The Quantum Times

Volume 5, Number 2
Third Quarter, 2010

Newsletter of the Topical Group on Quantum Information

American Physical Society

Inside this issue
- Eve defends herself, p.3
- Hacking the unhackable, p.4
- Book review: Byrne's bio of Everett, p.5
- Quantum simulation: dream or nightmare?, p.7

Trading Resources in Quantum Communication

Mark M. Wilde and Min-Hsiu Hsieh

A quantum channel has different capacities for communication, depending upon the type of information being transmitted and whether assisting resources are available. For example, an information processing task could generate or consume public classical communication, private classical communication, secret key, quantum communication, and entanglement along with the consumption of many uses of a quantum channel. An optimization question then arises for future "quantum telephone companies": How can we optimally trade these resources for a given quantum channel? Here, we do not answer the full question for all five resources, but instead overview two different but related trade-off questions.

The transmission of information over a noisy quantum channel is one of the fundamental tasks in quantum Shannon theory. This theory bears many similarities with Shannon's classical theory, but it also admits several striking differences because a quantum channel has various capacities for information transmission, depending upon the type of resource that a sender wishes to transmit to a receiver and whether any assisting resources are available [1]. Several examples of resources that we can consider are public classical communication, private classical communication, secret key, quantum communication, and entanglement.

A quantum channel has a capacity for generating each of the aforementioned resources on its own, but one can also consider the task of transmitting some of the resources simultaneously, while using others for assistance. The simplest strategy for the simultaneous transmission of different resources is to use a particular communication strategy for one resource for a fraction of the channel uses and employ a different strategy for the other resource for the other fraction of the channel uses. This naive strategy is known as time-sharing, but it is often not the optimal strategy. For example, consider the case where a sender would like to transmit both classical and quantum information [4]. Time-sharing is the optimal strategy for certain channels such as the noiseless qubit channel and the quantum erasure channel, but it is not the optimal strategy for other channels such as the dephasing channel [4].

In recent work, we have made much progress in understanding two different trade-off settings [2, 5, 6, 7, 8, 9, 10]. The first setting involves the trade-off between classical communication, quantum communication, and entanglement when many uses of a quantum channel are available [2, 6, 7, 8, 10]. In this first setting (the CQE setting), we do not distinguish whether the classical communication is public or private. Our main result in these works is a theorem that we call the quantum dynamic capacity theorem. It gives the full trade-off between these resources regardless of whether a given protocol generates or consumes them in addition to the usage of the quantum channel. We also found an important formula that characterizes this trade-off, and we showed how additivity of it allows one to simplify the description of the three-dimensional capacity region [10]. A

Continued on next page

careful analysis of this formula even leads to an explicit analytic description of the capacity region for several channels such as erasure channels, dephasing channels, and cloning channels.

The second trade-off setting we have considered is that between public classical communication, private classical communication, and secret key [5, 9]. Our goal in the second setting (the RPS setting) was to study the information-theoretic analog of the Collins-Popescu analogy—this analogy states that classical communication, quantum communication, and entanglement tend to interact with each other similarly to the way that public classical communication, private classical communication, and secret key interact [3]. The latest work in Ref. [9] gives a capacity theorem that is analogous to the quantum dynamic capacity theorem. We also found another important formula that plays an analogous role in this setting, and we can compute and plot the capacity region for several examples of channels.

We review here the important results and a simple example. The requisite protocols for achievability in the CQE setting are teleportation, super-dense coding, entanglement distribution, and a protocol we named the classically-enhanced father protocol [8]. The classically-enhanced father protocol exploits the "piggybacking" technique from Ref. [4] in order to "piggy-back" classical information "on top of" entanglement-assisted quantum codes. The cleanest method we have developed for proving the converse part of the capacity theorem is the catalytic, information-theoretic proof in Section 4 of Ref. [10]. This technique assumes that the sender and receiver have some amount of each resource in the CQE setting available for consumption and that they are trying to generate each resource as well. We then obtain bounds on the net rates for each resource, regardless of whether the protocol ends up generating or consuming it.

The important protocols for achievability in the RPS setting are a protocol we named the publicly-enhanced private father protocol [5], the one-time pad, private-to-public transmission, and secret key distribution. The publicly-enhanced private father protocol is analogous to the classically-enhanced father, and we even exploited similar techniques for proving its achievability. Section 4 of a recent paper also develops a catalytic, information-theoretic converse proof for this setting [9]. The main difference between this setting and the CQE setting is the lack of an analogy of the super-dense coding protocol, as Collins and Popescu first observed [3]. This has dramatic consequences for the shape of the RPS capacity region when compared to the CQE region.

One of the major contributions of these works is the analysis of the capacity regions for several examples of channels. Brádler et al. first realized that a particular class of channels, known as the Hadamard channels, have "single-letter" capacity regions, meaning that it is only necessary to evaluate the formulas for the region over one use of the channel [2]. Channels in this class include the practically relevant dephasing channels and cloning channels. Our later work follows up on this result in full generality for the CQE and RPS settings [9, 10], while also including proofs for the erasure channel. Figure 1 plots both capacity regions for the qubit dephasing channel with dephasing parameter equal to 0.2.

