Title: Sausages and Quantum Errors: when it's better not to see how they're made

Date: Jan 30, 2006 04:00 PM

URL: http://pirsa.org/06010021

Abstract: I will discuss the design of degenerate quantum error correcting codes for an arbitrary Pauli channel. At noise levels slightly beyond those for which a random stabilizer code does not allow high fidelity transmission with a nonzero rate, our codes usually have a rate which is strictly positive. In fact, there exist Pauli channels for which our codes outperform a random stabilizer code whenever the random coding rate is less than 0.04, which is a couple of orders of magnitude larger than the previous examples of this effect. I'll also present a fairly straightforward explanation of why these codes work and discuss how their performance scales with block size and what this scaling suggests even better codes will look like.

Sausages and Quantum Errors

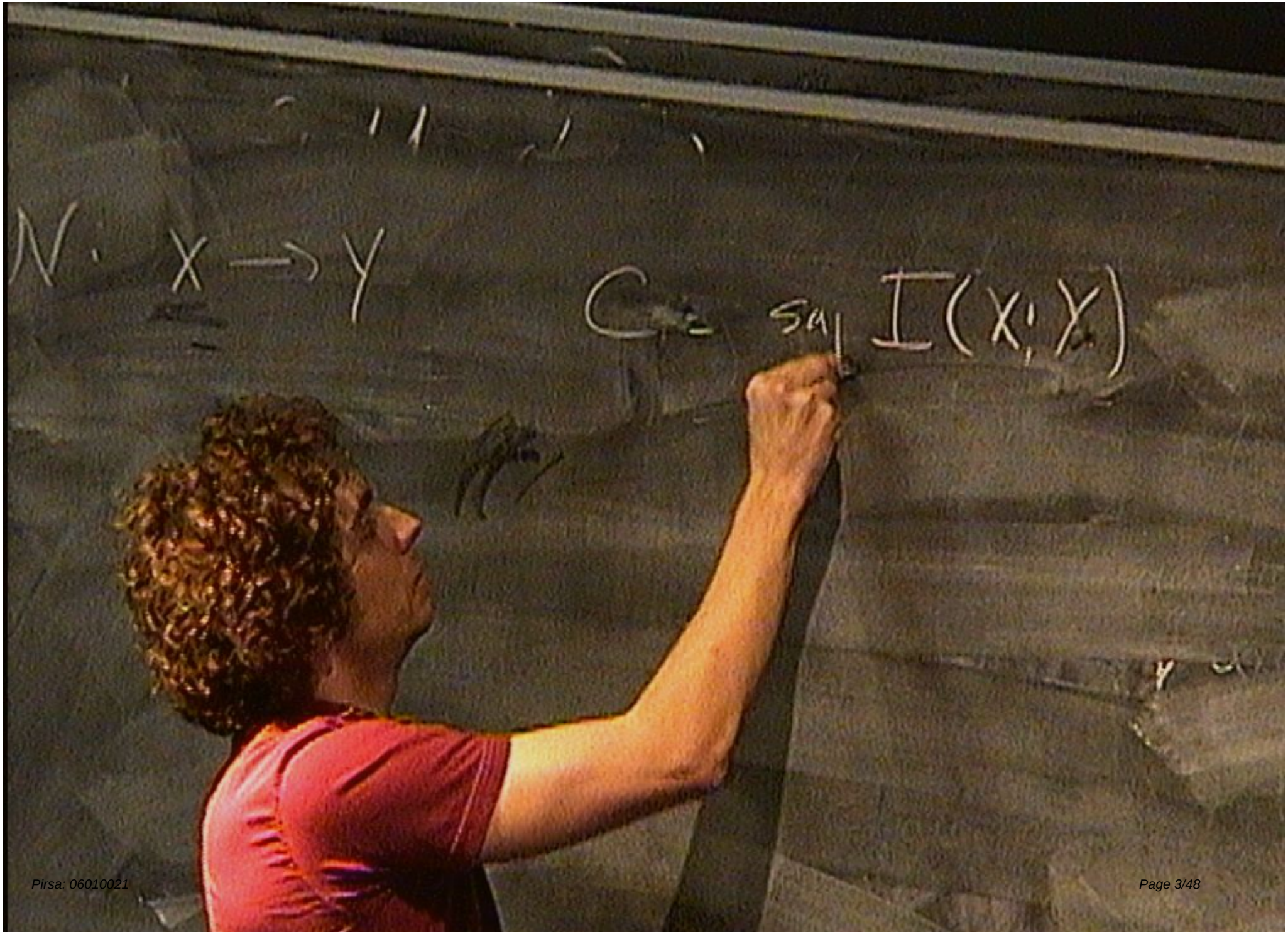
Graeme Smith

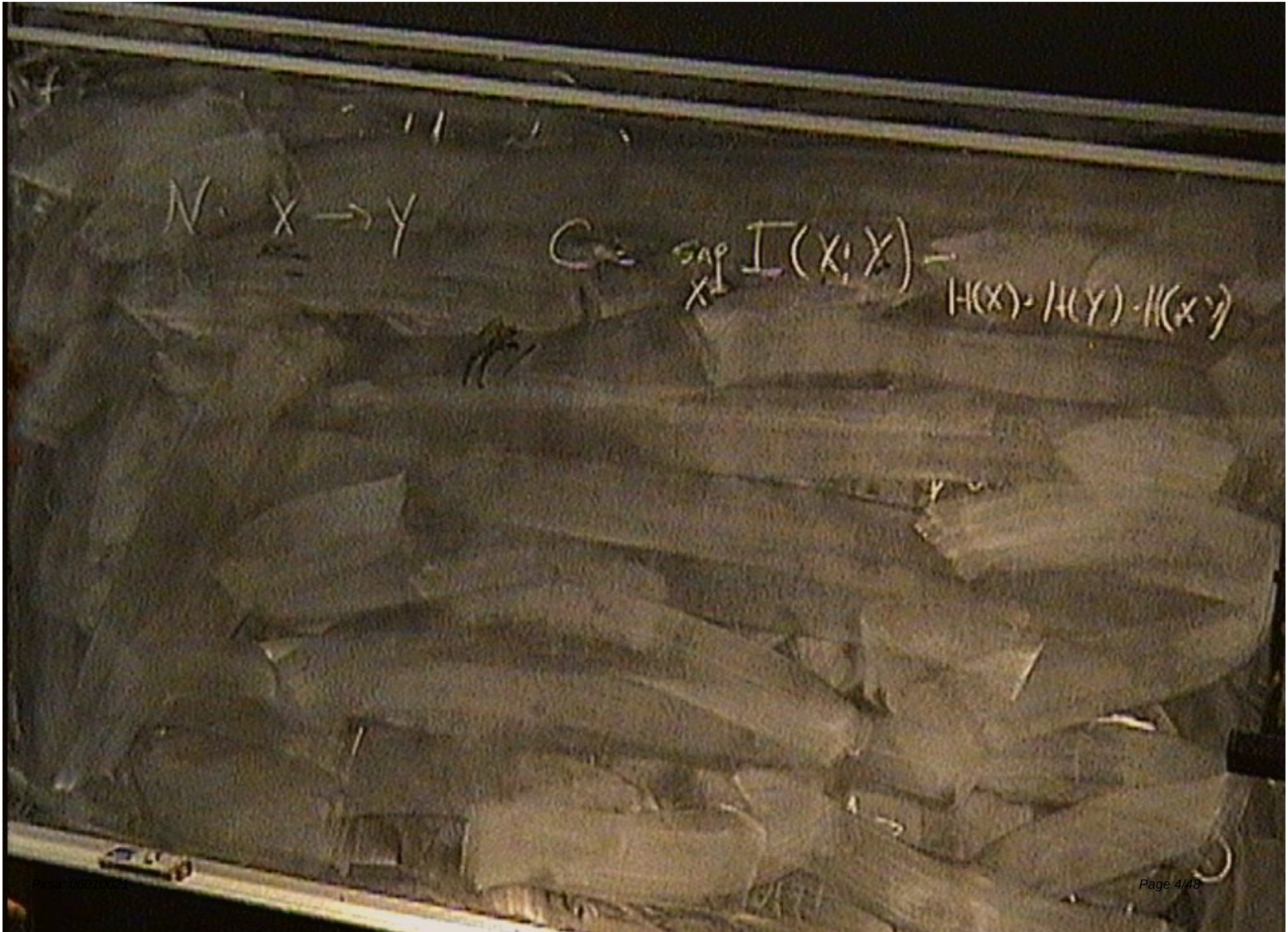
PI Seminar, Jan. 30 2006

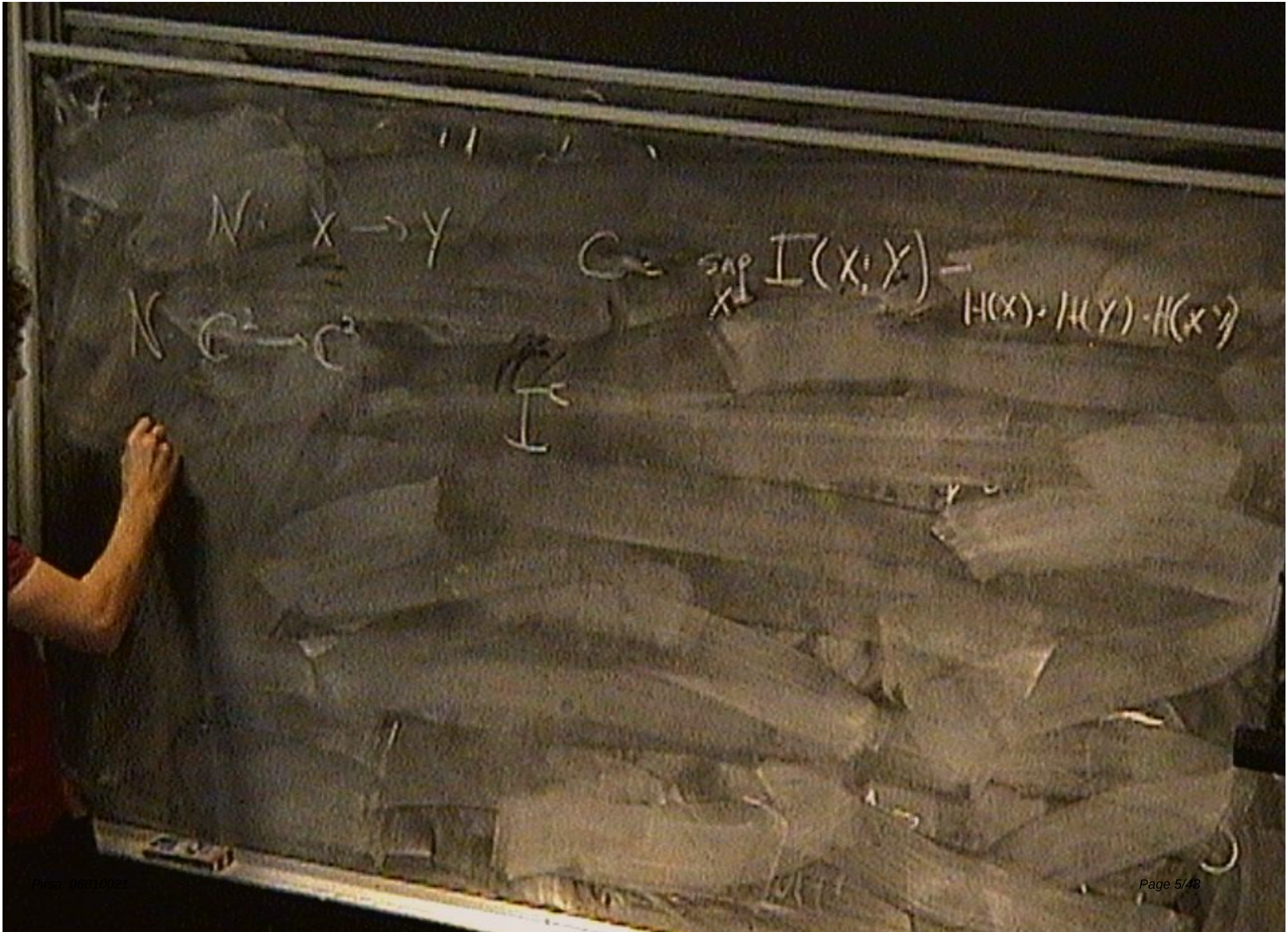
"Laws are like sausages, it is better not to see them being made."

