Quantum information science: Current developments and terra incognita

Mark M. Wilde
Louisiana State University

June 13, 2016

Abstract

It's surely an exciting time to pursue research in quantum information science. With a number of experimental groups the world over making remarkable advances on developing various quantum computing platforms, such as superconducting qubits [1] and semiconductor spin qubits [2], it is inevitable that we will soon have small-scale quantum computers, consisting of tens or perhaps even hundreds of qubits. In the near term, these small-scale quantum computers will not necessarily be fault tolerant or be able to perform Shor's famous factoring algorithm [3], but many strongly suspect that small-scale quantum computers should be able to outperform classical computers at various tasks, such as the simulation of quantum systems and certain quantum chemistry calculations [4]. The experimental group at IBM has already made their five-qubit superconducting quantum computer available through the IBM cloud [5], such that anyone in the world can access it and perform whatever five-qubit quantum algorithm they can think of. This has led to a number of theory groups accessing the platform and conducting experiments on it that had never been conducted before [6, 7, 8, 9]. Companies such as Google and Microsoft also have dedicated research teams working on developing quantum computers. The challenge for experimental quantum computing over the next few years will be to scale up to more qubits and to reduce the amount of noise present in these small-scale quantum computers, by both hardware and software improvements.

In step with experimental quantum computing progress, there have been impressive advances in quantum communication experiments as well. Perhaps the most notable is the recent loophole-free violation of a Bell inequality [10], but we'll need a little background before discussing it. To put this experiment into context, we have to go all the way back to 1935. One of the most well known early (but ultimately mistaken) criticisms of quantum mechanics was put forward in a paper by Einstein, Podolsky, and Rosen (EPR) in 1935 [11], in which they argued quantum mechanics to be incomplete. In short, they thought that one could construct a situation in which Heisenberg's uncertainty principle [12] could be violated, and they also argued that any theory of nature should be local, in the sense that distant particles should not be able to affect each other, and "real," in the sense that attributes of the particles, such as position or momentum, should always have definite values. Many years went by, and then in 1964 Bell devised a way to test whether the predictions of EPR were correct [13]. That is, Bell proved a mathematical bound on two-particle correlations that applies if the particles obey EPR's principles of local realism (as they would in a classical theory), but he also showed that quantum particles could violate this bound. This test

is now known as a Bell inequality and has a number of experimentally challenging requirements in order to demonstrate it convincingly. There should be two parties involved, traditionally called Alice and Bob, who possess one particle each and have a significant spatial separation between them, such that a referee could in principle send questions to Alice and Bob and they should respond quickly with answers. The long distance between Alice and Bob is necessary to make sure that they cannot communicate the questions to each other before they output their answers. Also, they should possess very good detectors of their particles so that there are few missed events (i.e., they nearly always respond for a given test). If these two requirements are not met, then the test is said to have loopholes: the first known as the locality loophole and the second as the detection loophole. A number of experimental groups have conducted tests of the Bell inequality for a long time (see references in [10]), but many of these experiments could not close both of the aforementioned loopholes at the same time.

However, for the first time, last year an experimental group demonstrated a "loop-hole free" violation of a Bell inequality in which both of the above loopholes were closed [10]. One of the main ideas behind the loophole-free experiment was actually to employ another idea of Bell [14], in which there is an "event-ready" signal to determine whether a given experiment will take place or be called off. The experiment from [10] featured three separate laboratories: one for Alice, one for Bob, and one (call it Charlie's lab) to determine the event-ready signal. In the laboratory of Alice, she prepares two particles in an entangled state: one is the spin of a nitrogen vacancy center in a diamond and the other is a photon.[1] The photon is sent off to Charlie. The same exact procedure occurs in Bob's lab. Charlie then performs a quantum measurement of the two photons received from Alice and Bob, which if successful, has the effect of swapping the entanglement such that Alice and Bob's spins become entangled. Local measurements randomly selected from a fixed set (corresponding to questions of the referee) are then performed on Alice and Bob's spins, and the measurement outcomes are recorded. This way of performing the experiment has the effect of closing both loopholes: sending the photons to Charlie and having an event-ready signal overcomes the locality loophole, while measuring the spins overcomes the detection loophole because there are very efficient detectors for spins. The result of the experiment in [10] is to demonstrate that classical mechanics (at least in the form of EPR's local realism) cannot describe the very strong correlations that quantum particles can share. We really do live in a universe not described by local realism! A great challenge for the future is to increase the distance over which such an experiment can be carried out and to increase the rate of event-ready signals generated.

