Key Technical Insights

kti-1: The entropy of an information source, representing the expected value of its Shannon information content, directly correlates to the efficiency of optimal compression systems. As uncompressed string length increases, the average bits required for encoding approaches the source's entropy, under the assumption of encoding individual symbols. As data and information systems grow, ensuring security without compromising scalability gets more difficult. QKD offers a pathway to enhance rather than sacrifice security in tandem with the expansion of data networks and communication systems.

kti-2: Slepian-Wolf coding reveals that compressing two correlated information sources can be optimized by using information from one source to reduce the encoding bits needed for the other.

kti-3: A Nash equilibrium represents each player's best response to the given set of strategies of the other players. 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.

kti-4: Unconditionally secure encryption, exemplified by the one-time pad, offers rigorous security but is impractical for widespread use due to key distribution challenges and single-use limitations. Conversely, computational security, though less theoretically robust, is more feasible in common applications. Quantum Key Distribution (QKD) could make unconditionally secure methods like the one-time pad more practical.

kti-5: The maximum entropy principle, which advises selecting the distribution with maximized entropy based on known data, offers a decision-making framework in uncertain scenarios. Harremoës and Topsøe [1, p. 23] introduce the idea in an interesting way; by constructing a game in which the optimal strategy for one of the players (Nature) turns out equivalent to applying the maximum entropy principle. For me, the example highlighted the dialectic between *discovery* and *invention* in mathematics.

kti-6: The no-cloning theorem, a result of quantum gate reversibility, dictates that quantum information cannot be copied or destroyed. This prevents a simple transfer of classical error correction methods, posing a significant hurdle in quantum computation development.

Key Learnings

kl-1: The linking identity [1, p. 8] gives the relationship between average code length, source entropy, and the divergence from assumed to true distribution, and for me, it offers the most intuitive understanding of KL-divergence.

kl-2: While bits can be encoded in qubits, the inverse isn't true, presenting challenges in information theory. However, since observations of quantum systems collapse to classical states, bits remain the fundamental information unit epistemologically, despite the richer ontological structure of qubits.

kl-3: Digital information's abstraction from physical reality has been key to its scalability and dominance. Quantum information theory, however, is more intimately tied to physical realities. While quantum information theory can optimize specific tasks, digital information remains more practical for a broader range of applications. This contrast between digital and quantum information highlights a fundamental scalability trade-off: the ease and flexibility of scaling digital information systems versus the physical tethering of quantum systems.

kl-4: We can never achieve perfect certainty that a message is received perfectly when sent through a channel, but we can engineer systems to guarantee arbitrarily high certainty depending on how much we are willing to sacrifice in latency, throughput, money etc.

kl-5: Achieving maximum coding capacity with negligible error is only theoretically possible for infinitely long messages. Current research focuses on optimizing coding schemes for practical message lengths. However, another line of research seeks to construct coding schemes with tolerably non-negligible errors, but potentially higher capacity.

kl-6: I think we are gradually gaining insight into compression as a form or requisite of intelligence (I'm thinking of GPTs as fancy text compressors which then miraculously mimic intelligence). Synthesizing this with the thought "data compression emphasizes structure" [1, p. 38] we might benefit from looking at intelligence as the thing that identifies and encodes structure while intelligently discarding unstructure.

Quantum Information and Computation 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 a qubit changes erroneously from $|0\rangle$ to $|1\rangle$. However, qubits are additionally susceptible to phase errors, e.g. a state like $\alpha|0\rangle + \beta|1\rangle$ changing to $\alpha|0\rangle - \beta|1\rangle$.

There are very fresh reports that a team at AWS have improved quantum error correction 100-fold by separating out the different types of qubit flips and tackling them individually [4], but a technical publication is yet to emerge.

Shor's prime factorization algorithm was published in 1997, and the first successful implementation only 4 years later in 2001 [5], and yet the algorithm still has not been applied to gain a practical speed increase compared to classical computers, so naturally a great deal of the energy and money going to into quantum research has been on incremental improvements to implementations.

There are two main approaches to making progress on practical applications of quantum systems to information and computation problems: 1. To design algorithms with lower coherence requirements, 2. To design physical devices with better coherence guarantees. Progress on the algorithms side in relation to the variational eigenvalue solving was published in 2014 [2]. The technique has much lower requirements for coherence than the quantum phase estimation algorithm, and therefore made some computations newly feasible. However, satelite-based entanglement distribution [6], a landmark technology introduced in 2017, drastically increased practical coherence distance without a big increase in coherence time.

Harremoës and Topsøe [1, p. 38] noted that the *additivity conjecture* remained unproven in 2008, but that same year Smith and Yard [3] published a counterexample to the conjecture, two quantum channels each with zero capacity, but when combined have non-zero capacity. The unsettling implication is that the capacity of a quantum channel does not fully describe its ability to transmit information.

Quantum Information and Computation from now until 2028

We inch closer to quantum engineering capabilities that we know theoretically will be highly disruptive. The trend lines of quantum coherence guarantees and quantum algorithm requisites are steadily converging. But, I think there is also a good possibility of new breakthrough technologies emerging more quickly out of the blue. The key to quantum information and computation is in leveraging its fundamental oddities, and I think there is still a great deal of headroom in exploring the truly novel capabilities quantum information might facilitate when we unshackle ourselves from classical idioms. The discovery that certain quantum channels are *non-additive* is an example of the kind of out-of-the-blue quantum weirdness that might lead to equally surprising practical applications in the coming years.

The classical computation framework already serves us very well for tackling almost any problem, albeit at limited scales, and so researchers in quantum will focus on tasks where the quantity, the scale, has a quality of its own.

References

[1] Peter Harremoës and Flemming Topsøe. "The Quantitative Theory of Information". In: *Philosophy of Information*. Elsevier, 2008. Chap. 1, p. 171.

[2] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O'Brien. "A variational eigenvalue solver on a photonic quantum processor". In: *Nature Communications* 5.1 (July 23, 2014), p. 4213. ISSN: 2041-1723. DOI: 10.1038/ncomms5213. URL: https://doi.org/10.1038/ncomms5213.

[3] Graeme Smith and Jon Yard. "Quantum Communication with Zero-Capacity Channels". In: *Science* 321.5897 (2008), pp. 1812–1815. DOI: 10.1126/science.1162242. eprint: https://www.science.org/doi/pdf/10.1126/science.1162242. URL: https://www.science.org/doi/abs/10.1126/science.1162242.

[4] Matt Swayne. *AWS Reveals Quantum Chip That Suppresses Bit Flip Errors By 100X*. Nov. 2023. URL: https://thequantuminsider.com/2023/11/29/aws-reveals-quantum-chip-that-suppresses-bit-flip-errors-by-100x/ (visited on 12/01/2023).

[5] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". In: *Nature* 414.6866 (Dec. 2001), pp. 883–887. ISSN: 1476-4687. DOI: 10.1038/414883a. URL: https://doi.org/10.1038/414883a.

[6] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. "Satellite-based entanglement distribution over 1200 kilometers". In: *Science* 356.6343 (2017), pp. 1140–1144.