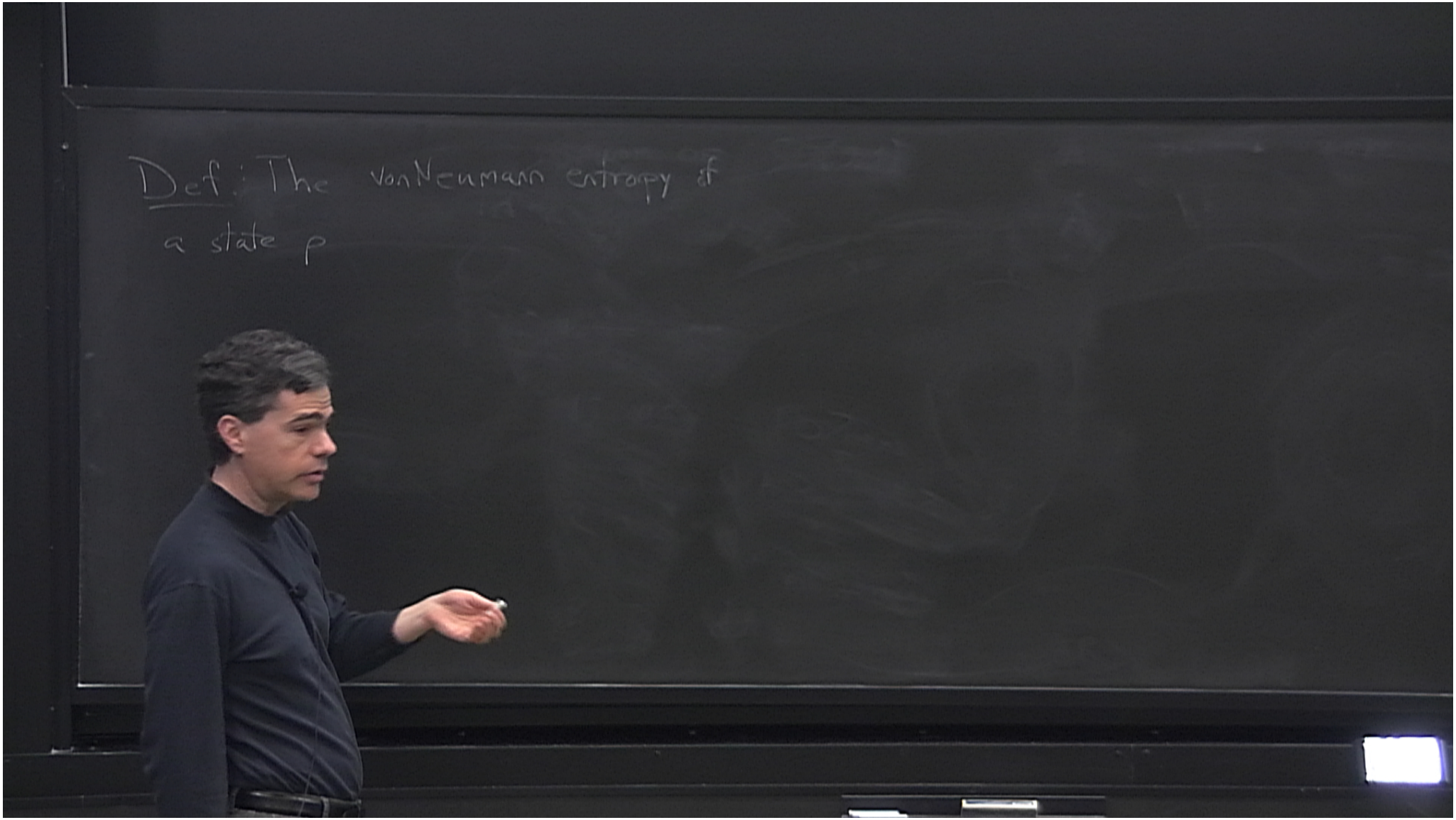
Title: PSI 2017/2018 - Quantum Information - Lecture 13

Date: Mar 08, 2018 11:30 AM

URL: http://pirsa.org/18030026

Abstract:


Def: The von Neumann entropy of
a state ρ

Def: The von Neumann entropy of a state ρ is $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$.

The Shannon entropy of a probability distribution $\{p_i\}$ is $H(\{p_i\}) = -\sum_i p_i \log p_i$.