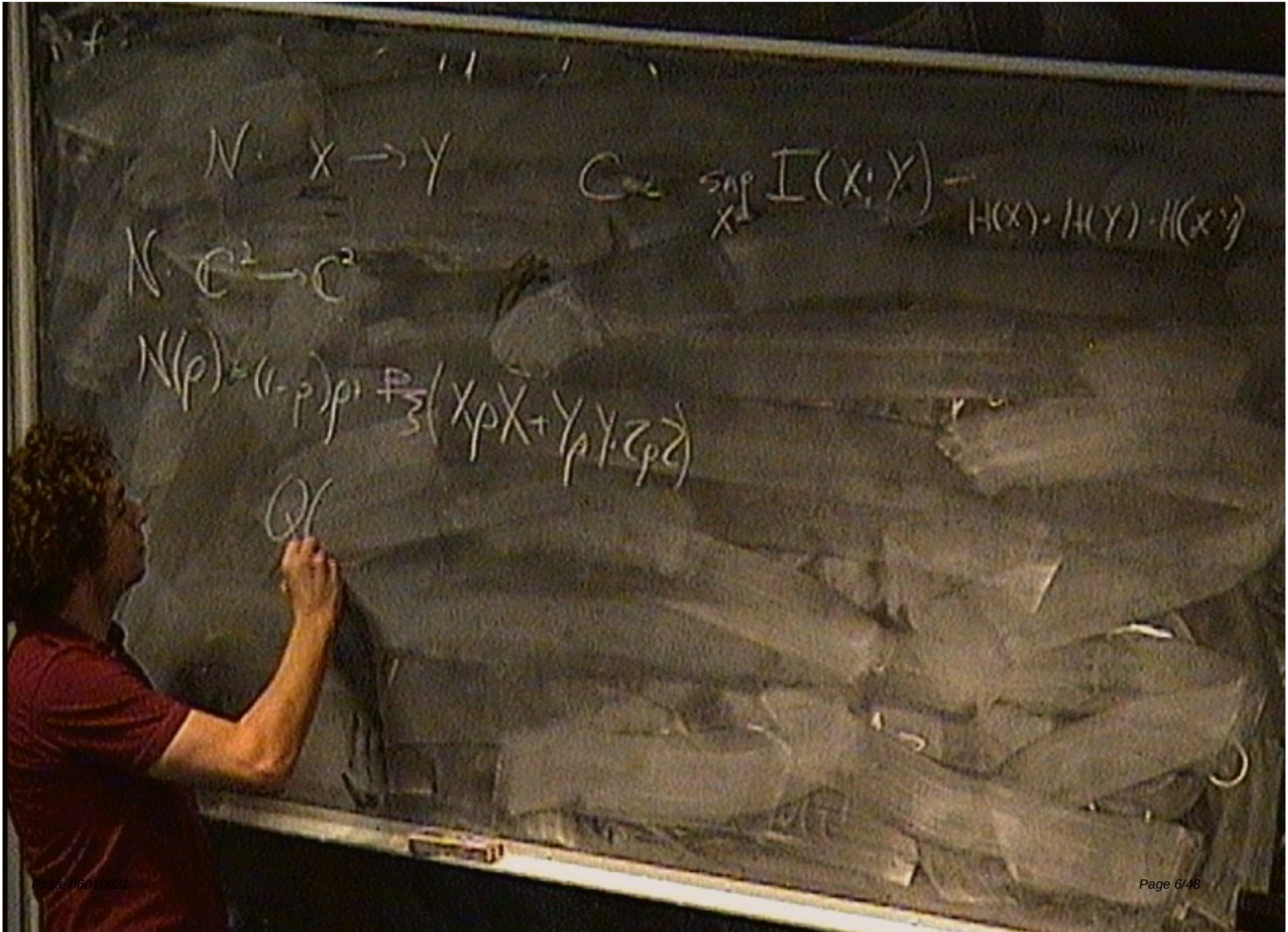
-Otto von Bismarck

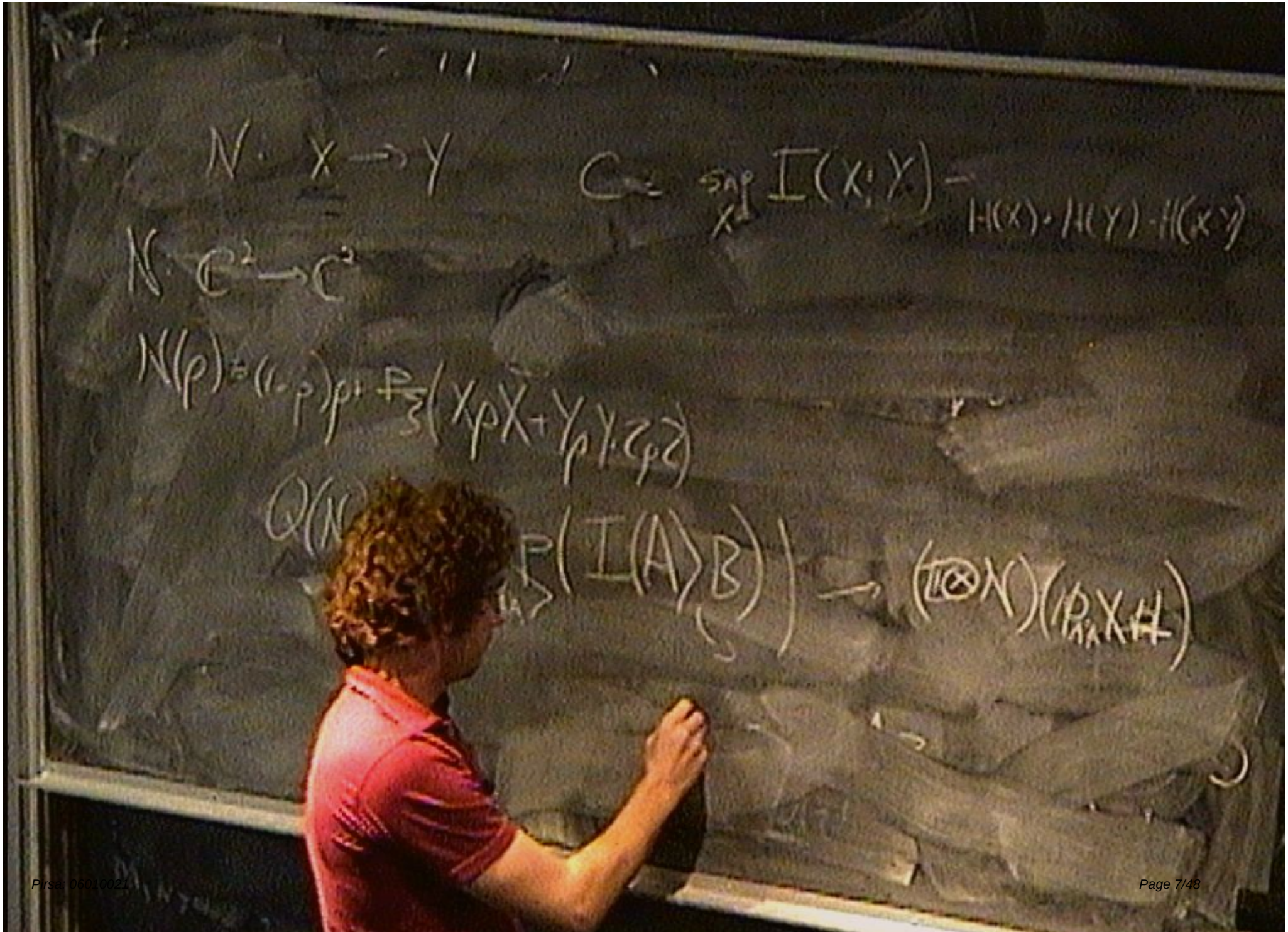
Joint work with John Smolin

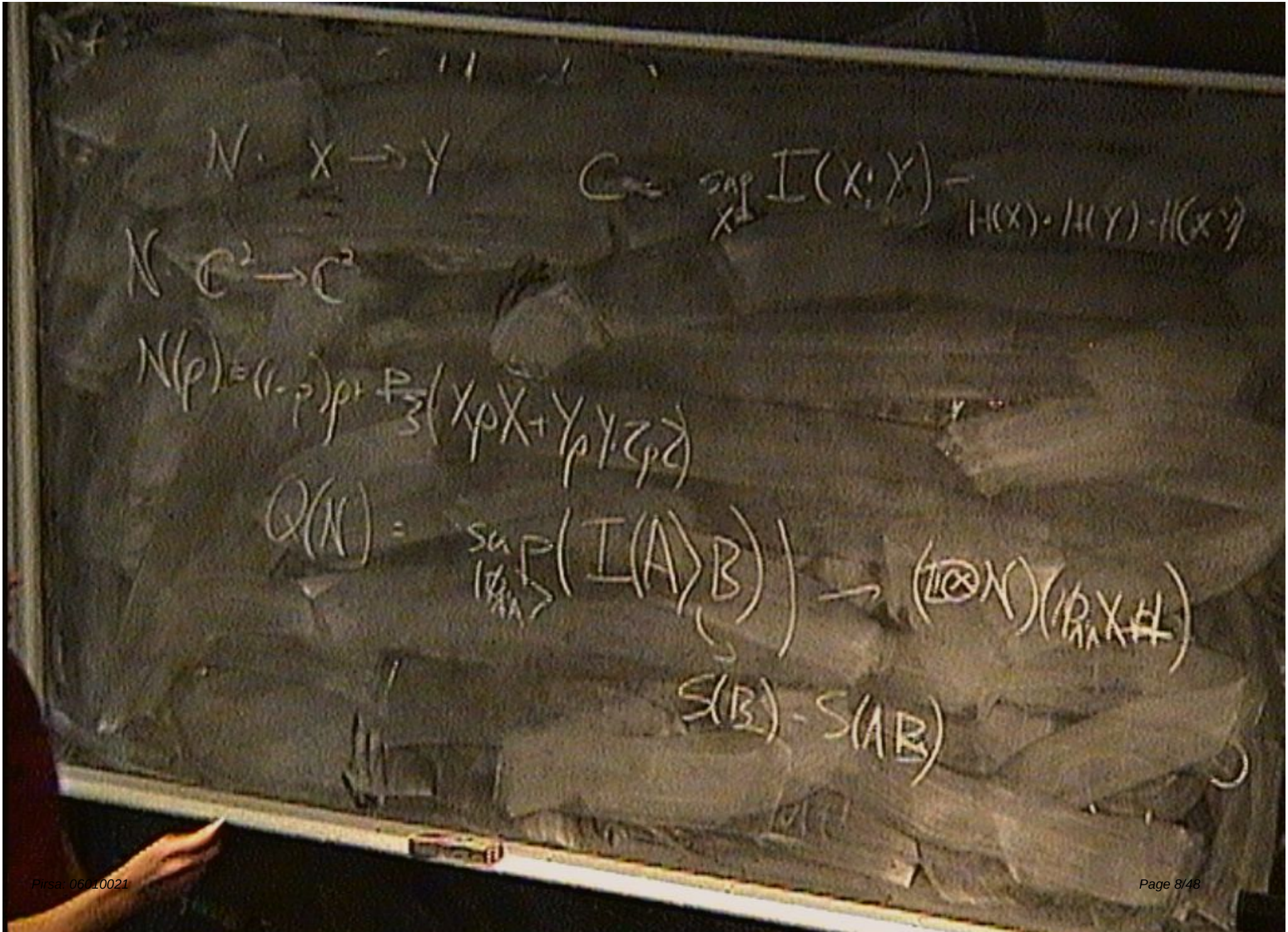

N · X → Y
C = sup I(X;Y)

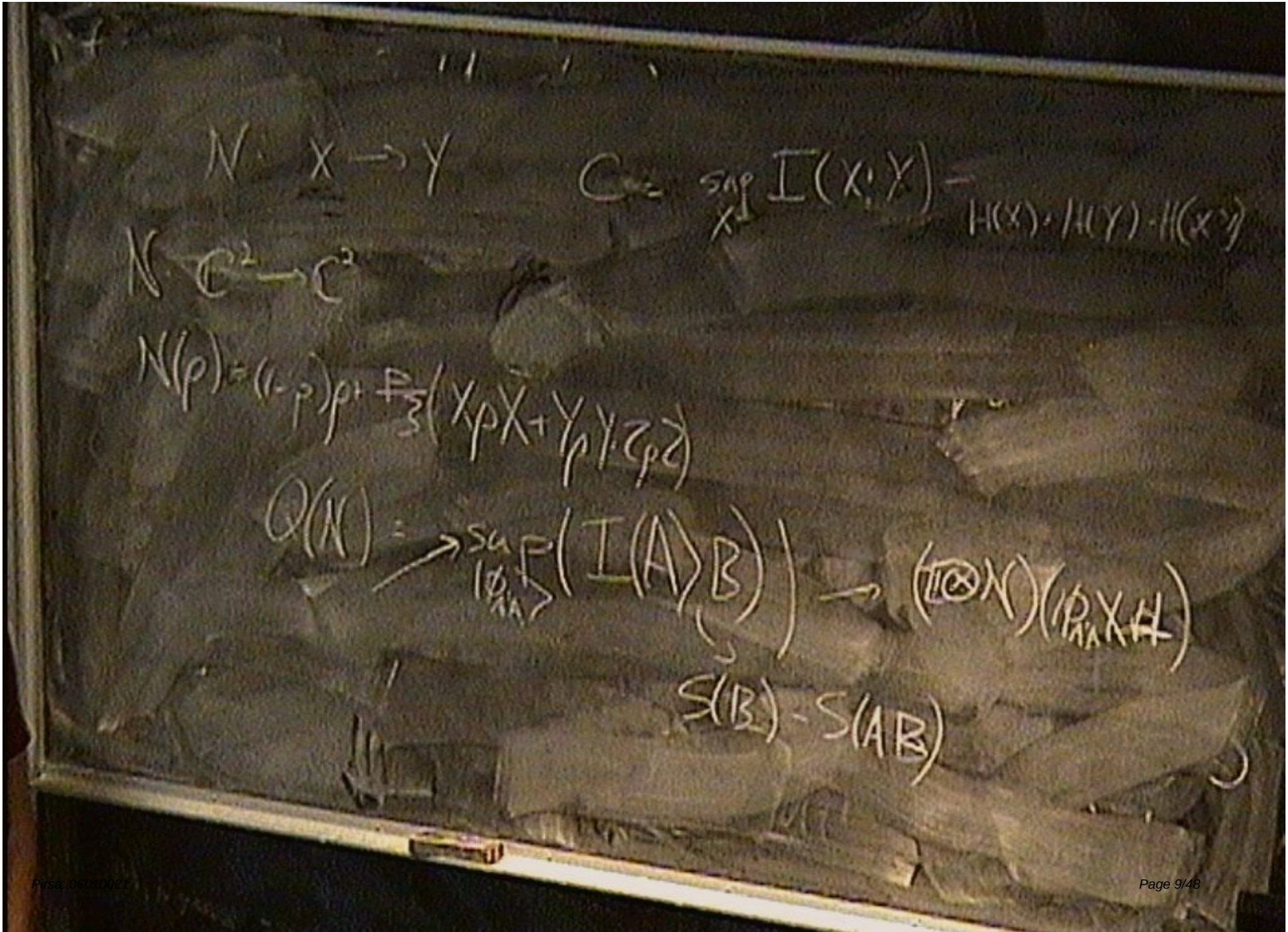

N: X → Y
C = sup I(X;Y) = H(X) + H(Y) - H(X,Y)

