Operator structures in quantum information theory

Mary Beth Ruskai (Tufts University);
Marius Junge (Univeristy of Illinois); David Kribs (University of Guelph);
Patrick Hayden (McGill University); Andreas Winter (University of Bristol)

February 26 to March 2, 2012

1 Overview of the Field

Physicists have long recognized that the appropriate framework for quantum theory is that of a Hilbert space $\mathcal{H}$ and in the simplest case the algebra of observables is contained in $\mathcal{B}(\mathcal{H})$. This motivated von Neumann to develop the more general framework of operator algebras and, in particular C^*- algebras and W^*- algebras (with the latter also known as von Neumann algebras). In the 1970's these were used extensively in the study of quantum statistical mechanics and quantum field theory.

Although at the most basic level, quantum information theory (QIT) is expressed using matrix algebras, interactions with the environment play a critical role. This requires the study of open quantum systems in which the effects of noise can be studied. Operator spaces are used implicitly starting with the identification of completely positive (CP) trace-preserving maps (CPT maps) with quantum channels. During the past five years, the role of operator spaces has played an increasingly important and more explicit role.

In many situations, even when the underlying Hilbert space is finite dimensional, many interesting questions, particularly those involving channel capacity require asymptotic limits for infinitely many uses of the channel. In many situations, generic properties are important. Random matrices, free probability, and high dimensional convex analysis have all played an important role.

The first workshop on operator structures held at BIRS in February 2007, brought together experts in these areas and people working in quantum information theory. This was followed by a second workshop at the Fields Institute in July, 2010. The use of operator structures is now an integral component of work in QIT, as demonstrated in the presentations at this workshop.

Some of the major open questions in 2007, particularly the so-called "additivity conjecture" have now been solved, in part due to activity begun during that workshop. Nevertheless, many open questions remain and discussions of these questions were as important a component of this workshop as the presentation of recent developments. In view of the diverse interdisciplinary nature of the group, some expository talks were included and all speakers endeavored to make their talks accessible to this diverse group.

2 Major Topics of Discussion

2.1 Operator systems

In operator spaces, the role of norms plays a fundamental role. Recently, it has been recognized that structures in which order plays the central role are also important. These are known as operator systems. The workshop began with an expository talk by Vern Paulsen showing how this viewpoint provides a new perspective on such familiar topics as separable and entangled states using tensor products of operator spaces.

Graphs have long been used in QIT in a variety of ways, beginning with the concept of stabilizer states, used in quantum error correction and in one-way quantum computing. Winter's talk described recent work on "non-commutative graphs" which a quantum generalization of the Lovasz theta functions has important implications for the zero-error capacity problem. This can be framed in terms of operator systems and Hilbert modules.

2.2 Bell inequalities and quantum XOR games

Bell inequalities have long played a fundamental tool in distinguishing quantum correlations from classical ones. The ground-breaking paper [24] used techniques from operator spaces and tensor norms to resolve a long-standing open question in physics by showing that tripartite systems could have unbounded violations of Bell inequalities. Their work raised a number of open questions, including one about the form of the states which achieved these violations and showed that it could be framed as equivalent to a 30 year-old open question about Banach algebras. This was subsequently resolved by Briet et al [5]. This work also recognized that Bell inequalities could be viewed as a quantum analogue of XOR games in computer science. A series of talks on Thursday described the developments in this area, demonstrating the interplay between different viewpoints building on each other to provide striking progress on a series of complex questions.

The session about ”Bell inequalities and functional analysis techniques” was divided into four talks. The first one, given by David Perez-Garca, was an introduction to the topic. He spent most of the time motivating the interest of studying Bell inequalities, or equivalently multi prover one round games. He did it from a historical point of view, starting from the independent discovery of these objects in the foundations of quantum mechanics (Bell, 60's) and in the study of inapproximability results in computational complexity (Arora, Raz, 90's). He then moved into recent applications of this concept in a Quantum Information context: quantum key distribution, certifiable random number generation and position based quantum cryptography. In the last part of the talk, he sketched why tensor norms and operator spaces are the natural mathematical framework to deal with Bell inequalities.

The second talk, given by Carlos Palazuelos, focused on the recent use of operator spaces to analyze quantum multi prover one round games. He showed how, using a non-commutative version of Grothendieck's theorem, one can obtain interesting results for a particular type of these games (called rank-one games): first an efficient algorithm to approximate the value of this games to a constant precision; second, the lack of a perfect parallel repetition result in this context.

