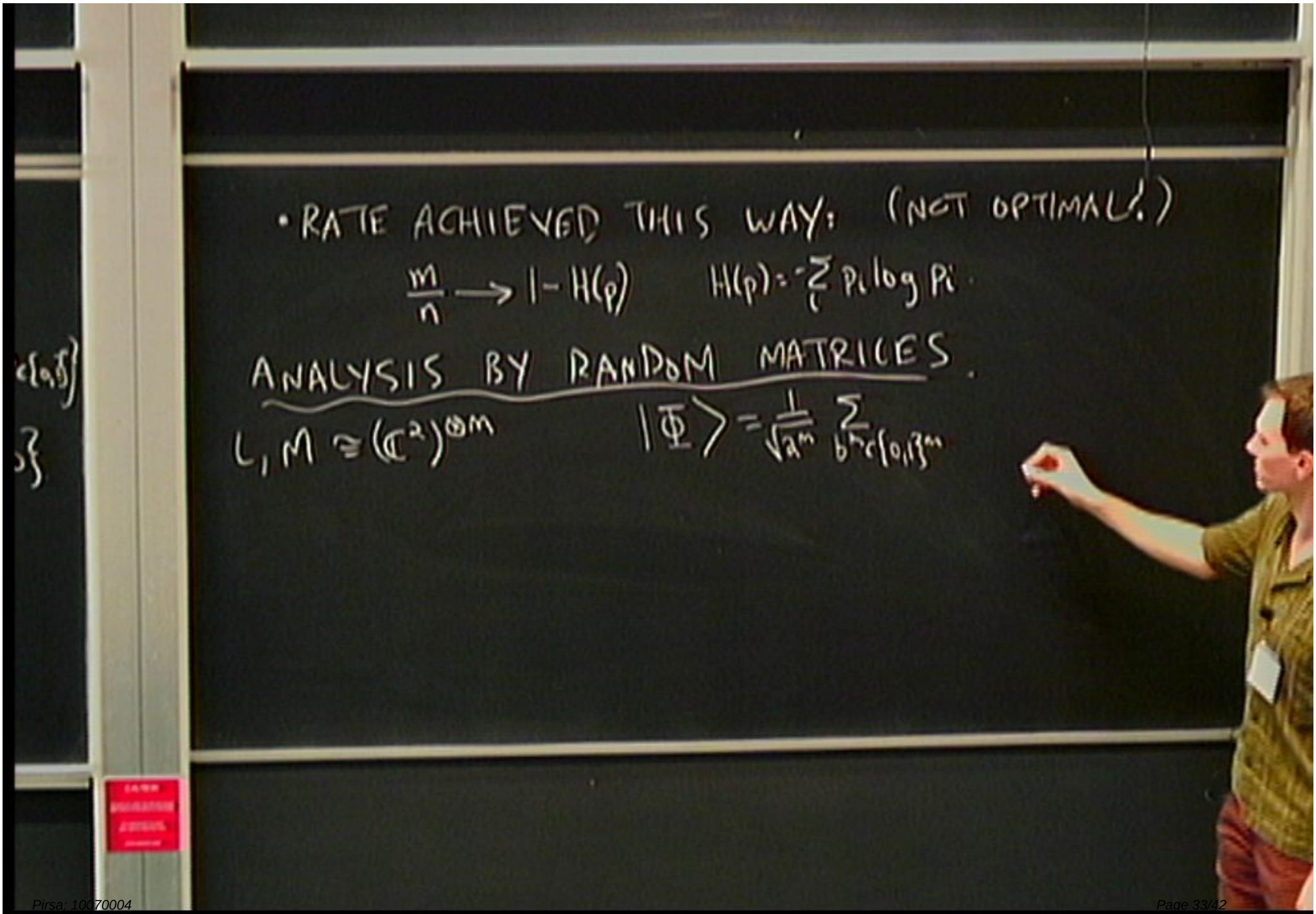
ANALYSIS BY RANDOM MATRICES.