Continued on next page

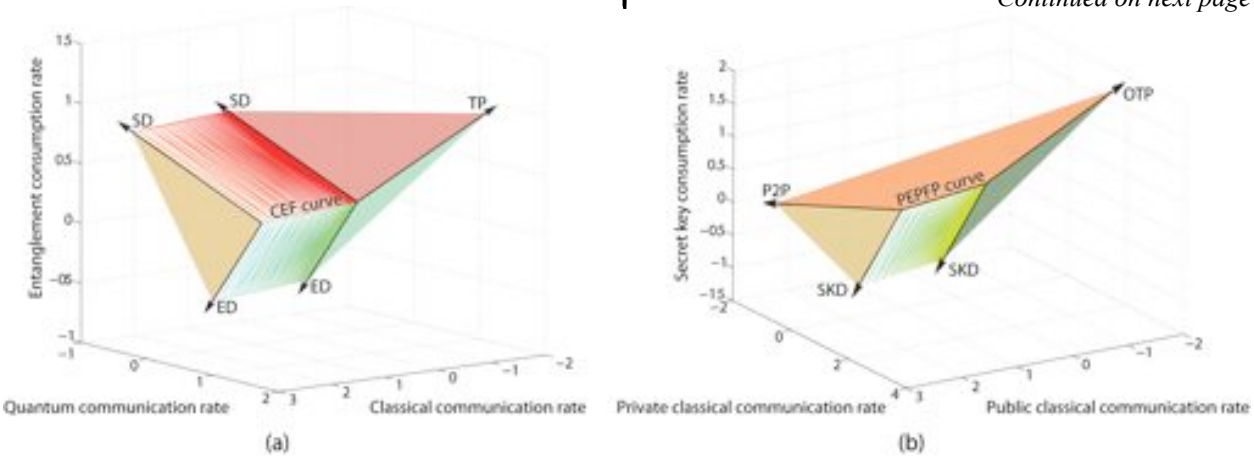


Figure 1: The capacity regions for a qubit dephasing channel with parameter p = 0.2. (a) The classically-enhanced father (CEF) trade-off curve lies along the boundary of the capacity region. The rest of the region is the combination of the CEF points with teleportation (TP), super-dense coding (SD), and entanglement distribution (ED). (b) The private dynamic triple trade-off for the same channel. P2P is in the direction of private-to-public transmission, SKD is in the direction of secret-key distribution, OTP is in the direction of the one-time pad protocol, and PEPFP is the publicly-enhanced private father trade-off curve. The region exhibits a non-trivial resource trade-off only on the surface below the PEPFP trade-off curve in the direction of secret key distribution. Observe that the two regions are dramatically different: (a) has two regions where non-trivial trade-offs occur, but (b) has only one.

Wilde & Hsieh, continued

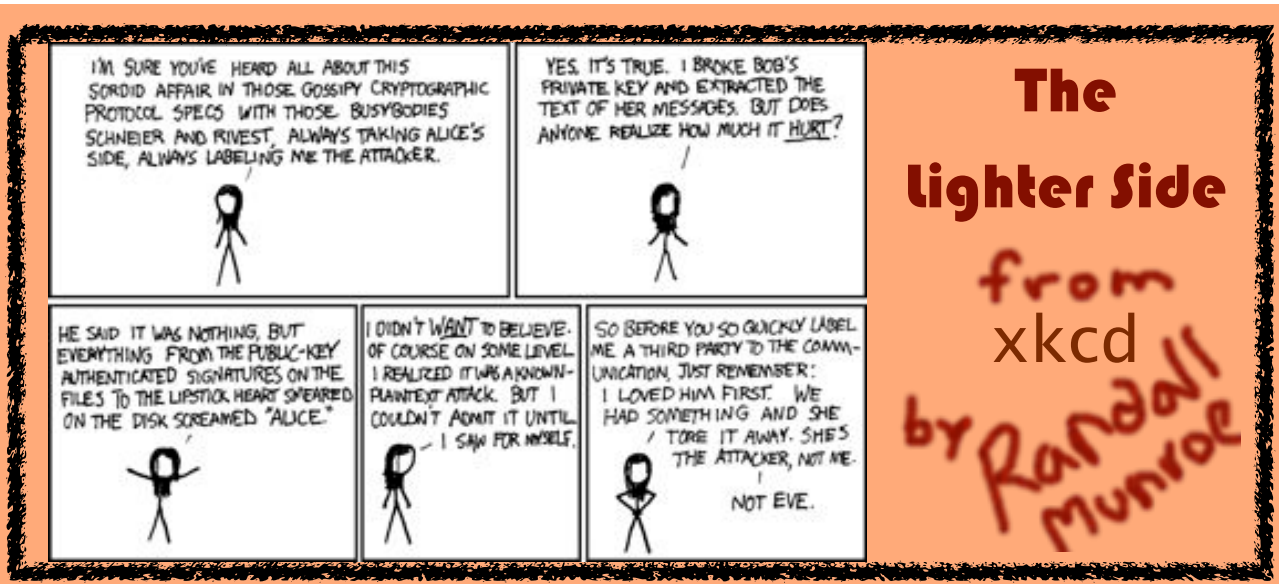
There are many questions to consider going forward for this line of inquiry. Are there other examples of channels besides Hadamard or erasure channels for which we can obtain analytic expressions for the capacity regions? Are there other interesting trade-offs to consider besides the ones that we have studied so far? What is the analysis for the capacity regions of bipartite quantum states instead of quantum channels? (We have a solution for the CQE region of a state in Ref. [7], but the analysis is not quite as clean as those for channels in Refs. [9,10].) What are the trade-offs for communication settings in network quantum Shannon theory? The answers to these and other questions should further illuminate the nature of information transmission over quantum channels.

We acknowledge the many useful conversations with our colleagues Kamil Brádler and Dave Touchette and those with our mentors David Avis, Igor Devetak, and Andreas Winter. We are especially grateful to Patrick Hayden for his guidance, insight, and encouragement.

