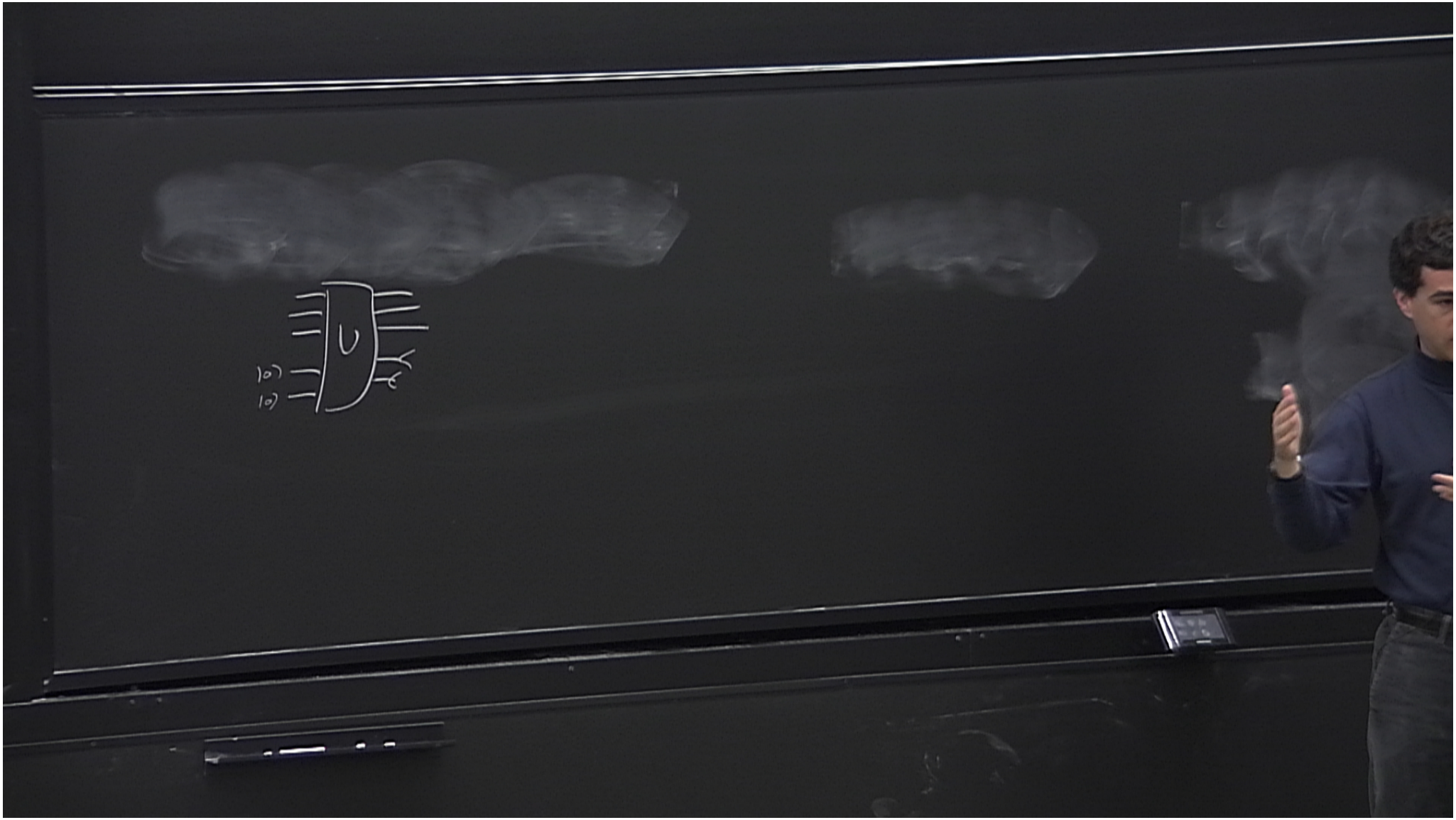
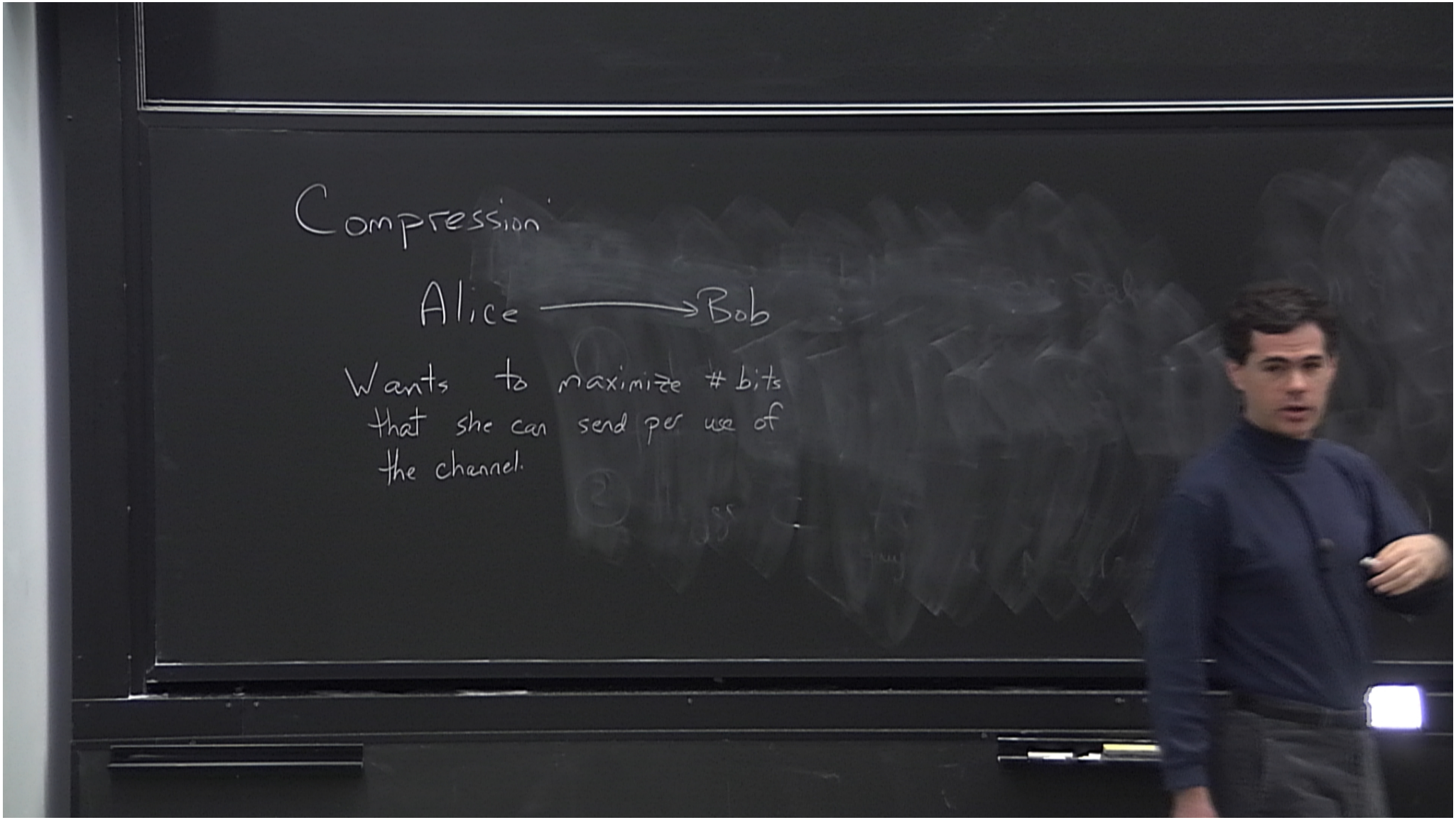
Title: Quantum Information (Review) - Lecture 11

