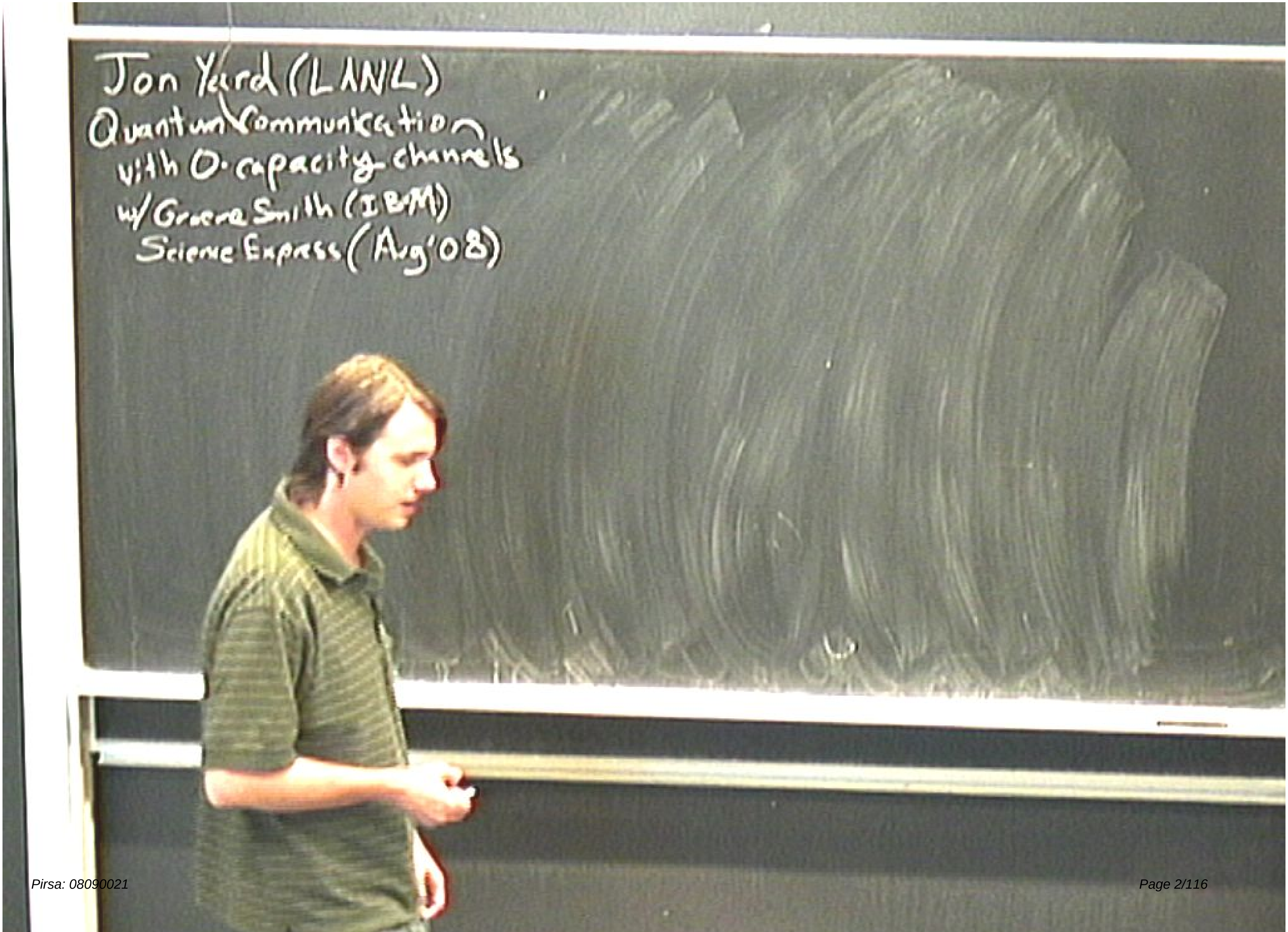
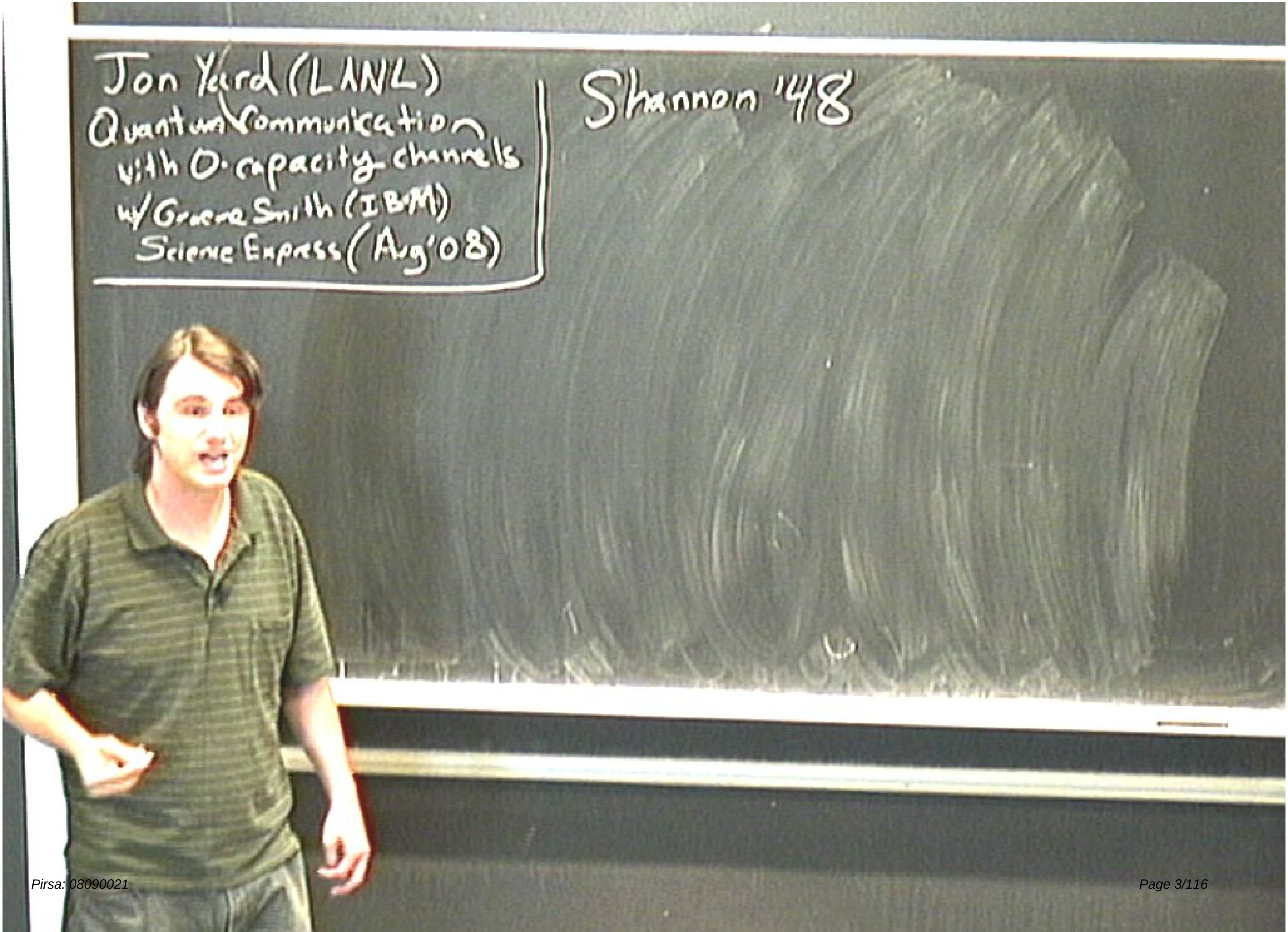
Title: Quantum communication with zero-capacity channels

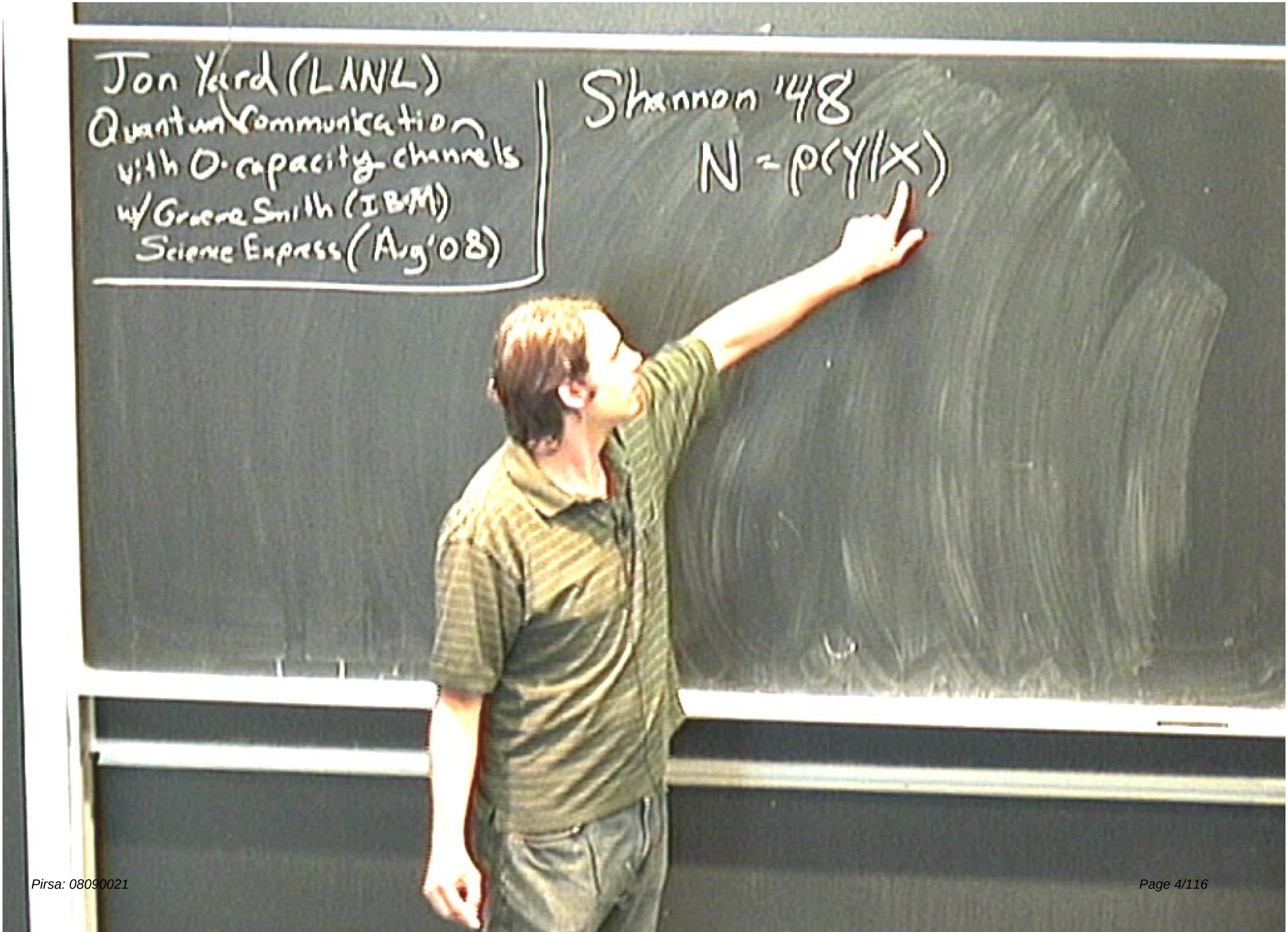
Date: Sep 24, 2008 04:00 PM

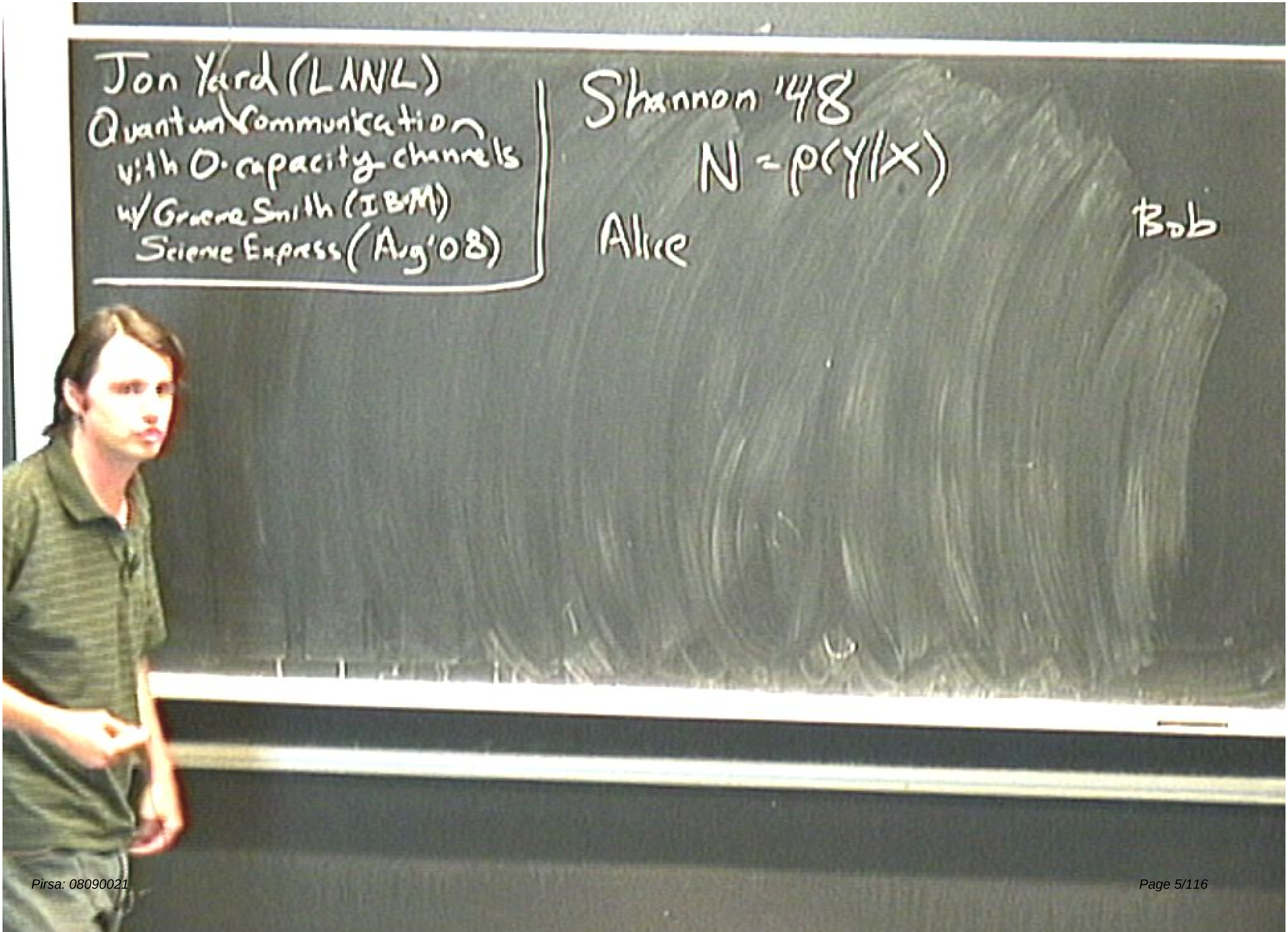
URL: http://pirsa.org/08090021

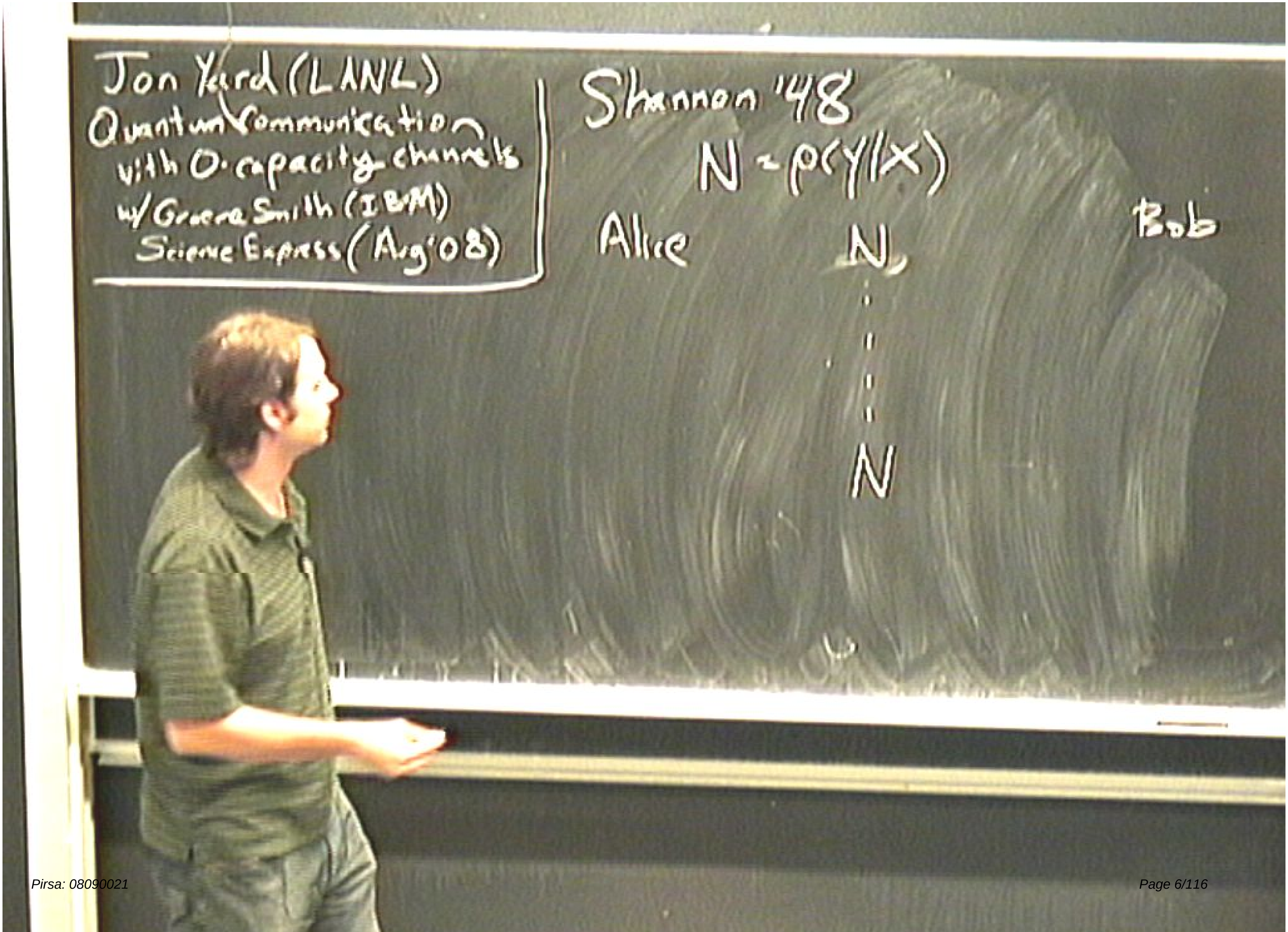
Abstract: A quantum channel models a physical process in which noise is added to a quantum system via interaction with its environment. Protecting quantum systems from such noise can be viewed as an extension of the classical communication problem introduced by Shannon sixty years ago. A fundamental quantity of interest is the quantum capacity of a given channel, which measures the amount of quantum information which can be protected, in the limit of many transmissions over the channel. In this talk, I will show that certain pairs of channels, each with a capacity of zero, can have a strictly positive capacity when used together, implying that the quantum capacity does not completely characterize a channel\'s ability to transmit quantum information. As a corollary, I will show that a commonly used lower bound on the quantum capacity - the coherent information, or hashing bound - is an overly pessimistic benchmark against which to measure the performance of quantum error correction because the gap between this bound and the capacity can be arbitrarily large.

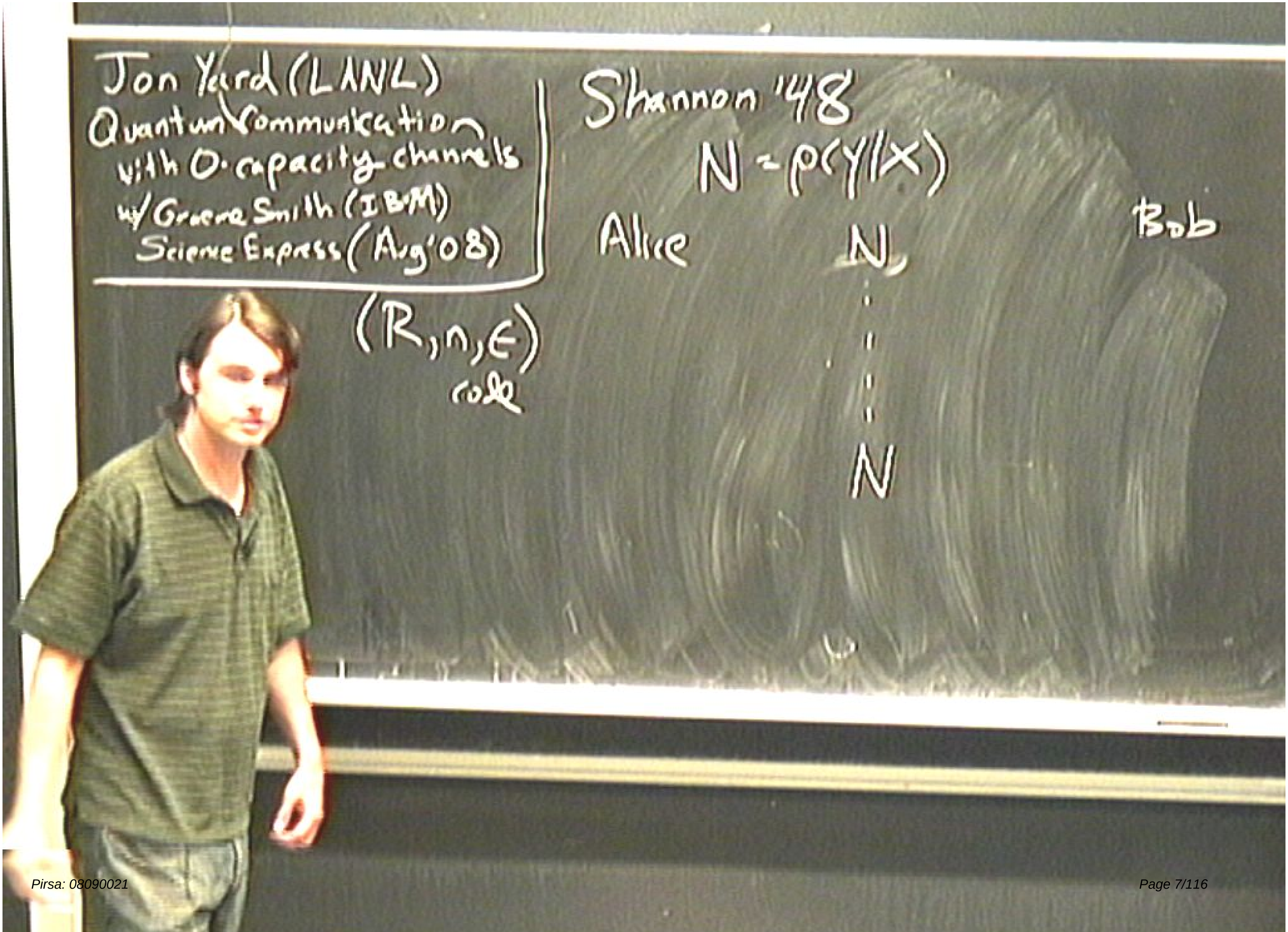

Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)


Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug'08)
Shannon '48

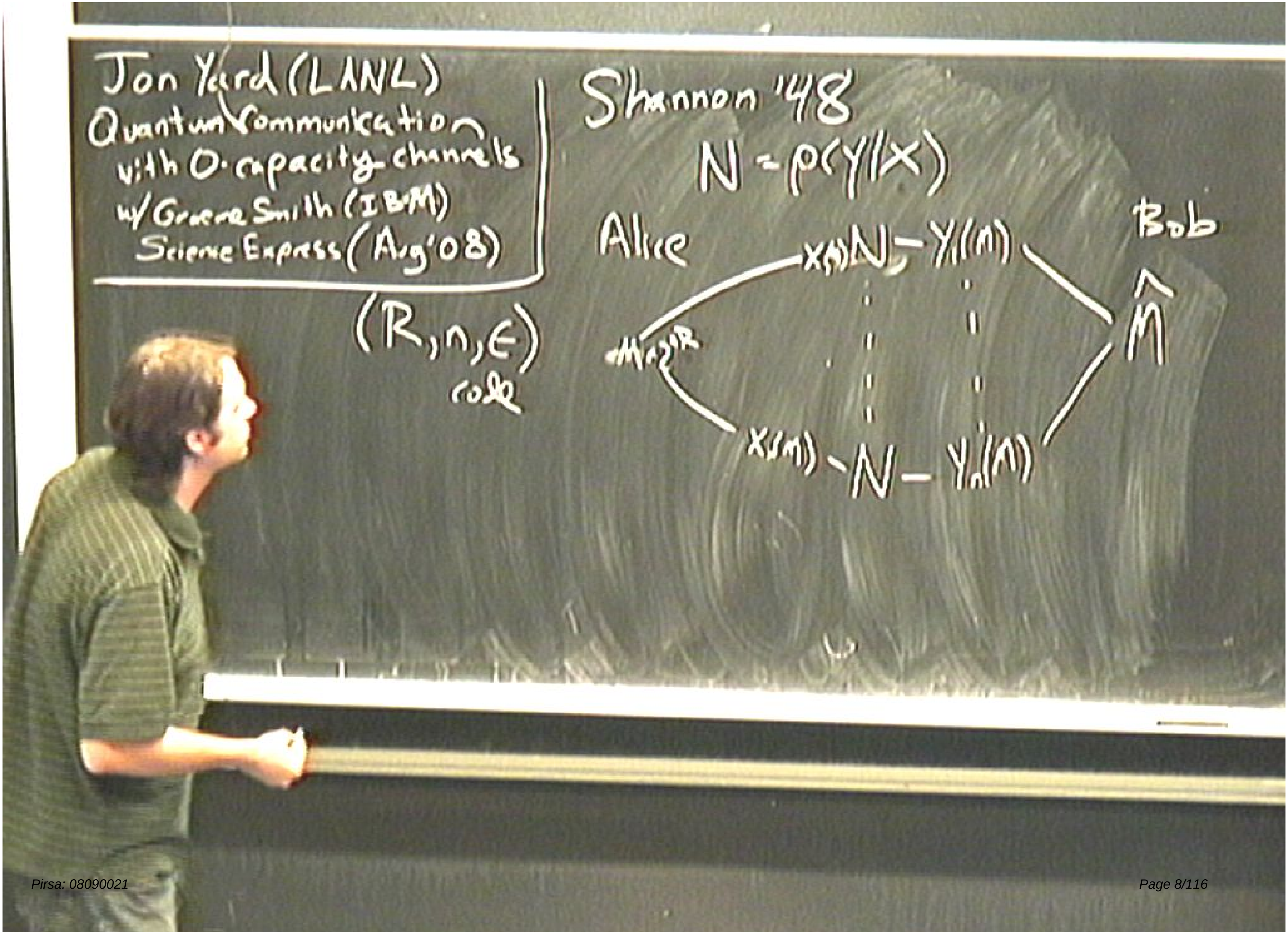

Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
Shannon '48
N = p(Y|X)

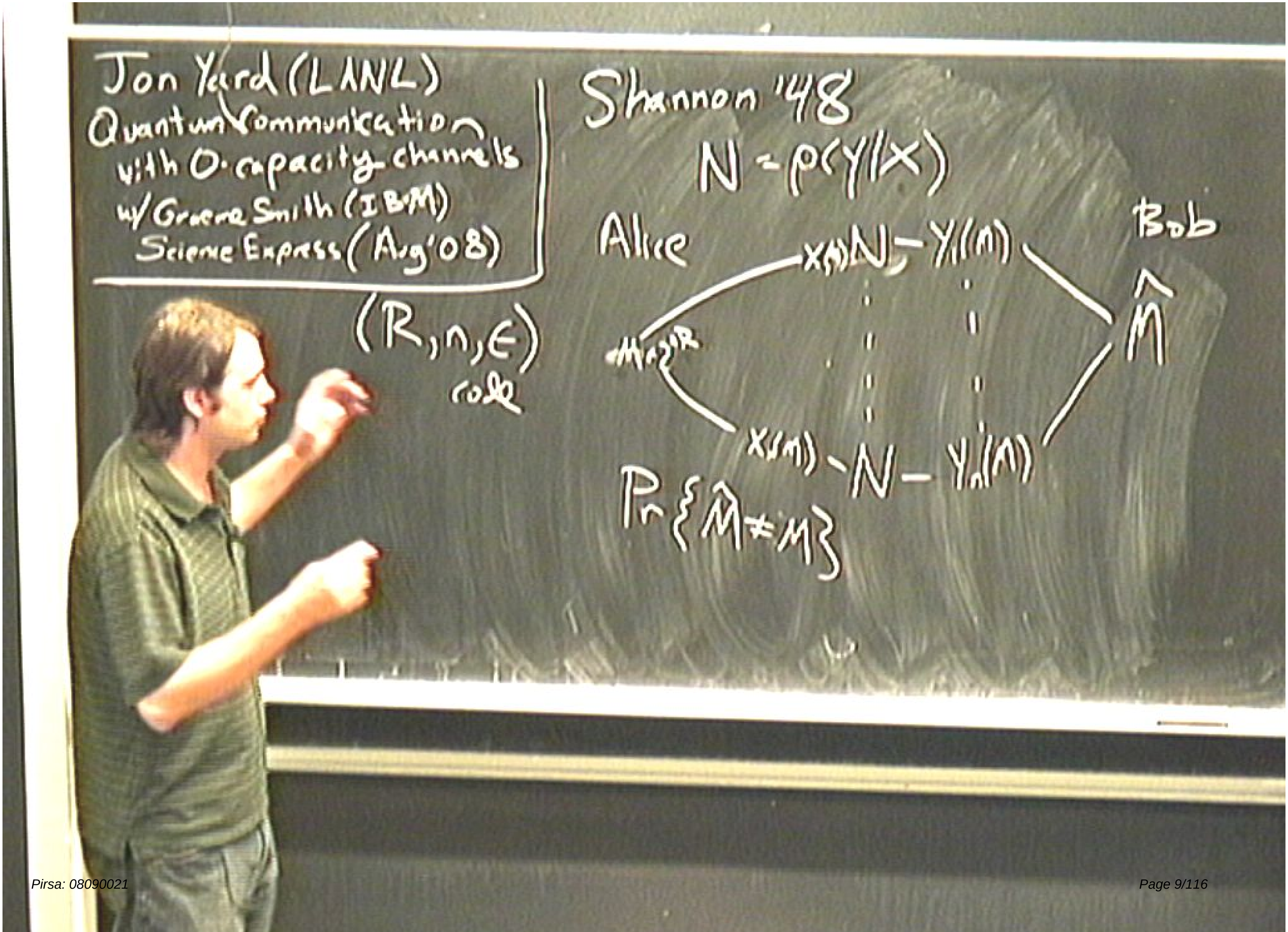

Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
Shannon '48
N = p(y|x)
Alice
Bob

