Title: PSI 2018/2019 - Quantum Information Review - Lecture 14

Speakers: Daniel Gottesman

Collection: PSI 2018/2019 - Quantum Information Review (Gottesman)

Date: March 21, 2019 - 11:30 AM

URL: http://pirsa.org/19030051

Authentication:

$A_k : m \longmapsto (m, \sigma_k(m))$

$V_k : (m, \sigma) \longmapsto$ yes/no

Completeness: $V_k(m, \sigma_k(m)) =$ yes

Soundness: $\forall E : (m, \sigma_k(m)) \longmapsto (m', \sigma)$, $m' \neq m$

w/ high prob. (k) $V_k(E(m, \sigma_k(m))) =$ no.

Von Neuman Entropy:

Given ρ, $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$.

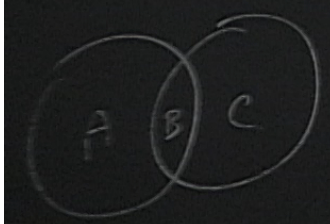
Shannon entropy: $H(\{p_i\}) = -\sum_i p_i \log_2 p_i$.

$$S(\rho_A) = S(A). \qquad S(\rho_{AB}) = S(A,B)$$

Properties of $S(\rho)$:

1. On a Hilbert space of dim D, $S(\rho) \le \log D$. $=$ when $\rho = \frac{I}{D}$
2. $S(\rho) \ge 0$. $S(\rho) = 0$ iff ρ is a pure state.
3. Triangle inequality or Araki-Lieb inequality: $S(A,B) \ge |S(A) - S(B)|$.
4. Subadditivity: $S(A,B) \le S(A) + S(B)$ $=$ if uncorrelated.
5. Strong subadditivity: $S(A,B,C) \le S(A,B) + S(B,C) - S(B)$.
6. If ρ_{AB} is pure, then $S(A) = S(B)$.

$\sum_i p_i \log_2 p_i$.



Data compression:

Classical

$A \longrightarrow B$

maximize # messages / channel use.

Example:

Alice has 4 possible messages:

A w/ prob. $\frac{1}{2}$

B w/ prob. $\frac{1}{4}$

C w/ prob. $\frac{1}{8}$

D w/ prob. $\frac{1}{8}$

Naive encoding: 2 bits per message

ssible messages:

$\frac{1}{2}$

$\frac{1}{4}$

$\frac{1}{8}$

bits per message

$A \longrightarrow 0$

$B \longrightarrow 10$

$C \longrightarrow 110$

$D \longrightarrow 111$

$$\text{Average \# bits} = \frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{8}(3) + \frac{1}{8}(3)$$

$$= 1\frac{3}{4} < 2$$

$\frac{1}{8}(3) + \frac{1}{8}(3)$

Block coding:

Independent identically distributed (i.i.d) source.

$\{p_i\}$ If n messages, prob. of getting n_i i messages in a particular sequence

$$\prod_i p_i^{n_i}$$

Any sequence w/ $\{n_i\}$: $\frac{n!}{\prod_i n_i!} \prod_i p_i^{n_i} \longrightarrow n_i \approx p_i n$

Typical set

$$\log \frac{n!}{\prod_i (p_i n)!} \approx n \log n - \sum_i (p_i n) \log (p_i n)$$

$$= n \log n - \sum_i (p_i n)(\log p_i + \log n)$$

$$= \cancel{n \log n} - \cancel{\left(\sum_i p_i\right) n \log n} - \sum_i p_i n \log p_i$$

$$= n H(\{p_i\})$$

Thm: (Shannon's Source Coding Theorem)

Suppose we have an i.i.d. source w/ entropy H & we want to encode n messages w/ prob. of failure $\to 0$ as $n \to \infty$. Then we need at least $nH - o(n)$ bits & exist compression schemes using only $nH + o(n)$ bits.

Typical set

curary)

) entropy H

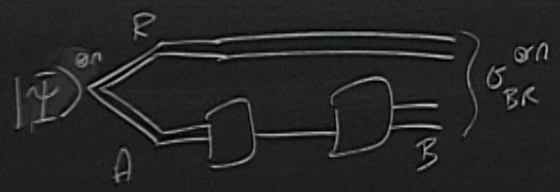
b. of failure $\to 0$

$nH - o(n)$ bits

$nH + o(n)$ bits

Schumacher compression:

p_i of $|\psi_i\rangle \rightsquigarrow \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.



Want $\sigma_{BR}^{\otimes n}$ to have high fidelity to $|\Psi\rangle_{AR}^{\otimes n}\langle\Psi|_{AR}^{\otimes n}$

Achieve by diagonalizing ρ. Use classical protocol $\Rightarrow$ Need $S(\rho)n$ qubits.

$$C = \max_{\text{distr. } X} I(X:Y)$$

with X is prob. distribution over channel inputs (single use)

Y is prob. distribution of channel outputs if you put X through the noisy channel

$$I(X:Y) = H(X) + H(Y) - H(X,Y)$$

Mutual information