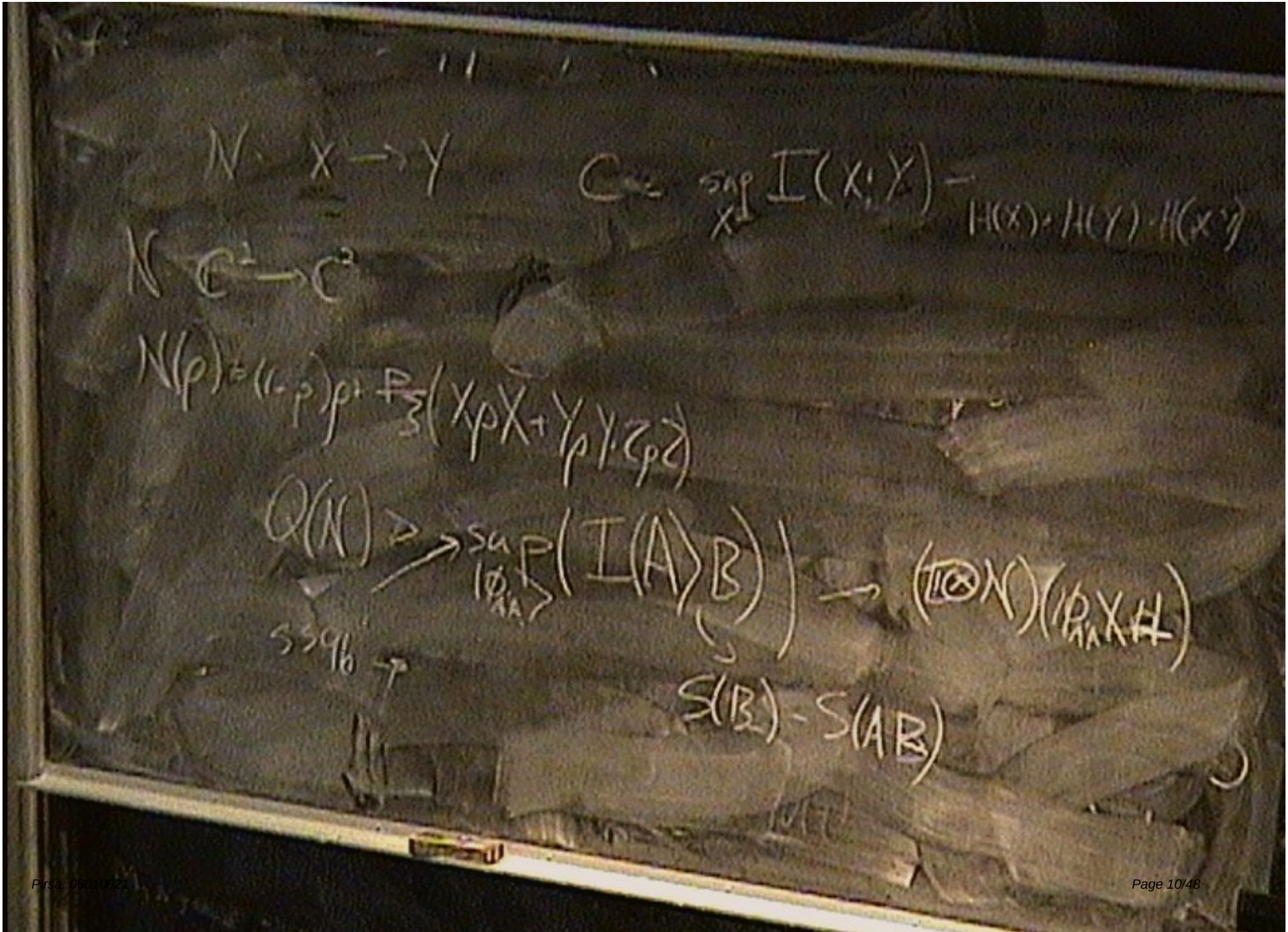

N: X → Y
C = sup I(X;Y) =
H(X) + H(Y) - H(X,Y)
N: C² → C²
I

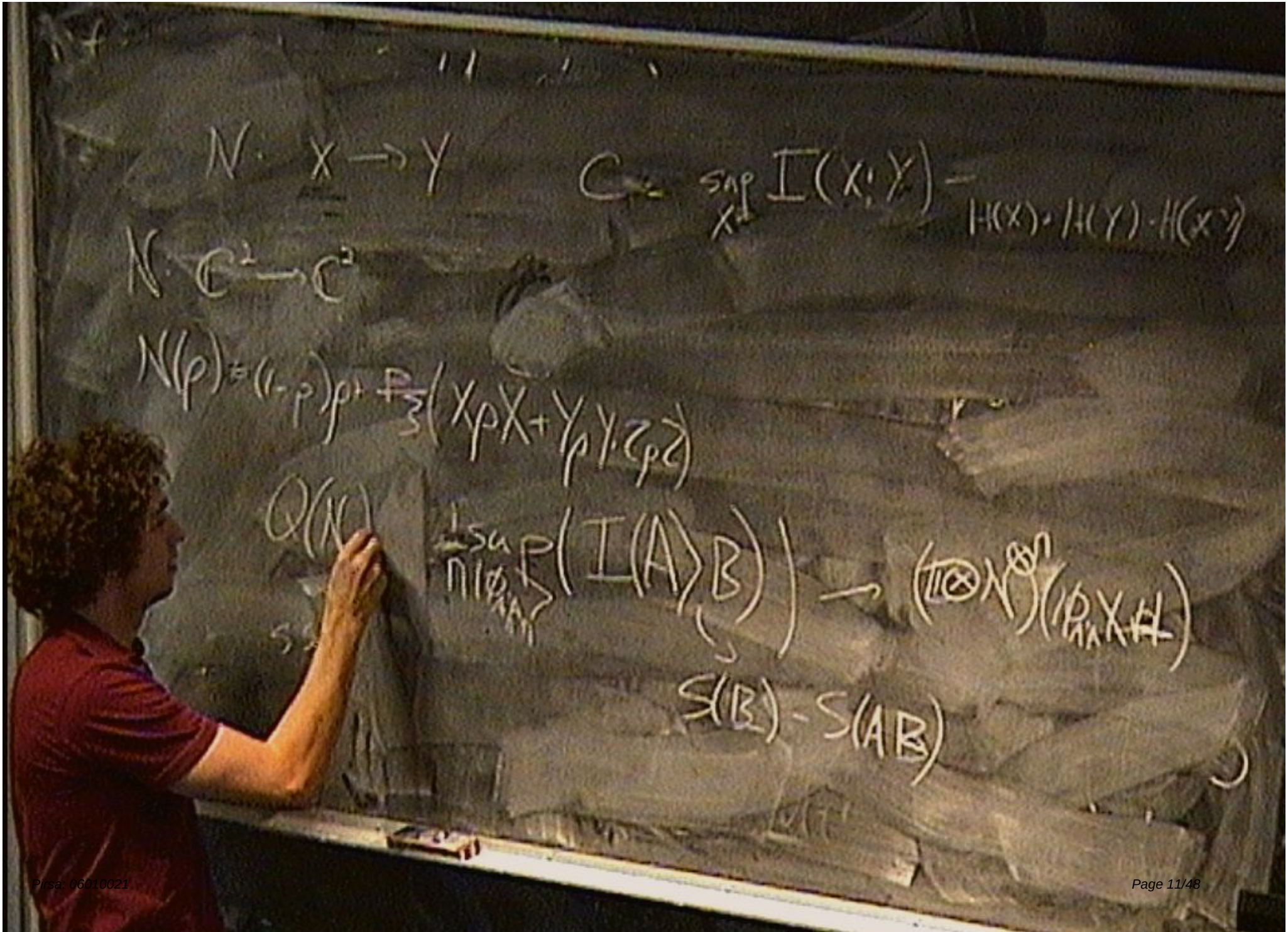

N : X → Y
C = sup I(X;Y) = H(X) + H(Y) − H(X,Y)
N : C² → C²
N(ρ) = (1 − p)ρ + p/3 (XρX + YρY + ZρZ)

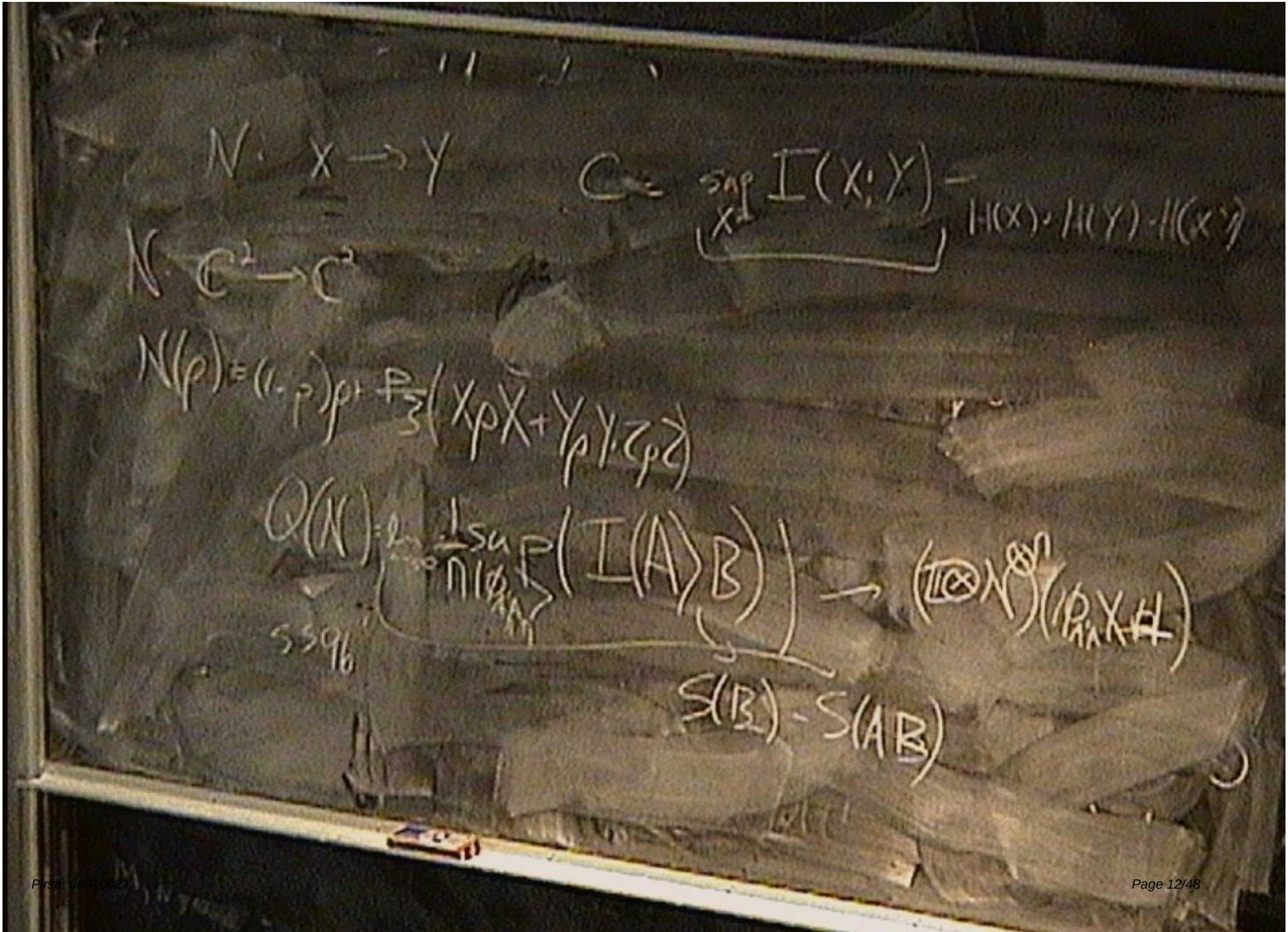

N : X → Y
C = sup_{X} I(X;Y) = H(X) + H(Y) − H(X,Y)
N : C² → C²
N(ρ) = (1 − p) ρ + p Tr(X ρ X + Y ρ Y + Z ρ Z)
Q(N) = lim_{n→∞} (1/n) sup I(A⟩B)
(I ⊗ N)(|Φ⟩⟨Φ|)

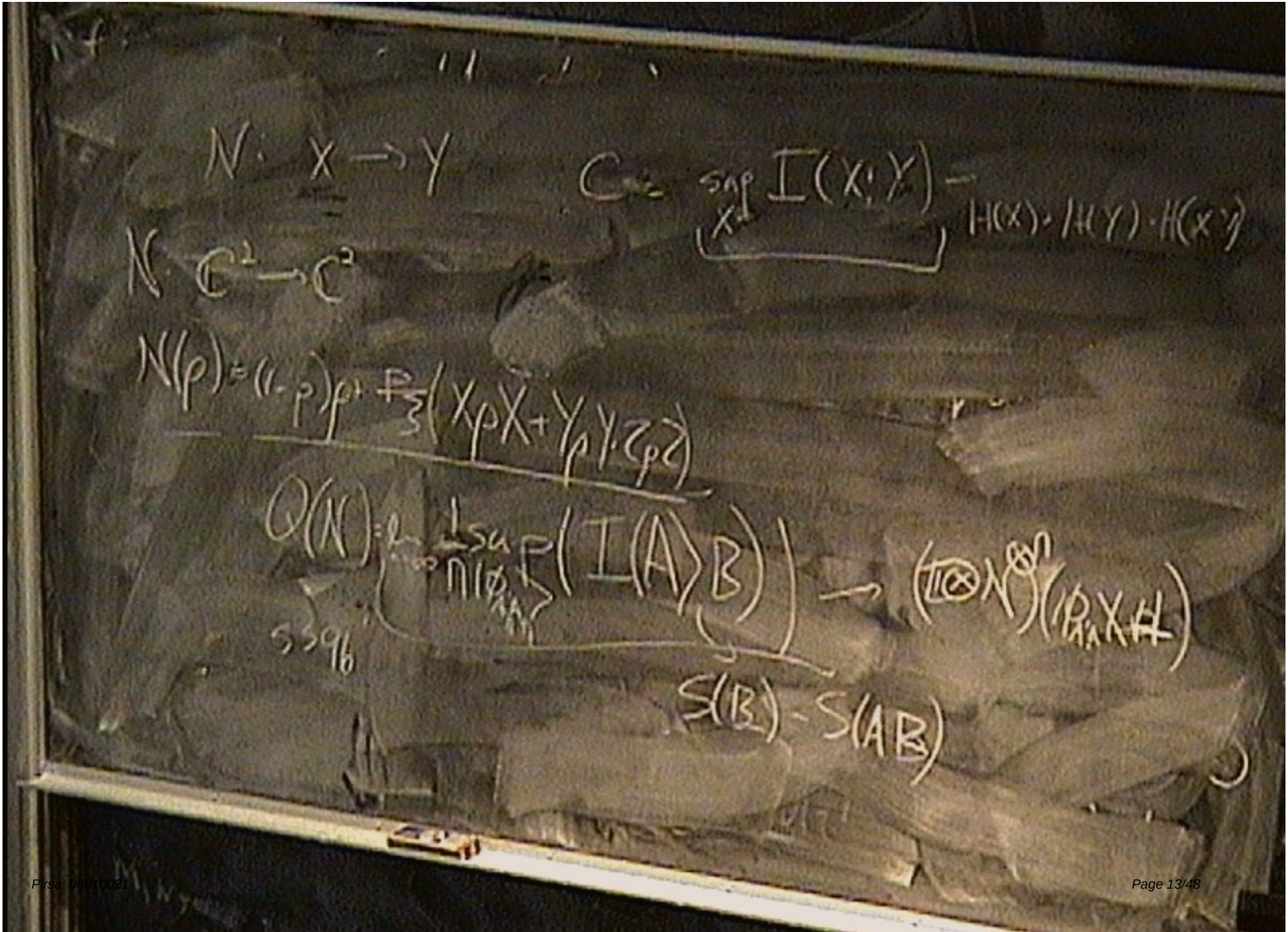

N : X → Y
C = sup_{X} I(X;Y) = H(X) + H(Y) − H(X,Y)
N : C² → C²
N(ρ) = (1 − p) ρ + p/3 (X ρ X + Y ρ Y + Z ρ Z)
Q(N) = sup_{|ψ_AA'⟩} I(A⟩B)_{(1⊗N)(|ψ_AA'⟩⟨ψ_AA'|)}
S(B) − S(AB)