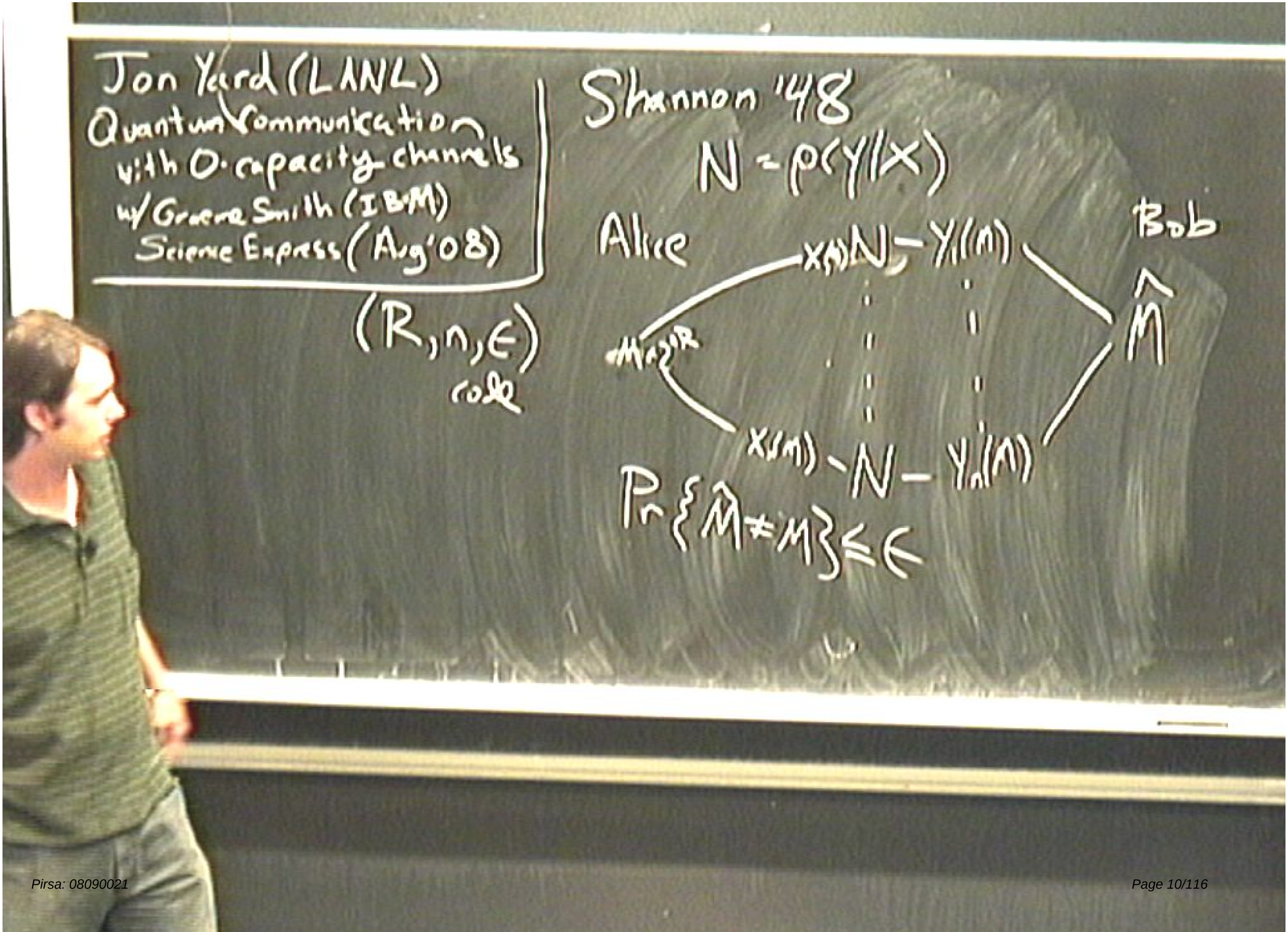

Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
Shannon '48
N = p(Y|X)
Alice
N
N
Bob

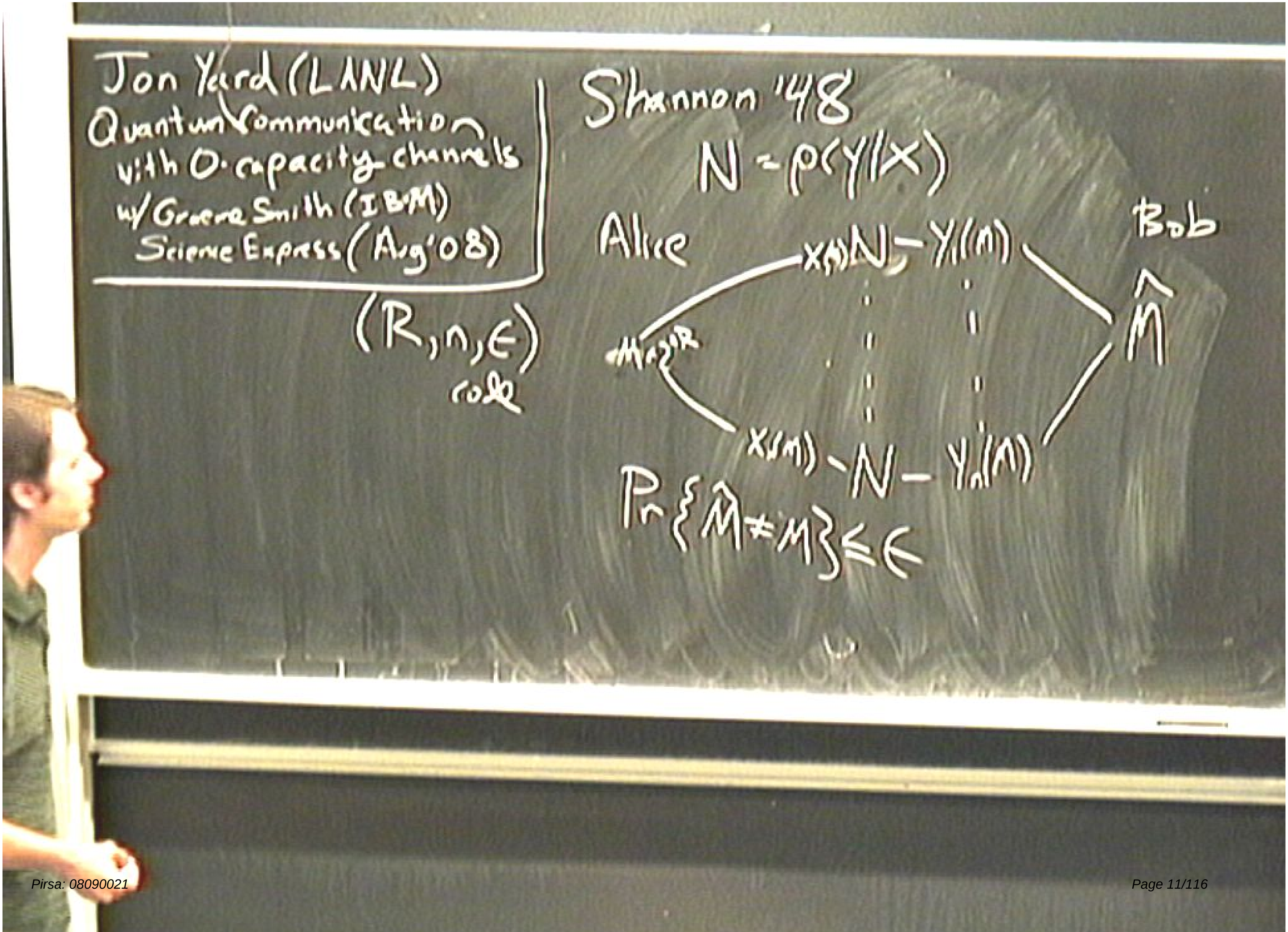


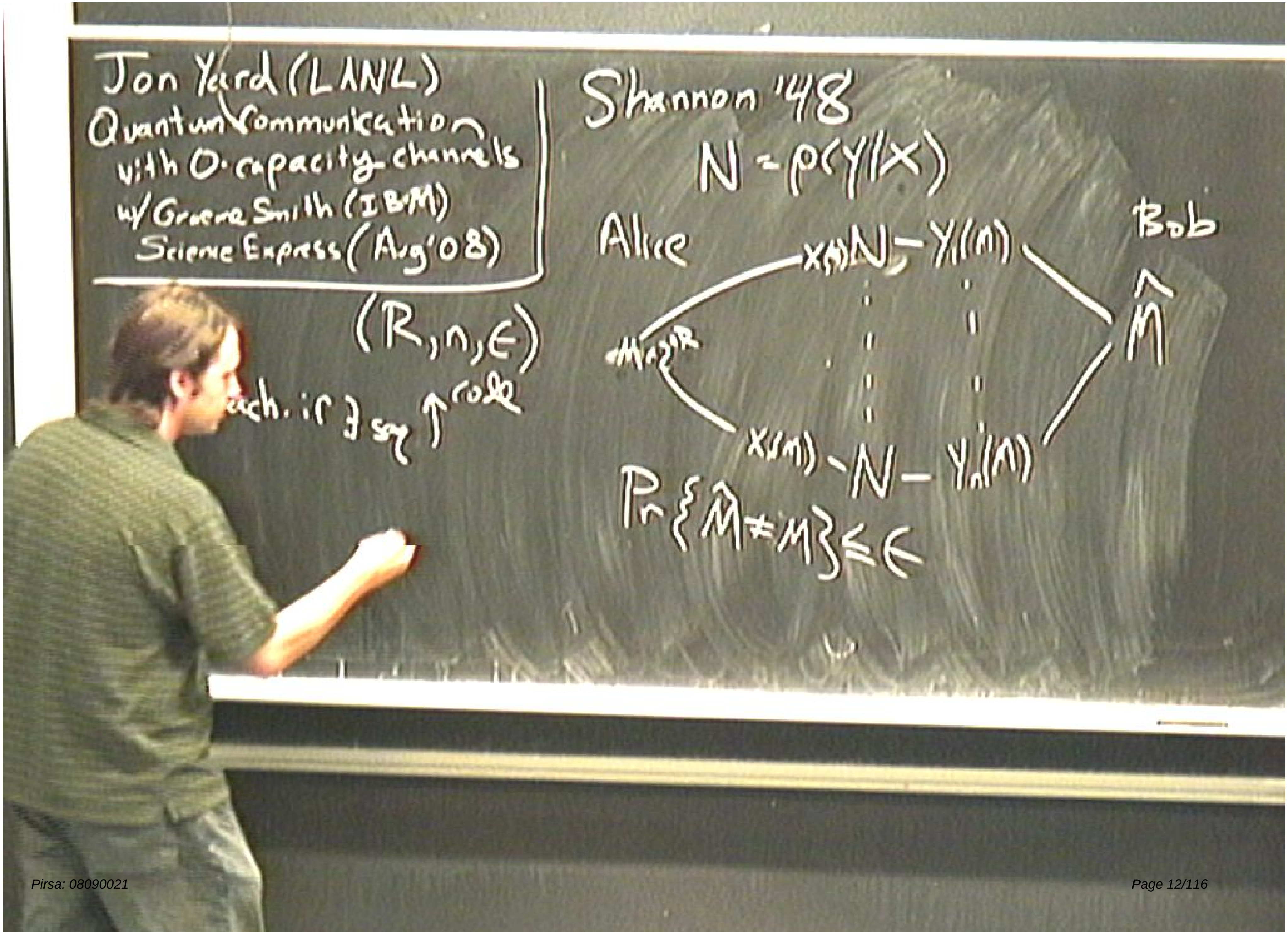
Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
(R, n, ε)
code
Shannon '48
N = p(y|x)
Alice
N
N
Bob


Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
(R, n, ε)
code
Shannon '48
N = p(Y|X)
Alice
Bob
$X_1(M)$ – N – $Y_1(M)$
$M \in 2^{nR}$
$X_n(M)$ – N – $Y_n(M)$
$\hat{M}$


Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
(R, n, ϵ)
code
Shannon '48
$N = p(Y|X)$
Alice
Bob
$X_1(M)$ — N — $Y_1(M)$
$M \in 2^{nR}$
$X_n(M)$ — N — $Y_n(M)$
$\hat{M}$
$\Pr\{\hat{M} \neq M\}$


Jon Yard (LANL)
Quantum Communication with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
Shannon '48
N = p(Y|X)
Alice
Bob
(R, n, ε)
rate
Pr{M̂ ≠ M} ≤ ε


Jon Yard (LANL)
Quantum Communication with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
(R, n, ε) code
Shannon '48
N = p(Y|X)
Alice
Bob
M ∈ 2^{nR}
X₁(M) N – Y₁(M)
Xₙ(M) – N – Yₙ(M)
M̂
Pr{M̂ ≠ M} ≤ ε


Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)
(R, n, ε)
ach. if ∃ seq ↑ code
Shannon '48
N = p(Y|X)
Alice
Bob
X1(M) N − Y1(M)
M ∈ 2^nR
Xn(M) − N − Yn(M)
M̂
Pr{M̂ ≠ M} ≤ ε

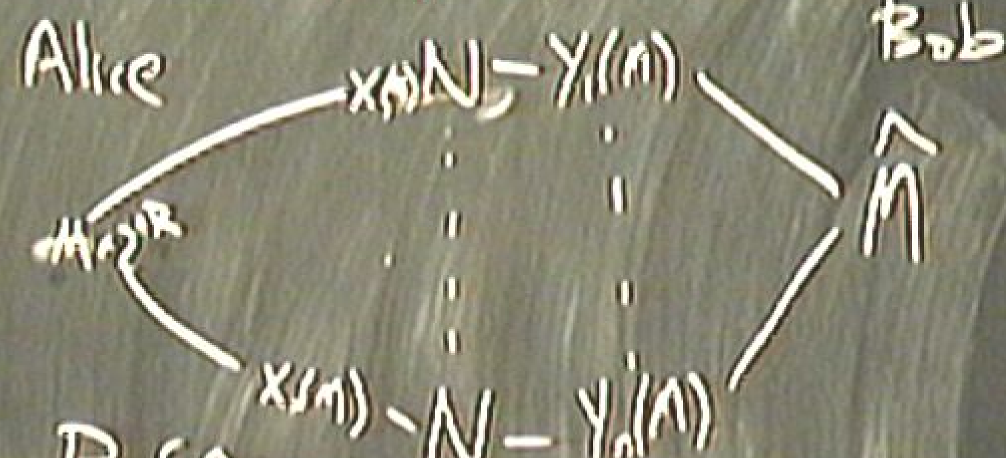
Jon Yard (LANL)
Quantum Communication with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)

(R, n, ϵ)

R ach. if $\exists$ seq $\uparrow$ rate, $\epsilon \to 0$

Shannon '48

$N = p(Y|X)$



$\Pr\{\hat{M} \neq M\} \leq \epsilon$

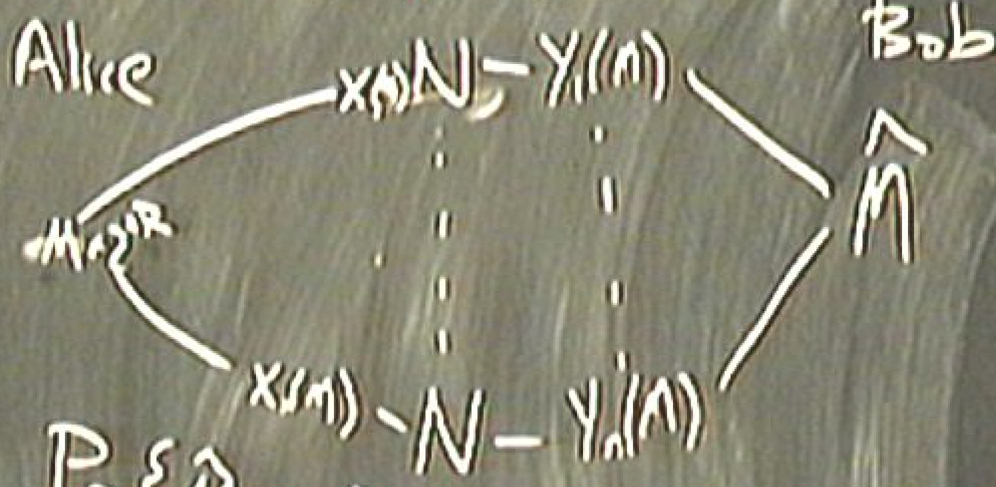
Jon Yard (LANL)
Quantum Communication with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)

Shannon '48

$N = p(Y|X)$

(R, n, ϵ)

R ach. if $\exists$ seq $\uparrow$ rate, $\epsilon \to 0$

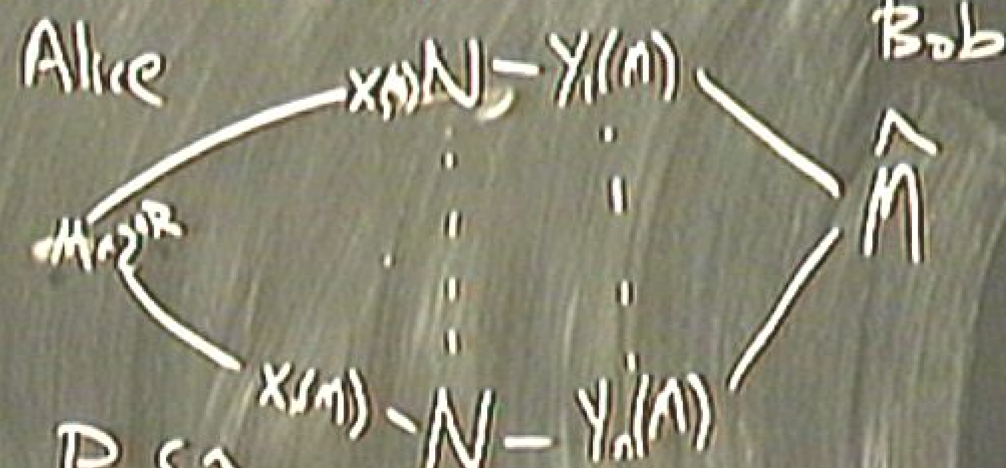


$\Pr\{\hat{M} \neq M\} \leq \epsilon$

Jon Yard (LANL)
Quantum Communication
with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)

Shannon '48

$N = p(Y|X)$



(R, n, ϵ)

R ach. if $\exists$ seq $\uparrow$ code $\epsilon \to 0$

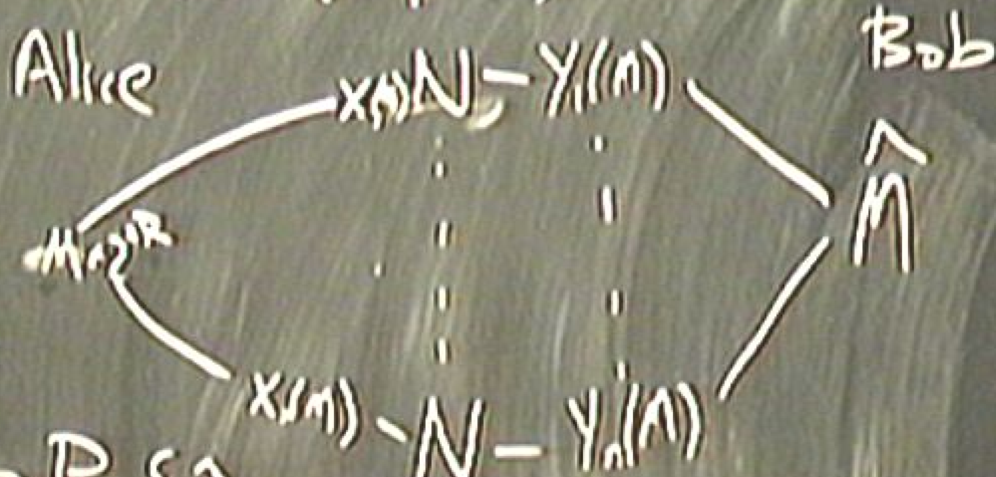
$C(N) =$ Sup. ach. rates R

$\Pr\{\hat{M} \neq M\} \leq \epsilon$

Jon Yard (LANL)
Quantum Communication with 0-capacity channels
w/ Graeme Smith (IBM)
Science Express (Aug '08)

Shannon '48

$N = p(Y|X)$

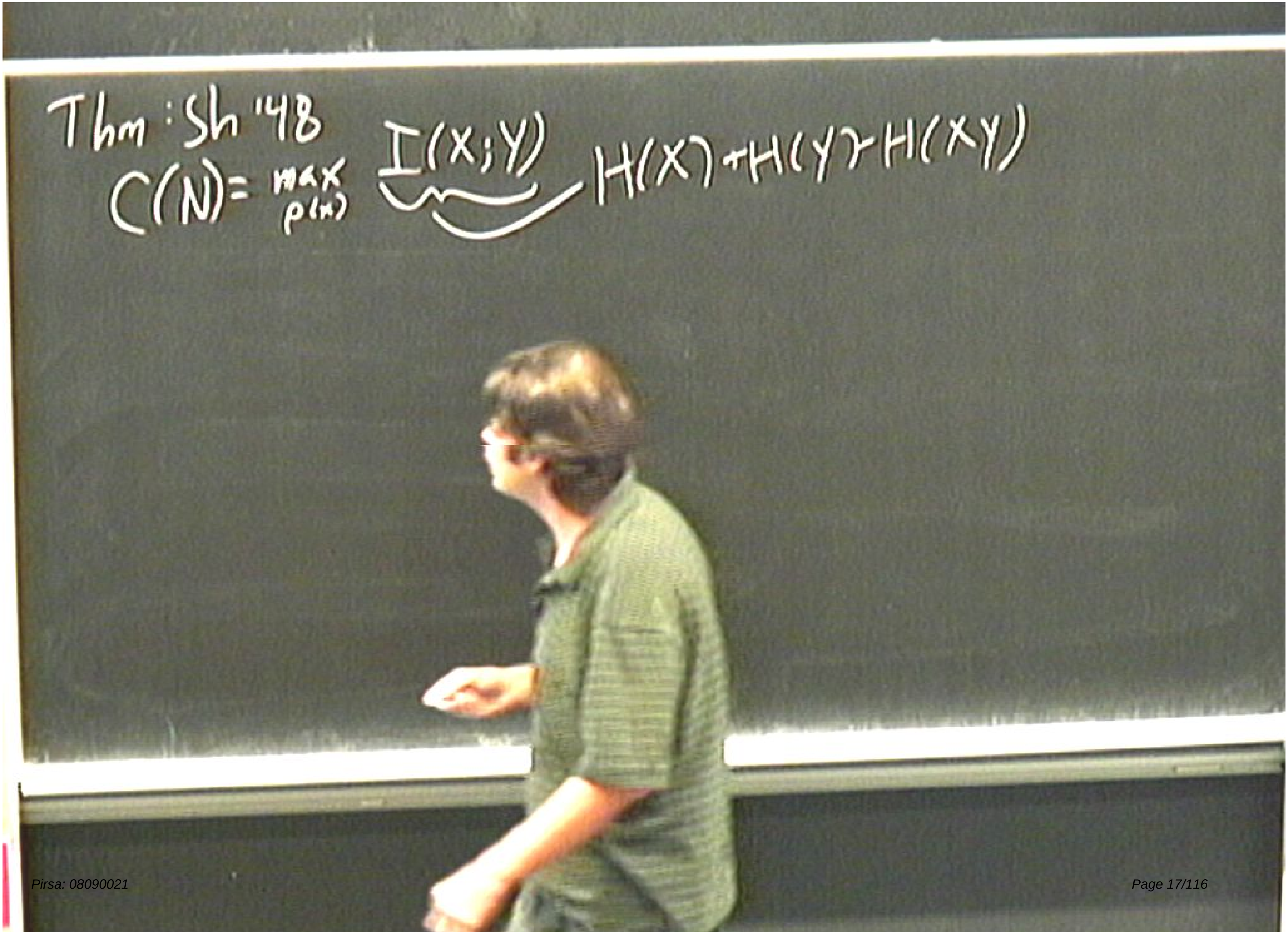


(R, n, ϵ)

R ach. if ∃ seq ↑ code, $\epsilon \to 0$

$$\boxed{C(N) = \text{Sup. ach. rates } R}$$

$$\Pr\{\hat{M} \neq M\} \le \epsilon$$


Thm: Sh '48
$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

$$C(N) = 0 \Leftrightarrow X \perp Y$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

$$C(N) = 0 \Leftrightarrow X \perp Y$$

$$C(N_1 \otimes N_2)$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

$$C(N) = 0 \iff X \perp Y$$

$$C(N_1 \otimes N_2) = C(N_1) + C(N_2)$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

$$C(N) = 0 \Leftrightarrow X \perp Y$$

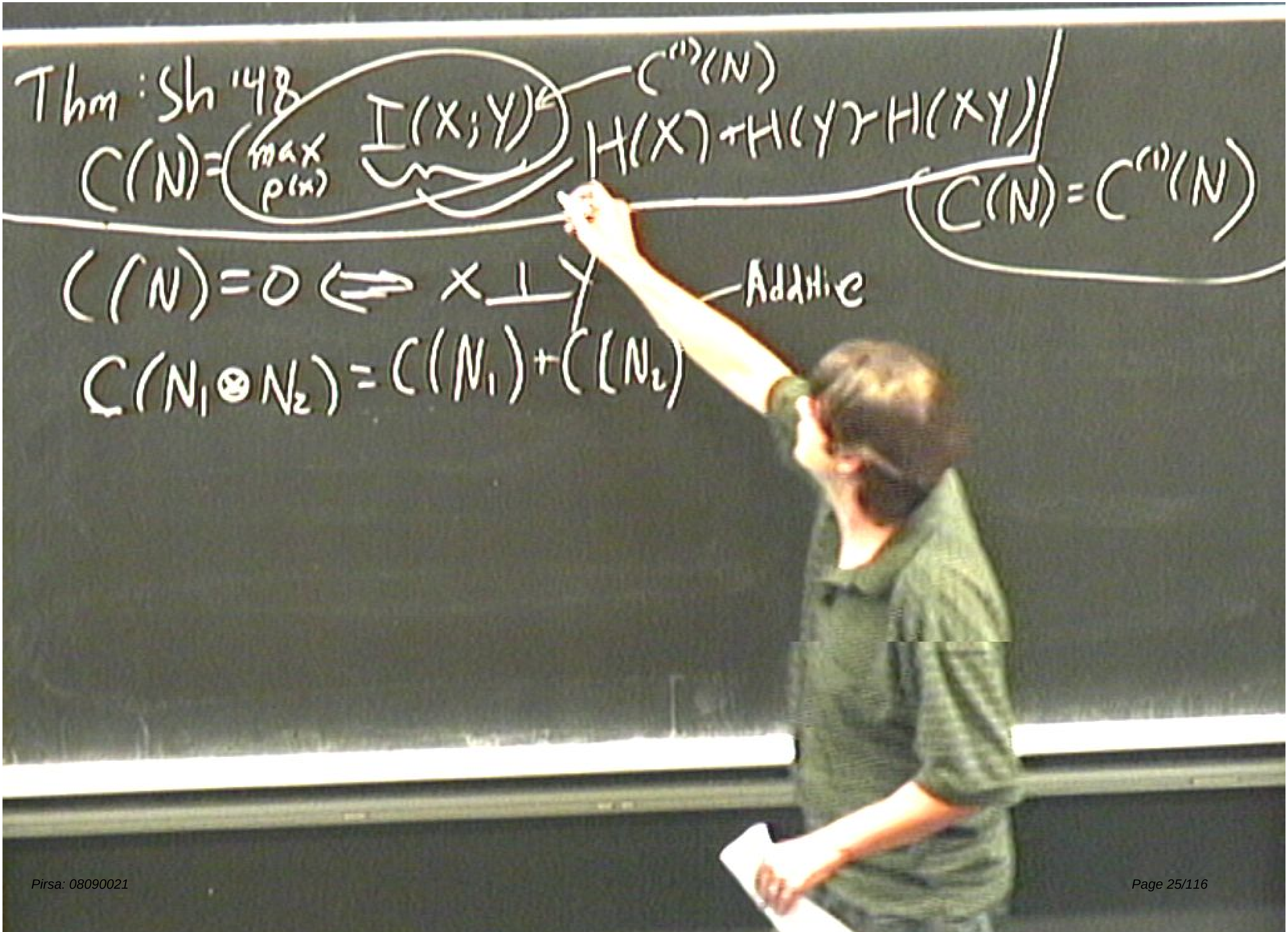
$$C(N_1 \otimes N_2) = C(N_1) + C(N_2)$$

Thm: Sh '48

$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)}$$

$$C(N) = 0 \iff X \perp Y$$

$$C(N_1 \otimes N_2) = C(N_1) + C(N_2)$$ Additive


Thm: Sh '48
$C(N) = \max_{p(x)} I(X;Y)$
$C^{(1)}(N)$
$H(X) + H(Y) - H(XY)$
$C(N) = C^{(1)}(N)$
$C(N) = 0 \iff X \perp Y$
Additive
$C(N_1 \otimes N_2) = C(N_1) + C(N_2)$