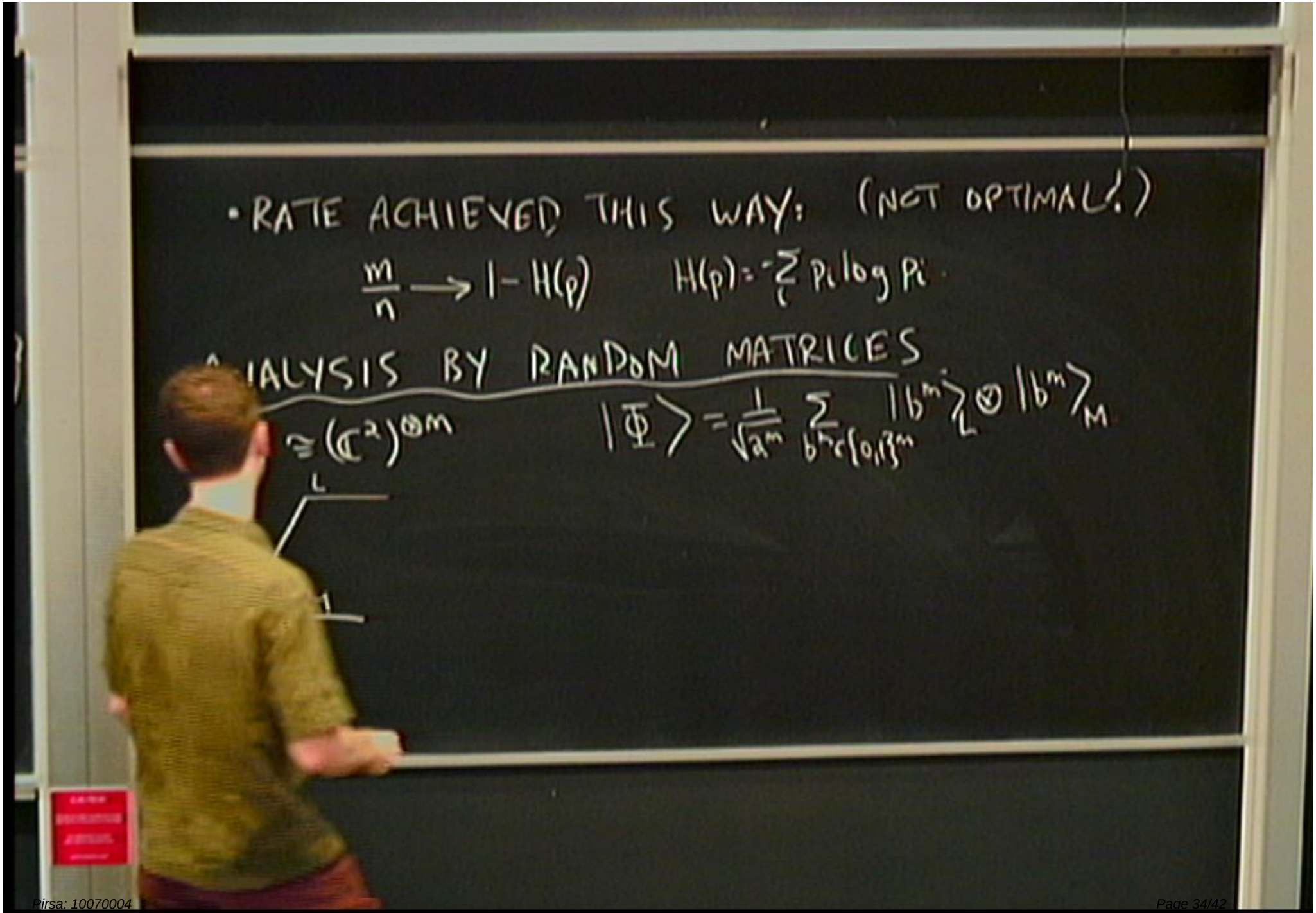
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES.

$L, M \cong (\mathbb{C}^2)^{\otimes m}$


• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)
$\frac{m}{n} \to 1 - H(p)$ $H(p) = -\sum_i p_i \log p_i$
ANALYSIS BY RANDOM MATRICES
$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $|\Phi\rangle = \frac{1}{\sqrt{2^m}} \sum_{b_1 \ldots b_m \in \{0,1\}^m}$

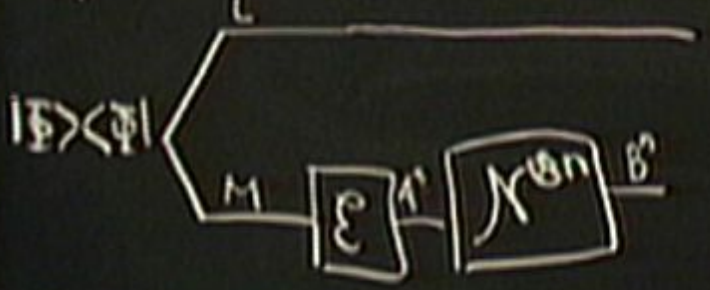

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)
$\frac{m}{n} \longrightarrow 1 - H(p)$ $H(p) = -\sum_i p_i \log p_i$
ALYSIS BY RANDOM MATRICES
$\cong (\mathbb{C}^2)^{\otimes m}$
$|\Phi\rangle = \frac{1}{\sqrt{a^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$\frac{m}{n} \longrightarrow 1 - H(p)$ $\quad H(p) := -\sum_i p_i \log p_i$