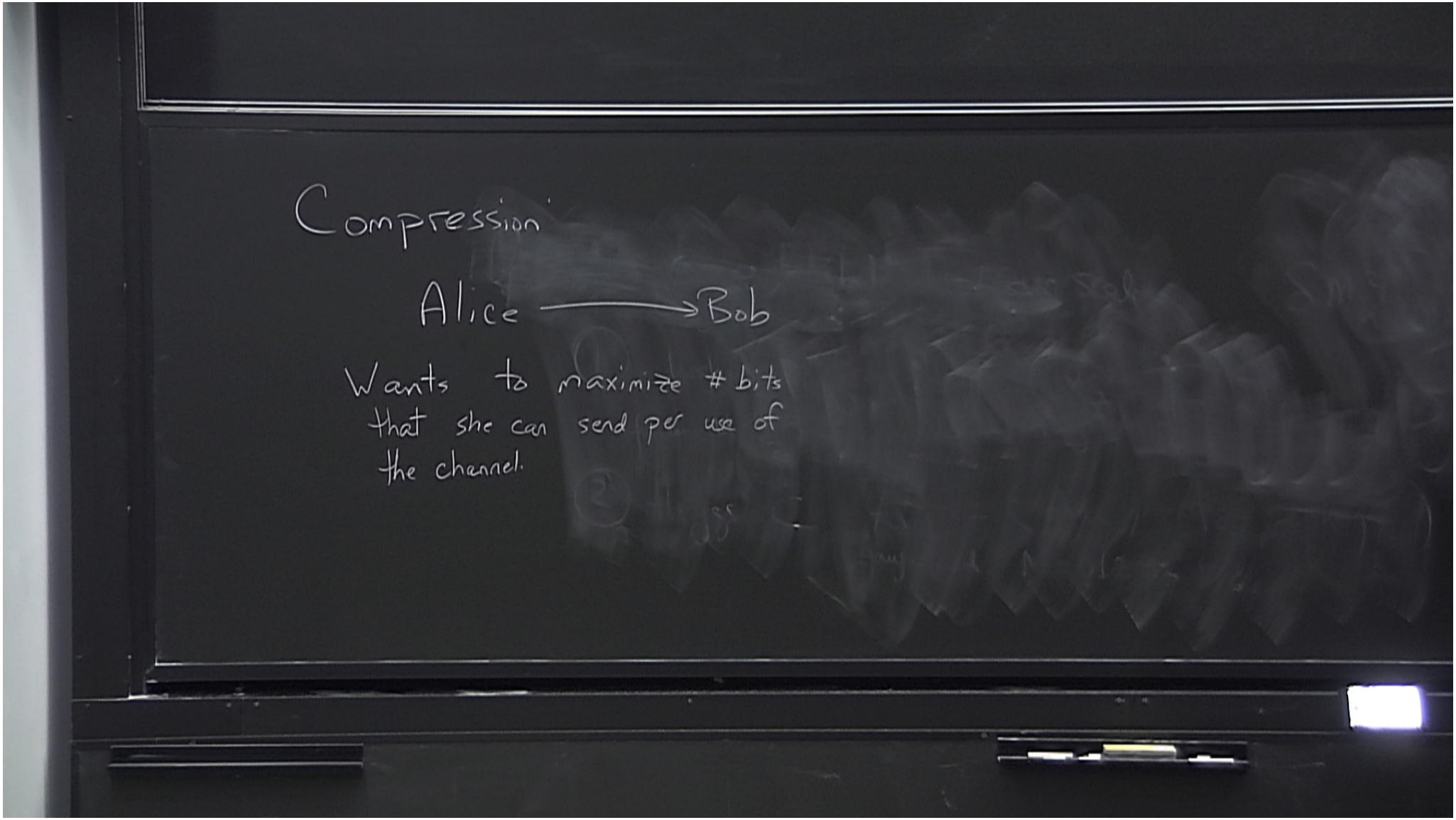
Date: Feb 28, 2012 10:15 AM

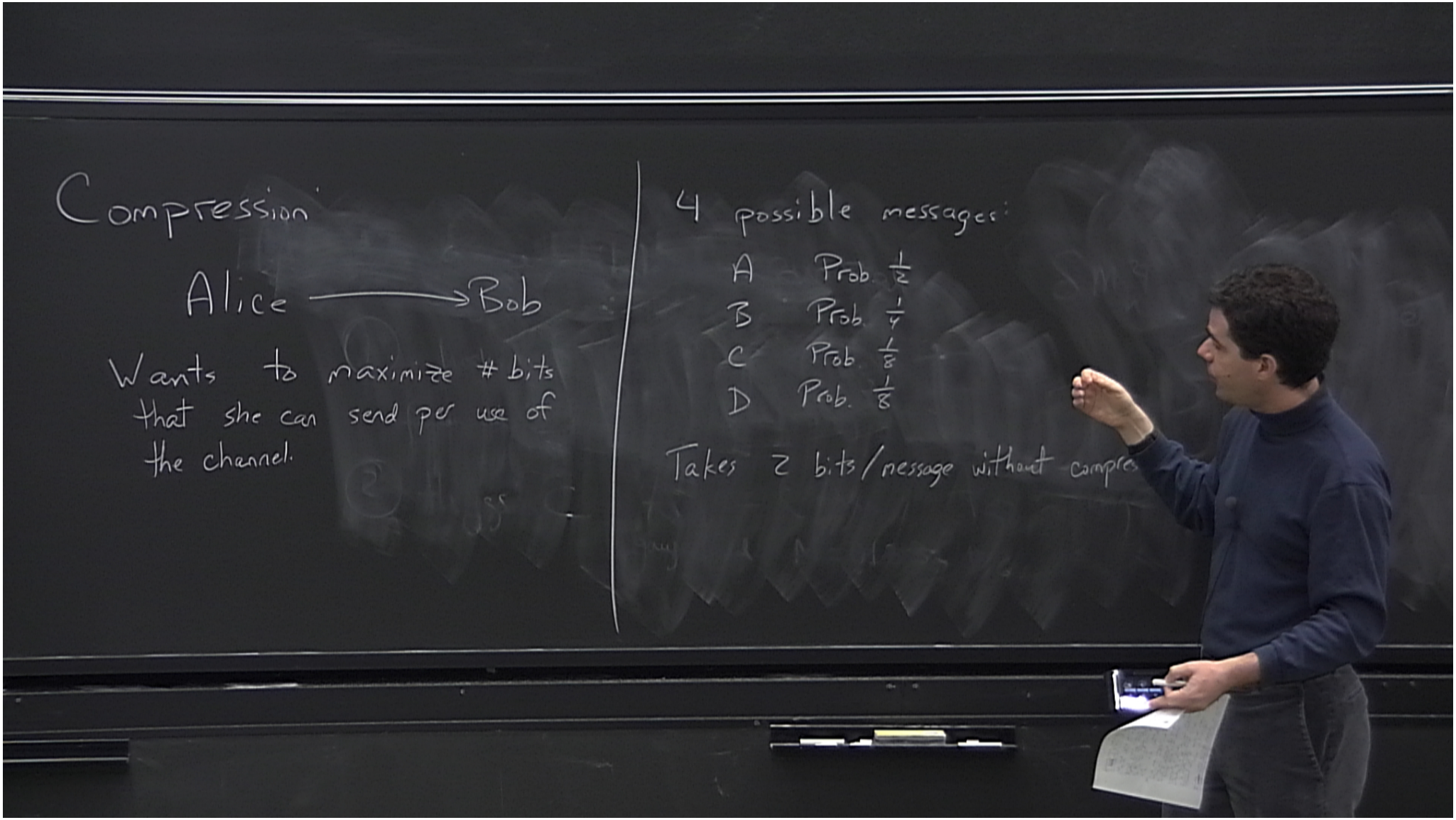
URL: http://pirsa.org/12020045

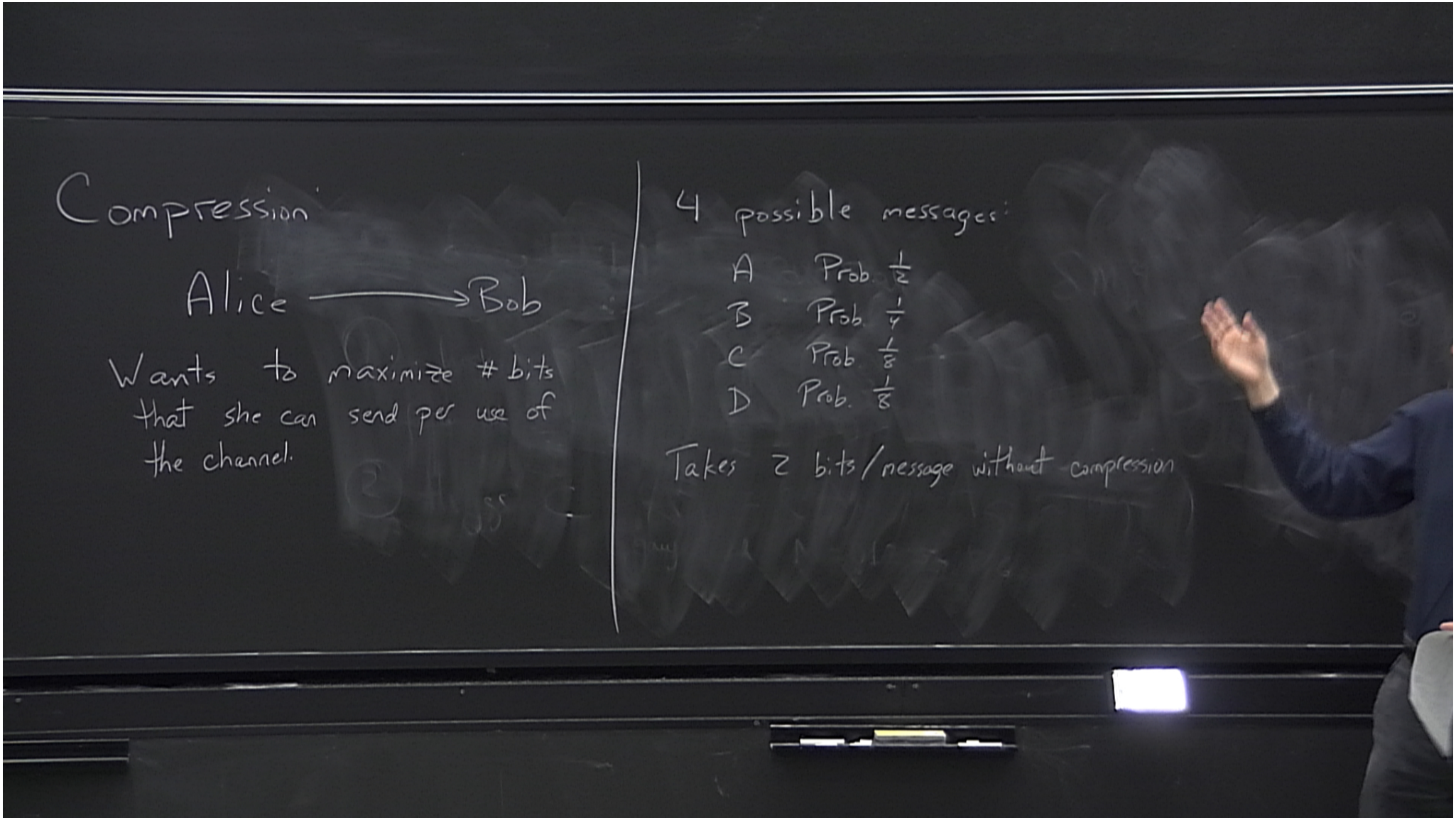
Abstract:


U
|0⟩
|0⟩


Compression
Alice
Bob
Wants to maximize # bits that she can send per use of the channel.


Compression
Alice
Bob
Wants to maximize # bits that she can send per use of the channel.


Compression
Alice → Bob
Wants to maximize # bits that she can send per use of the channel.
4 possible messages:
A Prob. 1/2
B Prob. 1/4
C Prob. 1/8
D Prob. 1/8
Takes 2 bits/message without compres


Compression
Alice → Bob
Wants to maximize # bits that she can send per use of the channel.
4 possible messages:
A Prob. 1/2
B Prob. 1/4
C Prob 1/8
D Prob. 1/8
Takes 2 bits/message without compression

Compression

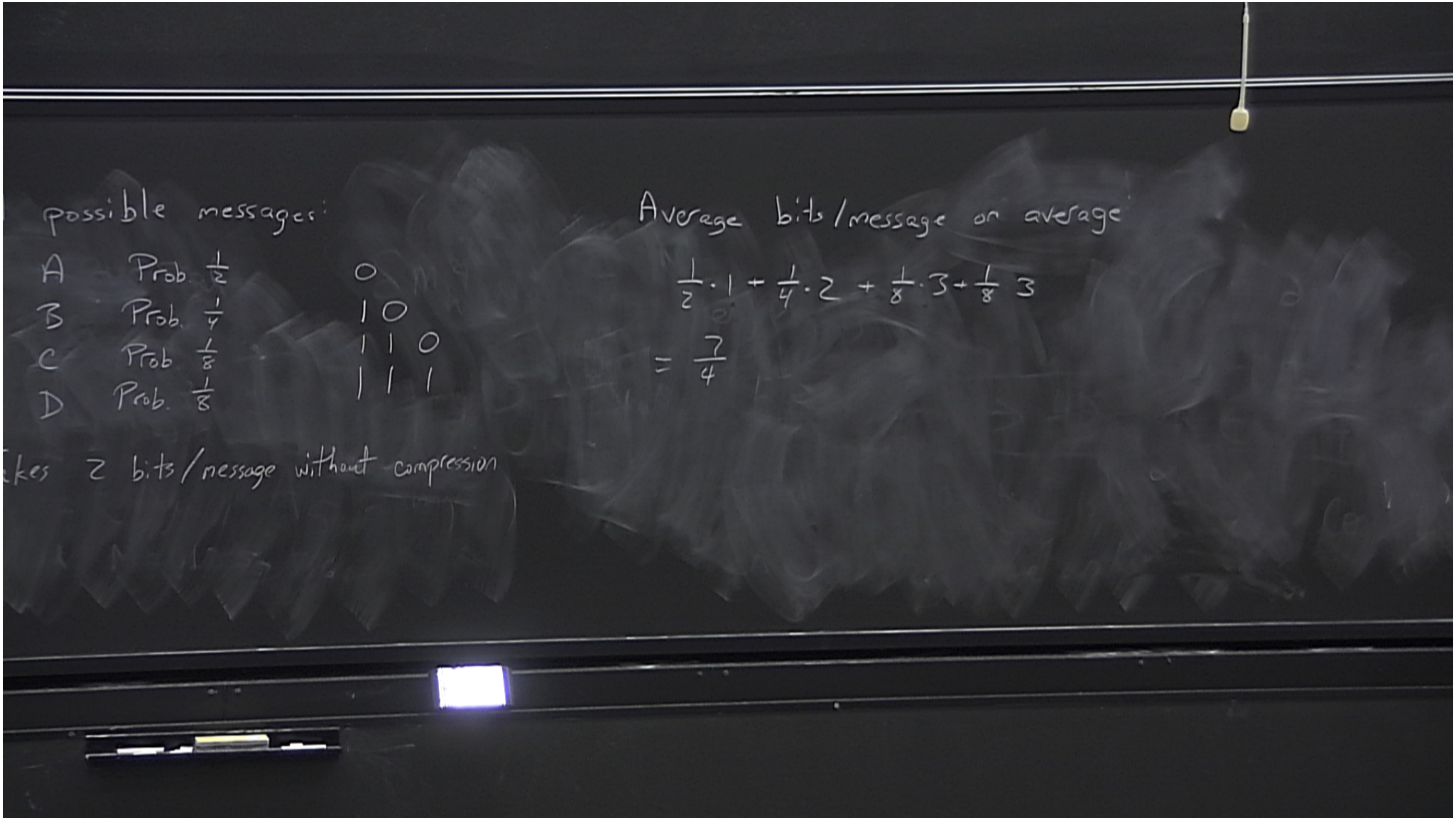
Alice ⟶ Bob

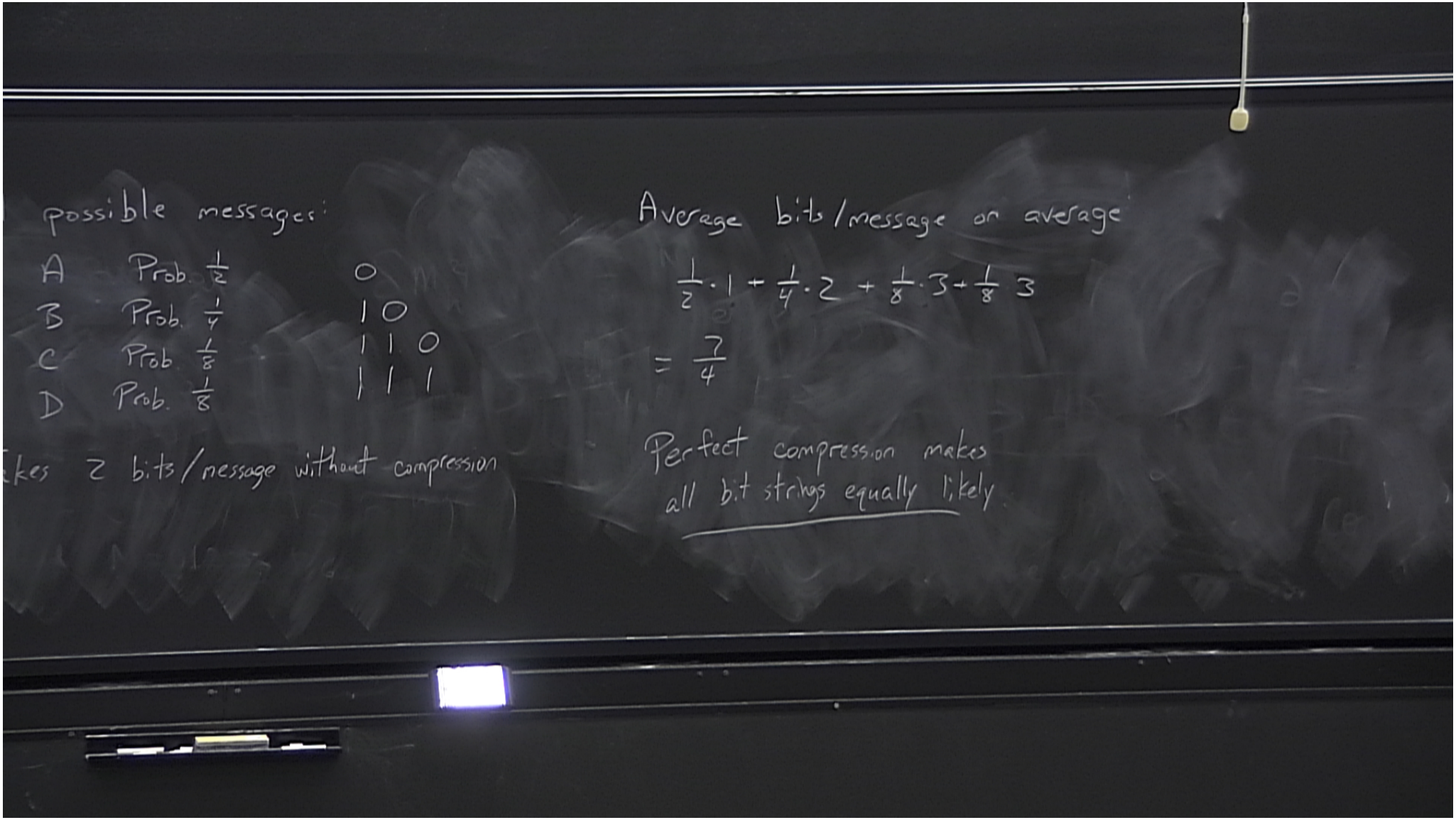
Wants to maximize # bits that she can send per use of the channel.

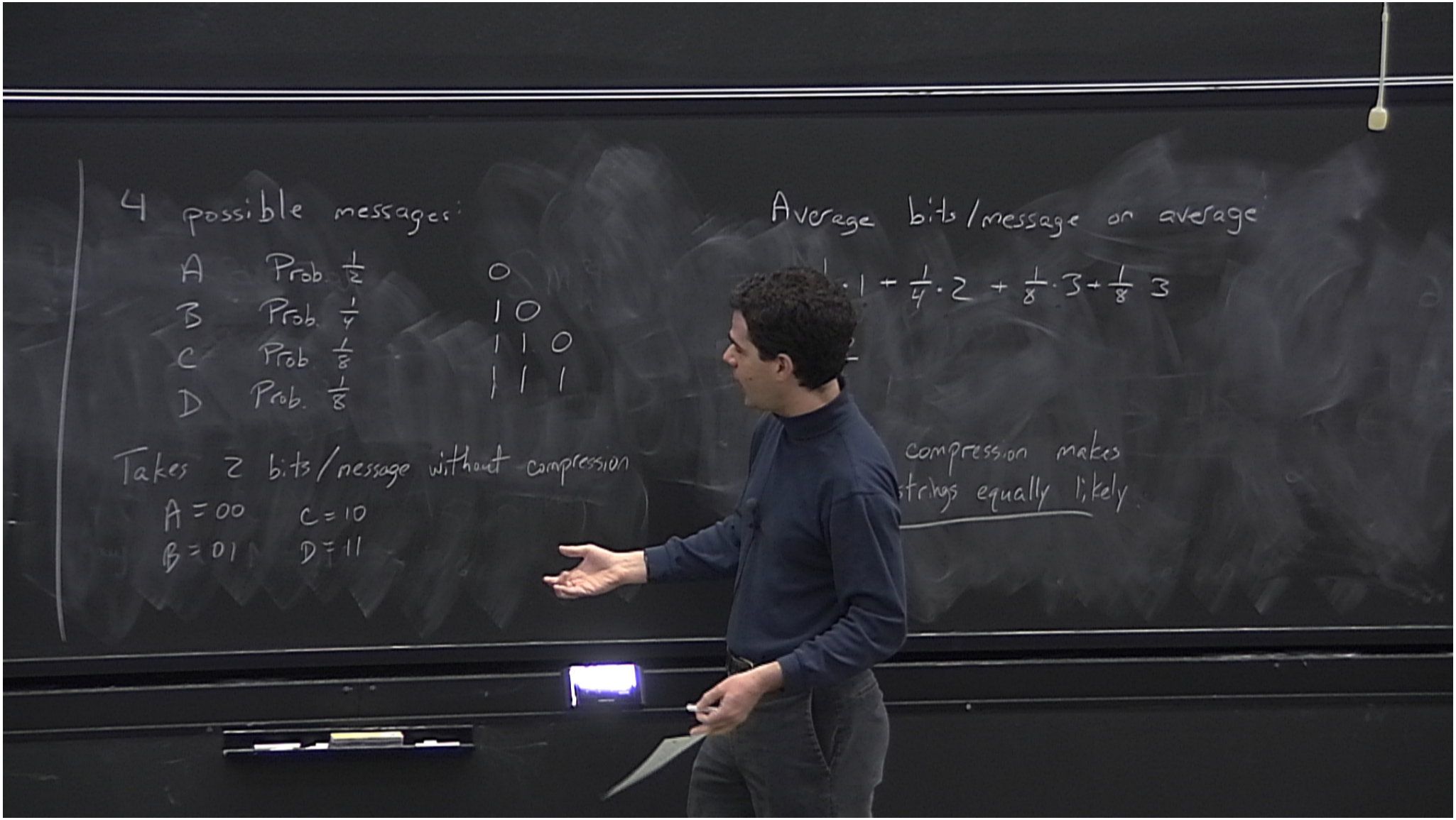
4 possible messages:

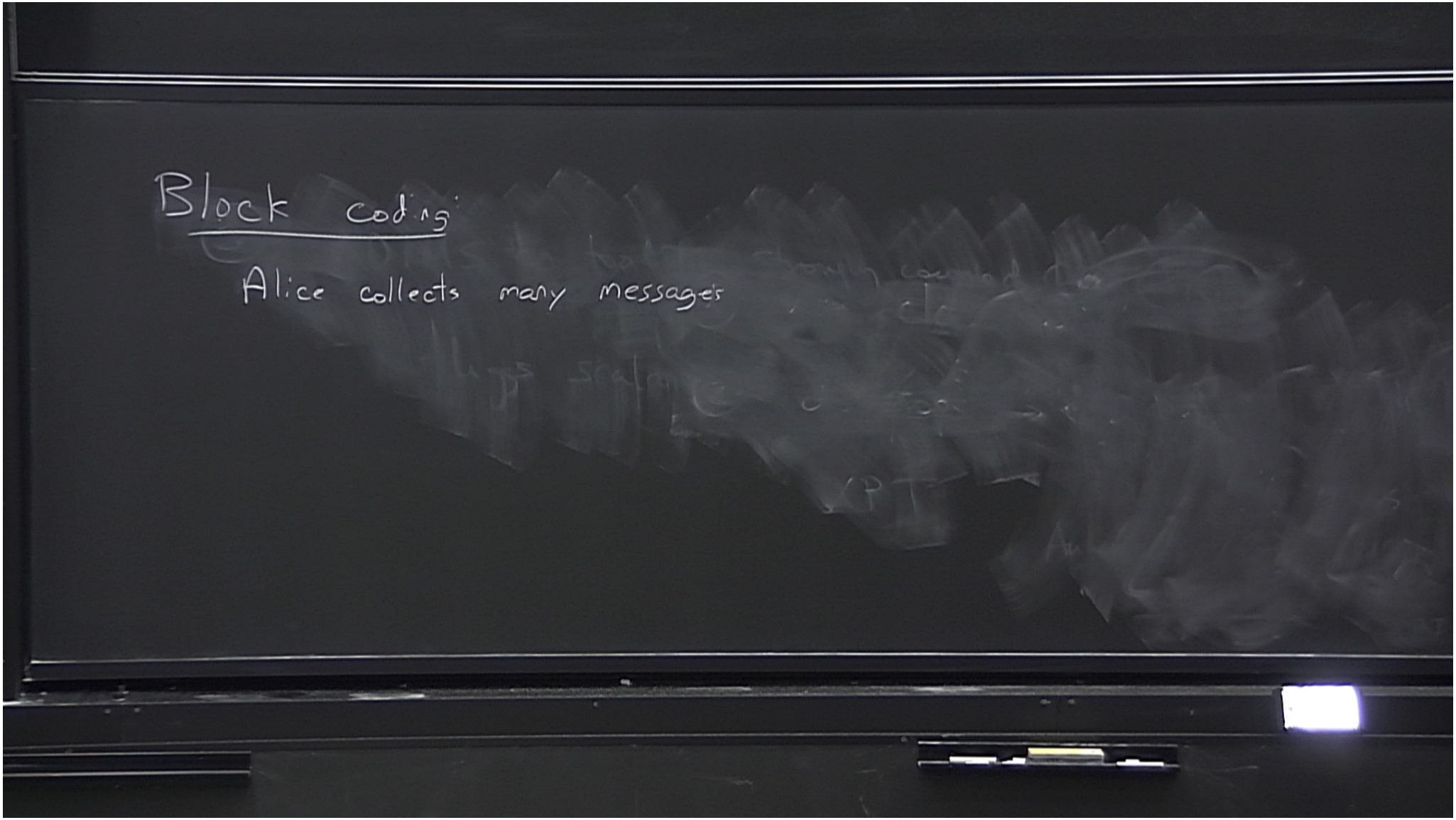
A	Prob $\frac{1}{2}$	0
B	Prob $\frac{1}{4}$	1 0
C	Prob $\frac{1}{8}$	1 1 0
D	Prob $\frac{1}{8}$	1 1 1

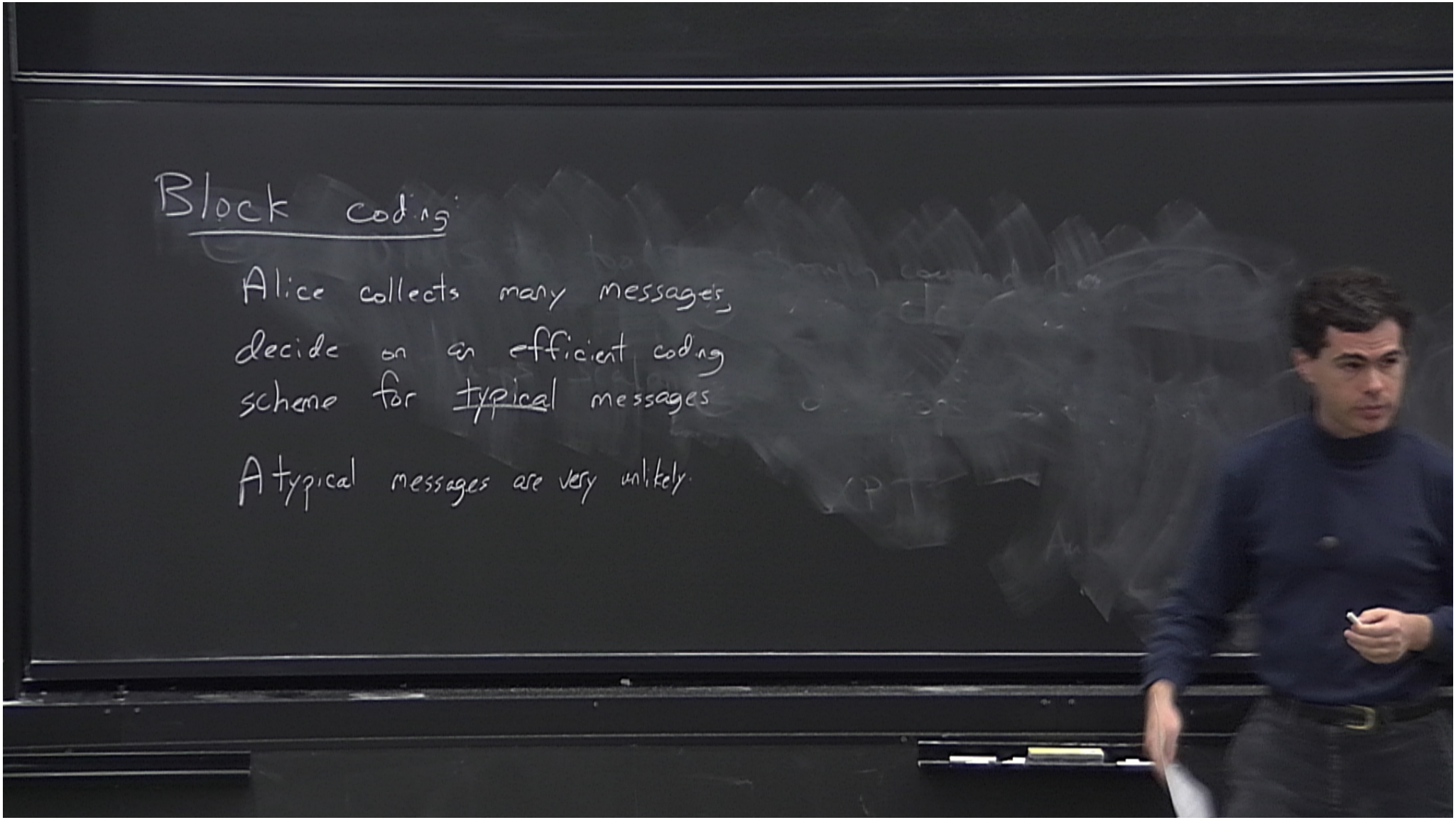
Takes 2 bits/message without compression


possible messages:
A Prob. 1/2 0
B Prob. 1/4 1 0
C Prob 1/8 1 1 0
D Prob. 1/8 1 1 1
kes 2 bits/message without compression
Average bits/message or average
1/2 · 1 + 1/4 · 2 + 1/8 · 3 + 1/8 3
= 7/4


possible messages:
A Prob. 1/2 0
B Prob. 1/4 1 0
C Prob 1/8 1 1 0
D Prob. 1/8 1 1 1
kes 2 bits/message without compression
Average bits/message or average
1/2 · 1 + 1/4 · 2 + 1/8 · 3 + 1/8 3
= 7/4
Perfect compression makes
all bit strings equally likely


4 possible messages:
A Prob. 1/2 0
B Prob. 1/4 1 0
C Prob 1/8 1 1 0
D Prob. 1/8 1 1 1
Takes 2 bits/message without compression
A = 00 C = 10
B = 01 D = 11
Average bits/message on average
1/2 · 1 + 1/4 · 2 + 1/8 · 3 + 1/8 3
compression makes
strings equally likely


Block coding
Alice collects many messages

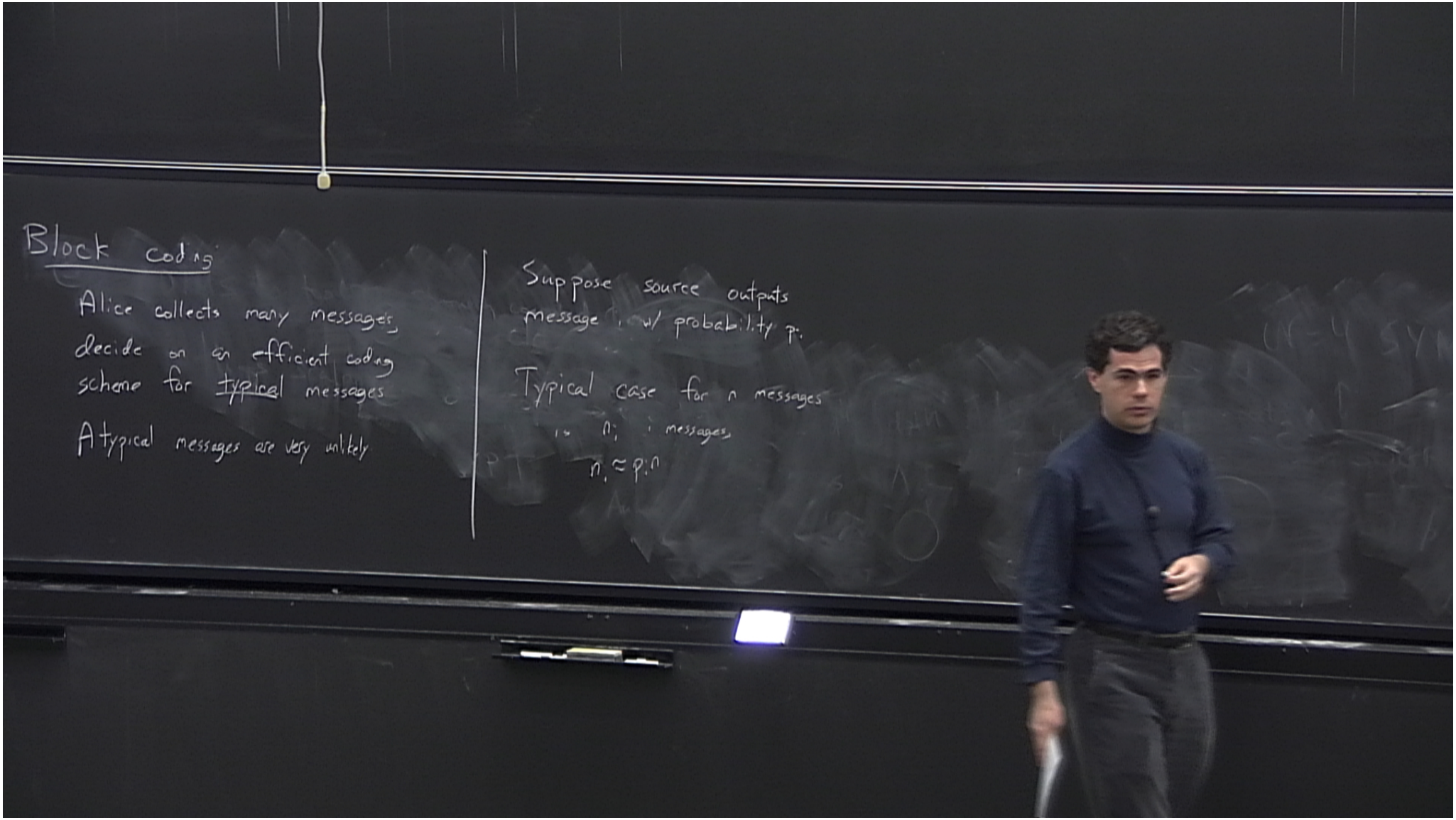

Block coding
Alice collects many messages,
decide on an efficient coding
scheme for typical messages
Atypical messages are very unlikely.

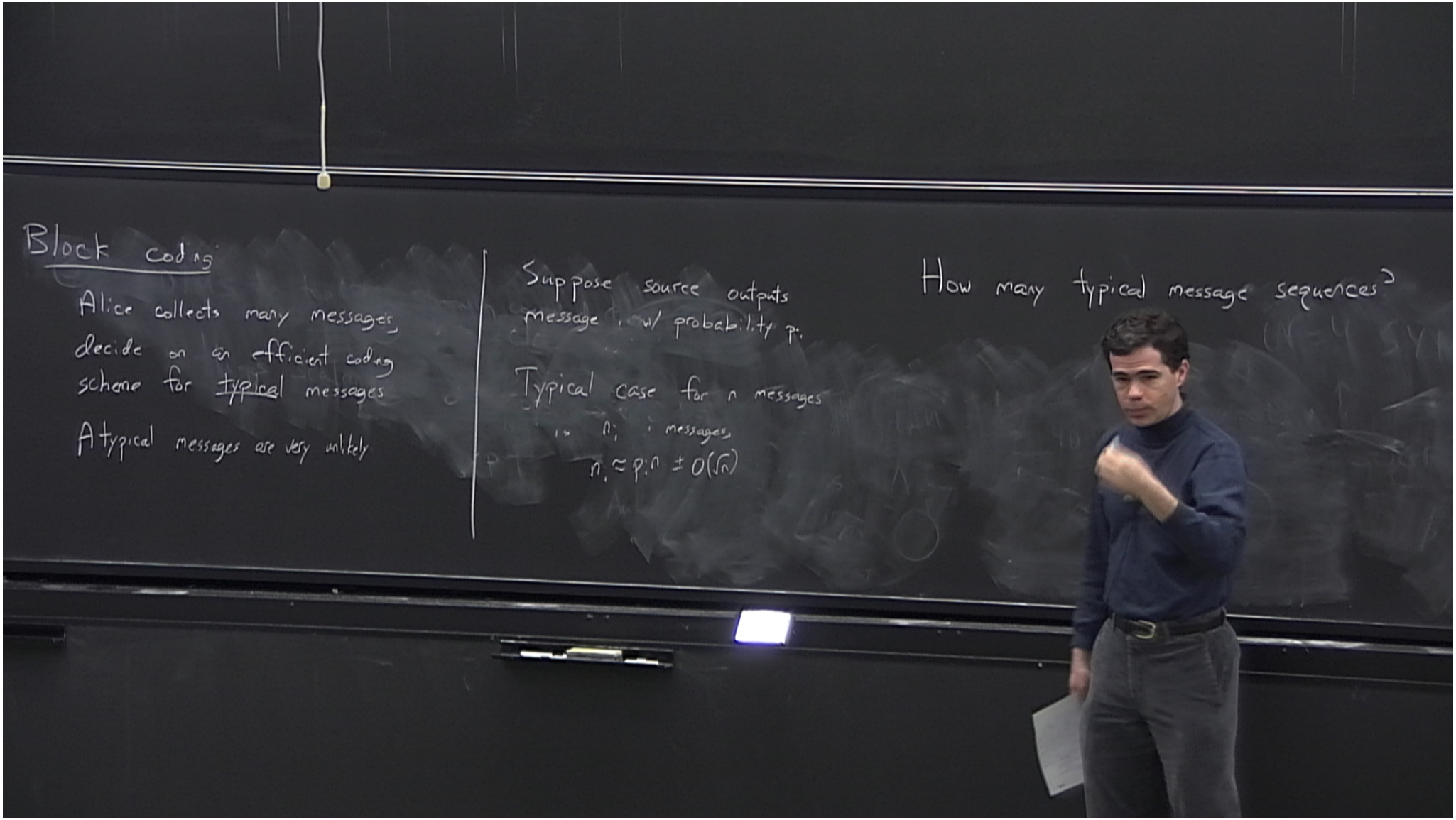
Block coding

Alice collects many messages, decide on an efficient coding scheme for typical messages

Atypical messages are very unlikely.