Thm: Sh '48

$$C(N) = \max_{p(x)} I(X;Y) \leftarrow C^{(1)}(N)$$

$$I(X;Y) = H(X) + H(Y) - H(XY)$$

$$C(N) = C^{(1)}(N)$$

$$C(N) = 0 \iff X \perp Y$$

$$C(N_1 \otimes N_2) = C(N_1) + C(N_2)$$

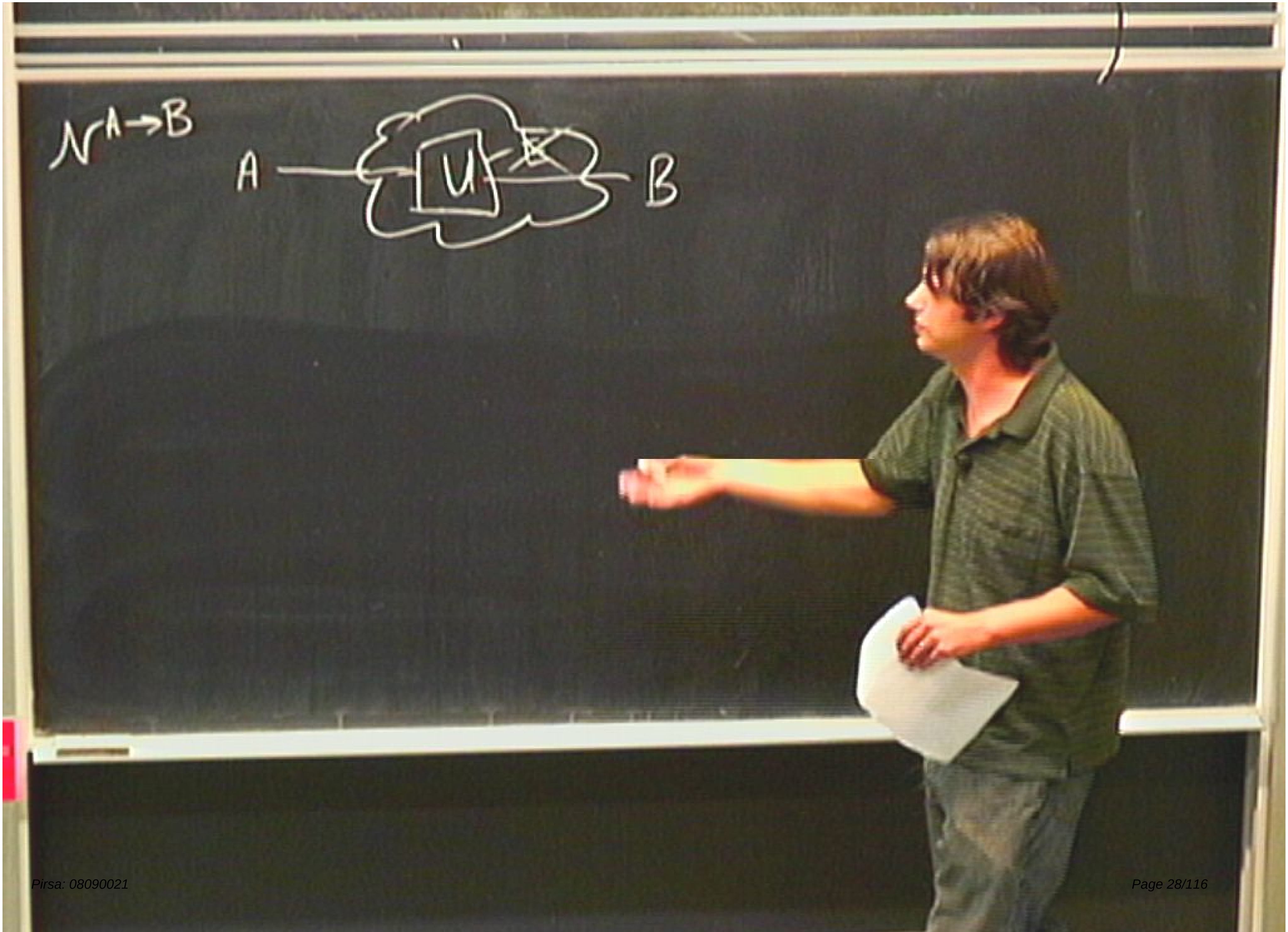
Thm: Sh '48

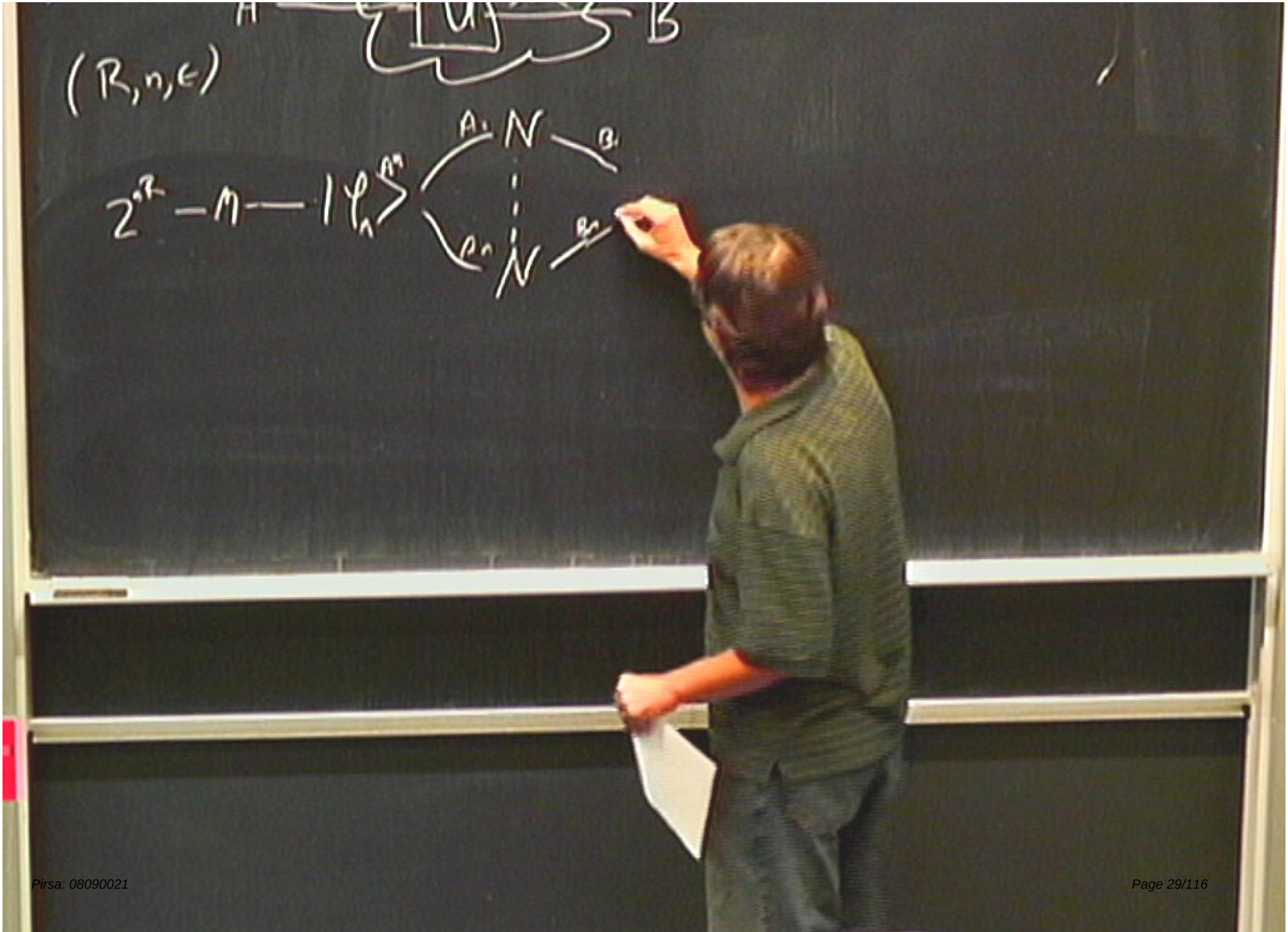
$$C(N) = \max_{p(x)} \underbrace{I(X;Y)}_{H(X)+H(Y)-H(XY)} \leftarrow C^{(1)}(N)$$

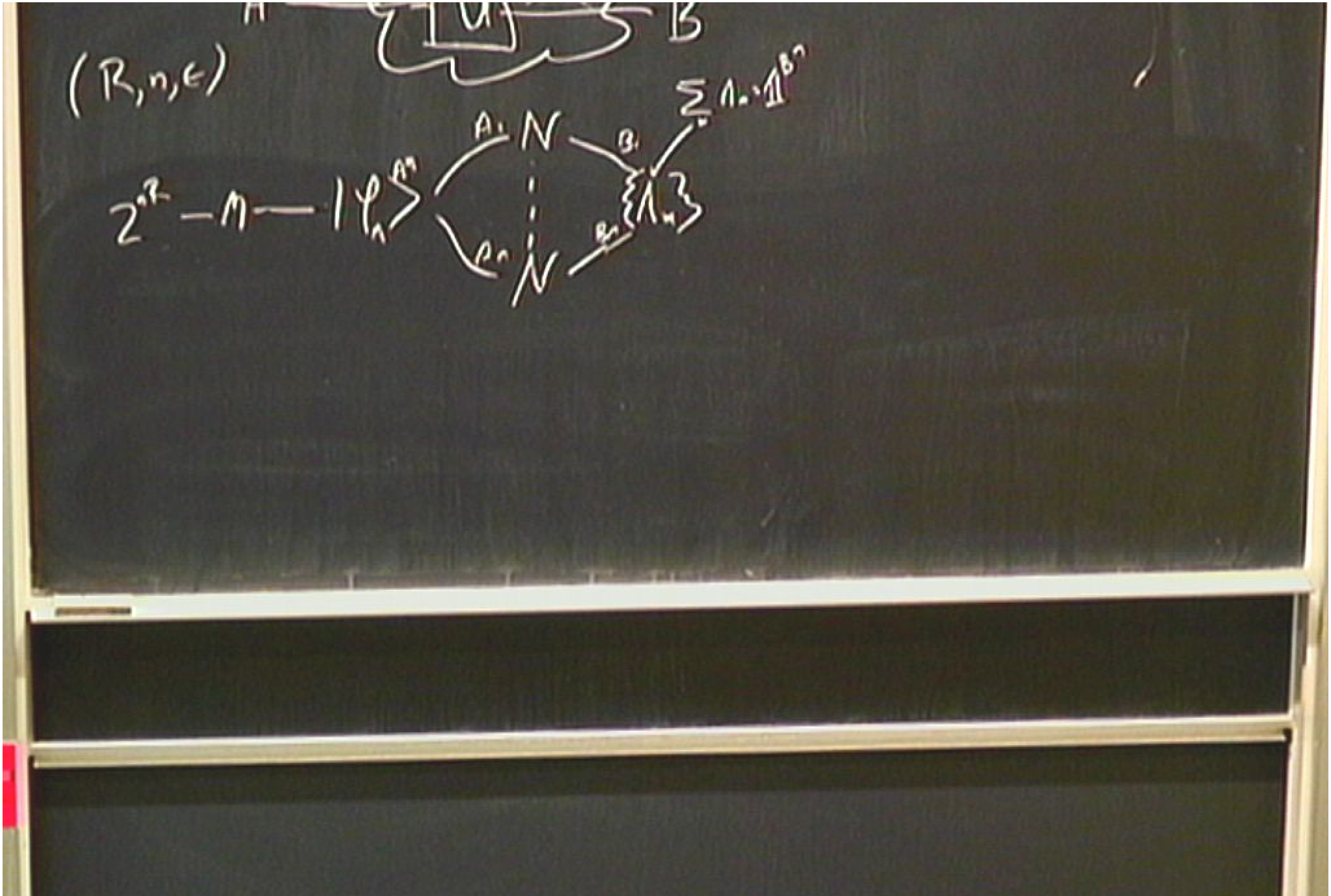
$$C(N) = C^{(1)}(N)$$

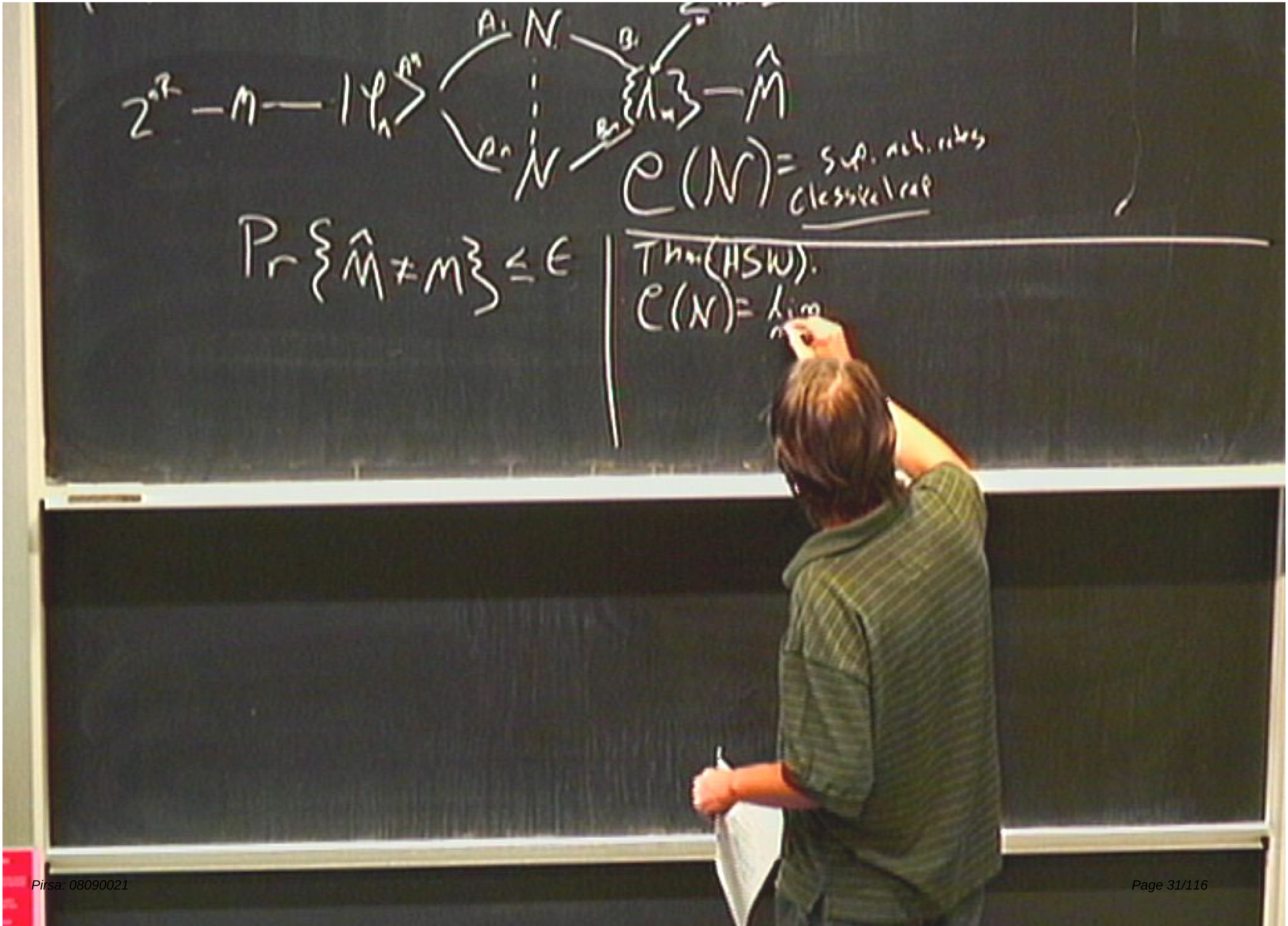
$$C(N) = 0 \iff X \perp Y$$

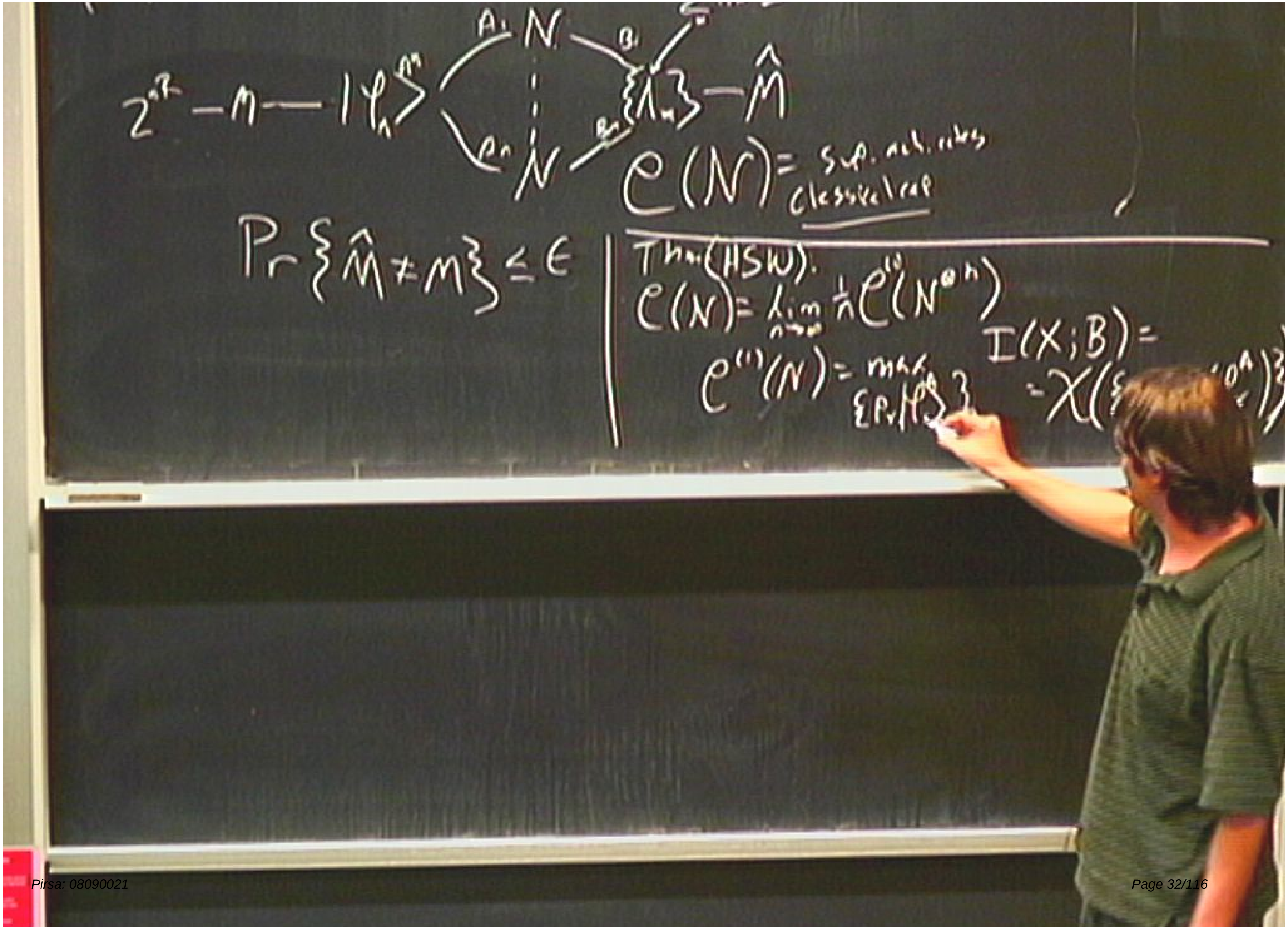
$$C(N_1 \otimes N_2) = C(N_1) + C(N_2) \leftarrow \text{Additive}$$

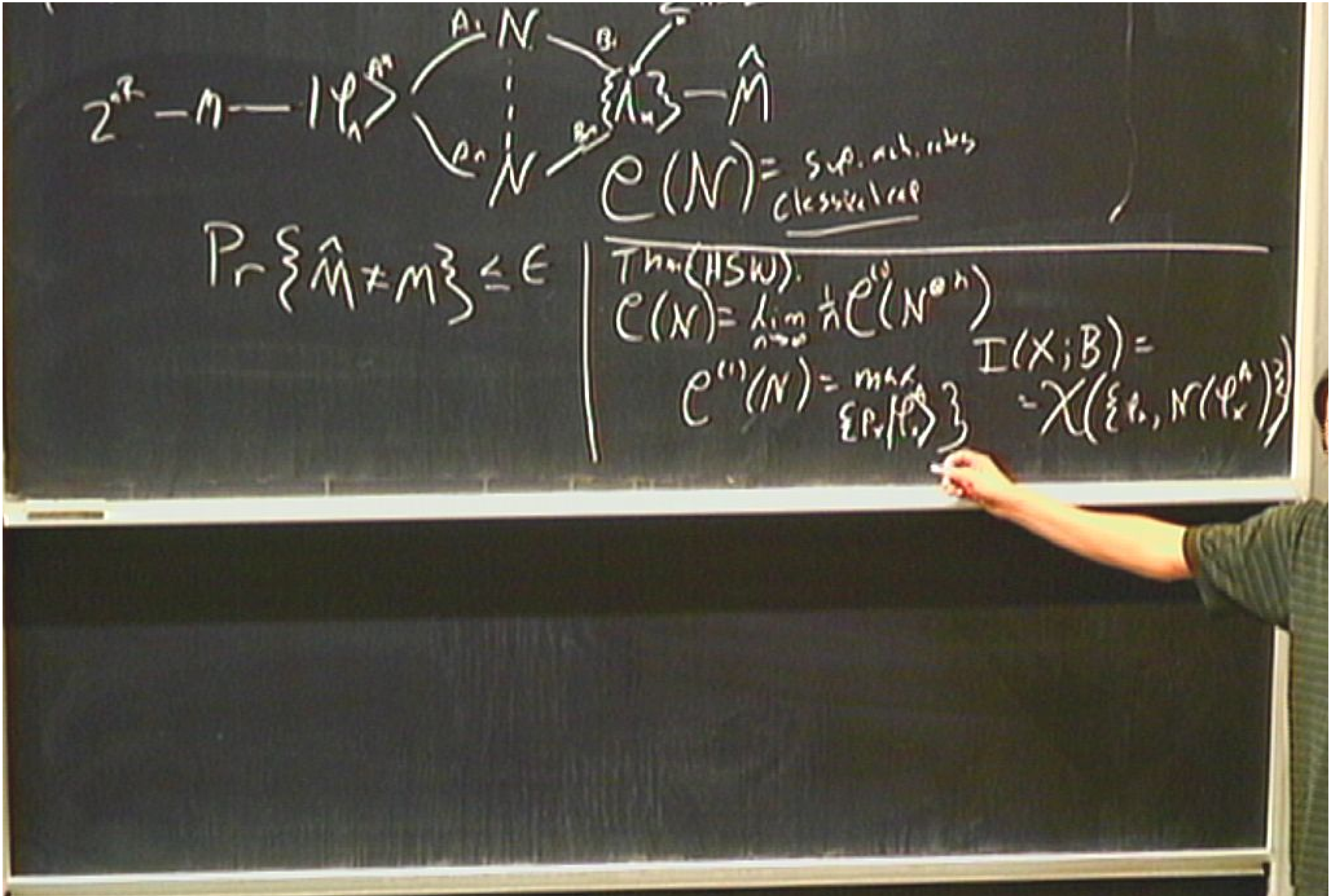

$\mathcal{N}^{A\to B}$
A
U
E
B


A
B
(R, n, ϵ)
A_1 N B_1
2^{nR} — M — $|\varphi_n\rangle$
A_n N B_n


(R, n, ε)
B
N
N


Pr{m̂ ≠ m} ≤ ε
C(N) = sup. achiev. rates
classical rate
Thm (HSW):
C(N) = lim


2^{nR} — m — $|\varphi_m\rangle$ — N — $\{\Lambda_m\}$ — $\hat{m}$
$\Pr\{\hat{m} \neq m\} \leq \epsilon$
$C(N) =$ Sup. ach. rates
Classical cap
Thm (HSW).
$C(N) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(N^{\otimes n})$
$C^{(1)}(N) = \max_{\{p_x, |\varphi_x\rangle\}}$
$I(X;B) =$

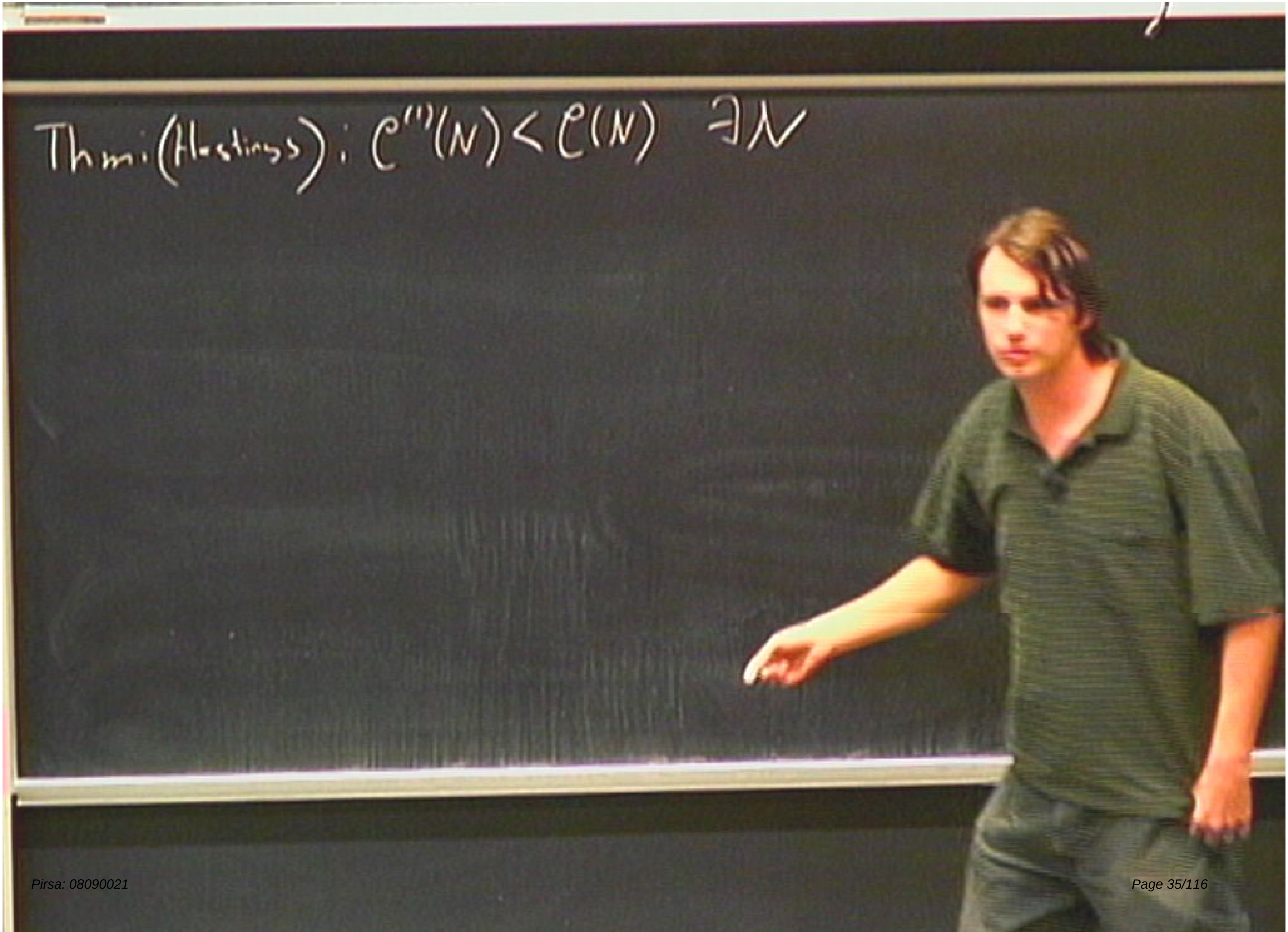

2^{nR} — m — $|\varphi_n\rangle^{A^n}$
A_1 N B_1
A_n N B_n
$\{\Lambda_m\}$ — $\hat{m}$
$C(N)$ = sup. ach. rates
classical cap
$\Pr\{\hat{m}\neq m\}\le\epsilon$
Thm (HSW):
$C(N)=\lim_{n\to\infty}\frac{1}{n}C^{(1)}(N^{\otimes n})$
$C^{(1)}(N)=\max_{\{p_x,|\varphi_x\rangle\}}$
$I(X;B)=$
$=\chi(\{p_x, N(\varphi_x^A)\})$

$$\Pr\{\hat{m} \neq m\} \leq \epsilon$$

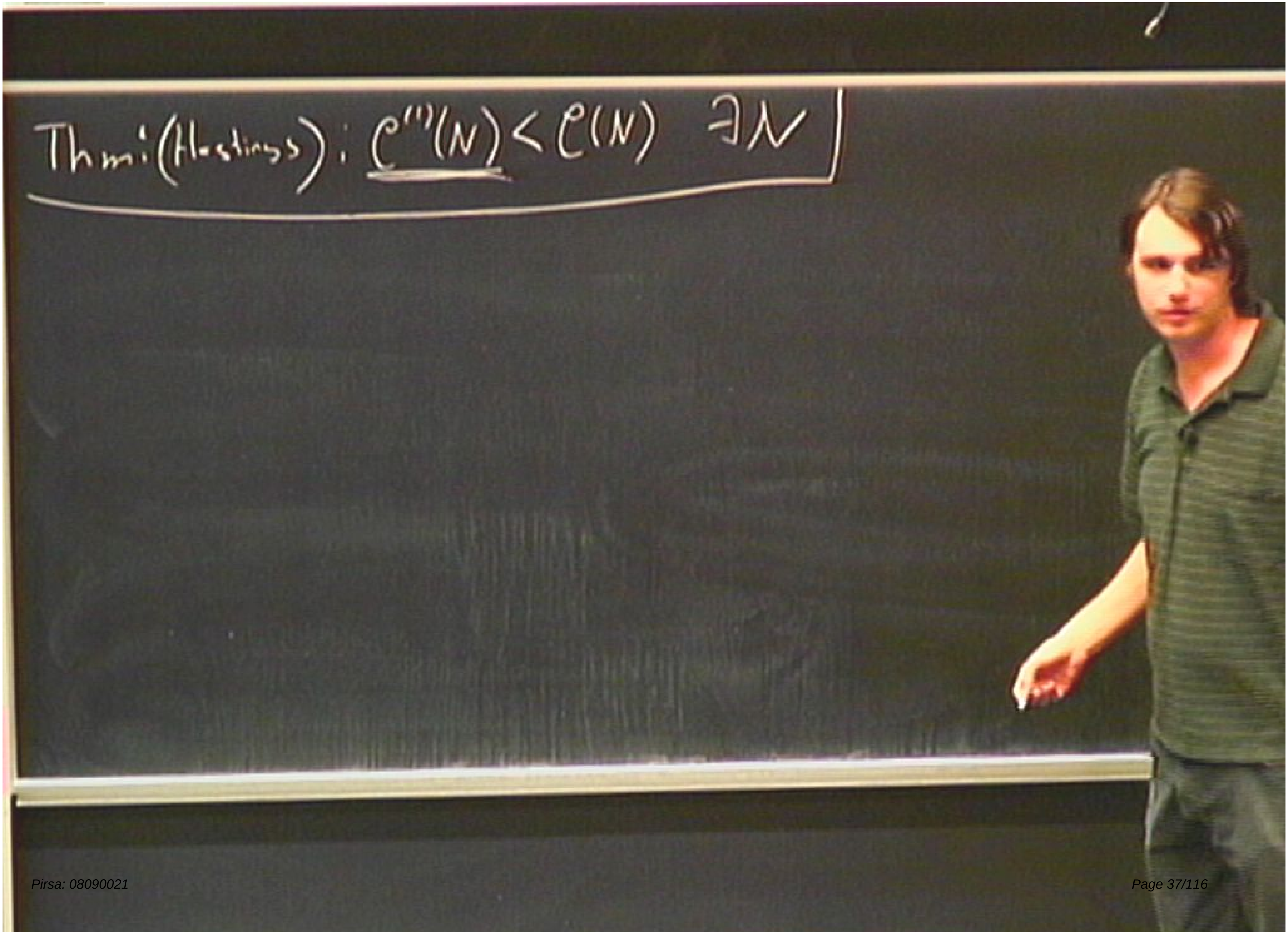
Thm (HSW):