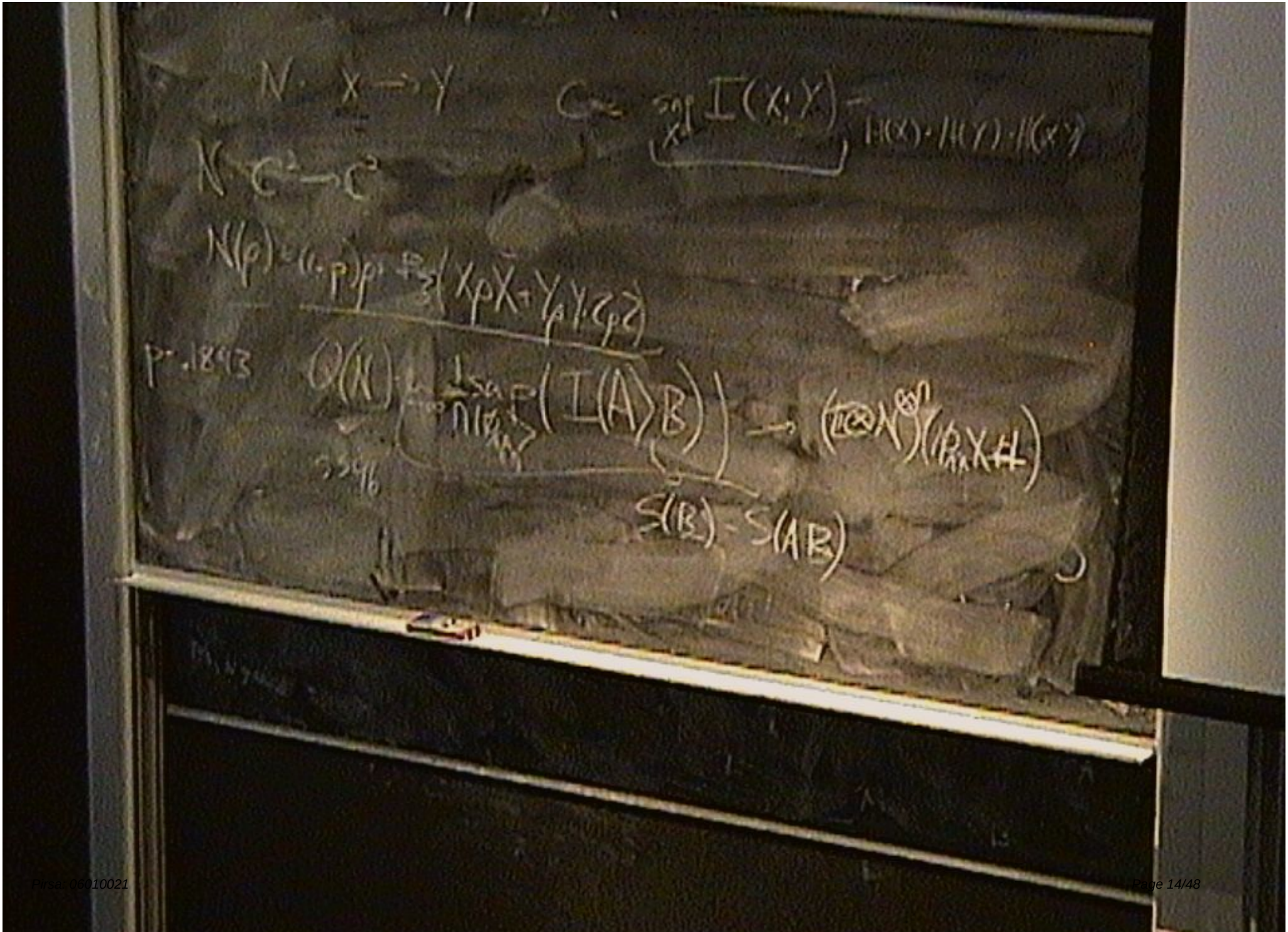

N: X → Y
C = sup_X I(X:Y) = H(X) + H(Y) − H(X,Y)
N: C² → C²
N(ρ) = (1 − p)ρ + p/3 (X ρ X + Y ρ Y + Z ρ Z)
Q(N) = sup_{|Φ_AA⟩} I(A⟩B)
(I ⊗ N)(|Φ_AA⟩⟨Φ_AA|)
S(B) − S(AB)

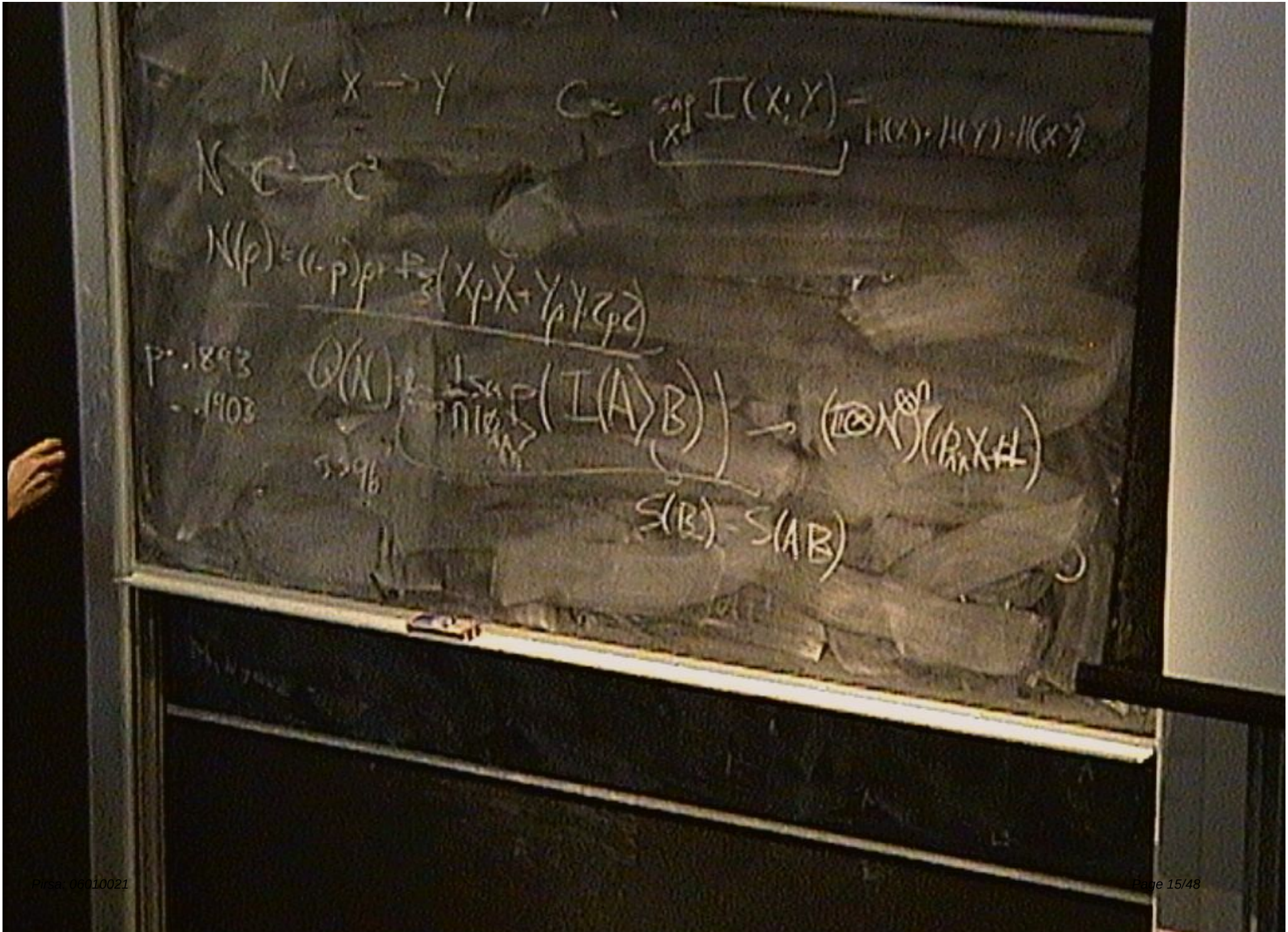

N : X → Y
C = sup_X I(X;Y) − H(X) + H(Y) − H(X,Y)
N : C¹ → C²
N(ρ) = (1 − p)ρ + p Tr(X ρ X† + Y ρ Y† + Z ρ Z†)
Q(N) = sup_{|Φ_AA'⟩} I(A⟩B)
S(B) − S(AB)


N : X → Y
C = sup_{X} I(X;Y) = H(X) + H(Y) − H(X,Y)
N : C² → C²
N(ρ) = (1 − p)ρ + p/3 (XρX + YρY + ZρZ)
Q(N) = lim_{n→∞} sup_{ρ} (1/n) I(A⟩B)
S(B) − S(AB)


N : X → Y
C = sup I(X;Y) − H(X) − H(Y) − H(X')
N : C² → C²
N(ρ) = (1 − p)ρ + p/3 (X_ρ X + Y_ρ Y + Z_ρ Z)
Q(N) = lim 1/n sup I(A;B)
S(B) − S(AB)


$N: X \to Y$
$C = \sup_{X} I(X;Y) - H(X) \cdot H(Y) \cdot H(X)$
$N: \mathbb{C}^2 \to \mathbb{C}^2$
$N(\rho) = (1-p)\rho + p_3(X\rho X + Y\rho Y + Z\rho Z)$
$Q(N) = \lim \frac{1}{n} \sup_{n(\phi_{AA'})} S(I(A)B)) \to (\Pi \otimes N^{\otimes n})(\rho_{AA'} \times \mathbb{H})$
$S(B) - S(AB)$


N : X → Y
C = sup I(X;Y)
H(X) · H(Y) · H(X,Y)
N : C² → C²
N(ρ) = (1 − p)ρ + p/3 (X_ρ X + Y_ρ Y + C_ρ Z)
Pr 1893
O(N)
S(B) − S(AB)


N : X → Y
C = sup I(X;Y)
N : C² → C²
N(ρ) = (1 − p) ρ + p/3 (X_ρ X + Y_ρ Y + Z_ρ Z)
1893
1903
Q(N) = lim 1/n I_coh(ρ, N^⊗n)
S(B) S(AB)

The Deal

We the undersigned agree that in exchange for the optimality of randomly chosen objects, we will forego any chance of actually constructing specific examples of optimal objects.

Name	Date
Paul Erdős	02/07/1934
Charles Edward Sherman	04/08/1943
Nina Adams	11/20/1972
Joel Spencer	10/30/1976
⋮	

Outline

- Random Stabilizer Codes
- Repetition Codes for Pauli Channels
  "Big" deviations from hashing
- "Almost" bitflip channels require long codes.
- Conditional Channels: application to depolarizing ch
- A (new) channel whose capacity we can ~~calculate.~~ conjecture

Stabilizer Codes

P_n - Pauli Group $\{I, X, Y, Z\}^n$

S - abelian subgroup of P_n, $|S| = 2^{n-k}$

$C = \{|\psi\rangle \mid s|\psi\rangle = |\psi\rangle \ \forall s \in S\}$

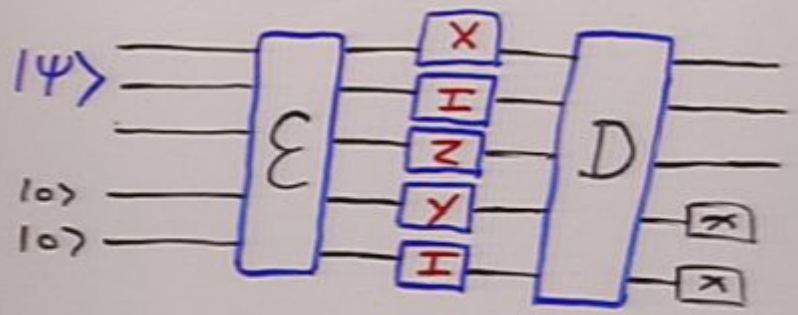
$\dim(C) = 2^k$

error $E \in P_n$ has syndrome $\omega(E, S_i)$

where $S_i E = (-1)^{\omega(E,S_i)} E S_i$

and $\{S_i\}_{i=1}^{n-k}$ generate S.

Stabilizer Codes



encoding operation $\mathcal{E}$
decoding operation D
error $XIZYI$

Random Stabilizer Codes

Depolarizing Channel: $\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$

$$\mathcal{N}^{\otimes n} \Rightarrow \quad \mathcal{E}_{typ} = \left\{ E \in P_n \;\middle|\; \#X, \#Y, \#Z \sim \tfrac{p}{3} n \right\}$$

# of Typical Errors: $|\mathcal{E}_{typ}| \sim 2^{n H(1-p, \frac{p}{3}, \frac{p}{3}, \frac{p}{3})}$
$= 2^{n(H(p) + p \log_2 3)}$

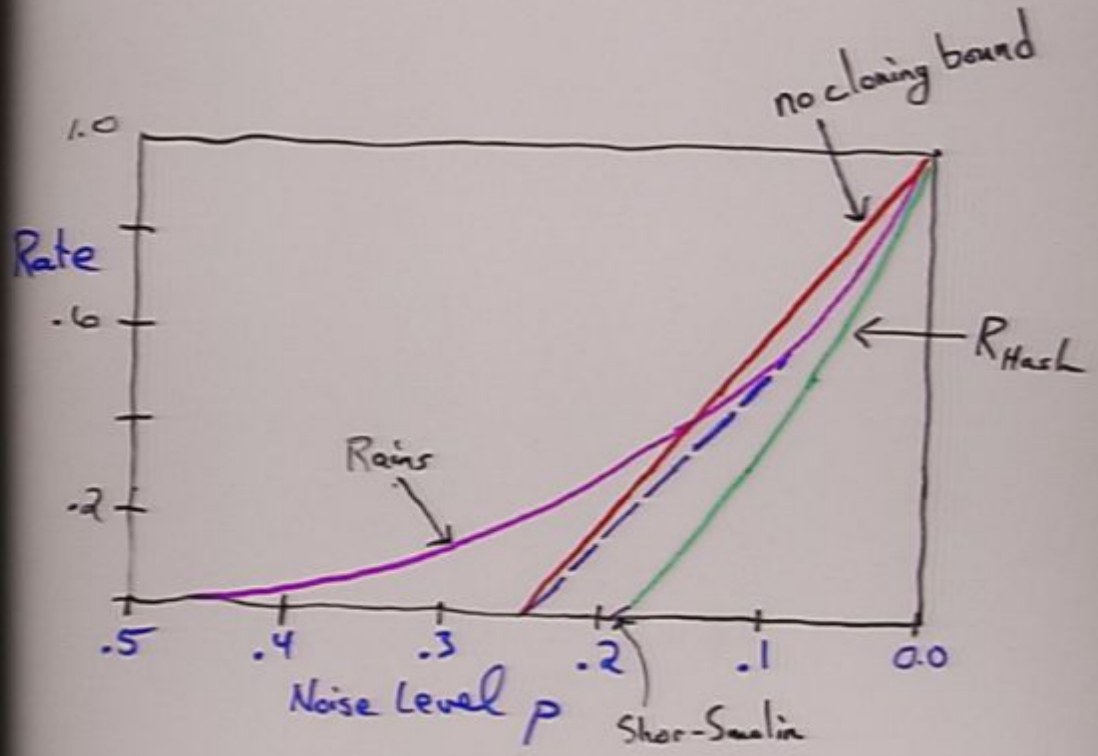
Random $S_1 \in P_n$ commutes with $\sim \frac{1}{2}$ of $\mathcal{E}_{typ}$
anticommutes with $\sim \frac{1}{2}$ of $\mathcal{E}_{typ}$

In fact, each generator in $\{S_1, \ldots, S_{n-k}\}$ will give ~ 1 bit of information about the error.

