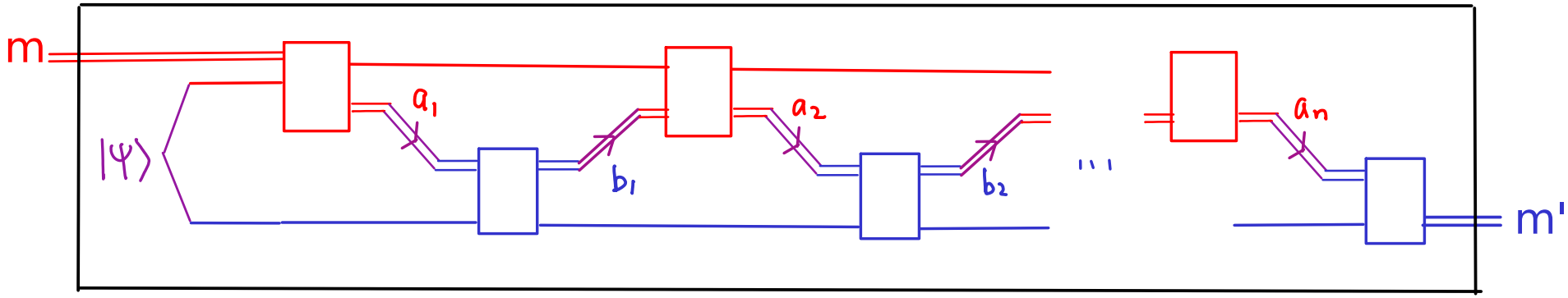
CO781 / QIC 890. Self-study notes, Sept 27, 2020.

1. On an earlier puzzle whether C2 and C3 holds in the presence of back communication

C2 says that even with an arbitrary entanglement state shared between Alice and Bob, Alice cannot comm one out of s+t messages using a noiseless classical channel with input size s, for positive integers s and t.

We proved this by assuming, in contradiction, that there is a protocol P achieving, and replacing the noiseless classical channel in P with Bob guessing the output randomly. For the uniform input, the insufficient communication results in correlation between Alice's input and Bob's output, contradicting C1.

If unlimited classical back communication is allowed from Bob to Alice, the most general protocol for Alice to comm classical messages to Bob is more complicated:



In the above, we absorb all of Alice's registers into the top single-red line (so, she has a copy of m, b1, etc in her local memory, and her k-th operation can depend on m, a1, b1, a2, b2, ..., a_{k-1}, b_{k-1}).

Similarly, Bob's k-th operation depends on a1, b1, ..., ak.

C2 holds even with unllimited back communication from Bob to Alice.

Suppose a1 varies over s1 values, a2 varies over s2 values, ... Then, we should set s = s1 * s2 * ... * sn.

If we let Bob randomly generate a1, a2, ..., an, he still has prob 1/s to have all of them as in protocol P, and our original proof for C2 holds.

Similarly, C3 holds in the presence of back communication from Bob to Alice.

CO781 / QIC 890. Self-study notes, Sept 27, 2020.

2. On information gain implies disturbance

See, for example:

Information Gain vs. State Disturbance in Quantum Theory
Chris Fuchs
https://arxiv.org/abs/quant-ph/9611010

3. On uniform spherical measure and Haar measure

One source is "Theory of Quantum Information" by Watrous

Section 7.2 provides an introduction to both,
and Section 7.3 connects to measure concentration and applications in quantum information.

There are many manifestations of the information gain implies disturbance. Both information and disturbance can be quantified in many ways. The tradeoff can be formulated under many different settings. In general, one can fix the information gain and lower bound the disturbance to the unknown state, or fix the disturbance to the unknown state and upper bound the information gain. But each quantitative tradeoff is a separate calculation, and should be made for the researcher's specific need.

Likewise, probabilistic arguments are tremendously useful, and there are often multiple inequivalent proofs leading to the same information theoretical result.

Both topics are too broad to be covered with a simple reference ...