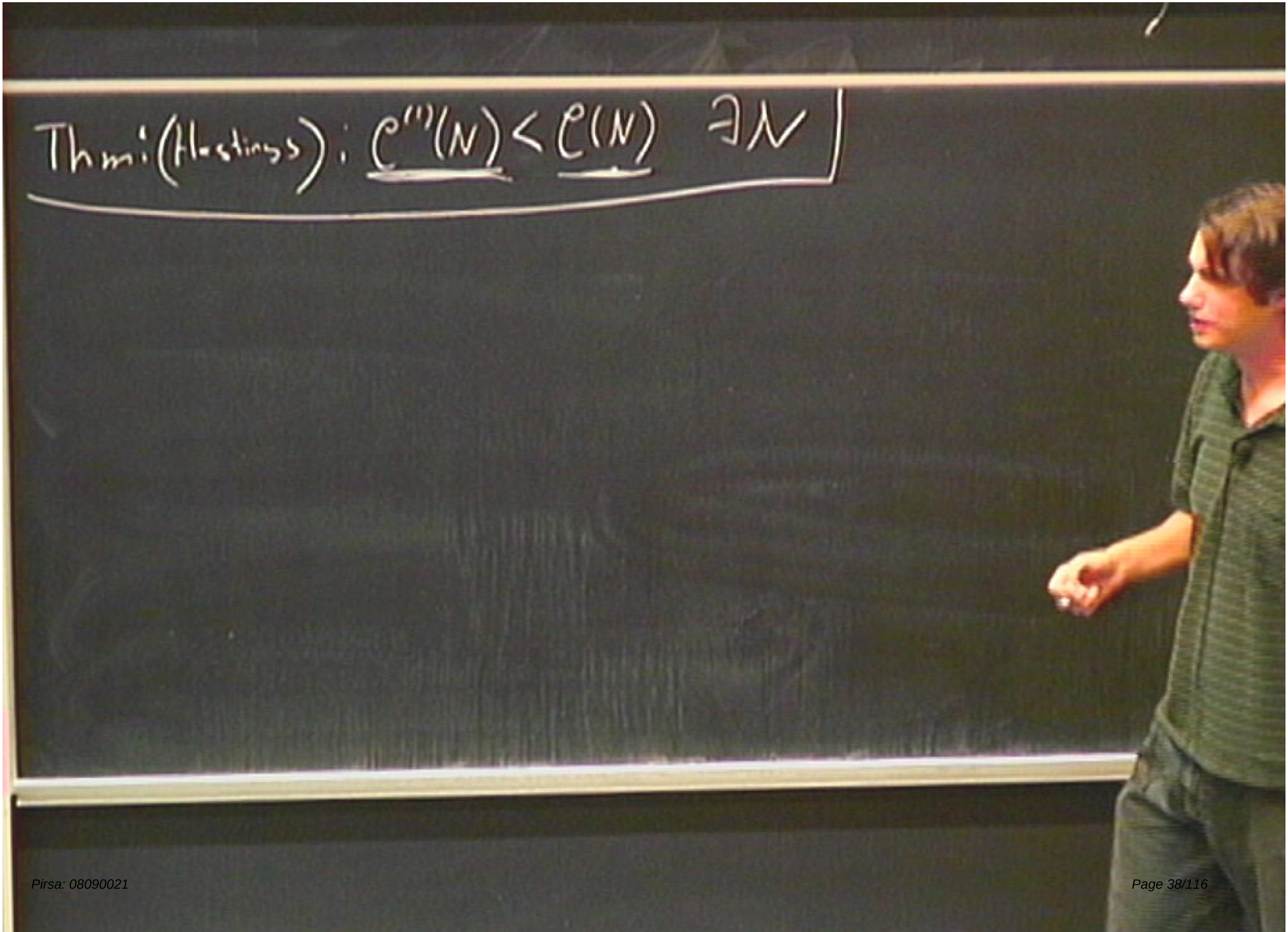
$$C(N) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(N^{\otimes n})$$

$$C^{(1)}(N) = \max_{\{p_x, |\varphi_x\rangle\}} I(X;B) = \chi(\{p_x, N(\varphi_x^A)\})$$

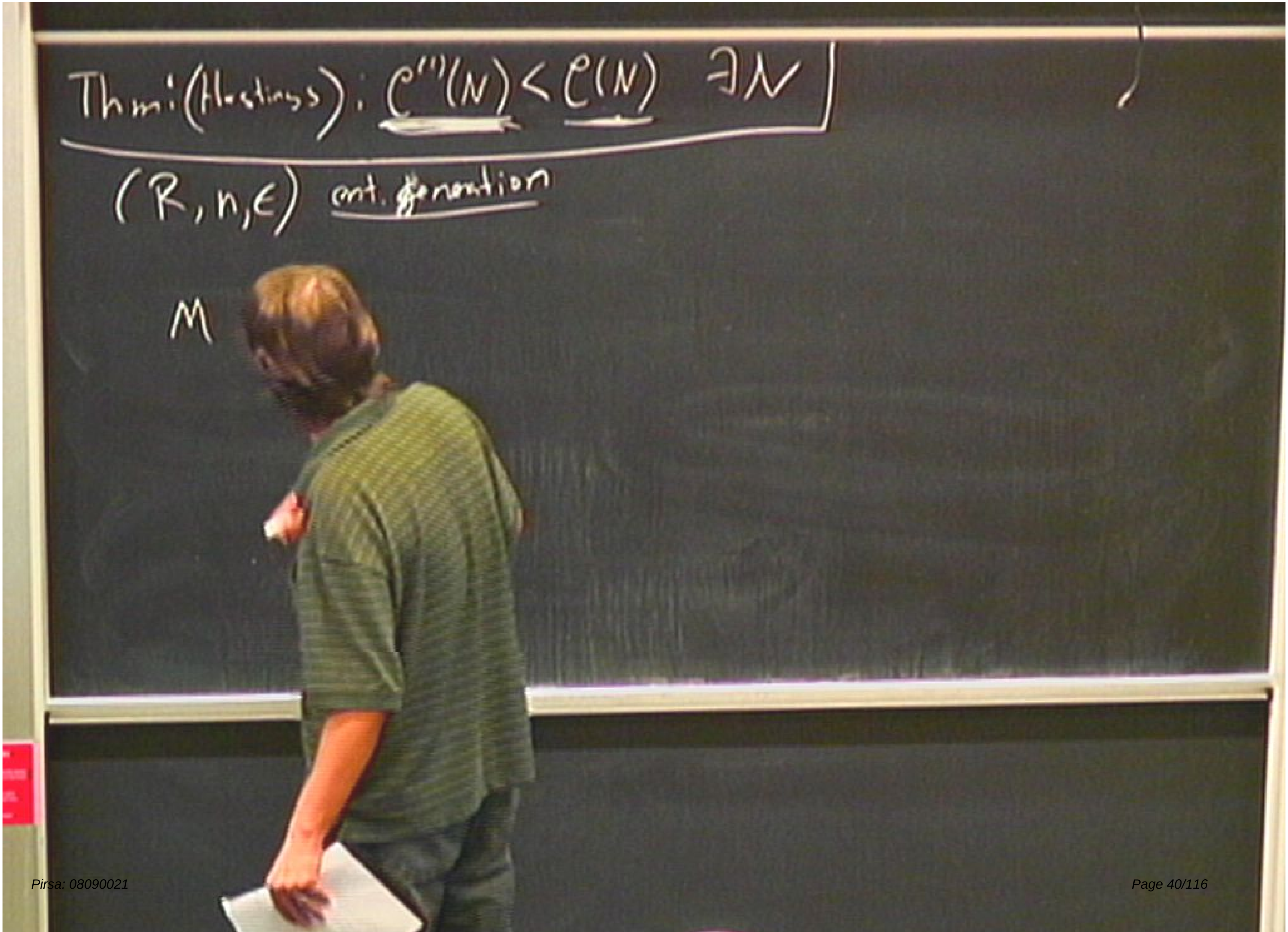

Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$

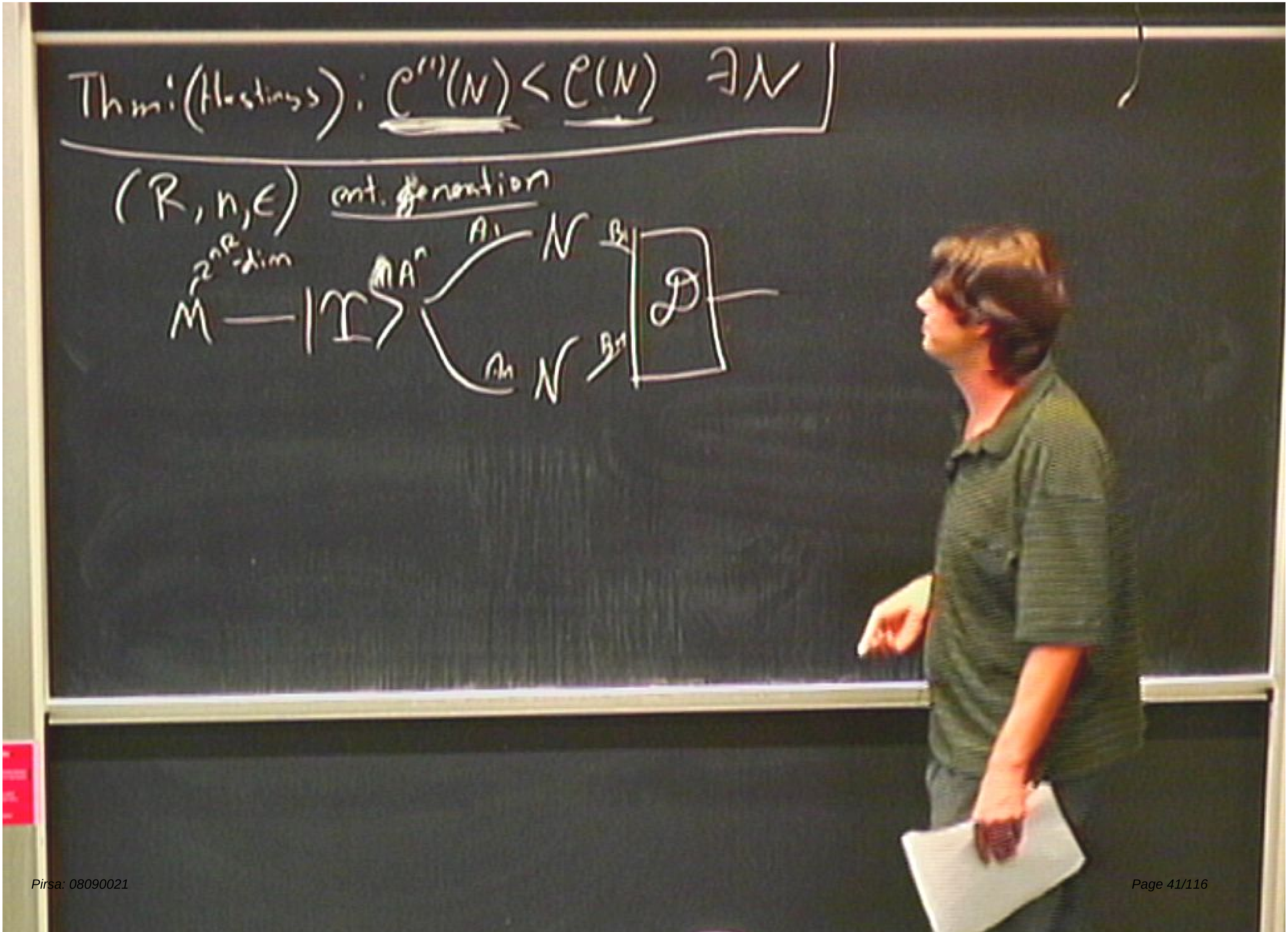
Thm: (Hastings): $\rho^{(1)}(N) < \rho(N)$ $\exists N$

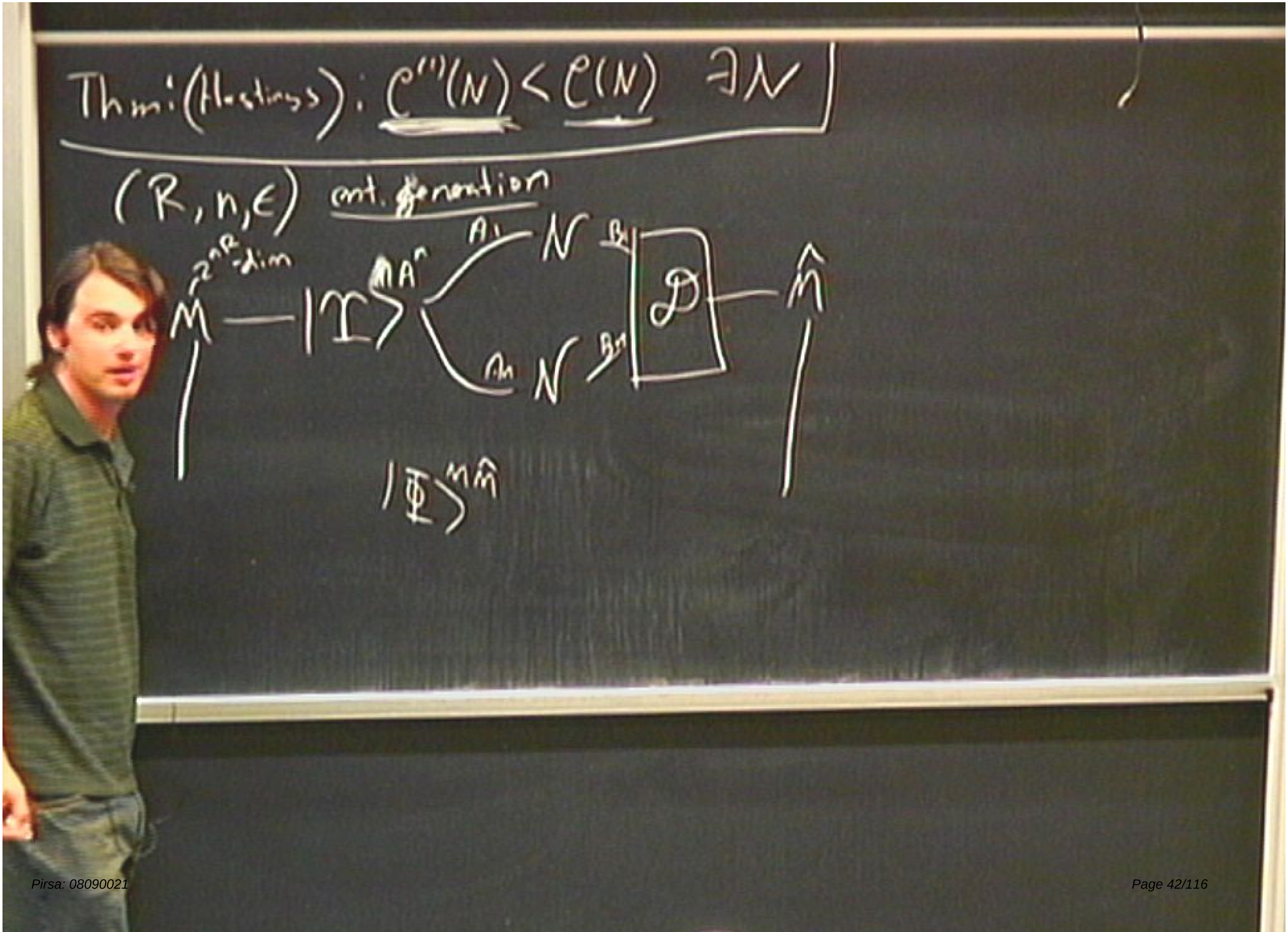

Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$

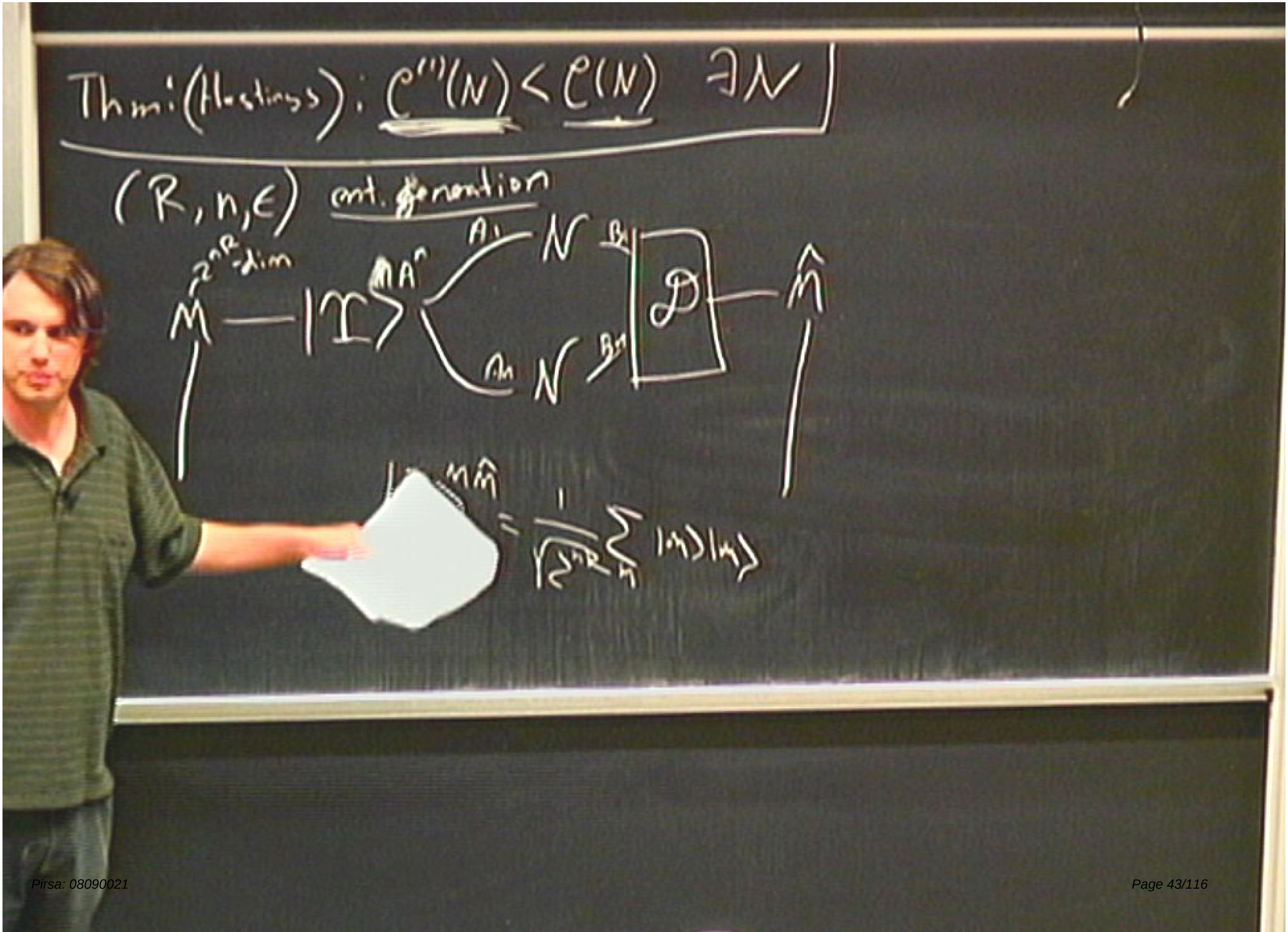

Thm: (Hastings): $\rho^{(n)}(N) < \rho(N) \quad \exists N$

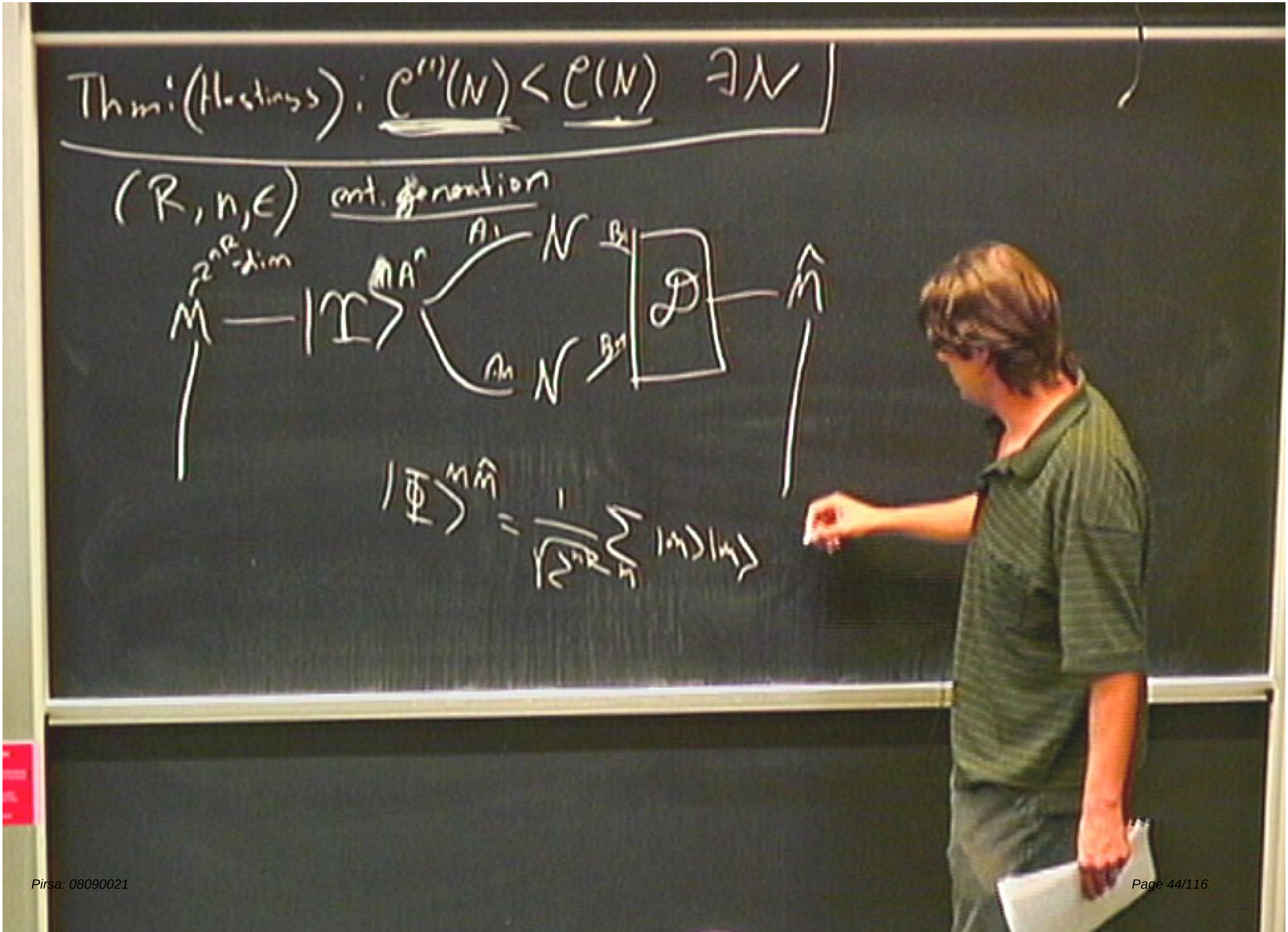
$\boxed{\text{Thm: (Hastings): } \underline{C^{(1)}(N)} < \underline{C(N)} \quad \exists N}$

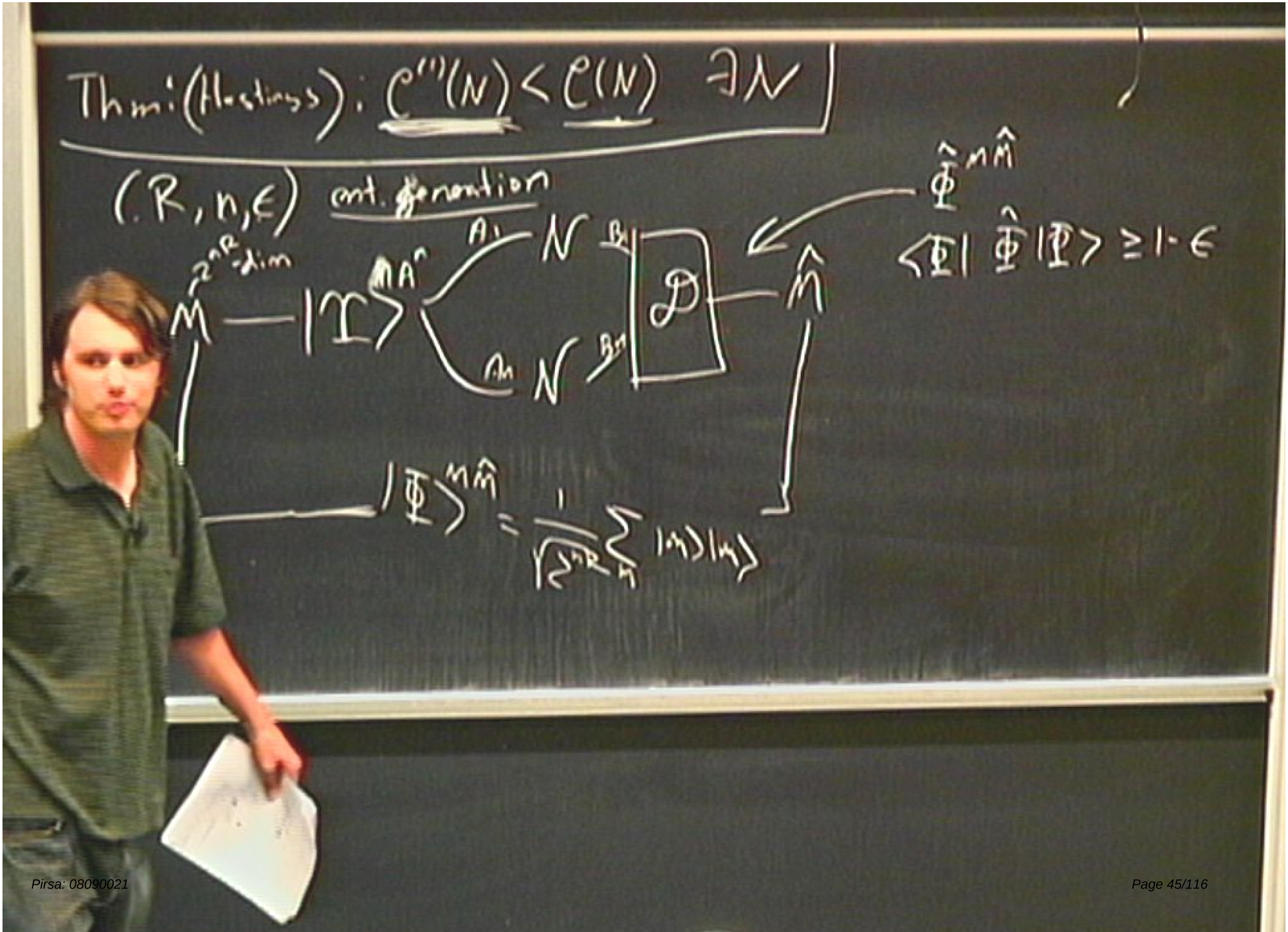

Thm: (Hastings): $C^{(m)}(N) < C(N)$ $\exists N$
(R, n, ϵ) ent. generation
M

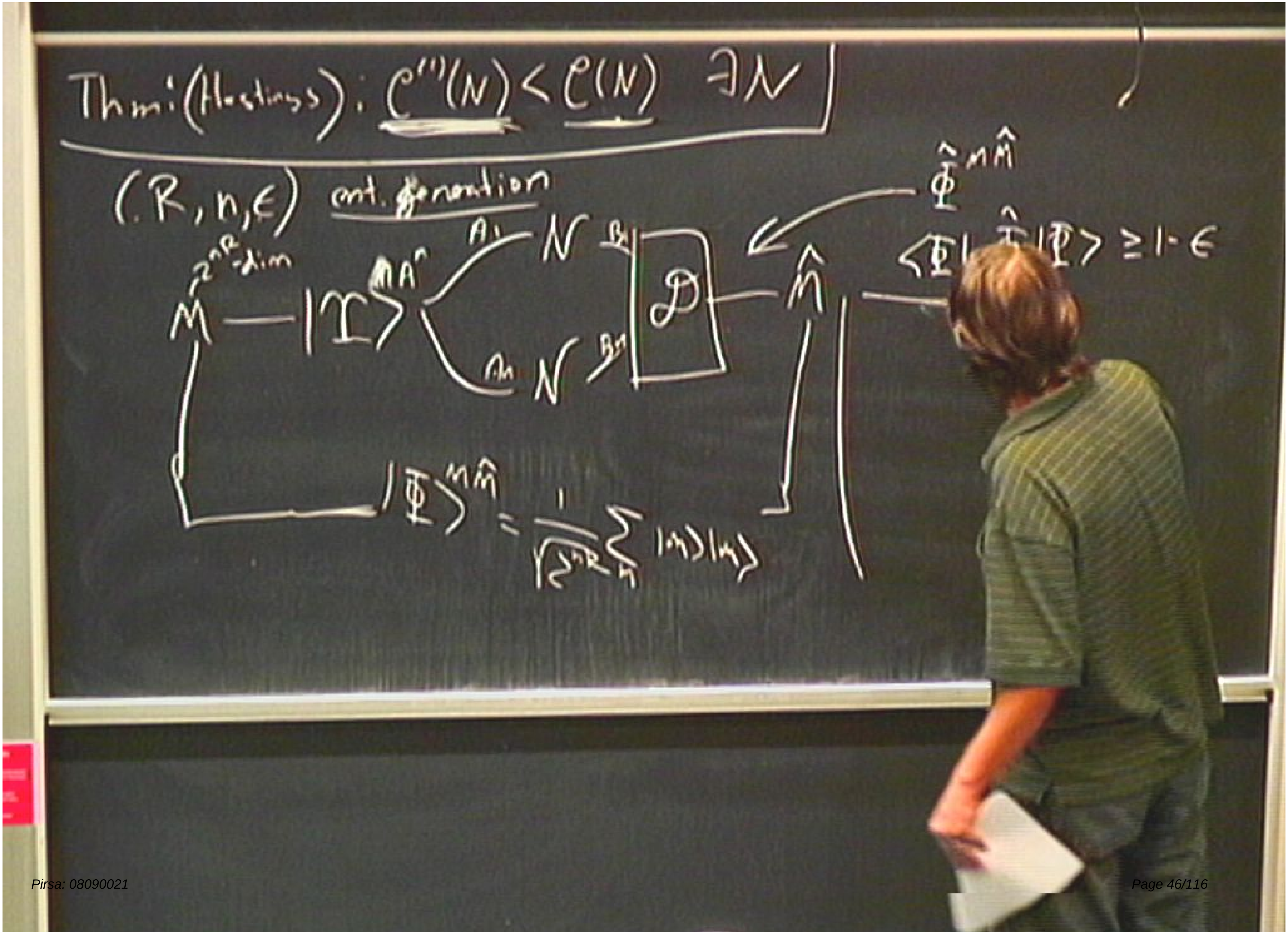

Thm: (Hastings): C^(1)(N) < C(N) ∃N
(R, n, ε) ent. generation
2^nR-dim
M
A^n
A1
N
B1
An
N
Bn
D

