BIRS Workshop 07w5119
Operator Structures in Quantum Information Theory

David W. Kribs (University of Guelph) and Mary Beth Ruskai (Tufts University)

February 11 to February 16, 2007

1 Overview of the Field

This workshop brought together two distinct communities, mathematicians working on operator structures and mathematically oriented scientists in several disciplines working in quantum information theory (QIT). Based on feedback and observations during the workshop, it was extremely successful. There was no perceptible decline in attendance at talks or variation with subtopic.

It seems clear that this workshop will lead to an increased role for operator spaces in quantum information theory, and may be a landmark event. With a few exceptions, their role in QIT has been limited to the implicit use of a few concepts, such as a type of completely bounded norm, or a particular operator algebra, without recognition of the larger mathematical structure. The workshop has unequivocally changed this view. A few days after it ended, several participants posted the paper [64] "Unbounded violation of tripartite Bell inequalities" demonstrating the value of tools from operator spaces and tensor norms. In addition to obtaining a striking new result with important physical implications, the authors reformulate a question about commutative Banach algebras, which has been open for over 30 years, as a question about the types of states which give unbounded violations of Bell inequalities. At the August BIRS workshop 07w5013 Operator Spaces and Group Algebras, Ed Effros began with a talk on "Quantized functional analysis and quantum information theory".

Because of the varied backgrounds of the participants, the first three mornings were devoted to expository talks on operator spaces, quantum error correction and quantum Shannon theory. These were extremely valuable, with considerable demand for copies of the speakers notes and slides. The remaining time was divided between longer invited talks on important aspects of current research and short reports on recent results. We also had two sessions on open problems and time for discussion and relaxation.

Two important new results were announced at the workshop, in the talks by Junge [40] and Klappenecker [45], which are described in Sections 2.1 and 2.3, respectively. Several new collaborations were started during the workshop; one of these [47] uncovers a new connection between quantum cryptography and error correction based on complementary channels. A new result [55] was obtained on one of the open problems during the workshop. (See item D of Section 3.)

In July 2007, counter-examples were found [32, 84] to the so-called multiplicativity conjecture for tensor products of quantum channels, which had been open for over 5 years. This has significant implications for another important group of four equivalent "additivity" conjectures involving tensor products; these conjectures have been open for about 15 years and the different forms were shown to be globally equivalent by Shor in 2003 [74] As explicitly acknowledged in the announcements [32, 84], these breakthroughs were the result of the open problem sessions at the workshop and subsequent discussions among some of the participants. For additional information, see Section 5.6 of [70].

2 Summary of Scientific Developments Reported

2.1 Operator spaces

Edward Effros and Vern Paulsen gave a pair of well received introductory lectures on the abstract theory of operator spaces. Effros discussed some of the historical development of the subject, pointed out various subdisciplines of mathematics in which operator spaces arise, and prepared the audience for some of the technical complexities which arise in Pisier's L_p version.

Paulsen focussed on concrete operator spaces. He described a technique he had developed and presented elsewhere, but not written up, to compute completely bounded (CB) norms. In his approach, the CB norm can also be computed in a different way using the commutant. Although operator algebraists have not been enthusiastic about this reformulation, it seems likely that it will be useful in QIT where the commutant describes the algebra associated with the environment. One group [47] has already begun to explore this approach. Paulsen's talk was met with an exceptionally high level of interest from researchers in quantum information, and numerous inquiries from participants motivated Paulsen to write up his notes [62]. This talk was the genesis for the paper [37].

Ruskai (in discussions and her subsequent short talk) pointed out that in the usual models of quantum information, the algebra of observables for the environment is the commutant of those for the quantum information processing system. This suggests a new interpretation of the physical significance of the commutant in more abstract settings, and allows one to define concepts like the complement of a channel in these settings. Moreover, because the interplay between system and environment is important, it is often useful to have an alternative description in terms of the environment's algebra, as Paulsen has done for CB norms.[1]

Both Effros and Paulsen emphasized the important role of the Haagerup tensor product, which was new to most of the audience and has yet to be exploited in quantum information theory. An underlying theme of Effros and Paulsen was the notion that any good mathematical concept can be quantized. von Neumann algebras have long been regarded as quantizations of (single variable) integration theory; operator spaces can be considered as quantizations of Banach space theory which yield a non-commutative version of vector-valued integration. Of course, it is not always clear when a quantized version of a mathematical concept models a physical quantum system, as demonstrated in Neufang's talk.

Marius Junge then spoke on the L_p version of operator spaces. He announced a counter-example (with Q. Xu) [40] to a convexity conjecture of Lieb and Carlen [13], which was open for over ten years. Their conjecture can be interpreted as an attempt at a non-commutative generalization of Minkowski's inequality to three spaces on which one has a Schatten L_p norm with $1 < p < 2$. The counter-example establishes that in non-commutative situations which require mixed L_p spaces, the naive formula $\left(\mathrm{Tr}_1(\mathrm{Tr}_2 A_{12}^p)^{q/p}\right)^{1/q}$ does not yield a norm. Thus, one is inevitably led to operator spaces, in particular, the non-commutative vector-valued L_p spaces for which Pisier defined norms using complex interpolation [39, 65, 66, 67].

Junge also described the CB-entropy, a form of conditional information which arises by differentiating a suitable CB-norm at $p = 1$ and can be used to define the minimal CB entropy of a quantum channel. The minimal CB entropy of the identity channel on M_d is $-\log d$ which is consistent with the fact that it preserves maximal entanglement. When one interprets the minimal CB entropy as a measure of optimal entanglement preservation, the seemingly anomalous fact that the CB norm of the identity map is $d^{1/p} \neq 1$ becomes quite natural.

Matthias Neufang gave a talk on quantum groups and an associated class of multiplier algebras, based on recent joint work with Junge, Ruan, and Spronk. He noted that these algebras yield natural "quantum" channels for which the minimal CB entropy can be computed explicitly and shown to be positive. Thus, these channels are "classical" in the sense that they do not preserve enough entanglement to yield even one EPR pair. Nevertheless, they may have useful properties for quantum error correction, as they appear to have an abundance of noiseless subsystems, decoherence-free subspaces, and unitarily correctable codes. This may be less perplexing in view of the fact that some of the most useful quantum codes are derived from known classical codes.

[1] Earlier Jencova [36] had simplified the proof of additivity of CB entropy by showing that a particular CB norm could be expressed as the norm of the channel lifted to the commutant. It seems worth asking whether this is a special case of Paulsen's result or if both are special cases of a more general relationship.

2.2 Quantum Shannon Theory

The concept of a completely positive map on an operator algebra predates operator spaces and plays an important role in quantum information theory. When the system and environment are initially disentangled, the effect of noise, which comes from interactions with the environment is described mathematically by a completely positive, trace preserving (CPT) map on the algebra of the system. The term "quantum channel" is often used when a CPT map represents noise. Shannon developed the mathematical theory for dealing with noise in classical communication. Extending this to quantum systems is challenging and much richer because of the many different types of quantum information processing protocols.

Patrick Hayden gave an introductory overview of the current state of the art in the quantum information analogue of Shannon's communication theory. He described Schumacher's typical subspace theorem and the recent progress [4] made in quantum distributed compression of correlated sources (quantum Slepian-Wolf theorem and fully quantum version thereof, aka "mother protocol"), which greatly unify the theory of entanglement distillation and quantum channel capacities. The information-theoretic significance of these results lies in their giving operational significance to quantities like the quantum conditional entropy.

Graeme Smith discussed the notorious problem of the non-additivity of the coherent information (with the implication that the quantum channel capacity is not known except for so-called degradable channels, on which Mary Beth Ruskai gave an overview with open problems). To approach this problem, he introduced a single-letter upper bound [77], whose good properties allowed the derivation of the best upper bounds on the capacity of the depolarising channel to-date.

Ruedi Seiler presented the work of his group in Berlin [8, 9] on the quantum version of Sanov's theorem, which is about hypothesis testing of a set of alternatives against a single null hypothesis. As in the classical case, the optimal rate of discrimination is given by a (minimal) relative entropy; strangely, however, the optimum is not achieved by a universal strategy. Related to this topic, Arleta Szkola and Koenraad Aundeaert explained their complementing work on the quantum Chernoff bound, described in Section 2.5. i.e. error-symmetric distrimination between two hypotheses in the asymptotic regime. The resolution of this problem relies on a beautiful new trace inequality discovered to evaluate the asymptotics of the optimal test.

Andreas Winter discussed at length an open question originating from joint work with John Smolin and Frank Verstraete, which they call the "asymptotic quantum Birkhoff conjecture". (See Conjecture 13 in [78] and Problem 30 at [83].) It is well-known that bistochastic quantum channels have more extremal points than the unitary conjugations. However, there are indications that in the limit of high tensor powers of a bistochastic channel it becomes asymptotically well approximated by mixtures of unitary conjugations. Winter's talk was followed by a vigorous discussion about alternative conjectures. One issue is whether it is reasonable to expect that unitary conjugations will suffice when the known sets of extreme points include partial isometries.

2.3 Quantum error correction

The workshop included a series of talks that focussed on mathematical aspects of error correction in quantum computing. David Kribs started with an introductory lecture on the basic framework for quantum error correction. In the standard noise model, the state is corrupted by a quantum channel represented by a CPT map $\mathcal{E}$. The goal of quantum error correction is to find a subspace $\mathcal{C} \subset \mathcal{H}$ and a recovery operation, $\mathcal{R}$, also a CPT map such that $(\mathcal{R} \circ \mathcal{E})$ acts like the identity on the convex set of density matrices associated with the code subspace $\mathcal{C}$. If P denotes the projection onto $\mathcal{C}$, this can be stated formally as

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \qquad \forall\, \rho \,\in\, P\mathcal{B}(\mathcal{H})P \tag{1}$$

When the CPT map is written in the Choi-Kraus operator sum form $\mathcal{E}(\rho) = \sum_a E_a \rho E_a^*$, it is well-known that Eq. (1) is equivalent to the condition

$$PE_a^* E_b P = \lambda_{ab} P \tag{2}$$

for some complex set of numbers λ_{ab} and $\mathcal{C} = P\mathcal{H}$. The intuition behind this equivalence is best seen by considering the special case in which $E_a = t_a U_a$ with U_a unitary and t_a^2 interpreted as the probability that the error $U_a : \psi \mapsto U_a\psi$ occurs. Then $\lambda_{ab} = x_a \delta_{ab}$ says that the different unitary errors map vectors in $\mathcal{C}$ into orthogonal subspaces. The recovery operation can then be thought of as the two-step process

i) identify the orthogonal subspace, $U_a\mathcal{C}$, and

ii) apply the inverse operation U_a^*.

The sufficiency of the condition Eq. (2) can then be regarded as arising from the fact that the operators E_a are only determined up to a unitary transformation which can be used to "diagonalize the error operators" so that $\lambda_{ab} = x_a\delta_{ab}$.

Ruskai initiated a vigorous discussion which clarified some of the limitations of this viewpoint. For example, there are non-unital qubit channels (of which only the amplitude-damping channel has been studied extensively) with exactly two (non-unitary) error operations E_1, E_2 for which no change of basis can make one of them the identity. Thus, one can not associate a probability with particular error operator, and the channel (almost) always changes the state. Nevertheless, any code and recovery process which corrects all unitary one qubit errors, will correct all one qubit errors, including these non-unital ones. In this case, one can correct errors that can not even be detected! This is a consequence of the quantum measurement process which has the effect of either correcting the error or converting it to a detectable one; mathematically, this can be viewed as a consequence of the fact that the set of correctable errors froms a vector space. (The error detection condition is given by Eq. (2) with $E_a = I$.)

In most discussions of quantum error code construction, one deals with error models which are even more specialized than the random unitary model mentioned above. One considers only errors which are tensor products of the identity and the three Pauli matrices. An Abelian subgroup of the group generated by such errors is called a stabilizer and the simultaneous eigenspace is called a stabilizer code. Although examples of codes which do not arise from the stabilizer formalism exist [69, 76] most work has concentrated on stabilizer codes.

Kribs also discussed the important new framework of "operator quantum error correction" [48, 49]. This is a unified framework for quantum error correction that includes the standard active framework discussed above, as well as the fundamental passive techniques for error correction – decoherence-free subspaces and noiseless subsystems. Technically speaking, a quantum system A is a *subsystem* of a Hilbert space $\mathcal{H}$ if there is a subsystem B such that $C = A \otimes B$ is a subspace of $\mathcal{H}$. Then A is correctable for the action of $\mathcal{E}$ if there is a CPT map $\mathcal{R}$ such that

$$\forall \rho^A \, \forall \rho^B \, \exists \, \tau^B \, : \, (\mathcal{R} \circ \mathcal{E})(\rho^A \otimes \rho^B) = \rho^A \otimes \tau^B. \tag{3}$$

Intuitively, quantum information is encoded into the A subsystem, and the recovery operation $\mathcal{R}$ is not concerned with noise acting on the ancilla subsystem B. For this reason, these codes have been popularly called "subsystem codes". Simply put, the standard active case corresponds to $\dim A = 1$ with general $\mathcal{E}$, $\mathcal{R}$, and decoherence-free subspaces (respectively noiseless subsystems) are captured when no recovery is required ($\mathcal{R} =$ identity map) and $\dim A = 1$ (respectively $\dim A > 1$). Other cases correspond to situations not recognized in any formal way previously within quantum error correction.

Andreas Klappenecker gave an expository talk on the state of the art for subsystem code constructions. Because the Pauli matrcies form a basis for M_2, any code which can correct all one-qubit Pauli errors can correct arbitrary one qubit errors, including some very strange ones, as described above. In view of this, Knill defined a general notion of "nice error bases" in higher dimensions. Klappenecker reviewed his work with Rötteler [43] in which they found new codes based on these nice error bases, only to find that most of them could also be realized as stabilizer codes. Then, he described the light at the end of the tunnel in which the group representation theory which had led to so much frustration finally found a natural place under the umbrella of subsystem codes [3, 44, 45]. He concluded with the announcement of two new results. First he gave a negative answer to Poulin's question [68] of whether a subsystem code might require fewer syndrome measurements than an optimal stabilizer code. Then he described the construction of a subsystem code which can beat classical Hamming bound [45].

