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

Lecture 15: October 20, 2020

Lecturer: Aram Harrow *Scribe: Michael DeMarco, Leon Ding*

15.1 Proofs of the quantum capacity formula

1. Coherent Classical Communication and C_E
2. Decoupling and merging

The first proof is a simpler one that Aram came up with, but has fewer generalizable insights for quantum information.

Recall that the formal definition of the quantum capacity is:

$$Q = \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \log \max \left\{ d : d\text{-dimensional subspace } V \text{ of } A^n \text{ s.t. } \forall \left|\psi\right\rangle \in V,\ \mathcal{D}(N^{\otimes n}(\psi)) \approx_\epsilon \psi \right\} \tag{15.1}$$

Remember that $\approx_\epsilon$ means approximately equal with some error proportional to ϵ, the log of a dimension corresponds to a number of qubits, and $\mathcal{D}$ is a decoding map.

15.1.1 Detour: Cobits

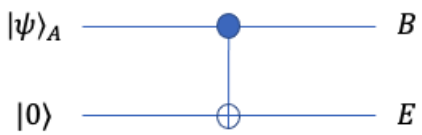
A coherent bit, or cobit (can think of this as intermediate between classical communication and quantum),

$$[q \to q] : a \left|0\right\rangle_A + b \left|1\right\rangle_A \to a \left|0\right\rangle_B + b \left|1\right\rangle_B \tag{15.2}$$

Or more succinctly,

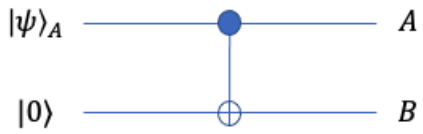
$$\left|x\right\rangle_A \to \left|x\right\rangle_B \text{ for } x \in \{0,1\}, \text{ isometry} \tag{15.3}$$

Consider classical communication as $[c \to c] : \left|x\right\rangle_A \to \left|x\right\rangle_B \otimes \left|x\right\rangle_E$ using a CNOT gate from $\left|\psi\right\rangle_A \otimes \left|0\right\rangle \to (B, E)$.



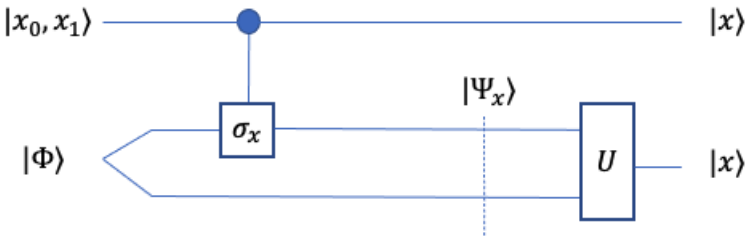
Instead of giving one bit to the environment, what happens if one of the outputs remains on Alice's side?

$$[c \to cc] \left|x\right\rangle_A \to \left|x\right\rangle_A \otimes \left|x\right\rangle_B \tag{15.4}$$



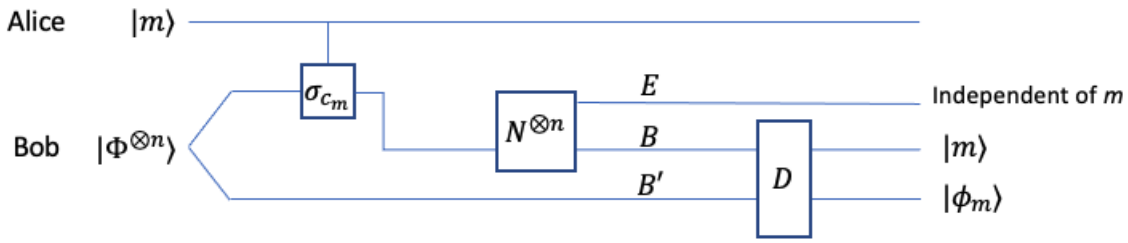
This is the cobit channel. Now, $[q \to q] \geq [c \to cc] \geq [c \to c]$. In fact, we will see that asymptotically $[c \to cc] = \frac{1}{2}([q \to q] + [qq])/2$.

This equality is true because of *decoupling*. Now, cbits (in input or output) do not necessarily leak to E, or at least there is nothing in the environment that leaks to E.



Output Rule (concerning the case with decoupled outputs): super-dense coding $[q \to q] + [qq] \geq 2[c \to c]$ does not leak to environment, hence if we do not throw out bits we get a free upgrade to $[q \to q] + [qq] \geq 2[c \to cc]$. Here, instead of performing a bell-state measurement at the end of the circuit, Bob just applies a unitary U to transform the bell states back to the computational basis.

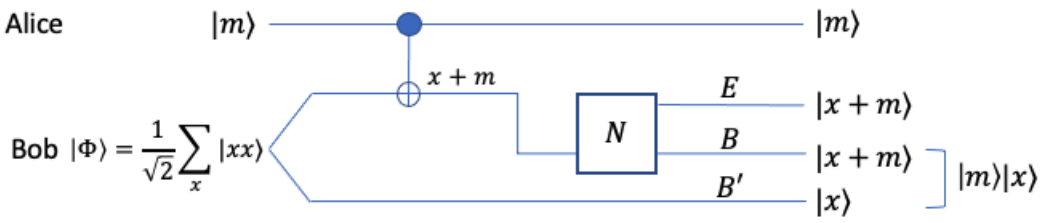
In general, coherently decoupled $[c \to c]$ (ie where the environment cannot break superpositions of outputs) can turn into $[c \to cc]$.