The result of the above experiment certainly has had profound implications for the foundations of quantum mechanics, demonstrating that entangled particles cannot be described by the classical theory of local realism. On the other hand, one might wonder whether the experiment has any practical consequences. The exciting answer is yes; indeed, there are strong practical applications for the generation of random numbers [15] and secret keys for secured communication [16].

Here, let's focus on the application to quantum key distribution. One protocol for quantum key distribution (QKD) was invented in 1984 by Bennett and Brassard (BB84) [17], whereby they proposed to use encodings in quantum states in order to generate a secret key that could be ultimately shared by spatially separated parties Alice and Bob. Once Alice and Bob share a secret key, they could use it in a "one-time pad" protocol to encrypt a message as long as the key (but no longer). The latter protocol of the one-time pad was known for quite some time in advance of BB84, but the novelty of BB84's proposal was to solve the key distribution problem via quantum

[1] You can think of an entangled state as a "super-correlated" quantum state of these two particles.

mechanics. Another protocol for quantum key distribution is more closely linked with Bell tests of entanglement. A number of years after BB84, Ekert proposed to use Bell inequalities to certify whether Alice and Bob possess entangled states from which they could generate secret keys [18]. He realized that if Alice and Bob indeed possess entangled particles, this implies that no other third party could share correlations with their particles, a property now known as the monogamy of entanglement. This approach to QKD is now known as entanglement-based QKD or also as device-independent QKD, because the protocol is specified independent of the devices in which it is operating. Alice and Bob merely feed in classical inputs to the protocol, they receive classical outputs from it, and they decide whether a secure key has been generated based on deterministic rules applied to the classical inputs and outputs.

It turns out that device-independent QKD relies on a loophole-free experiment of the sort in [10] in order to guarantee security. The main concern with realistic implementations of QKD is that there might be security loopholes in an implementation not accurately described or realized by the theory. So these device-independent protocols aim to remove all such loopholes by relying on a loophole-free Bell test. The way that a device-independent QKD protocol works is that Alice and Bob are located at a large distance from each other and another party, who could even be a malicious party, sends them entangled particles (one to each). As mentioned above, they conduct Bell experiments on randomly chosen subsets of the particles to certify whether they really are entangled. If a sufficient number of the Bell experiments succeed, then this guarantees that another fraction of the entangled particles can be used to generate secret keys, as was proved recently in [16]. It is a major open question to devise security proofs that can guarantee larger noise tolerance and higher rates of secret key generation. There are also still huge experimental challenges to be solved before this kind of protocol will become a reality.

We'll now move on to the frontier of quantum communication theory developments. For the past few years, a number of quantum information theorists have been focusing their efforts on what tasks can be accomplished with a small number of qubits (motivated in part by current experimental concerns), and this has certainly pushed the theory forward in remarkable ways that were perhaps not thought to be possible a decade or so ago. One central object of study in quantum information theory is a noisy communication channel, which is meant to model a realistic physical link between Alice and Bob. Such a channel could be a fiber-optic link, a wireless link, a satellite-to-satellite link, etc. For such channels, we would like to know their ultimate abilities for transmitting information, and to do so we need to model them in a fully quantum mechanical way [19]. For example, Alice and Bob might be interested in communicating classical, ordinary bits, or quantum bits, or they might even share entanglement before communication begins. These various tasks lead to different capacities of a communication channel, known as the classical capacity, the quantum capacity, and the entanglement-assisted capacity, respectively (see [20] for a review of these concepts). Additionally, private capacity corresponds to the scenario in which the goal is to generate secret classical bits using a communication channel, and as such, it is relevant as a benchmark for the performance of QKD protocols.

The capacity of a quantum channel has traditionally been defined in an asymptotic way, meaning that we allow Alice and Bob as many independent uses of a given channel as they need in order to make the communication error as low as possible. The rate of communication is equal to the number of bits transmitted per channel use, and the classical capacity of a quantum channel is equal to the maximum rate of communication such that the error probability becomes arbitrarily small. The quantum capacity is defined in the same way as the classical capacity, except that the