The expository error correction talks concluded with a discussion by Andrew Cross on the basics of fault tolerant quantum computing. Cross also presented joint work with Aliferis [1] showing how the use of a particular subsystem code, the so-called "Bacon-Shor codes" appears to significantly improve threshold estimates by reducing the number of measurements required in recovery operations. The implications of subsystem codes for quantum computing are still very much being explored. This was particularly evident at a Perimeter Institute workshop on fault tolerant quantum computing held in June, 2007, a few months after the BIRS workshop, in which subsystem codes were a predominant theme in discussions.

Fault tolerant computation seems to require codes which, at least in principle, permit perfect recovery. However, in other types of quantum information processing, as in classical information theory, there is a role for codes which lead to optimal recovery in certain situations [23, 89]. Bernhard Bodmann described work with Kribs and Paulsen [10] which finds optimal encoding schemes when one subsystem is essentially noiseless and the other is subject to a phase-damping channel.

Cedric Beny spoke about his recent work with Kempf and Kribs [7] that further generalizes the basic quantum error correction framework to operator algebras by considering the Heisenberg picture, and how the new approach provides a formalism for the correction of hybrid classical and quantum information [50].

Holbrook and Zyczkowski described joint work [15, 16, 17, 18] with Choi and Kribs motivated by the fundamental equation Eq. (2). For a fixed operator T they seek solutions of the matrix equation $PTP = xP$ with P a projection and $x \in \mathbf{C}$. When P is rank one, the set of x is precisely the numerical range of U and is the convex hull of the eigenvalues of T. Therefore, they call the set of x for which P has rank k the "rank-k numerical range of T" and conjecture that for normal T this is equal to the intersection of the convex hulls obtained from all possible choices of $N - k + 1$ eigenvalues. They can verify the conjecture when T is self-adjoint and reduce the general normal case to T unitary, for which significant partial results were reported. (See the open problems section for an update.) The long range goal of this work would be to construct new codes from the compatibility of the allowable projectors P_a for different T_a. Ruskai pointed out some interesting open problems described in [38] and [75] on which this approach to code construction could be tested.

2.4 Lattice spin models

The mathematical study of quantum spin models has had close interactions with developments in the theory of operator algebras for many decades. Many results of physical interest have been rigorously derived in the operator algebra framework. It is an instance of an almost perfect match between mathematics and physics where the pursuit of rigor does not require a sacrifice of physical interest. More recently, a new dimension has been added to this fruitful interaction. The exciting developments in quantum information theory, especially the study of entanglement, has provided new insight in the structure of physical states of quantum spin models, particularly their ground states.

Frank Verstraete gave a comprehensive review of new techniques he and others [71, 72, 80, 81] have created for the computational study of quantum spin models based on new ideas from quantum information theory. These developments are especially timely because of the impressive progress by experimental physicists in their ability to create strongly correlated and entangled states exhibiting a wide variety of quantum phase transitions, Bose-Einstein condensation and other exotic states of matter. Matrix Product States (MPS), also known as Finitely Correlated States (FCS) and their higher-dimensional generalizations called Projected Entangled Pair States (PEPS) were particularly highlighted. These are special states that have good computational properties and which form the basis for a host of efficient and very successful algorithms collectively known as Density Matrix Renormalization Group (DMRG) methods.

Bruno Nachtergaele gave an overview of Lieb-Robinson bounds and applications to quantum information theory. The original work by Lieb and Robinson [53], dating back to the early seventies, provided a proof that the Heisenberg dynamics of a translation invariant quantum spin system on a lattice has a bounded group velocity. The key step is a commutator estimate. Recently, Nachtergaele and Sims [58] found an improved commutator estimate which enable one to extend Lieb and Robinson's result to a rather general class of systems defined on a metric graph, which covers almost any conceivable architecture for a quantum information processing device. One example of a recent application that was presented is a lower bound for the time required to establish significant correlations between two regions in space using any local dynamics. The lower bound is linear in the distance between the regions [12, 21, 60]. Another application is a Lieb-Schultz-Mattis Theorem in arbitrary dimensions [28, 59], which shows that under certain conditions low-energy excitations will occur even in the absence of continuous symmetry breaking.

When a spin chain is in a pure state, the entanglement entropy S_n of a block of length n in a pure state is the entropy of the reduced density matrix of this block. It is called the entanglement entropy because it corresponds to the standard measure of the entanglement between this block and the rest of the chain. In many situations, as the length of the chain becomes infinite, $\frac{1}{n}S_n \to 0$ which implies that S_n grows sublinearly with n. Numerical experiments by Vidal,et al [82] suggested logarithmic growth $S_n \sim \log n$ at a critical

point. This was subsequently proved rigorously by Jin and Korepin [35] for the ground state of the XX model. Although Korepin was originally scheduled to talk about this work, personal circumstances forced him to cancel. Therefore, Milan Mosonyi included an overview of entanglement entropy for spin chains in his talk. Mosonyi, then described related work with Fannes and Haegeman [22] in which they showed that one can construct quasi-free states for which $S_n \sim n^\alpha$ for any $0 < \alpha < 1$.

For lattices, it has been conjectured that away from a critical point the entanglement entropy obeys scales like the "area" of the boundary. This implies a uniform bound away from the critical point in the case of a spin chain. Subsequently, it was realized that the circumstances under which an area law does or does not hold depends on additional properties [24] of the lattice model. This topic was touched upon briefly in both Mosonyi's and Verstraete's lecture. Since the workshop, there has been considerable progress [29, 87] on this topic, exploiting the improved Lieb-Robinson bounds described in Nachtergaele's lecture.

In quantum statistical mechanics, the use of quasi-local algebras plays an important role in showing that the infinite volume thermodynamic limit exists for certain types of lattice systems. In generalizing the concept of cellular automata to quantum systems, one challenge is to allow an initially finite lattice system to grow without bound in any direction. R. Werner described his approach [73] to quantum cellular automata based on quasi-local algebras.

2.5 Quantum state discrimination

Two speakers, Szkola and Audenaert, gave talks about their recent work on state discrimination. Taken together their results determine the quantum Chernoff bound, thereby settling a problem which has been open for several years. The problem is to find the best measurement for distinguishing two (known) quantum states ρ and σ. In general this cannot be done with full certainty (unless the states are orthogonal), and so the goal is to find the minimum error $\mathrm{MinErr}(\rho, \sigma)$. Assuming that multiple copies of the states are available, this leads to the question of finding the best way to distinguish $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, and hence to find the asymptotic rate $\lim_{n\to\infty} \frac{1}{n} \log \mathrm{MinErr}(\rho^{\otimes n}, \sigma^{\otimes n})$. The corresponding rate in the classical problem was found by Chernoff, and there has been a search for the quantum version in recent years. In a major breakthrough in 2006, Szkola and Nussbaum showed that the rate is lower bounded by the quantity $\log \big(\min_{0\le s\le 1} \mathrm{Tr}\rho^s\sigma^{1-s} \big)$, which is almost a direct translation of the classical Chernoff bound into quantum language. Szkola described this result in her talk and discussed its relation to the notion of the quantum Hellinger arc which interpolates between the states ρ and σ.

At the end of 2006, in another breakthrough, Audenaert and his collaborators proved that this quantity is also an upper bound for the rate, thereby establishing equality. In his talk Audenaert emphasized the properties of the quantum Chernoff bound as a measure of the distance between two states, and showed how it induces a metric on the state space. He explained how the Chernoff bound follows from a new matrix inequality which states that for positive matrices A, B and all $0 \le s \le 1$

$$\tfrac{1}{2}(\mathrm{Tr}(A+B) - \mathrm{Tr}|A-B|) \le \mathrm{Tr}A^s B^{1-s}. \tag{4}$$

This inequality, which has other applications, allows one to relate the trace-norm distance of two states to their Renyi relative entropy.

In a related talk on state discrimination, Anna Jencova described her work [26] with Guta on quantum statistics, which is concerned with using results of measurements to infer properties of quantum states and systems. In particular she described results about local asymptotic normality. This property applies to a sequence of two dimensional random variables whose distributions depend on an (unknown) parameter. When localized in the neighborhood of some fixed point of the parameter space, the property implies convergence to a family of Gaussian distributions. Jencova talked about the theory of quantum statistical experiments, and showed how this leads to a quantum version of local asymptotic normality. For both classical and qubit systems, it has been shown that weak and strong convergence are equivalent. Whether or not this holds for general quantum systems is still open. However, Guta and Jencova are able to prove weak convergence for general quantum systems.

2.6 Other Topics Covered

Robert Alicki gave a provocative talk based on the assertion that a scalable quantum computer would be a "perpetuum mobile of the second kind". The key assumption is that the system is initially in a metastable state which is almost a KMS state. The talk was punctuated by a vigorous discussion of the validity of these assumptions. In the end, many participants felt what was presented was a proof by "reductio ad absurdum" from dubious assumption and that what was needed was an argument based on rigorous bounds.

Jen Eisert reported on some recent work [25, 41] regarding the so-called cluster states, which have high multi-article entanglement in the sense that entanglement within some subsystems persists after repeated measurements. These states have important applications in the development of the so-called "one-way" quantum computer. Eisert described modified protocols which can tolerant some noise or imperfect clusters.

Wolf reported on recent work with Cirac [86] on the question of whether or not a quantum channel can be written non-trivially as the composition of two other channels. It may be surprising that there are situations in which this cannot be done; for qubits, these are precisely the channels with exactly three Kraus operators. More generally, one can ask when a channel T can be written as $T = S^n$. Even for T very close to the identity channel, this need not always be possible because T completely positive need not imply that $T^{1/n}$ is completely positive. After giving an overview of the various phenomena which can occur in different situations, Wolf described some of the open questions which remain.

Dennis Kretschmann presented recent work (with Dirk Schlingemann and Reinhard Werner) [46] concerning a continuity theorem for the Stinespring representation of a quantum channel. Stinespring's Theorem guarantees that every quantum channel can be represented (non-uniquely) in the Heisenberg picture by an isometric embedding into a larger space. This suggests that two channels which are 'close' in some sense should be representable by isometries which are also close. As Kretschmann and co-authors showed, the correct notion of closeness for channels in this context is the completely bounded or 'cb' norm, which is a regularized version of the operator norm. The authors prove inequalities comparing the cb norm of the difference of two channels with the minimal operator norm of the difference of the isometries in their Stinespring representations. These inequalities provide dimension-independent bounds for the information-disturbance tradeoff inherent in any measurement of a system. The inequalities also allow a continuity estimate for the no-broadcasting theorem, and a strengthened proof of impossibility for quantum bit commitment.

3 Open problems

One of the highlights of the workshop were two sessions reserved for discussion of open problems, to which the participants responded enthusiastically. Ruskai started things off by distributing a preliminary draft of [70]. Many participants described open problems during their talks, as well as in the dedicated sessions. Participants were asked to write up these problems and send them to R. Werner for inclusion on his open problem web site. A list of the major problems follows, with comments on recent progress.

List of open problems

A. The first 6 sections in Ruskai's list [70] were discussed in the workshop. Some contain several related problems. The 7-th section was outside the scope of the workshop and added later. The main sections are

   1. Extreme points of CPT maps: As a consequence of the workshop, Ruskai showed that what are sometimes called "quasi-extreme" points which have Choi rank d but are not true extreme points of the convex set are in the closure of the set of extreme points. This allows a clearer statement of the open problems.
   2. Convex decompositions of CPT maps or A block matrix generalization of Horn's lemma (with K. Audenaert).
   3. Generalized depolarized channels: The original emphasis was on the generalized Werner-Holevo channel. However, the developments in [84] suggested a further generalization using any channel that is very noisy to replace the completely noisy one.
      Progress: Michalakis [56] has solved Problem 6 for p = 2. It seems likely that his methods can be extended to provide some results for Problem 7 and for Problem 12.

4. Random sub-unitary channels
5. Additivity and multiplicativity conjectures: Very few changes were made to earlier versions of this section despite the recent breakthroughs. It seemed better to leave things in the original form to emphasize the impact of that work. One minor modification was the extension of Shor's Theorem 3 in Section 5.3 to $p < 1$ by the use of the general form of Klein's inequality, which then gives a single simple argument for all $p > 0$. This may be useful in doing numerical work to move from existence theorems to explicit counter-examples.

   Progress: Section 5.6 describes the current status of counter-examples [31, 32, 84] to multiplicativity conjectures and the implications for additivity. It also contains weaker versions of multiplicativity conjectures. It should again be emphasized that these counter-examples were stimulated by the open problem session and discussion at the workshop.
6. Coherent information and degradability: This problem was presented in Ruskai's talk at the workshop based on work in [19] which may contain some related open questions.
7. Local invariants for N-representability

B. Entropic uncertainty relations for more than two observables by D. Leung, S. Wehner, and A. Winter

C. Quantum Birkhoff Conjecture. This is conjecture 13 in [78] and Problem 30 at [83]. After Winter's talk there was a vigorous discussion as to whether or not it might be necessary to extend the conjecture to include partial isometries, such as the random sub-unitary maps described in Section 4 of [70]. A 1958 paper [54] entitled "The convex hull of sub-permutation matrices" and related work from that era might be useful to those who favor including random sub-unitary maps.

D. Best Constant in Norm bounds on Commutators: This problem was posed in [11] and presented to workshop participants by K. Audenaert along with a summary of known results.

   Progress: During the workshop, S. Michalakis [55] solved this problem for the commutator $[X, X^*]$ by showing that $\sqrt{2}$ is sharp in $\| [X, X^*] \|_2 \leq \sqrt{2}\|X\|_2^2$.

E. Structure of the nth matrix range of an operator, by V.I. Paulsen.

F. Structure of higher rank numerical ranges, by M.-D. Choi, J.A. Holbrook, D.W. Kribs, K. Zyczkowski, as outlined above.

   Progress: Shortly after this workshop, a flurry of work came to light from mathematicians working on higher rank numerical ranges. Most importantly, a related convexity conjecture was settled in the affirmative by Woerdeman [85], and then by Li and Sze [52] using different techniques which they were able to apply to the normal case. Thus, the door has been further opened for potential applications in quantum error correction.