The third talk was given by Jop Briet. He presented a new proof (in collaboration with T. Vidick) of a result by Prez-Garca, Wolf, Palazuelos, Villanueva and Junge (2008) showing that there can exist unbounded violations to tripartite correlation Bell inequalities. The techniques were based on tensor norms and random estimates, as opposed to the operator space flavor of the original proof. With their new tools, they were able to improve the old result in all possible directions (smallest number of all parameters appearing in the problem), and even show the (almost) optimality of their result.

The fourth talk was given by Tobias Fritz. He presented a connection between some Bell inequality problems and some objects in operator algebra theory. This allowed him to reprove some known results (i.e about the semidefinite hierarchy of Navascus, Pironio and Acn) and to show a connection between Tsirelson problem and Connes embedding problem.

The participants liked a lot the way this session was developed and the smooth transition into talks, which helped non-experts in the area participate actively also in the lively discussions that took place during this session.

2.3 Reformulation of major conjectures in operator algebras

A major open question in operator algebras is known as the “Connes embedding problem” raised by Alain Connes [11] in the mid 70's. This problem has been extensively studied by operator algebraists, leading to a number of reformulations of the problem such as that of Kirchberg [20]. Recent work in quantum information theory [19] has connected it to other conjectures, including one known as Tsirelson's problem. A resolution of this problem would have deep implications in several areas of mathematics as discussed in the reviews [8, 22]

Because the original problem is somewhat technical, we focus on Tsirelson's question. Roughly speaking, this asks whether two commuting algebras of observables can always be represented as the tensor product of two algebras of observables. Because this question is closely connected to issues about non-locality which play a major role in QIT there has been a burst of interest in the Connes embedding problem from an entirely new direction, and new conjectures which have implications for this collection of problems. Some of these were discussed in the talk by Tobias Fritz.

A new and different reformulation of the problem was presented by Haagerup and Musat in their work on factorizable maps. Although this work originated in operator algebras, it has important implications for QIT. In particular, they showed that a question about unital quantum channels known as the asymptotic quantum Birkhoff conjecture (raised as an open question in the 2007 BIRS workshop) is false, by showing that it is false for any non-factorizable channel. They also described several new classes of unital quantum channels. And they resolved another long-standing open question by exhibiting a class of channels that are extreme points of the convex set of unital quantum channels which are not extreme points of either the set of unital CP maps or the set of trace-preserving CP maps.

Paulsen's talk concluded with a reformulation of the Connes embedding problem in the language of operator systems. He also gave a presentation in the open problems session with implications for this question.

2.4 Developments in LOCC

The set of protocols refereed to as LOCC (local operations and classical communication) play a major role in QIT and are usually described in terms of a physical process. A "local operation" is easily described as the tensor product of trace-decreasing CP maps on a tensor product space, for which it suffices to consider operations in which one term is the identity within a larger protocol. However, a proper description of "classical communication" is rarely given; it involves a pair of operations which can be written in the simplest case as

- a measurement is performed using a formal object called an "instrument" which records the outcome in a classical algebra

$$(\mathfrak{A} \otimes \mathcal{I})(\rho^{AB}) = \sum_k |\phi_k^A\rangle\langle\phi_k^A| \otimes |k\rangle\langle k| \otimes \rho_k^B = \bigoplus_k |\phi_k^A\rangle\langle\phi_k^A| \otimes \rho_k^B$$

- an operation $\mathfrak{B} = \bigoplus_k \mathfrak{B}_k$ conditioned on the classical algebra so that

$$(\mathcal{I} \otimes \mathfrak{B}) \circ (\mathfrak{A} \otimes \mathcal{I})(\rho^{AB}) = \bigoplus_k |\phi_k^A\rangle\langle\phi_k^A| \otimes \mathfrak{B}_k(\rho_k^B)$$

By contrast a separable operation is merely a sum of local operations

$$\sum_k \mathfrak{A}_k \otimes \mathfrak{B}_k$$

Although it has long been known that there are separable operations which are not LOCC, it is not at all trivial to provide examples of separable operations and show that they can not be rewritten as LOCC in some way.

Since orthogonal product states can always be distinguished by separable operations, the existence of an orthonormal basis of product states which can not be distinguished by LOCC leads to a special class of separable maps which do not come from LOCC operations. The first such example was given in [3]. Mancinska and Oozols present recent work [9] which gave a new and simpler proof of this result and resolved an open question raised in [3]. Their approach also leads to a new measure of non-locality.