ANALYSIS BY RANDOM MATRICES

$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $\quad |\Phi\rangle_{LM} = \frac{1}{\sqrt{2^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$



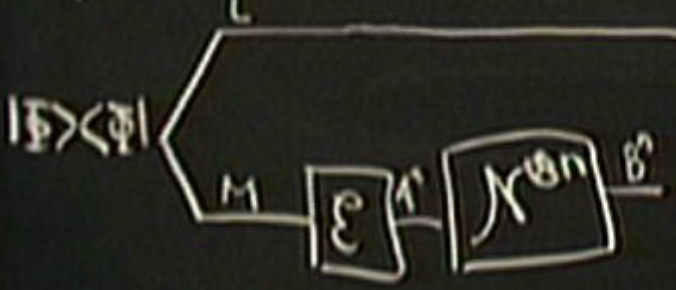
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) := -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $\qquad |\Phi\rangle_M = \frac{1}{\sqrt{2^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$

NOTE: $\mathcal{N}(\rho) = \mathrm{tr}_C U_{\mathcal{N}} \rho U_{\mathcal{N}}^*$



$U : A \longrightarrow B \otimes C$

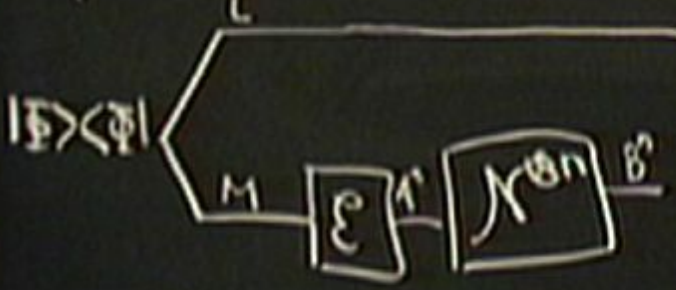
• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) := -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $\qquad |\Phi\rangle_M = \frac{1}{\sqrt{2^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$

NOTE: $\mathcal{N}(\rho) = \mathrm{tr}_C U_{\mathcal{N}} \rho U_{\mathcal{N}}^{\dagger}$



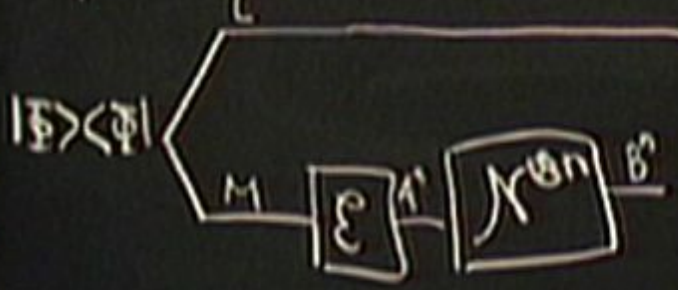
$U : A \longrightarrow B \otimes C$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$\frac{m}{n} \longrightarrow 1 - H(p)$ $\quad H(p) := -\sum_i p_i \log p_i$

ANALYSIS BY RANDOM MATRICES

$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $\quad |\Phi\rangle_M = \frac{1}{\sqrt{2^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle_M$



NOTE: $\mathcal{N}(\rho) = \mathrm{tr}_C U_{\mathcal{N}} \rho U_{\mathcal{N}}^\dagger$

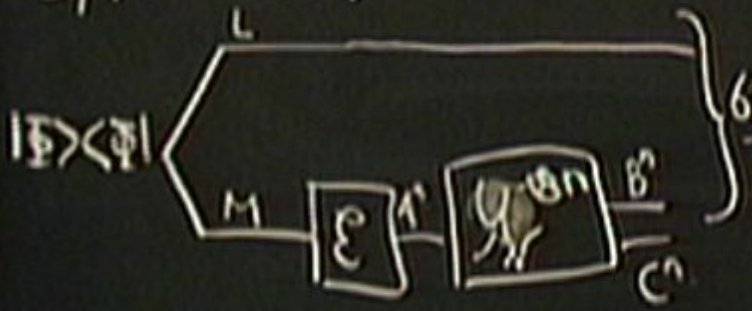
$U_{\mathcal{N}} : A \to B \otimes C$ $\quad U_{\mathcal{N}} |\psi\rangle = \sum_{i=0}^{2} \sqrt{p_i}\, \sigma_i |\psi\rangle_B |i\rangle_C$