4 Appendices attached as pdf files

A. Some open problems in quantum information theory by M.B. Ruskai

B. Entropic uncertainty relations for more than two observables by, D. Leung, S. Wehner, and A. Winter

C. Structure of the nth matrix range of an operator, by V.I. Paulsen.

D. Best Constant in Norm bounds on Commutators by K. Audenaert

E. Abstract of E. Effros for BIRS workshop 07w5013 on Operator Spaces and Group Algebras

References

[1] P. Aliferis, A. W. Cross, Subsystem fault tolerance with the Bacon-Shor code, *Phys. Rev. Lett.* 98 (2007), 220502.

[2] P. Aliferis, D. Gottesman, J. Preskill, Accuracy threshold for postselected quantum computation, quant-ph/0703264.

[3] S.A. Aly, A. Klappenecker, P.K. Sarvepalli, Subsystem Codes, quant-ph/0610153.

[4] A. Abeyesinghe, I. Devetak, P. Hayden, A. Winter, The mother of all protocols: Restructuring quantum information's family tree, quant-ph/0606225.

[5] W. Arveson, "Subalgebras of C*-Algebras" *Acta Mathematica* **123** (1969), 141–224.

[6] K.M.R. Audenaert, J. Calsamiglia, Ll. Masanes, R. Munoz-Tapia, A. Acin, E. Bagan, F. Verstraete The Quantum Chernoff Bound, *Phys. Rev. Lett.* 98 (2007), 160501.

[7] C. Beny, A. Kempf, D.W. Kribs, Generalization of Quantum Error Correction via the Heisenberg Picture, *Phys. Rev. Lett.* 98 (2007), 100502.

[8] I. Bjelakovic, J.-D. Deuschel, T. Krueger, R. Seiler, Ra. Siegmund-Schultze, A. Szkola, A quantum version of Sanov's theorem, *Commun. Math. Phys.*, to appear.

[9] I. Bjelakovic, J.-D. Deuschel, T. Krueger, R. Seiler, Ra. Siegmund-Schultze, A. Szkola, Typical support and Sanov large deviations of correlated states, math.PR/0703772.

[10] B.G. Bodmann, D.W. Kribs, V.I. Paulsen, Decoherence-Insensitive Quantum Communication by Optimal C^*-Encoding, *IEEE Trans. Inf. Thy.*, to appear.

[11] A. Böttcher and D. Wenzel, How big can the commutator of two matrices be and how big is it typically?, *Lin. Alg. Appl.* **403** (2005) 216–228.

[12] S. Bravyi, M. B. Hastings, F. Verstraete, Lieb-Robinson bounds and the generation of correlations and topological quantum order, *Phys. Rev. Lett.* 97, 050401 (2006).

[13] E. Carlen and E. Lieb, A Minkowski type trace inequality and strong subadditivity of quantum entropy, *Amer. Math. Soc. Transl.* **189**, 59–62 (1999). Reprinted in [51].

[14] M.-D. Choi, Completely Positive Linear Maps on Complex Matrices, *Lin. Alg. Appl.* **10**, 285–290 (1975).

[15] M.-D. Choi, D.W. Kribs, A method to find quantum noiseless subsystems, *Phys. Rev. Lett.*, 96, 050501 (2006).

[16] M.-D. Choi, D.W. Kribs, K. Zyczkowski, Quantum error correcting codes from the compression formalism, *Rep. Math. Phys.*, 58 (2006), 77-91.

[17] M.-D. Choi, D.W. Kribs, K. Zyczkowski, Higher-rank numerical ranges and compression problems, *Lin. Alg. Appl.*, 418 (2006), 828-839.

[18] M.-D. Choi, J.A. Holbrook, D.W. Kribs, K. Zyczkowski, Higher-rank numerical ranges of unitary and normal matrices, *Lin. & Mult. Alg.*, to appear.

[19] T. Cubitt, M.B. Ruskai and G. Smith, in preparation.

[20] E. G. Effros and Z. J. Ruan, *Operator Spaces* (Oxford Univ. Press, 2000).

[21] J. Eisert, T.J. Osborne, General entanglement scaling laws from time evolution, *Phys. Rev. Lett.* 97, 150404 (2006).

[22] M. Fannes, B. Haegeman, M. Mosonyi, Entropy growth of shift-invariant states on a quantum spin chain, math-ph/0306055.

[23] A.S. Fletcher, P.W. Shor, M.Z. Win, Optimum quantum error recovery using semidefinite programming, quant-ph/0606035.

[24] D. Gioev, I. Klich, Entanglement entropy of fermions in any dimension and the Widom conjecture, *Phys. Rev. Lett.* 96, 100503 (2006)

[25] D. Gross, J. Eisert, N. Schuch, D. Perez-Garcia Measurement-based quantum computation beyond the one-way model arXiv:0706.3401

[26] M. Guta, A. Jencova, Local asymptotic normality in quantum statistics, *Commun. Math. Phys.*, in press (2007).

[27] M. Guta, B. Janssens, J. Kahn, Optimal estimation of qubit states with continuous time measurements, *Commun. Math. Phys.*, to appear.

[28] Matthew B. Hastings, Lieb-Schultz-Mattis in Higher Dimensions *Phys.Rev. B* 69 104431 (2004.) arXiv:cond-mat/0305505

[29] M. B. Hastings, An area law for one dimensional quantum systems, arXiv:0705.2024.

[30] M.B. Hastings, T. Koma, Spectral Gap and Exponential Decay of Correlations *Commun.Math.Phys.* 265 (2006) 781-804

[31] A. Harrow, D. Leung, A. Winter, private communication.

[32] P. Hayden, The maximal p-norm multiplicativity conjecture is false, arXiv:0707.3291.

[33] P. Hayden, D. Leung, A. Winter, Aspects of generic entanglement *Commun. Math. Phys.* 265, 95–117 (2007).

[34] P. Hayden, M. Horodecki, J. Yard, A. Winter, A decoupling approach to the quantum capacity, quant-ph/0702005.

[35] A. R. Its, B.-Q. Jin, V. E. Korepin, Entanglement in XY Spin Chain, *J. Phys. A: Math. Gen.* 38 (2005), 2975-2990.

[36] A. Jencŏvá , A relation between completely bounded norms and conjugate channels, *Commun. Math. Phys.* 266 (2006), 65–70. quant-ph/0601071.

[37] N. Johnston, D.W. Kribs, V. Paulsen, Computing stabilized norms in quantum information, preprint.

[38] S.P. Jordan, E. Farhi, P.W. Shor, Error correcting codes for adiabatic quantum computation, *Phys. Rev. A* 74, 052322 (2006).

[39] M. Junge, Factorization theory for spaces of operators, Habilitation thesis Kiel University (1996).

[40] M. Junge, Q. Xu, Counterexamples for the convexity of certain matricial inequalities, arXiv:0709.0433

[41] K. Kieling, D. Gross, J. Eisert Cluster state preparation using gates operating at arbitrary success probabilities arXiv:quant-ph/0703045

[42] A. Klappenecker, M. Rötteler, Beyond Stabilizer Codes I: Nice Error Bases; II : Clifford Codes, *IEEE Trans. Info. Theory* 48 (2002), 2392–2399.

[43] A. Klappenecker, M. Rötteler, Remarks on Clifford codes, quant-ph/0312228.

[44] A. Klappenecker, P. K. Sarvepalli, Clifford Code Constructions of Operator Quantum Error Correcting Codes, quant-ph/0604161.

[45] A. Klappenecker, P. K. Sarvepalli, On subsystem codes beating the Hamming or Singleton bound, quant-ph/0703213.

[46] D. Kretschmann, D. Schlingemann, R.F. Werner, The information-disturbance tradeoff and the continuity of Stinespring's representation, quant-ph/0605009.

[47] D. Kretschmann, D.W. Kribs, R. Spekkens, Complementarity of correctable and private subsystems, preprint.

[48] D.W. Kribs, R. Laflamme, D. Poulin, A unified and generalized approach to quantum error correction, *Phys. Rev. Lett.*, 94, 180501 (2005).

[49] D.W. Kribs, R. Laflamme, D. Poulin, M. Lesosky, Operator quantum error correction, *Quant. Inf. & Comp.*, 6 (2006), 382-399.

[50] G. Kuperberg, The capacity of hybrid quantum memory *IEEE Trans. Inf. Theory* 49 (2003), 1465-1473. arXiv:quant-ph/0203105

[51] *Inequalities: Selecta of E. Lieb*, M. Loss and M.B. Ruskai, eds (Springer, 2002).

[52] C.-K. Li, N.-S. Sze, Canonical forms, higher-rank numerical ranges totally isotropic spaces, and matrix equations, preprint.

[53] E. Lieb and D. Robinson, The finite group velocity of quantum spin systems. *Comm. Math. Phys.* 28 (1972), 251–257.

[54] N.S. Mendelsohn, A.L. Dulmage, The convex hull of sub-permutation matrices, Proc. Amer. Math. Soc., 9 (1958), 253–254.

[55] S. Michalakis, private communication during BIRS workshop.

[56] S. Michalakis, Multiplicativity of the maximal output 2-norm for depolarized Werner-Holevo channels, arXiv:0707.1722.

[57] S. Michalakis, B. Nachtergaele, Entanglement in finitely correlated spin states, *Phys. Rev. Lett.* 97 (2006) 140601.

[58] B. Nachtergaele, R. Sims, Lieb-Robinson bounds and the exponential clustering theorem, *Commun. Math. Phys.*, 265 (2006) 119-130.

[59] B. Nachtergaele, R. Sims, A multi-dimensional Lieb-Schultz-Mattis theorem, math-ph/0608046.

[60] B. Nachtergaele, Y. Ogata, R. Sims, Propagation of correlations in quantum lattice systems, *J. Stat. Phys.* 124 (2006), 1-13.

[61] V. Paulsen, *Completely Bounded Maps and Operator Algebras* (Cambridge University Press, 2002).

[62] V. Paulsen, BIRS.

[63] D. Perez-Garcia, F. Verstraete, M.M. Wolf, J.I. Cirac, Matrix Product State Representations, *Quantum Inf. Comput.* 7 (2007), 401.

[64] D. Perez-Garcia, M.M Wolf, C. Palazuelos, I. Villanueva, M. Junge, Unbounded violation of tripartite Bell inequalities, quant-ph/0702189.

[65] G. Pisier, The Operator Hilbert Space OH, Complex Interpolation and Tensor Norms, *Memoirs AMS*, 122 (American Mathematical Society, 1996).

[66] G. Pisier, Non-commutative vector valued L_p-spaces and completely p-summing maps (Société Mathématique de France, 1998).

[67] G. Pisier, *Introduction to Operator Space Theory* (Cambridge University Press, 2003).

[68] D. Poulin, Stabilizer formalism for operator quantum error correction, *Phys. Rev. Lett.* 95 (2005), 230504.

[69] E.M. Rains, R. H. Hardin, P. W. Shor, N. J. A. Sloane, A nonadditive quantum code *Phys. Rev. Lett.* 79 (1997), 953–954.

[70] M.B. Ruskai. Some open problems in quantum information theory, arXiv:0708.1902.

[71] N. Schuch, M.M. Wolf, F. Verstraete, J.I. Cirac, The computational complexity of PEPS, *Phys. Rev. Lett.* 98 (2007), 140506.

[72] N. Schuch, M.M. Wolf, F. Verstraete, J.I. Cirac, Entropy scaling and simulability by matrix product states, arXiv:0705.0292.

[73] B. Schumacher, R.F. Werner, Reversible quantum cellular automata, quant-ph/0405174.

[74] P.W. Shor, Equivalence of additivity questions in quantum information theory, *Comm. Math. Phys.* 246 (2004), 453–472.

[75] G. Smith, J.A. Smolin, Degenerate quantum codes for Pauli channels, *Phys. Rev. Lett.* 98, 030501 (2007)

[76] J.A. Smolin, G. Smith, S. Wehner, A simple family of nonadditive quantum codes, quant-ph/0701065.

[77] G. Smith, J.A. Smolin, A. Winter, The quantum capacity with symmetric side channels, quant-ph/0607039.

[78] J.A. Smolin, F. Verstraete, A. Winter, Entanglement of assistance and multipartite state distillation, *Phys. Rev. A*, 72 (2005), 052317.

[79] W.F. Stinespring, Positive functions on C^*-algebras, *Proc. Amer. Math. Soc.* 6 (1955), 211–216.

[80] F. Verstraete, D. Porras, J.I. Cirac, DMRG and periodic boundary conditions: a quantum information perspective, *Phys. Rev. Lett.* 93 (2004), 227205.

[81] F. Verstraete, M. M. Wolf, D. Perez-Garcia, J.I. Cirac, Criticality, the area law, and the computational power of PEPS *Phys. Rev. Lett.* 96 (2006), 220601.

[82] G. Vidal, G., Latorre, J. I., Rico, E., and Kitaev, A., Entanglement in quantum critical phenomena *Phys. Rev. Lett.* 90, 227902 (2003). arXiv:quant-ph/0211074

[83] R. Werner's open problem web site http://www.imaph.tu-bs.de/qi/problems/problems.html

[84] A. Winter, The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$, arXiv:0707.0402.

[85] H. Woerdeman, The higher-rank numerical range is convex, Lin. & Mult. Alg., to appear.

[86] M.M. Wolf, J.I. Cirac, Dividing quantum channels, math-ph/0611057.

[87] M.M. Wolf, F. Verstraete, M.B. Hastings, J.I. Cirac, Area laws in quantum systems: mutual information and correlations, arXiv:0704.3906.

[88] M.M. Wolf, D. Perez-Garcia, Quantum capacities of channels with small environment, quant-ph/0607070.

[89] N. Yamamoto, S. Hara, K. Tsumura, Suboptimal quantum-error-correcting procedure based on semidefinite programming, *Phys. Rev. A* 71 (2005), 022322.

Open Problems in Quantum Information Theory

Mary Beth Ruskai*
Department of Mathematics, Tufts University, Medford, MA 02155
Marybeth.Ruskai@tufts.edu

August 14, 2007

Abstract

Some open questions in quantum information theory (QIT) are described. Most of them were presented in Banff during the BIRS workshop on Operator Structures in QIT 11-16 February 2007. New material has been added in view of the recent counter-examples to p-norm multiplicativity.