Subsequently, they joined Chitambar and Winter [10] in a very nice clarification of the LOCC issues in precise mathematical terms, as well as a precise formulation of the use of a sequence of LOCC operations on multiple copies of a state in a process known as distillation. We anticipate that this will make the field more accessible to people working in operator algebras by enabling major questions to be stated in mathematical as well as physical language.

One session was devoted to an overview and discussion of the long-standing open question of whether NPT bound entanglement exists. If a bipartite state is separable, it is known the the partial transpose must be positive semi-definite, known as the PPT condition. However, it is also known that for $d > 2$ this is only a necessary, but not a sufficient condition for separability. And it is not possible to distill entanglement from entangled states which have this so-called PPT property. Such states are said to have bound entanglement. It is a long-standing open question as to whether or not states which are not PPT (called NPT) can always be distilled to a maximally entangled state. This question can be reformulated as one about positive maps on operator algebras. Thus, there was intense interest in this topic. The session began with an overview of the problem and what is known about it by Michael Horodecki, including some reformulations and related questions. John Watrous then explained [27] why there are states from which entanglement can be distilled from n copies of a state, although none can be distilled using fewer copies. This result demonstrates the difficulty of the analysis which would to resolve this question. The participants then engaged in a lively discussion about the problem until dinner.

2.5 Channels and capacity

Quantum Shannon theory is much richer than its classical counterpart because of the many different ways in which quantum systems can be used to transmit both classical and quantum information. Graeme Smith gave an overview of this subject. He explained how there were even situations in which the tensor product of a pair of channels with zero capacity could have non-zero capacity.

Because the capacity for transmission of quantum information can rarely be calculated exactly, obtaining good bounds is extremely important. Marius Junge explained how the completely bounded entropy can be used to obtain both upper and lower bounds on the capacity of certain types of channels.

Collins review recent results related to the study of the behavior of typical quantum channels, and techniques to study them, including free probability and Weingarten calculus. He described quantities related to additivity problems and discussed two different models of randomness: channels defined via Haar isometries and random unitary channels with i.i.d. Haar unitary operators.

In his thesis Renner introduced the concept of max- and min-entropy which proved to be very useful tools in quantum crytopgraphy. These quantities satisfy the usual properties of entropy and one can recover the von Neumann entropy as a limit; however, they are not smooth. Subsequently smoothed versions were introduced [26] which proved extremely useful, not only in cryptography, but in the study of channel capacity. However, all of these notions were defined only on matrix algebras.

Scholz gave an overview of these concepts and the issues involved in extending them to the more general setting of von Neumann algebras. Jencova in her talk discussed quantum channels defined between general finite dimensional C^*-algebras, and a related notion called "quantum combs" that has been utilized lately in the physics literature to describe quantum networks. Hayden outlined a conjecture of his on the approximation of operators on tensor product spaces, and the intersection of operator subspaces in particular, motivated by problems in multiuser quantum information theory.

2.6 Computational complexity

QIT arose from the realization that a quantum computer could solve certain types of problems more efficiently than classical computers. There is a large body of work discussing the various types of problems on which a quantum speed-up can be attained. This has led to new complexity classes for the different types of problems a quantum computer can solve.

The classical PCP theorem in computer science says, roughly speaking, that it is hard (in fact, NP-hard) to find approximate solutions to certain NP-complete problems such as SAT, even given a fairly weak sense of approximation. Matt Hastings explained this result and discussed the quantum PCP conjecture, which conjectures that approximation of certain quantum problems is even harder (so-called QMA-hard). He described a possible program for attacking the quantum PCP conjecture. This program involves showing results that forbid topological order in systems with certain interaction graphs, and it leads to some interesting conjectures in topology and C*-algebras.

Many optimization problems over polynomials are NP-hard to solve exactly, but can be approximated using methods such as the semi-definite programming (SDP) hierarchies of Lasserre, Parrilo, and others. Aram Harrow explained how explain how quantum techniques tools from QIT yield hardness results, as well as ways to prove the effectiveness of SDP hierarchies based on work in [16, 4].

2.7 Other

Other talks included Szkola's presentation on the construction of positive operator valued measures for detecting a true quantum state among a finite number of hypothetic ones. Her algorithm can be viewed as a quantum generalization of the maximum likelihood method to this setting, in that it recovers the classical rule in the special case of commuting states. Eisert discussed analysis of the timing of dissipative quantum processes that can be sometimes used to protect quantum information from noise. And Gross in his talk presented an analysis of the quantum time evolutions that can be realized in one-dimensional quantum lattice systems, showing there is a single invariant that takes a value in an abelian group which solves three basic classification problems for such systems.

