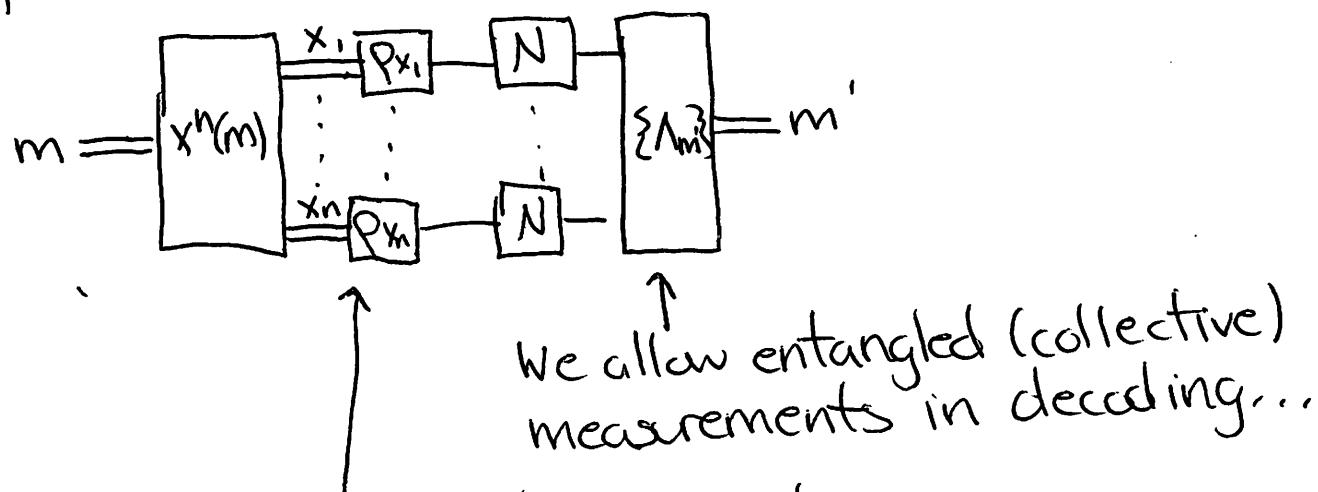


Lecture 18

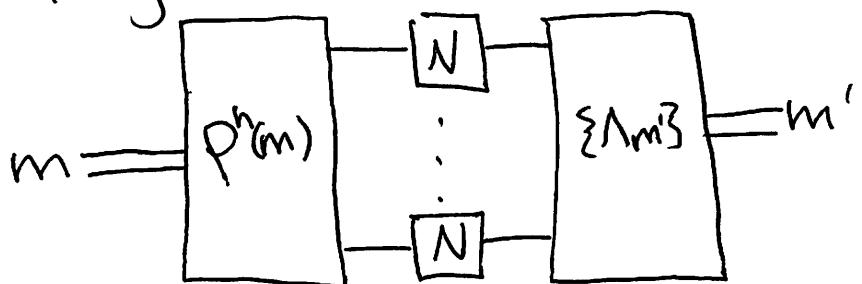
①

So, does this version of the HSW theorem give us the optimal rate of classical comm through a Q channel? Not necessarily. The coding procedure did not fully optimize over all possible encodings:



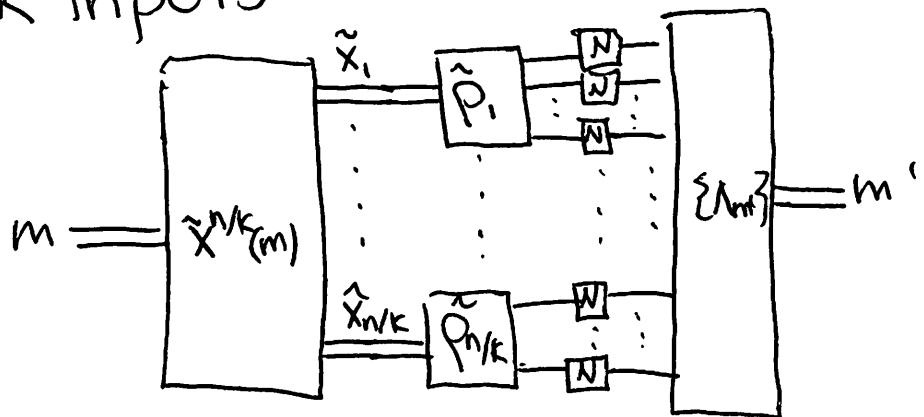
...but the encoding is only over product states.

What if we instead allowed our codewords to be entangled across all the channel inputs?



Clearly, such a class of protocols includes our original scheme, and so must do at least as well.

We can approach this as a limiting procedure. ②
 Suppose we allow our inputs to be entangled across K inputs:



We can treat each "bundle" of K channel uses as a new channel $N \otimes \dots \otimes N = N^{\otimes K}$. By the HSW theorem we've already proven,

$$\frac{1}{K} X(N^{\otimes K})$$

is an achievable rate for classical comm.
 We take the limit as $K \rightarrow \infty$ and get

$$X_{\text{reg}}(N) \equiv \lim_{K \rightarrow \infty} \frac{1}{K} X(N^{\otimes K})$$

the regularized Holevo information.