Contents

*Partially supported by the National Science Foundation under Grant DMS-0604900

1 Extreme points of CPT maps

In QIT, a channel is represented by a completely-positive trace-preserving (CPT) map $\Phi : M_{d_1} \mapsto M_{d_2}$, which is often written in the Choi-Kraus form

$$\Phi(\rho) = \sum_k A_k \rho A_k^\dagger \qquad \text{with} \qquad \sum_k A_k^\dagger A_k = I_{d_1}. \tag{1}$$

The state representative or Choi matrix of Φ is

$$\Phi(|\beta\rangle\langle\beta|) = \tfrac{1}{d} \sum_{jk} |e_j\rangle\langle e_k| \Phi(|e_j\rangle\langle e_k|) \tag{2}$$

where $|\beta\rangle$ is a maximally entangled Bell state. Choi [8] showed that the A_k can be obtained from the eigenvectors of $\Phi(|\beta\rangle\langle\beta|)$ with non-zero eigenvalues. The operators A_k in (1) are known to be defined only up to a partial isometry and are often called Kraus operators. When a minimal set is obtained from Choi's prescription using eigenvectors of (2), they are defined up to mixing of those from degenerate eigenvalues and we will refer to them as Choi-Kraus operators. Choi showed that Φ is an extreme point of the set of CPT maps $\Phi : M_{d_1} \mapsto M_{d_2}$ if and only if the set $\{A_j^\dagger A_k\}$ is linearly independent in M_{d_1}. This implies that the Choi matrix of an extreme CPT map has rank at most d_1. We will refer to the rank of (2) as the *Choi rank* of Φ. (Note that this is *not* the same as the rank of Φ as a linear operator from M_{d_1} to M_{d_2}.)

It is often useful to consider the set of all CPT maps with Choi rank $\leq d_1$. In [44] these were called "generalized extreme points" and shown to be equivalent to the closure of the set of extreme points for qubit maps. This is true in general. Let $\mathcal{E}(d_1, d_2)$ denote the extreme points of the convex set of CPT maps from M_{d_1} to M_{d_2}.

Theorem 1. *The closure $\overline{\mathcal{E}(d_1, d_2)}$ of the set of extreme points of CPT maps $\Phi : M_{d_1} \mapsto M_{d_2}$ is precisely the set of such maps with Choi rank at most d_1.*

Proof: Let Let A_k be the Choi-Kraus operators for a map $\Phi : M_{d_1} \mapsto M_{d_2}$ with Choi rank $r \leq d_1$ which is not extreme, and let B_k be the Choi-Kraus operators for a true extreme point with Choi-rank d_1. When $r < d_1$ extend A_k by letting $A_m = 0$ for $m = r+1, r+2, \ldots d_1$ and define $C_k(\epsilon) = A_k + \epsilon B_k$. There is a number ϵ_* such that the d_1^2 matrices $C_j^\dagger(\epsilon)C_k(\epsilon)$ are linear independent for $0 < \epsilon < \epsilon_*$. To see this, for each $C_j^\dagger(\epsilon)C_k(\epsilon)$ "stack" the columns to give a vector of length d_1^2 and let $M(\epsilon)$ denote the $d_1^2 \times d_1^2$ matrix formed with these vectors as columns. Then $\det M(\epsilon)$ is a polynomial of degree d_1^4, which has at most d_1^4 distinct roots. Since the matrcies $A_j^\dagger A_k$ were assumed to be linearly dependent, one of these roots is 0; it suffices to take ϵ_* the next largest root (or $+1$ if no roots are positive). Thus, the operators $C_j^\dagger(\epsilon)C_k(\epsilon)$ are linearly independent for $\epsilon \in (0, \epsilon_*)$. The map $\rho \mapsto \sum_k C_k(\epsilon)\rho\, C_k^\dagger(\epsilon)$ is CP, with

$$\sum_k C_k^\dagger(\epsilon)\, C_k = (1+\epsilon^2)I + \epsilon(A_k^\dagger B_k + B_k^\dagger A_k) \equiv S(\epsilon).$$

For sufficiently small ϵ the operator $S(\epsilon)$ is positive semi-definite and invertible, and the map $\Phi_\epsilon(\rho) = C_k(\epsilon)S(\epsilon)^{-1/2}\rho S(\epsilon)^{-1/2}C_k^\dagger(\epsilon)$ is a CPT map with Kraus operators $C_k(\epsilon)S(\epsilon)^{-1/2}$. Thus, one can find ϵ_c such that $\epsilon \in (0, \epsilon_c)$ implies that $\Phi_\epsilon \in \mathcal{E}(d_1, d_2)$. It then follows from $\lim_{\epsilon \to 0+} \Phi_\epsilon = \Phi$ that $\Phi \in \overline{\mathcal{E}(d_1, d_2)}$. **QED**

When $d_1 = 2$, one can use the singular value decomposition (SVD) to show that that the Kraus operators of CPT maps with Choi rank at most two can be written in the form

$$A_1 = \sum_{j=1,2} \alpha_j |v_j\rangle\langle u_j| \qquad A_2 = \sum_{j=1,2} \sqrt{1-\alpha_j^2}\,|w_j\rangle\langle u_j| \tag{3}$$

where $0 \leq \alpha_j \leq 1$, $|u_j\rangle$ is pair of orthonormal vectors in $\mathbf{C}_2$, and $|v_j\rangle, |w_j\rangle$ are two pairs of orthonormal vectors in $\mathbf{C}_{d_2}$. This gives all CPT maps in $\overline{\mathcal{E}(2, d_2)}$. Although it may seem artificial from a physical point of view to consider $d_1 \neq d_2$, several reduction results in quantum Shannon theory require consideration of maps with $d_1 \neq d_2$.

Problem 1. *Characterize, classify and/or parameterize the closure $\overline{\mathcal{E}(d_1, d_2)}$ of the set of extreme points of CPT maps $\Phi : M_{d_1} \mapsto M_{d_2}$ for $d_1 > 2$ and d_2 arbitrary.*

Although this problem is of some interest in its own right, we will give additional motivation in Section 5.5 where we observe that certain conjectures for CPT maps with $d_1 = d_2$ can be reduced to case of the channels in the closure of extreme points with $d_1 \geq d_2$.

2 Convex decompositions of CPT maps or A block matrix generalization of Horn's lemma

Based on joint work with K. Audenaert

Since the set of CPT map $\Phi : M_{d_1} \mapsto M_{d_2}$ is convex, it can be written as a convex combination of extreme maps, and one expects that $d_1^2(d_2^2-1)$ will suffice. For maps on qubits, it was shown in [44] that if all maps in $\overline{\mathcal{E}(d_1,d_2)}$ are permitted, then only two are needed and they can be chosen so that the weights are even. This result generalizes to any CPT map with qubit output, i.e., for $\Phi : M_d \mapsto M_2$ one can write

$$\Phi = \tfrac{1}{2}(\Phi_1 + \Phi_2) \tag{4}$$

where Φ_1 and Φ_2 have Choi rank $\leq d$. We conjecture that this result extends to arbitrary CPT maps.

Conjecture 2. (Audenaert-Ruskai) *Let $\Phi : M_{d_1} \mapsto M_{d_2}$ be a CPT map. One can find d_2 CPT maps Φ_m with Choi rank at most d_2 such that*

$$\Phi = \sum_{m=1}^{d_2} \tfrac{1}{d_2}\Phi_m. \tag{5}$$

The adjoint or dual of a CPT map is a unital CP map and it is useful to restate the conjecture in this form.

Conjecture 3. *Let $\Phi : M_{d_2} \mapsto M_{d_1}$ be a CP map with $\Phi(I_2) = I_1$. One can find d_2 unital CP maps Φ_m with Choi rank at most d_1 such that*

$$\Phi = \sum_{m=1}^{d_2} \tfrac{1}{d_2}\Phi_m. \tag{6}$$

In this form, the conjecture can be viewed as a statement about block matrices, and it is useful to restate it explicitly in that form.

Conjecture 4. *Let $\mathbf{A}$ be a d_1d_2 positive semi-definite matrix consisting of $d_2 \times d_2$ blocks A_{jk} each of size $d_1 \times d_1$, with $\sum_j A_{jj} = M$. Then one can find d_2 block matrices $\mathbf{B}_m$, each of rank at most d_1, such that $\sum_j B_{jj} = M$, and*

$$\mathbf{A} = \sum_{m=1}^{d_2} \tfrac{1}{d_2}\,\mathbf{B}_m \tag{7}$$

If Conjecture 4 holds, then Conjecture 3 (and hence Conjecture 2) follows immediately. One need only let $\mathbf{A} = \Phi(|\beta\rangle\langle\beta|)$ be the Choi matrix of Φ for which $M = \frac{1}{d_2} I_{d_2}$. It would suffice to prove Conjecture 5 for the case $M = I_{d_2}$. The general case then follows by multiplying on the right and left by the matrix $\frac{1}{\sqrt{d_2}}\sqrt{M} \otimes I_{d_2}$. (May be some subtleties if M is non-singular.)

For $d_1 = 1$, Conjecture 4 is a consequence of Horn's Lemma[1] [23, 24] which says that a necessary and sufficient condition for the existence of a positive semi-definite matrix with eigenvalues λ_k and diagonal elements a_{kk} is that λ_k majorizes a_{kk}.

Corollary 2. *Let A be a $d \times d$ positive semi-definite matrix with $\operatorname{Tr} A = 1$. Then there are d normalized vectors $\mathbf{x}_m$ such that*

$$A = \sum_{m=1}^{d} \tfrac{1}{d} \mathbf{x}_m \mathbf{x}_m^\dagger \tag{8}$$

Proof: Note that any set of non-negative eigenvalues λ_k with $\sum_k \lambda_k = 1$ majorizes the vector $(\frac{1}{d}, \frac{1}{d}, \ldots, \frac{1}{d})$. Therefore, by Horn's lemma, one can find a unitary U and a self-adjoint matrix B such that $A = UB^2U^\dagger$ and the diagonal elements of B^2 are all $\frac{1}{d}$. (In fact, U, B can be chosen to have real elements.) Write $U = \sum_k \mathbf{u}_k \mathbf{e}_k^\dagger$ where $\mathbf{u}_k$ denotes the k-th column of U and $\mathbf{e}_k$ the standards basis. Let $\mathbf{x}_m = \sqrt{d} \sum_j \mathbf{u}_j b_{jm}$. Then

$$\begin{aligned} A &= \sum_{jk} \mathbf{u}_j \langle \mathbf{e}_j B^2 \mathbf{e}_k \rangle \mathbf{u}_k^\dagger \\ &= \sum_{jk} \sum_m \mathbf{u}_j \langle \mathbf{e}_j B \mathbf{e}_m \rangle \langle \mathbf{e}_m, B \mathbf{e}_k \rangle \mathbf{u}_k^\dagger \\ &= \sum_m \tfrac{1}{d} \mathbf{x}_m \mathbf{x}_m^\dagger \end{aligned} \tag{9}$$

and, since the columns of a unitary matrix are orthonormal,

$$\begin{aligned} \|\mathbf{x}_m\|^2 &= d \sum_{jk} \mathbf{u}_j^\dagger \overline{b}_{jm} b_{km} \mathbf{u}_k = d \sum_{jk} \overline{b}_{jm} b_{km} \mathbf{u}_j^\dagger \mathbf{u}_k \\ &= \sum_{jk} \delta_{jk} \overline{b}_{jm} b_{km} = d(B^2)_{mm} = d\tfrac{1}{d} = 1. \qquad \textbf{QED} \end{aligned} \tag{10}$$

This suggests that we restate the conjecture (7) using vectors of block matrices of the form $\mathbf{X}_m^\dagger = \begin{pmatrix} X_{1m}^\dagger & X_{2m}^\dagger & \ldots & X_{d_2 m}^\dagger \end{pmatrix}$ with each block $d_1 \times d_1$.

[1] See Theorem 4.3.32 of [24]. Note that [23] is by Alfred Horn, but that [24] is co-authored by Roger A. Horn.

Conjecture 5. *Let* $\mathbf{A}$ *be a* $d_1 d_2$ *positive semi-definite matrix consisting of* $d_2 \times d_2$ *blocks* A_{jk} *each of size* $d_1 \times d_1$*, with* $\sum_j A_{jj} = M$*. Then one can find* d_2 *vectors* $\mathbf{X}_m$ *composed of* d_2 *blocks* X_{jm} *of size* $d_1 \times d_1$ *such that*

$$\mathbf{A} = \sum_{m=1}^{d_2} \tfrac{1}{d_2} \mathbf{X}_m \mathbf{X}_m^\dagger, \quad \textit{and} \tag{11}$$

$$\sum_k X_{km} X_{km}^\dagger = M \qquad \forall\ m \tag{12}$$

There is no loss of generality in replacing B_m by $\mathbf{X}_m \mathbf{X}_m^\dagger$ with $\mathbf{X}_m$ of the above form. If X is $d_1 d_2 \times d_1 d_2$ with rank d_1, then by the SVD it can be written as $X = UDV^\dagger$ with U, V unitary and D diagonal with $d_{jj} = 0$ for $j > d$. If $\widetilde{D}$ retains only the first d_1 columns of D, then $\widetilde{X} = U\widetilde{D}$ has the desired form and $\widetilde{X}\widetilde{X}^\dagger = XX^\dagger$. thus, Conjecture 5 is clearly a generalization of Horn's lemma to block matrices.

