1. Specific events and activities which took place during your CRG in 2011:

   The CRG planned a workshop at the University of Washington in Spring/Summer 2011, which was to be led by David Bacon. As David suddenly resigned his academic position in spring to assume an industrial position, the workshop was cancelled. Without sufficient warning, a substitute workshop was not possible. PIMS was informed of this unfortunate cancellation.

2. List of CRG participants in 2011:

   a. PIMS Faculty - Leaders
      - **i.** Barry Sanders – University of Calgary
      - **ii.** Robert Raußendorf – University of British Columbia
      - **iii.** Petr Lisonek – Simon Fraser University
      - **iv.** Aram Harrow – University of Washington

   b. Other faculty
      - **i.** Philip Stamp – University of British Columbia
      - **ii.** William Unruh – University of British Columbia
      - **iii.** David Feder – University of Calgary
      - **iv.** Gilad Gour – University of Calgary
      - **v.** Peter Høyer – University of Calgary
      - **vi.** Alex Lvovsky – University of Calgary
      - **vii.** Christoph Simon – University of Calgary
      - **viii.** Wolfgang Tittel – University of Calgary
      - **ix.** Leslie Ballentine – Simon Fraser University
      - **x.** Paul Haljan – Simon Fraser University
      - **xi.** Boris Blinov – University of Washington
      - **xii.** Subhadeep Gupta – University of Washington
      - **xiii.** Mark Oskin – University of Washington

   c. Visitors

      David Kribs (University of Guelph) visited University of Calgary (29 November – 3 December 2010).

      Netanel Lindner (California Institute of Technology) visited University of British Columbia (6 – 13 March 2011) and University of Calgary (14 – 17 March 2011).

      Patrick Hayden (McGill University) visited between University of British Columbia (9 – 12 March 2011) and University of Washington (13 – 20 March 2011).

Fernando G.S.L. Brandão (Universidade Federal de Minas Gerais, Belo Horizonte, Brazil) visited University of Washington (10 – 16 July 2011) and University of Calgary (17 – 23 July 2011).

Shmuel Friedland (University of Illinois at Chicago) visited University of Calgary (7 – 12 November 2011).

d. PDF's and graduate students who were part of your CRG. Where are they now?

i. Past Graduate Students:

1. Alexander Hentschel. Supervisor: Barry Sanders (University of Calgary). Graduated 2011. Currently: Research Scientist, Corporate Technology Division, Siemens, Munich.
2. Saleh Rahimi-Keshari. Supervisor: Barry Sanders (University of Calgary). Graduated 2010. Currently visitor at the University of Rostock and commences PhD study at the University of Queensland January 2012.

ii. Past PDFs:

1. Ben Fortescue. Supervisor: Barry Sanders (University of Calgary). Now postdoctoral fellow with Mark Byrd (Southern Illinois University).

3. Brief summaries of research projects fostered by your CRG.

a. *Quantum secret sharing.* The Raußendorf, Sanders and Gour groups investigate quantum secret sharing. The CRG supported this common research effort by supporting Ben Fortescue's visit to UBC. The three groups continue research in this area.

b. *Measurement-based quantum computation.* The Raußendorf group demonstrated that the two-dimensional Affleck-Kennedy-Lieb-Tasaki state on a honeycomb lattice is a universal resource for measurement-based quantum computation. Due to the percolation aspect of the problem, a mathematician with expertise in percolation theory would be a great asset on the project.

c. *Quantum codes.* The Sanders group undertakes research on feedback iterative decoding of sparse quantum codes, and postdoc Yunjiang Wang will soon visit the Raußendorf and Lisonek groups to share results and seek collaboration. The Raußendorf group completed its research project on efficient decoders for topological quantum codes The Harrow group has developed a general method for turning any stabilizer code into a subsystem stabilizer code that has spatially local syndrome measurements, which related to measurement-based quantum computing schemes so collaboration on these codes with the Raußendorf group is being pursued. The Lisonek group employed a geometric approach to construct quantum stabilizer states that violate the LU-LC Conjecture, which was listed as one of the main 29 open problems in quantum information theory in 2005. The Lisonek employs a synthetic, computer-free construction is being used to attack the conjecture for higher

dimensions where the problem remains open, and the Raußendorf group provides feedback on this work.

d. *New project: Dynamics of single and coupled qubit pair systems coupled to a spin bath*. PIMS CRG MQI Postdoc Martitza Hernandez is working under Philip Stamp's direction on this project and expects results in 2012.

4. Main scientific accomplishments derived from your CRG: any noteworthy theorems or breakthroughs? Lists of 2011 publications.

   a. Y. J. Wang, B. C. Sanders, B.-M. Bai and X.-M. Wang, Enhanced feedback iterative decoding of sparse quantum codes, *IEEE Transactions on Information Theory*, 23 August 2011, arXiv.org:0912.4546. (accepted or in press).

