8.S372/18.S996 Quantum Information Science III **Fall 2020**

Lecture 12: October 8, 2020

Lecturer: Aram Harrow *Scribe: Yuan Lee, Adam Bene Watts*

Previously, we saw that feedback (and hence shared randomness) has no effect on the classical channel capacity. However, quantum mechanics *does* affect the way we think about channel coding, and it shows up in a variety of ways. Some examples follow.

1. **Entanglement assistance:** using entanglement as a resource to transmit classical messages. This can increase the capacity of a quantum or classical channel (i.e. superdense coding, depolarizing channel example on pset 5).
2. **Entangled inputs:** even if Alice and Bob don't share entanglement, Alice can entangle her inputs across many uses of the channel. This extends the idea of correlations in classical codebooks by using entanglement resources.
3. **Quantum capacities:** where the goal is to transmit quantum messages.

Quantum capacities are further related to secret key capacities through quantum key distribution (QKD): transmitting one qubit allows the sender and recipient to share one secret bit.

12.1 Resource Notation

We keep track of communication resources using the following scheme.

- $[c \to c]$ or $[c \leftarrow c]$ = noiseless transmission of one cbit (classical bit).
- $[cc]$ = one rbit (shared random bit).
- $[q \to q]$ or $[q \leftarrow q]$ = noiseless transmission of one qubit.
- $[qq]$ = one bit of shared entanglement ("ebit"): specifically, the Bell pair $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2})$.
- $\langle N \rangle$ = one channel use $N_{A' \to B}$.
- $\langle \rho \rangle$ = one copy of ρ.

We say that $a \geq b$ if the combination of resources in a can generate the resources in b using a protocol with asymptotically vanishing error and inefficiency (note that we only care about the rate achieved in the limit of many uses of a). This definition will lets us define a partial order on resources.

The achievability portion of the channel capacities we saw before can now be written using this resource notation.

- classical capacity: $\langle N \rangle \geq C(N)[c \to c]$.
- quantum capacity: $\langle N \rangle \geq Q(N)[q \to q]$.
- entanglement-assisted capacities:

$$\langle N \rangle + \infty[qq] \geq C_E(N)[c \to c] \text{ and } \langle N \rangle + \infty[qq] \geq Q_E(N)[q \to q].$$

- distillable entanglements:

$$\langle \rho \rangle + \infty[c \to c] \geq E_{D,1}(\rho)[qq] \text{ (1-way distillable entanglement) and}$$
$$\langle \rho \rangle + \infty[c \to c] + \infty[c \leftarrow c] \geq E_{D,2}(\rho)[qq] \text{ (2-way distillable entanglement).}$$

As an example of the partial ordering on resources, we give the following diagram of relationships, where $a \to b$ means $a \geq b$ and entries without arrows between them are incomparable.

$$\begin{tikzcd}
& {[q \to q]} \arrow[dl] \arrow[dr] & & {[q \leftarrow q]} \arrow[dl] \arrow[dr] & \\
{[c \to c]} \arrow[drr] & & {[qq]} \arrow[d] & & {[c \leftarrow c]} \arrow[dll] \\
& & {[cc]} & &
\end{tikzcd}$$

We can also write describe quantum teleportation and superdense coding using resource notation.

- **teleportation** can be written as $[qq] + 2[c \to c] \geq [q \to q]$.
- **superdense coding** can be written as $[q \to q] + [qq] \geq 2[c \to c]$.

(Resource notation obscures the fact that these protocols work non-asymptotically.)

12.2 Assorted Topics

12.2.1 Channel Simulation

$\langle N\rangle \geq C(N)[c \to c]$ implies that we can simulate $\approx nC(N)$ copies of $[c \to c]$ using n uses of channel N. Could we simulate N using $[c \to c]$ instead? The classical reverse Shannon theorem says we can (note N is classical channel):

$$C(N)[c- > c] + \infty[cc] \geq \langle N\rangle.$$

But what does it mean precisely simulate a channel?