$S(A) = S(\rho_A)$, $\rho_A = \mathrm{tr}_{\overline{A}} \rho$

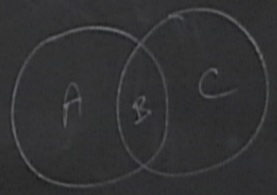
$S(A,B) = S(\rho_{AB})$, $\rho_{AB} = \mathrm{tr}_{\overline{AB}} \rho$

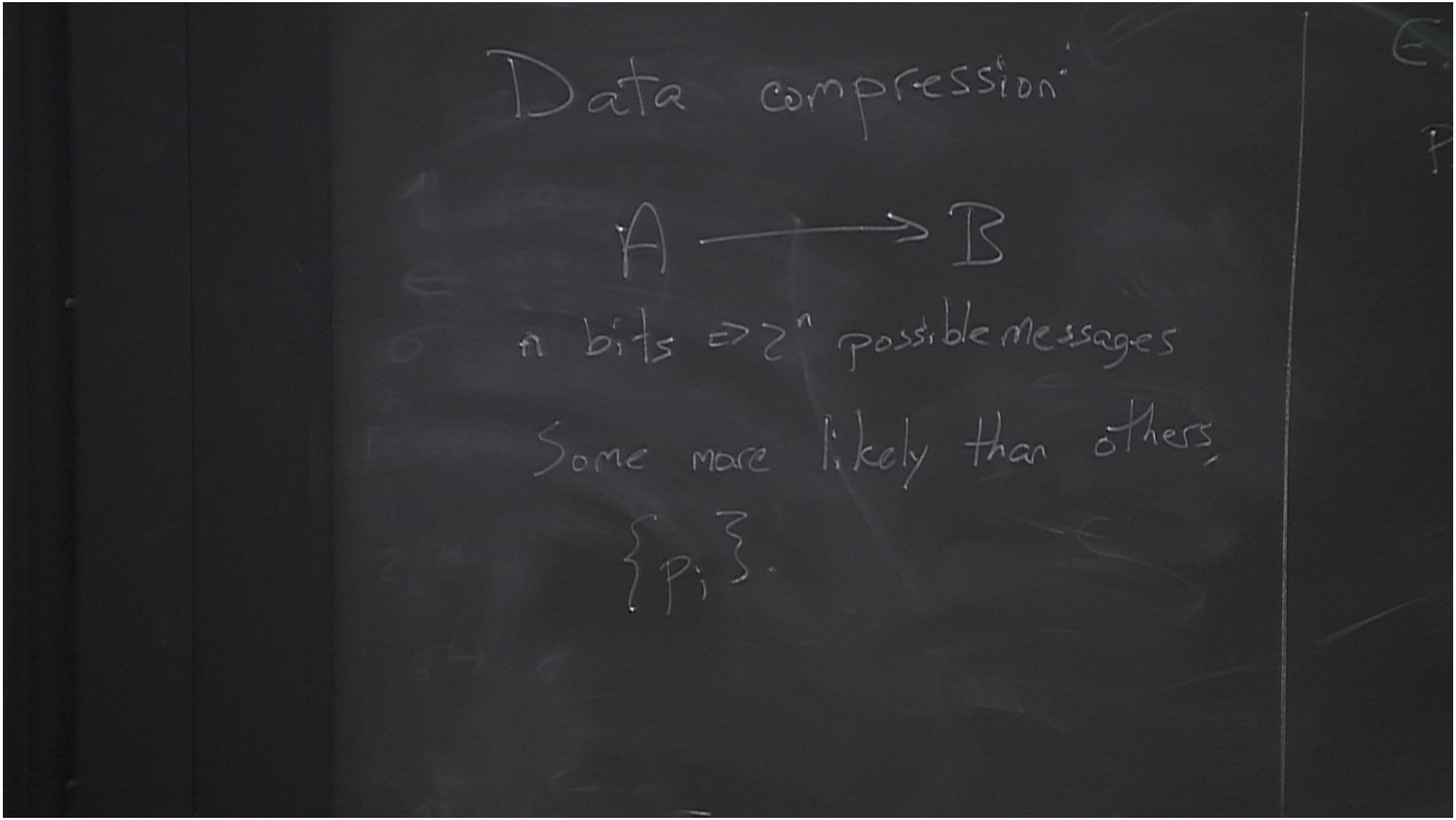
Properties of $S(\rho)$:

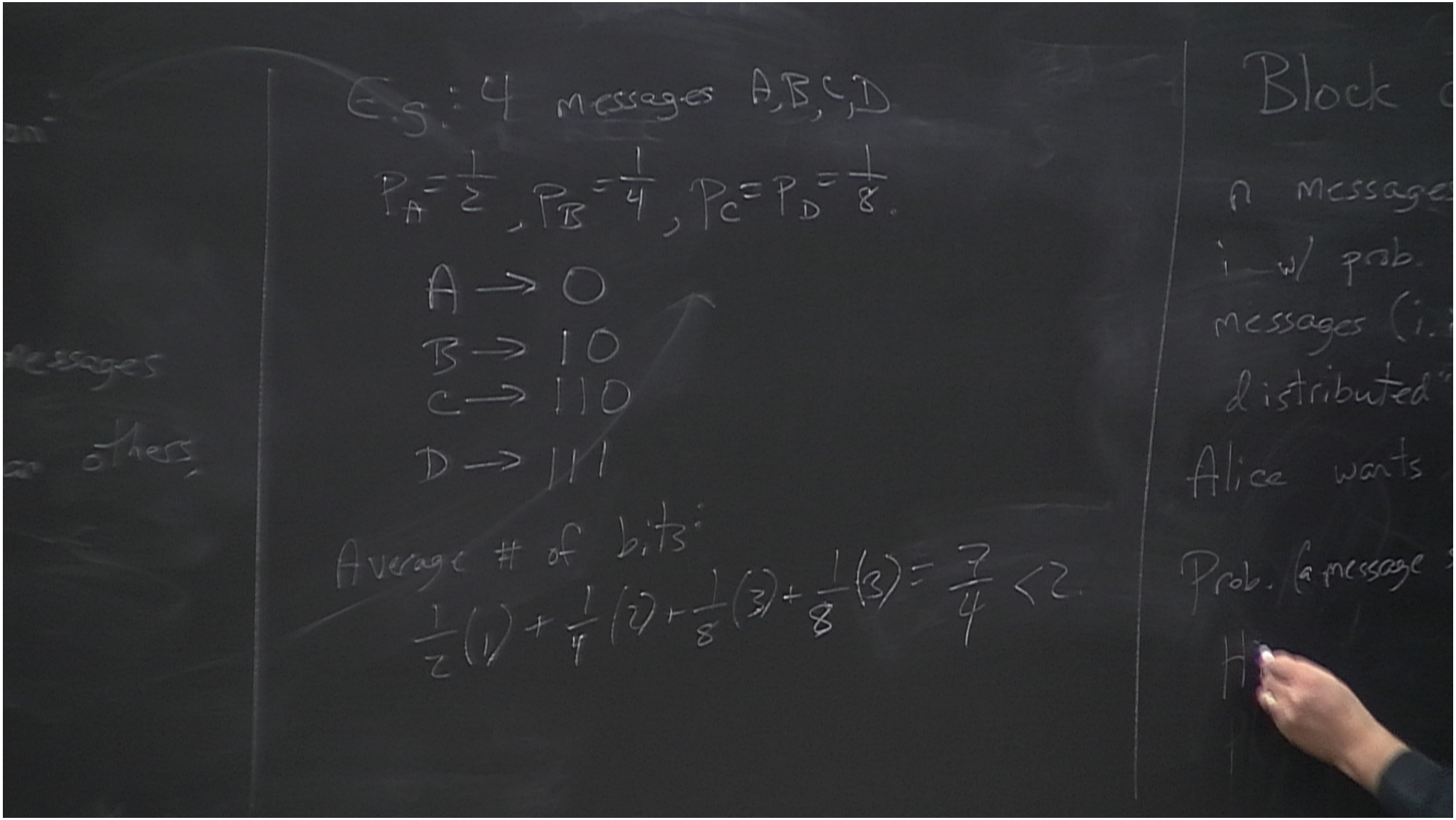
1. If Hilbert space has dimension D, $S(\rho) \leq \log D$.
   = when $\rho = I/D$.
2. $S(\rho) = 0$ iff ρ is a pure state.
3. Triangle inequality / Araki-Lieb inequality: $S(A,B) \geq |S(A) - S(B)|$
4. Subadditivity: $S(A,B) \leq S(A) + S(B)$.