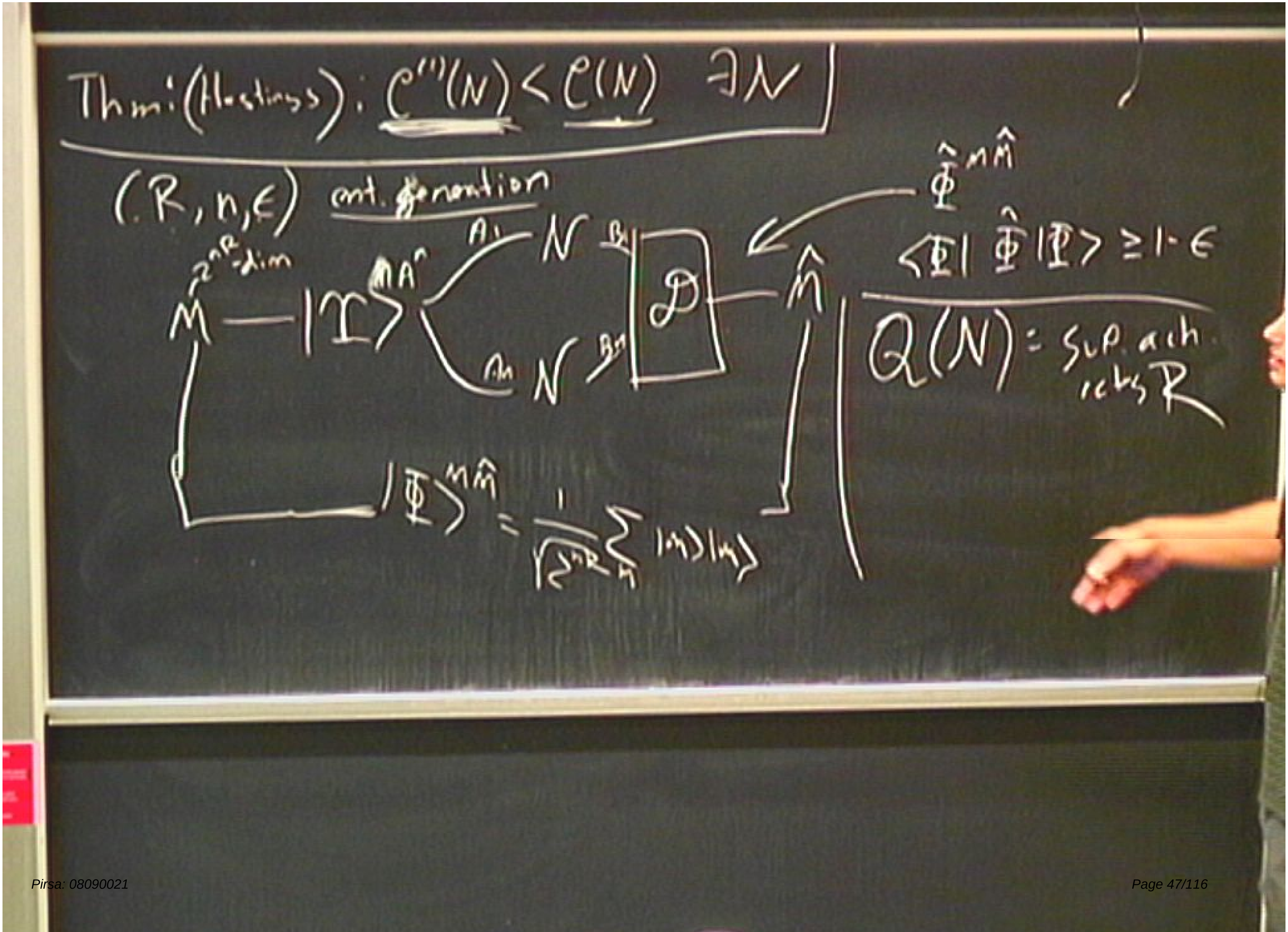

Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$
(R, n, ϵ) ent. generation
2^{nR}-dim
M
$|\Upsilon\rangle^{MA^n}$
A_1
N
B_1
A_n
N
B_n
$\mathcal{D}$
$\hat{M}$
$|\Phi\rangle^{M\hat{M}}$


Thm: (Hastings): C^(1)(N) < C(N) ∃N
(R, n, ε) ent. generation
2^nR-dim
N
N
D


Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$
(R, n, ϵ) ent. generation
2^{nR}-dim
$|\Phi\rangle^{m\hat{m}} = \frac{1}{\sqrt{2^{nR}}} \sum_m |m\rangle |m\rangle$

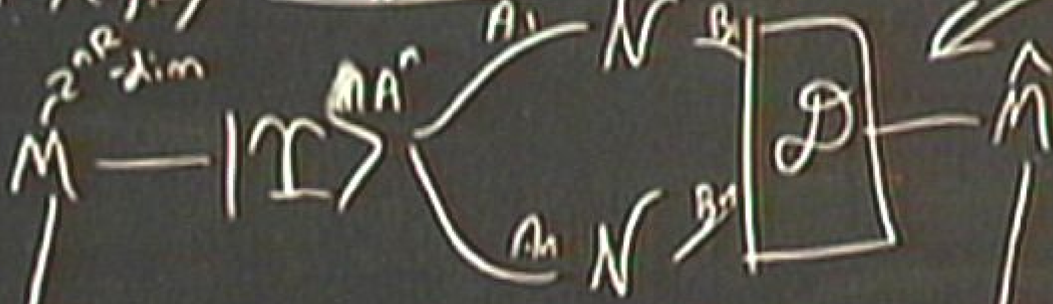

Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$
(R, n, ϵ) ent. generation
2^{nR}-dim
$\langle\Phi|\hat{\Phi}|\Phi\rangle \geq 1-\epsilon$
$|\Phi\rangle^{M\hat{M}} = \frac{1}{\sqrt{2^{nR}}}\sum_m |m\rangle|m\rangle$


Thm: (Hastings): $C^{(1)}(N) < C(N)$ $\exists N$
(R, n, ϵ) ent. generation
2^{nR}-dim
$\langle \Phi | \hat{\Phi} | \Phi \rangle \geq 1 - \epsilon$
$|\Phi\rangle^{m\hat{m}} = \frac{1}{\sqrt{2^{nR}}} \sum_m |m\rangle |m\rangle$


Thm: (Hastings): C^(1)(N) < C(N) ∃N
(R, n, ε) ent. generation
2^nR-dim
M — |Υ>^MA^n
A1 N B1
An N Bn
D
M̂
Φ̂^MM̂
⟨Φ| Φ̂ |Φ⟩ ≥ 1 - ε
Q(N) = sup. ach. rates R
|Φ⟩^MM̂ = 1/√(2^nR) Σ_m |m⟩|m⟩

Thm: (Hastings): $\underline{C^{(1)}(N)} < \underline{C(N)}$ $\exists N$

(R, n, ϵ) ent. generation

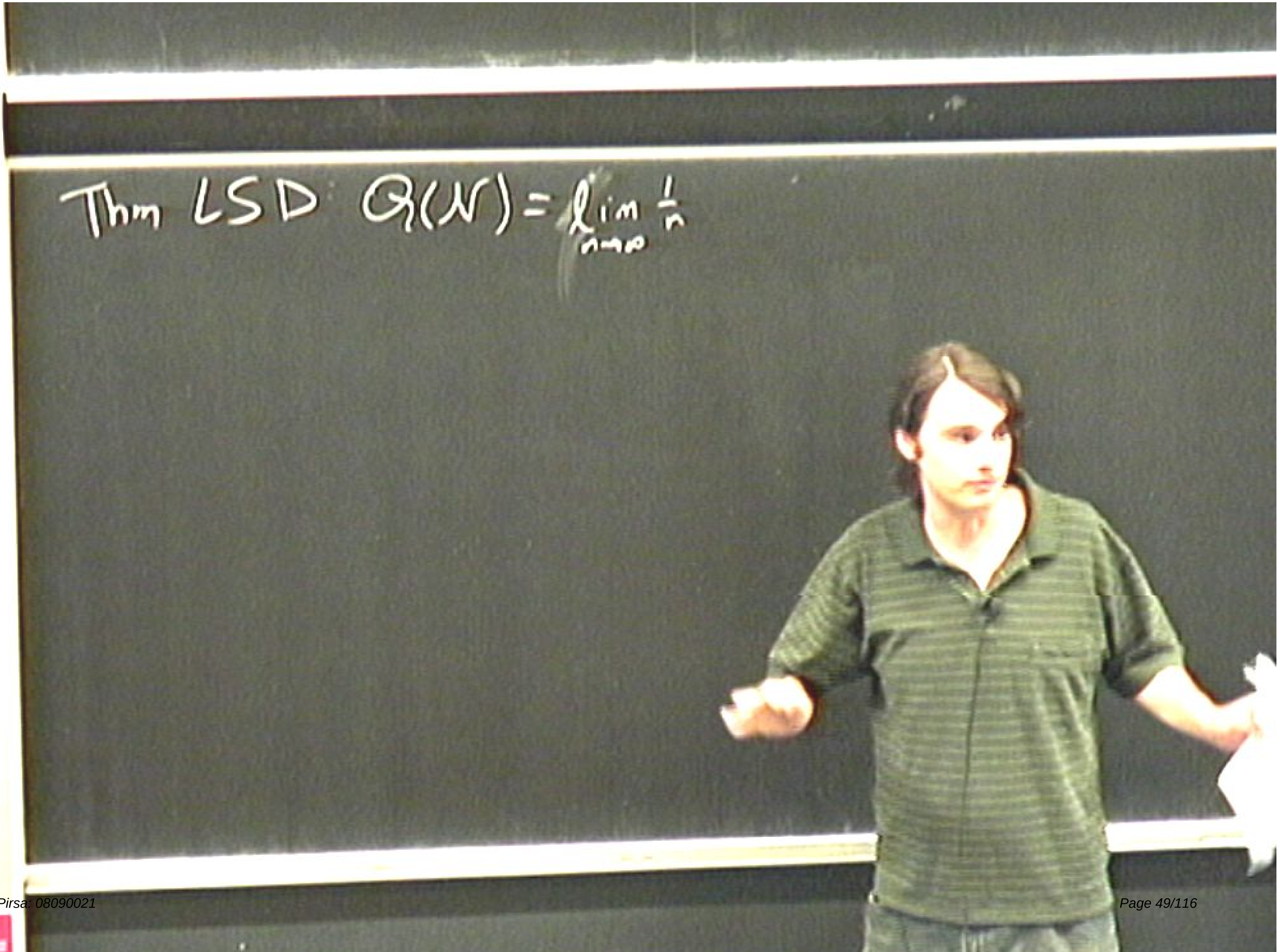


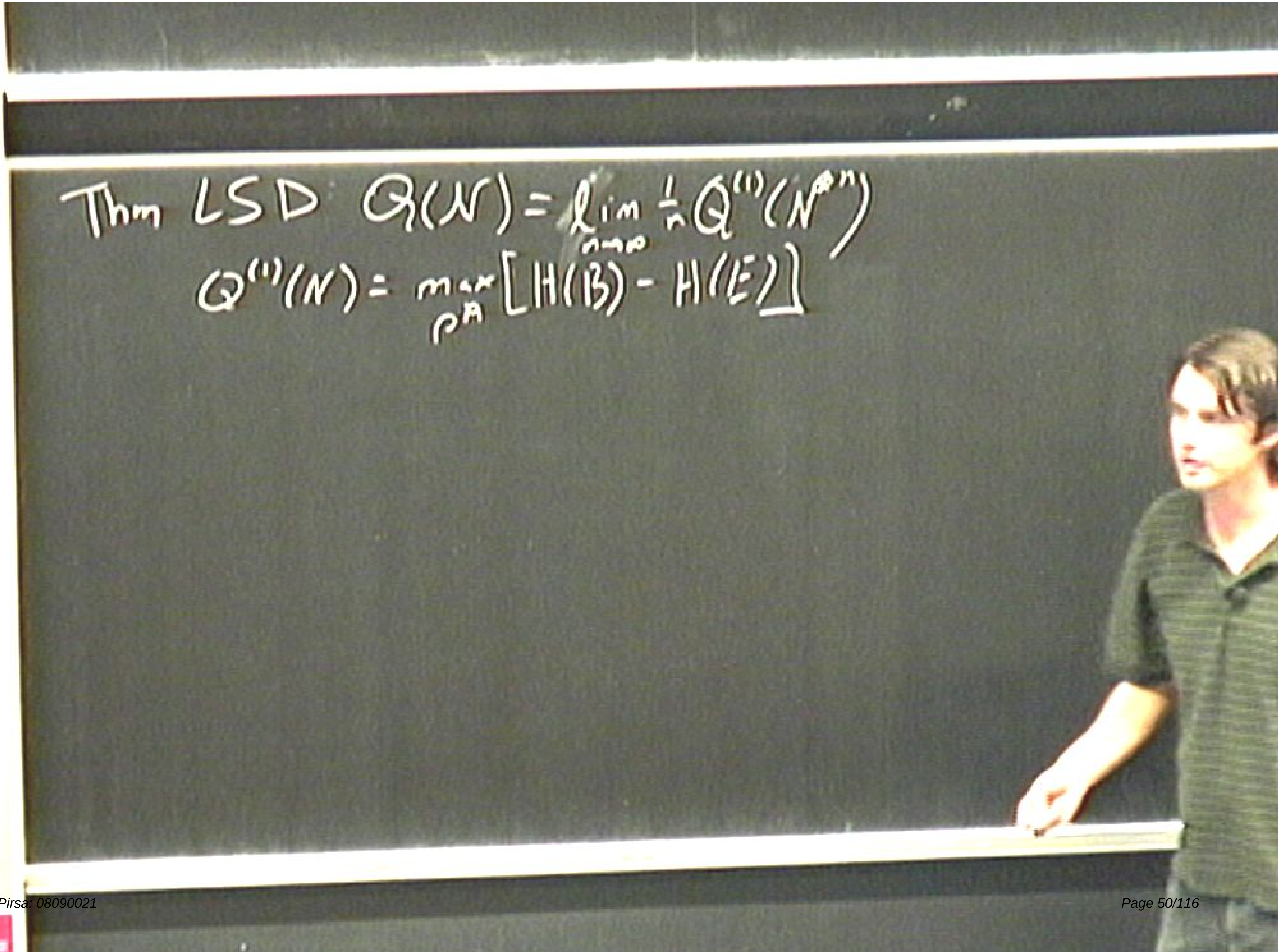
$|\Phi\rangle^{M\hat{M}} = \frac{1}{\sqrt{2^{nR}}} \sum_m |m\rangle|m\rangle$

$\hat{\Phi}^{M\hat{M}}$

$\langle\Phi| \hat{\Phi} |\Phi\rangle \geq 1-\epsilon$

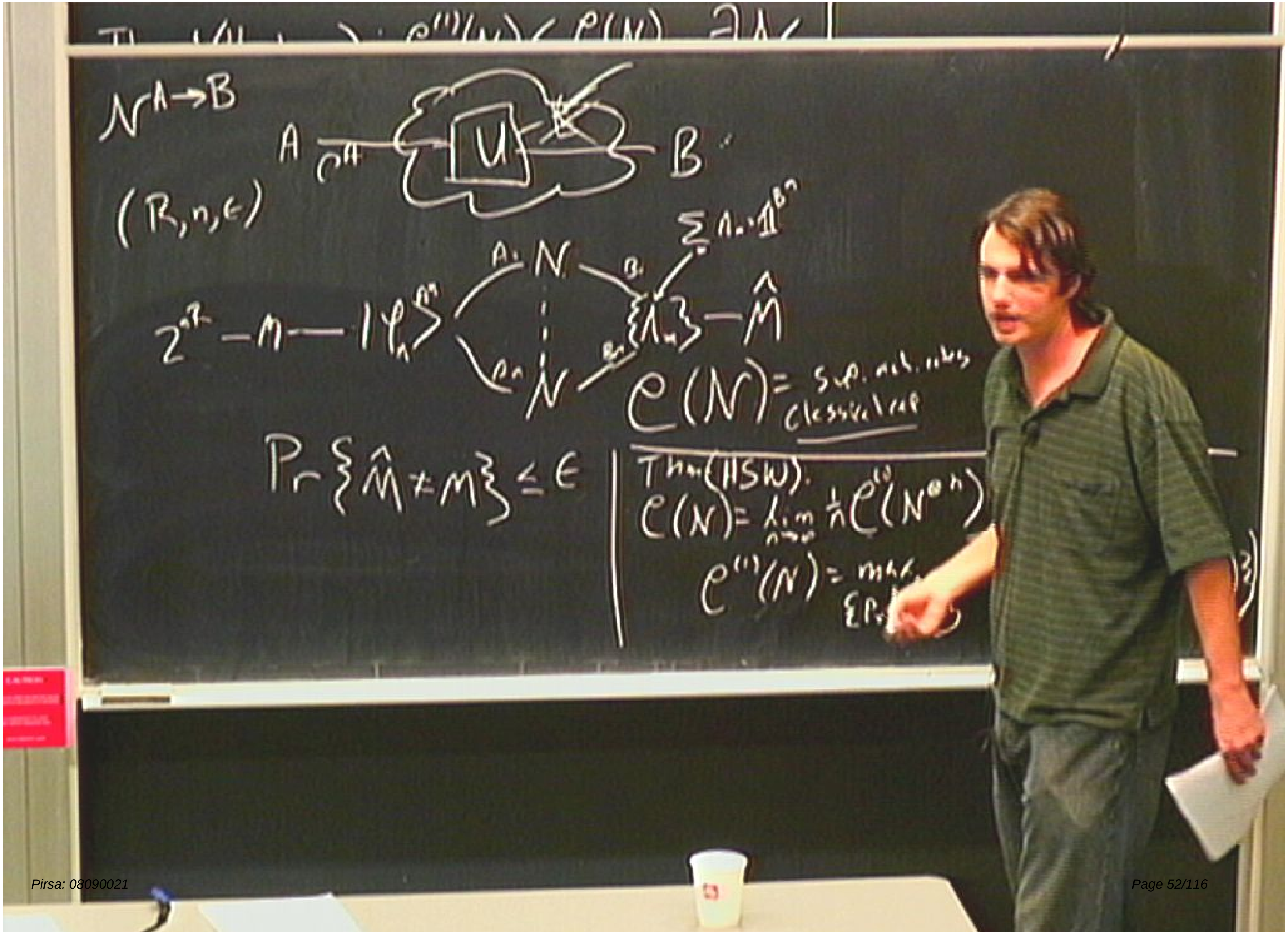
$Q(N)$ = sup. ach. rates R


Thm LSD $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}$


Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$
$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$

Thm LSD $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n})$

$$Q^{(1)}(\mathcal{N}) = \max_{\rho^A} [H(B) - H(E)]$$



N^{A→B}
(R, n, ε)
A
U
B
N
M̂
Pr{M̂ ≠ m} ≤ ε
Thm (HSW):

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$$

Thm SS '06 $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$ coherent info.

Thm SS '96 $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$ ← coherent info.

Thm SS '06 $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$$ coherent info.

Thm SS '06 $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$ ← coherent info.

Thm SS '96 $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$ coherent info.

Thm: SS '96 $Q(N) > Q^{(1)}(N) = 0$

$2^{nR} - m - |\varphi_m\rangle^{A^n}$ — N — $\{\Lambda_m\}$ — $\hat{m}$

$C(N) = $ sup. achievable classical rate

$\Pr\{\hat{m} \neq m\} \leq \epsilon$

Thm (HSW):

$C(N) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(N^{\otimes n})$

$C^{(1)}(N) = \max_{\{p_x, |\varphi_x\rangle\}} I(X;B) = \chi(\{p_x, N(\varphi_x)\})$

Thm (Hastings): ...

(R, n, ϵ) ent. generation

$\hat{\Phi}^{M\hat{M}}$

$\langle\Phi|\hat{\Phi}|\Phi\rangle \geq 1-\epsilon$

M (2^{nR}-dim) — $|\Upsilon\rangle^{MA^n}$ — N — $\mathcal{D}$ — $\hat{M}$

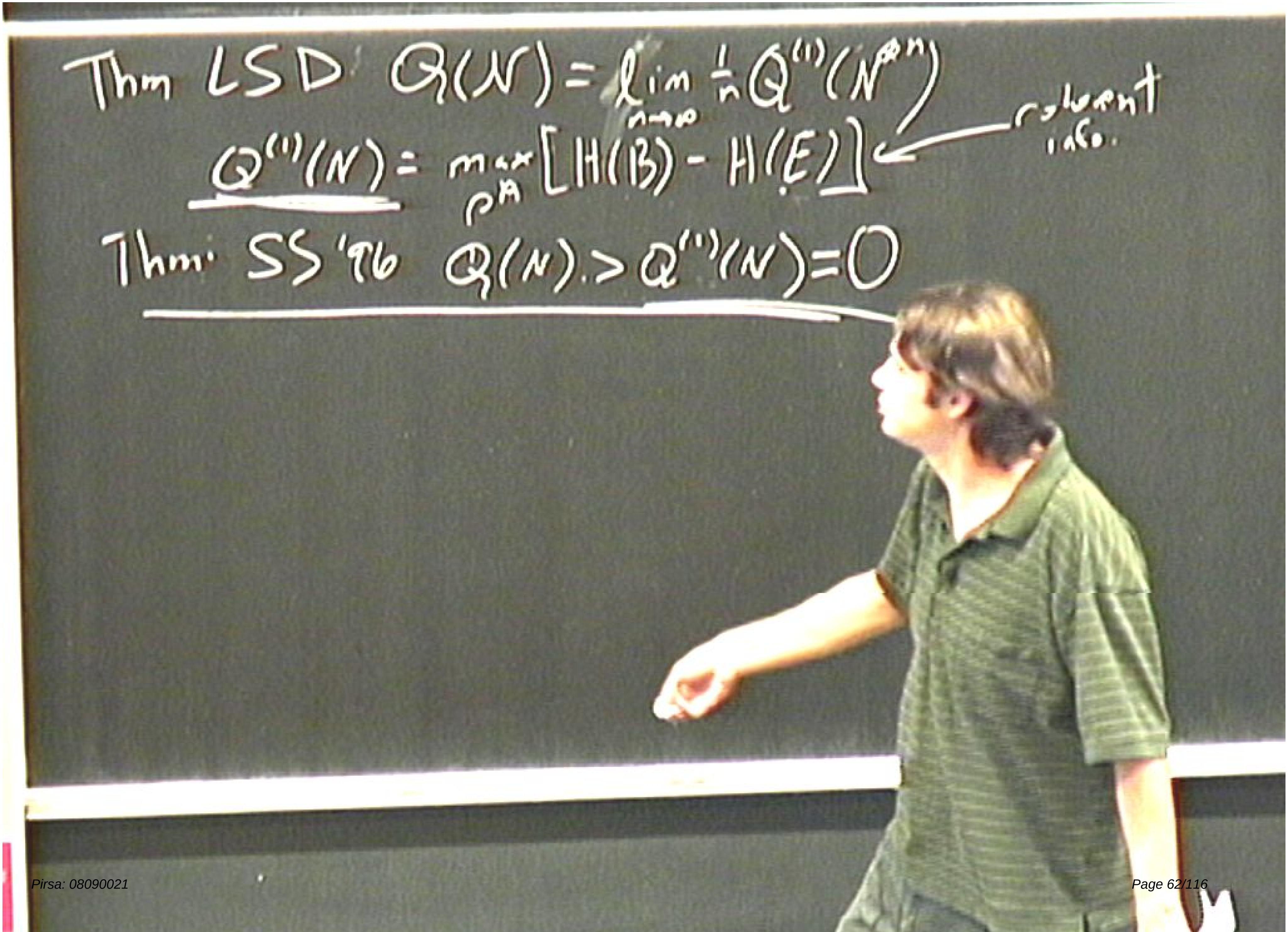
$Q(N) = $ sup. ach. rates R

$|\Phi\rangle^{M\hat{M}} = \frac{1}{\sqrt{|M|}} \sum |m\rangle|m\rangle$

Thm LSD $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n})$

$$Q^{(1)}(\mathcal{N}) = \max_{\rho^A} [H(B) - H(E)]$$ ← coherent info.