We say that we can simulate the target channel N if our protocol produces a channel M that is close to N. Two metrics for channels are:

- **diamond norm** $\|M - N\|_\diamond = \|\mathrm{id} \otimes M - \mathrm{id} \otimes N\|_{1\to 1}$;
- $1 \to 1$ **norm** $\|M - N\|_{1\to 1}$, defined by

  $$\|\mathcal{E}\|_{1\to 1} = \sup_X \frac{\|\mathcal{E}(X)\|_1}{\|X\|_1}.$$

  If $\mathcal{E}$ is the difference between two channels, an equivalent definition is $\|\mathcal{E}\|_{1\to 1} = \max_\rho \|\mathcal{E}(\rho)\|_1$.

The diamond norm gives the strongest condition on “closeness”, whereas the $1 \to 1$ norm gives a weaker condition. Intuitively, this is because some channels can be better distinguished by feeding in states entangled with some reference system.

We can use either of these metrics to define the accuracy of our channel simulation. The diamond norm gives the strongest constraint, and bounds the ammount of error we can incur by replacing a channel $\mathcal{N}$ by a simulation $\mathcal{M}$ in some protocol. Both the diamond norm and 1 to 1 norm apply to blind inputs, where Alice does not have a classical description of her state. We can also consider the case where Alice has a description of her state ρ, and Bob wants to construct the state $\mathcal{N}(\rho)$. This gives an even weaker condition on “closeness”.

12.2.2 Resource Arithmetic

For any positive ϵ, we cannot do

$$(2 - \epsilon)[c \to c] + 1000[qq] \geq [q \to q]. \tag{12.1}$$

(The coefficient of 1000 is illustrative; take it to be an arbitrary large number.)

Proof. Equation (12.1) violates the no-signalling theorem through superdense coding. If a protocol achieves (12.1), then we can use one extra ebit to obtain

$$(2-\epsilon)[c \to c] + 1001[qq] \geq [q \to q] + [qq] \geq 2[c \to c].$$

If this were possible, then for sufficiently large n, there will be two possible received messages corresponding to the same input message, distinguished only by the ebit $[qq]$. If we fix this input message, then we can use entanglement to transmit a classical bit, contradicting the no-signalling theorem.

12.2.3 Remote State Preparation

Let "ψ" refer to the classical description of the n-qubit state ψ. Then, *remote state preparation* refers to a protocol in which Bob prepares the state ψ with Alice's help. Alice has access to the classical description of ψ, n ebits (shared with Bob) and $n(1+\delta)$ cbits (for some $\delta > 0$):

$$\text{“}\psi\text{”} + n[qq] + n(1+\delta)[c \to c] \Rightarrow \psi.$$

The proof of remote state preparation is relatively involved.

Remote state preparation can be thought of as a simulation of the identity channel with visible inputs. Comparing the resource cost of this to the resource cost of simulating the identity channel on blind inputs (i.e. generating the resource $[q \to q]$) derived above shows the difference in resource cost between visible and blind simulation.

12.3 Entangled Inputs

The HSW theorem gives the classical capacity of a CQ channel.

For a general quantum channel N, the capacity with product state inputs only is

$$\chi(N) = \max_{\rho} I(X;B)_\rho$$

where ρ is chosen from the set of states with form $\rho = \sum_x p(x) \left|x\right\rangle \left\langle x\right|_X \otimes N_{A' \to B}(\psi^x_{A'})$. This bound essentially comes from the original HSW theorem and the observation that, even when communicating through a quantum to quantum channel N, Alice must make a classical choice of a message x to transmit to Bob, then send an associated pure state $\psi^x_{A'}$ through the channel to Bob. (She could also send mixed states but we could always decompose those into pure states and add extra labels, which would only increase channel capacity).

However, the inputs to $N^{\otimes n}$ over n channel uses can be entangled. The classical channel capacity of N is defined to be the regularization of χ:

$$C(N) = \lim_{n\to\infty} \frac{1}{n}\chi(N^{\otimes n}).$$

This capacity C is generally hard to compute.

Facts about χ and C.