3 Open Problems

The open problems session was chaired by Ruskai who began with a brief recap of problems from the 2007 meeting noting which had been solved and which remained open.

The following problems were presented. Some of the presenters wrote up the details, which are included in the Appendix below.

A) L. Macinskia and M. Ozols defined a measure of non-locality for an orthogonal set of vectors on a bipartite space, and explained its significance for state discrimination. Since the parameter is difficult to compute explicitly in most situations, a method for finding good bonds is an important open problem.

B) Vern Paulsen described a generalization of numerical range called the“j-th matrix range” of a matrix. It is an open question whether or not an associated limit as $j \to \infty$ is 0.

The question is important because it is equivalent to a long-standing open question about operator systems known as the Smith-Ward problem. It is rather surprising that there are equivalent formulations which reduce to questions about systems of dimension 2 or dimensions 3. Furthermore, these reformulations are conjectured to have implications for both the Connes embedding problem and Tsirelson's problem.

C) Andreas Winter raised questions about the Petz condition for sufficiency and equality in strong subadditivity. In particular, he asked for conditions under which one could obtain precise bounds for the decrease in monotonicity of the relative entropy under CPT maps. This has a number of important applications, including improving the bounds on the squashed entanglement described in Christandl's presentation on the work in [7]. Subsequently, this problem was solved by Li and Winter.

D) S. Szarek raise a question with arises in recent work [2] about the size of ancilla dimensions which lead to separable states. Related results about the ancilla dimensions for PPT states and class of states defined by another necessary condition for separability have recently appeared [**?**].

E) Aram Harrow described a question about the trace distance of certain recently defined families of states from the separable states.

F) David Perez-Garcia pointed out that recently proved existence theorems about unbounded violations of Bell inequalities do not give explicit bounds on the dimension required to obtain violations of a given size. Finding such bounds would have many important implications as indicated in Section **??**sect:Bell above.

G) Matthias Christandl raised the following question. A channel can be called PPT if its Choi-Jamiolkowski state is PPT. It is well-known that this is a necessary, but not sufficient condition for a channel to be entanglement breaking. Is the composition of two PPT channels entanglement breaking?

H) Arleta Szokla raised the following question during her talk.

The quantum extension of the Chernoff distance as well as its operational meaning within quantum binary hypothesis testing were provided a few years ago. These results were presented at the BIRS workshop in 2007 (07w5119). In the meantime, a quantum analogue of the multiple Chernoff distance has been considered as well. It is conjectured, that similarly to the binary special case, it represents an achievable bound on the error exponent in quantum multiple hypothesis testing. The conjecture has been proven for large classes of finite sets of quantum states (quantum hypotheses) giving a strong evidence in favor of the conjecture. However, a general proof is still missing. In contrast to the classical multiple hypothesis testing as well as the quantum binary special case, in multiple quantum hypothesis testing asymptotically optimal tests are not known explicitely. From mathematical point of view, quantum tests are represented by positive operator valued measures (POVM) corresponding to decompositions of identity into positive elements of a given *-algebra. The recently introduced quantum maximum likelihood type tests turn out to be asymptotically optimal under some technical restrictions on the set of hypothetic density operators. They were presented at this workshop and the potential of the corresponding construction algorithm to provide a general solution was been discussed as one of the open problems.

I) The Connes embedding conjecture, Tsirelson's problem and several reformulations and related questions were discussed in Section 2.3 above.

J) The NPT problem was discussed in Section 2.4 above.

K) The quantum PCP conjecture was the subject of Matt Hastings talk

In addition to these specific problems, many speakers included open questions in their talks.

A L. Macinskia and M. Ozols: A Problem on State Discrimination with LOCC

Consider a set of orthonormal vectors $S = \{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ in a bipartite vector space $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$.
Definition For any $a \in \mathrm{Pos}(\mathbb{C}^{d_A})$ and $b \in \mathrm{Pos}(\mathbb{C}^{d_B})$, let $G_{ij} := \langle\psi_i|(a \otimes b)|\psi_j\rangle$ where $i, j \in \{1, \dots, n\}$. We say that $\eta > 0$ satisfies *the nonlocality constraint for S* if

$$\eta \cdot \left(\frac{\max_k G_{kk}}{\sum_{j=1}^{n} G_{jj}} - \frac{1}{n} \right) \leq \max_{i \neq j} \frac{|G_{ij}|}{\sqrt{G_{ii} G_{jj}}} \tag{1}$$

holds for all $a \in \mathrm{Pos}(\mathbb{C}^{d_A})$ and $b \in \mathrm{Pos}(\mathbb{C}^{d_B})$ such that $G_{ii} > 0$ for all $i \in \{1, \dots, n\}$.