References

1. Charles H. Bennett and Peter W. Shor. Quantum channel capacities. *Science*, **303**(5665): 1784-1787, March 2004.
2. Kamil Brádler, Patrick Hayden, Dave Touchette, and Mark M. Wilde. Trade-off capacities of the quantum Hadamard channels. To appear in *Physical Review A*, 2010. arXiv:1001.1732.
3. Kamil Brádler, Patrick Hayden, Dave Touchette, and Mark M. Wilde. Trade-off capacities of the quantum Hadamard channels. *Physical Review A* 81, 062312 (2010).
4. Igor Devetak and Peter W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, **256** (2):287-303, 2005.
5. Min-Hsiu Hsieh and Mark M. Wilde. Public and private communication with a quantum channel and a secret key. *Physical Review A*, **80**(2): 022306, August 2009.
6. Min-Hsiu Hsieh and Mark M. Wilde. *Theory of Quantum Computation, Communication, and Cryptography*, volume 5906 of *Lecture Notes in Computer Science*, chapter Optimal Trading of Classical Communication, Quantum Communication, and Entanglement, pages 85-93. Springer-Verlag, May 2009.
7. Min-Hsiu Hsieh and Mark M. Wilde. Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. *IEEE Transactions on Information Theory*, **56**, pp.4705-4730, September 2010. arXiv:0901.3038.
8. Min-Hsiu Hsieh and Mark M. Wilde. Entanglement-assisted communication of classical and quantum information. *IEEE Transactions on Information Theory*, **56**, pp. 4682-4704, September 2010. arXiv:0811.4227.
9. Mark M. Wilde and Min-Hsiu Hsieh. Public and private resource trade-offs for a quantum channel, May 2010. arXiv:1005.3818.
10. Mark M. Wilde and Min-Hsiu Hsieh. The quantum dynamic capacity formula of a quantum channel. April 2010. arXiv:1004.0458.

Mark M. Wilde *is a postdoctoral fellow with the Quantum Computing Group in the School of Computer Science at McGill University.* ***Min-Hsiu Hsieh*** *is with the ERATO-SORST Quantum Computation and Information Project of the Japan Science and Technology Agency in Tokyo, Japan. Both completed their PhDs in Electrical Engineering in 2008 at the University of Southern California under the supervision of Todd Brun. The opinions expressed here are their own and do not reflect those of any other organization or individual.*



Bits, BYTES, and Qubits

QUANTUM NEWS & NOTES

Photonic quantum computers...

A team of physicists led by Jeremy O'Brien of the UK's Centre for Quantum Photonics at Bristol University has created an ultra-fast optically driven computer chip a fraction of the size of a penny. The chip consists of 21 coupled and parallel optical waveguides, each about 700 μm in length. The individual waveguides are separated by about 2.8 μm for a short distance thus allowing light to leak from one waveguide to another, thus putting the leaked photons into a superposition of two possible paths. The result is similar to the behavior of light passing through a beamsplitter. The 21 parallel waveguides allows pairs of photons to take a quantum walk which would enable the chip to implement certain quantum computing search algorithms. Theoretically these quantum algorithms solve certain problems considerably faster than their classical counterparts.

With a 2.8 μm separation, connecting the output to individual photon detectors would have been nearly impossible. As such, the waveguides fan out to a separation of 125 μm. But in order to do this with typical waveguides, which usually consist of silicon dioxide cores clad in silicon, the waveguides would have needed to be several meters long to prevent photon absorption at bends in the guide itself. So instead, O'Brien's group created waveguides using silicon oxynitride.

In addition to the researchers from Bristol, the group led by O'Brien included researchers from Tohuku University in Japan, the Weizmann Institute in Israel and Twente University in the Netherlands. The research was published in the September 16th issue of *Science*.

...or graphene quantum computers?

Why not both? Quantum dot-based quantum computing has been around for quite some time and utilizes spin as its basic binary property. But these implementations generally suffer from problems of decoherence due to spin-orbit interactions and hyperfine splitting. As it turns out, however, the use of graphene in place of conventional semiconductor materials can overcome these problems and delay decoherence, according to a paper recently published in *Physical Review Letters* by a group at ETH Zürich consisting of Johannes Güttinger, Tobias Frey, Christoph Stampfer, Thomas Ihn, and Klaus Ensslin.

The quintet studied both ground and excited state transport through small (d = 70 nm) graphene quantum dots. Of interest is how the spin successively fills orbital states. This is detected by measuring the ground state energy as a function of a magnetic field. The group measured both out-of-plane (perpendicular) and in-plane (parallel) magnetic fields. For the in-plane case, they measured the Zemann splitting of the spin states, obtaining results compatible with a g-factor of 2. The out-of-plane case exhibited a linear Zeeman splitting.

More problems for peer review

Stefan Thurner and Rudolf Hanel of the Medical University of Vienna in Austria have conducted a ground-breaking study of the peer review system and have found that even a very small number of poor referees can fairly dramatically reduce the overall quality of the scientific papers that end up being published. Thurner and Hanel created a generic discipline which they then assumed was populated by a group of scientists whose quality followed a Gaussian (normal) distribution. What they found was that when a mere one-tenth of the referees behaved in what they deemed a detrimental way, the quality of accepted papers dropped by a full standard deviation. If that number increased enough, quality dropped so far as to be indistinguishable from randomness, i.e. the system didn't perform much better than it would have had papers been chosen for publication by simply flipping a fair coin. Whether it was intentional or simply ironic, their paper has (so far) only appeared on the arXiv preprint server.

But quantum cryptography is reliable, right?