1. Computing χ is an NP-complete optimization problem (scaling in terms of the dimension of the channel.)
2. $C \geq \chi$ (since we can just use product states). Sometimes, $C > \chi$.
3. The complexity of C is unknown. It could be polynomial, it could be uncomputable.
4. χ is easy to compute for CQ channels. C_E is also easy to compute.
5. Let an additivity violation for a capacity χ refer to the existence of channels N_1 and N_2 such that $\chi(N_1 \otimes N_2) > \chi(N_1) + \chi(N_2)$. Then Shor (quant-ph/0305035) showed that

   $$\chi \text{ additivity violation} \Leftrightarrow E_F \text{ additivity violation} \Leftrightarrow S_{\min} \text{ additivity violation},$$

   where $S_{\min}(N) = \min_\rho S(N(\rho))$ is the entropy of the least-mixed output. Hastings (0809.3972) later proved additivity violation.
6. χ is known to be additive in the following cases.
   - **Entanglement-breaking channels**. We say that N is entanglement-breaking if $(\mathrm{id}\otimes N)(\rho) \in \mathrm{Sep}$ for all inputs ρ. Equivalently, N is entanglement-breaking iff it can be written as a measure-and-prepare (or QCQ) channel.
   - **Depolarizing channels** $N(\rho) = (1-p)\rho + pI/d$ for some probability p.
   - **Erasure channels** $N(\rho) = (1-p)\rho + p\,|e\rangle\,\langle e|$, where $|e\rangle$ is an erasure flag.
   - **Unital qubit channels** $N(I/d) = I/d$.
   - **Purely lossy bosonic channels**, where the output mode a_k' can be described in terms of input modes a_k and b_k as $a_k' = \sqrt{\eta_k}a_k + \sqrt{1-\eta_k}b_k$.

- **Hadamard channels**. If the Stinespring representation of N is $N(\rho) = \mathrm{tr}_E V_{A'\to BE}\rho V_{A'\to BE}^\dagger$, then the complement of N is $N^c(\rho) = \mathrm{tr}_B V_{A'\to BE}\rho_{A'} V_{A'\to BE}^\dagger$. Then N is a Hadamard channel iff N^c is an entanglement-breaking channel.

We conclude with a brief outline of the main ideas of Hastings' proof of superadditivity. Hastings showed existence of a channel $\mathcal{N}$ which satisfied

$$S_{min}(\mathcal{N} + \overline{\mathcal{N}}) \leq S_{min}(\mathcal{N}) + S_{min}(\overline{\mathcal{N}})$$

(the channel $\overline{\mathcal{N}}$ is obtained by taking the complex conjugate of everything in $\mathcal{N}$).

The channel $\mathcal{N}$ is defined act randomly on the state ρ with one of D possible unitaries (D is a constant independent of the dimension of the state): $\mathcal{N}(\rho) = \sum_{i=1}^{D} U_i \rho U_i^\dagger$.

To understand why entanglement state inputs to the channel $\mathcal{N} + \overline{\mathcal{N}}$ can lead to a lower output entropy, consider sending the maximally mixed state Φ through the channel $\mathcal{N} \otimes \overline{\mathcal{N}}$. Then

$$\begin{aligned}\mathcal{N} \otimes \overline{\mathcal{N}}(\Phi) &= \frac{1}{d^2}\left(\sum_i (U_i \otimes \overline{U_i})\Phi(U_i \otimes \overline{U_i}) + \sum_{i\neq j}(U_i \otimes \overline{U_j})\Phi(U_i \otimes \overline{U_j})\right) \\ &= \frac{1}{d}\Phi + \frac{1}{d^2}\left(\sum_{i\neq j}(U_i \otimes \overline{U_j})\Phi(U_i \otimes \overline{U_j})\right),\end{aligned}$$

where we used that $(I \otimes \overline{U_i})\Phi = (\overline{U_i}^\top \otimes I)\Phi = \left(U_i^{-1} \otimes I\right)\Phi$. From this, a not-to-hard calculation shows

$$S_{min}(\mathcal{N} \otimes \overline{\mathcal{N}}) \leq S(\mathcal{N} \otimes \overline{\mathcal{N}}(\Phi)) \leq 2\ln(D) - \frac{\ln(D)}{2}.$$

A very hard calculation shows that

$$S_{min}(\mathcal{N}) \geq \ln(D) - \frac{C}{D} - D^{O(1)}\sqrt{\frac{\ln(N)}{N}}$$

(C is a constant, N is the dimension of the channel), which proves the result.