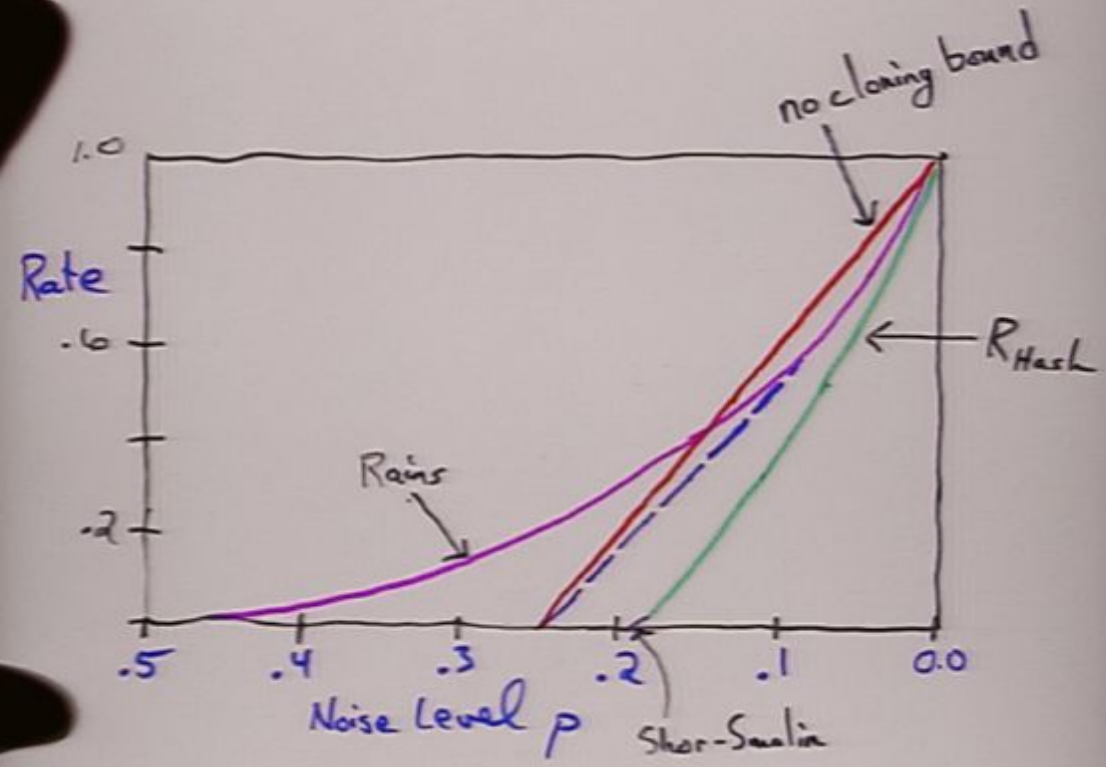
$\Rightarrow$ letting $\frac{k}{n} < \boxed{R_{Hash} = 1 - H(p) - p \log_2 3}$

we get high fidelity w.h.p.

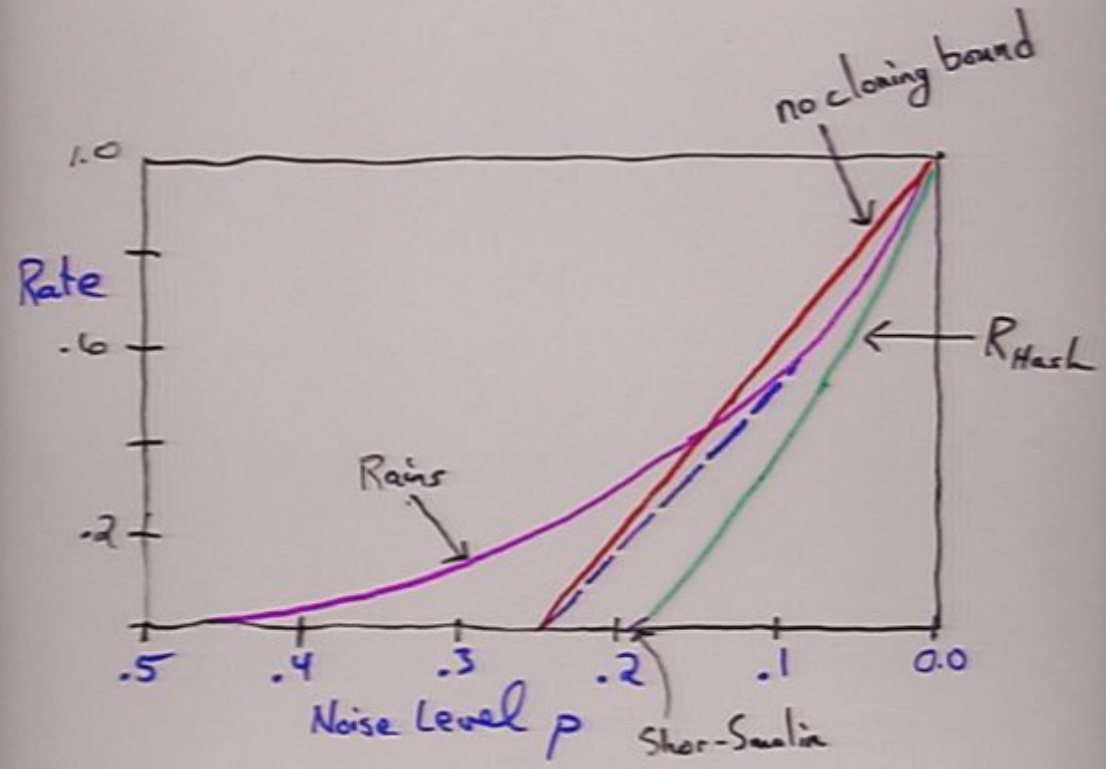
Bounds on the Capacity of Depolarizing Channel



Bounds on the Capacity of Depolarizing Channe



Bounds on the Capacity of Depolarizing Channel



Pauli Channels:

$$\mathcal{N}(\rho) = (1-p)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

$p = p_x + p_y + p_z$

Hashing Rate: $1 - H(1-p, p_x, p_y, p_z)$

Can we do better?

Repetition Codes

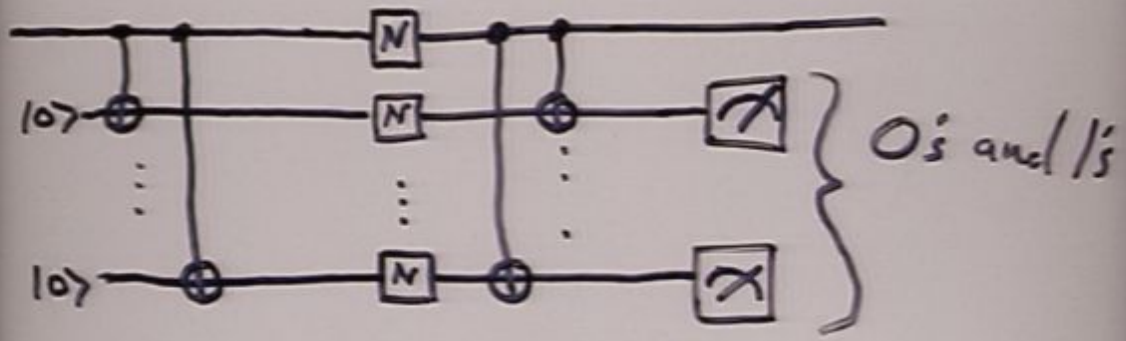
note: Throughout, we take $p_x \geq p_z \geq p_y$

m-qubit rep. - $|\bar{0}\rangle = |0\rangle^{\otimes m}$ $|\bar{1}\rangle = |1\rangle^{\otimes m}$

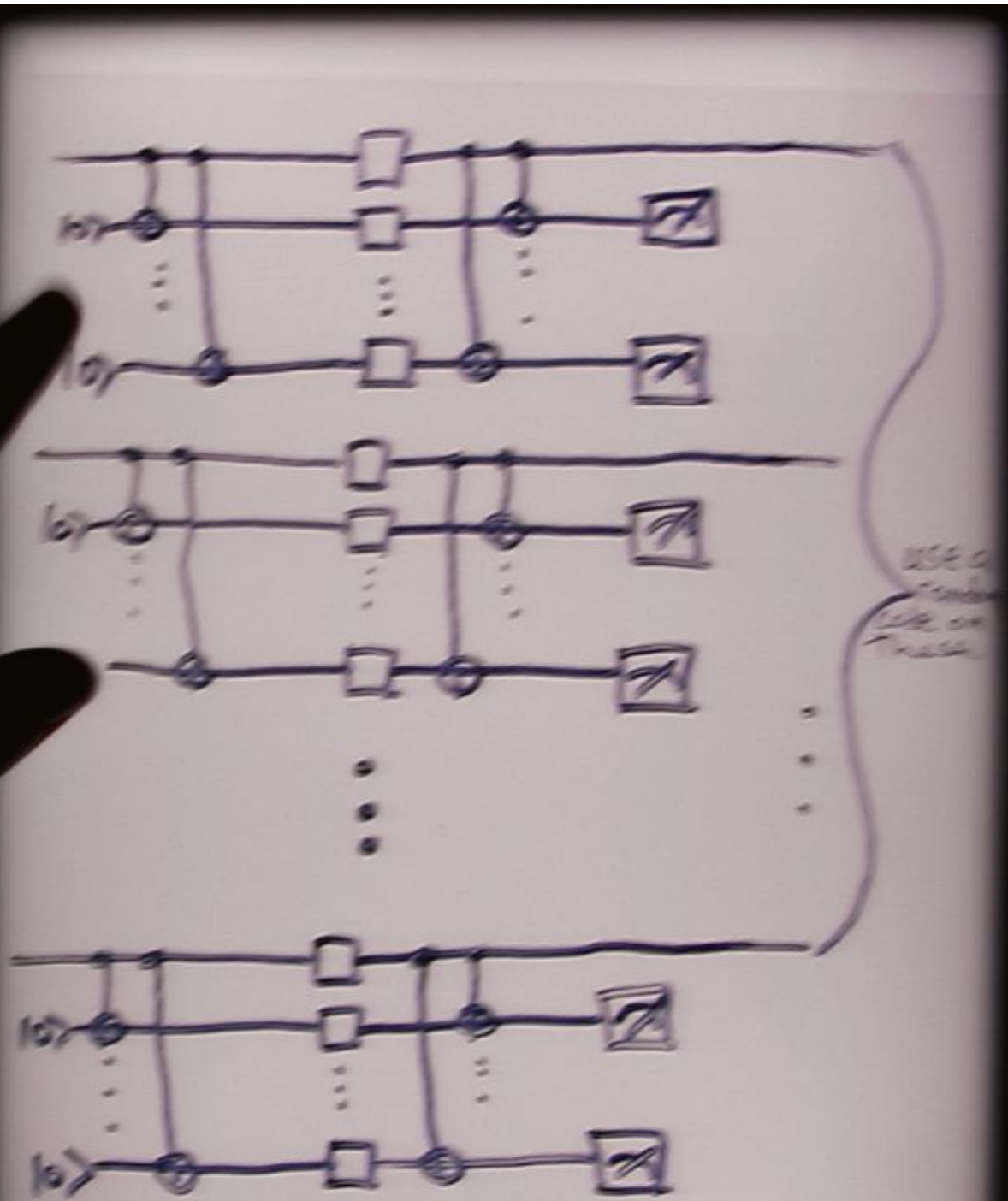
$S = \langle Z_1 Z_2, Z_1 Z_3, \ldots, Z_1 Z_m \rangle$

