1 Key Technical Take-Aways

1. Unconditionally secure encryption algorithms exist and are conceptually quite simple, but have properties that make them impractical in a lot of scenarios. The one-time pad is an example; it requires out-of-band distribution of a secret key which must be as long as or longer than the messages to be sent, and can only be used once while maintaining unconditional security. For various reasons the more common type of encryption in use relies on computational security, i.e. encryption that can be reversed by an attacker but requires prohibitively large computations to undo.

2. The entropy of an information source is the expected value of the Shannon information content of samples from that information source, and this quantity is directly related the best possible compression system for the information source. More precisely, as the length of the uncompressed string goes to infinity, the average number of bits needed to optimally encode symbols from the information source goes to the entropy of the information source. This relationship holds when we assume that each codeword in the compression system encodes as single symbol, not a sequence of symbols.

3. The Slepian and Wolf result shows us that when we want to compress to distinct but correlated information sources we can use information from one of the sources to reduce the number of bits needed to encode the second source.

4. A Nash equilibrium represents each player's best response to the given set of strategies of the other palyers. It does not necessarily correspond to the optimal outcome for all players involved – it is a state of mutual best response, not necessarily a state of optimal collective payoff.

5. The linking identity (1.9) in the main text relates the actual average code length of when applying a code κ to a distribution P to two important quantities; 1. The entropy of the true distribution P being encoded, and 2. The divergence of true distribution P from the assumed distribution Q to which the id-code is adapted, $D(P||Q)$. While the linking identity is derived from other definitions in the text, it is also reasonable to use the linking identity as a definition of divergence, and derive the properties of divergence in the other direction.

6. Bits can be encoded as qubits, but qubits cannot be encoded as bits, presenting a challenge to the field of information theory where the bit is the fundamental unit. However, it can still be argued that the bit remains a valid fundamental unit in information theory. This is because a qubit's superposition state, which cannot be encoded in bits, also cannot be queried or observed directly. In essence, any observation we make about a quantum system ultimately collapses to a classical state, resulting in information that is expressed in bits. Therefore, even though qubits represent a more complex state of information theoretically, any information we can effectively obtain and communicate about the system is in the form of bits. This reality reinforces philosophically the bit as the basic unit of information epistemologically, even if the qubit does introduce a richer ontological structure.

2 Key Learnings

3 Quantum Error Correction since 2008

A major challenge in practical application of quantum information theory is the instability of quantum systems, which means, for instance, that it is very difficult to store a qubit for a long period of time. One of the avenues of research that is providing solutions to this problem is in Quantum Error Correction. As with classical bits, quantum bits are in practice susceptible to bit flips, e.g. if the state of qubit changes erroneously from $|0\rangle$ to $|1\rangle$. However, qubits are additionally susceptible to phase errors, e.g. a state like $|0\rangle + \beta|1\rangle$ changing to $|0\rangle - \beta|1\rangle$.[1]

[1] Simon J Devitt, William J Munro, and Kae Nemoto. "Quantum error correction for beginners". In: *Reports on Progress in Physics* 76.7 (June 2013), p. 076001. ISSN: 1361-6633. DOI: 10.1088/0034-4885/76/7/076001. URL: http://dx.doi.org/10.1088/0034-4885/76/7/076001.