Peer-review is in danger, Arctic sea ice is melting, and there's oil sludge on the bottom of the Gulf of Mexico. At least we can rely on quantum cryptography in an increasingly unreliable world... or so we thought.

Plenty of loopholes in quantum cryptography have been identified over the years, but all were eventually closed (for the most part). Some weaknesses were identified in a theoretical paper by Aysajan Abidin and Jan-Åke Larsson, both with Linkoping University, last year, but suggestions for reducing this weakness were provided in the very same paper.

Now comes word that a group at the Norwegian University of Science and Technology in Trondheim and the Max Planck Institute for the Science of Light in Erlangen, Germany, has successfully "hacked" a commercial quantum cryptographic system, fully retrieving the key while leaving no trace of their presence. How is this possible, you ask? The nature of quantum mechanics seems to indicate that Eve can't obtain information about the key without unintentionally announcing her presence.

The method the group used was deceptively simple and ingenious. Since all existing commercial quantum cryptographic devices are photonic, the information carrier, i.e. the light, can be quantum or it can be

Continued on next page

classical. Thus the team simply blasted Bob's detector with a laser while intercepting Alice's data and then sending Bob a classical bit. Since the detectors always register a 0 or a 1, they can't tell the difference between a classical and a quantum bit. In other words, while Eve can't *copy* a qubit sent by Alice she can *measure* it. This destroys the qubit, but since the end result will necessarily be a 0 or a 1, Eve can then simply send a *classical* 0 or 1 along to Bob whose detector can't tell the difference.

The group tested the hack on two commercially available systems – one from ID Quantique of Geneva and one from MagiQ Technologies of Boston – and it successfully worked on both. The results were shared with company officials before publishing the work so that appropriate patches could be made available. Group member Vadim Makarov was quick to point out that quantum cryptography is still the most secure cryptographic system in existence. The research appeared in *Nature Photonics*.

Guess what your neighbor is thinking

Entanglement (and thus nonlocality) is, arguably, at the heart of almost everything in quantum information. The no-signaling theorem, however, prevents us from exploiting this to transmit information faster than the speed of light, hence (supposedly) preserving causality. So now imagine N people arranged in a circle. Each player receives a bit (a 0 or a 1) to start off with. Then each player guesses what bit their neighbor on their right received and emits the matching bit. The distribution of possible input bits is known at the start but, otherwise, there is no communication among the players. Winning the game amounts to having the highest number of correct guesses after a certain number of rounds. Clearly signaling of some sort (in which one player communicated his or her bit to another) would make this game a lot easier.

But would quantum correlations necessarily be more advantageous than classical correlations? Not according to Mafalda L. Almeida (ICFO), Jean-Daniel Bancal (Genève), Nicolas Brunner (Bristol), Antonio Acín (ICFO/ICREA), Nicolas Gisin (Genève), and Stefano Pironio (Bruxelles) in an article appearing in *Physical Review Letters*. In this case, quantum correlations do not proffer an advantage. However, somewhat surprisingly, they demonstrate that if the correlations are governed *solely* by the no-signaling theorem, players can actually outperform both the quantum and classical scenarios. What this ultimately means is that, in multipartite situations, there is a point at which quantum nonlocality is superseded by even stronger correlations. (And now, thanks to this article, your fearless editor has a Gordon Lightfoot song stuck in his head...)

–ITD

book review

The Many Worlds of Hugh Everett III: Multiple universes, mutual assured destruction, and the meltdown of a nuclear family

by Peter Byrne

Oxford University Press, 2010, **$45.00**
ISBN13: 9780199552276
ISBN10: 0199552274

With the publication of Peter Byrne's biography of Hugh Everett, the story of the sometimes troubled life of the father of the many-worlds interpretation of quantum mechanics has finally been released from its abode in dusty boxes stored in a basement in California. As Everett's son Mark put it his foreword to Byrne's book,

> I knew the day was coming when the boxes would have to be opened. I just didn't want to be the one to do it. Although I've been lucky enough to end up being happy with my life (part hard work, part miracle) and feeling at peace with my family history, I still don't relish going back to that world. If I play a concert in the Washington, D.C. area, the moment I step off the plane I can smell death in the air. I was sure those boxes held the same smell...Luckily Peter Byrne came along to smell those boxes for me.

Byrne's well-researched summary of those boxes (and other sources) have brought the enigmatic Hugh Everett back to life.

Hugh Everett's name has (largely posthumously) become associated with one of the most indelible and controversial ideas in modern physics, the many-worlds interpretation of quantum mechanics (the term 'many-worlds' was coined by Bryce DeWitt) despite the fact that his only publication in the field of quantum mechanics was his 1957 PhD thesis. But, while we as people interested in quantum physics may be most interested in the genesis and subsequent ascendancy of this idea, it only consumed a small portion of his life.

More than anything, Hugh Everett's life was defined by his work in operations research where he found his niche in the military-industrial complex essentially attempting to turn ethics and morality into a mathematics problem. In a report for the Weapons Systems Evaluation Group (WSEG), Everett developed the notion of maximizing fatalities from radiation as a function of the total megatonnage utilized in a nuclear attack. He was a strong believer in the idea that the

Continued on next page

best way to prevent a nuclear war was to plan for one. Ironically, chemist Linus Pauling credited Everett and his co-author George Pugh by name in his 1962 Nobel Lecture upon receiving the Nobel Peace Prize for his work on nuclear disarmament.

Everett's work with Pugh, often referred to as the "fallout study," served as a foundation for the now infamous WSEG Report 50 that introduced the notion of assured destruction (referred to by the media as *mutually* assured destruction thanks to its acronym – MAD). This concept was to serve as the dominant paradigm of military planning for most of the remainder of the Cold War.