      Abstract: Decoding sparse quantum codes can be accomplished by syndrome-based decoding using a belief propagation (BP) algorithm. We significantly improve this decoding scheme by developing a new feedback adjustment strategy for the standard BP algorithm. In our feedback procedure, we exploit much of the information from stabilizers, not just the syndrome but also the values of the frustrated checks on individual qubits of the code and the channel model. Furthermore we show that our decoding algorithm is superior to belief propagation algorithms using only the syndrome in the feedback procedure for all cases of the depolarizing channel. Our algorithm does not increase the measurement overhead compared to the previous method, as the extra information comes for free from the requisite stabilizer measurements.

   b. B. Fortescue and G. Gour, Reducing the quantum communication cost of quantum secret sharing, arXiv.org:1108.5541, 29 August 2011.

      Abstract: We demonstrate a construction for perfect quantum secret sharing (QSS) schemes based on imperfect "ramp" secret sharing combined with classical encryption, in which the individual parties' shares are split into quantum and classical components, allowing the former to be of lower dimension than the secret itself. We show that such schemes can be performed with smaller quantum components and lower overall quantum communication than required for existing methods. Finally, we demonstrate that one may further combine both imperfect quantum and imperfect classical secret sharing to produce an overall perfect QSS scheme; we construct examples of such schemes and prove that they have the smallest quantum and classical share components possible for their access structures.

   c. P. Sarvepalli, Efficient Decoding of Topological Color Codes, arXiv:1111.0831v1 3 November 2011.

      Abstract: Color codes are a class of topological quantum codes with a high error threshold and large set of transversal encoded gates, and are thus suitable for fault tolerant quantum computation in two-dimensional architectures. Recently, computationally efficient decoders for the color codes were proposed. We describe an

alternate efficient iterative decoder for topological color codes, and apply it to the color code on hexagonal lattice embedded on a torus. In numerical simulations, we find an error threshold of 7.8% for independent dephasing and spin flip errors.

d. J. Chen, T. S. Cubitt, A. W. Harrow and G. Smith, Entanglement can completely defeat quantum noise, arXiv:1109.0540, (to appear in *Phys. Rev. Lett.*), 2 September 2011.

We describe two quantum channels that individually cannot send any information, even classical, without some chance of decoding error. But together a single use of each channel can send quantum information perfectly reliably. This proves that the zero-error classical capacity exhibits superactivation, the extreme form of the superadditivity phenomenon in which entangled inputs allow communication over zero capacity channels. But our result is stronger still, as it even allows zero-error quantum communication when the two channels are combined. Thus our result shows a new remarkable way in which entanglement across two systems can be used to resist noise, in this case perfectly. We also show a new form of superactivation by entanglement shared between sender and receiver.

e. A.W. Harrow, A. Montanaro, A. J. Short, Limitations on quantum dimensionality reduction, arXiv:1012.2262. *Proc. of ICALP 2011* **6755/2011**, pp. 86-97, 26 June 2011.

The Johnson-Lindenstrauss Lemma is a classic result which implies that any set of n real vectors can be compressed to O(log n) dimensions while only distorting pairwise Euclidean distances by a constant factor. Here we consider potential extensions of this result to the compression of quantum states. We show that, by contrast with the classical case, there does not exist any distribution over quantum channels that significantly reduces the dimension of quantum states while preserving the 2-norm distance with high probability. We discuss two tasks for which the 2-norm distance is indeed the correct figure of merit. In the case of the trace norm, we show that the dimension of low-rank mixed states can be reduced by up to a square root, but that essentially no dimensionality reduction is possible for highly mixed states.

f. S. Bravyi, A. W. Harrow, and A. Hassidim, Quantum algorithms for testing properties of distributions, arXiv:0907.3920. *IEEE Transactions on Information Theory*, **57**(6), pp. 3971--3981 (June 2011).

Suppose one has access to oracles generating samples from two unknown probability distributions P and Q on some N-element set. How many samples does one need to test whether the two distributions are close or far from each other in the L_1-norm ? This and related questions have been extensively studied during the last years in the field of property testing. In the present paper we study quantum algorithms for testing properties of distributions. It is shown that the L_1-distance between P and Q can be estimated with a constant precision using approximately N^{1/2} queries in the

quantum settings, whereas classical computers need \Omega(N) queries. We also describe quantum algorithms for testing Uniformity and Orthogonality with query complexity O(N^{1/3}). The classical query complexity of these problems is known to be \Omega(N^{1/2}).

g. W. Harrow and D. W. Leung, A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities, arXiv:0803.3066. *IEEE Transactions on Information Theory* **57**(8), pp. 5504 - 5508 (Aug 2011).