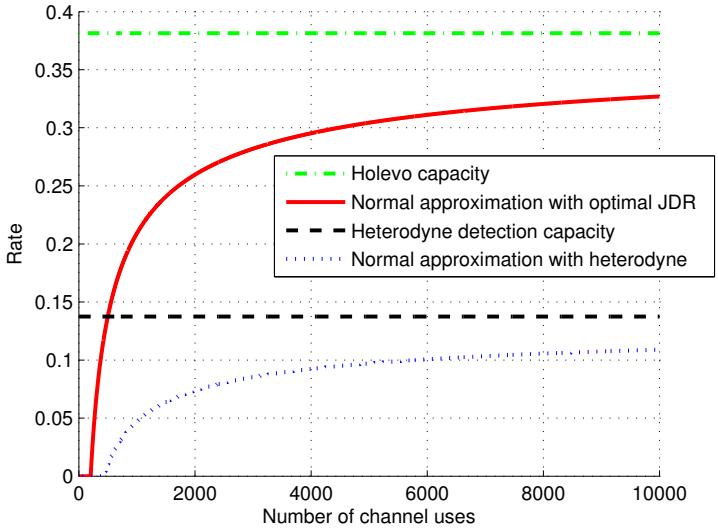

Figure 1: Figure taken from [21]. Comparison of ultimate capacity (top line) of a lossy optical channel, with approximation (red line) of achievable rates and number n of channel uses for error probability $\varepsilon = 10^{-6}$, capacity with a classical detection strategy (dashed black line), and approximation (dotted blue line) to what is achievable for finite number of channel uses with a classical detection strategy.

rate is quantified in terms of the number of qubits transmitted per channel use and communication error is measured in a different way. Researchers have made great progress on capacity questions over a long time period and have been able to determine the capacities of a number of important communication channels.

However, as discussed above, the notion of capacity is an asymptotic concept and so has limited applicability in practical settings in which the number of channel uses might be severely limited. Consider, for example, that the current state of the art in quantum computing is the coherent manipulation of only five to ten qubits. Thus, this has motivated researchers to develop a theory of quantum communication that applies to the transmission of information using a small number of quantum systems. The typical finding in many studies [22, 23, 24, 21, 25, 26] is that we can approximate communication rates over quantum channels with two numbers, that are each a function of the quantum channel of interest. To describe these results, let us denote a quantum channel by the symbol $\mathcal{N}$ (for "noise"), and let us denote n independent uses of this channel by $\mathcal{N}^{\otimes n}$. Then we can let $R^*(\mathcal{N}^{\otimes n}, \varepsilon)$ denote the maximum rate at which we can send classical bits by using a channel n times and such that the error probability is no larger than a number $\varepsilon \in (0, 1)$. What many recent studies have found is that the following approximation is a good one for several channels of interest:

$$R^*(\mathcal{N}^{\otimes n}, \varepsilon) = C(\mathcal{N}) + \sqrt{V(\mathcal{N})/n}\Phi^{-1}(\varepsilon) + O([\log n]/n), \tag{1}$$

where $C(\mathcal{N})$ is the capacity of the channel (always non-negative and found for several channels in earlier studies), $V(\mathcal{N})$ is a new, non-negative quantity known as the dispersion of the channel, and $\Phi^{-1}(\varepsilon)$ is the inverse of the cumulative Gaussian distribution function, which is negative whenever

$\varepsilon < 1/2$. The capacity and the dispersion are often simple functions to compute when given a mathematical description of a quantum communication channel. So characterizations like that in (1) capture all of the earlier works on capacity, because taking the limit as $n \to \infty$ leaves only the capacity term. But they say more because they provide a refinement of capacity for a finite number n of channel uses. The second term $\sqrt{V(\mathcal{N})/n}\Phi^{-1}(\varepsilon)$ represents the backoff from capacity for any fixed n and ε, and it can be derived by employing strong refinements of the central limit theorem from probability theory, in addition to some other mathematical manipulations. Figure 1 (taken from [21]) plots this approximation as a function of n for the "pure-loss" channel, which models the loss of photons transmitted over a fiber-optic link. The figure also plots the rates achievable using a traditional detection strategy at the channel's receiving end, known as heterodyne detection. The figure demonstrates that there can be significant gains over classical detection strategies by employing a fully quantum detection strategy. The plot in the figure is typical of findings in recent studies in quantum information theory and demonstrates how capacity is really an asymptotic quantity, only approachable in the limit of many channel uses. At the same time, there can be a significant backoff from capacity when using the channel only a finite number of times.