When $d_2 = 2$, the argument in [44] (due to S. Szarek) is easily extended to give a proof of Conjecture 4 . Then $\mathbf{A} > 0$ is equivalent to

$$\mathbf{A} = \begin{pmatrix} \sqrt{A_{11}} & 0 \\ 0 & \sqrt{A_{22}} \end{pmatrix} \begin{pmatrix} I & W \\ W^\dagger & I \end{pmatrix} \begin{pmatrix} \sqrt{A_{11}} & 0 \\ 0 & \sqrt{A_{22}} \end{pmatrix} \tag{13}$$

with W a contraction. Write the SVD of W as

$$\begin{aligned} W &= U \begin{pmatrix} \cos\theta_1 & 0 & 0 & \dots & 0 \\ 0 & \cos\theta_2 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & \cos\theta_d \end{pmatrix} V^\dagger \\ &= \tfrac{1}{2} U \begin{pmatrix} e^{i\theta_1} & 0 & 0 & \dots & 0 \\ 0 & e^{i\theta_2} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & e^{i\theta_d} \end{pmatrix} V^\dagger + \tfrac{1}{2} U \begin{pmatrix} e^{-i\theta_1} & 0 & 0 & \dots & 0 \\ 0 & e^{-i\theta_2} & 0 & \dots & 0 \\ \vdots & 0 & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & e^{-i\theta_d} \end{pmatrix} V^\dagger \\ &= \tfrac{1}{2}(W_1 + W_2) \end{aligned} \tag{14}$$

with W_1 and W_2 unitary. When W is a $d_1 \times d_1$ unitary, $\begin{pmatrix} I & W \\ W^\dagger & I \end{pmatrix}$ has rank d_1. Therefore, substituting (14) into (13) shows that $\mathbf{A}$ is the midpoint of two matrices with rank at most d_1 and the same blocks on the diagonal as $\mathbf{A}$.

This argument suggests that one might strengthen the conjecture to require that each $\mathbf{B}_m$ have the same diagonal blocks as $\mathbf{A}$. However, this does not appear to hold

in the limiting case $d_1 = 1$ with $d_2 > 2$. In the proof of Corollary 2, it is tempting to replace B by $C = BV$ with V unitary. However, in (10) we would obtain $(C^\dagger C)_{mm}$ which, unlike $CC^\dagger$ need not have diagonal elements $\frac{1}{d}$.

The original proof of Horn's lemma used a complicated induction argument based on the properties of augmenting a matrix by a row and column. Since we know that (11) holds when $d_2 = 2$ or $d_1 = 1$, we have the starting points for a (probably non-trivial) double induction argument. Although Audenaert has found extensive numerical evidence for the validity of Conjectures 2-5, a proof seems to be elusive.

3 Generalized depolarized channels

3.1 Depolarized Werner-Holevo channels

The Werner-Holevo channel $\mathcal{W}(\rho) = \frac{1}{d-1}\big((\mathrm{Tr}\,\rho)\, I - \rho^T\big)$ has been extensively studied, especially in connection with the conjectured mutliplicativity of the maximal output p-norm, defined as $\nu_p(\Phi) = \sup_\rho \|\Phi(\rho)\|_p$. For $d = 3$, the maximal output p-norm is not multiplicative for $p > 4.79$. However, it is known that $\nu_p(\mathcal{W} \otimes (\mathcal{W}) = [\nu_p(\mathcal{W})]^2$ for $1 \leq p \leq 2$. For larger d one obtains a counter-example to multiplicativity only for correspondingly large p. In fact, it has been argued [19] that for $d > 2^p$ the WH channel is multiplicative.

$\mathcal{W}$ maps any pure state $|\psi\rangle\langle\psi|$ to $\frac{1}{d-1}E$ with $E = I - |\psi\rangle\langle\psi|$. Therefore, when d is large, $\mathcal{W}$ behaves much like the completely noisy map (although it is never EB). It is natural to consider channels of the form

$$\Phi_x = x\mathcal{I} + (1-x)\mathcal{W} \tag{15}$$

and ask if they also satisfy the multiplicativity conjecture (24) for $1 \leq p \leq 2$. Channels of the form (15) were considered by Ritter [42] in a different context.

Problem 6. *Show that the channel $\Phi_x = x\mathcal{I} + (1-x)\mathcal{W}$ satisfies the multiplicativity property $\nu_p(\Phi_x) \otimes (\Phi_x) = [\nu_p(\Phi_x)]^2$ for $1 \leq p \leq 2$.*

When $d = 3$ and $x = \frac{1}{3}$, the channel (15) becomes

$$\Phi_{1/3}(\rho) = \tfrac{1}{3}\big(I + \rho - \rho^T\big) \tag{16}$$

which has many interesting properties. It seems to have been first considered by Fuchs, Shor and Smolin, who published only an oblique remark at the end of [16]. They wrote it in a very different form, which is also given in [28]. Let $|1\rangle, |2\rangle, |3\rangle$ be

an orthonormal basis for $\mathbf{C}_3$ and define

$$\begin{aligned}
|\psi_0\rangle &= 3^{-1/2}\big(|1\rangle + |2\rangle + |3\rangle\big) \\
|\psi_1\rangle &= 3^{-1/2}\big(|1\rangle - |2\rangle - |3\rangle\big) \\
|\psi_2\rangle &= 3^{-1/2}\big(|1\rangle - |2\rangle + |3\rangle\big) \\
|\psi_3\rangle &= 3^{-1/2}\big(|1\rangle + |2\rangle - |3\rangle\big).
\end{aligned}$$

Now let Ψ be the channel whose Kraus operators are $\frac{\sqrt{3}}{2}|\psi_k\rangle\langle\psi_k|$ for $k = 0, 1, 2, 3$. This channel has the following properties:

1. $\Psi = \Phi_{1/3} = \frac{1}{3}\mathcal{I} + \frac{2}{3}\mathcal{W}$. Although this is not obvious, it is easily verified and implies (16). Thus, Ψ maps every real density matrix to the maximally mixed state.

2. Ψ is unital and the Holevo capacity satisfies

$$C_{\mathrm{Hv}}(\Phi) = \log 3 - S_{\min}(\Phi) \tag{17}$$

   but requires 6 (non-orthogonal) input states to achieve this capacity. It is not hard to see that $S_{\min}(\Phi)$ is achieved on inputs which are permutations of $(1, \pm i, 0)^T$.

3. Ψ is an extreme point of the EB channels which is neither CQ nor an extreme point of the CPT maps [28].

A solution of Problem 6 in the case $p = 2$ was recently reported by Michalakis [40].

3.2 Further generalizations of depolarization

In [51] channels $\mathcal{M}_\epsilon$ which whose output is always close to a maximally mixed state in the sense $\|\Phi(\rho) - \frac{1}{d}I\| < \epsilon$ play an important role. It seems natural to define a polarization of such channels

$$\Phi_{x,\epsilon} = x\mathcal{I} + (1-x)\mathcal{M}_\epsilon \tag{18}$$

For x close to 1, one explects multiplicativity to holds, and it is natural to ask several questions.

Problem 7. *Does $\Phi_{x,\epsilon}$ satisy* (24) *for $1 \le p \le 2$? For sufficiently small ϵ?*
If not, for what values of x and/or p does (24) *holds and how do they depend on ϵ?*

4 Random sub-unitary channels

We now introduce a class of extreme points motivated by the WH channel.

The Kraus operators for the WH channels with $d = 3$ can be written as

$$A_k = \tfrac{1}{2} X^k \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad k = 0, 1, 2 \tag{19}$$

where X is the shift operator $X|e_j\rangle = |e_{j+1}\rangle$. This suggests a natural generalization to channels with Kraus operators

$$A_k = \tfrac{1}{2} X^k \begin{pmatrix} u_{11} & u_{12} & 0 \\ u_{21} & u_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} = \tfrac{1}{2} X^k \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, 2 \tag{20}$$

with u_{jk} the elements of a 2×2 unitary U. The choice $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ does not give a counterexample to (24), although the effect of a tensor product on a maximally entangled state is the same as the WH channel. This is because changing -1 to $+1$ allows a "purer" optimal output for a single use of the channel; to be precise, for $+1$ the input $\frac{1}{\sqrt{3}}(1, 1, 1)$ yields an output with eigenvalues $\frac{2}{3}, \frac{1}{6}, \frac{1}{6}$ as compared to eigenvalues $\frac{1}{2}, \frac{1}{2}, 0$ for -1.

By contrast, the standard generalization of the WH channel to $d > 3$ involves $\binom{d}{2}$ choices of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ as the only non-zero block of a $d \times d$ matrix. It would seem natural to study channels with d Kraus operators of the form

$$\tfrac{1}{d-1} X^k \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, \ldots d-1. \tag{21}$$

where U is a $d-1 \times d-1$ unitary matrix. Such channels are generically extreme and always in the closure $\overline{\mathcal{E}(d, d)}$. Limited attempts to find new counter-examples of this type have found similar behavior to changing $+1$ to -1; they have outputs which are "too pure" for a single use of the channel.

Nevertheless, channels with Kraus operators of the form (21) have interesting properties that makes them worth further study. Moreover, it is not necessary to use the same U in every Kraus operator. One can choose

$$A_k = \tfrac{1}{d-1} X^k \begin{pmatrix} U_k & 0 \\ 0 & 0 \end{pmatrix} \qquad k = 0, 1, \ldots d-1. \tag{22}$$

with U_k any set of unitaries in M_{d-1}. With a few exceptions, channels whose Kraus operators have the form (22) are extreme points of the CPT maps on M_d, and are always in $\overline{\mathcal{E}}(d,d)$.

The WH channel gives a counter-example to multiplicativity for large p because maximally entangled states have outputs whose p-norms are relative maxima of $\|(\mathcal{W}\otimes\mathcal{W})(\rho)\|_p$, Nathanson [41] has shown analytically that for any p the output of any maximally entangled state gives a critical point, but Shor has found numerical evidence [49] that this is a relative maximum only for $p \geq 3$. This suggests that one look at other random sub-unitary channels.

Problem 8. *Let Φ be a channel with Kraus operators of the form* (22)*. Does the set of relative maxima of $\|(\Phi\otimes\Phi)(\rho)\|_p$ always include outputs whose input is maximally entangled? If not, for what p and under what circumstances do maximally entangled inputs yield outputs which are relative maxima?*

Despite the failure of Ruskai's very limited attempt to find new counter-examples of this type for $d = 4, 5$, more extensive numerical investigations, perhaps with different, randomly chosen, U_k, could be worthwhile. Further suggestions about numerical searches are given in Section 5.3. Even a negative result could provide some insight.

Problem 9. *Search for new counterexamples to* (24) *with Φ a channel with Kraus operators of the form* (22)*.*

In addition to looking at the optimal output purity of these channels, one can also ask about their coherent information and quantum capacity.

Problem 10. *What are the properties of the coherent information of random sub-unitary channels? When are they degradable? When is their coherent information additive?*

Remark: (added 11 August 2007). There has been recent interest in the question of multiplicativity of minimal output rank [22, 10]. For $d = 4$, the sub-unitary channel Φ with 3×3 unitary operators corresponding to the permutations $(123), (134), (142), (243)$ has minimal output rank 3. The channel $\Phi\otimes\Phi$ acting on a maximally entangled state has output rank 10, which does not give a violation. However, the behavior of this channel suggests that numerical investigations of similar examples for somewhat higher d might be worth investigating for counter-examples to the multplicativity question for $p < 1$ as discussed further in Section 5.6.

5 Additivity and multiplicativity conjectures

5.1 Prelude

Soon after the 14 June 2007 version of this manuscript was posted on the BIRS web site, counter-examples were found to the multiplicativity conjectures for all $p > 1$ [51, 21]. Nevertheless, the additivity conjectures and many related questions remain open. Therefore, I have made only minor changes to most of this section and discuss the recent developments and new questions they raise in Section 5.6. Moreover, these existence of counter-examples also raises new questions. Thus, there may still be value in some of the old material, such as Theorem 3.

5.2 The conjectures

One of the outstanding open problems in quantum information is the additivity of minimal output entropy, i.e.,

$$S_{\min}(\Phi \otimes \Omega) = S_{\min}(\Phi) + S_{\min}(\Omega) \tag{23}$$

where $S_{\min}(\Phi) = \inf_{\gamma} S[\Phi(\gamma)$ where the infimum is taken over the set of density matrices γ so that $\gamma > 0$ and $\operatorname{Tr}\gamma = 1$. This conjecture has considerable importance because Shor [48] has shown that it is globablly equivalent to the conjectured additivity of Holevo capacity and several conjectures about entanglement of formation. Shirokov [45, 46] has even shown that additivity in all finite dimensions would have implications for certain infinite dimensional channels. Fukuda [17] and Wolf [18] have given some additional reductions.

Amosov, Holevo and Werner [4] realized that (23) would follow if the following conjecture holds for $p \in (1, 1+\epsilon)$ with $\epsilon > 0$.

$$\nu_p(\Phi \otimes \Omega) = \nu_p(\Phi)\nu_p(\Omega) \tag{24}$$

where $\nu_p(\Phi) = \inf_{\gamma} \|\Phi(\gamma)\|_p$. Although, Werner and Holevo [50] found a counter-example to (24) for large p, it seems reasonable to conjecture that (24) holds for $1 \leq p \leq 2$. This conjecture can be rewritten [1, 21] using the Renyi entropy, which is essentially the difference quotient at $p = 1$ of $p \log \|\gamma\|_p$, i.e.,

$$S^p(\gamma) \equiv \tfrac{1}{p-1} \log \operatorname{Tr}\gamma^p. \tag{25}$$

This expression is meaningful for any $p \geq 0$ with the understanding that $S^0(\gamma) = \log \operatorname{rank}(\gamma)$ and $S^1(\gamma)$ the usual von Neumann entropy. Then (24) can be rewritten as

$$S^p_{\min}(\Phi \otimes \Omega) = S^p_{\min}(\Phi) + S^p_{\min}(\Omega) \tag{26}$$

with $S^p_{\min}(\Phi) = \inf_{\gamma} S^p[\Phi(\gamma)]$.

5.3 Finding counter-examples

It is surprising that no counter-example to (24) is known other than the WH channel [50] and very small perturbations of it. Moreover, one has no counter-example for $p < 4.79$. Some authors [36] have conjectured that (24) holds for $1 \leq p \leq 2$. If so, one would expect to have a family of counter-examples for $p > 2$. More generally, if the conjecture holds for $1 < p < p_c$, one would expect to find counter-examples for $p > p_c$ arbitrarily close to to p_c.

Problem 11. *Find more counter-examples to* (24)*. Do they suggest that the conjecture holds for* $1 \leq p \leq 2$*?*

One strategy for finding new counter-examples, is to first search numerically for additional counter-examples for very *large* p using Theorem 3 below. For any new examples found, study the critical points numerically and determine the values of p for which one ceases to have a counter-example and for which one ceases to even have a relative maximum for entangled inputs. Perhaps this will give some insight into the nature of counter-examples that will allow one to find some in the range $2 < p < 4.79$. The reason for starting with large p is that the algorithm for finding relative maxima using Theorem 3 is faster and more robust for large p.