Properties of $S(\rho)$:

1. If Hilbert space has dimension D, $S(\rho) \leq \log D$.
   = when $\rho = I/D$.
2. $S(\rho) = 0$ iff ρ is a pure state.
3. Triangle inequality / Araki-Lieb inequality: $S(A,B) \geq |S(A) - S(B)|$
4. Subadditivity: $S(A,B) \leq S(A) + S(B)$.
5. Strong subadditivity: $S(A,B,C) \leq S(A,B) + S(B,C) - S(B)$
6. For a global pure state of AB, $S(A) = S(B)$.




Data compression
A → B
n bits ⇒ 2^n possible messages
Some more likely than others
{p_i}.


E.g.: 4 messages A, B, C, D
$P_A = \frac{1}{2}$, $P_B = \frac{1}{4}$, $P_C = P_D = \frac{1}{8}$.
A → 0
B → 10
C → 110
D → 111
Average # of bits:
$\frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{8}(3) + \frac{1}{8}(3) = \frac{7}{4} < 2$.
Block
n messages
i w/ prob.
messages (i.
distributed
Alice wants
Prob. (a message

Block coding

n messages, each message is i w/ prob. p_i, independent of other messages (i.i.d. source = "independent identically distributed")

Alice wants to send Bob typical cases

Prob. (a message sequence w/ n_i i messages) $= \prod_i p_i^{n_i}$

Highly peaked around $n_i \approx p_i n$.

Let typ

are those

Tot

$= \frac{7}{4} < 2$

Let typical set of message sequences are those with $|n_i - p_i n| = o(n)$

Total number of such typical sequences is $2^{nH(\{p_i\})}$

Compression scheme: Say which typical message sequence you have.

Requires $nH(\{p_i\})$.

Block coding

n messages, each message is i w/ prob. p_i, independent of other messages (i.i.d. source = "independent identically distributed")

Alice wants to send Bob typical cases

Prob. (message sequence w/ n_i i messages) $= \prod_i p_i^{n_i}$

Highly peaked around $n_i \approx p_i n$

Let typical set of message sequences are those with $|n_i - p_i n| = o(n)$

Total number of such typical sequences is $\geq 2^{nH(\{p_i\})}$

Compression scheme: Say which typical message sequence you have

Requires $nH(\{p_i\})$.

Shannon's source coding theorem: Suppose we have a scheme to encode n messages from an i.i.d. source with entropy H with asymptotic failure prob. $\to 0$ as $n \to \infty$. Then the scheme uses $\geq nH + o(n)$ bits & $\exists$ compression schemes

Block coding

n messages, each message is
i w/ prob p_i, independent of other messages (i.i.d. source = "independent identically distributed")

Alice wants to send Bob typical cases

Prob. (message sequence w/ n_i i messages) $= \prod_i p_i^{n_i}$

Highly peaked around $n_i \approx p_i n$

Let typical set of message sequences are those with $|n_i - p_i n| = o(n)$

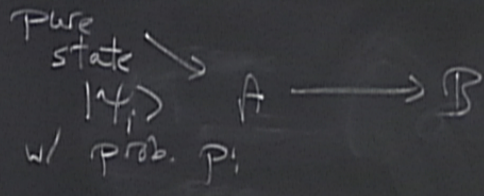
Total number of such typical sequences is $\approx 2^{nH(\{p_i\})}$

Compression scheme: Say which typical message sequence you have.

Requires $nH(\{p_i\})$.

Shannon's source coding theorem: Suppose we have a scheme to encode n messages from an i.i.d. source with entropy H with asymptotic failure prob. $\to 0$ as $n \to \infty$. Then the scheme uses $\geq nH + o(n)$ bits & $\exists$ compression schemes that do this

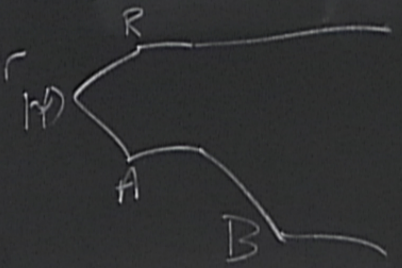
Quantum data compression



A is receiving $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

B should reconstruct a state with high fidelity to $|\psi_{i_0}\rangle \otimes |\psi_{i_1}\rangle \otimes \ldots$