The above definition is significant due to the following theorem [9]

Theorem A.1. *Let $\eta > 0$ be any constant that satisfies the nonlocality constraint for S. Then any quantum protocol aiming to perfectly discriminate the states from S using only local quantum operations and classical communication (LOCC) errs with probability*

$$p_{\mathrm{error}} \geq \frac{2}{27} \frac{\eta^2}{n^5}. \tag{2}$$

Problem A.2. *For which sets of orthogonal vectors $S \subset \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ can one explicitly find an $\eta > 0$ satisfying the nonlocality constraint (particularly interesting is the case when S consists of orthogonal* product *vectors)? Only very few examples are known where an explicit value of $\eta > 0$ satisfying the nonlocality constraint has been found. Hence, besides a complete characterization even any new examples would be very useful. Especially useful are examples with large values of $\eta > 0$, since those translate into stronger lower bounds on the error probability (see the above theorem). Also it would be helpful to come up with a* general *approach for finding $\eta > 0$ satisfying the nonlocality constraint.*

Examples

1. *Standard basis.* When S is standard basis, no $\eta > 0$ satisfies the nonlocality constraint, since we can always choose matrices a, b to be trace one and diagonal with distinct diagonal elements. For such a and b, we have $|G_{ij}| = 0$ for all i, j but $\max_k G_{kk} > \frac{1}{n}$ and hence Equation (1) is not satisfied for any $\eta > 0$.

2. *Domino states.* Consider the following orthonormal product basis $S \subset \mathbb{C}^3 \otimes \mathbb{C}^3$, first introduced in [**?**]:

$$|\psi_1\rangle = |1\rangle|1\rangle, \tag{3}$$
$$|\psi_{2,3}\rangle = |0\rangle|0 \pm 1\rangle, \tag{4}$$
$$|\psi_{4,5}\rangle = |2\rangle|1 \pm 2\rangle, \tag{5}$$
$$|\psi_{6,7}\rangle = |1 \pm 2\rangle|0\rangle, \tag{6}$$
$$|\psi_{8,9}\rangle = |0 \pm 1\rangle|2\rangle, \tag{7}$$

   where $|i \pm j\rangle := (|i\rangle \pm |j\rangle)/\sqrt{2}$. In [9] it has been shown that $\eta = \frac{1}{8}$ satisfies the nonlocality constraint for S. In fact when $S \subset \mathbb{C}^3 \otimes \mathbb{C}^3$ is a set of orthogonal product states, a complete characterization of when there exists $\eta > 0$ satisfying the nonlocality constraint is known [13]. For these cases an explicit value of η that satisfies the nonlocality constraint has been given in citeCLMO .

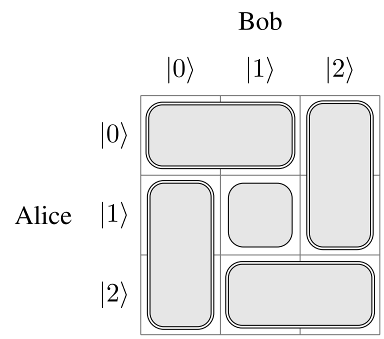

Figure 1: Graphical representation of the domino states.

B V. Paulsen: j-th numerical range

B.1 Statement of the problem

I will first state the problem and then discuss its ramifications.

Given an element T of a C*-algebra $\mathcal{A}$ the **j-th matrix range of T** is defined as the following set of $j \times j$ matrices:

$$W^j(T) = \{\Phi(T) : \Phi : \mathcal{A} \to M_j \text{ unital, completely positive } \}.$$

When $T \in M_n$ then by Stinespring's theorem, one sees that $W^j(T)$ consists of all $j \times j$ matrices that one can get by compressing the matrix $T \otimes I_E$ to a j-dimensional subspace.

The problem that we are interested in is:

How much does knowledge of $W^j(T)$ determine T or $W^n(T)$ for $n >> j$?