The following extension of Shor's algorithm for finding relative minima of the minimal ouput entropy (see Appendix of [12]) was proved by C. King using Hölder's inequality in the case $p > 1$. We present a different proof, valid for all $p > 0$. We first note that Shor's argument uses the positivity of relative entropy, which is based on Klein's inequality, using the more general form in Ruelle [43] for convex functions

$$\operatorname{Tr} f(A) - \operatorname{Tr} f(B) \geq \operatorname{Tr} (A - B) f'(B) \tag{27}$$

where A, B are positive semi-definite matrices. Since the function $f(x) = x^p$ with $p > 1$ is convex, this gives

$$\operatorname{Tr} A^p - \operatorname{Tr} B^p \geq p(A - B)B^{p-1}. \tag{28}$$

Theorem 3. *Let* $p > 0$ *and* Ω *a CPT map with* $\widehat{\Omega}$ *its adjoint with respect to the Hilbert-Schmidt inner product. For fixed* $\gamma = |\psi_0\rangle\langle\psi_0|$ *and* $\left\{ \begin{array}{c} p < 1 \\ p > 1 \end{array} \right\}$*, let* ψ_1 *be the eigenvector corresponding to the* $\left\{ \begin{array}{c} \textit{smallest} \\ \textit{largest} \end{array} \right\}$ *eigenvalue of* $\widehat{\Omega}\Big[\Omega(\gamma)\Big]^{p-1}$*. Then* $\|\Omega(|\psi_1\rangle\langle\psi_1|)\|_p \left\{ \begin{array}{c} \leq \\ \geq \end{array} \right\} \|\Omega(|\psi_0\rangle\langle\psi_0|)\|_p$

Proof: First consider $p > 1$. The max min principle implies that

$$\langle\psi_1 \widehat{\Omega}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^{p-1}\psi\rangle \geq \langle\psi_0 \widehat{\Omega}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big]^{p-1}\psi_0\rangle. \tag{29}$$

which can be rewritten as

$$\operatorname{Tr}\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)]^{p-1} \geq \operatorname{Tr}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)]^p \tag{30}$$

Then using (28) with $A = \Omega\big(|\psi_1\rangle\langle\psi_1|\big), B = \Omega\big(|\psi_0\rangle\langle\psi_0|\big)$ gives

$$\begin{aligned}\operatorname{Tr}\big[\Omega\big(|\psi_1\rangle\langle\psi_1|\big)]^p &- \operatorname{Tr}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)]^p \\ &\geq\ p\Big(\operatorname{Tr}\Omega\big(|\psi_0\rangle\langle\psi_0|\big)\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)]^{p-1} - \operatorname{Tr}\big[\Omega\big(|\psi_0\rangle\langle\psi_0|\big)]^p\Big)\ \geq\ 0.\end{aligned}$$

where the last inequality follows from (30). Taking p-th roots gives the desired result.

For $0 < p < 1$, the function $f(x) = x^p$ is concave and the same argument goes through with all inequalities reversed. **QED**

Using this result repeatedly with ψ_{k+1} the eigenvector corresponding to the largest eigenvalue of $\widehat{\Omega}\big[\Omega(|\psi_k\rangle\langle\psi_k|)\big]^{p-1}$, gives a sequence converging to a relative maximum of $\|\Phi(\gamma)\|_p$.

5.4 Specific multiplicativity problems

Proving multiplicativity of the depolarized WH channel was already mentioned in Section 3.1. Recently, Michalakis reported [40] a proof for $p = 2$. In view of the fact that some depolarized WH channels do *not* satisfy the very unappealing conditions based on positive entries used in [36, 35], the approach in [40] may be useful in investigating other classes of channels.

Problem 12. *For what classes of channels can* (24) *be proved for* $p = 2$.

In [41], a class of channels is defined using mutually unbiased bases, with each basis defining an"axis". These channels can be described by "multipliers" in a manner similar to unital qubits channels, and when all multipliers are non-negative they seem very similar. However, even for a single use of a channel some questions are open. See Conjecture 9 of [41]. If this conjecture is true, then additivity and multiplicativity can be reduced to the case of "maximally squashed" channels which are generalizations of the two-Pauli qubit channel.

Problem 13. *Find a proof of multiplicativity for the two-Pauli qubit channel, which does not use unitary equivalence to channels with negative multipliers.*

Since most recent investigations of additivity (23) have approached the problem through the multiplicativity conjecture, it is worth noting that Amosov has obtained some results [2, 3] in special cases by a very different approach using the montonicity of relative entropy. Also recall that Shor's proof [47] of additivity for entanglement breaking channels used entropy arguments based on strong subadditivity. Although these basic properties of entropy are unlikely to suffice for more general channels, they do demonstrate that multiplicativity is not the only route to additivity.

5.5 Reduction to extreme points

Although the set of CPT maps $\Phi : M_{d_A} \mapsto M_{d_B}$ is convex, one can not use convexity to reduce additivity or multiplicativity to that of the extreme channels. One can, however, use the notion of complementary channels to obtain a kind of global reduction to extreme channels.

The notion of complementary channel was first used in quantum information theory in a paper of Devetak and Shor [15] and then studied in detail in [25, 34]. This concept is equivalent to one obtained much earlier in a more general context by Arveson [6] in the section on lifting commutants. (See the appendxi to [11] for details.)

If $\Phi : M_{d_A} \mapsto M_{d_B}$, its complement is a CPT map $\Phi^C : M_{d_A} \mapsto M_{d_E}$ with Choi rank d_B. Whenever $d_B \leq d_A$, the complement belongs to the class of generalized extreme points. Therefore, the results in [25, 34] imply that if we can prove additivity for all maps in $\overline{\mathcal{E}(d_1, d_2)}$, it will hold for all CPT maps with $d_B \leq d_A$. Moreover, Shor's channel extensions [48] used to establish the equivalence of various additivity results increase only d_A. Hence, additivity for tensor products of all extreme maps with $d_A \geq d_B$ would imply it for all maps with $d_A = d_B$.

Problem 14. *Identify new classes of extreme CPT maps for which additivity and/or multiplicativity can be proved.*

Problem 15. *Can one prove* (24) *for random sub-unitary channels, at least for* $p = 2$. *If not, do these channels provide additional counter-example?*

5.6 New counter-examples and their implications

Very recently (July, 2007), Winter [51] solved Problem 11 by showing the existence of counter-examples for all $p > 2$. Moreover, his approach failed at $p = 2$, which seemed to provide support for the validity of multiplicativity in the range $1 < p \leq 2$. But soon after, Hayden [21] showed that there exist counter-examples for $1 < p < 2$ and this was extended to $p = 2$ by Winter.

Hayden [21] also provided an analysis of his examples that indicates that (23) still holds for these channels and suggested that one try to establish additivity by proving (26) for $p < 1$. King [32] announced that his arguments for multplicativity of entanglement breaking channels [31] extend to $0 < p < 1$. He also observed that the proofs of (24) for unital qubit channels [29] and depolarizing channels, [30] were basd on the following inequality of Lieb-Thirring [38]

$$\mathrm{Tr}\,(AB)^p \leq \mathrm{Tr}\,A^p B^p \tag{31}$$

for $p \geq 1$ and A, B positive semi-definite. Since Araki [5] has shown that the reverse inequality is valid for $0 \leq p < 1$, his results for unital qubit and for general depolarizing channels should also readily extend to $0 < p < 1$.

However, hopes for validity of (26) for $0 \leq p < 1$ were shattered when Harrow, Leung and Winter [22] announced counter-examples for $p = 0$. These examples differ from those for $p > 1$. But they are also based on the results and methods introduced in [22] on the prevalence of nearly maximally entangled states in large dimension. It seems only a matter of time until counter-examples are shown to exists for any $p \in (0, 1)$.

Nevertheless, it is worth emphasizing that none of the counter-examples are uniform in p, i.e., as p approaches 1 the counter-example fails and a new one must be found with dimension increasing to infinity as $p \mapsto 1$. Thus, the following much weaker forms of (24) and (26) are not excluded. The validity of any one of the four conjectures which follow would imply that (23) and all the equivalent additivity conjectures hold.

Conjecture 16. *For any fixed pair of channels Φ, Ω, there is a $p^* > 0$ such that either*

(i) $p^* < 1$ and (26) holds for all $p \in (p^*, 1)$, or

(ii) $p^* > 1$ and (26) holds for all $p \in (1, p^*)$.

Conjecture 17. *For any fixed integer d there is a $p_d > 0$ such that either*

(i) $p_d < 1$ and (26) holds whenever $\Phi : M_{d'} \mapsto M_{d'}$, $d' \leq d$ and $p_d < p < 1$, or

(ii) $p_d > 1$ and (26) holds whenever $\Phi : M_{d'} \mapsto M_{d'}$, $d' \leq d$ and $1 < p < p_d$

For brevity we stated the conjectures above in pairs, but in each case the form (i) or (ii) is a separate conjecture.

If the additivity conjectures are true, proving either of the above conjectures seems less likely than proving (23) directly. Moreover, Shor's channel extension methods give global equivalences which require consideration of CPT maps $\Phi : M_d \mapsto M_{d'}$ with $d \geq d'$. Thus one should extend the above conjectures to include the case $d > d'$. However, we preferred to state them in the simpler form.

Although based on similar techniques, the actual form of the channels giving counter-examples for $p > 1$ and $p < 1$ seems to be different. This leads to

Problem 18. *Does there exists a channel or pair of channels that violates (26) for both some $p_1 > 1$ and some p_2 with $0 < p_2 < 1$?*

If the answer is negative, then (23) holds because one can always approach $p = 1$ from either above or below. This seems a rather unlikely approach to proving (23), but thinking about it might provde some insight about this additivity conjecture.

The need for large dimensions to find counter-examples raises the question of whether channels for smaller dimensions might satisfy (26) for two copies, but not for a large number.

Problem 19. *Find an example of a channel Φ, an integer m and a $p > 0$ such that $S^p_{\min}(\Phi^{\otimes n}) = nS^p_{\min}(\Phi)$ for $n < m$ but $S^p_{\min}(\Phi^{\otimes m}) < mS^p_{\min}(\Phi)$.*

Current results do not even exclude the possibility that a non-unital qubit channel violates additivity for $\Phi^{\otimes m}$. Curiously, (24) has only been proved [33] for non-unital qubit maps when $p = 2$ or $p \geq 4$.

All of the counter-example results obtained thus far are given as existence theorems. It would be useful to have explicit counter-examples.

Problem 20. *Find explicit examples of channels which violate* (24) *for $p \neq 1$.*

In the case of Winter's examples [51] for $p > 2$, one can show that the so-called CB entropy [14] is positive and the coherent information is negative. (When the coherent information is achieved with a maximally entangled state, the CB entropy and coherent information differ only by a sign change.) Thus, although these channels are not entanglement breaking (EB), they preserve very little entanglement – not even enough to allow one to recover a single EPR pair in the sense of Horodecki, Oppenheim and Winter [27, **?**]. The WH counter-examples also have positive CB entropy except for $d = 3$ when it is exactly zero. Thus, for $p > 2$, the known counter-examples suggest that entanglement does not enhance the optimal output purity until the channel is very close to EB. One can ask if this holds for other examples, particularly those for $p < 2$.

Problem 21. *Do all counter-examples to multiplicativity* (24) *have non-negative CB entropy and/or zero coherent information?*

Finally, one can ask whether or not additivity itself holds. It is worth recalling that the equivalent capacity conjecture was stated in [7] in a form that seemed to favor superadditivity. Thus, the ultimate open question is still.

Problem 22. *Prove* (23) *or find a counter-example.*

6 Coherent information and degradability

In [11] on degradability several questions were raised of which we mention one.

Problem 23. *Find pairs of channels $\mathcal{M}, \mathcal{N}$ that are mutually degradable in the sense that there exist channels $\mathcal{X}, \mathcal{Y}$ such that*

$$\mathcal{X} \circ \mathcal{M} = \mathcal{N}^C \qquad \mathcal{Y} \circ \mathcal{N} = \mathcal{M}^C. \tag{32}$$

At present, the only examples known have $\mathcal{M} = \mathcal{I}$ which is universal in the sense that $\mathcal{N}$ is arbitrary. This works because $\mathcal{I}$ is universally degradable and its complement Tr is a universal degrador. Can other examples be found? It may be that when $\mathcal{N}$ has Choi rank d^2, one must have $\mathcal{M} = \mathcal{I}$. Therefore, it seems worth looking for examples in which both have lower Choi-rank. It would be particularly interesting to find pairs in which both have Choi-rank d, but are not individually degradable.

7 Local invariants for N-representability

In the 1960's a variant of the quantum marginal problem known as N-representability attracted considerable interest. The question is to find necessary and sufficient conditions on a p-particle reduced density matrix $\rho_{1,2,\ldots t}$ in order that there exists an anti-symmetric (or symmetric for bosons) N-particle density matrix $\rho = \rho_{1,2\ldots N}$ such that $\mathrm{Tr}_{t+1,t+2,\ldots N}\rho_{1,2\ldots N} = \rho_{1,2,\ldots t}$. The pure N-representability problem, for which one requires that the preimage $\rho_{1,2\ldots N} = |\Psi\rangle\langle\Psi|$ come from an anti-symmetric (or symmetric) pure state $|\Psi\rangle$ is also of interest.

A full solution was found only to the mixed state problem for the one-particle density matrix, for which it is necessary and sufficient that the eigenvalues of ρ_1 are $\leq \frac{1}{N}$ when $\mathrm{Tr}\,\rho_1 = 1$. Other results were obtained for a few very special situations, and some reformulations were found. For the two-particle reduced density matrix, a collection of necessary inequalities were obtained, but little else was known. For over 30 years, there was very little progress until two recent breakthroughs. Klyachko [37] solved the pure state 1-representability problems. Liu, Christandl and Verstraete [39] showed that some version are QMA complete.

Although many open questions remain, we consider only one which may be amenable to quantum information theorists. As Coleman pointed out, N-representability must be independent of the 1-particle basis used to write the density matrix, i.e., the solution can be expressed in terms of what one might call local invariants. These are parameters which are invariant under transformations of the form $U \otimes U \otimes \ldots \otimes U = U^{\otimes p}$. For the 1-matrix, these are just unitary invariants, which are known to be the eigenvalues. For $p = 2$ the set of local invariants includes the eigenvalues, but must contain other parameters as well. Surprisingly, no complete set of local invariants in which N-representability conditions for the 2-matrix can be expressed is known.