One of the key ingredients to Report 50 was Everett's generalization of the Lagrange Multiplier method that enabled complex problems to be broken down into smaller, more tractable ones. This generalization came to be known as the Everett Algorithm and has played a key role in operations research ever since. Since the Lagrange Multiplier method (and thus the Everett Algorithm) employed the Greek letter λ (lambda), it is no surprise that when Everett and a few of his colleagues left WSEG to start their own company, they called it Lambda Corporation.

Everett's personal life was partly typical of the times in which he lived except that Everett seemed to take things to extremes. While others merely dabbled in the excesses produced by the liberated culture of the 1960s, Everett imbibed, both figuratively and literally. He was an alcoholic who had trouble with the types of normal conversation that play out in typical middle class American homes and he had a penchant for philandering. John Bell once said that quantum mechanics "carries in itself the seeds of its own destruction." The same might have been said of Hugh Everett.

Peter Byrne's meticulously researched biography provides a detailed and intimate look at one of the most seminal figures in 20th century physics and mathematics. The writing is a bit uneven in spots (most notably in the first few chapters) and the copy editing was surprisingly weak (the book is filled with typographical errors). But, all told, it is a remarkable – and long-overdue – biography. As Susanne Misner (wife of Charles Misner) once apparently said, "Most physicists end up as footnotes." The publication of this remarkable book ensures that Hugh Everett will endure no such fate.

***Ian T. Durham** is the editor of this rag. In his day job, he is Associate Professor and Chair of the Department of Physics and Director of the Computational Physical Sciences Program at Saint Anselm College in Manchester, New Hampshire. He lives on the coast of Maine and blogs about quantum empiricism at http://quantummoxie.wordpress.com. He is on a lifelong quest to avoid ending up as a footnote.*

The Quantum Times is a publication of the Topical Group on Quantum Information of the American Physical Society. It is published four times per year, usually in March, June, September, and December, though times may vary slightly.

Editor
Ian T. Durham
Department of Physics
Saint Anselm College
Manchester, NH
idurham@anselm.edu

Contributions
Contributions from readers for any and all portions of the newsletter are welcome and encouraged. We are particularly keen to receive

- **op-ed pieces and letters** (the APS is *strongly* encouraging inclusion of such items in unit newsletters)
- **books reviews**
- **review articles**
- **articles describing individual research** that are aimed at a broad audience
- **humor** of a nature appropriate for this publication

Submissions are accepted at any time. They must be in electronic format and may be sent to the editor at idurham@anselm.edu. Acceptable forms for electronic files (other than images) include LaTeX, Word, Pages (iWork), RTF, PDF, and plain text.

Editorial policy
All opinions expressed in *The Quantum Times* are those of the individual authors and do not represent those of the Topical Group on Quantum Information or the American Physical Society in general.

op-ed

Quantum Simulation: Dream or Nightmare?

When I was a postdoc at NIST in Gaithersburg in 1994, Artur Ekert came to give the colloquium. Ekert was the person who introduced me (and many of my fellow quantum opticians) to the whole idea of quantum information. I remember plenary talks at Optical Society meetings that he gave on the subject of quantum cryptography and the relationship to Bell's inequalities when I was a graduate student in the early 1990s, and how fascinating it was to learn about the ways in which the strange properties of quantum systems could be put to use for secret key generation. In 1994, just before the time of the colloquium, Shor had developed his groundbreaking algorithm. It had not yet been published, but Ekert told us about it in personal discussions. He was, understandably, very excited about this development and the prospects for implementing a practical quantum computer that could solve important problems. So, following this visit, NIST organized a mini workshop, with Ekert's help, to evaluate the field. Peter Shor was there and described his algorithm (which was completely incomprehensible to almost all of us at the time). In addition, there were a variety of experts, both theorists and experimentalists, to discuss the prospects for actually implementing a quantum computer. Mind you this was 1994, so the speakers were drawn from an elite small group of the specialists in a field that didn't even have a name yet.

Amongst the speakers at the 1994 workshop, one that sticks in my mind is Bill Unruh. Unruh had worked on the theory of decoherence and established some of the foundational results on the subject [1]. In that year he wrote a paper that addressed the issue of decoherence and quantum computation [2], following the school of thought advocated by Rolf Landauer. Landauer, the godfather of the "physics of information", was an outspoken skeptic of quantum information, famously writing an article entitled "Is Quantum Mechanics Useful?" [3]. Landauer believed that the unitarity of quantum evolution made quantum coherence unsuitable for information processing. Unruh showed that the exponential speedup afforded by Shor's algorithm would require states that were exponentially sensitive to decoherence. Thus, a scalable quantum computation couldn't be carried out, even in principle, with the approach being considered at the time. In 1994 the quantum computer was envisaged as an essentially analog device and errors would accumulate exponentially fast, another point raised by Landauer [4]. So, my recollection is that at the end of this workshop the "jury was out" as to the real usefulness of quantum computation.

Of course we know the history. Quantum computation theory evolved very quickly in the few years that followed. Part of the physics approach is to persevere even in the face of daunting challenges. As my mentor Bill Phillips recently said (paraphrasing), if we didn't pursue an experiment because we knew how hard it would be, we would never do anything. The attitude is thus; let's get started, see how far we can get, what the challenges are, and how we might overcome them. In 1995, soon after this workshop, Ignacio Cirac and Peter Zoller wrote the seminal paper on implementing quantum logic with trapped ultracold ions [5], and very soon thereafter Chris Monroe and the group of Dave Wineland carried out the first demonstration of a controlled-not [6]. A variety of physical platforms were then proposed as possible approaches to implementing quantum computation. Nonetheless, the fundamental problem of decoherence remained and Unruh's analysis had not yet been answered.

