QIP 2009, Jan. 12-16 2009, Santa Fe NM

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

January 22, 2008

1. General information

2. Summary of talks I've found most interesting
   - Matt Hastings - A counterexample to additivity
   - Graeme Smith - Quantum communication with zero-capacity channels
   - Steve Fammia et al - Most quantum states are useless for measurement-based quantum computation
   - Gilles Brassard et al - Key distribution and oblivious transfer a la Merkle
   - Bryan Eastin and Emanuel Knill - Restrictions on transversal encoded quantum gate sets
   - Michael Nielsen - Informal talk on the future of science and scientific collaboration

General information

- Location: Santa Fe, New Mexico

General information

- Location: Santa Fe, New Mexico
- Little bit more precise: $35^\circ 41' 23.60'' N$, $105^\circ 56' 23.12'' W$

General information

- Location: Santa Fe, New Mexico
- Little bit more precise: $35^\circ 41' 23.60'' N$, $105^\circ 56' 23.12'' W$
- Primary focus: quantum information theory

General information

- Location: Santa Fe, New Mexico
- Little bit more precise: $35^\circ 41' 23.60'' N$, $105^\circ 56' 23.12'' W$
- Primary focus: quantum information theory
- 7 Invited talks, 32 contributed talks and 80 posters

General information

- Location: Santa Fe, New Mexico
- Little bit more precise: $35^\circ 41' 23.60'' N$, $105^\circ 56' 23.12'' W$
- Primary focus: quantum information theory
- 7 Invited talks, 32 contributed talks and 80 posters
- Some participants/speakers: Michael Nielsen (Perimeter), Peter Shor (MIT), John Preskill (Caltech), Richard Jozsa (Bristol), Daniel Gottesman (Perimeter), Charles Bennett (IBM), Patrick Hayden (McGill), Debbie Leung (Waterloo), Matt Hastings (LANL), Graeme Smith (IBM), John Smolin (IBM) et al

- Reasonable-sized conference

- Reasonable-sized conference
- Nice location

- Reasonable-sized conference
- Nice location
- No parallel sessions

- Reasonable-sized conference
- Nice location
- No parallel sessions
- All talks were video-recorded and will soon be available at the conference website: http://info.phys.unm.edu/qip2009

- Reasonable-sized conference
- Nice location
- No parallel sessions
- All talks were video-recorded and will soon be available at the conference website: http://info.phys.unm.edu/qip2009
- Some comments about the talks can be found at http://scienceblogs.com/pontiff

- Reasonable-sized conference
- Nice location
- No parallel sessions
- All talks were video-recorded and will soon be available at the conference website: http://info.phys.unm.edu/qip2009
- Some comments about the talks can be found at http://scienceblogs.com/pontiff
- Our work: Poster - "Location of quantum information in additive quantum codes"

Matt Hastings - A counterexample to additivity

- Reference: arXiv:0809.3972 [quant-ph]

Matt Hastings - A counterexample to additivity

- Reference: arXiv:0809.3972 [quant-ph]
- We present a random construction of a pair of channels which gives, with non-zero probability for sufficiently large dimensions, a counterexample to the minimum output entropy conjecture. As shown by Shor, this implies a violation of the additivity conjecture for the classical capacity of quantum channels. The violation of the minimum output entropy conjecture is relatively small.

Matt Hastings - A counterexample to additivity

- Reference: arXiv:0809.3972 [quant-ph]
- We present a random construction of a pair of channels which gives, with non-zero probability for sufficiently large dimensions, a counterexample to the minimum output entropy conjecture. As shown by Shor, this implies a violation of the additivity conjecture for the classical capacity of quantum channels. The violation of the minimum output entropy conjecture is relatively small.

The classical (or Holevo) capacity of a quantum channel

$$\mathcal{C}(\mathcal{E}) = \min_{\{p_i,\rho_i\}} \left\{ H\left(\sum_i p_i \mathcal{E}(\rho_i)\right) - \sum_i p_i H\left(\mathcal{E}(\rho_i)\right) \right\}$$

Matt Hastings - A counterexample to additivity

- Reference: arXiv:0809.3972 [quant-ph]
- We present a random construction of a pair of channels which gives, with non-zero probability for sufficiently large dimensions, a counterexample to the minimum output entropy conjecture. As shown by Shor, this implies a violation of the additivity conjecture for the classical capacity of quantum channels. The violation of the minimum output entropy conjecture is relatively small.