Problem 24. *Find a minimal complete set of local invariants for an anti-symmetric (or symmetric)* 2*-particle density matrix.*

References

[1] R. Alicki and M. Fannes, "Note on multiple additivity of minimal entropy output of extreme $SU(d)$-covariant channels" *Open Systems and Information Dynamics* **11**, 339–342 (2004). quant-ph/0407033.

[2] G.G. Amosov, "On Weyl channels being covariant with respect to the maximum commutative group of unitaries" *J. Math. Phys.* **48**, 2104–2117 (2007). arXiv:quant-ph/0605177

[3] G.G. Amosov, "The strong superadditivity conjecture holds for the quantum depolarizing channel in any dimension" *Phys. Rev. A* **75**, 060304 (2007) arXiv:0707.1097

[4] G. G. Amosov, A. S. Holevo, and R. F. Werner, "On Some Additivity Problems in Quantum Information Theory", *Problems in Information Transmission*, **36**, 305–313 (2000). eprint math-ph/0003002

[5] H. Araki, "On an inequality of Lieb and Thirring" *Lett. in Math. Phys.* **19**, 167–170 (1990).

[6] W. Arveson, "Subalgebras of C*-Algebras" *Acta Math.* **123**, 141–224 (1969).

[7] C. H. Bennett, C. A. Fuchs and J. A. Smolin, "Entanglement-enhanced classical communication on a noisy quantum channel", *Quantum Communication, Computing and Measurement*, edited by O. Hirota, A. S. Holevo, and C. M. Caves (Plenum Press, NY, 1997), pages 79–88. (quant-ph/9611006)

[8] M-D Choi, "Completely Positive Linear Maps on Complex Matrices" *Lin. Alg. Appl.* **10**, 285–290 (1975).

[9] A.J. Coleman, "The structure of fermion density matrices" *Rev. Mod. Phys.* **35**, 668–687 (1958).

[10] T. S. Cubitt, A. Montanaro and A. Winter, "On the dimension of subspaces with bounded Schmidt rank" arXiv:0706.0705

[11] T. Cubbit, M.B. Ruskai and G. Smith, in preparation

[12] N. Datta and M.B. Ruskai, "Maximal output purity and capacity for asymmetric unital qudit channels" *J. Phys. A: Math. Gen.* **38**, 9785–9802 (2005). (quant-ph/0505048)

[13] N. Datta, M. Fukuda and A.S. Holevo, "Complementarity and additivity for covariant channels" *Quant. Info. Proc.* **5**, 179–207 (2006).

[14] I. Devetak, M. Junge, C. King, and M. B. Ruskai, "Multiplicativity of completely bounded p-norms implies a new additivity result" *Commun. Math. Phys.* **266**, 37–63 (2006). (quant-ph/0506196).

[15] I. Devetak and P. W. Shor "The capacity of a quantum channel for simultaneous transmission of classical and quantum information" *Commun. Math. Phys.* **256**, 287–303 (2005). quant-ph/0311131

[16] C. Fuchs, "Nonorthogonal quantum states maximize classical information capacity", *Phys. Rev. Lett.* **79**, 1162–1165 (1997).

[17] M. Fukuda, "Simplification of additivity conjecture in quantum information theory" arXiv:quant-ph/0608010

[18] M. Fukuda and M.M. Wolf, "Simplifying additivity problems using direct sum constructions" arXiv:0704.1092

[19] V. Giovannetti, S. Lloyd and M. B. Ruskai, "Conditions for multiplicativity of maximal l_p-norms of channels for fixed integer p", *J. Math. Phys.* **46**, 042105 (2005). quant-ph/0408103.

[20] A. Harrow, D. Leung and A. Winter, private communication

[21] Patrick Hayden "The maximal p-norm multiplicativity conjecture is false" arXiv:0707.3291

[22] P. Hayden. D. Leung and A. Winter, "Aspects of generic entanglement" *Commun. Math. Phys.* **265**, 95–117 (2007).

[23] A. Horn, "Doubly stochastic matrices and the diagonal of a rotation matrix" *Amer. J. Math.* **76**, 620–630(1954).

[24] R.A. Horn and C.R. Johnson, *Matrix Analysis* (Cambridge University Press, 1985).

[25] A. S. Holevo, "On complementary channels and the additivity problem" quant-ph/0509101 published as part of [13].

[26] M.Horodecki, J. Oppenheim and Andreas Winter "Partial quantum information" *Nature*, **436**, 673–676 (2005); posted as "Quantum information can be negative" quant-ph/0505062

[27] M.Horodecki, J. Oppenheim and Andreas Winter, "Quantum state merging and negative information" *Commun. Math. Phys.* **269**, 107–136 (2007).

[28] M.Horodecki, P. Shor, and M. B. Ruskai "Entanglement Breaking Channels" *Rev. Math. Phys* **15**, 629–641 (2003). (quant-ph/030203)

[29] C. King, "Additivity for unital qubit channels", *J. Math. Phys.* **43**, no. 10 4641–4653 (2002).

[30] C. King, "The capacity of the quantum depolarizing channel", *IEEE Trans. Inform. Theory* **49**, no. 1 221–229, (2003).

[31] C. King, "Maximal p-norms of entanglement breaking channels", *Quantum Information and Computation*, **3**, no. 2, 186–190 (2003).

[32] C. King, reported at the AMS-PTM meeting in Warsaw, Poland, 2 August 2007.

[33] C. King and N. Koldan "New multiplicativity results for qubit maps" arXiv:quant-ph/0512185

[34] C. King, K. Matsumoto, M. Nathanson and M. B. Ruskai, "Properties of Conjugate Channels with Applications to Additivity and Multiplicativity" (quant-ph/0509126.

[35] C. King, M. Nathanson and M. B. Ruskai, "Multiplicativity results for entrywise positive maps" *Lin. Alg. Appl.* **404**, 367–379 (2005). quant-ph/0409181.

[36] C.King and M. B. Ruskai, "Comments on multiplicativity of maximal p-norms when p = 2" in *Quantum Information, Statistics and Probability* ed. by O. Hirota, 102–114 (World Scientific, 2004) quant-ph/0401026.

[37] A. Klyachko, "Quantum marginal problem and N-representability" *Journal of Physics: Conf. Series* **36**, 72–86 (2006). quant-ph/0511102

[38] E. Lieb and W. Thirring, "Inequalities for the Moments of the Eigenvalues of the Schrödinger Hamiltonian and Their Relation to Sobolev Inequalities", in *Studies in Mathematical Physics*, E. Lieb, B. Simon, A. Wightman eds., pp. 269–303 (Princeton University Press, 1976). Reprinted in [**?**]

[39] Y.-K. Liu, M. Christandl, F. Verstraete "N-representability is QMA-complete" quant-ph/0609125

[40] Spyridon Michalakis, "Multiplicativity of the maximal output 2-norm for depolarized Werner-Holevo channels" arXiv:0707.1722

[41] M. Nathanson and M.B. Ruskai "Pauli Diagonal Channels Constant on Axes" *J. Phys. A: Math. Theor.* **40**, 8171–8204 (2007). quant-ph/0611106

[42] G. W. Ritter, "Quantum Channels and Representation Theory" *J. Math. Phys.* **46**, (2005) (quant-ph/0502153).

[43] D. Ruelle, *Statistical Mechanics* (Benjamin, 1969) Section 2.5.2.

[44] M. B. Ruskai, S. Szarek, E. Werner, "An analysis of completely positive trace-preserving maps M_2" *Lin. Alg. Appl.* **347**, 159 (2002).

[45] M.E. Shirokov "The Holevo capacity of infinite dimensional channels and the additivity problem" *Commun. Math. Phys.* **262**, 137–159 (2006). quant-ph/0408009

[46] M. E. Shirokov "The Convex Closure of the Output Entropy of Infinite Dimensional Channels and the Additivity Problem" quant-ph/0608090

[47] P. Shor, "Additivity of the classical capacity of entanglement-breaking quantum channels" *J. Math. Phys.* **43**, 4334–4340 (2002).

[48] P. W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory", *Commun. Math. Phys.* **246**, 453–472 (2004). quant-ph/0305035

[49] P. W. Shor, private communication. This result has been confirmed by M. Nathanson.

[50] R. F. Werner and A. S. Holevo, "Counterexample to an additivity conjecture for output purity of quantum channels", *J. Math. Phys.* **43**, 4353–4357 (2002).

[51] Andreas Winter, "The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$" arXiv:0707.0402

Entropic uncertainty relations for more than two observables

[1]*Contacts: Debbie Leung, wcleung@iqc.ca;*
Stephanie Wehner, wehner@cwi.nl;
Andreas Winter, a.j.winter@bris.ac.uk
(Dated: 4th March 2007)

Background. The uncertainty principle is one of the fundamental ideas of quantum mechanics. Since Heisenberg's uncertainty relations for canonically conjugate variables (formalised by Robertson for arbitrary observables), it has been one of the staples. This, and later, formulations are about the tradeoff between the "uncertainties" in the value of non-commuting observables on the same state preparation; in other words, they are comparing counterfactual situations.

Traditionally, the comparison is between variances of the observables, but it was eventually realised that other measures of "spread" of the distribution on measurement outcomes can be used. Arguably the universal such measure is the entropy of the distribution, and Białynicki-Birula and Mycielski [1] proved an entropic uncertainty relation for systems of n canonical pairs of position and momentum coordinates X_i and P_i:

$$H(X_1 \dots X_n|\varphi) + H(P_1 \dots P_n|\varphi) \geq n \log(e\pi),$$

where $H(Q_1 \dots Q_n|\varphi)$ refers to the (differential) Shannon entropy of the joint distribution of the coordinates $Q_1, \dots Q_n$ when measured on the state φ. In [1] it is shown that this relation implies the Heisenberg uncertainty relation.

After that, following initial work by Deutsch and in response to a conjecture by Karl Kraus, the following inequality was proved by Maassen and Uffink [2] for observables in finite dimension d with eigenbases $\mathcal{B}_j = \{|b_1^j\rangle, \dots, |b_d^j\rangle\}$ ($j = 1, 2$) and an arbitrary state φ:

$$H(\mathcal{B}_1|\varphi) + H(\mathcal{B}_2|\varphi) \geq -\log \max_{x,y} |\langle b_x^1|b_y^2\rangle|^2, \tag{1}$$

where $H(\mathcal{B}_j|\varphi) = H\left(\{|\langle b_x^j|\varphi\rangle|^2 : x = 1, \dots, d\}\right)$ is the Shannon entropy of measuring the state φ in basis $\mathcal{B}_j$. In particular, for mutually unbiased bases, i.e. when all the inner products on the right hand side above are equal to $1/d$, we obtain that the entropy sum is lower bounded by $\log d$. This is tight, as the example of $|\varphi\rangle = |b_x^j\rangle$ shows.

Note that in both cases we get a lower bound on the entropy sum of two non-commuting (and indeed non-coexistent) observables which is independent of the underlying state. This lower bound is not necessarily tight (as can be seen rather easily in the case of the general Maassen-Uffink inequality), but its usefulness lies in the fact that it is in terms of *very simple* geometric information of the relative position of the bases.

The problem. Traditionally, uncertainty relations were restricted to pairs of "conjugate" observables. But the finite-dimensional inequalities, culminating in the Maassen-Uffink one, show that it is really the property of mutual unbiasedness that makes for maximal uncertainty. Since this realisation, one could ask for the entropic uncertainty tradeoff between more than two observables. This may be physically interesting, since there exists in every dimension d a large number of mutually unbiased bases, up to $d + 1$ (see problem 13 on these pages).

In [3] it was shown that for k observables in $\mathbb{C}^d$, with eigenbases $\mathcal{B}_j = \{U_j|x\rangle : x = 1, \dots, d\}$, the expression

$$h(d; U_1, \dots, U_k) := \min_{\varphi} \frac{1}{k} \sum_{j=1}^{k} H(\mathcal{B}_j|\varphi)$$

has information-theoretic significance in the context of "information locking". Here, $H(\mathcal{B}_j|\varphi) = H\left(\{|\langle x|U_j^*|\varphi\rangle|^2 : x = 1, \ldots, d\}\right)$ is the Shannon entropy of the measurement of basis $\mathcal{B}_j$ on the state φ.

Note that always

$$0 \leq h(d; U_1, \ldots, U_k) \leq \left(1 - \frac{1}{k}\right) \log d, \tag{2}$$

and the problem of the entropic uncertainty relations at its most general is to find an expression for or at least a lower bound on $h(d; U_1, \ldots, U_k)$ in "simple" terms of the geometry of the set of bases $\mathcal{B}_j$.

In the applications as the cited one [3], one is interested in maximally unbiased observables, i.e., in

$$h(d; k) := \max_{U_1,\ldots,U_k} h(d; U_1, \ldots, U_k),$$

and a characterisation of the maximisers. Note that if there exist, in dimension d, k mutually unbiased bases, then by virtue of (1) and the above (2),

$$\frac{1}{2} \log d \leq h(d; k) \leq \left(1 - \frac{1}{k}\right) \log d,$$

and one would like to have a characterisation of the sets of unitaries attaining the maximum.

Seeing thus the scaling of $h(d; k)$ with $\log d$, and assuming an asymptotic viewpoint of large dimension, we consider finally the quantity

$$h(k) := \lim_{d\to\infty} \frac{1}{\log d} h(d; k)$$

[if the limit exists, otherwise take the lim inf], which depends now only on k. For example, $h(2) = 1/2$, and it is clear that

$$h(k + k') \geq \frac{k}{k + k'} h(k) + \frac{k'}{k + k'} h(k'),$$

but we don't know if $h(k)$ actually strictly grows with k. If so, does it approach the value $1 - 1/k$ suggested by the upper bound, or at least $1 - 1/f(k)$ with some growing function f of k?

Partial results. In [3] (see the eprint version) numerical work on three and more mutually unbiased bases in dimensions up to 29 is reported, which are consistent with a behaviour of $1 - O(1/k)$ of $h(k)$. The mutually unbiased bases are taken as a subset of the "stabiliser construction" MUBs in prime power dimension.