Quantum information science made a quantum leap almost immediately thereafter. In 1995 Shor rocked the world again by introducing the idea of quantum error correction [7]. The fact that decoherence could, in principle, be mitigated by proper encoding was a revolution and the biggest surprise for any physicist who ever studied open quantum systems. Still, the question of whether a scalable quantum computer could, in principle, be built was not definitively answered. In a famous 1996 opinion piece written by Serge Haroche and Jean-Michel Raimond entitled "Quantum Computing: Dream or Nightmare?" the authors questioned whether the theorist's dream of a quantum computer would be an experimentalist's nightmare [8]. Though the idea of quantum error correction had been introduced at the time their article was written, the notion of fault-tolerance had not yet reached the full community. Haroche and Raimond correctly questioned whether error correction could be carried out, even in principle, since the process doing so would have to be done perfectly (without faults).

Lighting struck for yet a third time as Shor showed that fault-tolerant quantum computation was in fact possible in a paper that first appeared on the arXiv in 1996 [9]. In principle, all imperfections in a quantum computer were correctable as long as the probability of these imperfections was sufficiently small. Of course, the practicality of implementing a quantum computation is not definitive. Reaching sufficiently below the error threshold, whatever that might be, may still be a nightmare. But to me, the very existence of a threshold for fault tolerant quantum computation is one of the most profound and important discoveries of quantum information science. It says that quantum computer is, in fact, not an analog device but a digital one. In some sense, a quantum computer is both analog and digital at the same time – a modern version of the complementarity of particles and waves. We

Continued on next page

have quantum logic gates that are always implemented with some imprecision, and decoherence always contaminates the desired states into a statistical mixture with erroneous states, but when encoded and processed correctly, these continuous sets of errors are discretized and projected onto the desired results with high probability. I think it is safe to say that no physicist pre-1996 would have thought this was possible. It took a computer scientist with fresh eyes, a different canon of knowledge, not to mention some real genius, to see a path forward. The field of quantum information science was born at the interface between computer science and quantum physics, and this interdisciplinary mode enabled new approaches to intractable problems.

Sixteen years after Shor announced his algorithm that ignited the quantum information revolution, we are at another crossroad. While experimentalists and theorists continue on the quest for a universal, fault-tolerant quantum computer, challenges continue. In the meantime, the tools for quantum control have improved and enable us to carry out a variety of groundbreaking experiments today. Can we put these tools to use to perform important tasks without a full-fledged fault tolerant quantum computer? Today many workers in the field are excited by the prospect of a "quantum simulator". By this, they mean a special-purpose quantum information processor whose physical interactions are engineered to simulate the working of another quantum system, in a manner similar to that originally envisioned by Feynman [10]. As has been noted, with just 40 spins, we are reaching a many-body system whose state cannot be simulated on current classical computers. Surely we're reaching a threshold of quantum control to enable us to simulate interesting quantum many-body physics, even if we don't have a fully functioning fault-tolerant quantum computer.

An important example that greatly spurred the thinking about quantum simulators was the idea [11] and experiment [12] to observe the Mott-insulator to superfluid transition, as predicted by the Bose-Hubbard model, using ultracold atoms in an optical lattice. In this seminal work, a quantum phase transition was observed by first loading a Bose-Einstein condensate into a lattice of a certain depth. After an equilibration time, the atoms were released, the gas expanded, and an image was taken of the final distribution. The nature of the interference of the matter waves contained signatures of the correlation function that distinguishes the Mott-insulator from the superfluid. This experiment was not only groundbreaking in cold-atom physics, but also opened a new trend in quantum information science at the nexus of AMO and condensed matter physics. Could an optical lattice be used as a quantum simulator to help crack some of the toughest problems in strongly correlated quantum systems? For example, could one simulate the 2D repulsive Fermi-Hubbard model with ultracold fermionic atoms in an optical lattice [13], and thereby address the thorny question of the pairing mechanism responsible for high-T_c superconductivity that has so long eluded us [14]?

To quote Haroche and Raimond, "at this stage (I) think that some critical reflection is required in a field boiling with excitement" [8]. A quantum simulator such as the optical lattice experiment described above is fundamentally an analog device. As such, it is generally not robust to errors, and it behooves us to address the very same questions we grappled with 16 years ago as we debated whether a quantum computer could be built to reliably perform Shor's algorithm. In the case of the Bose-Hubbard model, the quantum-many-body problem can be solved exactly with analytic methods [15]. The results of the experiment can then be checked against the theoretical predictions and they agree stunningly – a testament to our understanding of cold-atom physics and the tour de force of quantum control exhibited in the lab [12]. But ultimately we want to use our quantum simulator to give us information about a many-body system that we believe we cannot calculate (efficiently) with any classical methods, pencil and paper or (classical) supercomputer. How can we trust the results of our quantum simulator? For it is without doubt that the simulator will have imperfections. The optical lattice will have inhomogeneous depth, there will be some photon scattering, there are some background fields, and the detection system has a finite signal-to-noise ratio. Is the answer we seek robust to these errors, and how would we know?