There are currently many open directions to pursue regarding finite-size quantum information theory. Is it possible that a formula like that in (1) could describe achievable rates for any task and any channel? This is an extreme challenge, representing wide open territory, but I would guess likely not solvable in the near future as we do not even know the capacity term for several channels and a number of information processing tasks. Nevertheless, it would be prudent to push forward in this direction for the channels of the highest practical interest. In the absence of general formulas, can we establish bounds on the left-hand side of (1) for various tasks? Progress in this direction has been accomplished in [23, 24, 25, 26]. Can we establish bounds in the context of network channels, with multiple senders or multiple receivers? This would be applicable to communication in a network setting, and thus relevant in more general contexts. Can we go beyond the independent and identically distributed setting of a channel of the form $\mathcal{N}^{\otimes n}$ and instead consider channels with memory [27] or less restrictive structure? The Beyond i.i.d. conference series was born in 2013 and has recurred on an annual basis to address these questions and more.

In summary, I believe that it is more than ever an exciting time to pursue research in quantum information science, whether it be of an experimental or theoretical flavor, as there remain a number of great challenges to overcome to bring quantum technologies closer to reality. At the same time, I believe that quantum information science is a good bet, as I expect that we will be seeing several of these quantum technologies put to good use to improve upon what one can accomplish using classical strategies alone.

References

[1] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339(6124):1169–1174, March 2013.

[2] M. Veldhorst, J. C. C. Hwang, C. H. Yang, A. W. Leenstra, B. de Ronde, J. P. Dehollain, J. T. Muhonen, F. E. Hudson, K. M. Itoh, A. Morello, and A. S. Dzurak. An addressable quantum dot qubit with fault-tolerant control-fidelity. *Nature Nanotechnology*, 9(12):981–985, December 2014. arXiv:1407.1950.

[3] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Scientific Computing*, 26(5):1484–1509, October 1997. arXiv:quant-ph/9508027.

[4] B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik, and A. G. White. Towards quantum chemistry on a quantum computer. *Nature Chemistry*, 2(2):106–111, February 2010. arXiv:0905.0887.

[5] IBM. The quantum experience. URL http://www.research.ibm.com/quantum/, 2016.

[6] Daniel Alsina and José Ignacio Latorre. Experimental test of Mermin inequalities on a 5-qubit quantum computer. May 2016. arXiv:1605.04220.

[7] Simon J. Devitt. Performing quantum computing experiments in the cloud. May 2016. arXiv:1605.05709.

[8] R. P. Rundle, Todd Tilma, J. H. Samson, and M. J. Everitt. Quantum state reconstruction made easy: a direct method for tomography. May 2016. arXiv:1605.08922.

[9] Mario Berta, Stephanie Wehner, and Mark M. Wilde. Entropic uncertainty and measurement reversibility. November 2015. arXiv:1511.00267.

[10] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, October 2015. arXiv:1508.05949.

[11] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[12] Werner Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Zeitschrift für Physik*, 33:879–893, 1925.

[13] John Stewart Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[14] John Stewart Bell. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press, 2004.

[15] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. *In Proceedings of the 44th symposium on Theory of Computing, STOC '12*, pages 61–76, 2011. arXiv:1111.6054.

[16] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113(14):140501, September 2014. arXiv:1210.1810.

[17] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[18] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[19] Jeffrey H. Shapiro. The quantum theory of optical communications. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1547–1569, November 2009.

[20] Mark M. Wilde. From classical to quantum Shannon theory. 2016. arXiv:1106.1445v7.

[21] Mark M. Wilde, Joseph M. Renes, and Saikat Guha. Second-order coding rates for pure-loss bosonic channels. *Quantum Information Processing*, 15(3):1289–1308, March 2016. arXiv:1408.5328.

[22] Marco Tomamichel and Masahito Hayashi. A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Transactions on Information Theory*, 59(11):7693–7710, November 2013. arXiv:1208.1478.

[23] Marco Tomamichel and Vincent Y. F. Tan. Second-order asymptotics for the classical capacity of image-additive quantum channels. *Communications in Mathematical Physics*, 338(1):103–137, August 2015. arXiv:1308.6503.

[24] Nilanjana Datta, Marco Tomamichel, and Mark M. Wilde. On the second-order asymptotics for entanglement-assisted communication. *Quantum Information Processing*, 15(6):2569–2591, June 2016. arXiv:1405.1797.

[25] Marco Tomamichel, Mario Berta, and Joseph M. Renes. Quantum coding with finite resources. *Nature Communications*, 7:11419, May 2016. arXiv:1504.04617.

[26] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. February 2016. arXiv:1602.08898.

[27] Filippo Caruso, Vittorio Giovannetti, Cosmo Lupo, and Stefano Mancini. Quantum channels and memory effects. *Reviews of Modern Physics*, 86(4):1203–1259, December 2014. arXiv:1207.5435.