Consider the above example circuit for entanglement assisted communication. Here,

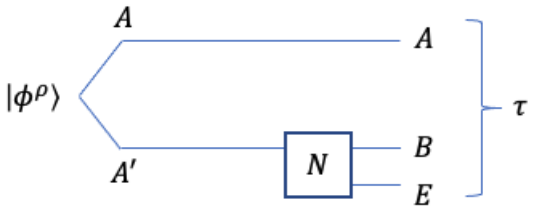
Alice and Bob share n copies of the Bell state $|\Phi\rangle$ (of course, it doesn't have to be a Bell state in the general case). Alice performs a controlled Pauli operation depending on some code-word c_m, $\mathcal{N}$ is a noisy channel, and $\mathcal{D}$ is Bob's decoder which produces m. Bob can erase the content of $|\phi_m\rangle$ using his knowledge of m, in which case he is left with a cobit.

Suppose that N is a cbit channel, $m \in \{0, 1\}$. Consider the circuit:



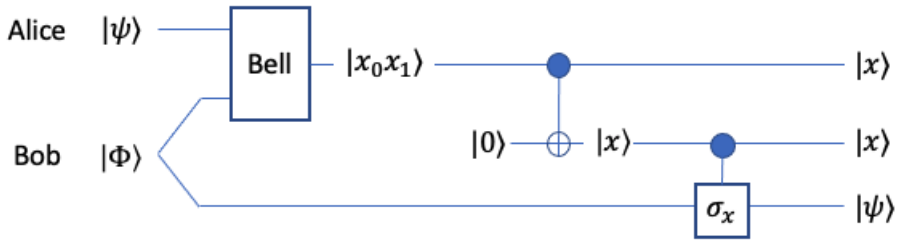
This is a Vernom cipher or one-time pad. Here, Bob may unitarily transform his result into $|m\rangle\,|x\rangle$, without Eve determining the content of m. Cobits are, in a sense, the quantum version of the one-time pad.

In fact, the ebit cost is $S(A)$:



and here $\langle N\rangle + S(A)[qq] \geq I(A:B)[c \to cc]$

Input Rule: cobits in decoupled inputs yield ebit teleportation:



First, Alice, instead of doing a Bell measurement, does a unitary transformation from the Bell basis into the standard basis. In normal teleportation, this state would be

used to control a controlled-σ_x operation, and Bob would be left with the teleported state. Instead of using this classical communication of the bit, we now use a cobit to transmit the information to Bob, with the additional benefit of retaining to two ebits. In resource notation, this process has produced $2[c \to cc] + [qq] \geq 2[qq] + [q \to q]$. However, considering coherent superdense coding $[qq] + [q \to q] \geq 2[c \to cc]$. Hence $2[c \to cc] = [qq] + [q \to qq]$, where the equality holds catalytically. This means that we had one unit of $[qq]$ which was just there as a catalyst.

15.1.2 Coherent Classical Communication and C_E

Combining this with our earlier observation, we have that $\langle N \rangle + S(A)[qq] \geq \frac{I(A:B)}{2}([q \to q] + [qq])$. This implies:

$$S(A) - \frac{I(A:B)}{2} = \frac{2S(A) - (S(A) + S(B) - S(E))}{2} = \frac{I(A:E)}{2} \tag{15.5}$$

which implies that:

$$\langle N \rangle + \frac{1}{2} I(A:E)[qq] \geq \frac{I(A:B)}{2}[q \to q] \tag{15.6}$$

This is called the 'father' protocol because we can combine it with $[q \to q] \geq [qq]$ (entanglement distribution) to get that:

$$\langle N \rangle \geq \frac{I(A:B) - I(A:E)}{2}[q \to q] = I_C[q \to q] \tag{15.7}$$

where the equality follows from expanding mutual information in terms of entropies. (requires catalytic entanglement use). If we combine the 'father' protocol with superdense coding, we get

$$\langle N \rangle + S(A)[qq] \geq I(A:B)[c \to c] \tag{15.8}$$

Aside: there is also a 'mother' protocol:

$$\langle \rho \rangle + \frac{1}{2} I(A:E)[q \to q] \geq \frac{I(A:B)}{2}[qq] \tag{15.9}$$

which we can combine with teleportation to get:

$$\langle \rho \rangle + I(A:E)[c \to c] \geq I_c(A \rangle B)[qq] \tag{15.10}$$

More details at `quant-ph=0307031` and `quant-ph/03/08/0447`.

15.1.3 Decoupling and Merging

Quantum state merging and negative information `quant-ph/0512247` and `quant-ph/0606225`. The 'mother' protocol leads to the mother of all protocols.

The merging task: purify ρ^{AB} to ψ^{ABR}. Think of R as a reference system that keeps track of the original message. Goal is for Alice to transmit her half of the state to Bob. Allow free LOCC, ebit cost of merging is $S(A|B)$. If $S(A|B) > 0$, merging is possible by consuming $S(A|B) + \delta$ ebits $\forall \delta > 0$. If $S(A|B) < 0$, then merging is possible while generating $-S(A|B) - \delta$ ebits $\forall \delta > 0$. Either way, we use $I(A:R)$ cbits.

Examples:

1. $\rho = \frac{I}{2}^A \otimes \sigma^B, |\psi\rangle^{ABR} = |\psi\rangle^{AR} \otimes |\phi\rangle^{BR'}$ comm cost is 1.
2. $\rho = \phi^{AB}$, comm cost is -2

(Proof to be covered in detail next lecture.)