The classical (or Holevo) capacity of a quantum channel

$$\mathcal{C}(\mathcal{E}) = \min_{\{p_i,\rho_i\}} \left\{ H\left(\sum_i p_i \mathcal{E}(\rho_i)\right) - \sum_i p_i H\left(\mathcal{E}(\rho_i)\right) \right\}$$

The additivity conjecture for the classical capacity

$$\mathcal{C}(\mathcal{E}_1 \otimes \mathcal{E}_2) = \mathcal{C}(\mathcal{E}_1) + \mathcal{C}(\mathcal{E}_2)$$

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

The minimum output entropy

$$H^{min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

The minimum output entropy

$$H^{min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

The minimum output entropy conjecture

$$H^{min}(\mathcal{E}_1 \otimes \mathcal{E}_2) = H^{\min}(\mathcal{E}_1) + H^{\min}(\mathcal{E}_2)$$

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

The minimum output entropy

$$H^{min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

The minimum output entropy conjecture

$$H^{min}(\mathcal{E}_1 \otimes \mathcal{E}_2) = H^{\min}(\mathcal{E}_1) + H^{\min}(\mathcal{E}_2)$$

- Used random construction that leads to a counterexample to the minimum output entropy conjecture.

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

The minimum output entropy

$$H^{min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

The minimum output entropy conjecture

$$H^{min}(\mathcal{E}_1 \otimes \mathcal{E}_2) = H^{\min}(\mathcal{E}_1) + H^{\min}(\mathcal{E}_2)$$

- Used random construction that leads to a counterexample to the minimum output entropy conjecture.
- The violation is relatively small, but is present!

- Shor showed that the additivity conjecture for the classical capacity is equivalent to the *minimum output entropy conjecture*.

The minimum output entropy

$$H^{min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

The minimum output entropy conjecture

$$H^{min}(\mathcal{E}_1 \otimes \mathcal{E}_2) = H^{\min}(\mathcal{E}_1) + H^{\min}(\mathcal{E}_2)$$

- Used random construction that leads to a counterexample to the minimum output entropy conjecture.
- The violation is relatively small, but is present!
- For more details see the preprint.

Graeme Smith - Quantum communication with zero-capacity channels

- Reference: arXiv:0807.4935 [quant-ph]

Graeme Smith - Quantum communication with zero-capacity channels

- Reference: arXiv:0807.4935 [quant-ph]
- The capacity of a noisy quantum channel for quantum communication is the fundamental limit for quantum error correction. Here we show that two quantum channels, each of whose capacity is zero, can have a nonzero capacity when used together. This uniquely quantum mechanical effect unveils a rich structure in the theory of quantum communications and points to the existence of incomparable types of quantum information, implying that the quantum capacity of a channel does not uniquely specify its ability for transmitting quantum information.

- The quantum capacity $\mathcal{Q}(\mathcal{E})$ of a quantum channel $\mathcal{E}$ is the number of qubits per channel use that can be reliably transmitted via many noisy transmissions, where each transmission is modeled by $\mathcal{E}$.

- The quantum capacity $\mathcal{Q}(\mathcal{E})$ of a quantum channel $\mathcal{E}$ is the number of qubits per channel use that can be reliably transmitted via many noisy transmissions, where each transmission is modeled by $\mathcal{E}$.

Coherent information

$$\mathcal{Q}^{(1)}(\mathcal{E}) = \max_{\rho_{input}} (H(\rho_{output}) - H(\rho_{environment}))$$

- The quantum capacity $\mathcal{Q}(\mathcal{E})$ of a quantum channel $\mathcal{E}$ is the number of qubits per channel use that can be reliably transmitted via many noisy transmissions, where each transmission is modeled by $\mathcal{E}$.

Coherent information

$$\mathcal{Q}^{(1)}(\mathcal{E}) = \max_{\rho_{input}} (H(\rho_{output}) - H(\rho_{environment}))$$

- The best known formulat for quantum capacity is the *regularization* of the coherent information.