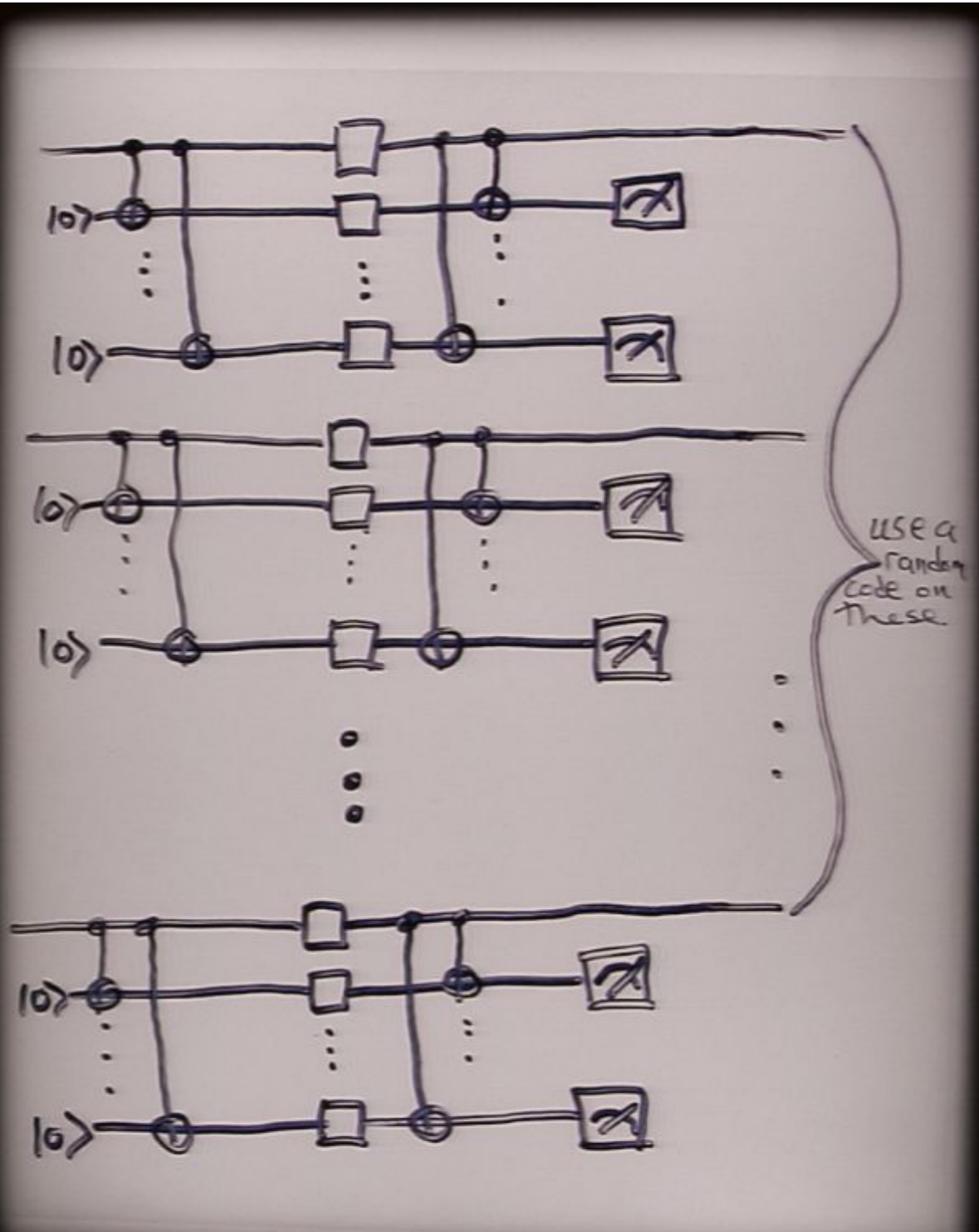
$\bar{X} = X^{\otimes m}$ $\bar{Z} = Z_1$

Encoding/Decoding:



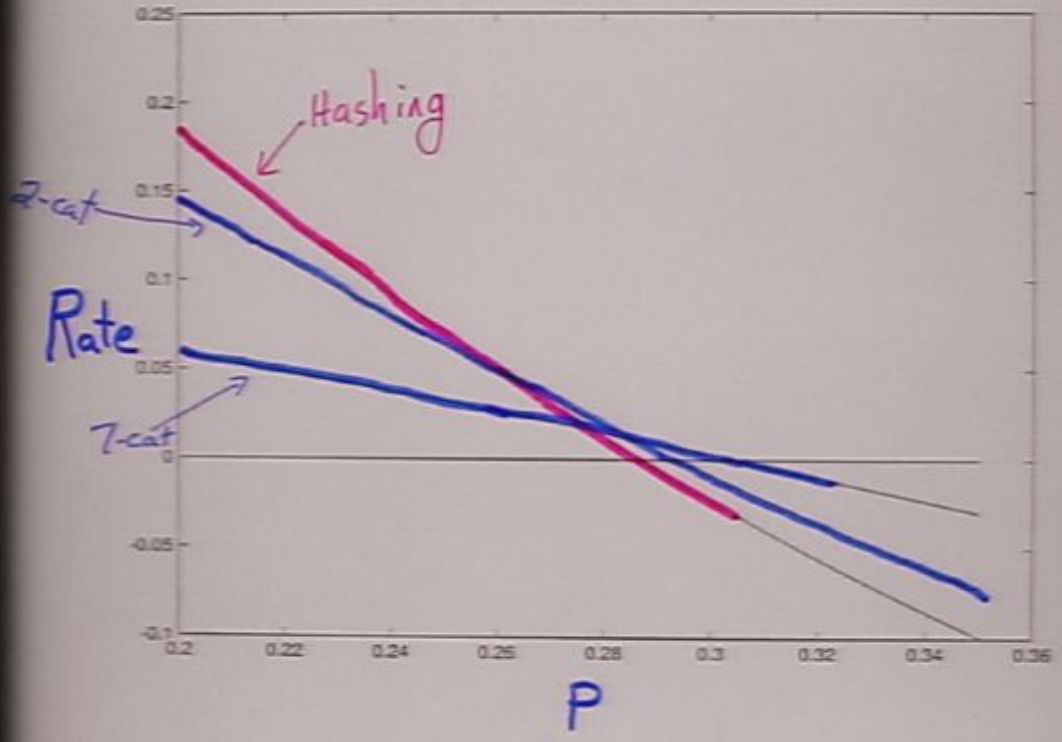
- degenerate — all Z_i same
- distance 1
- but, high "X-distance"


|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|0⟩


|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
|0⟩
use a random code on these

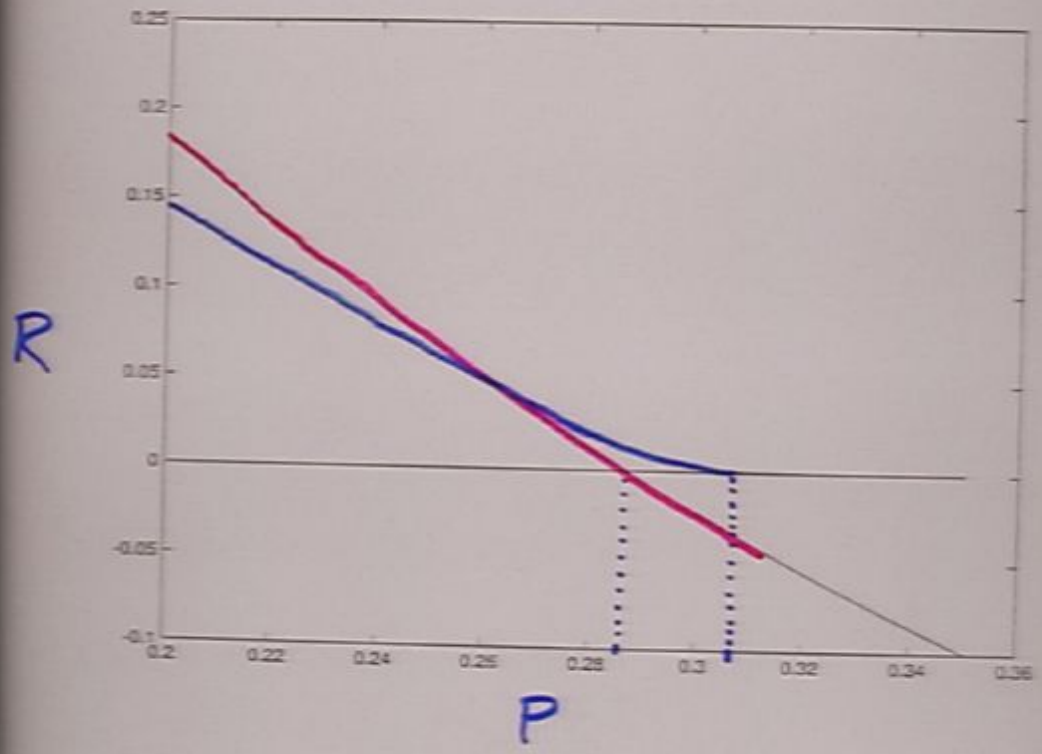
Cat Code Rates

$(p_x, p_y, p_z) = (.92p, .024p, .056p)$



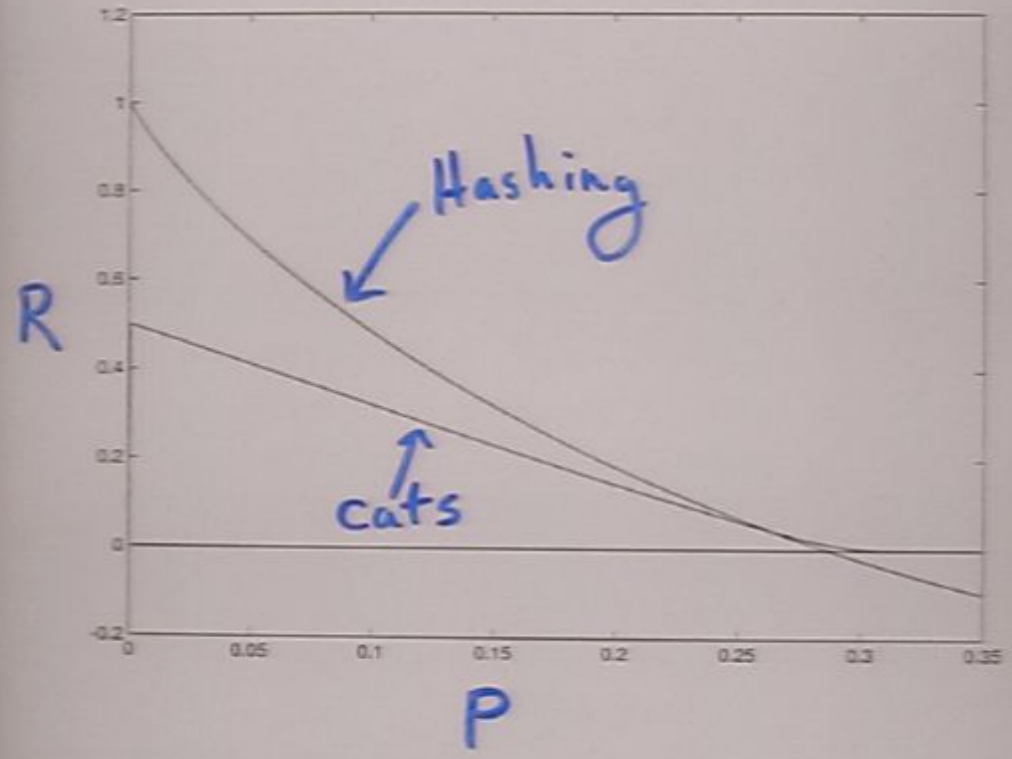
$$N(\rho) = (1-p_x-p_y-p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

BestCat Code Rates



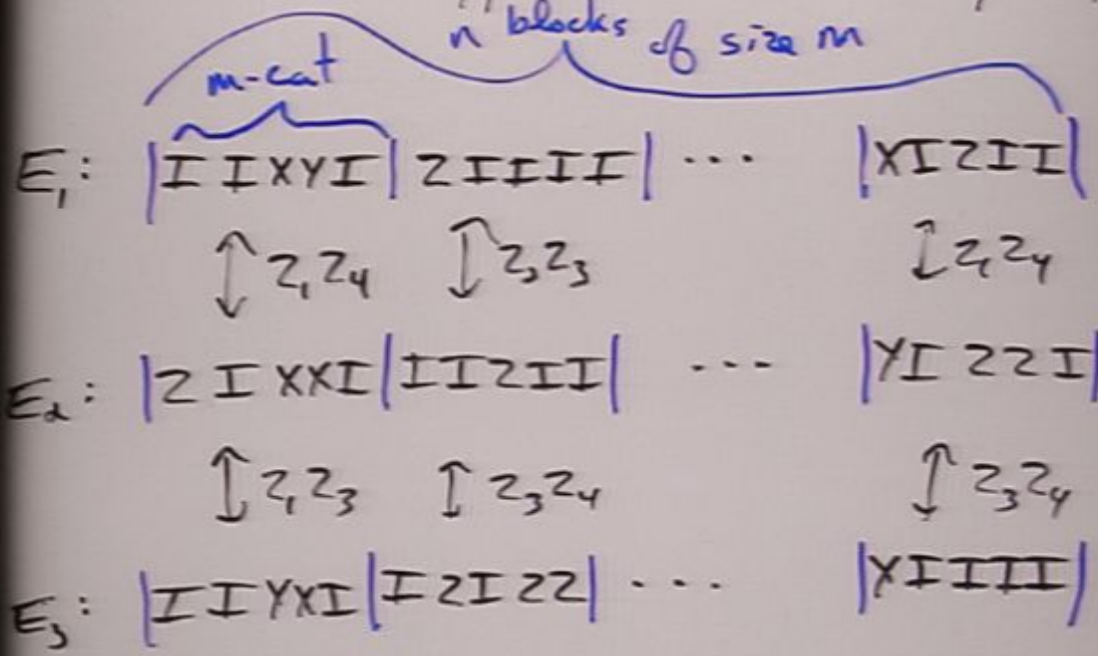
$$N(p) = (1 - p_x - p_y - p_z)p + p_x X_p X + p_y Y_p Y + p_z Z_p Z$$

$$(p_x, p_y, p_z) = (.92p, .024p, .056p)$$


1.2
1
0.8
0.6
0.4
0.2
0
-0.2
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
Hashing
cats
R
P

Where's the Degeneracy?

Consider some typical errors (#X's $\approx p_x nm$)



all of these have the same synd.

In fact there will be exponentially many typical errors with the same action on the codespace that have the same syndrome.

(Almost) (Bitflip Channels)

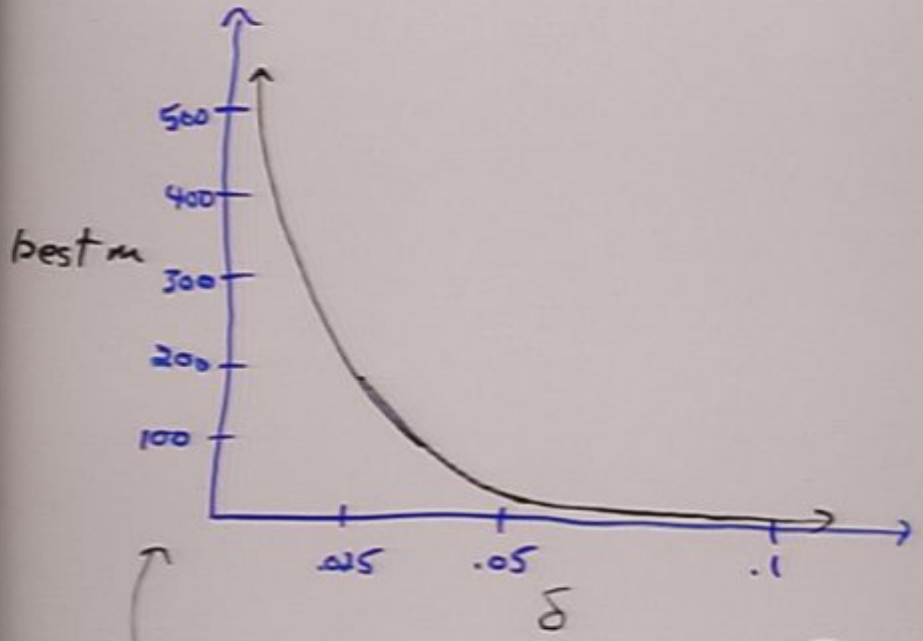
$p_x \gg p_z = \delta p_x$, p_y st. amp & phase errors indep.