Suppose source outputs message i w/ probability p_i.


Block coding
Alice collects many messages, decide on an efficient coding scheme for typical messages
Atypical messages are very unlikely
Suppose source outputs message i w/ probability p_i
Typical case for n messages
$\approx n_i$: messages i
$n_i \approx p_i n$


Block coding
Alice collects many messages, decide on an efficient coding scheme for typical messages
Atypical messages are very unlikely
Suppose source outputs message i w/ probability p_i
Typical case for n messages
$\approx n_i$: i messages
$n_i \approx p_i n \pm O(\sqrt{n})$
How many typical message sequences?

Coding

ce collects many messages,
ide on an efficient coding
eme for typical messages

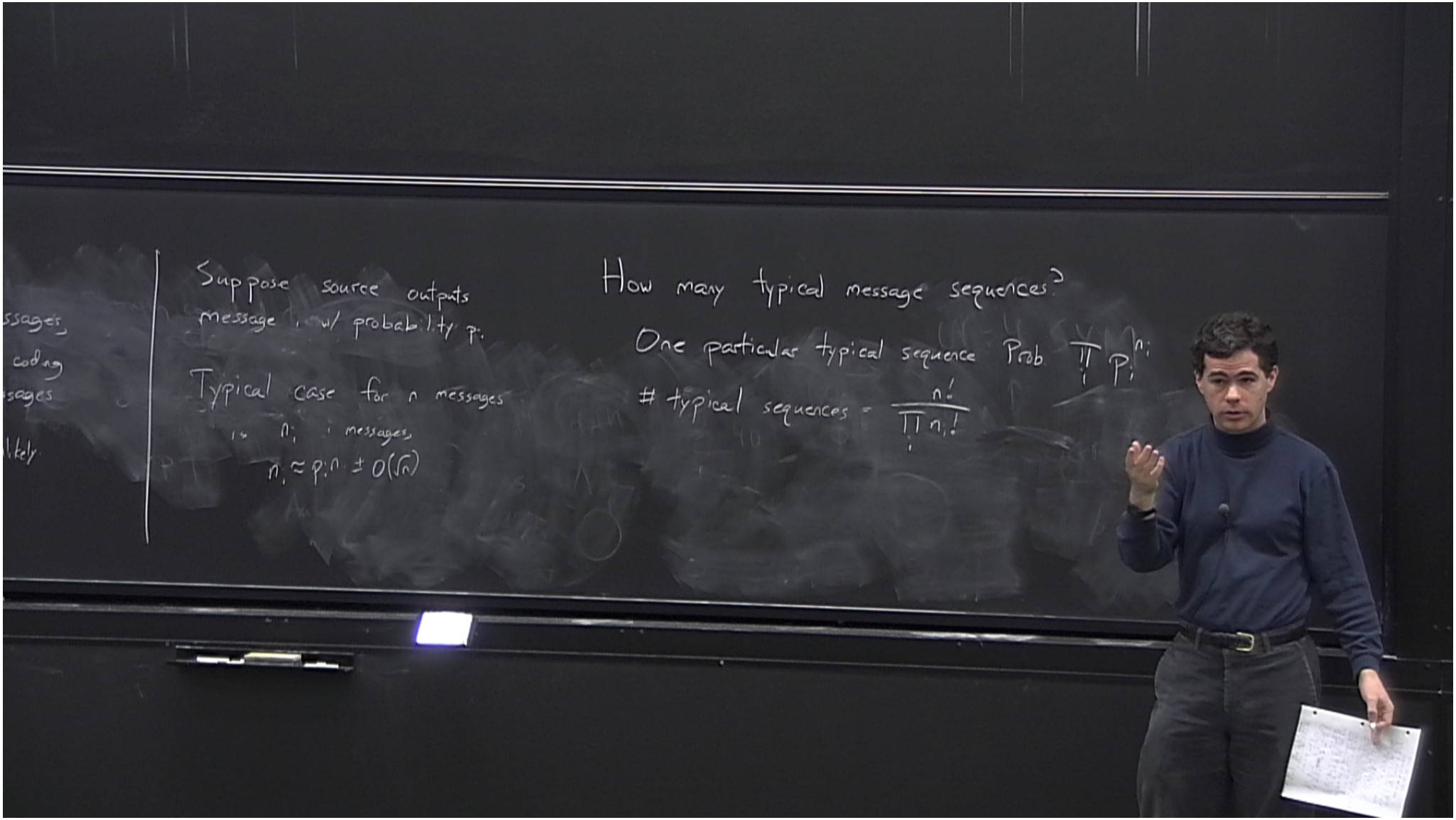
ypical messages are very unlikely

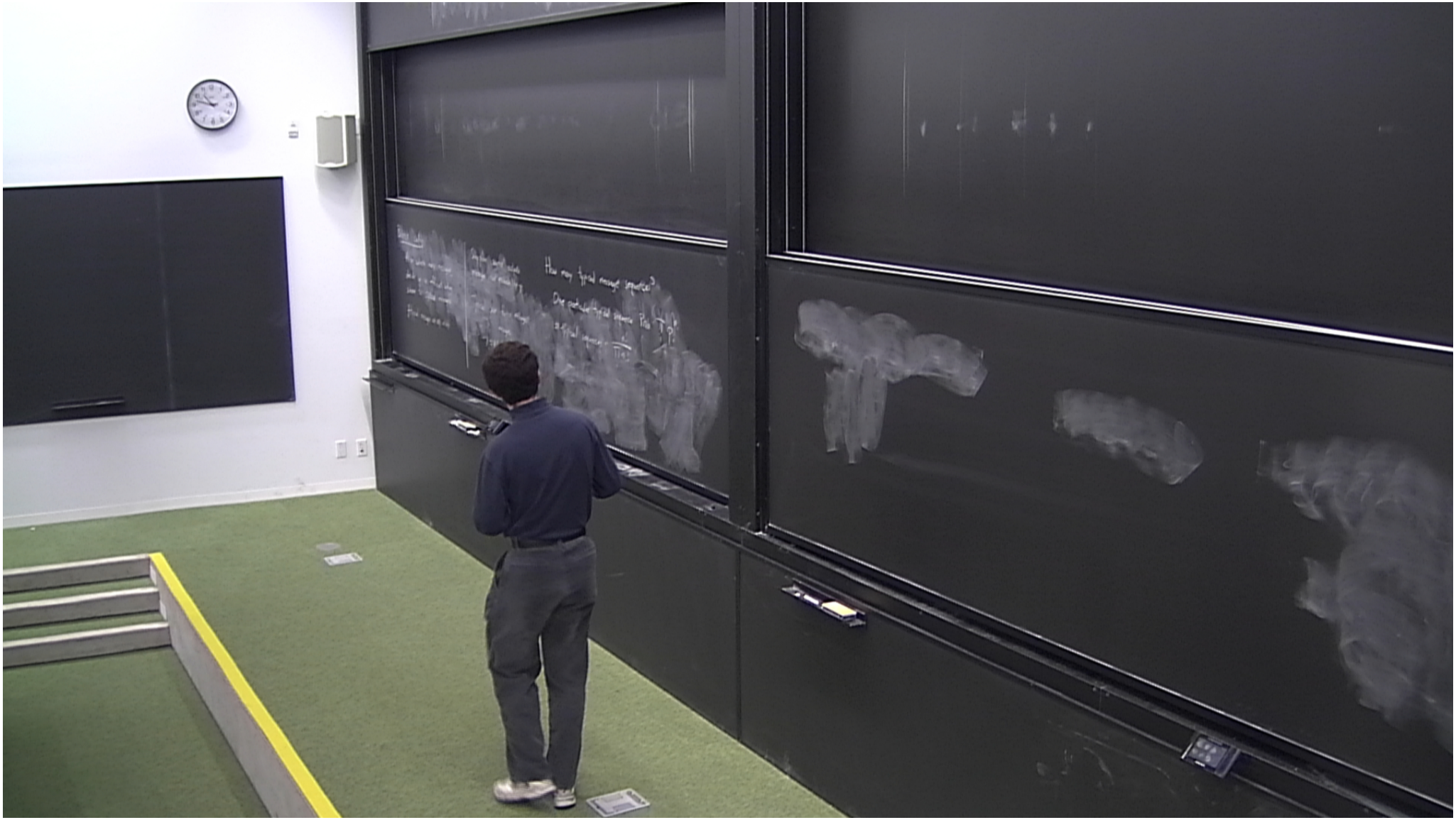
Suppose source outputs
message i w/ probability p_i

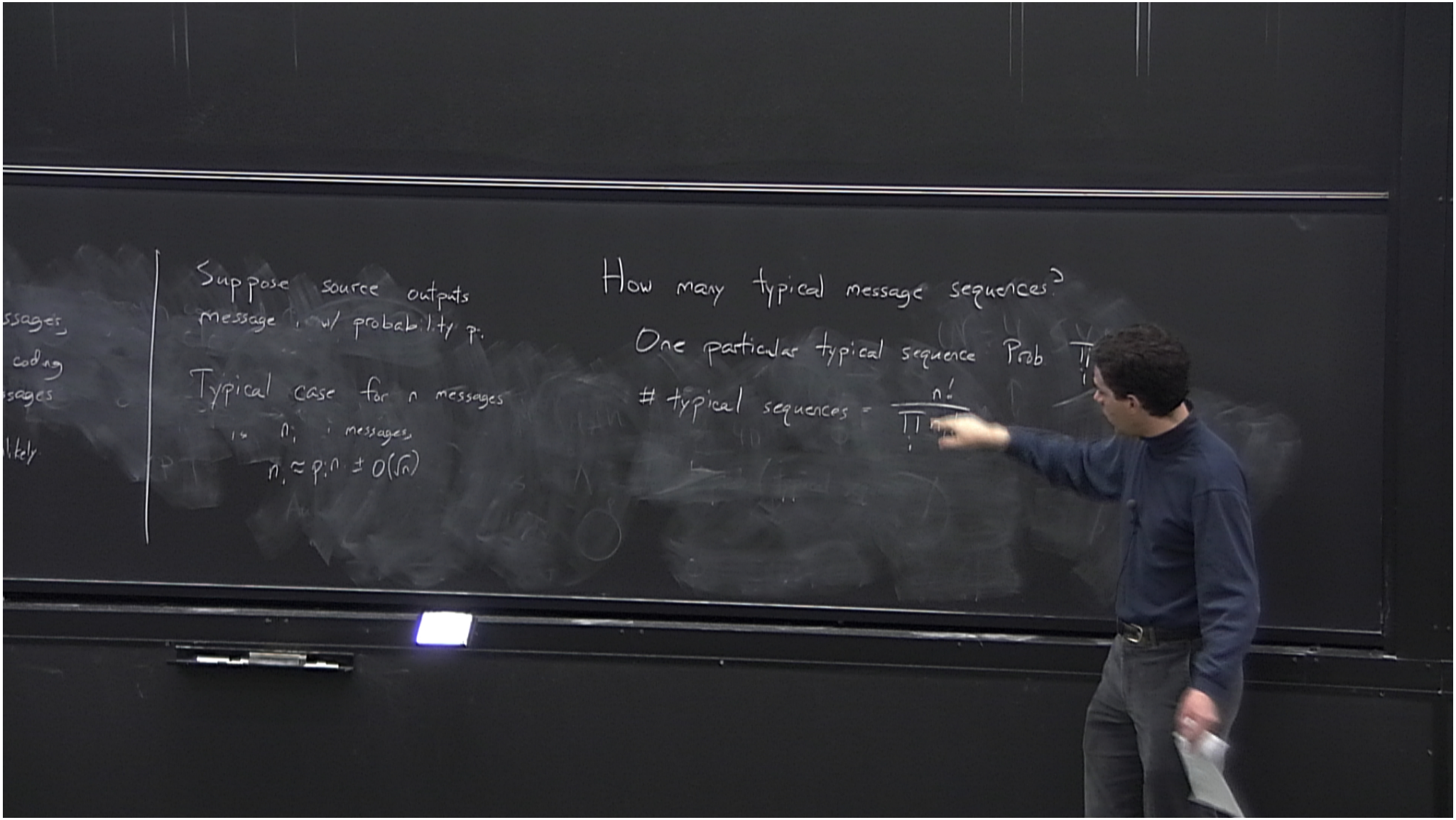
Typical case for n messages
i n_i i messages,
$n_i \approx p_i n \pm O(\sqrt{n})$

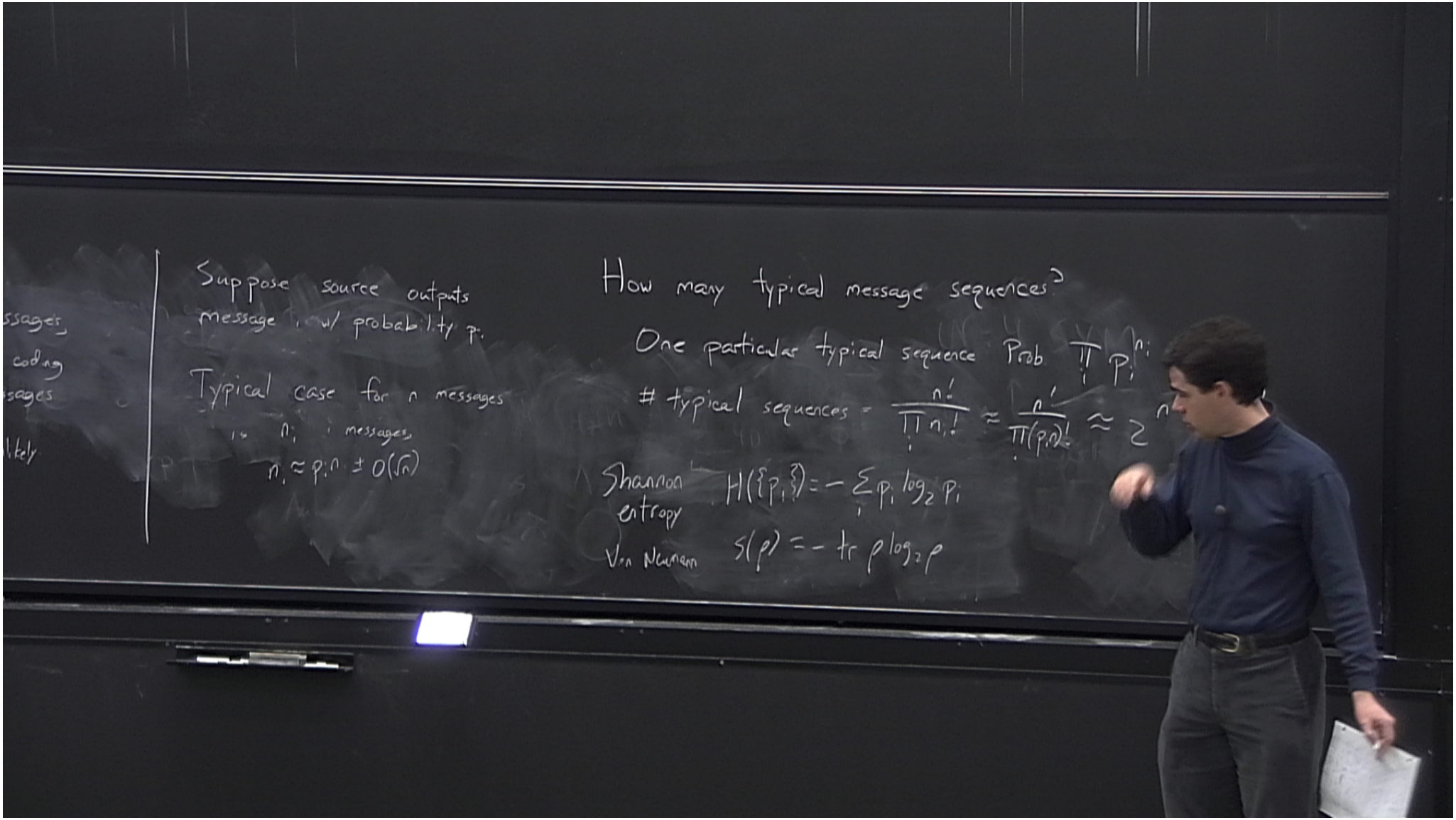
How many typical message sequences?