Precisely, let

$$W^{n,j}(T) = \{\sum_{k=1}^{K} A_k^* X_k A_k : X_k \in W^j(T), A_k \in M_{j,n}, \sum_{k=1}^{K} A_k^* A_k = I_n, \exists K\},$$

which is in some sense the $n \times n$ matrices that can be constructed as images under unital completely positive maps of elements of $W^j(T)$.

In fact $W^{n,j}(T)$ is the intersection of the sets $W^n(R)$ over all operators R, with $W^j(R) = W^j(T)$ and there is an operator R with $W^j(R) = W^j(T)$ such that $W^n(R) = W^{n,j}(T)$.

Now let

$$\alpha_{n,j} = \sup\{d(T, W^{n,j}(T)) : T \in M_n, \|T\| = 1\},$$

where $d(T, W^{n,j}(T)) = \inf\{\|T - Y\| : Y \in W^{n,j}(T)\}$ is the distance from T to the set $W^{n,j}(T)$. Thus, $\alpha_{n,j}$ is a measure of the maximum distance that an $n \times n$ matrix can be from $W^{n,j}(T)$ and gives us a measure of how little information about T is contained in $W^j(T)$.

Problem B.1. *Is* $\lim_{j \to +\infty}[\sup\{\alpha_{n,j} : n \geq j\}] = 0$*?*

B.2 Consequences

It seems very unlikely that this limit could be zero, but this is the only obstruction to settling a 30+ year old problem. On the other hand, requiring this limit to be zero is, essentially, a statement about, asymptotically, how well knowing all finite dimensional compressions of an operator gives knowledge of the operator. In that sense it fits quite well with some information theoretic questions.

The problem that determining the above limit would settle was motivated by the desire to generalize a result of Weyl.

Given a separable, infinite dimensional Hilbert space $\mathcal{H}$, let $B(\mathcal{H})$ denote the bounded operators on $\mathcal{H}$ and let $K(\mathcal{H})$ denote the compact operators on $\mathcal{H}$. Since the compact operators are an ideal there is also a quotient algebra, $B(\mathcal{H})/K(\mathcal{H}) = Q(\mathcal{H})$ often called the Calkin algebra. We let $\pi : B(\mathcal{H}) \to Q(\mathcal{H})$ denote the quotient map. When one talks about the **essential spectrum of an operator** T**,** they really mean the spectrum of $\pi(T)$.

Similarly, by the **essential j-th matrix range of T** we mean $W^j(\pi(T))$ the j-th matrix range of $\pi(T)$.

Weyl proved that given any $T \in B(\mathcal{H})$ there exists a compact operator $K \in K(\mathcal{H})$ such that $W^1(T + K) = W^1(\pi(T))$.

Smith-Ward extended this result by proving that given any j there is $K_j \in K(\mathcal{H})$ such that

$$W^k(T + K_j) = W^k(\pi(T)), 1 \leq k \leq j.$$

The Smith-Ward problem asks: Does there always exists $K \in K(\mathcal{H})$ such that $W^J(T+K) = W^j(\pi(T))$ holds for all j?

The answer is yes for many operators T but is unknown in general.

Here is the connection between the Smith-Ward problem, the above problem and other questions.

First, given $T \in B(\mathcal{H})$, let $\mathcal{S}^{n,j}(T) = \{A \in M_n : W^j(A) \subseteq W^j(T)\}$. It turns out that $\mathcal{S}^{n,j}(T) = \cup\{W^n(R) : W^j(R) = W^j(T)\}$ where the union is over all such operators R and in fact, there is always an operator R such that $W^j(R) = W^j(T)$ and $\mathcal{S}^{n,j}(T) = W^n(R)$.

Theorem B.2. *The following are equivalent:*

1. *The Smith-Ward problem has an affirmative answer,*
2. $\lim_{j\to+\infty} \sup\{\alpha_{n,j} : n \geq j\} = 0,$
3. *for every* $T \in B(\mathcal{H})$, $\lim_{j\to+\infty}[\sup\{d(\mathcal{S}^{n,j}(T), W^n(T)) : n \geq j\}] = 0,$
4. *for every 3 dimensional operator system* $\mathcal{S}$ *and every UCP map* $\phi : \mathcal{S} \to Q(\mathcal{H})$ *there exists a UCP map* $\psi : \mathcal{S} \to B(\mathcal{H})$ *such that* $\pi \circ \psi = \phi$,
5. *for every 3 dimensional operator system* $\mathcal{S}$, *for every C*-algebra* $\mathcal{A}$, *for every two-sided ideal* $J \subseteq \mathcal{A}$, *for every UCP map* $\phi : \mathcal{S} \to \mathcal{A}/J$ *there exists a UCP map* $\psi : \mathcal{S} \to \mathcal{A}$ *such that* $\pi \circ \psi = \phi$.

