Channel Superactivation and Quantum Data Hiding

Joseph M. Renes

1 Quantum Shannon Theory: The (Very) Broad Strokes

Ultimately, we arrive at a maximal entanglement between (A)lice and (B)ob, i.e. a state unitarily equivalent to \(|\psi_{AB}\rangle = \frac{1}{\sqrt{2}} \sum_i |E_i\rangle |K_i\rangle\). All the protocols of the quantum family tree boil down to generating maximal entanglement in some way.

One characterization of entanglement is the entropic statement \(H(AB) = -1\). But to build protocols, we characterize entanglement in one of three alternate ways:

1.1 Entanglement via Decoupling

\(AB\) is maximally entangled if \(A\) is decoupled from everything but \(B\) (and maximally mixed).

![Diagram of entanglement via decoupling](image)

Entropically: \(H(A|E) = H(A) = 1 \Rightarrow AB\) is maximally entangled. See [2].

1.2 Entanglement via Secrecy

\(AB\) is maximally entangled if Alice can generate a classical random variable \(X^A\) (e.g. a coin toss) which Bob can perfectly replicate, but is uncorrelated with anything else.

![Diagram of entanglement via secrecy](image)

\(H(X^A|E) = 0\) and \(H(X^A|E) = H(X^A) = 1 \Rightarrow AB\) is maximally entangled. See [1].

1.3 Entanglement via Complementary Classical Correlation (my own personal favorite)

\(AB\) is maximally entangled if there are two conjugate measurements Alice can make, leading to classical random variables \(X^A\) and \(Z\), either of which Bob can perfectly predict.

![Diagram of entanglement via complementary classical correlation](image)

\(H(X^A|E) = H(Z|E) = 0 \Rightarrow AB\) is maximally entangled. See [4].

2 Channel Superactivation

The quantum capacity \(Q(\mathcal{N}^{A|B})\) of a quantum channel \(\mathcal{N}^{A|B}\) from Alice to Bob characterizes its ability to generate entanglement between them. Channel superactivation refers to the strange phenomenon that two channels can separately each have zero capacity, \(Q(\mathcal{N}_1^{A|B}) = 0\) and \(Q(\mathcal{N}_2^{A|B}) = 0\), yet together have nonzero capacity, \(Q(\mathcal{N}_1^{A|B} \circ \mathcal{N}_2^{A|B}) > 0\).

2.1 Entanglement Generation over Quantum Channels

To generate entanglement between Alice and Bob using a channel \(\mathcal{N}^{A|B}\), Alice encodes half of an entangled state and sends it to Bob, who decodes it. The encoding and decoding operations depend on the channel.

![Diagram of entanglement generation](image)

From [4], the capacity \(Q(\mathcal{N}) > 1 - H(X^B|E) - H(Z|E)\), for \(B\) the output of the channel.

2.2 Private States and the Horodecki Channel \(\mathcal{N}_H^Z\)

The superactivation effect discovered by Smith & Yard [5] relies on a channel \(\mathcal{N}_H^Z\) incapable of generating entanglement, but nevertheless capable of generating a secret key [3]. Quantumly, secret keys are similar to entangled states, except that Alice holds two systems: one which becomes the key \(X\) upon measurement and another which shields the key from any eavesdropper. (Generally, the shield can be distributed between Alice and Bob.)

![Diagram of private state generation](image)

Entropically: \(H(X^B|E) = 0\) and \(H(Z|X^B|E) = 0\). Same as entanglement, except Bob needs the shield to predict the conjugate observable \(Z^A\). So send it to him!

2.3 Superactivation

Channel superactivation is now easy: send the shield through the 50% erasure channel!

![Diagram of superactivation](image)

Since \(\mathcal{N}_H\) produces a private state, \(H(X^B|\mathcal{N}_H) = 0\); because it cannot produce entanglement, \(H(Z^B|\mathcal{N}_H) = 1\). Half the time Bob obtains the shield from the erasure channel, in which case they share entanglement. So altogether \(\mathcal{N}_H\) and \(\mathcal{N}_H\) together can generate entanglement at (at least) half the rate at which \(\mathcal{N}_H\) generates private states.

3 Quantum Data Hiding

From channel superactivation of the Smith & Yard form, we can construct a set of quantum data hiding states. Quantum data hiding refers to a set of orthogonal quantum states \(\rho_{\text{hid}}\) which cannot be reliably distinguished using local operations and classical communication (LOCC) [6]. The set we can construct here are immune to 1-way LOCC.

3.1 Forward Communication Doesn’t Help

To construct the set, we just need to remember that forward classical communication from Alice to Bob cannot increase \(Q(\mathcal{N})\). Consider the states \(\rho_{\text{hid}}\) created by the 2nd measurement of \(A\) (\(z\) is the outcome of the measurement and labels the state).

![Diagram of quantum data hiding](image)

- Since the properly-decoded output of \(\mathcal{N}_H\) is a private state, \(H(Z^A|\mathcal{N}_H) = 0\), and the \(\rho_z\) must be disjoint, i.e. perfectly distinguishable.
- But by the analysis of 2.3, \(H(Z^A|\mathcal{N}_H) = 1\), or else \(Q(\mathcal{N}_H) > 0\). Thus, Bob’s marginal states \(\rho_{\text{hid}}\) are perfectly indistinguishable.
- Finally, since forward communication cannot increase \(Q\) attempts by Alice to measure the \(\mathcal{N}_H\) system and communicate the result to Bob are futile.

Hence, the \(\rho_{\text{hid}}\) are a set of data hiding states immune to 1-way LOCC, a fact which follows immediately using the formalism of 1.3.

References