That this choice may be significant became obvious only with [4] where it was shown that in square prime power dimensions $d = p^{2\ell}$ there exist up to $k = p^\ell + 1$ MUBs with $h(d; U_1, \ldots, U_k) = \frac{1}{2} \log d$ [8]. Furthermore, in any square dimension $d = d_0^2$ a number $k = d^{1/14.8}$ of mutually unbiased bases with the same property can be found. This shows that mutual unbiasedness is not enough to characterise a large $h(d; U_1, \ldots, U_k)$. Indeed, Ambainis [5] has shown that any three bases from the "standard" mutually unbiased bases construction in prime power dimension, $h(d; U_1, U_2, U_3) = \left(\frac{1}{2} + o(1)\right) \log d$, for large dimension, and assuming the Generalised Riemann Hypothesis. Furthermore, for any $0 \leq \epsilon \leq 1/2$, there always exist $k = d^\epsilon$ many of these bases such that $h(d; U_1, \ldots, U_k) = \left(\frac{1}{2} + \epsilon + o(1)\right) \log d$.

On the other hand, it was shown in [6] that $k = (\log d)^4$ unitaries U_j randomly and independently chosen from the Haar measure have $h(d; U_1, \ldots, U_k) \geq \log d - O(1)$ with high probability, and for sufficiently large dimension d.

It should be noted that in the application to information locking, one is interested in a small number of bases; however, for a complete set of mutually unbiased bases in dimension d, Sanchez-Ruiz [7] has shown that $h(d; U_1, \ldots, U_{d+1}) \geq \log(d+1) - 1$.

---

[1] I. Białynicki-Birula, J. Mycielski, "Uncertainty Relations for Information Entropy in Wave Mechanics", Comm. Math. Phys. **44**, 129-132 (1975).

[2] H. Maassen, J. B. M. Uffink, "Generalized Entropic Uncertainty Relations", Phys. Rev. Lett. **60**(12), 1103-1106 (1988).

[3] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, B. M. Terhal, "Locking Classical Correlations in Quantum States", Phys. Rev. Lett. **92**(6). 067902 (2004); quant-ph/0303088.

[4] M. A. Ballester, S. Wehner, "Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases", Phys. Rev. A **75**, 022319 (2007); quant-ph/0606244.

[5] A. Ambainis, work to appear (dated October 2006).

[6] P. Hayden, D. W. Leung, P. W. Shor, A. Winter, "Randomizing quantum states: Constructions and applications", Comm. Math. Phys. **250**, 371-391 (2004).

[7] J. Sanchez-Ruiz, "Entropic uncertainty and certainty relations for complementary observables", Phys. Lett. A **173**, 233-239 (1993).

[8] And many more if one relaxes the condition of mutual unbiasedness to approximate unbiasedness, using the techniques of [6].

1. A Problem Posed By Vern I. Paulsen

Given an operator $T \in B(\mathcal{H})$ it's n**-th matrix range** is the set

$$W^n(T) = \{\Phi(T) : \Phi : B(\mathcal{H}) \to M_n \text{ is completely positive and unital}\}.$$

This problem is concerned with how well knowledge of matrix ranges for small values determine them for larger values.

Let

$$\mathcal{S}_{n,j}(T) = \{A \in M_n : W^j(A) \subseteq W^j(T)\}.$$

Given $A \in M_n$ and $\mathcal{W} \subseteq M_n$, we let $d(A, \mathcal{W}) = \sup\{\|A - W\| : W \in \mathcal{W}\}$ denote the usual distant between a point and a set and given two sets of matrices $\mathcal{S}, \mathcal{W} \subseteq M_n$ we let $d(\mathcal{S}, \mathcal{W}) = \sup\{d(A, \mathcal{W}) : A \in \mathcal{S}\}$ denote the usual distance between sets.

Problem 1. *Does* $\lim_{j\to\infty} \sup_n d(\mathcal{S}_{n,j}(T), W^n(T)) = 0$ *for every* $T \in B(\mathcal{H})$*?*

This problem turns out to be equivalent to a problem about preserving what are called essential matrix ranges with compact perturbations.

I bring it up at this meeting because I believe that it could also be at the heart of some questions about quantum capacity. It is related to the following vague sort of question. Given a cp map $\Phi : M_n \to M_n$ if we can only have knowledge of $j \times j$ submatrices, with $j << n$, how well can we know the map?

Department of Mathematics, University of Houston, Houston, Texas 77204-3476, U.S.A.

E-mail address: vern@math.uh.edu

Best Constant in Norm Bounds on Commutators

Koenraad M.R. Audenaert
k.audenaert@imperial.ac.uk

September 18, 2007

1 Problem

Find the best constant c in the inequality

$$|| \, [X,Y] \, ||_2 \leq c \, ||X||_2 \, ||Y||_2, \tag{1}$$

where X and Y are arbitrary complex $d \times d$ matrices, $[X,Y]$ is their commutator $XY - YX$, and $||A||_2 = (\mathrm{Tr}[A^* A])^{1/2}$ is the Frobenius norm.

2 Background

Commutators come up almost everywhere, in diverse areas of mathematical physics, including quantum information theory. The actual answer to the above problem, the value of this best constant, is likely to be irrelevant for most applications of such bounds. Nevertheless it is quite an intruiging problem, since it is one of the simplest problems one can ask about commutators, and yet it has not been answered yet. The hope is that the tools used to solve it will provide additional handles on the structure of commutators, and may in this way be helpful to the solution of other problems involving them.

3 Partial Solution

It is well-known and easy to see that the inequality holds for $c = 2$. This is a straightforward application of the triangle inequality and submultiplicativity of unitarily invariant norms. In [2], A. Böttcher and D. Wenzel conjectured that, actually, $c = \sqrt{2}$ is the best constant (they only consider the real case, but the complex case most likely gives the same answer). One can certainly not do better, since $c = \sqrt{2}$ is achieved by two anti-commuting Pauli matrices. Say $X = \sigma_x$ and $Y = \sigma_z$, then $[X,Y] = -2i\sigma_y$, so that $||[X,Y]||_2 = 2||\sigma_y||_2 = 2\sqrt{2}$, while $||X||_2 = ||Y||_2 = \sqrt{2}$.

One of the matrices can be eliminated from the problem by regarding the matrices as vectors in a Hilbert space. Let $\mathrm{Vec}(X)$ be the operation that "stacks

the columns of X on top of each other", i.e. in terms of the standard matrix and vector basis elements, $\mathrm{Vec}(e^{ij}) = e^i \otimes e^j$. Then one easily sees that

$$\mathrm{Vec}([X,Y]) = (X \otimes \mathbb{1} - \mathbb{1} \otimes X^T)\,\mathrm{Vec}(Y).$$

Since the Frobenius norm has the special property that $||X||_2$ is equal to the Euclidian 2-norm $||.||_2$ of $\mathrm{Vec}(X)$, the norm inequality turns into

$$||(X \otimes \mathbb{1} - \mathbb{1} \otimes X^T)\,\mathrm{Vec}(Y)||_2 \leq c||X||_2\,||\,\mathrm{Vec}(Y)||_2.$$

The matrix Y can now be eliminated by noting that

$$\max_y \frac{||Ay||_2}{||y||_2} = ||A||,$$

where the maximisation is over all vectors and $||A||$ denotes the operator norm of A (largest singular value). Hence, an equivalent form of the problem is finding the best constant c in

$$||X \otimes \mathbb{1} - \mathbb{1} \otimes X^T|| \leq c\,||X||_2.$$

Known results are listed below:

1. When X is normal, the best c is indeed $\sqrt{2}$. Normality of X implies that X is unitarily diagonalisable. Thus there is a unitary U and diagonal Λ such that $UXU^* = \Lambda$. By unitary invariance of the operator norm and Frobenius norm, the inequality can then be converted to the diagonal case, which is an easy exercise to solve. Two proofs are presented in [2]. When X is not normal, one could try to exploit the singular value decomposition $X = U\Sigma V^*$, but the problem is that one cannot get rid of both U and V in the inequality.

2. When X and Y are real, $c \leq \sqrt{3}$; proven in [2].

3. When X and Y are real 2×2 matrices, or when one of the matrices is rank 1, $c = \sqrt{2}$; again, see[2].

4. When $X = Y^*$, $c = \sqrt{2}$; this case is due to Spiros Michalakis (unpublished).

A related problem is to see what happens when the right-hand side is based on other norms. It turns out that this gives rise to "boring" results. Given a UI norm $|||.|||$, one can define the corresponding Q-norm $||.||_Q$ by

$$||X||_Q := |||X^*X|||^{1/2}. \tag{2}$$

Theorem 1 *For general complex matrices X and Y, and for any UI norm $|||.|||$ with corresponding Q-norm $||.||_Q$, the following inequality holds:*

$$|||[X,Y]||| \leq 2||X||_Q||Y||_Q. \tag{3}$$

Proof. Follows from the triangle inequality and Hölder's inequality:

$$|||XY||| \leq ||| \, |X|^2 \, |||^{1/2} \; ||| \, |Y|^2 \, |||^{1/2}$$

see [1] (IV.42). QED

Despite the siicity of this derivation, the ensuing bound is sharp, as equality is obtained for X and Y two anticommuting Pauli operators. Take $X = \sigma_x$ and $Y = \sigma_z$, then $[X, Y] = -2i\sigma_y$, so that $|||[X, Y]||| = 2|||\mathbb{1}|||$ and $||X||_Q = ||Y||_Q = |||\mathbb{1}|||^{1/2}$.

For example, when applied to Schatten p-norms, this gives the bound

$$||[X, Y]||_p \leq 2||X||_{2p}||Y||_{2p}. \tag{4}$$

As a closing remark, one can replace X by $X + Z$ for any Z that commutes with Y, since this transformation does not change the commutator. It might, for example, make sense to replace X and Y by their traceless versions $X \mapsto X - \mathrm{Tr}(X)\mathbb{1}/d$.

References

[1] R. Bhatia, *Matrix Analysis*, Springer, Heidelberg (1997).

[2] A. Böttcher and D. Wenzel, "How big can the commutator of two matrices be and how big is it typically?", Lin. Alg. Appl. **403** (2005) 216–228.

Workshop on Operator Spaces and Group Algebras
at Banff International Research Station
August 19-24, 2007

Several aspects of amenability for groupoids

Claire Anantharaman-Delaroche

Abstract : We shall discuss various approaches of amenability for groupoids (mainly equivalence relations and group actions) and some applications. In particular we shall compare global and fiberwise amenability, and relate these notions to asymptotic properties of random walks on groupoids.

Real rank and stable rank of group C*-algebras

Rob Archbold

Abstract : We shall begin with a survey of results concerning real rank and stable rank for the C*-algebras associated with various classes of locally compact groups. In the second part of the talk, we shall describe recent results (joint with E. Kaniuth) on the real rank and stable rank of C*-algebras associated with compact transformation groups.

Operator algebraic rigidity of higher rank lattices

Bachir Bekka

Abstract : The following analogue of Margulis superrigidity theorem in the context of operator algebras was suggested by Connes and Jones. If Γ is a discrete group, view Γ as a subgroup of the unitary group $U(L(\Gamma))$ of its von Neumann algebra $L(\Gamma)$. Assume that Γ is a higher rank lattice. Let M a type II_1 factor and $U(M)$ its unitary group. Then every homomorphism $\pi : \Gamma \to U(M)$ with $\pi(\gamma)'' = M$ extends to a homomorphism $U(L(\Gamma)) \to U(M)$. As we will discuss, the answer is positive for arithmetic lattices like $SL_n(Z)$ for $n \geq 3$. As an application, the full C*algebra of this group has no faithful tracial state; this answers a question of Kirchberg in relation with Connes embedding problem.

Completely positive and completely bounded maps on Coxeter groups with applications

Marek Bożejko

Abstract : In our talk we present 2 classes of positive denite functions on Coxeter groups (W, S) with applications to constructions of a big class of operator spaces completely isomorphic with $R \cap C$. In this talk we give also the solution of Bessis-Moussa-Villani conjecture (BMV conjecture) for the generalized Gaussian random variables

$$G(f) = a(f) + a*(f),$$

Horn's inequalities and Connes' embbeding problem
Ken Dykema
(joint work with Benoit Collins)

Abstract : Connes embedding problem asks whether every separable II_1-factor can be embedded in the ultrapower of the hyperfinite II_1-factor; this is equivalent to asking whether every finite set in every II_1-factor has microstates. We relate this to questions concerning the possible spectral distributions of $a + b$, where a and b are self-adjoint elements in a II_1-factor having given spectral distributions. The finite-dimensional version of the spectral distribution question was solved by Klyatchko, Totaro, Knudson and Tao, in terms of inequalities first formulated by Horn.

Quantized Functional Analysis and Quantum Information Theory
Edward Effros

Abstract : For much of the Twentieth Century, the theory of quantum measurements consisted of various thought experiments which seemed remote from the real world. With the advent of devices that can manipulate individual photons and particles, this situation has drastically changed. Quantum channels are currently realizable both in and out of the laboratory. It is an ideal area for operator algebraists to gain a visceral feeling for the physics of quantum theory. Perhaps the most surprising mathematical aspect of QIT is the depth of the methods that are required. This is reflected in the fact that there are still unsolved problems at the most basic levels.

There have been some truly remarkable applications of quantized functional analysis to this area. This has been in part due to the remarkable work of Marius Junge and Mary Beth Ruskai. I will do my best to give a sketch of the physical and mathematical background for this new area.

Weak amenability of CAT(0) cubical groups
Erik Guentner

Abstract : A CAT(0) cubical complex is a complex in which the cells are Euclidean cubes, the attaching maps are isometries and the intrinsic metric satisfies the CAT(0) inequality. Basic examples are trees and Euclidean spaces. A group acting metrically properly on a CAT(0) cubical complex has the Haagerup property and it is natural to ask whether such a 'CAT(0) cubical group' is weakly amenable. In the talk we shall construct uniformly bounded representations of groups which admit a metrically proper action on a finite dimensional CAT(0) cubical complex. As a consequence, we can conclude that such groups are weakly amenable. The talk is based on joint work with Nigel Higson.