Statements (4) and (5) are known to be true for every *two* dimensional operator system and there are *four* dimensional operator systems for which (4) and (5) are known to be false. So the Smith-Ward problem is the only remaining dimension.

Similarly, in the theory of operator spaces, there are lifting properties known to hold for all one dimensional operator spaces, to fail for three dimensional operator spaces, but the case of two dimensional operator spaces is trickier. This shift in dimension comes about from the need to make operator spaces into operator systems. In particular, it is known that Pisier's OH(n) is not exact for every $n \geq 3$, but it is open for $n = 2$, which is the case needed for the Smith-Ward problem.

B.3 Why should I care?

Requiring the limit in Problem 1 to be zero is, essentially, a statement about, asymptotically, how well knowing all finite dimensional compressions of an operator gives knowledge of that operator. In that sense it fits quite well with some information theoretic questions and likely has some equivalent interpretations in that language.

Maybe not so surprisingly, the Smith-Ward problem has subtle connections with Connes embedding problem, a.k.a., the Tsirelson problem.

Here are two not too outlandish conjectures.

Conjecture 1: If Connes' embedding is true, then Smith-Ward is true.

After all, both reduce to asymptotic questions about finite dimensional approximations. Thus, if one could show that this conjecture is true and that the limit in the first problem is not zero, then that would give a route to showing that Connes' embedding is false.

Conjecture 2: Assuming that Connes' embedding is true and that Smith-Ward is true leads to a contradiction.

Our recent work almost proves this second conjecture. If, indeed, the Smith-Ward problem has an information theoretic interpretation, then this would give an example of Tsirelson being true implying the violation of something.

C Andreas Winter

See [21].

D S. Szarek: Almost sure entanglement of induced states.

Let $\mathcal{H}$ be an n-dimensional Hilbert space, $\mathcal{H}_a$ an ancilla space of dimension s, and let ψ be a (random) unit vector uniformly distributed on the sphere of $\mathcal{H} \otimes \mathcal{H}_a$. Then $\rho = \mathrm{tr}_{\mathcal{H}_a} |\psi\rangle\langle\psi|$ is a (random) induced state on $\mathcal{H}$. If, further, $n = d^2 > 1$ and $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$, one may ask whether ρ is typically entangled, PPT etc., with respect to this particular splitting.

It has been known since 2006 [17, 1] that, for large d, ρ is typically (i.e., with probability close to 1) separable if s/d^4 is sufficiently large and typically entangled if $s = d^2$. More recently, it has been established in [3] that a fairly sharp transition from "generic entanglement" to "generic separability" occurs when s is, up to a logarithmic factor, of order d^3. Here we ask a related question:

For which ancilla dimensions is the probability of separability exactly zero?

Partial results in this direction are listed in section 7.1 of [2] (where the reader is referred for further details on what follows). As pointed out there, it follows from known facts that the above happens when $s \leq (d-1)^2$, while for $s \geq d^2$ the probability in question is strictly between 0 and 1. However, determining the *precise* threshold for almost sure entanglement seems to require a new idea, and perhaps more than one idea: in the case $d = 2$ the transition occurs when s increases from 2 to 3, with the reasons for almost sure entanglement when $s = 2$ and for non-zero probability of separability when $s = 3$ being quite different. Actually, it is not right away clear that there *is* a threshold: while it is elementary to show that, for a fixed s, the probability of separability is a nonincreasing function of d (Lemma 4.3 in [3]), its monotonicity with respect to s (for fixed d) is not immediately apparent (at least to the authors of [3]) and would also be interesting to establish. However, the weaker property needed for the existence of a threshold (i.e., almost sure entanglement for given d, s_0 implies almost sure entanglement for the same d and all $s < s_0$) is relatively easy to show.

E Harrow

In [12] Doherty, Parrilo and Spedalieri gave a family of relaxations of the set of separable states (denoted Sep). The k'th level of their hierarchy yields the set of density matrices ρ^{AB} that can be extended to $\sigma^{AB_1 \cdots B_k}$ where $\rho^{AB} = \sigma^{AB_1}$, $\sigma^{B_1 \cdots B_k}$ is supported on the symmetric subspace and σ is PPT across all partitions. Call this set DPS(k).