This gives us the more complete version
 of the HSW theorem:

Thm (Holevo-Schumacher-Westmoreland) complete version (3)

The supremum over all achievable rates for classical comm over a Q channel is $X_{\text{reg}}(N)$ in the limit of many channel uses.

Proof ^{The Direct Coding Thm} Just follows from the earlier version of

the theorem using the channel $N^{\otimes k}$, and taking the limit of $\frac{1}{k}X(N^{\otimes k})$ as $k \rightarrow \infty$.

The Converse Thm

To prove the converse thm we instead prove a bound on the ~~optimal~~ optimal rate of common randomness production, which is clearly an upper bound on the rate of classical communication.

Alice prepares, ^{and shares w/ Bob} a maximally correlated state $\bar{\Phi}^{MM'}$, so the rate of common randomness production is $C - \delta = \frac{1}{n} \log_2 |M|$. Consider this

chain of inequalities:

$$\begin{aligned}\bar{\Phi}^{MM'} &= \frac{1}{M} \sum_{m=1}^{|M|} |m\rangle\langle m|^n \otimes |m'\rangle\langle m'|^n \\ \xrightarrow{\text{enc.}} \rho &= \frac{1}{M} \sum_{m=1}^{|M|} |m\rangle\langle m|^n \otimes P_m \xrightarrow{N^{\otimes n}} \frac{1}{M} \sum_{m=1}^{|M|} |m\rangle\langle m| \otimes N(P_m) \stackrel{B^n}{=} \tilde{\rho} \\ \xrightarrow{\text{dec.}} \frac{1}{M} \sum_{m,m'}^{|M|^n} &|m\rangle\langle m|^n \otimes \text{Tr}\left\{ \Lambda_m \cdot N(P_m) \right\} |m'\rangle\langle m'|^n \\ &\equiv \omega^{MM'}\end{aligned}$$

$$\begin{aligned}
 n(c-\delta) &= I(M; M')_{\bar{\omega}} \quad) \quad \text{Using } \|\bar{\Phi}^{MM'} - \omega^{MM'}\|_1 \leq \epsilon^+ \\
 &\leq I(M; M')_{\omega} + n\epsilon' \\
 &\leq I(M; B^n) \quad \text{at the } \epsilon' \quad) \quad \text{Data processing} \\
 &\leq X(N^{\otimes n}) + n\epsilon' \quad) \quad \begin{array}{l} \text{mutual info for a} \\ \text{classical-quantum state} \end{array}
 \end{aligned}$$

$\Rightarrow c-\delta \leq \frac{1}{n} X(N^{\otimes n}) \rightarrow X_{\text{reg}}(N).$

\square

The problem with $X_{\text{reg}}(N)$ is that in general there is no practical scheme for calculating regularized functions, analytically or numerically.

Things would simplify dramatically if $X_{\text{reg}}(N) = X(N)$.

This would follow if X were additive:

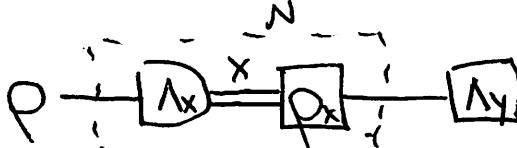
$$X(N_1 \otimes N_2) \stackrel{?}{=} X(N_1) + X(N_2).$$

We can calculate $X(N)$ explicitly for certain channels, and show that, indeed, it is additive for those channels.

I. Classical-Q channels

⑤

Because these channels are entanglement breaking



there is obviously no advantage to entangling across the inputs: $X_{\text{reg}}(N) = X(N)$.

II. Q Hadamard Channels

One can prove a nice result about a Q Hadamard channel N_H : for any other channel N ,

$$X(N_H \otimes N) = X(N_H) + X(N).$$

So classical capacity of such channels is additive.

III. Depolarizing channel

$$N_D(p) = (1-p)\rho + p\pi.$$

Here, too, one can prove that $X(N_D \otimes N) = X(N_D) + X(N)$ for any other channel N .

In fact, the optimal encoding strategy for N_D is quite simple: simply use classical random coding, choosing the input symbols uniformly from an orthonormal basis, $\{(t, |x\rangle)\}$, and measure each output with the projectors $P_x = |x\rangle\langle x|$.

IV. Erasure channel. $X(N)$ is also additive for the Q erasure channel; the capacity is $1-p$.

Is $X(N)$ additive?

⑥

Because every example where $X(N)$ was known in general was additive, it was conjectured that $X(N)$ was always additive. Shor in 2003 showed that this conjecture was equivalent to three other additivity conjectures: minimum output entropy of a Q channel; entanglement of formation; and strong superadditivity of the entanglement of formation.

However, in 2009 Hastings showed that $X(N)$ was not additive for a general channel. His proof was ingeniously indirect: he showed that in choosing from a random set of Q channels (random unitary channels), the ~~problem~~ probability that a channel \mathcal{E} and its conjugate channel $\bar{\mathcal{E}}$ will have non-additive minimum output entropy $H_{\min}(\mathcal{E} \otimes \bar{\mathcal{E}}) < H_{\min}(\mathcal{E}) + H_{\min}(\bar{\mathcal{E}})$ is nonzero.

This proof was clever, but nonconstructive. To my knowledge, no concrete example of a provably non-additive channel has yet been demonstrated.