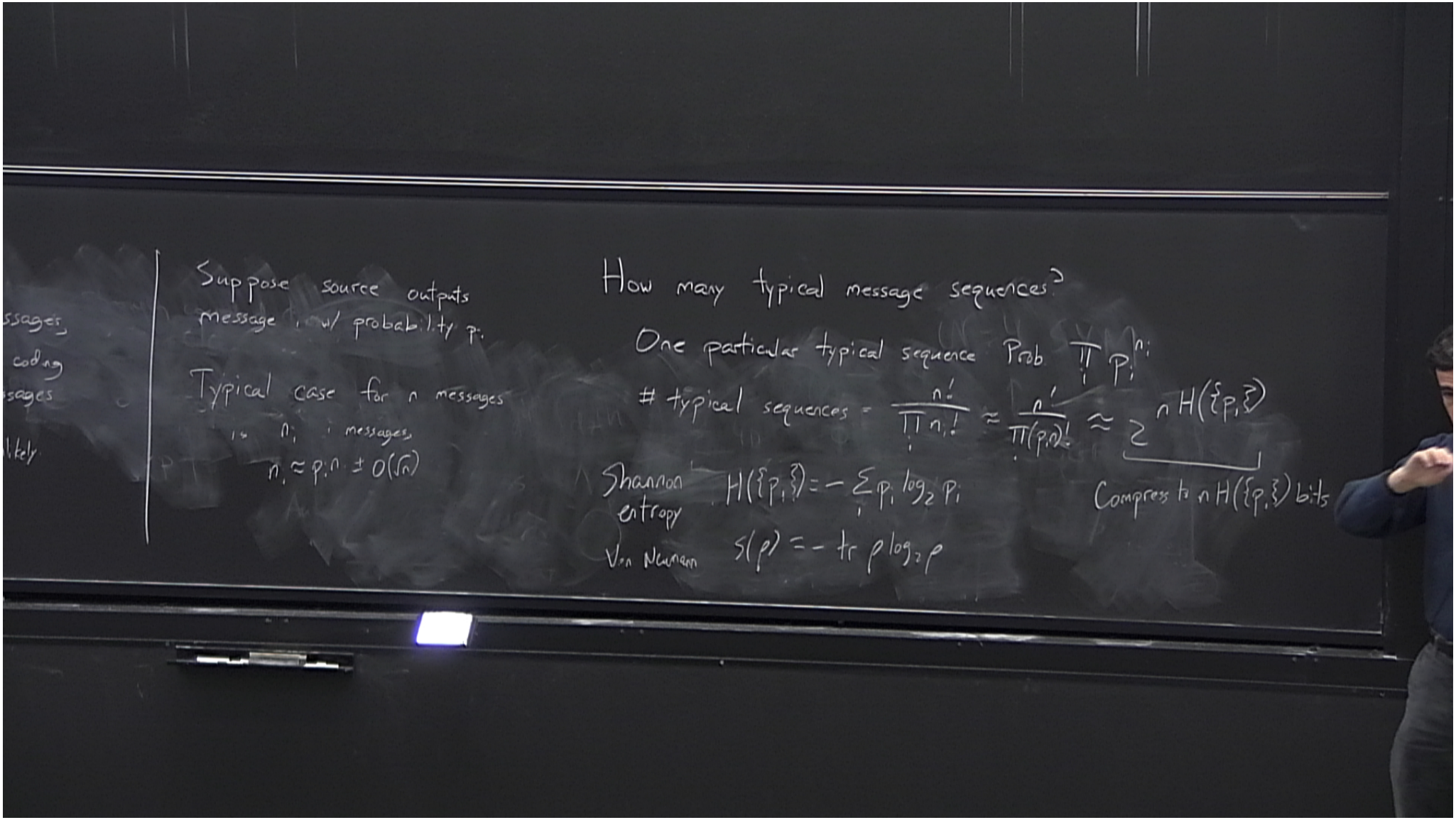
One particular typical sequence Prob $\prod_i p_i^{n_i}$

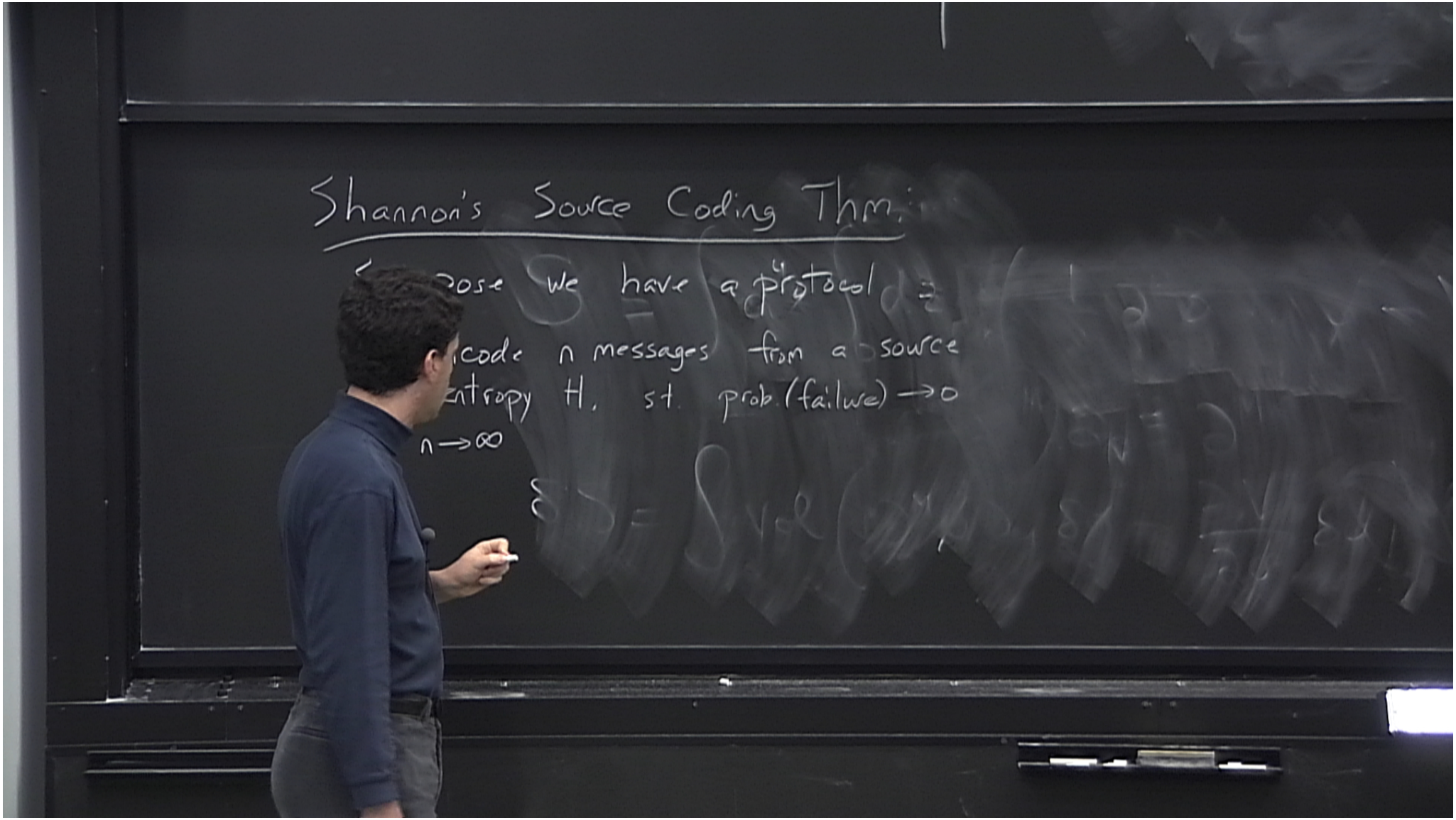

ssages
coding
ssages
likely
Suppose source outputs
message i w/ probability p_i
Typical case for n messages
is n_i i messages
$n_i \approx p_i n \pm O(\sqrt{n})$
How many typical message sequences?
One particular typical sequence Prob $\prod_i p_i^{n_i}$
typical sequences = $\frac{n!}{\prod_i n_i!}$

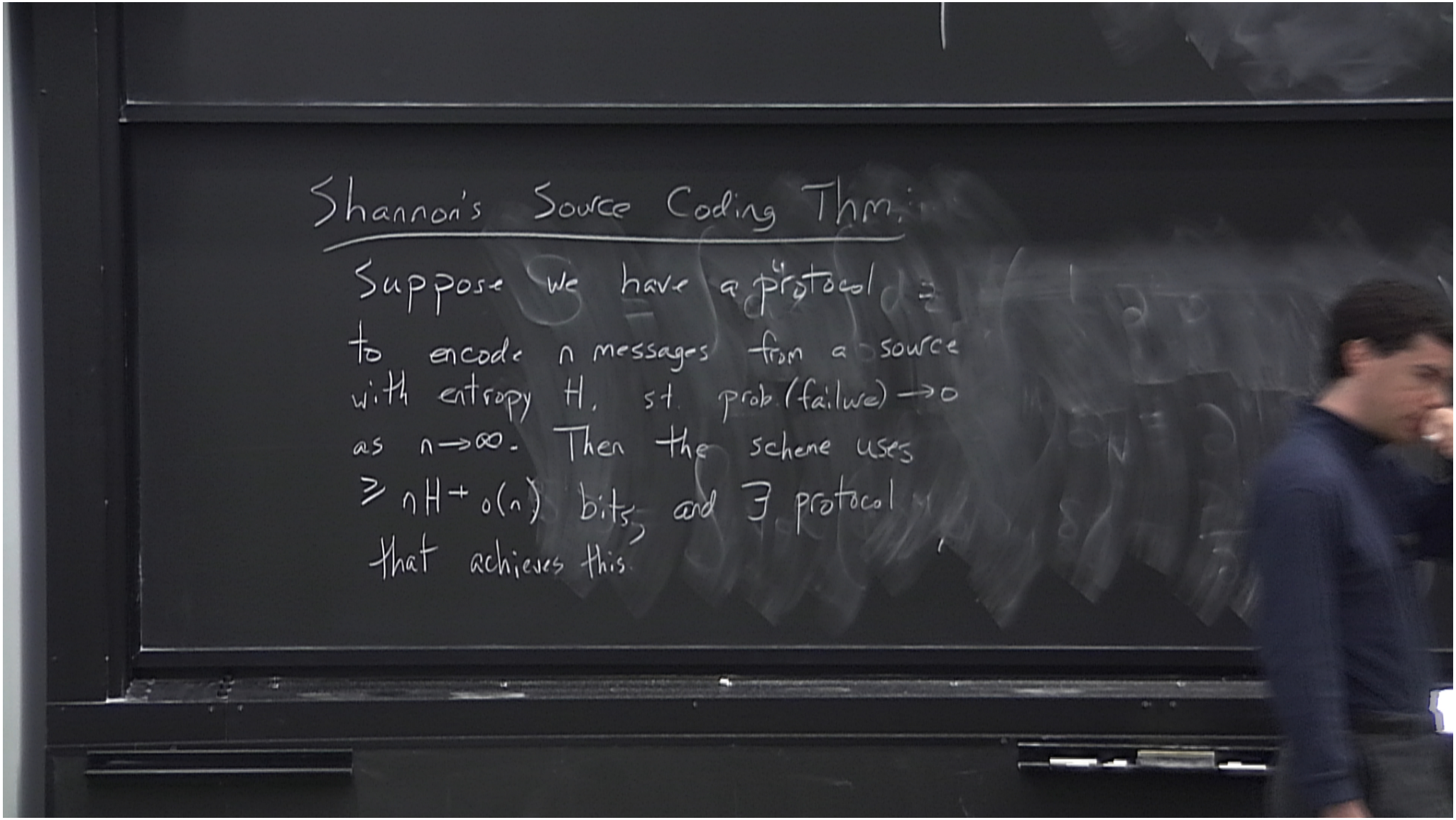

How many typical message sequences?