Thm SS '96 $Q(\mathcal{N}) > Q^{(1)}(\mathcal{N}) = 0$

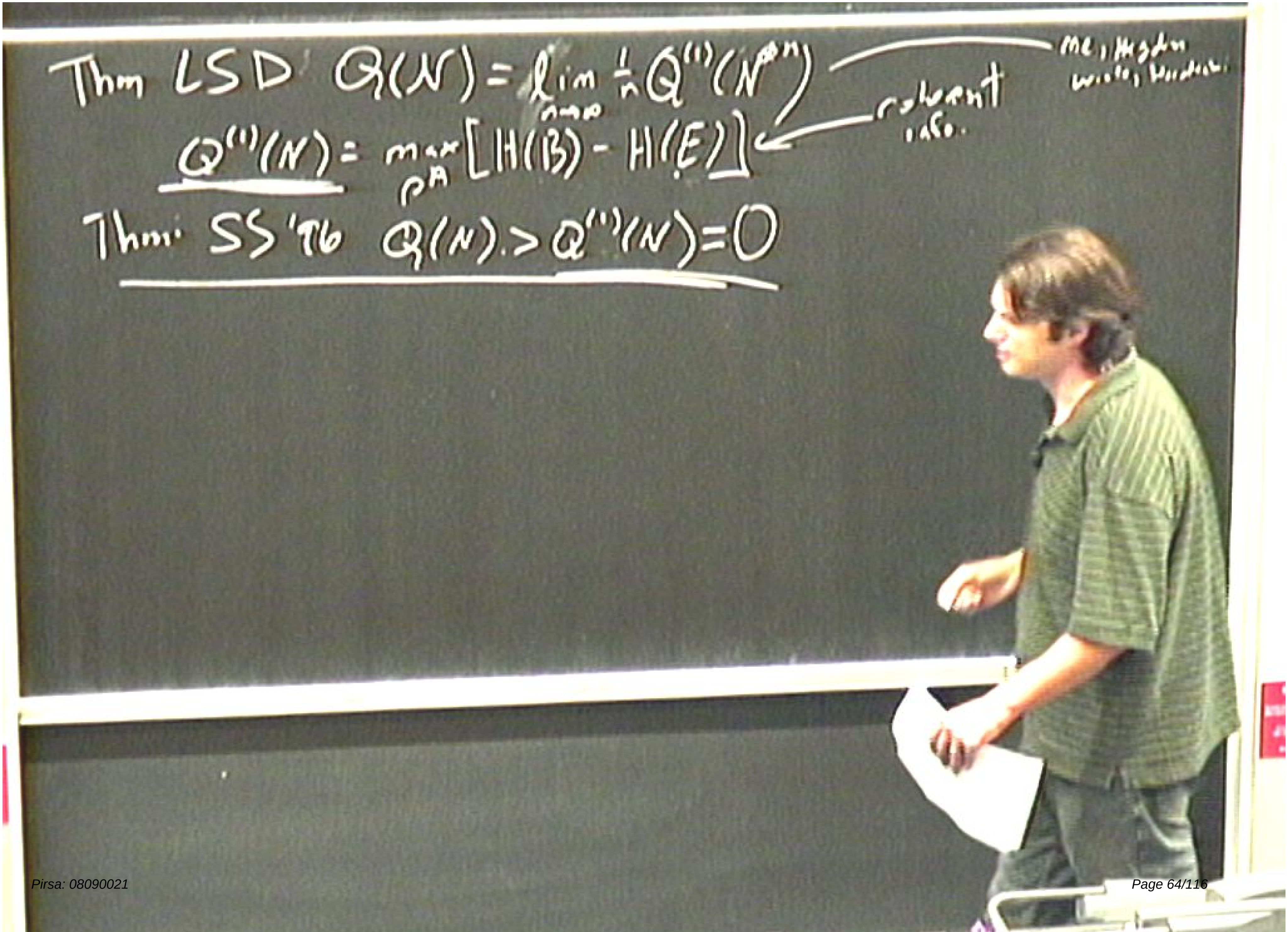

Thm LSD: $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$
$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$
coherent info.
Thm SS '96 $Q(N) > Q^{(1)}(N) = 0$

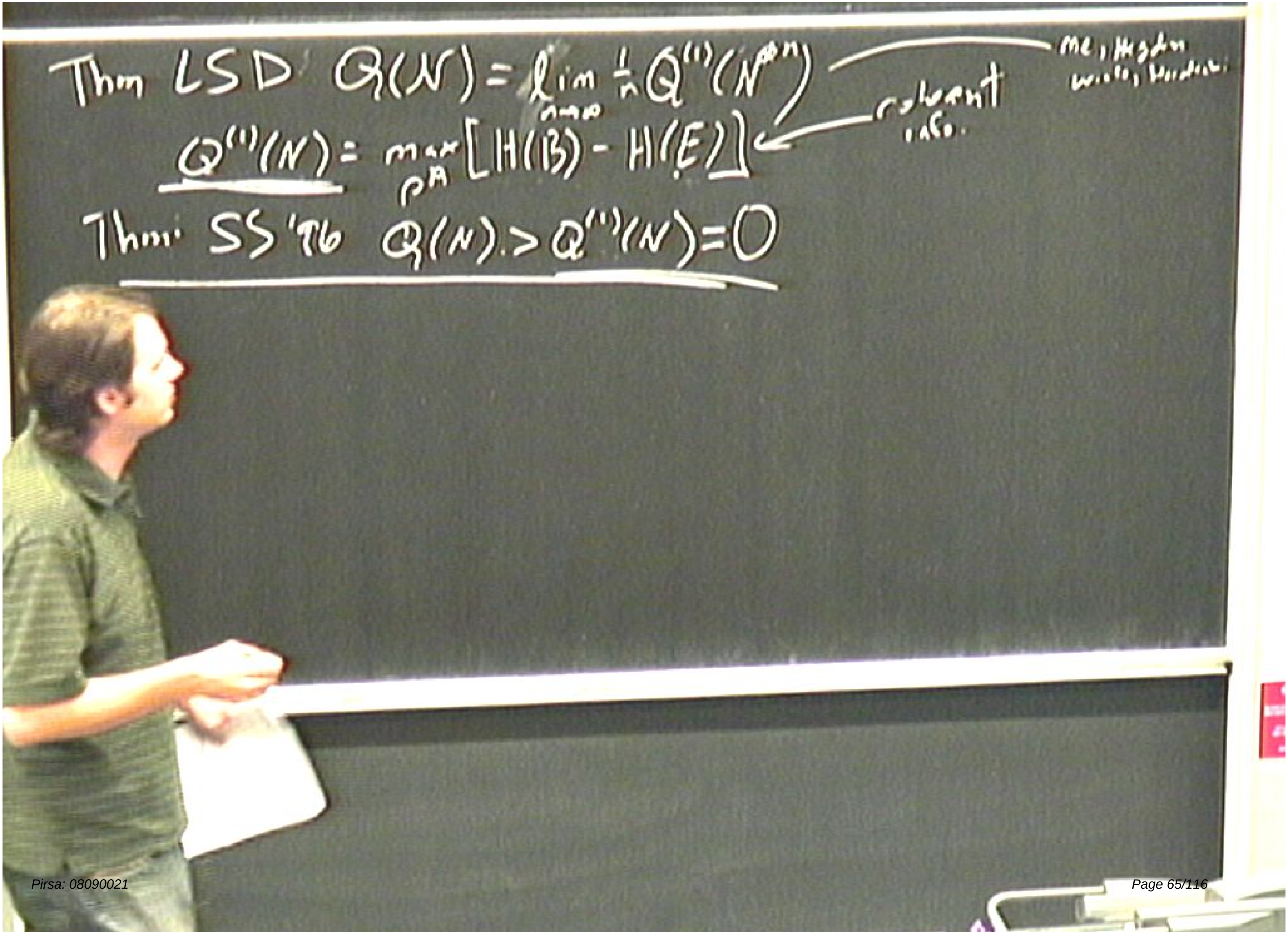
Thm LSD $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n})$

$$\underline{Q^{(1)}(N)} = \max_{\rho^A} [H(B) - H(E)]$$

coherent info.

Thm SS '96 $Q(N) > Q^{(1)}(N) = 0$


Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$
$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$
coherent info.
Thm: SS '06 $Q(N) > Q^{(1)}(N) = 0$


Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$
$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$
coherent info.
Thm SS $Q(N) > Q^{(1)}(N) = 0$

Thm LSD $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n})$

me, Hayden, Winter, Horodecki

$Q^{(1)}(\mathcal{N}) = \max_{\rho^A} [H(B) - H(E)]$

coherent info.

Thm: SS '08 $Q(\mathcal{N}) > Q^{(1)}(\mathcal{N}) = 0$

Thm LSD: $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$ — [illegible]

$Q^{(1)}(N) = \max_{\rho^A} [H(B) - H(E)]$ — coherent info.

Thm: SS '06 $Q(N) > Q^{(1)}(N) = 0$

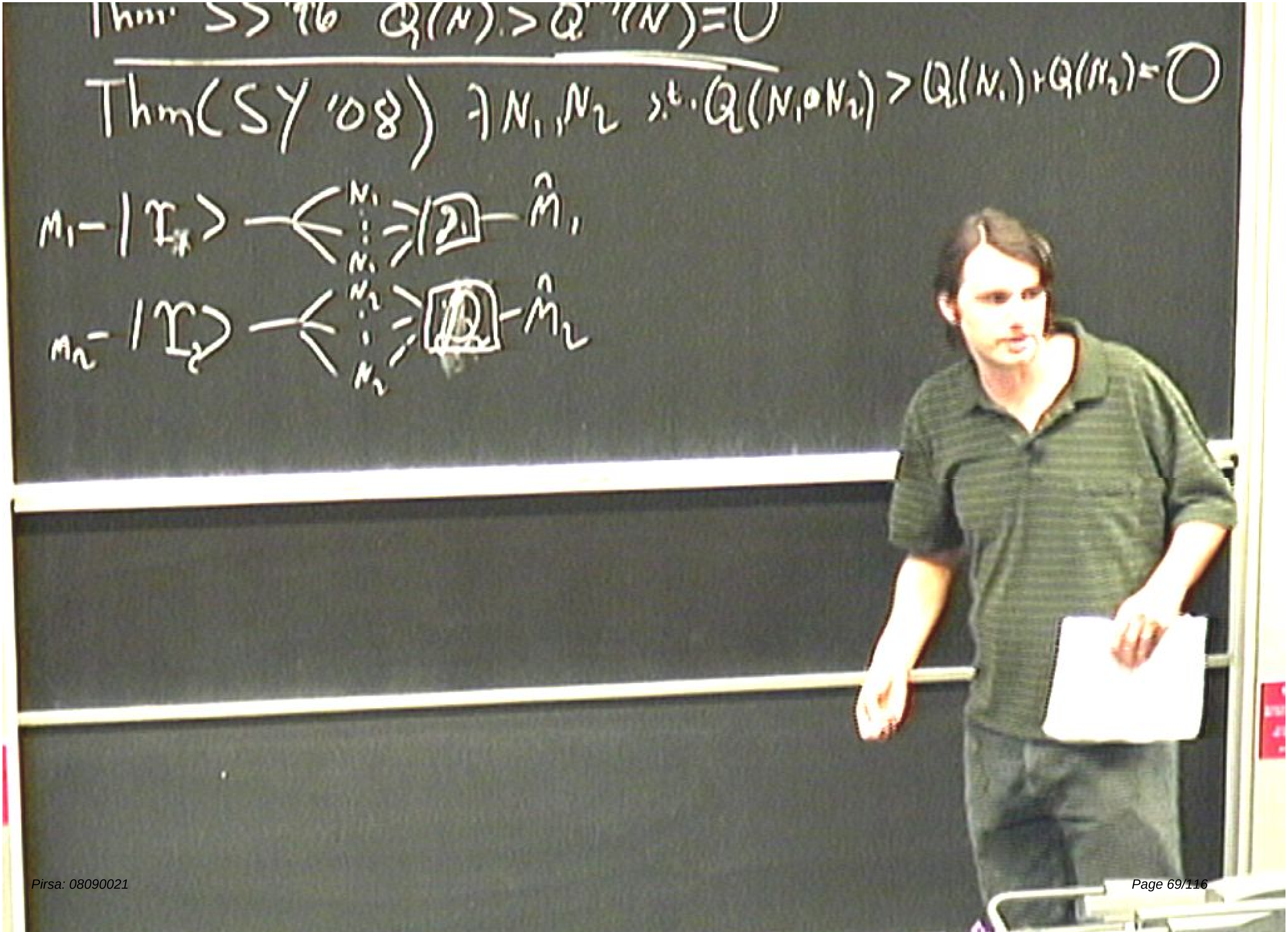
Thm (SY '08) $\exists N_1, N_2$ s.t. $Q(N_1 \otimes N_2)$

Thm LSD: $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$

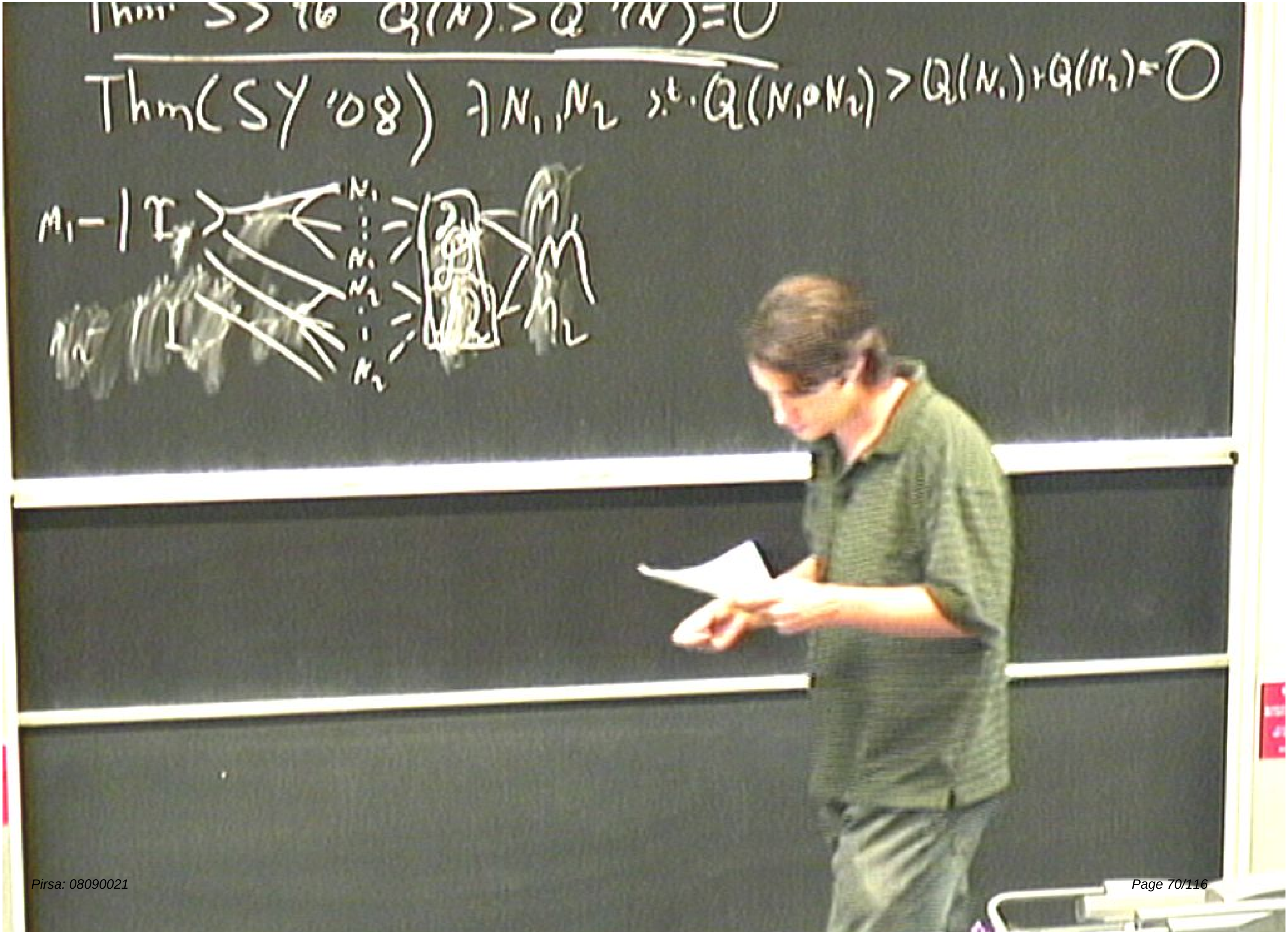
$\underline{Q^{(1)}(N)} = \max_{\rho^A} [H(B) - H(E)]$ ← coherent info.

Thm: SS '96 $Q(N) > Q^{(1)}(N) = 0$

Thm (SY '08) $\exists N_1, N_2$ s.t. $Q(N_1 \otimes N_2) > Q(N_1) + Q(N_2) = 0$



Thm SS '96 $Q(N) > Q^{(1)}(N) = 0$
Thm (SY '08) $\exists N_1, N_2$ s.t. $Q(N_1 \otimes N_2) > Q(N_1) + Q(N_2) = 0$


Thm(SY '08) ∃ N1, N2 s.t. Q(N1⊗N2) > Q(N1)+Q(N2)=0

Thm: SS '06 $Q(N) > Q^{(1)}(N) = 0$

Thm (SY '08) $\exists N_1, N_2$ s.t. $Q(N_1 \otimes N_2) > Q(N_1) + Q(N_2) = 0$

Thm LSD: $Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n})$ me, Hayden, Winter, Horodecki

$\underline{Q^{(1)}(\mathcal{N})} = \max_{\rho^A} [H(B) - H(E)]$ coherent info.

Thm: SS '06 $Q(\mathcal{N}) > \underline{Q^{(1)}(\mathcal{N})} = 0$

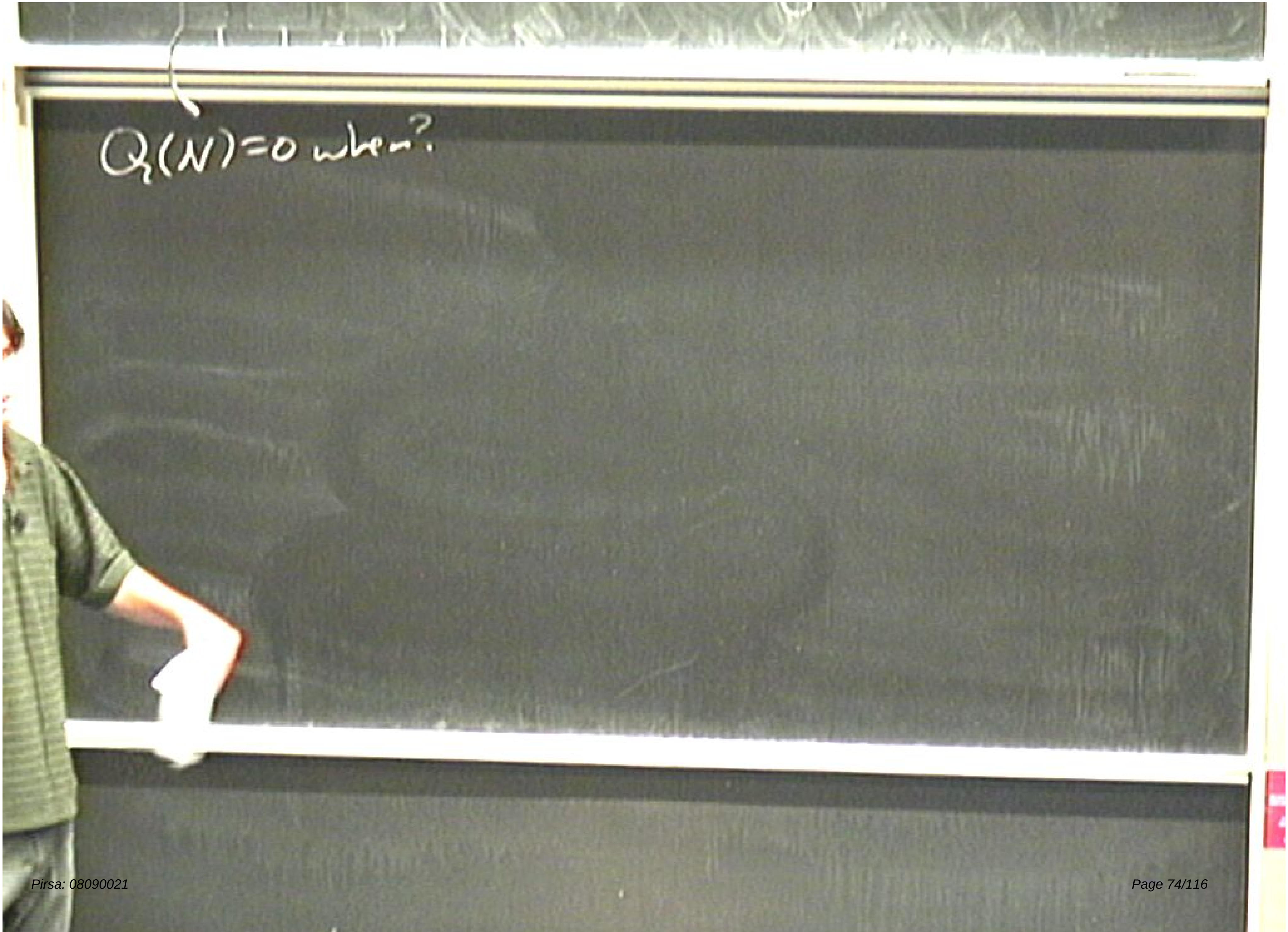
Thm (SY '08) $\exists \mathcal{N}_1, \mathcal{N}_2$ s.t. $Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > Q(\mathcal{N}_1) + Q(\mathcal{N}_2) = 0$

Thm LSD $Q(N) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}(N^{\otimes n})$ — coherent info.

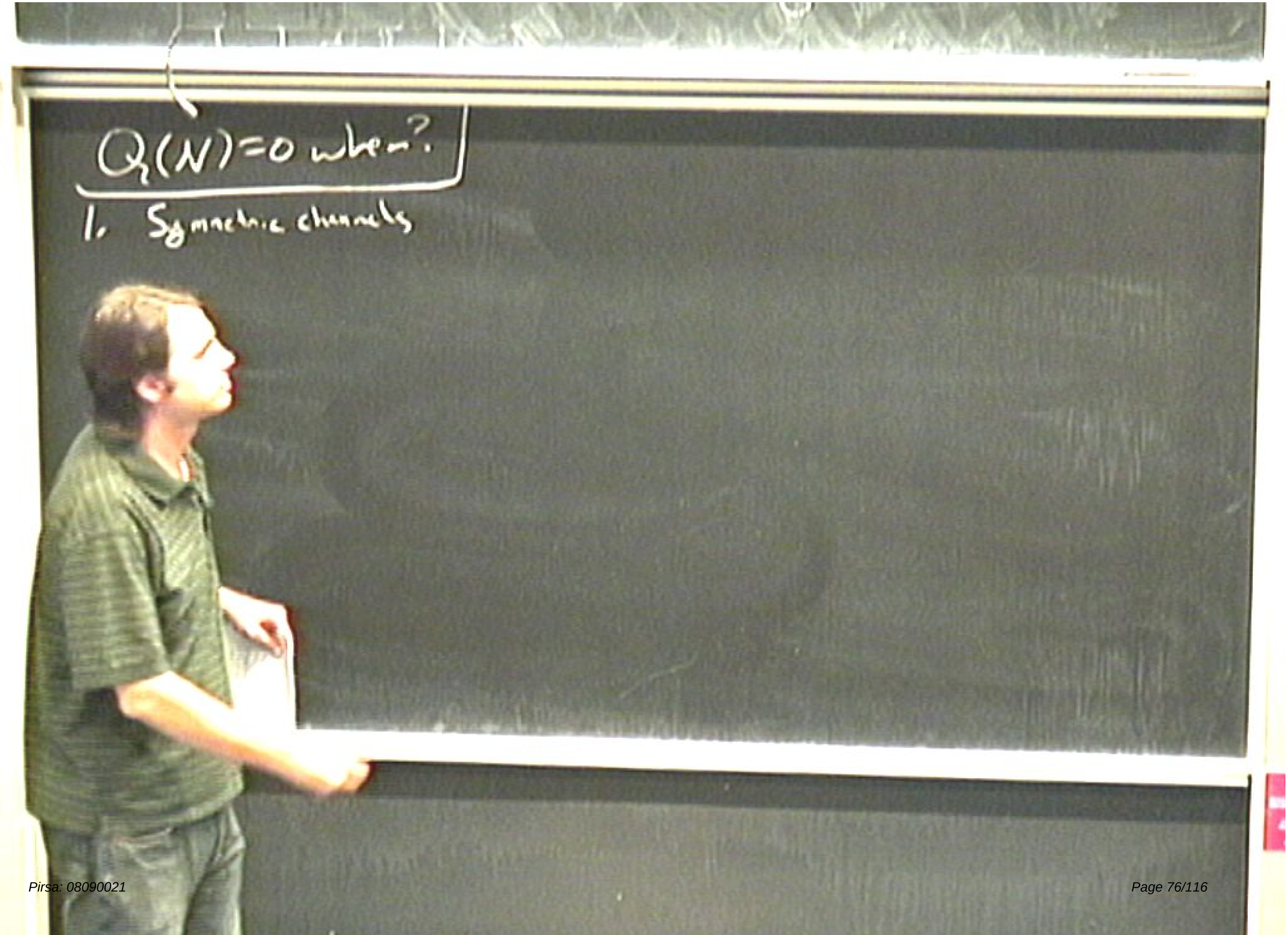
$\underline{Q^{(1)}(N)} = \max_{\rho^A} [H(B) - H(E)]$

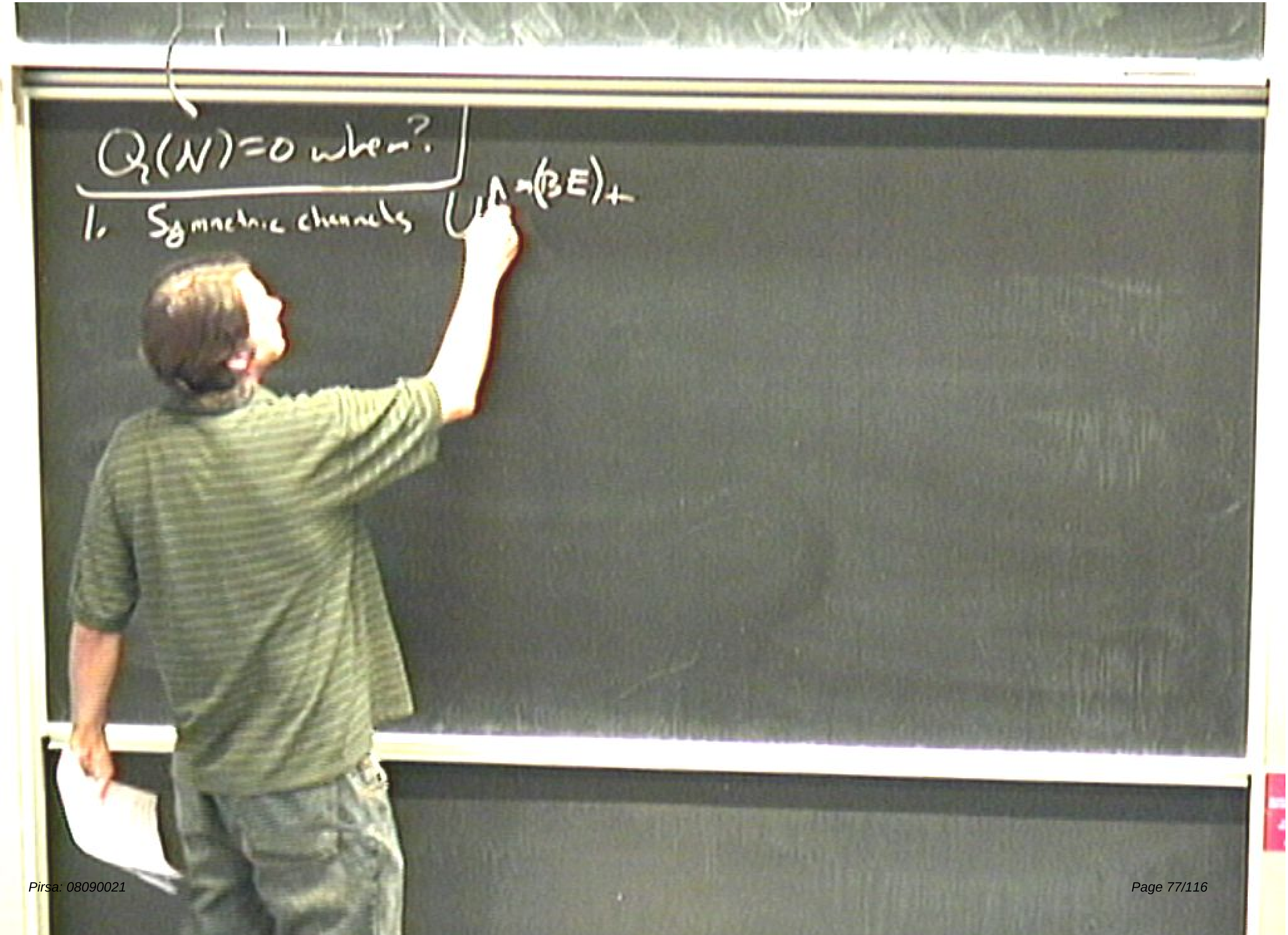
Thm: SS '96 $Q(N) > Q^{(1)}(N) = 0$

Thm (SY '08) $\exists N_1, N_2$ s.t. $Q(N_1 \otimes N_2) > \underline{Q(N_1) + Q(N_2) = 0}$


Q(N)=0 when?

$Q_1(N) = 0$ when?


$Q_1(N)=0$ when?
1. Symmetric channels


Q(N)=0 when?
1. Symmetric channels

$\boxed{Q(N)=0 \text{ when?}}$

1. Symmetric channels $U^{A\to BE}$, $Q^{(1)}=0$, $H(B)=H(E)$

   $Q=0$

2.

$\boxed{Q(N)=0 \text{ when?}}$

1. Symmetric channels $U^{A\to BE}$ $Q^{(1)}=0$ $H(B)=H(E)$

$Q=0$

2. Horodecki channels

$\boxed{Q(N)=0 \text{ when?}}$

1. Symmetric channels $U^{A\to(BE)}$ + $Q^{(1)}=0$ $\quad H(B)=H(E)$

$Q=0$

2. Horodecki channels (PPT, entang. binding)

$\boxed{Q_1(\mathcal{N}) = 0 \text{ when?}}$

1. Symmetric channels $U^{A \to (BE)_+}$ $\quad Q^{(1)} = 0 \quad H(B) = H(E)$

$Q_1 = 0$

2. Horodecki channels (PPT, entang. binding)

$\rho^{AB} = (\mathbb{1}^A \otimes \mathcal{N})(\rho^{AA'})$

$Q_1(N) = 0$ when?