Two dual questions in quantum information theory are to determine the communication cost of simulating a bipartite unitary gate, and to determine their communication capacities. We present a bipartite unitary gate with two surprising properties: 1) simulating it with the assistance of unlimited EPR pairs requires far more communication than with a better choice of entangled state, and 2) its communication capacity is far lower than its capacity to create entanglement. This suggests that 1) unlimited EPR pairs are not the most general model of entanglement assistance for two-party communication tasks, and 2) the entangling and communicating abilities of a unitary interaction can vary nearly independently. The technical contribution behind these results is a communication-efficient protocol for measuring whether an unknown shared state lies in a specified rank-one subspace or its orthogonal complement.

5. Examples of networking which can be directly attributed to your CRG. Exchanges that took place between the institutes are listed below. This list also relates to the "Seminar/Lecture Series Award Conditions".

a. List of talks given at the:

University of Calgary

9 November 2011 Shmuel Friedland [University of Chicago] The global and local additivity problems in quantum information theory

The capacity of the classical channel was investigated by Claude Shannon in 1948. This capacity is additive under the tensor products of two channels. The capacity of a quantum channel (QC) was introduced by Alexander Holevo in 1998. One of the fundamental problems in quantum information theory is whether the capacity of QC is additive or not under the tensor product. Equivalently, can entangled input increase the quantum capacity? In 2009 Matthew Hastings gave a positive answer to this problem! It was shown by Peter Shor in 2004 that the additivity of the Holevo capacity is equivalent to: - additivity of the minimum entropy output of a quantum channel, - additivity of the entanglement of formation, - strong superadditivity of the entanglement of formation. Contrary to the above result we will show that the local minimum entropy output of a quantum channel is additive. This result is a joint work with Gilad Gour.

17 August 2011 Aram Harrow [University of Washington] The princess and the EPR pair

In quantum information, entanglement has often been viewed as a resource. But in this talk, I will look at (pure bipartite) entanglement through the lens of superselection rules. The idea is that it requires quantum communication not only to create entanglement, but also to destroy it in a way that doesn't leak information to the environment. As a result, when communication is scarce, superpositions of different numbers of EPR pairs can be difficult to obtain. This constraint is not a strict superselection rule, but rather an approximate version that gives rigorous bounds on achievable fidelities. After describing the general phenomenon, I will show how it relates to communication complexity, information theory and fairy tales about princesses. This talk is based on 0803.3066, 0909.1557, 0912.5537 and other unpublished work.

20 July 2011 Fernando Brandão [Universidade Federal de Minas Gerais, Belo Horizonte, Brazil] Is it entangled? A quasi-polynomial time algorithm for the quantum separability problem.

Quantum mechanics predicts the existence of correlations between two quantum systems which cannot be described merely by shared randomness. Such correlations, termed entanglement, have been analysed from a fundamental perspective since the beginning of quantum theory and, more recently, as a resource for quantum information-theoretic tasks, such as quantum key distribution and teleportation. A fundamental problem in entanglement theory is the following: given the description of a quantum system of two parties as a density matrix, how can we decide if the state is entangled or separable? In this talk I will discuss the fastest known algorithm for solving this problem. The algorithm works by considering a sequence of SDP (semidefinite programming) relaxations to the problem, which are shown to converge quickly to the true solution. Finally I will discuss a few other applications of the techniques developed to quantum information theory and quantum complexity theory. The talk is based on joint work with Matthias Christandl and Jon Yard (STOC 2011 and Commun. Math. Phys. '11)

16 March 2011 Netanel Lindner [California Institute of Technology] Putting Floquet theory to work: Topology of time dependent Hamiltonians

Topological phases of matter have captured our imagination over the past few years, with tantalizing properties such as robust edge modes and exotic non-Abelian excitations, and potential applications ranging from semiconductor spintronics to topological quantum computation. Despite recent advancements in the field, our ability to control topological transitions remains limited, and usually requires changing material or structure properties. We show that a topological state can be induced in a semiconductor quantum well, initially in the trivial phase, by irradiation with microwave frequencies, without changing the well structure, closing the gap and crossing the phase transition. We show that the quasi-energy spectrum exhibits a single pair of helical edge states. We discuss the necessary experimental parameters for our proposal. This proposal provides an example

and a proof of principle of a new non-equilibrium topological state: a ``Floquet topological insulator".