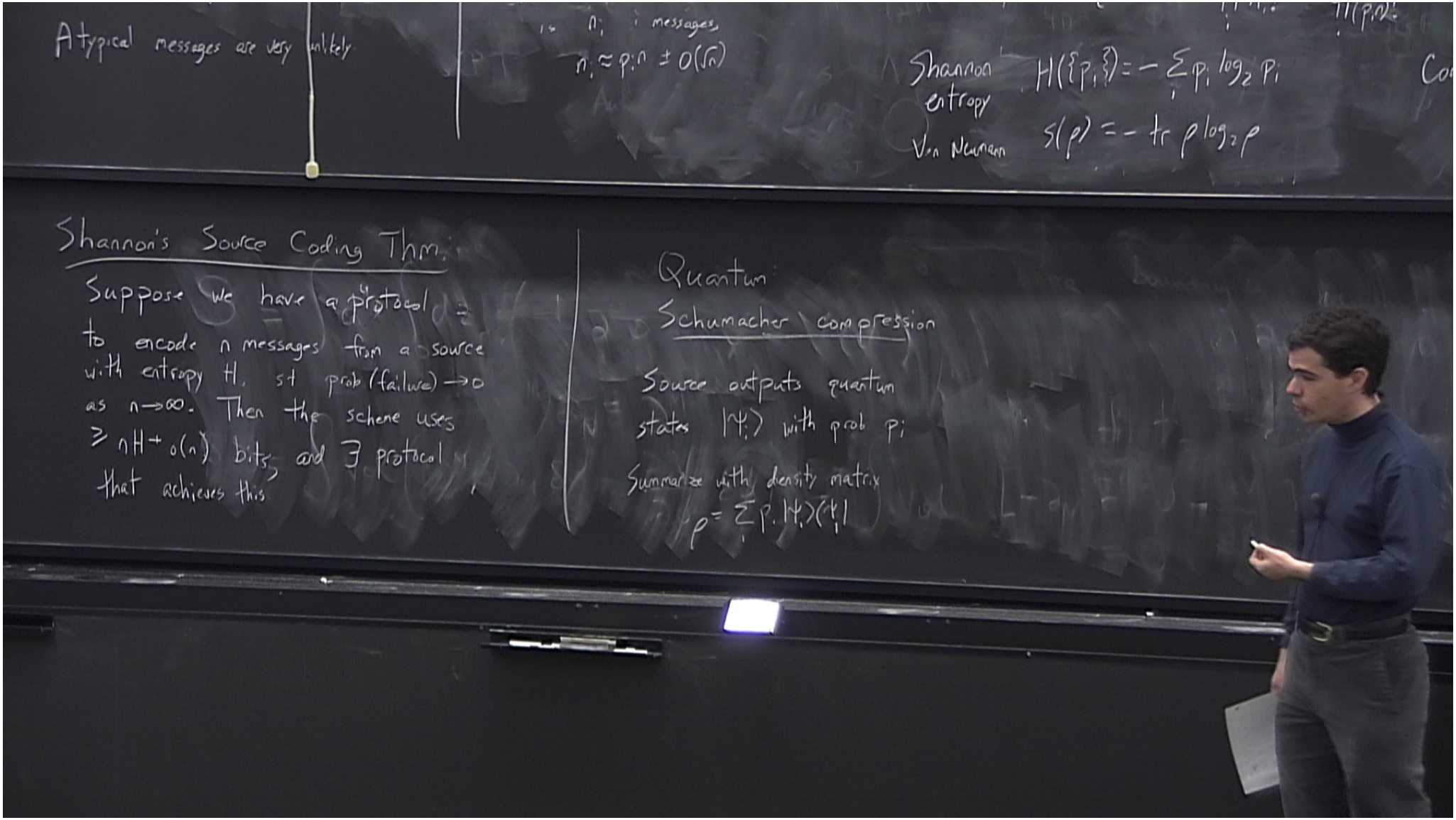

Suppose source outputs
message i w/ probability p_i
Typical case for n messages
is n_i i messages
$n_i \approx p_i n \pm O(\sqrt{n})$
How many typical message sequences?
One particular typical sequence Prob $\prod_i$
typical sequences = $\frac{n!}{\prod_i n_i!}$


Suppose source outputs
message i w/ probability p_i
Typical case for n messages
is n_i i messages
$n_i \approx p_i n \pm O(\sqrt{n})$
How many typical message sequences?
One particular typical sequence Prob $\prod_i p_i^{n_i}$
typical sequences = $\frac{n!}{\prod_i n_i!} \approx \frac{n^n}{\prod_i (p_i n)^{p_i n}} \approx 2^n$
Shannon entropy $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$
Von Neumann $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$


ssages
coding
ssages
likely
Suppose source outputs
message i w/ probability p_i
Typical case for n messages
is n_i i messages,
$n_i \approx p_i n \pm O(\sqrt{n})$
How many typical message sequences?
One particular typical sequence Prob $\prod_i p_i^{n_i}$
typical sequences $= \frac{n!}{\prod_i n_i!} \approx \frac{n^n}{\prod_i (p_i n)^{p_i n}} \approx 2^{n H(\{p_i\})}$
Compress to $n H(\{p_i\})$ bits
Shannon entropy $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$
Von Neumann $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$


Shannon's Source Coding Thm:
code n messages from a source
ntropy H. s.t. prob(failure) → 0
n → ∞


Shannon's Source Coding Thm:
Suppose we have a protocol
to encode n messages from a source
with entropy H, s.t. prob(failure) → 0
as n → ∞. Then the scheme uses
≥ nH + o(n) bits, and ∃ protocol
that achieves this.


Atypical messages are very unlikely
n_i : messages
$n_i \approx p_i n \pm O(\sqrt{n})$
Shannon entropy $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$
Von Neumann $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$
Shannon's Source Coding Thm:
Suppose we have a protocol to encode n messages from a source with entropy H, s.t. prob(failure) → 0 as n → ∞. Then the scheme uses ≥ nH + o(n) bits, and ∃ protocol that achieves this
Quantum Schumacher compression
Source outputs quantum states $|\psi_i\rangle$ with prob p_i
Summarize with density matrix
$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

messages are very unlikely

n_i : messages

$n_i \simeq p_i n \pm O(\sqrt{n})$

Shannon entropy $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$

Von Neumann $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$

Compress to $n H($

non's Source Coding Thm:

Suppose we have a protocol =

encode n messages from a source
entropy H, s.t. prob(failure) → 0
n → ∞. Then the scheme uses
nH + o(n) bits, and ∃ protocol
that achieves this

Quantum Schumacher compression

Source outputs quantum states $|\psi_i\rangle$ with prob p_i

Summarize with density matrix

$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Compression

Diagonalize ρ

In that basis, does classical block coding

⇒ Uses $S(\rho)\, n$ qubits

Entropy

Von Neumann $S(\rho) = -\mathrm{tr}\,\rho \log_2 \rho$

compression

quantum

prob. p_i

matrix

$|\psi_i\rangle\langle\psi_i|$

Compression

Diagonalize ρ

In that basis, does classical block coding

$\Rightarrow$ Uses $S(\rho)n$ qubits

- Alice sets entangled states with R. (reference system R.)

Bob's output BR should have fidelity $\to 1$ with AR as $n \to \infty$

Entropy

Von Neumann $S(\rho) = -\mathrm{tr}\,\rho \log_2 \rho$

compression

quantum

th prob p_i

ty matrix

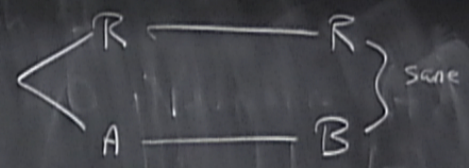
$\rangle\langle i|$

Compression

Diagonalize ρ

In that basis, does classical block coding

$\Rightarrow$ Uses $S(\rho)n$ qubits



- Alice sets entangled states with reference system R.

Bob's output BR should have fidelity $\to 1$ with AR as $n \to \infty$

Entropy

Von Neumann $S(\rho) = -\mathrm{tr}\,\rho \log_2 \rho$

...tum:

...acher compression

...utputs quantum

$|\psi_i\rangle$ with prob. p_i

...h density matrix

$\sum_i p_i |\psi_i\rangle\langle\psi_i|$

Compression

Diagonalize ρ

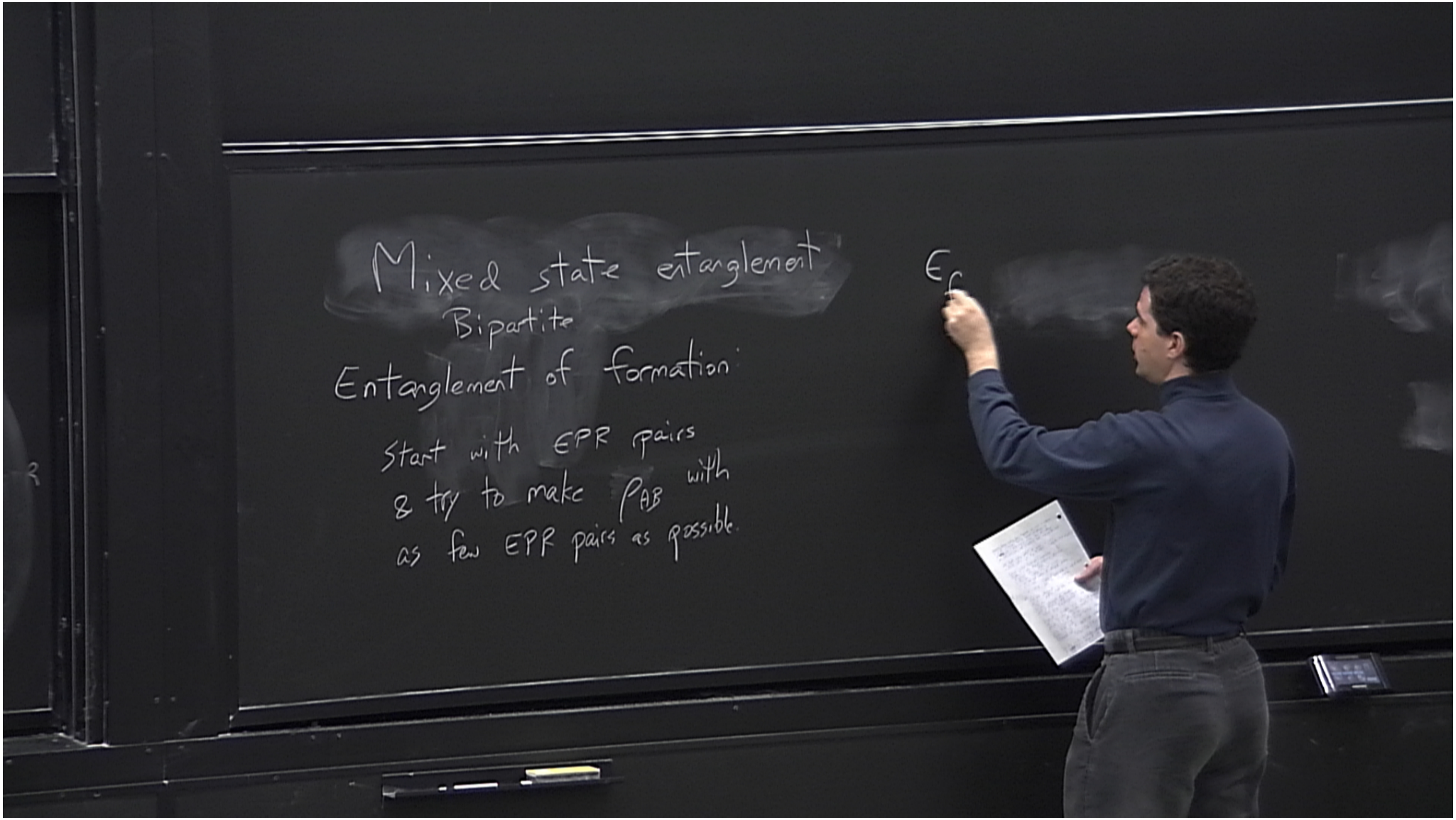
In that basis, does

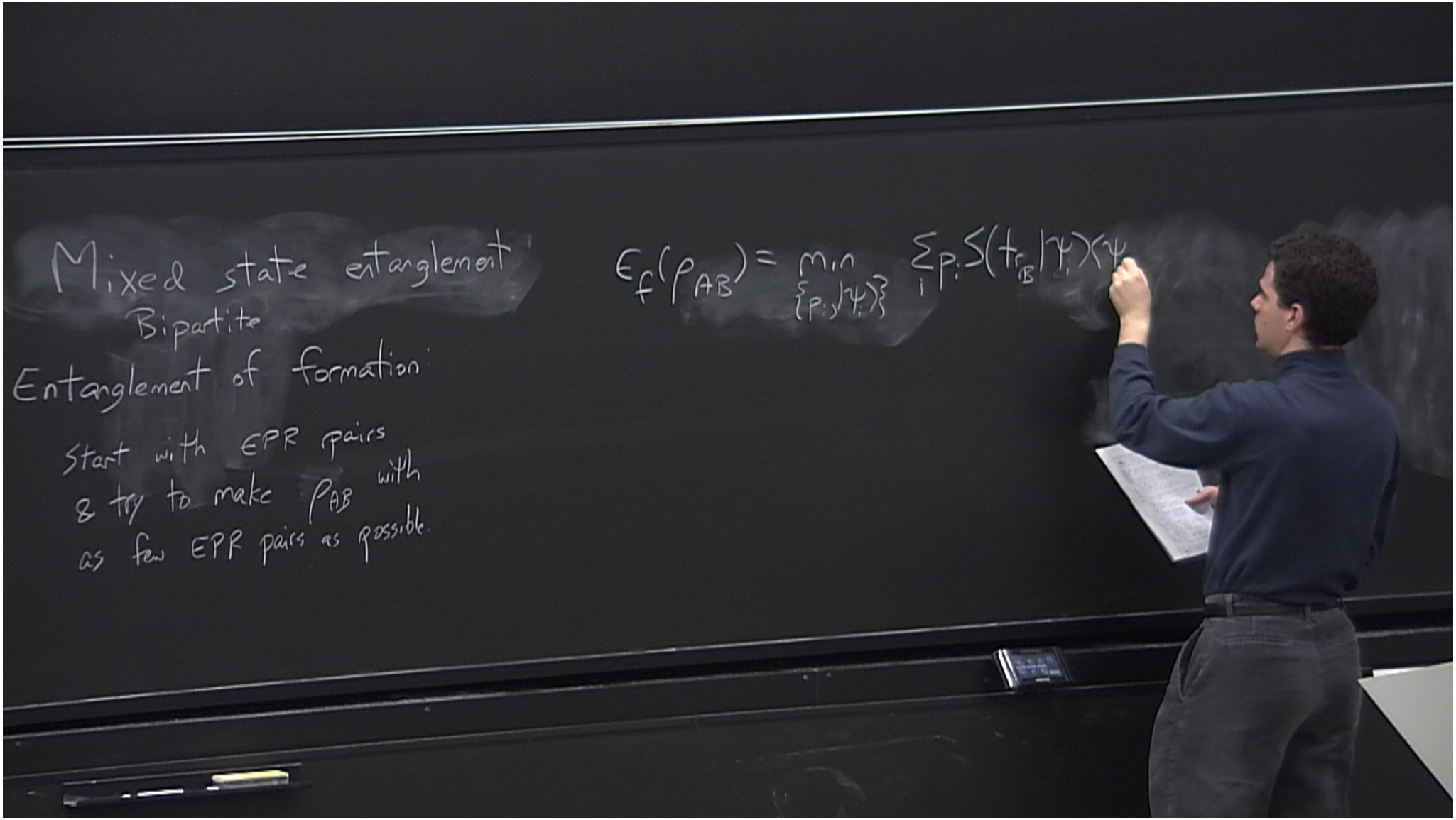
classical block coding.