- The quantum capacity $\mathcal{Q}(\mathcal{E})$ of a quantum channel $\mathcal{E}$ is the number of qubits per channel use that can be reliably transmitted via many noisy transmissions, where each transmission is modeled by $\mathcal{E}$.

Coherent information

$$\mathcal{Q}^{(1)}(\mathcal{E}) = \max_{\rho_{input}} (H(\rho_{output}) - H(\rho_{environment}))$$

- The best known formulat for quantum capacity is the *regularization* of the coherent information.

The quantum capacity

$$\mathcal{Q}(\mathcal{E}) = \lim_{n \to \infty} \frac{1}{n} \mathcal{Q}^1(\mathcal{E}^{\otimes n})$$

- Only two known classes of zero-capacity quantum channels are known.

- Only two known classes of zero-capacity quantum channels are known.
  - Symmetric channels - the joint quantum state of the output and environment is symmetric under interchange. Are quite different from Shannon's zero-capacity channels, as they display correlations between the input and output. However, they are useless by themselves for quantum communication because their symmetry implies that any capacity would lead to a violationof the no cloning theorem.

- Only two known classes of zero-capacity quantum channels are known.
  - Symmetric channels - the joint quantum state of the output and environment is symmetric under interchange. Are quite different from Shannon's zero-capacity channels, as they display correlations between the input and output. However, they are useless by themselves for quantum communication because their symmetry implies that any capacity would lead to a violationof the no cloning theorem.
  - Horodecki channels - can only produce very weakly entangled states satisfying a condition called positive partial transposition.

- Only two known classes of zero-capacity quantum channels are known.
  - Symmetric channels - the joint quantum state of the output and environment is symmetric under interchange. Are quite different from Shannon's zero-capacity channels, as they display correlations between the input and output. However, they are useless by themselves for quantum communication because their symmetry implies that any capacity would lead to a violationof the no cloning theorem.
  - Horodecki channels - can only produce very weakly entangled states satisfying a condition called positive partial transposition.
- Combining any two channels from the same class does not increase capacity.

- Only two known classes of zero-capacity quantum channels are known.
  - Symmetric channels - the joint quantum state of the output and environment is symmetric under interchange. Are quite different from Shannon's zero-capacity channels, as they display correlations between the input and output. However, they are useless by themselves for quantum communication because their symmetry implies that any capacity would lead to a violationof the no cloning theorem.
  - Horodecki channels - can only produce very weakly entangled states satisfying a condition called positive partial transposition.
- Combining any two channels from the same class does not increase capacity.
- Combine a symmetric channel with a Horodecki channel and get non-zero quantum capacity!

Steve Fammia et al - Most quantum states are useless for measurement-based quantum computation

- Reference: arXiv:0810.4331, 0812.3001 [quant-ph]

Steve Fammia et al - Most quantum states are useless for measurement-based quantum computation

- Reference: arXiv:0810.4331, 0812.3001 [quant-ph]
- It is often argued that entanglement is at the root of the speedup for quantum compared to classical computation, and that one needs a sufficient amount of entanglement for this speedup to be manifest. In measurement-based quantum computing (MBQC), the need for a highly entangled initial state is particularly obvious. Defying this intuition, we show that quantum states can be too entangled to be useful for the purpose of computation. We prove that this phenomenon occurs for a dramatic majority of all states: the fraction of useful n-qubit pure states is less than $\exp(-n^2)$. Computational universality is hence a rare property in quantum states.

- First, they show that families of states with a large amount of entanglement as quantified by the geometric measure of entanglement cannot be universal.

- First, they show that families of states with a large amount of entanglement as quantified by the geometric measure of entanglement cannot be universal.

The geometric measure of entanglement

$$E_g(|\psi\rangle) = -\log_2 \sup_{|\alpha\rangle \in \mathcal{P}} |\langle \alpha | \psi \rangle|^2$$

where $\mathcal{P}$ is the set of all product states.

- First, they show that families of states with a large amount of entanglement as quantified by the geometric measure of entanglement cannot be universal.

The geometric measure of entanglement

$$E_g(|\psi\rangle) = -\log_2 \sup_{|\alpha\rangle \in \mathcal{P}} |\langle \alpha | \psi \rangle|^2$$

where $\mathcal{P}$ is the set of all product states.