University of British Columbia:

11 March 2011 Patrick Hayden [McGill] Uncertainty, encryption and low-distortion embeddings

Abstract: Where should one look to find bases satisfying strong uncertainty relations? Position and momentum lead the way: it's hard to do better than any orthonormal basis and its Fourier transform. The natural generalization to so-called mutually unbiased bases, however, leaves a bit to be desired when it comes to uncertainty relations. Reframing the search in terms of low-distortion embeddings instead leads to bases satisfying much stronger uncertainty relations than had previously been known, plus a wealth of applications. I'll explain, for example, how to encrypt an n-bit message using a constant-sized secret key and how to perform equality testing of quantum states using a a constant amount of quantum communication. Based on joint work with Omar Fawzi and Pranab Sen. arXiv:1010.3007.

9 March 2011 Netanel Lindner [California Institute of Technology] Putting Floquet theory to work: Topology of time dependent Hamiltonians

Abstract: Topological phases of matter have captured our imagination over the past few years, with tantalizing properties such as robust edge modes and exotic non-Abelian excitations, and potential applications ranging from semiconductor spintronics to topological quantum computation. Despite recent advancements in the field, our ability to control topological transitions remains limited, and usually requires changing material or structure properties. We show that a topological state can be induced in a semiconductor quantum well, initially in the trivial phase, by irradiation with microwave frequencies, without changing the well structure, closing the gap and crossing the phase transition. We show that the quasi-energy spectrum exhibits a single pair of helical edge states. We discuss the necessary experimental parameters for our proposal. This proposal provides an example and a proof of principle of a new non-equilibrium topological state: a “Floquet topological insulator”.

University of Washington

14 March 2011 Patrick Hayden [McGill University] Uncertainty, encryption and low-distortion embeddings

Abstract: Where should one look to find bases satisfying strong uncertainty relations? Position and momentum lead the way: it's hard to do better than any orthonormal basis and its Fourier transform. The natural generalization to so-called mutually unbiased bases, however, leaves a bit to be desired when it comes to uncertainty relations. Reframing the search in terms of low-distortion embeddings instead leads to bases satisfying much stronger uncertainty relations than had previously been known, plus a

wealth of applications. I'll explain, for example, how to encrypt an n-bit message using a constant-sized secret key and how to perform equality testing of quantum states using a a constant amount of quantum communication. Based on joint work with Omar Fawzi and Pranab Sen. arXiv:1010.3007.

b. Collaboration projects started

From Fernando Brandao's visit to UW, we started a new collaboration on the problem of analyzing the higher moments of the unitary matrices obtained from random quantum circuits. We found that such circuits on n qubits with poly(n) length are k-designs for k=poly(n). Previously the best known such result held for k=3. This is joint work with Michal Horodecki (at the Univ. of Gdansk), and has already been accepted to QIP2012 as a Featured Talk. We plan to soon post our manuscript to arxiv.org and submit it to Communications in Mathematical Physics.

6. Did you obtain other sources of funding for events connected to your CRG? If so, please list them.

   As the 2011 workshop was cancelled, extra funding was neither sought nor received.

7. Did your CRG help attract new faculty to Western Canada in 2010? Can you give some examples?

   a. UW hired new faculty members in experimental quantum information at the University of Washington (Kai-Mei Fu) and at the University of Calgary (Paul Barclay).
   b. CRG has enabled interactions and collaborations between member institutions and enriched the research programs by bringing top visitors.

8. Projections for 2012:

   a. Originally the final CRG workshop and summer was to be held in Calgary in 2012, but, in order to fit into the national agenda for quantum information summer schools and student conferences, the PIMS CRG MQI summer school and workshop will be held in Calgary in 2013. As originally foreshadowed in the PIMS CRG proposal, the workshop and summer school and student conference will be funded externally (not by PIMS) so a carryover of funding is NOT required.
   b. The successful seminar series, which invites visitors to at least two of the four PIMS CRG MQI institutions, will continue in 2012. Gilad Gour is in the process of lining up future visitors.
   c. Four postdoctoral researchers are supported by the PIMS CRG program. Raußendorf is working on recruiting a fifth postdoc.
   d. The student travel support from the PIMS CRG MQI has enabled students to attend conferences to present theoretical work. This travel-support program will continue.
   e. Inter-node collaboration has been limited so far: principal investigators came to Calgary for the opening and one Calgary postdoc has visited UBC. This exchange

program will be fully operational in 2012. Already the following visits have been arranged: Ran Hee Choi (U Calgary MSc student in the Sanders group) and Vlad Gheorghiu (U Calgary Postdoc in the Gour group) will visit the Raußendorf and Lisonek groups for one week in February, and Mohammad Amin (D-Wave Systems in Vancouver) will visit Calgary in January. Yunjiang Wang (U Calgary postdoc in the Sanders group) is planning visits to the Raußendorf and Lisonek groups in the New Year; destinations are in the works.