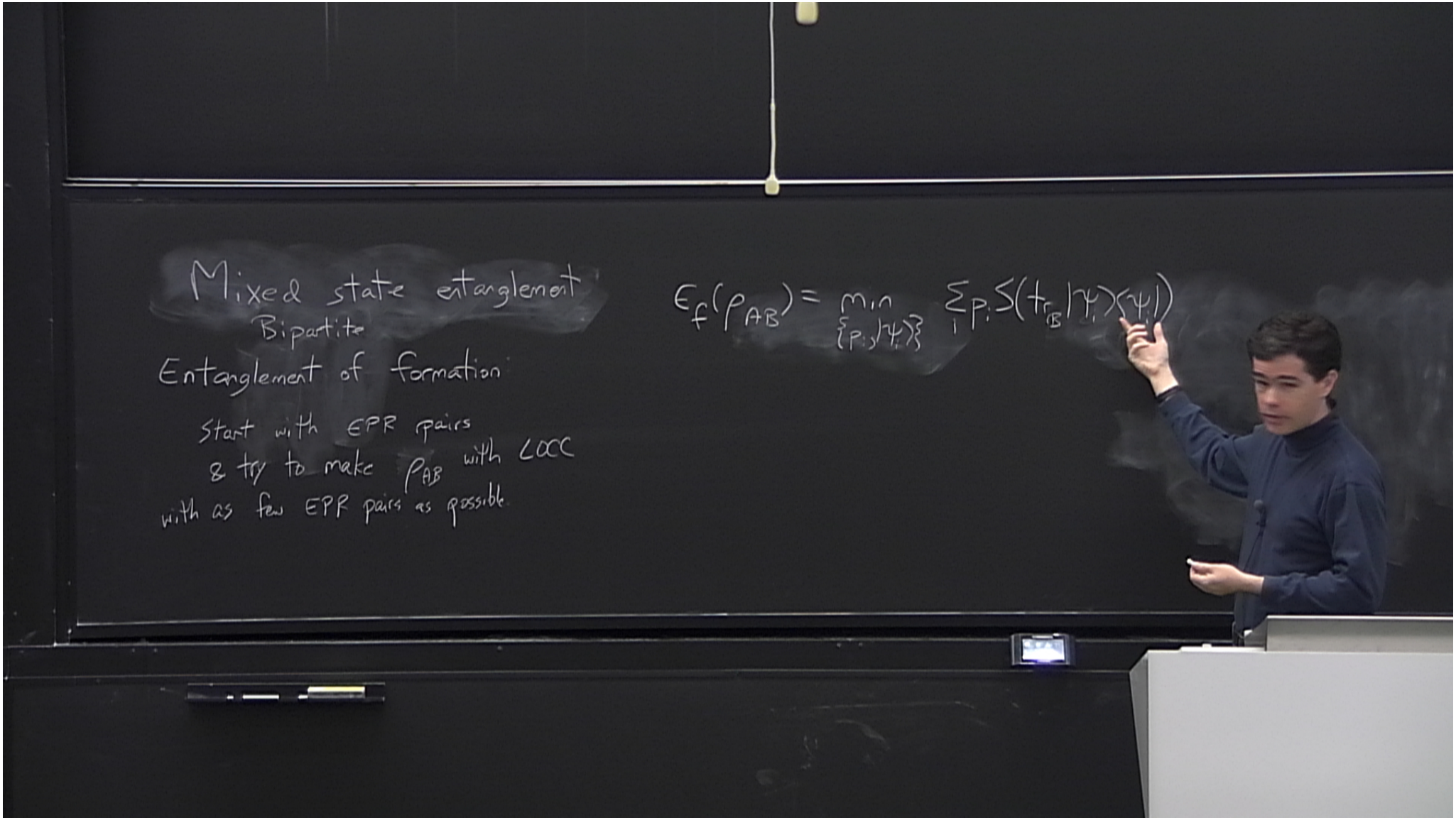
$\Rightarrow$ Uses $S(\rho)n$ qubits

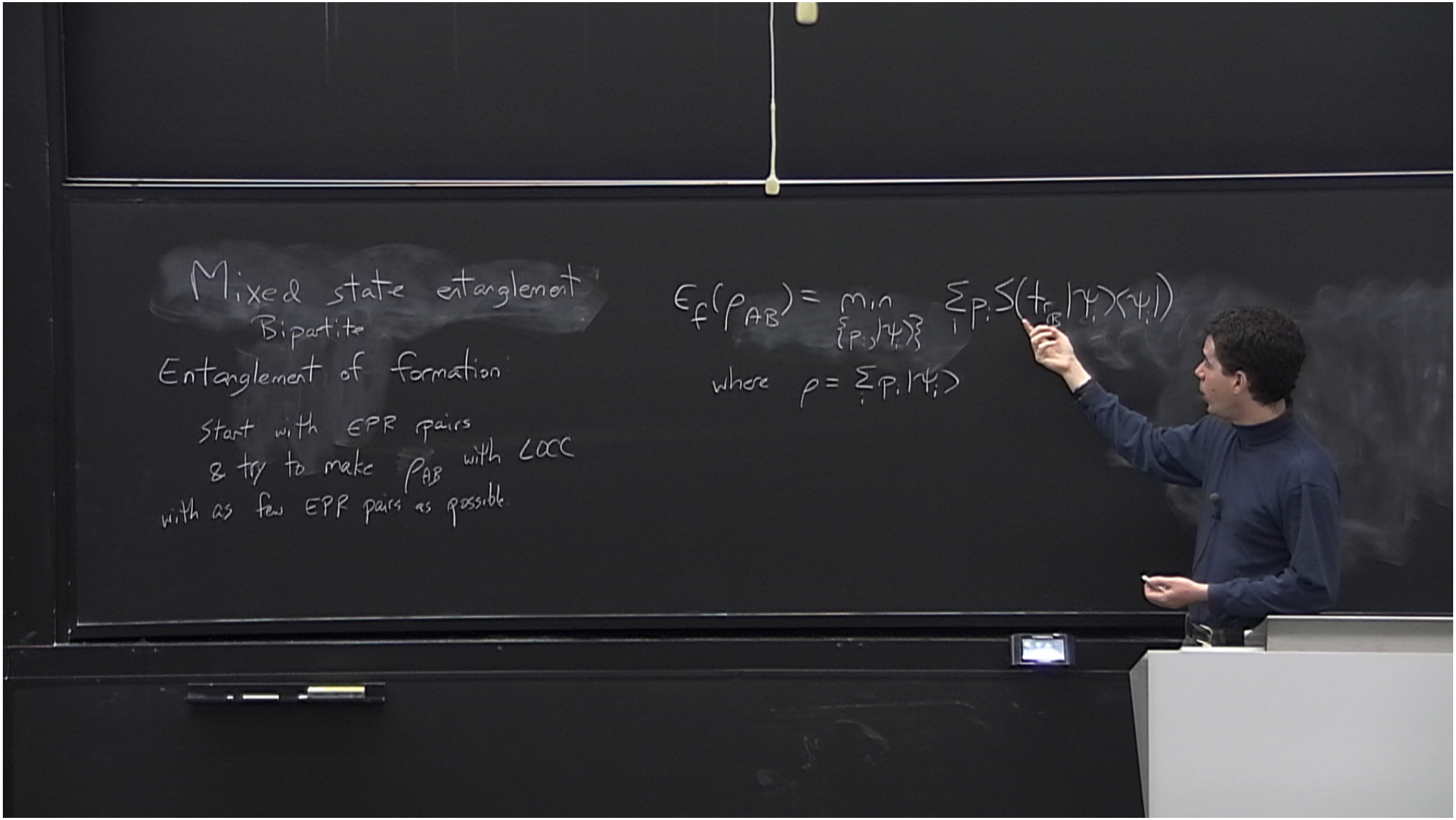
Alice gets entangled states with reference system R.

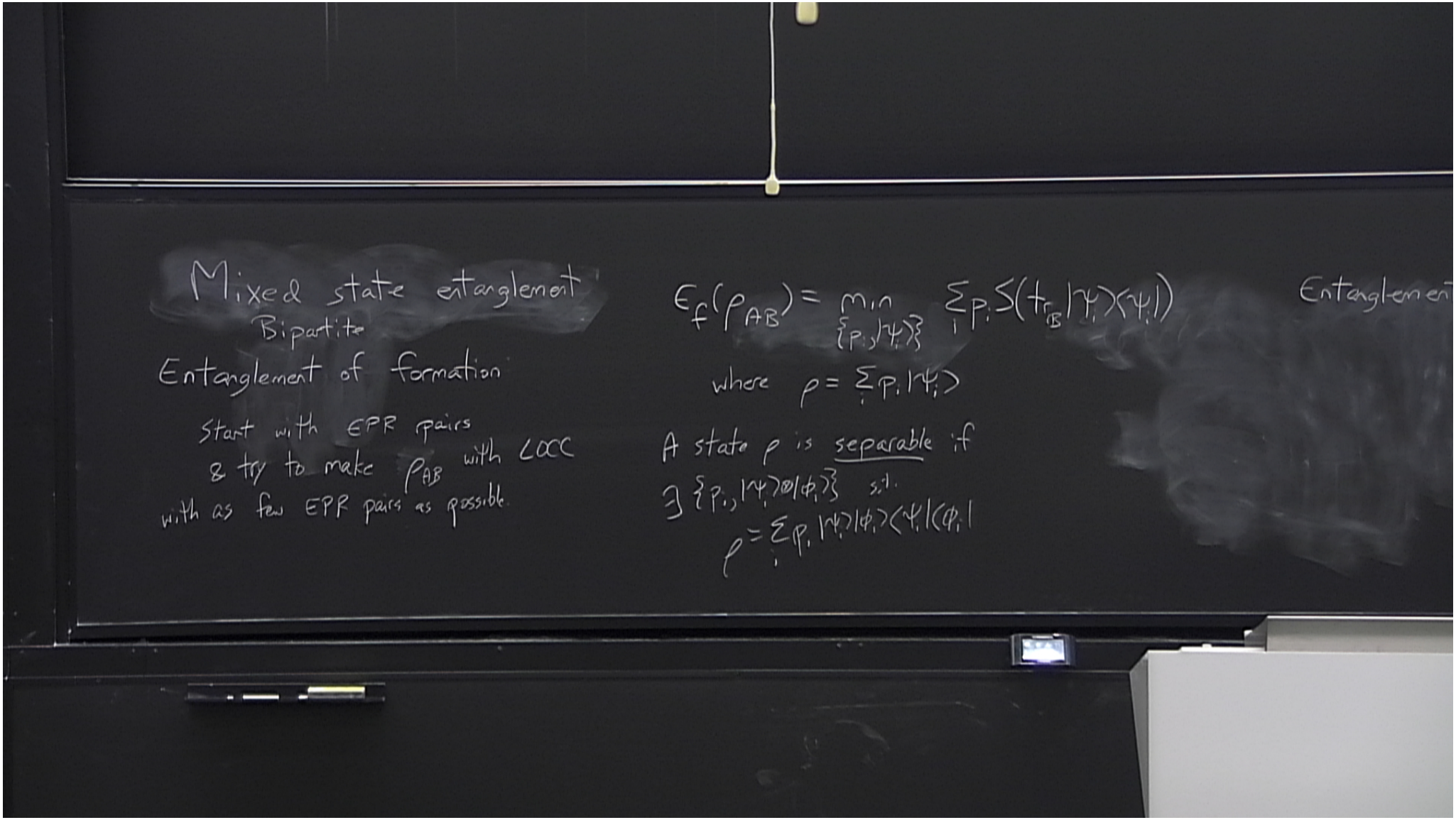
Bob's output BR should have fidelity $\to 1$ with AR as $n \to \infty$

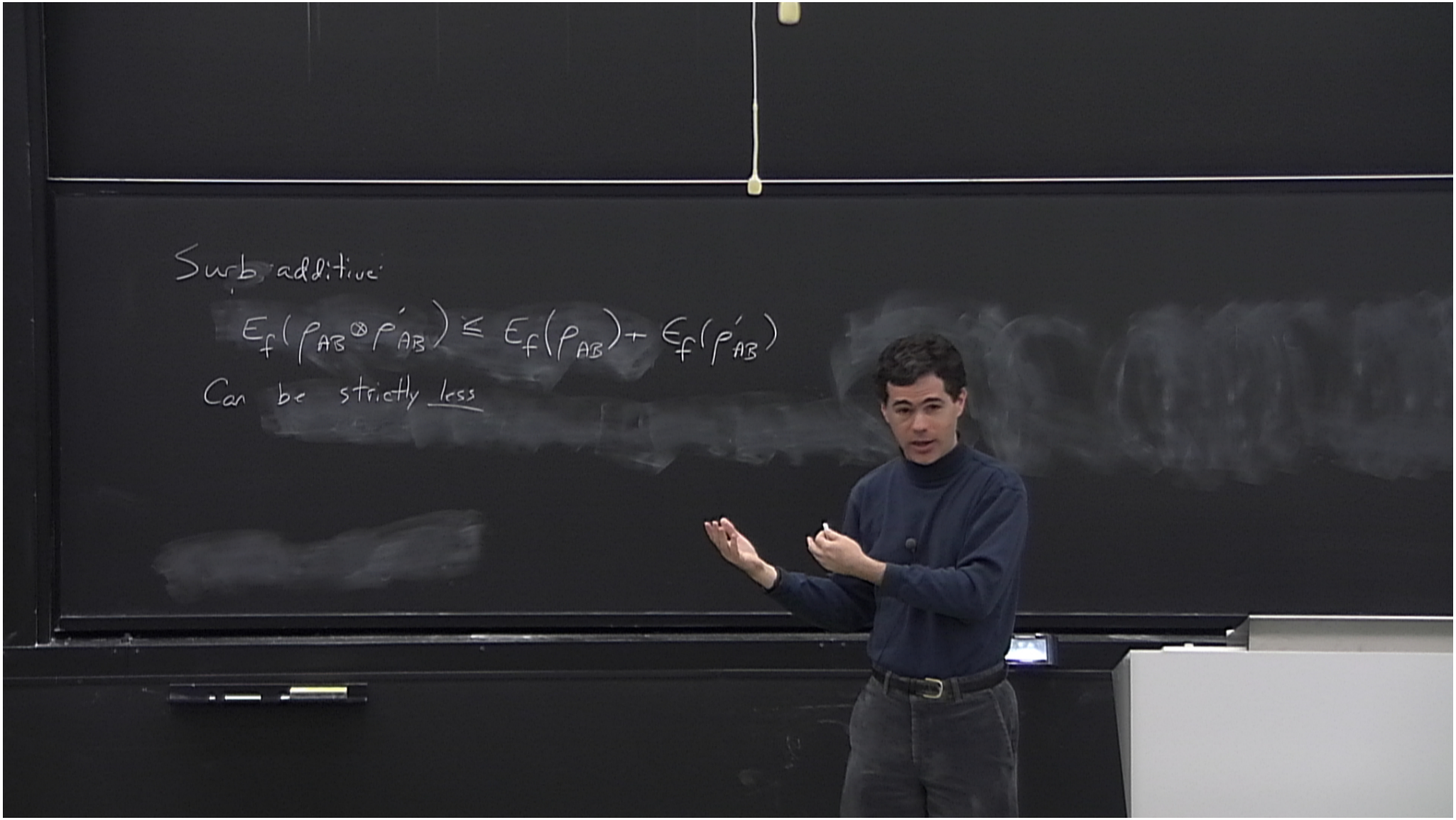

Mixed state entanglement
Bipartite
Entanglement of formation
Start with EPR pairs
& try to make ρ_{AB} with
as few EPR pairs as possible.
E_f

