Quantum

Lecture 8

- Shannon's channel capacity
- Classical information over quantum channel
- Quantum information over quantum channel

Shannon's Channel Capacity

A discrete memoryless channel (DMC) with (finite) input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, is described by a conditional pmf $p(y|x)$

For a fixed n, the channel takes input sequences $X^n \in \mathcal{X}^n$ and maps them to output sequences $Y^n \in \mathcal{Y}^n$

For $X^n = x^n$ the random sequence Y^n is described by

$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i)$$

Define an (M, n) block channel code for a DMC by

1. An index set $\mathcal{I}_M = \{1, \ldots, M\}$
2. An encoder mapping $\mathcal{E} : \mathcal{I}_M \to \mathcal{X}^n$. The set

$$\{x^n : x^n = \mathcal{E}(i),\ i \in \mathcal{I}_M\}$$

   of codewords is called the codebook
3. A decoder mapping $\mathcal{D} : \mathcal{Y}^n \to \mathcal{I}_M$

The rate of the code is

$$R = \frac{\log M}{n} \quad \text{[bits per channel use]}$$

An information symbol I is chosen uniformly from $\in \mathcal{I}_M$

If $I = i$, the codeword $x^n(i) = \mathcal{E}(i)$ is sent through the channel

The received sequence Y^n is decoded as $\mathcal{D}(Y^n) \in \mathcal{I}_M$

The average error probability is

$$P_e^{(n)} = 1 - \frac{1}{M} \sum_{i=1}^{M} \Pr(\mathcal{D}(Y^n) = i | I = i)$$

A rate R is achievable if there exists a sequence of (M_n, n) codes such that

$$\liminf_{n\to\infty} \frac{1}{n} \log M_n \geq R$$

and $P_e^{(n)} \to 0$ as $n \to \infty$

The capacity C is the maximum achievable rate

Shannon's coding theorem: The capacity of a DMC $p(y|x)$ is

$$\begin{aligned} C &= \max_{p(x)} I(Y;X) \\ &= \max_{p(x)} \left\{ \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p(y|x)p(x) \log \frac{p(y|x)}{\sum_{x\in\mathcal{X}} p(y|x)p(x)} \right\} \end{aligned}$$

(over pmf's $p(x)$ on $\mathcal{X}$)

Classical Information over a Quantum Channel

Consider a quantum channel (noisy quantum operation) $\mathcal{N}$ mapping states in $\mathcal{H}$ to states in $\mathcal{G}$

An (M, n) code for conveying a random $I \in \mathcal{I}_{M_n}$ is described by

1. An encoder $\mathcal{E}_n$, mapping $I \in \mathcal{I}_{M_n}$ to $\rho^{(n)} = \rho_1^{(k)} \otimes \cdots \otimes \rho_\ell^{(k)}$ with $\rho_j^{(k)} \in \mathcal{H}^{\otimes k}$ and for $n = k\ell$
2. A decoder $\mathcal{D}_n$, mapping $\sigma^{(n)} = \mathcal{N}^k(\rho_1^{(k)}) \otimes \cdots \otimes \mathcal{N}^k(\rho_\ell^{(k)})$ to $\mathcal{I}_{M_n}$, where $\mathcal{N}^k = \mathcal{N}^{\otimes k}$

A rate R is achievable if there exists a sequence $(\mathcal{E}_n, \mathcal{D}_n)$ such that

$$\liminf_{n\to\infty} \frac{1}{n} \log M_n \geq R$$

and $P_e^{(n)} = \Pr(\mathcal{D}_n(\sigma^{(n)}) \neq I) \to 0$

The capacity is the maximum achievable rate

The encoder and decoder agree on an ensemble $\{p(x), \rho_x^{(k)}\}$ and a classical codebook $\{x^\ell(i)\}$ of size M_n

For $I = i$ the encoder transmits the joint state

$$\rho^{(n)}(i) = \rho_{x_1(i)}^{(k)} \otimes \cdots \otimes \rho_{x_\ell(i)}^{(k)}$$

The decoder $\mathcal{D}_n$ is described by a measurement $\{K_i\}_{i=1}^{M_n}$, with POVM elements $E_i = K_i^* K_i$, such that $\mathcal{D}_n(\sigma^{(n)}) = i'$ when the outcome is i'

Note that

$$P_e^{(n)} = 1 - \sum_{i=1}^{M_n} \mathrm{Tr}(E_i(\mathcal{N}^k \rho_{x_1(i)}^{(k)} \otimes \cdots \otimes \mathcal{N}^k \rho_{x_\ell(i)}^{(k)}))$$

Also note that the coding happens over ℓ independent uses of the product channel $\mathcal{N}^k$, i.e. $n = k\ell$ uses of $\mathcal{N}$ in total

The equivalent DMC is $p(y|x) = \mathrm{Tr}(E_y \mathcal{N}^k \rho_x^{(k)})$

Holevo information of a channel

The Holevo information of the channel $\mathcal{N}$ is

$$\chi(\mathcal{N}) = \max_{\rho_{CQ}} \chi(p(x), \mathcal{N}(\rho_x))$$

over $\{p(x), \rho_x\}$ in the classical-quantum state

$$\rho_{CQ} = \sum_x p(x) |e(x)\rangle\langle e(x)| \otimes \mathcal{N}(\rho_x)$$