The open question is to determine the maximum trace distance of an element of DPS(k) from Sep. It is known from [23] that if each subsystem has dimension d, then this distance is at most $O((d/k)^2)$. But is this tight? Do there exists states in DPS(k) that are far from Sep whenever $k < d$?

It is known that the antisymmetric Werner state on d by d dimensions is (d-1)-extendable and is far from Sep, but this state is not PPT. It is also known (from the original DPS paper) that there exist, for any d and k, states which are is DPS(k), but not Sep; however, no nonzero lower bound is known on the distance. Finally, the construction of [7] can give a state on d dimensions that is in DPS(log d) and is far from separable. So the optimal value of k can be anywhere between O(log d) and O(d).

References

[1] G. Aubrun and S. J. Szarek, Tensor products of convex sets and the volume of separable states on N qudits. *Phys. Rev. A* **73** (2006) 022109.

[2] G. Aubrun, S. Szarek and D. Ye, Entanglement thresholds for random induced states. arXiv:1106.2264.

[3] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A* **59** (1999), 1070–1091

[4] Boaz Barak, Fernando G.S.L. Brando, Aram W. Harrow, Jonathan A. Kelner, David Steurer, Yuan Zhou , Hypercontractivity, Sum-of-Squares Proofs, and their Applications arXiv:1205.4484

[5] Jop Brit, Harry Buhrman, Ben Toner A generalized Grothendieck inequality and entanglement in XOR games arXiv:0901.2009

[6] Jop Briet, Thomas Vidick, Explicit lower and upper bounds on the entangled value of multiplayer XOR games arXiv:1108.5647

[7] squashed entanglement

[8] Valerio Capraro, A Survey on Connes' Embedding Conjecture, arXiv:1003.2076

[9] Andrew M. Childs, Debbie Leung, Laura Mancinska, Maris Ozols, A framework for bounding nonlocality of state discrimination arXiv:1206.5822

[10] Eric Chitambar, Debbie Leung, Laura Mancinska, Maris Ozols, Andreas Winter Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask) arXiv:1210.4583

[11] A. Connes, Classification of injective factors, *Ann. of Math.* **104** (1976), 73-115.

[12] , Doherty, Parrilo and Spedalieri (DPS) quant-ph/0308032

[13] Y. Feng and Y. Shi. Characterizing locally indistinguishable orthogonal product states. *IEEE Trans. Inf. Theor.* **55** (2009) 2799–2806.

[14] Tobias Fritz arXiv:1008.1168 [pdf, ps, other] Tsirelson's problem and Kirchberg's conjecture *Rev. Math. Phys.* **24**, (2012) 1250012.

[15] D. Gross, V. Nesme, H. Vogts, R.F. Werner, Index theory of one dimensional quantum walks and cellular automata *Commun. Math. Phys.* **310**, 419-454 (2012) arXiv:0910.3675

[16] Aram W. Harrow, Ashley Montanaro Testing product states, quantum Merlin-Arthur games and tensor optimisation arXiv:1001.0017

[17] P. Hayden, D. Leung and A. Winter, Aspects of generic entanglement. *Comm. Math. Phys.* **265** (2006) 95-117.

[18] Unbounded violations of bipartite Bell Inequalities via Operator Space theory arXiv:0910.4228

[19] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, R. F. Werner Connes' embedding problem and Tsirelson's problem *J. Math. Phys.* **52** 012102 (2011) arXiv:1008.1142

[20] E. Kirchberg, On semi-split extensions, tensor products and exactness of group C^*- algebras, *Inv. Math.* **112** (1993), 449-489.

[21] Ke Li, Andreas Winter, Relative entropy and squashed entanglement arXiv:1210.3181

[22] Ozawa, About the QWEP conjecture, *Intern. J. Math.* **15** (2004), 501-530.

[23] (Navascues, Owari and Plenio) arxiv: 0906.2731

[24] D. Perez-Garcia, M.M Wolf, C. Palazuelos, I. Villanueva, M. Junge Unbounded violation of tripartite Bell inequalities *Comm. Math. Phys.* **279**, 455 (2008) arXiv:quant-ph/0702189

[25] Renato Renner Security of Quantum Key Distribution arXiv:quant-ph/0512258

[26] Marco Tomamichel, Roger Colbeck, Renato Renner Duality Between Smooth Min- and Max-Entropies *IEEE Trans. on Inf. Theory* **56** (2010), 4674-4681 arXiv:0907.5238

[27] John Watrous, Many copies may be required for entanglement distillation arXiv:quant-ph/0312123