Or

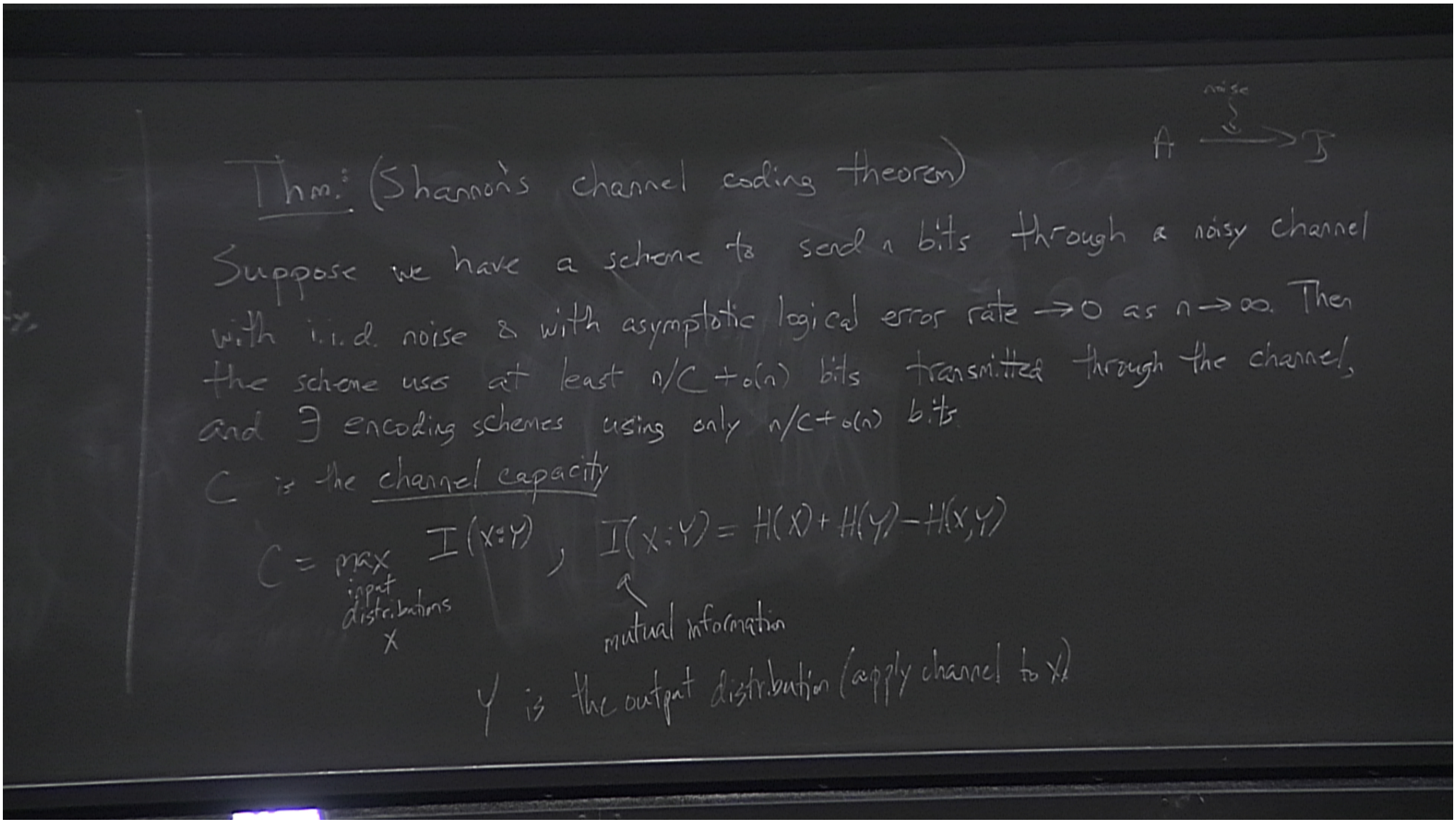


$\mathrm{tr}_R |\psi\rangle\langle\psi| = \rho$

Schumacher compression:

Diagonalize ρ, then do classical compression (reversibly, erasing scratch bits).

Optimal compression scheme achieves asymptotically $nS(\rho)$ qubits for n messages.


Thm: (Shannon's channel coding theorem)
noise
A
B
Suppose we have a scheme to send n bits through a noisy channel with i.i.d. noise & with asymptotic logical error rate → 0 as n → ∞. Then the scheme uses at least n/C + o(n) bits transmitted through the channel, and ∃ encoding schemes using only n/C + o(n) bits
C is the channel capacity
C = max I(X:Y), I(X:Y) = H(X) + H(Y) − H(X,Y)
input distr. X
mutual information
Y is the output distribution (apply channel to X)