That is

$$\chi(\mathcal{N}) = \max(H(p) + S(\sigma) - S(\rho_{CQ}))$$

over $\{p(x), \rho_x\}$, where $\sigma = \sum p(x)\mathcal{N}(\rho_x)$

The Holevo–Schumacher–Westmoreland coding theorem

The capacity C for sending classical information over the channel $\mathcal{N}$ is

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

Even if we use the channel $\mathcal{N}$ a number n independent times, this is not a single-letter expression for the capacity

C.f. the classical case, where we can use the single-letter expression $\max_{p(x)} I(X;Y)$ instead of

$$\lim_{n\to\infty} \max_{p(x^n)} \frac{1}{n} I(X^n;Y^n)$$

for memoryless channels

The Holevo information is in general not additive,

i.e. $\chi(\mathcal{N}_1 \otimes \mathcal{N}_2) \neq \chi(\mathcal{N}_1) + \chi(\mathcal{N}_2)$

Additivity holds for entanglement-breaking channels: i.e., channels $\mathcal{N} : \mathcal{H} \to \mathcal{G}$ such that if ρ is entangled in $\mathcal{H} \otimes \mathcal{H}'$ then $(\mathcal{N} \otimes I)\rho$ is not entangled

When additivity holds, we have a single-letter expression for capacity

$$C = \chi(\mathcal{N})$$

achieved by setting $k = 1$ and $\ell = n$. However, in general sending entangled states $\rho^{(k)}$ over ℓ uses of $\mathcal{N}^k$ gives higher rates

Preservation of Entanglement over a Quantum Channel

Suppose we have a state $|\psi\rangle$ in $\mathcal{H} \otimes \mathcal{R}$, but we can only access $\mathcal{H}$

Assume $\rho = |\psi\rangle\langle\psi|$ is pure in $\mathcal{H} \otimes \mathcal{R}$ (by purification), but entangled

With an encoder that operates on $\mathcal{H}$ over $\mathcal{N} : \mathcal{A} \to \mathcal{B}$, we wish to preserve ρ and the entanglement with $\mathcal{R}$, according to:

1. $\mathcal{E}_n$ maps $\rho \in \mathcal{H} \otimes \mathcal{R}$ as $(\mathcal{E}_n \otimes I)\rho$ to $\mathcal{A}^{\otimes n}$
2. The channel $\mathcal{N}$ is used n independent times
3. The received state is $\sigma^{(n)} = \mathcal{N}^n((\mathcal{E}_n \otimes I)\rho)$
4. $\mathcal{D}_n$ maps $\sigma^{(n)}$ to $\omega \in \mathcal{H}' \otimes R$

Assume $d_n = \dim \mathcal{H} = \dim \mathcal{H}'$

A rate Q is achievable if there exist a sequence $(\mathcal{E}_n, \mathcal{D}_n)$ such that

$$\liminf_{n\to\infty} \frac{1}{n} \log d_n \geq Q$$

and $V(\rho, \omega) = 1/2 \operatorname{Tr}|\rho - \omega| \to 0$

(or equivalently the entanglement fidelity $\to 1$)

The capacity C is the maximum achievable rate

Remember the no cloning theorem: For any Hilbert space $\mathcal{H}$ there is no unitary operation U such that for $|\psi\rangle, |\psi\rangle' \in \mathcal{H}$,

$$U(|\psi\rangle \otimes |\psi\rangle') = |\psi\rangle \otimes |\psi\rangle$$

Still, we have a positive capacity for quantum communication: The capacity is

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

where $\mathcal{Q}(\mathcal{N})$ is the coherent information of a channel $\mathcal{N}$

For a state $\rho \in \mathcal{A} \otimes \mathcal{B}$, we had the conditional entropy

$$S(\rho_{\mathcal{A}}|\rho_{\mathcal{B}}) = S(\rho) - S(\rho_{\mathcal{B}})$$

with $\rho_{\mathcal{A}} = \mathrm{Tr}_{\mathcal{B}}\rho$ and $\rho_{\mathcal{B}} = \mathrm{Tr}_{\mathcal{A}}\rho$

Since $S(\rho|\rho_{\mathcal{B}}) < 0$ when ρ is entangled, we also define the coherent information (for entangled states ρ)

$$\mathcal{Q}(\rho_{\mathcal{A}}\rangle\rho_{\mathcal{B}}) = -S(\rho|\rho_{\mathcal{B}})$$

The coherent information of channel $\mathcal{N}$ then is

$$\mathcal{Q}(\mathcal{N}) = \max_{\rho} \mathcal{Q}(\sigma_{\mathcal{A}'}\rangle\sigma_{\mathcal{B}})$$

over $\rho \in \mathcal{A} \otimes \mathcal{B}$ and for $\sigma = (\mathcal{N} \otimes I)\rho$ with $\mathcal{N} : \mathcal{A} \to \mathcal{A}'$

As for classical over quantum, the expression for C is in general not single-letter, since in general $\mathcal{Q}(\mathcal{N}_1 \otimes \mathcal{N}_2) \neq \mathcal{Q}(\mathcal{N}_1) + \mathcal{Q}(\mathcal{N}_2)$

Additivity holds for degradable channels, i.e. channels $\mathcal{N}$ that can be decomposed as

$$\mathcal{N}(\rho) = \mathcal{N}_1(\mathcal{N}_2(\rho))$$

Thus, for a degradable channel $\mathcal{N}$, we have $C = \mathcal{Q}(\mathcal{N})$