- Second, they proceed to demonstrate that their criterion for large entanglement is fulfilled by typical quantum states with overwhelming probability: they are too entangled to be useful in this sense.

- First, they show that families of states with a large amount of entanglement as quantified by the geometric measure of entanglement cannot be universal.

The geometric measure of entanglement

$$E_g(|\psi\rangle) = -\log_2 \sup_{|\alpha\rangle \in \mathcal{P}} |\langle \alpha | \psi \rangle|^2$$

where $\mathcal{P}$ is the set of all product states.

- Second, they proceed to demonstrate that their criterion for large entanglement is fulfilled by typical quantum states with overwhelming probability: they are too entangled to be useful in this sense.
- The proof involves substituting the quantum resource by a fair coin. In that sense, we show that even if one has complete knowledge about the state used and is capable of designing the most sophisticated measurement scheme, the distribution of themeasurement outcomes is not sufficiently different from that of a random string to afford a universal speedup.

Gilles Brassard et al - Key distribution and oblivious transfer a la Ralph Merkle

- Historic reference: http://merkle.com/1974

Gilles Brassard et al - Key distribution and oblivious transfer a la Ralph Merkle

- Historic reference: http://merkle.com/1974
- In the Fall of 1974 I enrolled in CS244, the Computer Security course offered at UC Berkeley and taught by Lance Hoffman. We were required to submit two project proposals, one of which we would complete for the course. I submitted a proposal for what is now known as Public Key Cryptography – which Hoffman rejected. I dropped the course, but kept working on the idea.
- Seminal ideas for public key distribution.

Gilles Brassard et al - Key distribution and oblivious transfer a la Ralph Merkle

- Historic reference: http://merkle.com/1974
- In the Fall of 1974 I enrolled in CS244, the Computer Security course offered at UC Berkeley and taught by Lance Hoffman. We were required to submit two project proposals, one of which we would complete for the course. I submitted a proposal for what is now known as Public Key Cryptography – which Hoffman rejected. I dropped the course, but kept working on the idea.
- Seminal ideas for public key distribution.
- The breaking time is only polynomial in the length key.

Gilles Brassard et al - Key distribution and oblivious transfer a la Ralph Merkle

- Historic reference: http://merkle.com/1974
- In the Fall of 1974 I enrolled in CS244, the Computer Security course offered at UC Berkeley and taught by Lance Hoffman. We were required to submit two project proposals, one of which we would complete for the course. I submitted a proposal for what is now known as Public Key Cryptography – which Hoffman rejected. I dropped the course, but kept working on the idea.
- Seminal ideas for public key distribution.
- The breaking time is only polynomial in the length key.

Open problem

No known classical public key-distribution algorithm that can not be broken with a quantum computer.

Bryan Eastin and Emanuel Knill - Restrictions on transversal encoded quantum gate sets

- Reference: arXiv:0811.4262 [quant-ph]

Bryan Eastin and Emanuel Knill - Restrictions on transversal encoded quantum gate sets

- Reference: arXiv:0811.4262 [quant-ph]
- Transversal gates play an important role in the theory of fault-tolerant quantum computation due to their simplicity and robustness to noise. By definition, transversal operators do not couple physical subsystems within the same code block. Consequently, such operators do not spread errors within code blocks and are, therefore, fault tolerant. Nonetheless, other methods of ensuring fault tolerance are required, as it is invariably the case that some encoded gates cannot be implemented transversally. This observation has led to a long-standing conjecture that transversal encoded gate sets cannot be universal. Here we show that the ability of a quantum code to detect an arbitrary error on any single physical subsystem is incompatible with the existence of a universal, transversal encoded gate set for the code.

Michael Nielsen - Informal talk on the future of science and scientific collaboration

- More Michael's comments and ideas at http://www.qinfo.org/people/nielsen/blog

Michael Nielsen - Informal talk on the future of science and scientific collaboration

- More Michael's comments and ideas at http://www.qinfo.org/people/nielsen/blog
- Now information is active.

Michael Nielsen - Informal talk on the future of science and scientific collaboration

- More Michael's comments and ideas at http://www.qinfo.org/people/nielsen/blog
- Now information is active.
- Sharing = faster progress.