One might ask the same question about using a fault-tolerant universal quantum computer to solve problems not in the complexity class NP. If we can't check the answer, how do we know it's right? I think this is a red herring. If we had a working fault-tolerant universal quantum computer we could use it to solve an NP problem, like factoring, for a number that can't be factored on a classical computer in any reasonable time. We could check the factors in polynomial time. If the machine got the factors right, we'd say it was a working quantum computer and we'd trust it to fault-tolerantly perform other quantum algorithms, like a quantum simulation of the 2D repulsive Fermi Hubbard model (assuming such an algorithm existed). But the optical lattice analog simulator is something different. It's not a universal machine, so we can't use it to check other computational problems. And since we can't find the solution to the actual problem we want to solve in other ways, we do not know how small variations in the parameters in the lab are expected to perturb the outcome of the experiment.

So, is an optical lattice quantum simulator something different from a working quantum computer? Does solving Shor's algorithm require fault tolerant error quantum error correction, but

Continued on next page

solving for important properties of the 2D Fermi-Hubbard model not? I have discussed this for the last year or so with many of my friends, colleagues, and students and have heard many different answers. An intuition that is often stated is that the condensed matter properties depend on local correlations, and are thus robust to the kind of imperfections I'm worried about. For Shor's algorithm, we care about the "whole wave function" and that is definitely more fragile to errors.

Let me probe this a little more deeply. To extract a result from any quantum information processor we measure some observable after the quantum state of the many-body system is appropriately prepared (initialization and control). In a typical quantum computation on a set of n qubits, we perform a projective measurement to estimate the probability distribution in the n-dimensional computational basis. For a good quantum algorithm, this probability distribution is highly peaked at one of the outcomes – the answer to the algorithm – so we only need to run the algorithm a polynomial number of times. In a quantum simulation, we are usually not interested in that level of detail about the wave function. We are typically interested in a correlation function related to some order parameter, e.g., the structure factor for spins on a lattice, $\Sigma_{ij}\langle\sigma_z^{(i)}\sigma_z^{(j)}\rangle$. Clearly such a two-body correlation function is generally less sensitive to perturbations than the probability distribution over the entire computational basis. The key word of the previous sentence is generally. Within a given phase of the system, the order parameter is a useful quantity surely because it is robust against certain perturbations. But at a quantum critical point, where fluctuations are important, we can have extreme sensitivity. And it is exactly these points that we would like to explore because they determine the nature of the phase diagram that we might want to map out. Moreover, these are the points that we cannot calculate with classical methods for problems of interest and other points are well approximated using the theoretical tools of condensed matter physics, e.g. mean field theory, quantum Monte Carlo, random phase approximation, matrix product states, density-matrix renormalization group, etc.

Now, I want to clearly distinguish different goals of experiments that might be called a quantum simulation. In one case we are trying to use the optical lattice to solve for some property of an idealized mathematical model, e.g., the phase diagram of the 2D repulsive Fermi-Hubbard model. In another case, we are trying to simulate the properties of a real material, e.g., a cuprate that exhibits high-T_c superconductivity. One might argue that the optical lattice is more like the second case in that the cuprate surely has imperfections and is not exactly described by an idealized Hubbard model. However, it is also certainly the case that the kinds of imperfections in the solid ceramic and the optical lattice are vastly different and I would conjecture these differences lead to vastly different behavior in the regimes where the phases are not robust. Moreover, I don't think we have a prayer of simulating the real complexity of a cuprate with an optical lattice, but we might have a chance of simulating idealized models in these very clean and controllable systems. For this reason, I will restrict my attention to the goal of using the quantum simulation to extract information about an idealized mathematical model, such as the 2D Fermi-Hubbard model.

The key issue is thus – under what conditions is the quantum state sufficiently robust that we can perform a useful quantum simulation without digital encoding for error correction, and when it is that robust, could we have obtained that information otherwise in an efficient calculation on a classical computer?

It seems to me only one of two answers is possible:

(1) An analog quantum simulator cannot reliably be used to extract information about a many-body Hamiltonian beyond what we could have otherwise learned with the same degree of approximation from other "classical" methods.
(2) An analog quantum simulator without error correction and fault tolerance can tell us something that we cannot calculate efficiently with classical methods.

Either alternative is an important result. If (1) is correct, we may learn about a connection between the class of problems that are classically solvable and the robustness of a many-qubit state to perturbations. Understanding the relationship between quantum correlations and computational power has been a long-standing problem in quantum information science and determining when such correlations are robust is a key issue for quantum simulators. From a practical point of view, (1) implies that to perform a computationally complex quantum simulation we must think more carefully about how to correct errors in a way that the simulation is reliable to the degree of tolerance we desire.

If (2) is correct, then we have a real revolution. It says that through appropriate engineering, we can produce highly quantum-correlated states of the sort we believe are created in nature, such as high-T_c superconductors, and these correlated states are sufficiently robust to the errors of the simulator. This is not out of the question. After all, if we believe that such highly quantum-correlated states exist in a cuprate with all its real imperfections, then perhaps they can exist at sufficiently low temperatures in an optical lattice, inhomogeneities and all. But, that result is not a given and we must more deeply probe whether this is possible at all. Of course, we could try to specially design the state to have topological order, and have the robustness built in, but I am excluding

Continued on next page

such cases from discussion here.

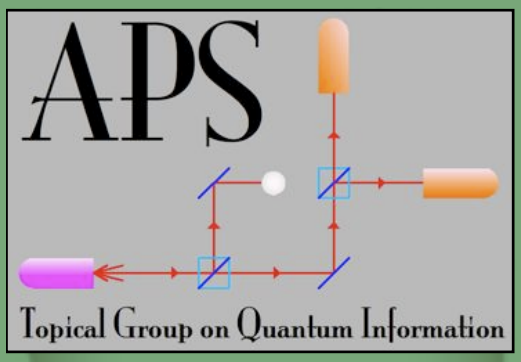
If (2) is true, which class of classically intractable problems can be solved on an analog quantum simulator, and which ones require a full-fledged fault tolerant quantum computer? Secondly, once we identify the class, can we use the analog quantum simulator to solve other computational problems beyond traditional quantum many-body problems by properly encoding the answer in a local correlation function? If an analog quantum simulator can be measured to give information that cannot be computed efficiently classically, then we should take full advantage of it.