Note: $\delta = 0$ => Bitflip channel
(Hashing is optimal)

Q: How does optimal m scale with δ?

How does size of effect scale?
(better $\to 0$ as $\delta \to 0$)

(Almost) (Bit flip Channel)



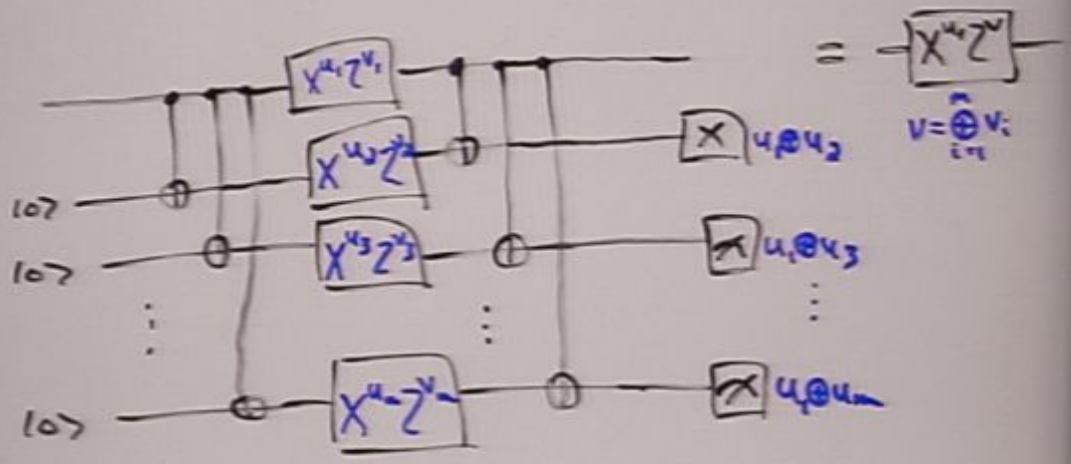
$p_z = \delta p_x$

optimal repetition length scales like $m \sim \frac{1}{\delta}$ for $\delta \ll 1$.

Why?

(Almost) (Bitflip Channel)

Idea: Want to figure out X errors without screwing up Z's too much.



Note: $H(\bigoplus_{i=1}^{m} v_i)$ increases with m, around $m \sim 1/p_2$ $H(\oplus v_i) < 1$, but much bigger and $H(\bigoplus v_i) \approx 1$

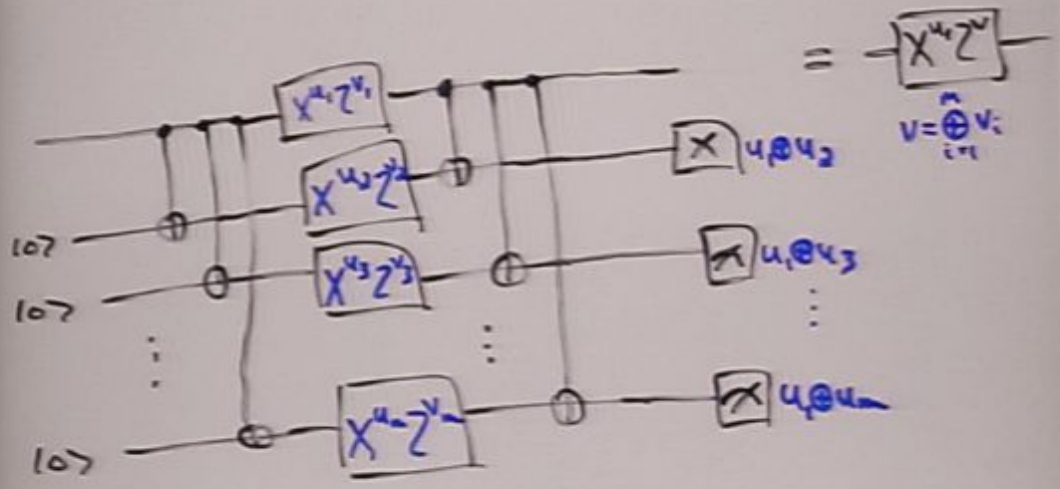
bigger m => learn more about u_i, but make v noisier.

for $m \sim \frac{1}{p_2}$, quite sure about u_i, v not so bad...

for Γ at hashing pt

(Almost) (Bitflip Channel)

Idea: Want to figure out X errors without screwing up Z's too much.



Note: $H(\bigoplus_{i=1}^{n} v_i)$ increases with n, around $n \sim 1/p_Z$ $H(\oplus v_i) < 1$, but much bigger and $H(\bigoplus v_i) \approx 1$

bigger n => learn more about u_1, but make v noisier.

for $n \sim \frac{1}{p_Z}$, quite sure about u_1, v not so bad...

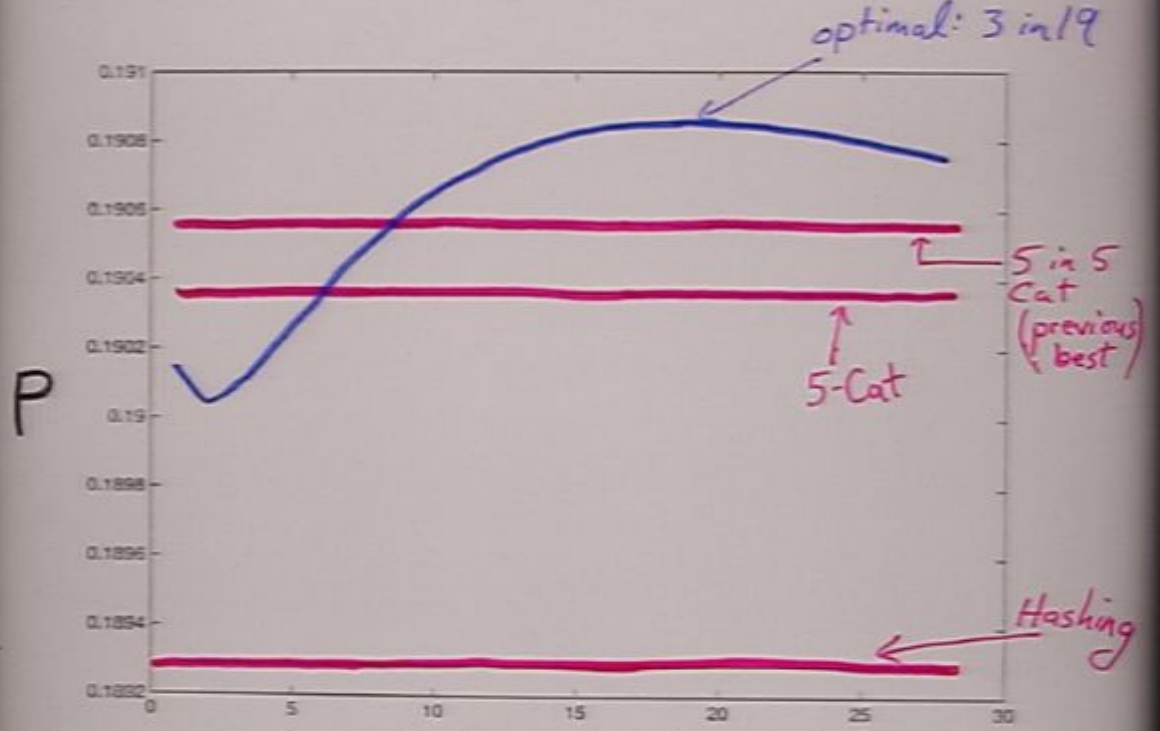
Conditional Channels + Concatenated Inner Codes.

Recall: When we use optimal Z code, we start with $p_x > p_z$, and end up with $p_z > p_x$ (exact values depend on syndrome)

The resulting channel(s) is perfect for an X-repetition code.

$$m \sim \frac{1}{p_x}$$

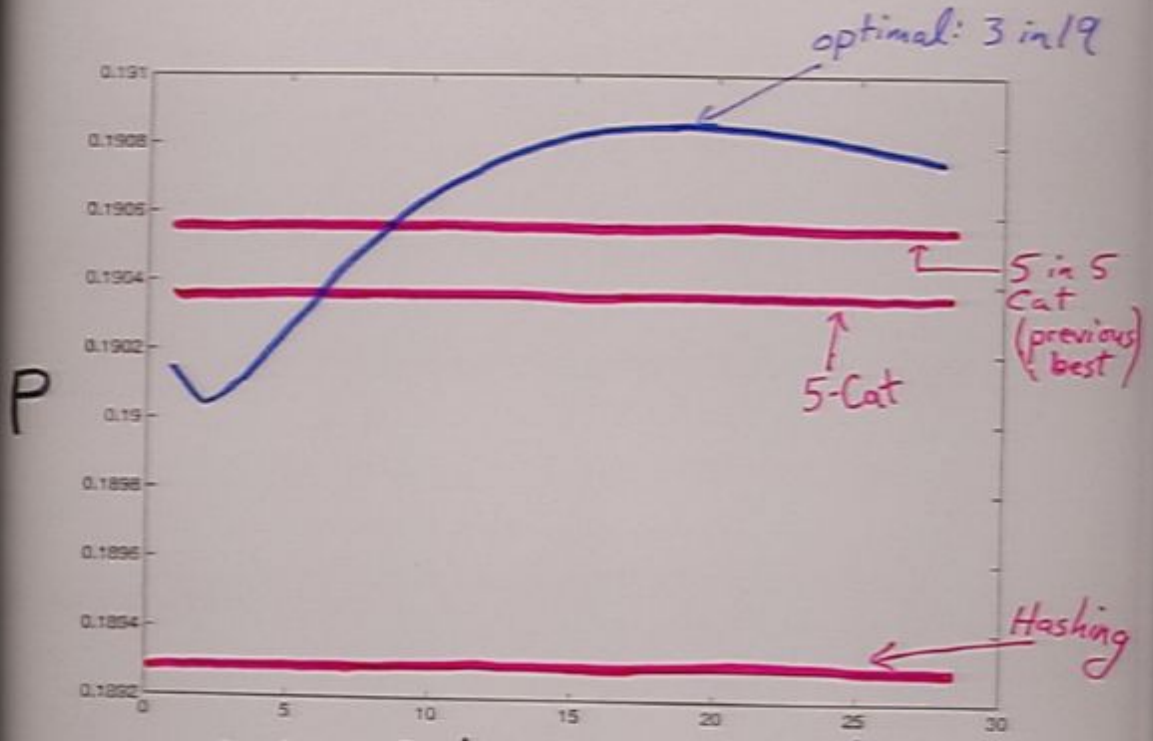
Zero Rate Curves
Inner Code Length m=3



Depolarizing Channel:

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z$$

Zero Rate Curves
Inner Code Length m=3



Depolarizing Channel:

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z$$

A special Channel

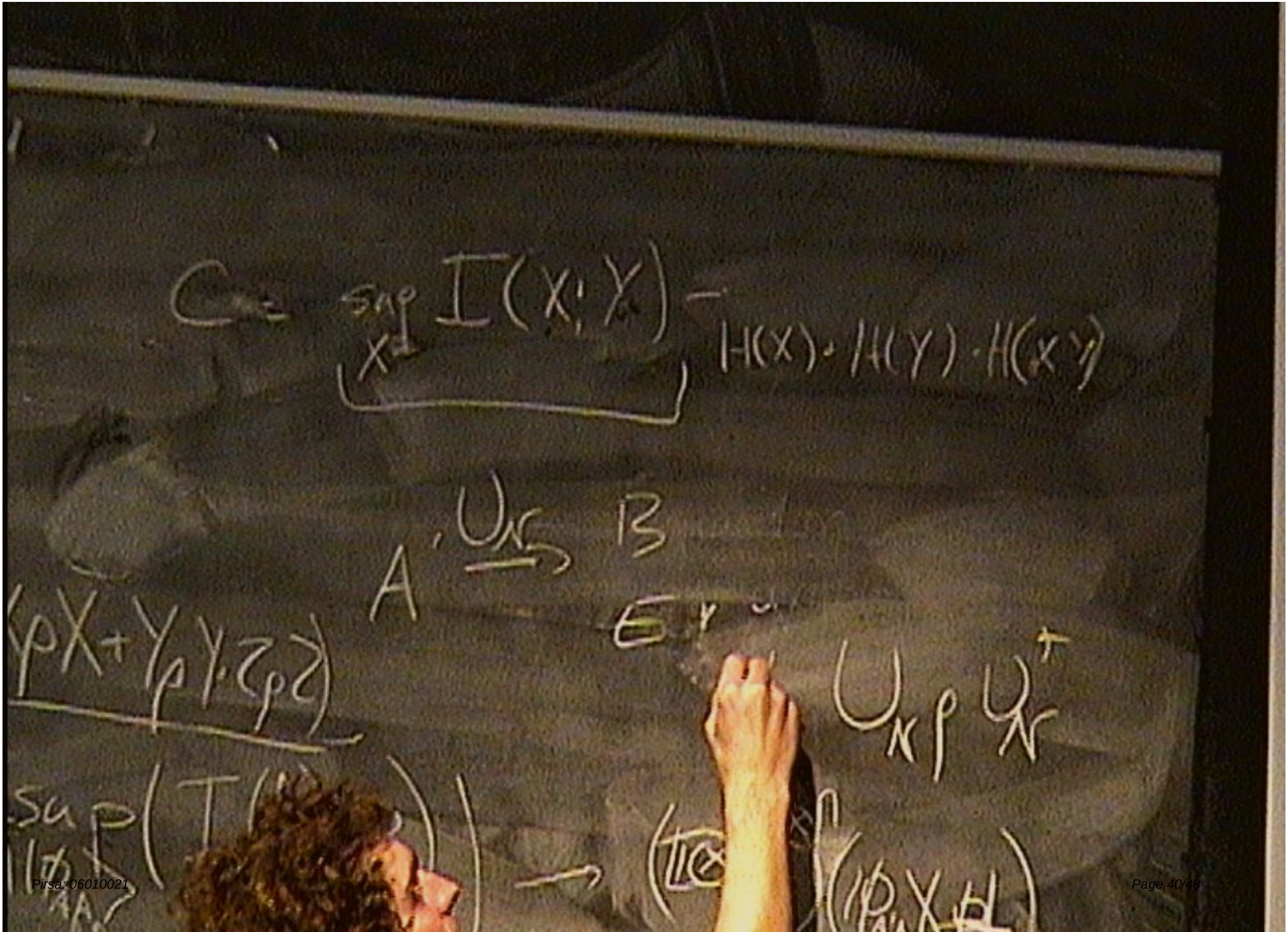
For basically all Pauli Channels, some repetition code beats hashing near $R=0$.