• RATE ACHIEVED THIS WAY: (NOT OPTIMAL!)

$$\frac{m}{n} \longrightarrow 1 - H(p) \qquad H(p) = -\sum_i p_i \log p_i$$

ANALYSIS BY RANDOM MATRICES

$L, M \cong (\mathbb{C}^2)^{\otimes m}$ $\qquad |\Phi\rangle_M = \frac{1}{\sqrt{2^m}} \sum_{b^m \in \{0,1\}^m} |b^m\rangle_L \otimes |b^m\rangle$

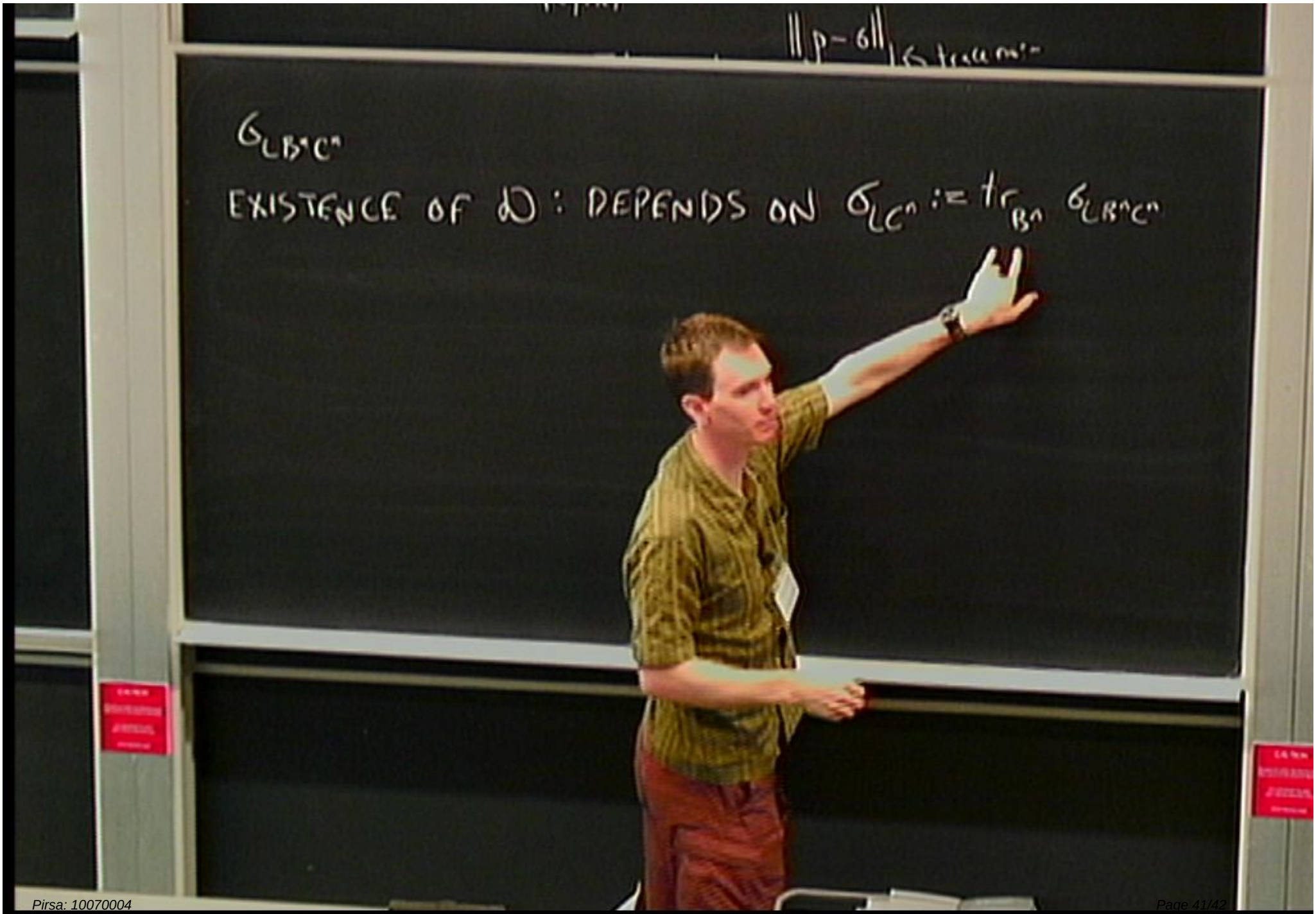


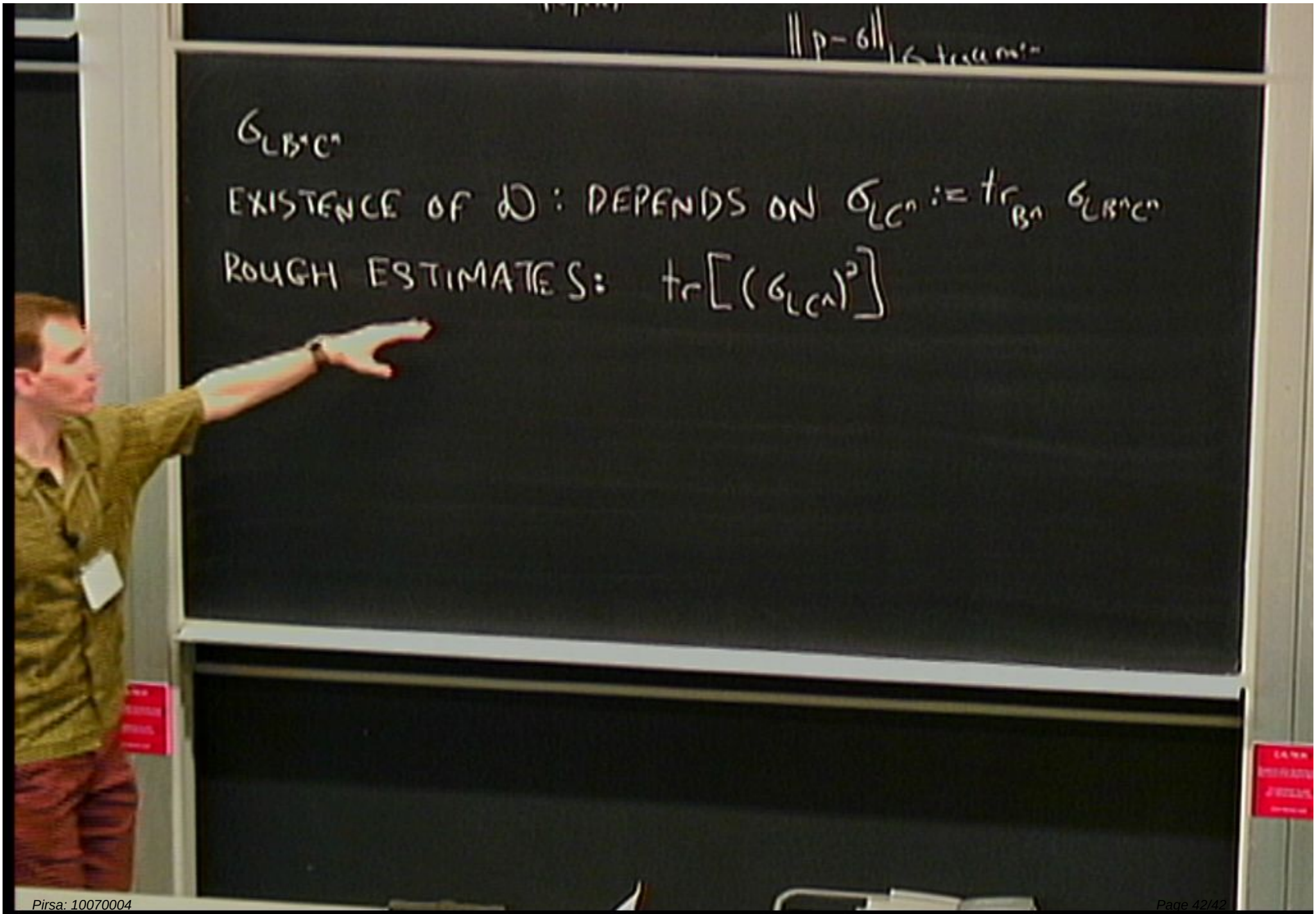
$|\Phi\rangle\langle\Phi|$ $\qquad$ block-wise $U_x : A \to B \otimes C$ $\qquad$ NOTE: $\chi(\rho) =$ $\qquad$ $U_x|\psi\rangle = \sum_{i=0}^{2} \sqrt{p_i}$

$\|p - 6\|$

GLB'C"

EXISTENCE OF $\mathcal{D}$


$\sigma_{LB'C''}$
EXISTENCE OF $\mathcal{D}$: DEPENDS ON $\sigma_{LC''} := tr_{B'} \sigma_{LB'C''}$


$G_{LB^nC^n}$
EXISTENCE OF ∂ : DEPENDS ON $\sigma_{LC^n} := tr_{B^n} G_{LB^nC^n}$
ROUGH ESTIMATES: $tr[(G_{LC^n})^2]$