1. Symmetric channels $U^{A\to(BE)_+}$ $Q^{(1)} = 0$ $H(B) = H(E)$

$Q_1 = 0$

2. Horodecki channels (PPT, entang. binding)

$\rho^{AB} = (\mathbb{1}^A \otimes N)(\rho^{AA'})$ $\rho^{AB} = \sum_{ij} |i\rangle\langle j| \, \rho_{ij}^T$

$\boxed{Q_1(N)=0 \text{ when?}}$

1. Symmetric channels $U^{A\to(BE)+}$ $\quad Q^{(1)}=0 \quad H(B)=H(E)$

$Q_1=0$

2. Horodecki channels (PPT, entang. binding)

$\rho^{AB}=(\mathbb{1}^A\otimes N)(\rho^{AA'})$ $\quad \rho^{AB}=\sum_{ij}|i\rangle\langle j|\,\rho_{ij}^T$

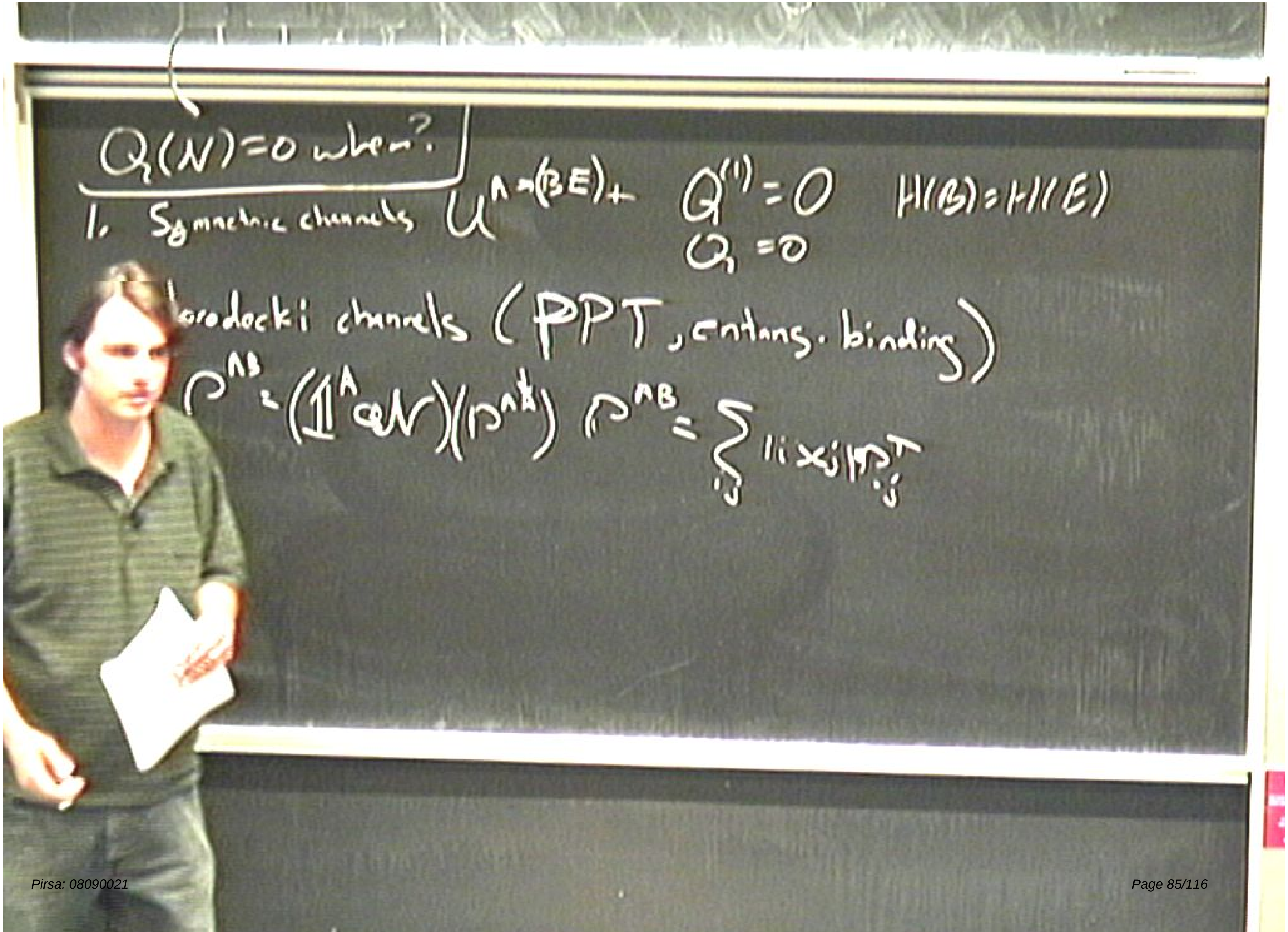
$Q_1(N)=0$ when?

1. Symmetric channels $U^{A\to(BE)_+}$ $\quad Q^{(1)}=0 \quad H(B)=H(E)$

$Q_1=0$

2. Horodecki channels (PPT, entang. binding)

$$\rho^{AB}=(\mathbb{1}^A\otimes N)(\rho^{AA'}) \qquad \rho^{AB}=\sum_{ij}|i\rangle\langle j|\otimes\rho_{ij}^T$$



$Q_1(N)=0$ when?
1. Symmetric channels $U^{A\to BE}_+$ $Q^{(1)}=0$ $H(B)=H(E)$
$Q_1=0$
Horodecki channels (PPT, entang. binding)
$\rho^{AB}=(\mathbb{1}^A\otimes N)(\rho^{AA'})$ $\rho^{AB}=\sum_{ij}|i\rangle\langle j|\otimes\rho_{ij}^T$

$Q_1(N) = 0$ when?

1. Symmetric channels $U^{A \to (BE)_+}$ $\quad Q^{(1)} = 0 \quad H(B) = H(E)$

   $Q_1 = 0$

2. Horodecki channels (PPT, entang. binding)

$$\rho^{AB} = (\mathbb{1}^A \otimes N)(\rho^{AA'}) \quad \rho^{AB} = \sum_{ij} |i\rangle\langle j| \, \rho_{ij}^T$$

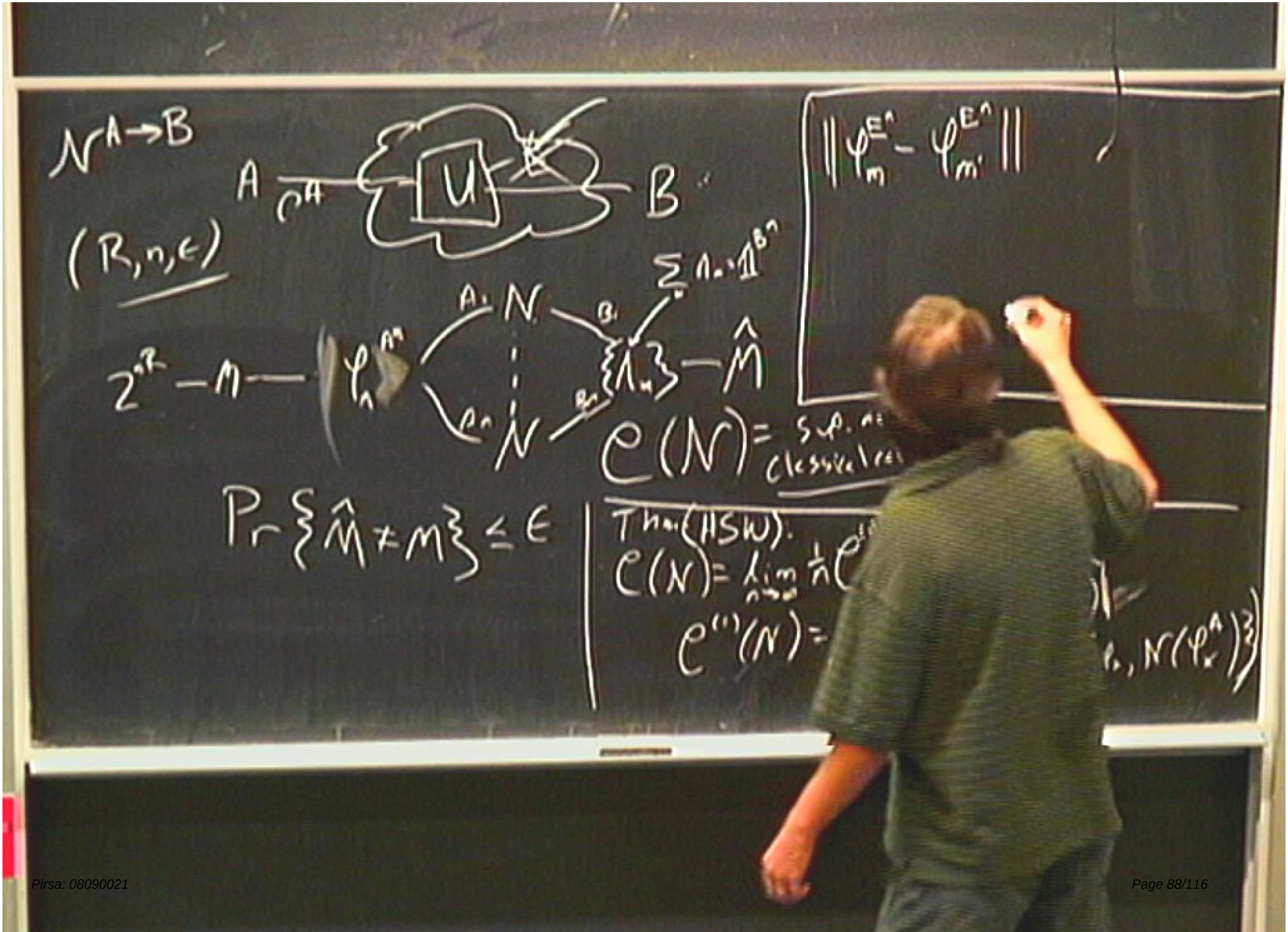
$Q_1(\mathcal{N}) = 0$ when?

1. Symmetric channels $U^{A \to (BE)_+}$ $Q^{(1)} = 0$ $H(B) = H(E)$

$Q_1 = 0$

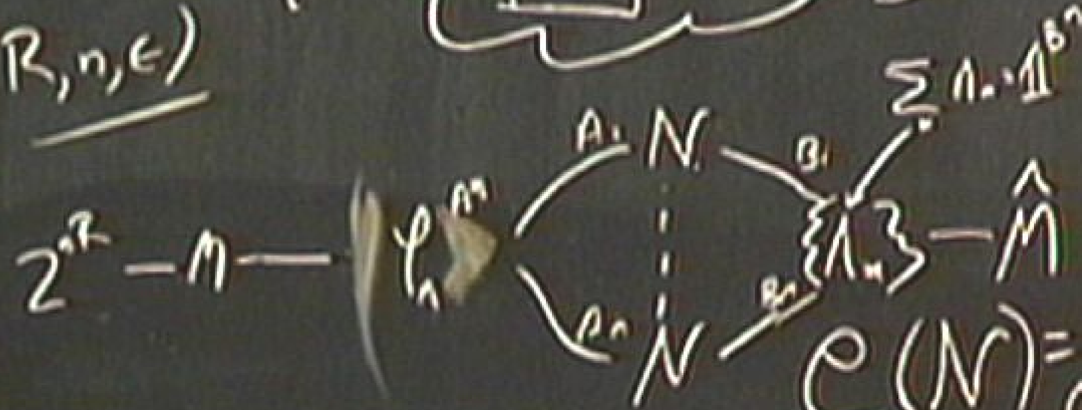
2. Horodecki channels (PPT, entang. binding)

$\rho^{AB} = (\mathbb{1}^A \otimes \mathcal{N})(\phi^{AA'})$ $\rho^{AB} = \sum_{ij} |i\rangle\langle j| \otimes \rho_{ij}^T$



$\mathcal{N}^{A \to B}$

(R, n, ϵ)



$$\boxed{\left\| \varphi_m^{E^n} - \varphi_{m'}^{E^n} \right\|_1 \le \epsilon}$$

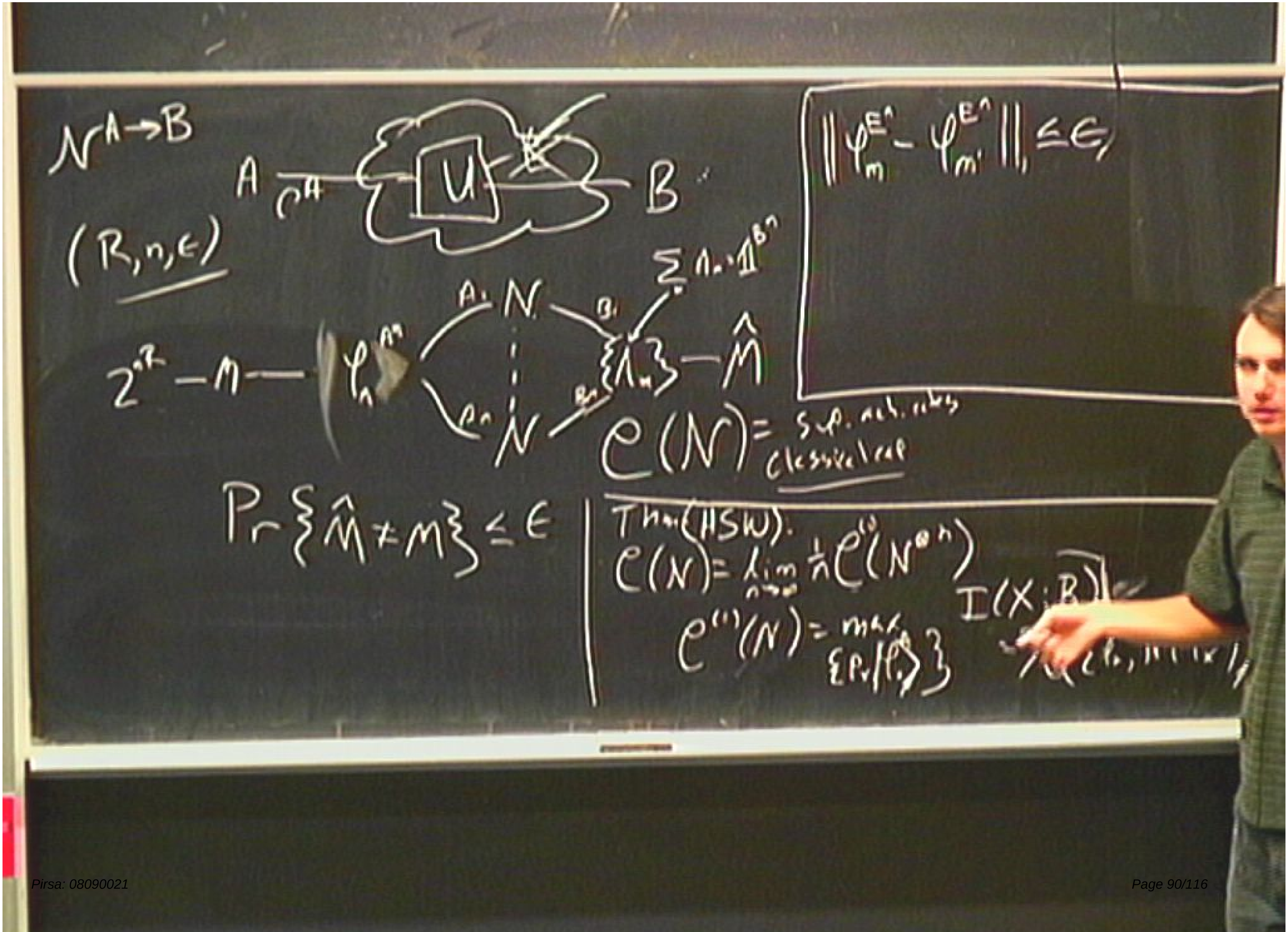
$C(N) = $ sup. ach. rates
classical cap

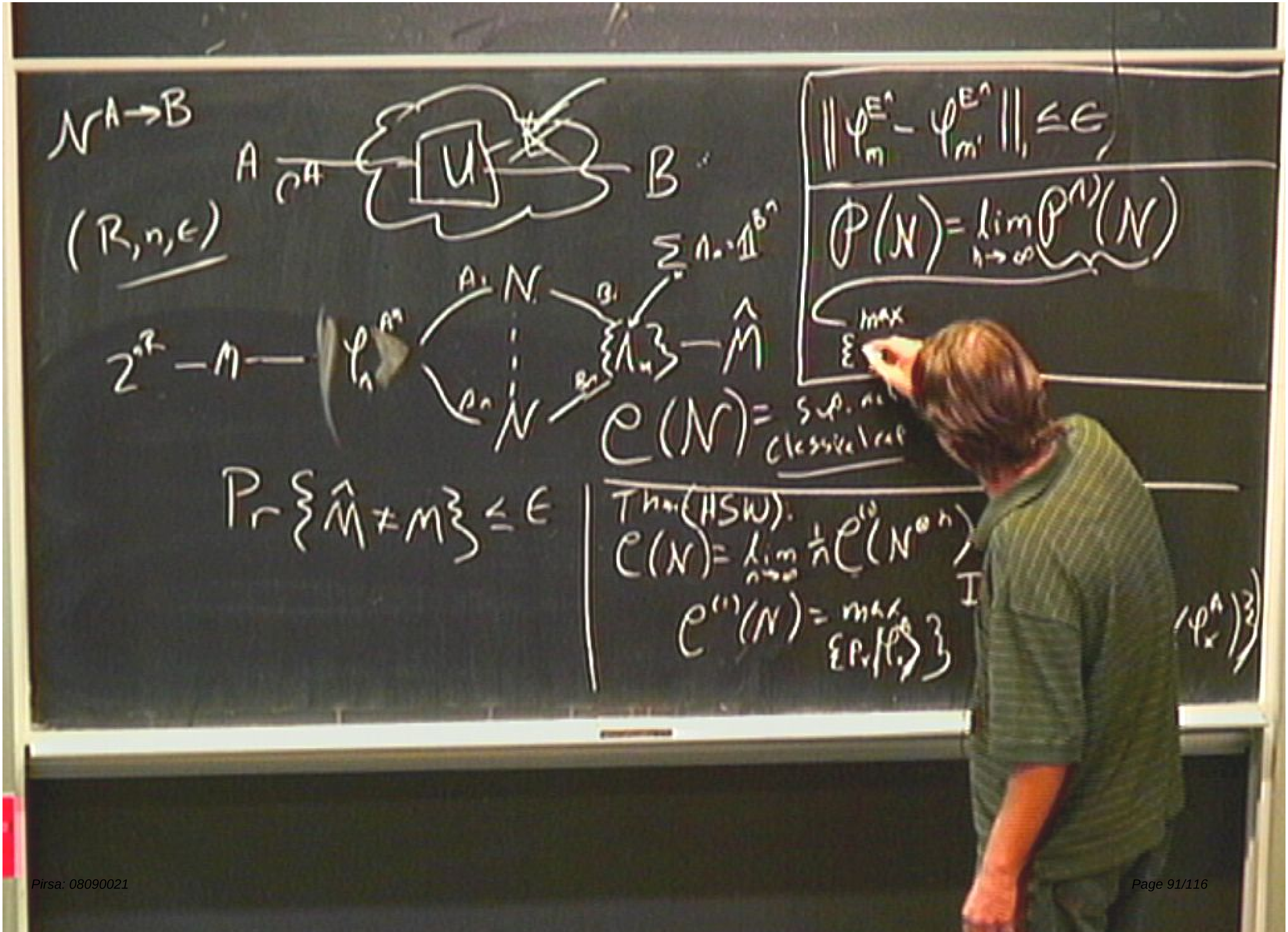
$$\Pr\{\hat{m} \neq m\} \le \epsilon$$

Thm (HSW).

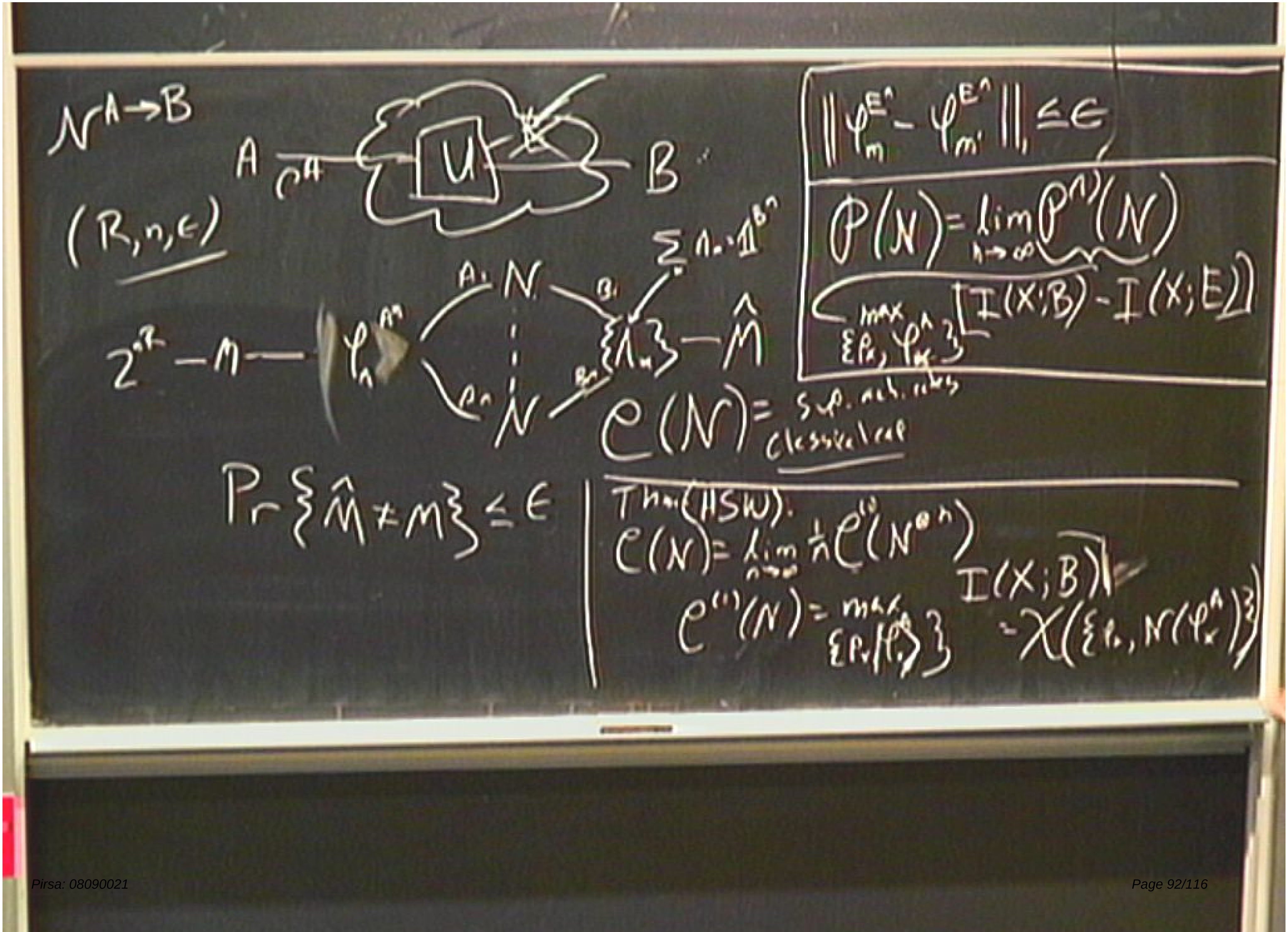
$$C(N) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(N^{\otimes n})$$

$$C^{(1)}(N) = \max_{\{p_x, \rho_x\}} I(X;B) = \chi(\{p_x, N(\rho_x)\})$$


$\mathcal{N}^{A\to B}$
(R,n,ϵ)
A
B
U
$\| \varphi_m^{E^n} - \varphi_{m'}^{E^n} \|_1 \le \epsilon$
2^{nR} — m — $\varphi_m^{A^n}$
N
$\{\Lambda_m\}$ — $\hat{m}$
$\sum \Lambda_m = \mathbb{1}^{B^n}$
$\mathcal{C}(N)$ = sup. ach. rates classical cap
$\Pr\{\hat{m} \neq m\} \le \epsilon$
Thm (HSW).
$\mathcal{C}(N) = \lim_{n\to\infty} \frac{1}{n} \mathcal{C}^{(1)}(N^{\otimes n})$
$\mathcal{C}^{(1)}(N) = \max_{\{p_x, |\varphi_x\rangle\}}$
$I(X;B)$



N^{A→B}
(R, n, ε)
2^{nR} — m — φ_m^{A^n}
Pr{m̂ ≠ m} ≤ ε
‖φ_m^{E^n} − φ_{m'}^{E^n}‖_1 ≤ ε
P(N) = lim_{n→∞} P^{(1)}(N)
C(N) = sup. achievable classical rate
Thm (HSW).
C(N) = lim_{n→∞} 1/n C^{(1)}(N^{⊗n})
C^{(1)}(N) = max_{{p_x, φ_x}}


N^{A→B}
(R, n, ε)
A
B
U
2^{nR}
Pr{M̂ ≠ m} ≤ ε
‖φ_m^{E^n} − φ_{m'}^{E^n}‖_1 ≤ ε
P(N) = lim P^{(n)}(N)
max [I(X;B) − I(X;E)]
C(N) = sup. ach. rates
Classical cap
Thm (HSW):
C(N) = lim 1/n C^{(1)}(N^{⊗n})
C^{(1)}(N) = max
I(X;B)

$\mathcal{N}^{A \to B}$

(R, n, ϵ)

$\sum_m \Lambda_m = \mathbb{1}^{B^n}$

$2^{nR} - m - \varphi_m^{A^n}$ — $A_1\ N\ B_1$, $A_n\ N\ B_n$ — $\{\Lambda_m\} - \hat{m}$

$\Pr\{\hat{m} \neq m\} \leq \epsilon$

$\mathcal{C}(N) = $ sup. ach. rates classical cap

$\| \varphi_m^{E^n} - \varphi_{m'}^{E^n} \|_1 \leq \epsilon$

$\mathcal{P}(N) = \lim_{n \to \infty} \mathcal{P}^{(n)}(N)$

$\max_{\{p_x, \varphi_x^{A^n}\}} [I(X;B) - I(X;E)]$

Thm (HSW).

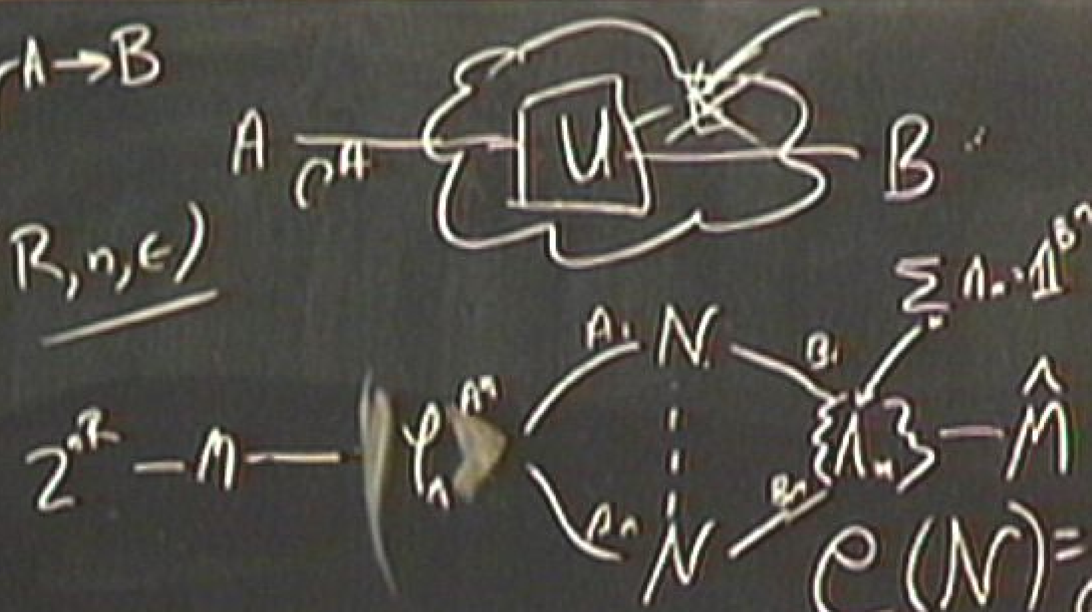
$\mathcal{C}(N) = \lim_{n \to \infty} \frac{1}{n} \mathcal{C}^{(1)}(N^{\otimes n})$

$\mathcal{C}^{(1)}(N) = \max_{\{p_x, |\varphi_x\rangle\}}$ $I(X;B)$

$= \chi(\{p_x, N(\varphi_x^A)\})$

$\mathcal{N}^{A\to B}$

(R, n, ϵ)



$$\Pr\{\hat{m} \neq m\} \leq \epsilon$$

$$\| \varphi_m^{E^n} - \varphi_{m'}^{E^n} \|_1 \leq \epsilon$$

$$P(\mathcal{N}) = \lim_{n\to\infty} P^{(1)}(\mathcal{N}^{\otimes n})/n$$

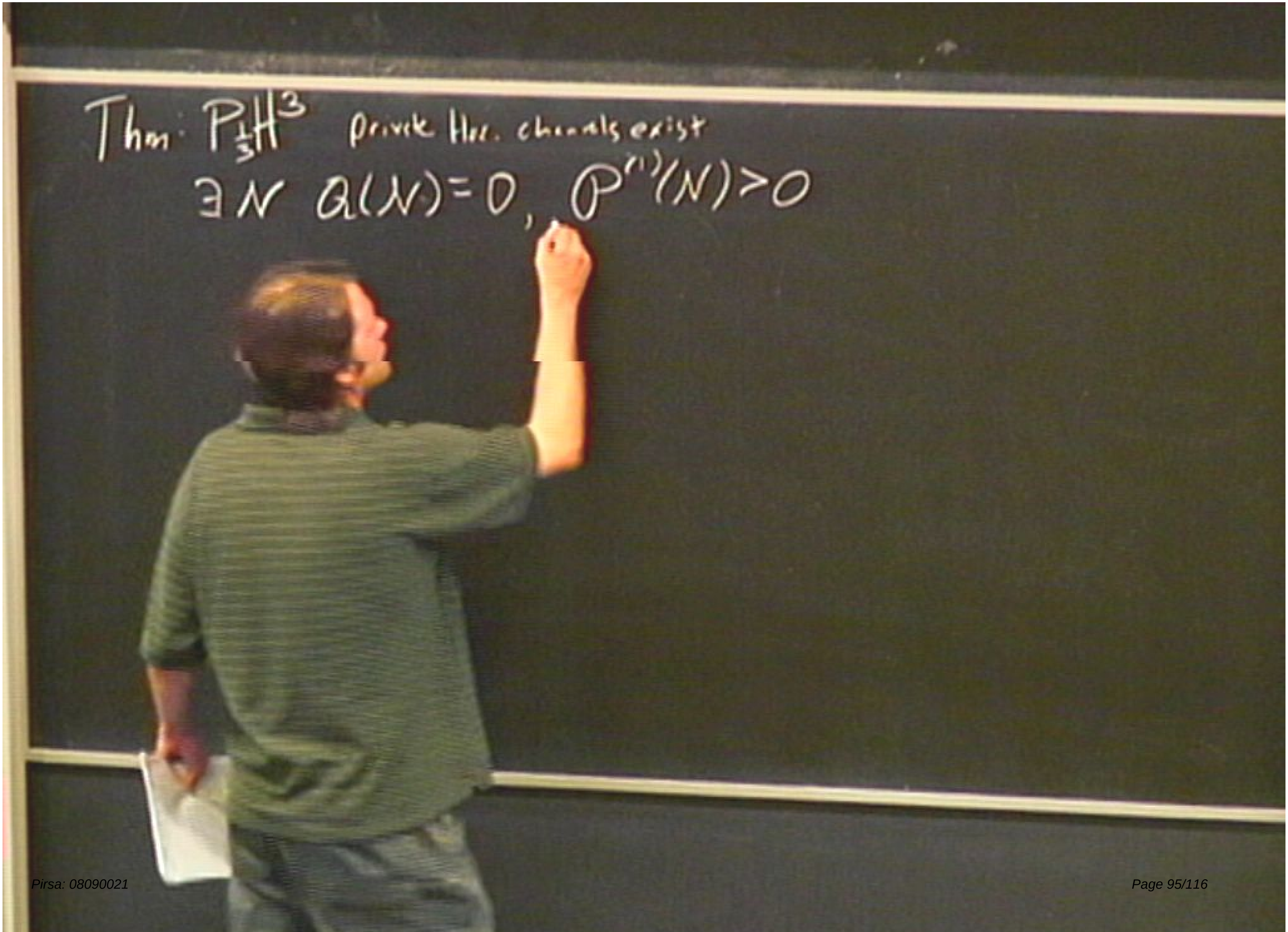
$$\max_{\{p_x, \varphi_x^A\}} [I(X;B) - I(X;E)]$$

$$C(\mathcal{N}) = \underset{\text{classical cap}}{\text{sup. ach. rates}}$$

Thm (HSW):