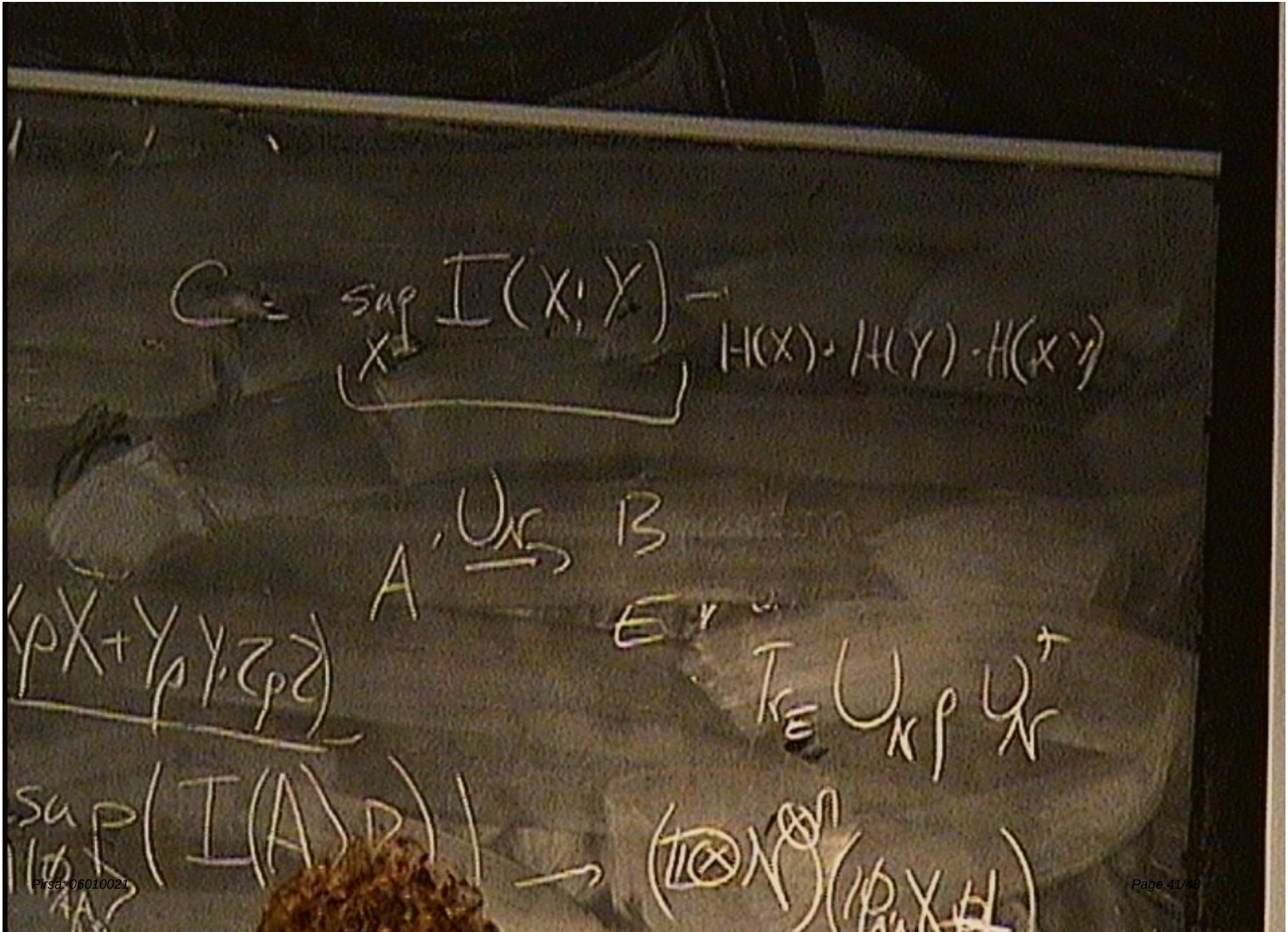
Two Exceptions:

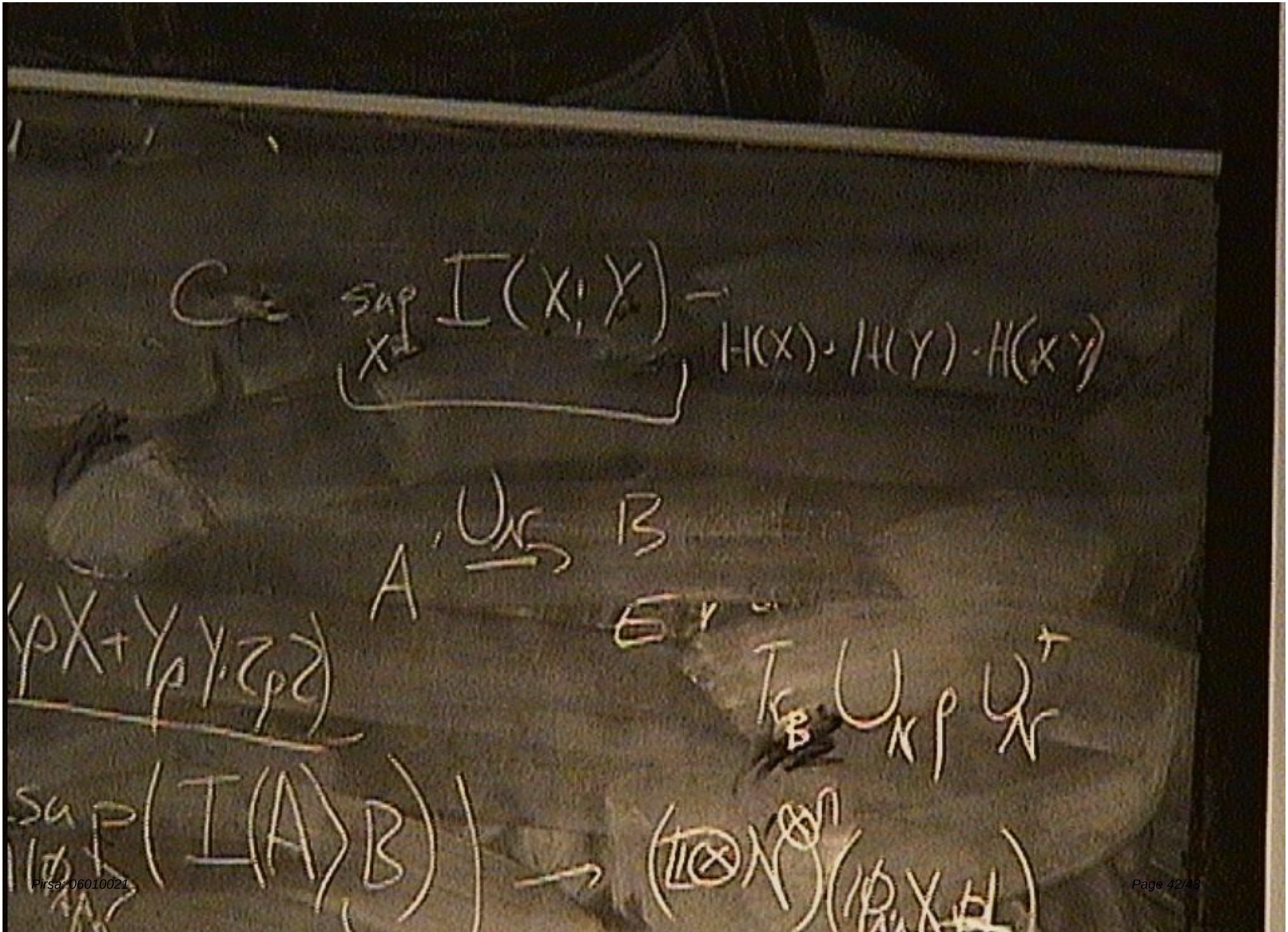
- Dephasing, etc. $N(\rho) = (1-p)\rho + Z\rho Z$
  - Hashing is optimal (Rains ~97)
- Two-Pauli, equal probs.

$N(\rho) = (1-p)\rho + \frac{p}{2} X\rho X + \frac{p}{2} Z\rho Z$

  - cat codes don't work
  - cat in cat doesn't either
  - $Q(N) \sim 1 - H(1-p, \frac{p}{2}, \frac{p}{2})$?
  - but it's not "degradable" (all known additive channels are).


C = sup I(X;Y) − H(X) · H(Y) · H(X Y)
A · U B
U ρ U†


C = sup I(X;Y) − H(X) · H(Y) · H(XY)
A · U_K B
E
T_K E U_K ρ U_K†


C = sup I(X;Y)
H(X) + H(Y) - H(X,Y)
A
B

A special Channel

For basically all Pauli Channels, some repetition code beats hashing near $R=0$.

Two Exceptions:

- Dephasing, etc. $N(\rho) = (1-p)\rho + Z\rho Z$
  - Hashing is optimal (Rains ~97)

- Two-Pauli, equal probs.

$N(\rho) = (1-p)\rho + \frac{p}{3} X\rho X + \frac{p}{3} Z\rho Z$

  - cat codes don't work
  - cat in cat doesn't either
  - $Q(N) \sim 1 - H(1-p, \frac{p}{3}, \frac{p}{3})$?
  - but it's not "degradable" (all known additive channels are).

What we know:

- best rep code finds out basically everything about X errors
- Manages not to completely scramble the Z's
- $m \sim \frac{1}{p_z}$ $p_x \geq p_0 \geq p_y$
- can concat cat codes b/c Z-cat: $p_x \geq p_z \rightarrow p_z \geq p_x$
- * only beats hashing near * where rate $\rightarrow 0$

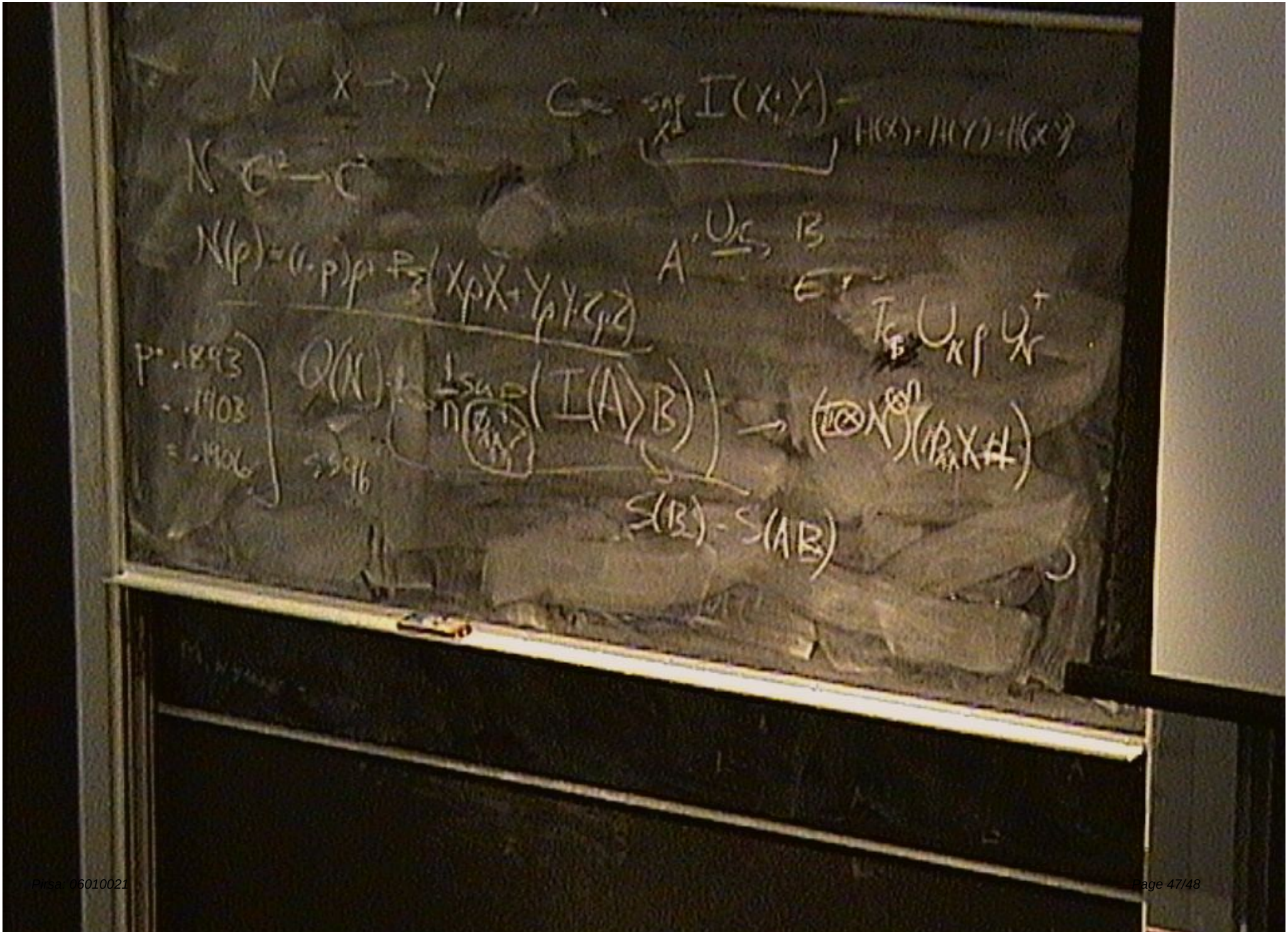
Observation:
- a repetition code has pretty bad rate if we just want to know X error
- every X measurement messes up the Z's more.

So:
- Use better code to measure X's. Fewer synd. measurements, so cleaner Z's.

Summary

- Repetition code in basis of less probable error allows nonzero rate where hashing fails
- block size ~ $1/p_2$ best
- Adapt 2nd level of rep. codes to conditional channels
  => better codes for depolar. channel. ↑did

- Two-Pauli: Additive? ↓speculation
- Repetition coding is not very smart. Better ideas?


N X → Y
C = sup I(X;Y)
H(X) + H(Y) − H(X,Y)
N: C^n → C^n
N(ρ) = (1−p)ρ + p Σ_i (X_i ρ X_i + Y_i ρ Y_i + Z_i ρ Z_i)
A, B
p* .1893
.1103
.1906
Q(N) = lim_{n→∞} (1/n) sup_{ρ_AA'} (I(A⟩B))
S(B) − S(AB)

Bounds on the Capacity of Depolarizing Channel