The field of quantum simulation is ripe for another lightning strike. But to achieve that, we must take a hard look at the essential issues. For this we need to reinvigorate the interdisciplinary nature of our field, where information science and physical science meet. I fear that our field is bifurcating. Rarely are there professional meetings anymore where the different communities of quantum information science really try to communicate with one another. If the dream of quantum simulation is to be realized we need a new breakthrough in our understanding of fault tolerance, digital information, and complexity. Otherwise, all the dreams will soon be forgotten as another fad that never reached fruition.

References

1. W. G. Uhruh and W. Zurek, "Reduction of a wave packet in quantum Brownian motion." *Phys. Rev. D*, **40**, 1071 (1989).
2. W. G. Uhruh, "Maintaining coherence in quantum computers." *Phys. Rev. A*. **51**, 992 (1995).
3. R. Landauer, "Is quantum mechanics useful?" *Phil. Trans. R. Soc. Lond. A*, **353** 367 (1995).
4. R. Landauer, "The physical nature of information." *Phys. Lett. A*, **217**, 188 (1996).
5. J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions." *Phys. Rev. Lett.* **74**, 4091 (1995).
6. C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate." *Phys. Rev. Lett.* **75**, 4714 (1995).
7. P. W. Shor, "Scheme for reducing decoherence in a quantum memory." *Phys. Rev. A* **52**, R2493 (1995).
8. S. Haroche and J-M Raimond, "Quantum computing: dream or nightmare?" *Phys. Today* **49**, 51 (1996).
9. P. W. Shor, "Fault-tolerant quantum computation." arXiv:quant-ph/9605011.
10. R. P. Feynman, "Simulating physics with computers." *Int. J. Theor. Phys.* **21**, 467 (1982).
11. D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, and P. Zoller, "Cold bosonic atoms in optical lattices." *Phys. Rev. Lett.* **81**, 3108 (1998).
12. M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Bloch, "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms." *Nature* **415**, 39 (2002).
13. W. Hofstetter, J.I. Cirac, P. Zoller, E. Demler, and M.D. Lukin, "High-temperature superfluidity of fermionic atoms in optical lattices," *Phys. Rev. Lett.* **89**, 220407 (2002).
14. P. W. Anderson, *The Theory of Superconductivity in the High-T_c Cuprate Superconductors*, Princeton University Press (1997).
15. M. P. A. Fisher, P. B. Weichman, G. Grinstein, and D. S. Fisher, "Boson localization and the superfluid-insulator transition", *Phys. Rev. B* **40**, 546 (1989).

Ivan Deutsch *is Professor and Associate Chair for Graduate Affairs at the Center for Quantum Information and Control (CQuIC) in the Department of Physics and Astronomy at the University of New Mexico. He is also the Secretary-Treasurer for GQI.*



Three two-year postdoctoral research associate positions are available immediately in the group of Barry Sanders, who is the iCORE Chair of Quantum Information Science and Director of the University of Calgary's Institute for Quantum Information Science (IQIS). Research foci are machine learning for quantum measurement, multi-partite quantum communication protocols, quantum simulation, electron transport in protein complexes, and theoretical support for the the experimental research groups of Paul Barclay, Alex Lvovsky, and Wolfgang Tittel in IQIS. Two-year positions may be renewed for a third year depending on performance and continued funding.

The successful candidates must possess a PhD or equivalent in theoretical physics, an excellent research track record, strong written and oral communication skills, and extensive computer programming experience. Candidates should submit their curriculum vitae, a two-page statement of research plans addressing one or more of the above research foci, names and contact details for four referees, and a copy of the best publication authored or co-authored by the candidate so far. All application material must be emailed to IQIS Administrator Ms Nancy Jing Lu at info@qis.ucalgary.ca

All qualified candidates are encouraged to apply; however, Canadians and permanent residents will be given priority. The University of Calgary respects, appreciates and encourages diversity.

ACS DIVISION OF
PHYSICAL CHEMISTRY
241st NATIONAL MEETING
Anaheim, CA
March 27-31, 2011

Call for Papers

The abstract deadline is **October 18, 2010**. For those interested in an oral presentation, please submit abstracts to the e-mail addresses listed below. The organizers (listed below) will select some contributed papers for oral presentation; contributions not selected for oral presentation will be assigned to the poster session.

QUANTUM INFORMATION AND COMPUTATION IN CHEMISTRY: EXPERIMENT AND THEORY

This symposium will explore the exciting interface of quantum information and computation and both theory and experiment in physical chemistry. Some of the topics at the trading zone between quantum information and chemistry that will be emphasized during the symposium are: the prospects of quantum computation for the calculation of molecular properties and for the simulation of chemical reaction dynamics; the realization and characterization of non-trivial entanglement and coherence properties of chemical systems; the use of new tools from quantum information such as tensor networks for the simulation of atoms and molecules using classical computers; the use of molecules as quantum information processors; and finally the use of quantum information concepts such as entanglement for the understanding of chemical concepts such as the chemical bond or non-covalent interactions.

***Alán Aspuru-Guzik**, Harvard University, aspuru@chemistry.harvard.edu*
***Ken Brown**, Georgia Institute of Technology, ken.brown@chemistry.gatech.edu*