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(\mathcal{N}^{\otimes n})$$

$$C^{(1)}(\mathcal{N}) = \max_{\{p_x, |\varphi_x\rangle\}} I(X;B) = \chi(\{p_x, \mathcal{N}(\varphi_x^A)\})$$



Thm: $P_{\frac{1}{3}}H^3$ private thr. channels exist
$\exists N \; Q(N)=0, \; \mathcal{P}^{(1)}(N)>0$

Thm: $P_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \; Q(N)=0, \; \underline{\mathcal{P}^{(1)}(N)>0}$

Thm: $Q_{\frac{1}{3}}H^3$ private Her. channels exist

$\exists N \quad Q(N)=0, \quad \underline{P^{(1)}(N)>0}$

Thm: $P \; H^3$: $\exists N$ on 2 qubits s.t. ↑

w.r.t unif ens. $\{|0\rangle\langle 0| \otimes \frac{1\!\!1_2}{2}, |1\rangle\langle 1| \otimes \frac{1\!\!1_2}{2}\}$, $I(X;B) - I(X;E) > .02$

Thm: $Q_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \; Q(N)=0, \; P^{(1)}(N)>0$

Thm: $P H^3$: $\exists N$ on 2 qubits st. ↑

w.r.t unif ens. $\left\{ |0\rangle\langle 0| \otimes \frac{\mathbb{1}_2}{2}, |1\rangle\langle 1| \otimes \frac{\mathbb{1}_2}{2} \right\}$, $I(X;B) - I(X;E) > .02$

Thm: $Q_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \quad Q(N)=0, \quad \underline{P^{(1)}(N)>0}$

Thm: PH^3: $\exists N$ on 2 qubits s.t. $\uparrow$

w.r.t. unif. ens. $\left\{ |0\rangle\langle 0| \otimes \frac{\mathbb{1}_2}{2}, |1\rangle\langle 1| \otimes \frac{\mathbb{1}_2}{2} \right\}$, I ... $I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^n\}$, $N^{n} \xrightarrow{E} B$, let $\mathcal{E}$

Thm: $Q_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \; Q(N)=0, \; P^{(1)}(N)>0$

Thm: PH^3: $\exists N$ on 2 qubits s.t. ↑

wrt unif ens. $\{|0\rangle\langle 0| \otimes \frac{\mathbb{1}_2}{2}, |1\rangle\langle 1| \otimes \frac{\mathbb{1}_2}{2}\}$, $I(X;B) - I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^n\}$, $N^{n} \xrightarrow{A \to B}$, let $\mathcal{E}$ be a 50% erasure channel

Thm: $\varphi_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \; Q(N)=0, \; P^{(1)}(N)>0$

Thm: PH^3 : $\exists N$ on 2 qubits s.t. ↑

w.r.t unif ens. $\{|0\rangle\langle 0| \otimes \frac{\mathbb{1}_2}{2}, |1\rangle\langle 1| \otimes \frac{\mathbb{1}_2}{2}\}$, $I(X;B) - I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A \to B}_{E}$, let $\mathcal{E}$ be a 50% erasure channel

with input dim $= \sum_x \text{rank}\, \rho_x^A$

Thm: $Q_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \quad Q(N)=0, \ P^{(1)}(N)>0$

Thm: PH^3: $\exists N$ on 2 qubits s.t. ↑

w.r.t. unif ens. $\{|0\rangle\langle 0|\otimes \frac{I_2}{2}, |1\rangle\langle 1|\otimes \frac{I_2}{2}\}$, $I(X;B)-I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A\xrightarrow{E}B}$, let $\mathcal{E}$ be a 50% erasure channel

with input dim $= \sum_x \text{rank}\, \rho_x^A$. Then $Q^{(1)}(N\otimes\mathcal{E}) \geq \frac{1}{2}\left[I(X;B)-I(X;E)\right]_\sigma$

Thm $\phi_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \quad Q(N)=0, \quad P^{(1)}(N)>0$

Thm: PH^3: $\exists N$ on 2 qubits s.t. ↑

w.r.t. unif. ens. $\left\{ |0\rangle\langle 0| \otimes \frac{I_2}{2},\ |1\rangle\langle 1| \otimes \frac{I_2}{2} \right\}$, $I(X;B) - I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A \to B}$ (with E), let $\mathcal{E}$ be a 50% erasure channel

with input dim $= \sum_x \mathrm{rank}\, \rho_x^A$. Then $Q^{(1)}(N \otimes \mathcal{E}) \geq \frac{1}{2}\left[I(X;B) - I(X;E) \right]$

Thm: $\frac{S}{3}H^3$ private Hor. channels exist

$\exists N \quad Q(N) = 0, \ P^{(1)}(N) > 0$

Thm: PH^3: $\exists N$ on 2 qubits s.t. ↑

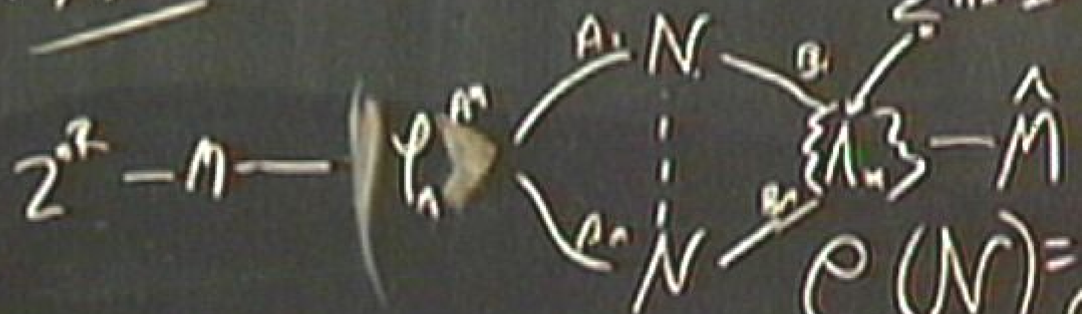
w.r.t. unif. ens. $\{|0\rangle\langle 0| \otimes \frac{\mathbb{1}_2}{2}, |1\rangle\langle 1| \otimes \frac{\mathbb{1}_2}{2}\}$, $I(X;B) - I(X;E) > .02$

Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A \to B}_{E}$, let $\mathcal{E}$ be a 50% erasure channel with input dim $= \sum_x \operatorname{rank} \rho_x^A$. Then $Q^{(1)}(N \otimes \mathcal{E}) \geq \frac{1}{2}[I(X;B) - I(X;E)]$

$\mathcal{N}^{A\to B}$

(R,n,ϵ)



$\Pr\{\hat{m} \neq m\} \le \epsilon$

$C(\mathcal{N}) = \underline{\text{sup. achievable classical rate}}$

$\|\varphi_m^{E^n} - \varphi_{m'}^{E^n}\|_1 \le \epsilon$

$P(\mathcal{N}) = \lim_{n\to\infty} P^{(1)}(\mathcal{N}^{\otimes n})/n$

$\max_{\{p_x, \varphi_x^A\}} [I(X;B) - I(X;E)]$

Thm (HSW):

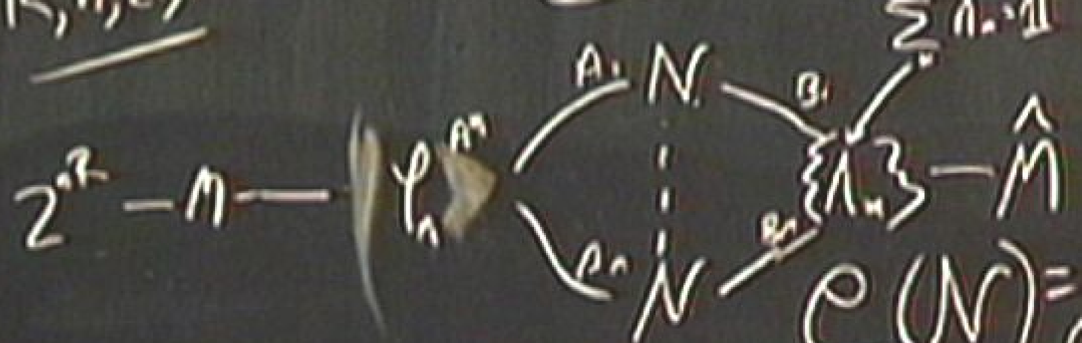
$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(\mathcal{N}^{\otimes n})$

$C^{(1)}(\mathcal{N}) = \max_{\{p_x, |\varphi_x\rangle\}} I(X;B)$

$= \chi(\{p_x, \mathcal{N}(\varphi_x^A)\})$

$\mathcal{N}^{A\to B}$

(R,n,ϵ)



$\Pr\{\hat{m} \neq m\} \leq \epsilon$

$\|\varphi_m^{E^n} - \varphi_{m'}^{E^n}\|_1 \leq \epsilon$

$P(\mathcal{N}) = \lim_{n\to\infty} P^{(1)}(\mathcal{N}^{\otimes n})/n$

$\max_{\{p_x, \varphi_x^A\}} [I(X;B) - I(X;E)]$

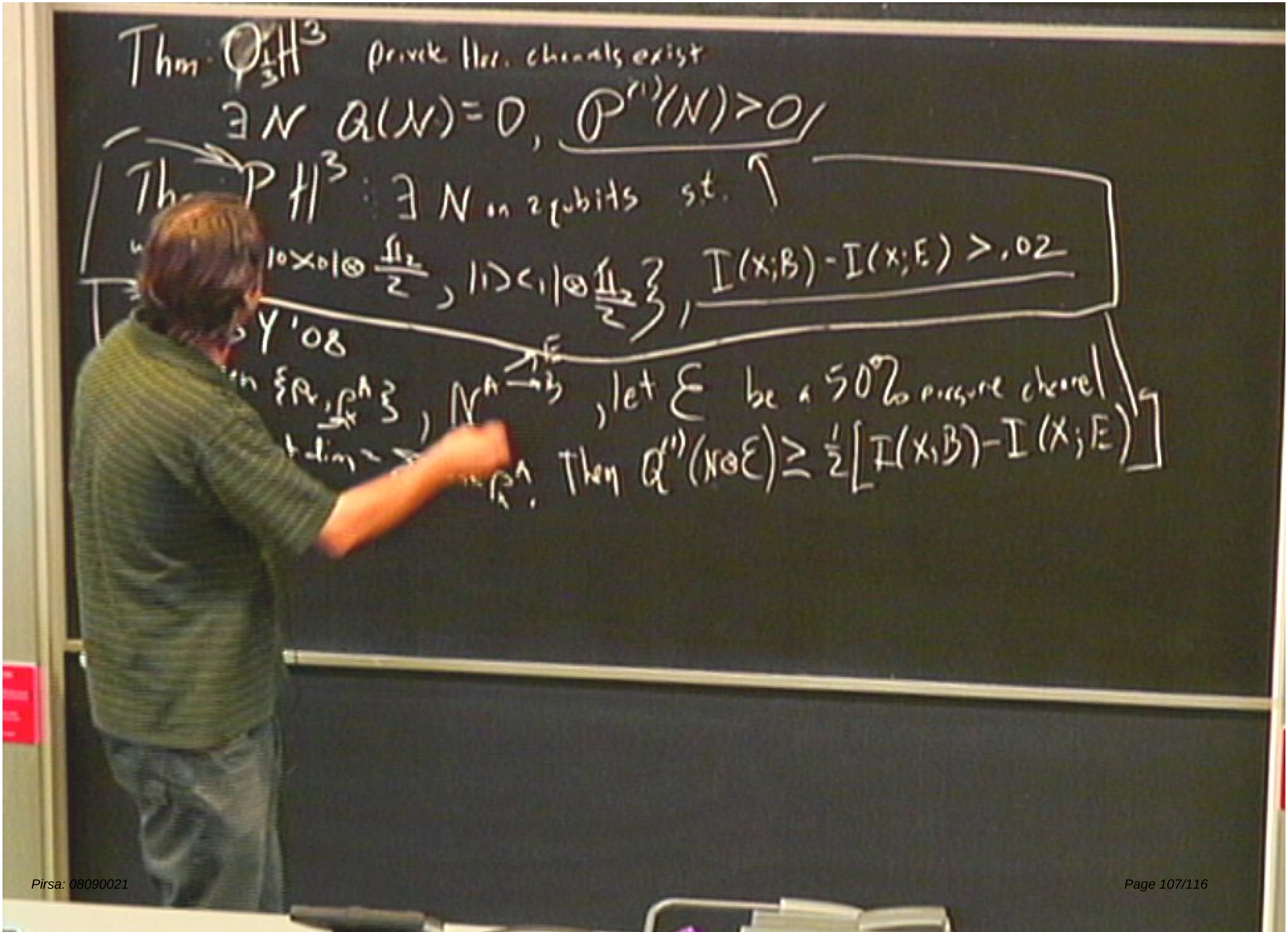
$C(\mathcal{N}) =$ sup. ach. rates classical cap

Thm (HSW):

$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}(\mathcal{N}^{\otimes n})$

$C^{(1)}(\mathcal{N}) = \max_{\{p_x, |\varphi_x\rangle\}} I(X;B)$

$I(X;B) = \chi(\{p_x, \mathcal{N}(\varphi_x^A)\})$


∃ N Q(N)=0, P^(1)(N)>0
∃ N on 2 qubits st.
I(X;B) - I(X;E) > .02
Y '08
let E be a 50% erasure channel
Then Q^(1)(N⊗E) ≥ ½[I(X;B) - I(X;E)]

Thm: $Q_{\frac{1}{3}}H^3$ private Hor. channels exist

$\exists N \quad Q(N)=0, \ \underline{P^{(1)}(N)>0}$

Thm: PH^3: $\exists N$ on 2 qubits s.t. ↑

wrt unif ens. $\left\{|0\rangle\langle 0| \otimes \frac{I_2}{2}, |1\rangle\langle 1| \otimes \frac{I_2}{2}\right\}$, $\underline{I(X;B) - I(X;E) > .02}$

Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A \to B}$, let $\mathcal{E}$ be a 50% erasure channel with input dim = $\sum_x \operatorname{rank} \rho_x^A$. Then $Q^{(1)}(N \otimes \mathcal{E}) \geq \frac{1}{2}\left[I(X;B) - I(X;E)\right]$

Thm: $\mathcal{Q}\frac{1}{3}H^3$ private H.c. channels exist

$\exists N \; Q(N)=0, \; P^{(1)}(N)>0$

Thm: PH^3: $\exists N$ on 2 qubits s.t.

w.r.t. unif. ens. $\{|0\rangle\langle 0|\otimes\frac{I_2}{2}, |1\rangle\langle 1|\otimes\frac{I_2}{2}\}$, $I(X;B)-I(X;E)>.02$

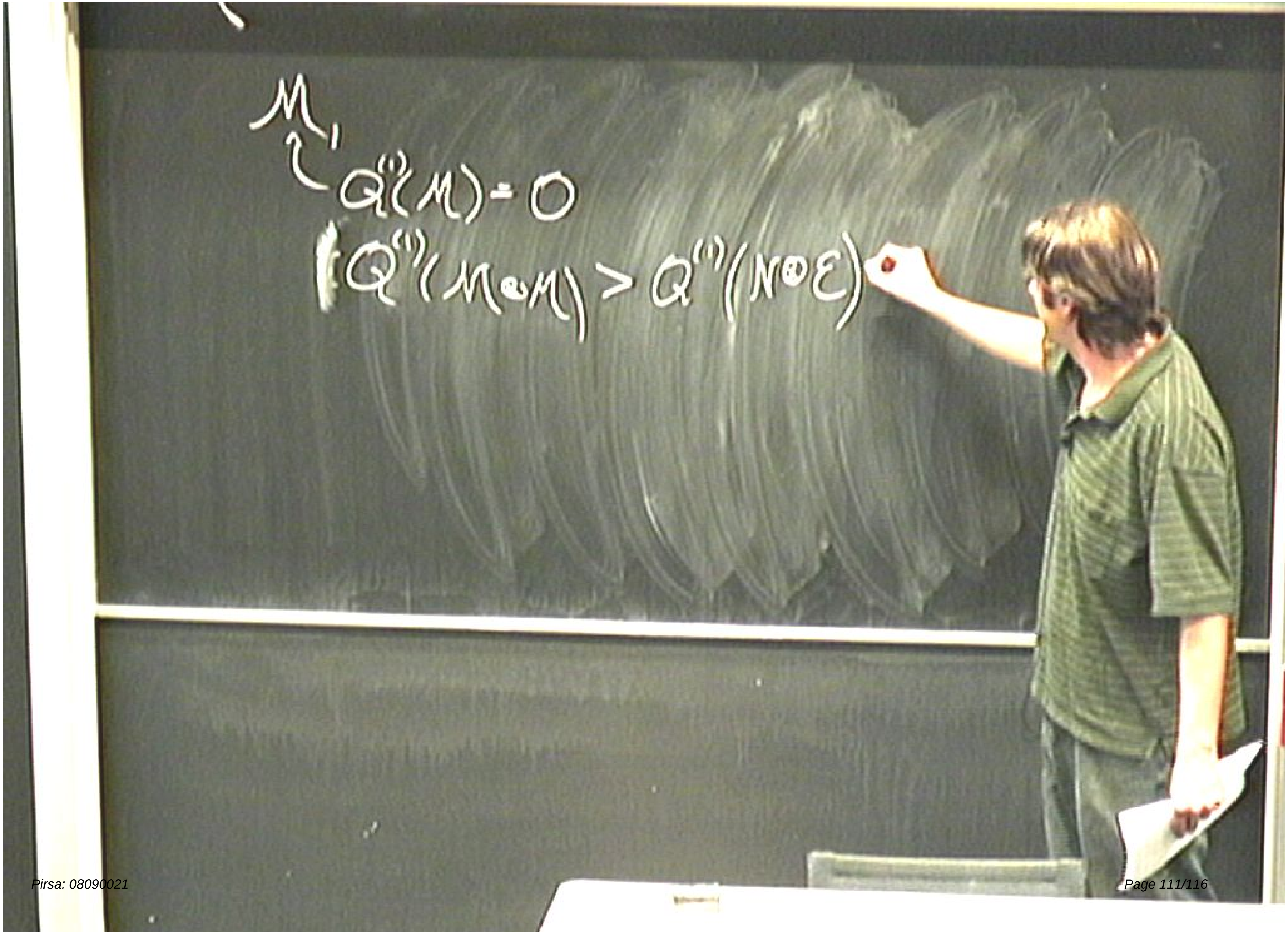
Thm SY '08

given $\{p_x, \rho_x^A\}$, $N^{A\to B}$, let $\mathcal{E}$ be a 50% erasure channel with input dim $=\sum_x \operatorname{rank}\rho_x^A$. Then $Q^{(1)}(N\otimes\mathcal{E})\geq\frac{1}{2}[I(X;B)-I(X;E)]$

$M,$

$Q^{(1)}(M) = 0$

$Q^{(1)}(M \otimes M)$


M,
Q(1)(M) = 0
Q(1)(M⊗M) > Q(1)(N⊗E)

$\mathcal{M}_1$ $\qquad$ $\mathcal{M}_k$ $\quad 2k+1$

$$\underline{Q^{(1)}(\mathcal{M}) = 0}$$

$$Q(\mathcal{M}) \geq Q^{(1)}(\mathcal{M} \otimes \mathcal{M}) > Q^{(1)}(N \otimes \mathcal{E}) > .01$$

$\mathcal{M}_1$ $\quad$ $\mathcal{M}_k$ $\quad$ $\underline{2k+1}$

$\mathcal{N}^{\otimes k}$

$\underline{Q^{(1)}(\mathcal{M}) = 0}$ $\quad$ $\mathcal{E}^{\otimes k}$

$Q(\mathcal{M}) \geq Q^{(1)}(\mathcal{M}\otimes\mathcal{M}) > Q^{(1)}(\mathcal{N}\otimes\mathcal{E}) > \underline{.01}$

$Q(\mathcal{M}_k) > .01k$

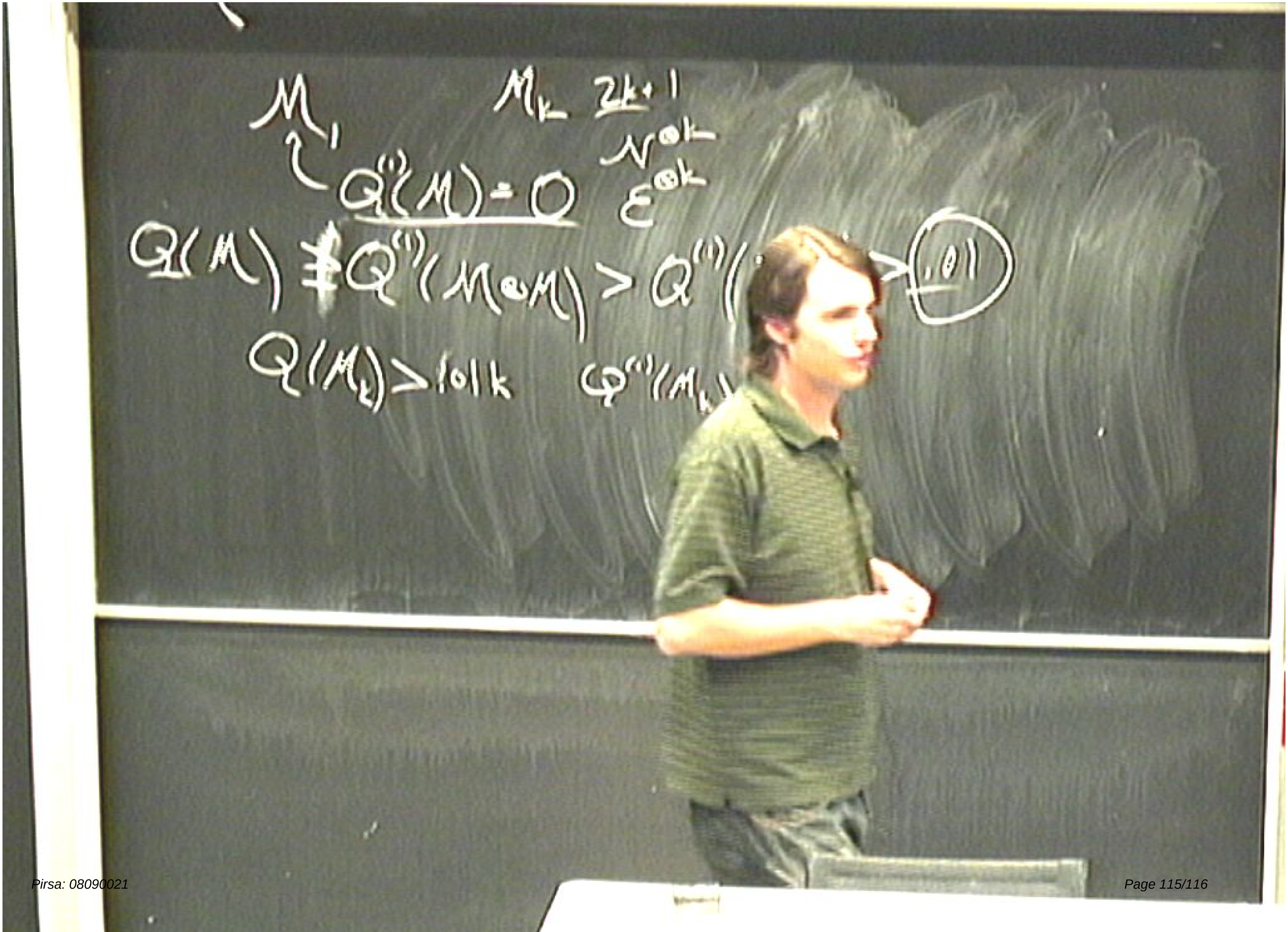
$\mathcal{M}_1$ $\qquad$ $\mathcal{M}_k$ $\quad \underline{2k+1}$

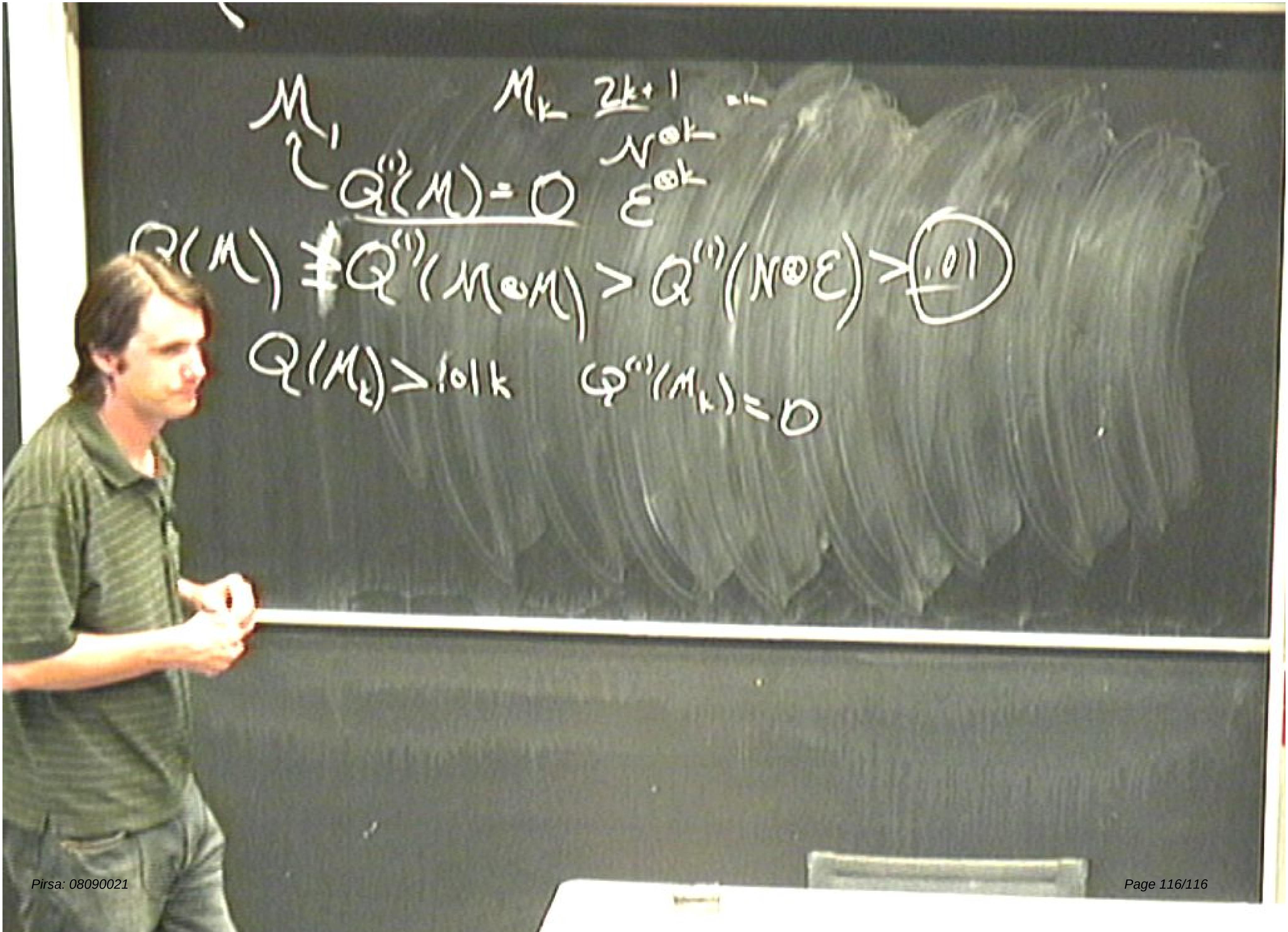
$\mathcal{N}^{\otimes k}$

$\underline{Q^{(1)}(\mathcal{M}) = 0}$ $\quad \mathcal{E}^{\otimes k}$

$$Q(\mathcal{M}) \geq Q^{(1)}(\mathcal{M}\otimes\mathcal{M}) > Q^{(1)}(\mathcal{N}\otimes\mathcal{E}) > .01$$

$$Q(\mathcal{M}_k) > .01k \qquad Q^{(1)}(\mathcal{M}_k) = 0$$


M_1
M_k $2k+1$
$N^{\otimes k}$
$Q^{(1)}(M) = 0$
$\varepsilon^{\otimes k}$
$Q(M) \geq Q^{(1)}(M \otimes M) > Q^{(1)}($
$> .01$
$Q(M_k) > .01k$
$Q^{(1)}(M_k)$


M_1
M_k $2k+1$
$N^{\otimes k}$
$Q^{(1)}(M) = 0$
$\mathcal{E}^{\otimes k}$
$Q(M) \geq Q^{(1)}(M \otimes M) > Q^{(1)}(N \otimes \mathcal{E}) > .01$
$Q(M_k) > .01k$
$Q^{(1)}(M_k) = 0$