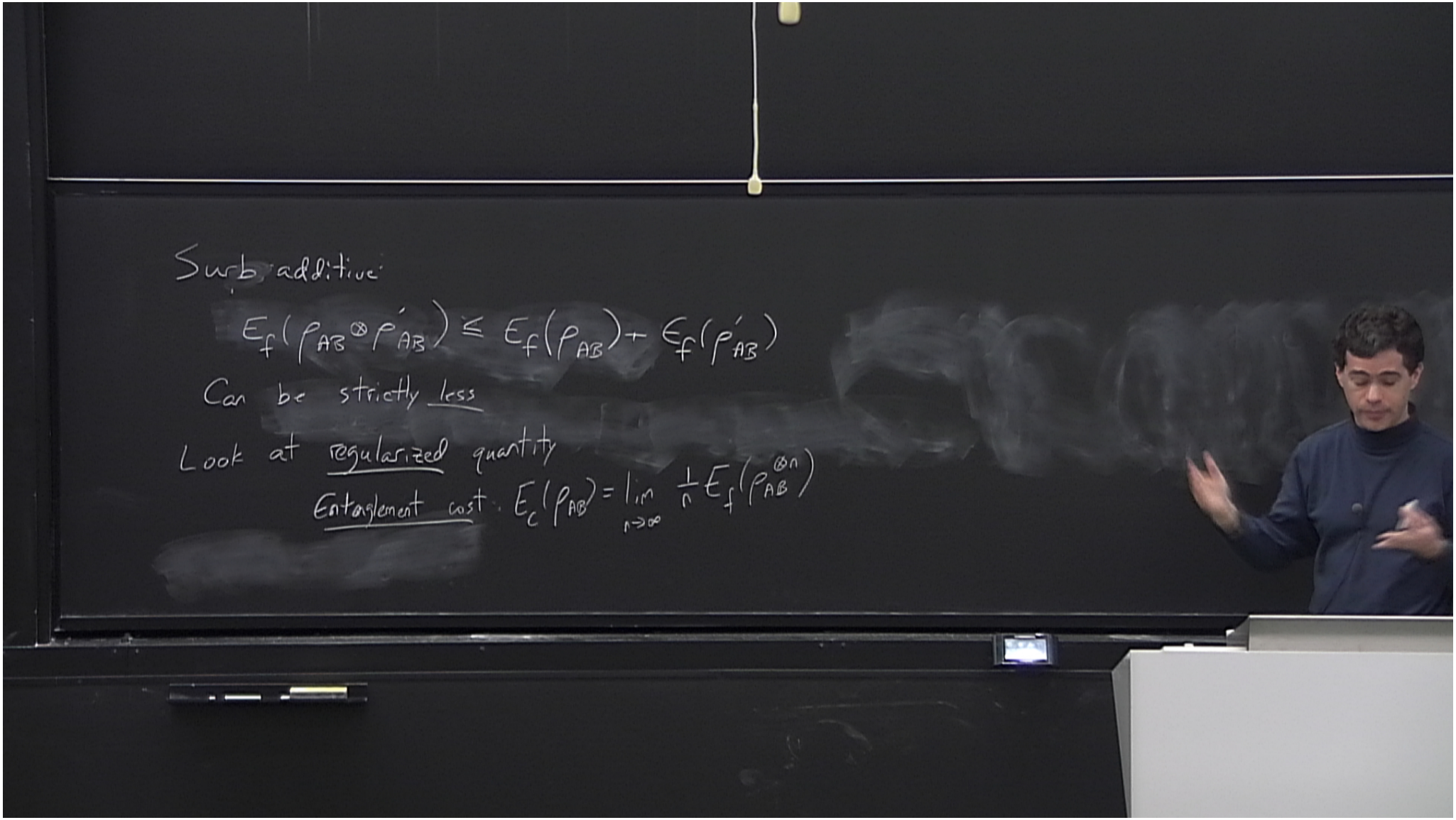

Mixed state entanglement
Bipartite
Entanglement of formation:
Start with EPR pairs
& try to make ρ_{AB} with
as few EPR pairs as possible.
$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{tr}_B |\psi_i\rangle\langle\psi$

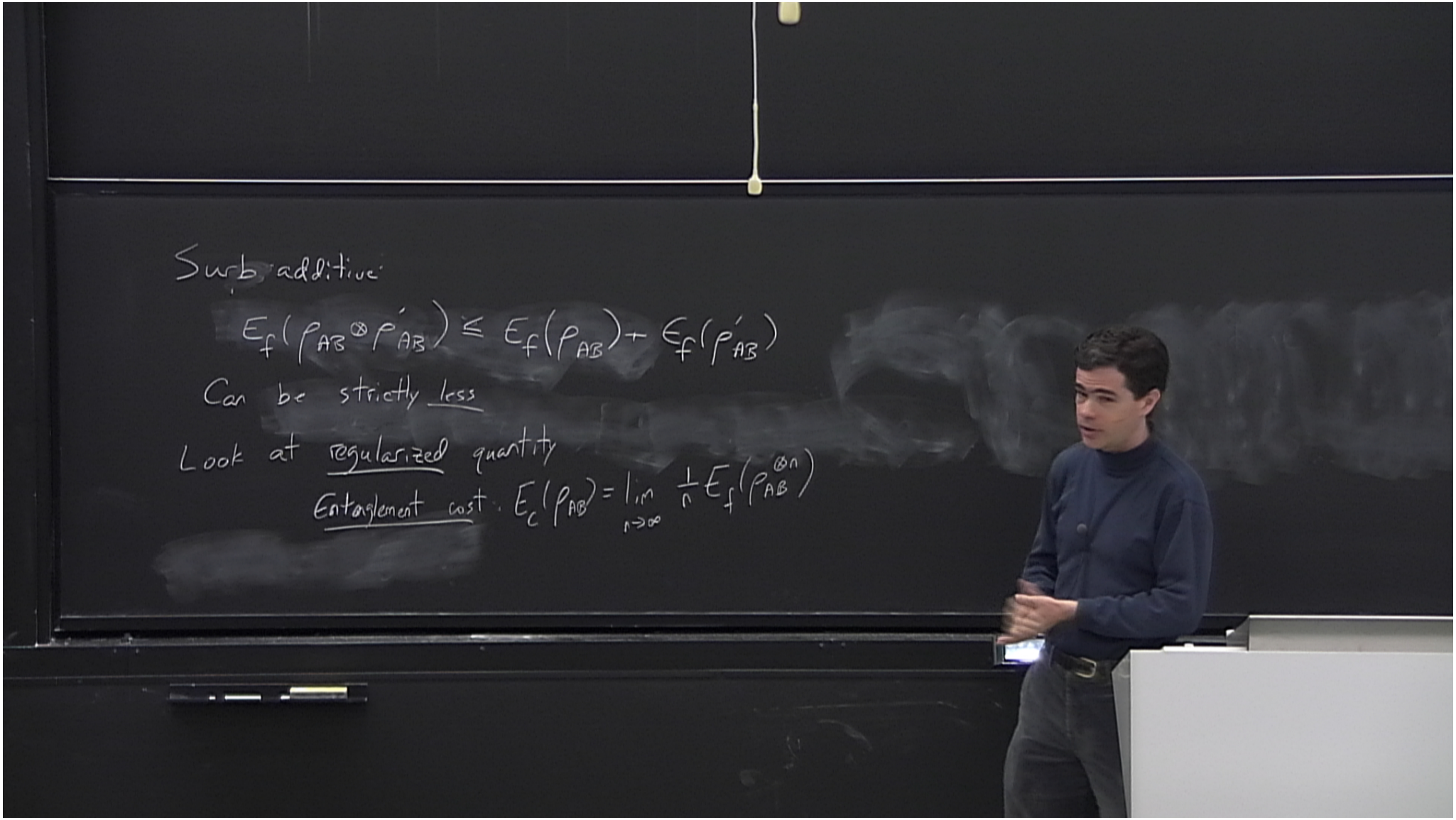

Mixed state entanglement
Bipartite
Entanglement of formation
Start with EPR pairs
& try to make ρ_{AB} with LOCC
with as few EPR pairs as possible
$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{tr}_B |\psi_i\rangle\langle\psi_i|)$

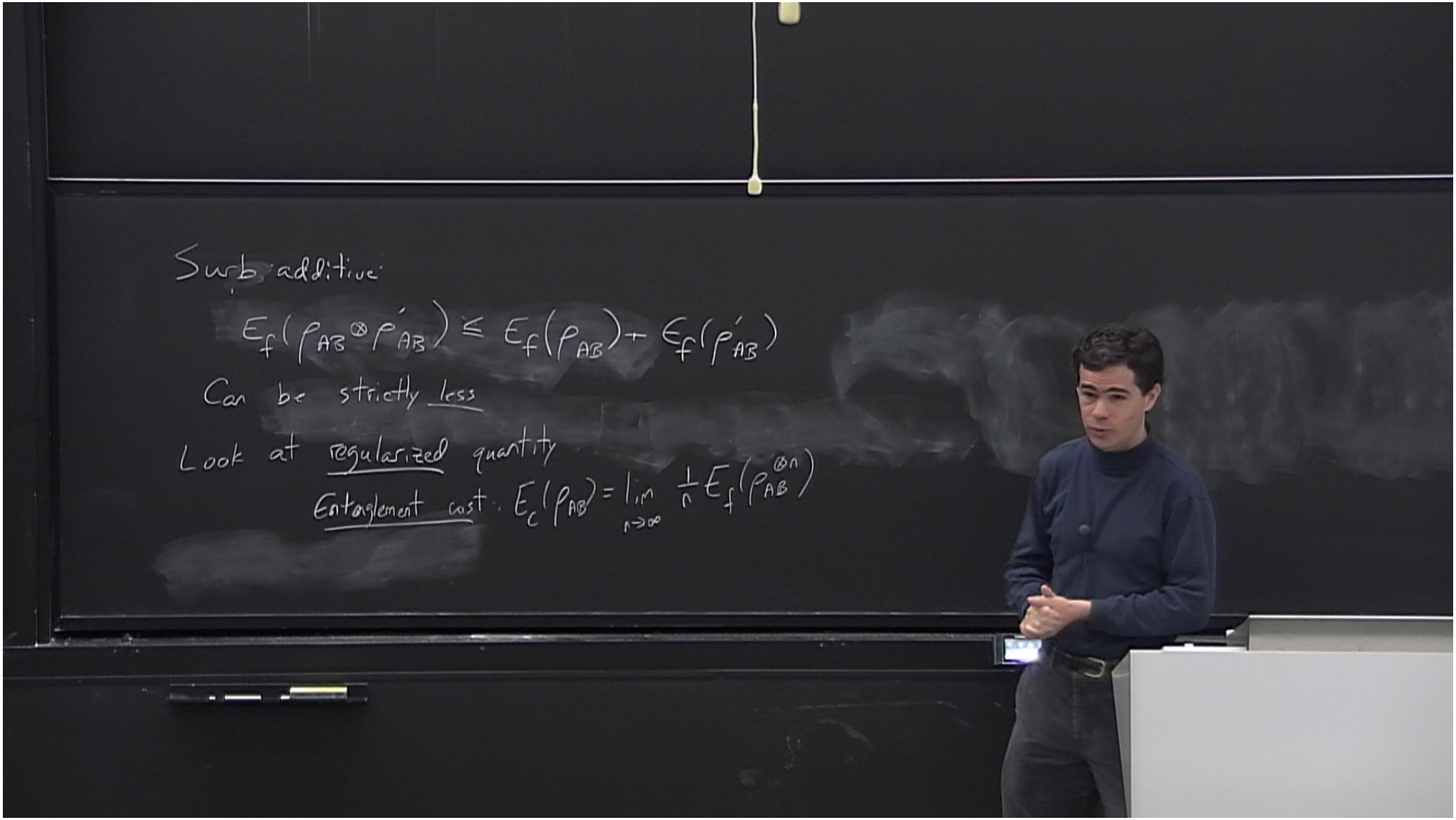

Mixed state entanglement
Bipartite
Entanglement of formation
Start with EPR pairs
& try to make ρ_{AB} with LOCC
with as few EPR pairs as possible
$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{tr}_B |\psi_i\rangle\langle\psi_i|)$
where $\rho = \sum_i p_i |\psi_i\rangle$

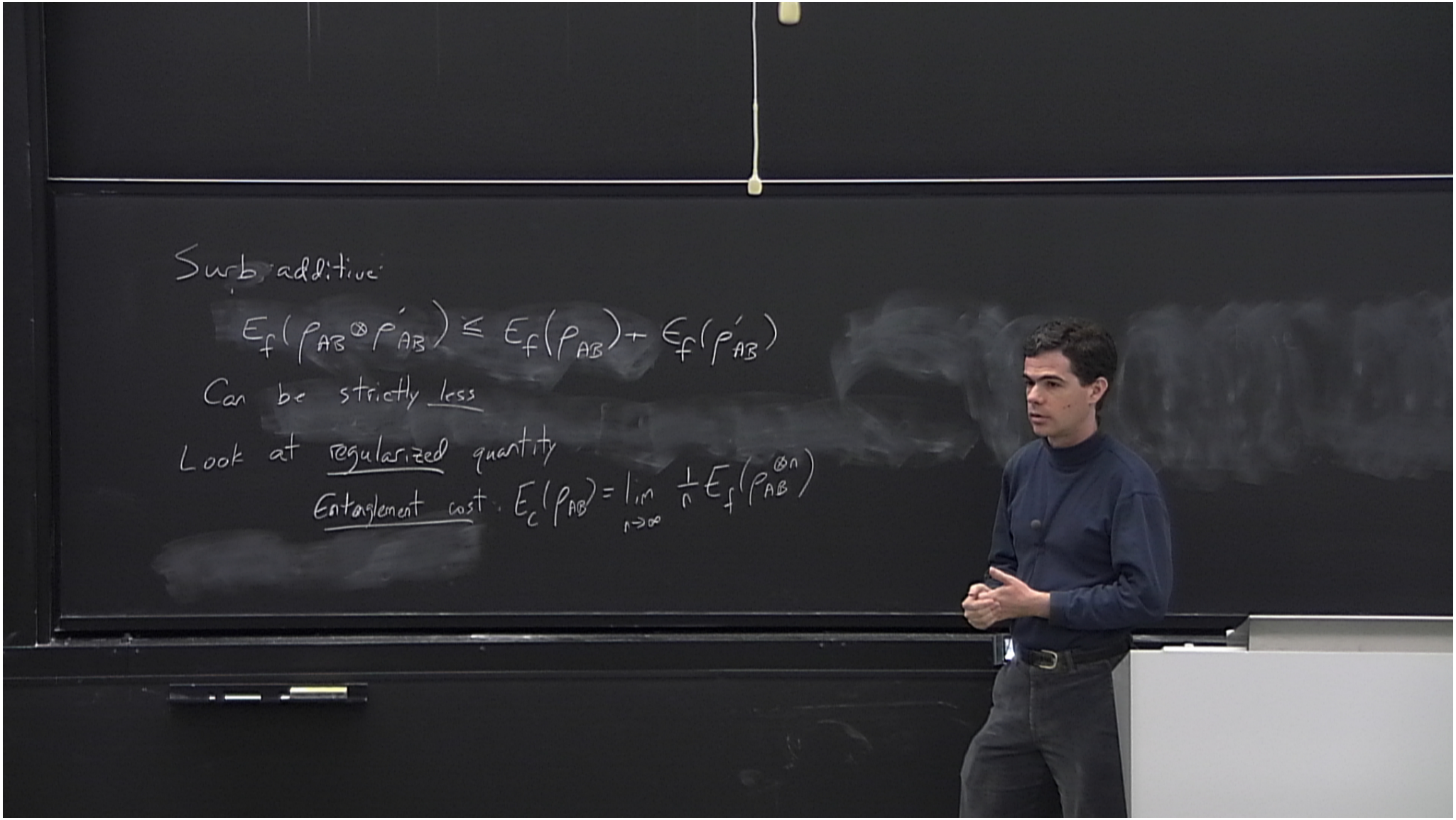

Mixed state entanglement
Bipartite
Entanglement of formation
Start with EPR pairs
& try to make ρ_{AB} with LOCC
with as few EPR pairs as possible
$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{tr}_B |\psi_i\rangle\langle\psi_i|)$
where $\rho = \sum_i p_i |\psi_i\rangle$
A state ρ is separable if
$\exists \{p_i, |\psi_i\rangle \otimes |\phi_i\rangle\}$ s.t.
$\rho = \sum_i p_i |\psi_i\rangle|\phi_i\rangle\langle\psi_i|\langle\phi_i|$
Entanglement


Subadditive
$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB})$
Can be strictly less


Subadditive
$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB})$
Can be strictly less
Look at regularized quantity
Entanglement cost $E_c(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$


Subadditive
$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB})$
Can be strictly less
Look at regularized quantity
Entanglement cost $E_c(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$


Subadditive
$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB})$
Can be strictly less
Look at regularized quantity
Entanglement cost $E_c(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$


Subadditive
$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB})$
Can be strictly less
Look at regularized quantity
Entanglement cost $E_c(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n})$